



Versão atual do XenMobile Server

Contents

Notas de versão de patches contínuos	3
Notas de versão do Patch contínuo 4 do XenMobile Server 10.13	3
Notas de versão do Patch contínuo 8 do XenMobile Server 10.12	4
Notas de versão do Patch contínuo 3 do XenMobile Server 10.13	5
Novidades no XenMobile Server 10.13	5
Novidades no XenMobile Server 10.12	17
Novidades no XenMobile Server 10.11	26
Avisos de terceiros	37
Substituição	37
Problemas resolvidos	51
Problemas conhecidos	53
Arquitetura	53
Requisitos do sistema e compatibilidade	56
Compatibilidade do XenMobile	60
Sistemas operacionais compatíveis de dispositivos	62
Requisitos de porta	64
Escalabilidade e desempenho	73
Licenciamento	77
Conformidade com FIPS 140-2	83
Suporte a idiomas	84
Instalar e configurar	86
Configurar o modo FIPS com o XenMobile	101
Configurar o clustering	104

Guia de recuperação de desastres	115
Ativar servidores proxy	116
Configurar SQL Server	119
Propriedades do servidor	122
Opções da interface de linha de comando	138
Introdução aos fluxos de trabalho para o console XenMobile	154
Certificados e autenticação	158
Citrix Gateway e XenMobile	174
Configure autenticação de domínio ou de domínio de segurança	184
Autenticação de certificado cliente ou certificado e domínio	192
Entidades PKI	215
Provedores de credenciais	243
Certificados APNs	251
SAML para logon único com Citrix Files	260
Azure Active Directory como IdP	270
Credenciais derivadas	282
Atualização	302
Contas de usuário, funções e registro	307
Perfis de registro	324
Configurar funções com RBAC	329
Notificações	351
Dispositivos	363
ActiveSync Gateway	372
Migrar do Device Administration para o Android Enterprise	375

Android Enterprise	381
Distribuir aplicativos Android Enterprise	506
Clientes do Android Enterprise herdado para Google Workspace (anteriormente G Suite)	534
iOS	573
macOS	593
Registro em massa de dispositivos Apple	600
Propriedades do cliente	608
Implantar dispositivos através do Programa de Implantação da Apple	619
Registrar dispositivos	631
Firestore Cloud Messaging	652
Integração com os recursos do Apple Educação	656
Distribuir aplicativos da Apple	695
Controle de Acesso da Rede	724
Samsung Knox	730
Registro em massa do Samsung Knox	733
Ações de segurança	739
Dispositivos compartilhados	754
XenMobile AutoDiscovery Service	759
Políticas de dispositivo	765
Políticas de dispositivo por plataforma	785
Política de dispositivo de espelhamento de AirPlay	787
Política de dispositivo do AirPrint	790
Política de configurações gerenciadas do Android Enterprise	791
Permissões do aplicativo Enterprise Android	802

Política de dispositivo do APN	804
Política de dispositivo de acesso aos aplicativos	807
Política de dispositivo de atributos de aplicativo	807
Política de dispositivo de configuração de aplicativo	808
Política de dispositivo de inventário de aplicativos	810
Política de dispositivo de bloqueio de aplicativo	811
Política de dispositivo de uso de rede de aplicativos	814
Política de dispositivo de notificações de aplicativo	815
Política de dispositivo de restrições de aplicativo	816
Política de dispositivo de encapsulamento de aplicativo	817
Política de dispositivo de desinstalação de aplicativo	820
Política de dispositivo de restrições de desinstalação de aplicativo	822
Política de dispositivo de atualizar automaticamente aplicativos gerenciados	822
Política de dispositivo BitLocker	823
Política de dispositivo de navegador	828
Política de dispositivo de calendário (CalDav)	829
Política de dispositivo celular	830
Política de dispositivo do gerenciador de conexões	831
Política de dispositivo de agendamento de conexão	832
Política de dispositivo de contatos (CardDAV)	834
Política de dispositivo Controlar atualizações do sistema operacional	836
Política de dispositivo Copiar aplicativos para o contêiner da Samsung	841
Política de dispositivo de credenciais	841
Política de dispositivo de XML personalizado	848

Política de dispositivo do Defender	850
Política de dispositivo de excluir arquivos e pastas	851
Política de dispositivo Excluir chaves e valores do Registro	851
Política de dispositivo de Atestado de Integridade de Dispositivo	852
Política de dispositivo de nome do dispositivo	853
Política de dispositivo Configuração de Educação	854
Política de dispositivo do Hub Empresarial	857
Política de dispositivo do Exchange	858
Política de dispositivo de arquivo	866
Política de dispositivo FileVault	869
Política de dispositivo de fonte	871
Política de dispositivo de layout de tela inicial	872
Política de dispositivo de importação do perfil de iOS e macOS	874
Política de dispositivo de gerenciamento de keyguard	875
Política de dispositivo do quiosque	879
Política de dispositivos de configuração de Launcher para Android	883
Política de dispositivo do LDAP	884
Política de dispositivo de localização	886
Política de dispositivo de email	893
Política de dispositivo de domínios gerenciados	896
Políticas de dispositivo das opções de MDM	898
Política de dispositivo de informação da organização	899
Política de dispositivo de código secreto	900
Política de dispositivo do ponto de acesso pessoal	914

Política de dispositivo de remoção de perfil	914
Política de dispositivo do perfil de provisionamento	916
Política de dispositivo da remoção de perfil de provisionamento	917
Política de dispositivo de proxy	917
Política de dispositivo do Registro	919
Suporte remoto à política de dispositivo	920
Política de dispositivo de restrições	921
Política de dispositivo em roaming	972
Política de dispositivo de chave de licença MDM Samsung	973
Política de dispositivo de firewall do Samsung SAFE	975
Política de dispositivo do SCEP	976
Siri e políticas de ditado	981
Políticas de dispositivo de conta SSO	982
Política de dispositivo de criptografia de armazenamento	984
Política de dispositivo de loja	985
Política de dispositivo de Calendários inscritos	985
Política de dispositivo dos termos e condições	986
Política de dispositivo de VPN	987
Política de dispositivo de papel de parede	1036
Política de dispositivo de filtro de conteúdo Web	1037
Política de dispositivo de clip web	1039
Política de dispositivo Wi-Fi	1041
Política de dispositivo do certificado do Windows CE	1055
Política de dispositivo Proteção de informações do Windows	1056

Políticas de dispositivo das opções de XenMobile	1061
Política de dispositivo de desinstalação do XenMobile	1065
Adicionar aplicativos	1065
Tipos de conector de aplicativo	1106
Atualizar aplicativos MDX ou empresariais	1107
Citrix Launcher	1109
Compra por volume da Apple	1112
Aplicativos e áreas de trabalho virtuais através do Citrix Secure Hub	1115
Usar Citrix Content Collaboration com XenMobile	1116
SmartAccess para aplicativos HDX	1132
Adicionar mídia	1151
Implantar recursos	1155
Macros	1170
Ações automatizadas	1201
Monitoração e suporte	1209
Anonimizar dados nos pacotes de suporte	1212
Verificações de conectividade	1213
Programa de Melhoria de Experiência do Cliente	1216
Logs	1218
Provedor de serviços móveis	1225
Relatórios	1226
SNMP monitoring	1231
Pacotes de suporte	1240
Opções de suporte e suporte remoto	1250

Syslog	1258
Exibir arquivos de log no XenMobile	1259
Ferramenta XenMobile Analyzer	1261
APIs REST	1277
Conector de Endpoint Management para Exchange ActiveSync	1279
Conector Citrix Gateway para Exchange ActiveSync	1332
Conceitos avançados	1348
Interação do XenMobile no local com o Active Directory	1348
Implantação do XenMobile	1353
Modos de gerenciamento	1354
Requisitos de dispositivo	1362
Segurança e experiência do usuário	1363
Aplicativos	1382
Comunidades do usuário	1390
Estratégia de email	1398
Integração do XenMobile	1407
Requisitos para vários locais	1416
Integração com Citrix Gateway e Citrix ADC	1418
Considerações sobre SSO e proxy para aplicativos MDX	1429
Autenticação	1434
Arquitetura de referência para implantações locais	1450
Propriedades do servidor	1461
Políticas de dispositivos e aplicativos	1464
Opções de registro do usuário	1476

Ajuste das operações do XenMobile	1480
Provisionamento e desprovisionamento de aplicativos	1488
Operações baseadas em painel	1491
Controle de Acesso Baseado em Função e Suporte XenMobile	1493
Monitoramento de sistemas	1496
Recuperação de desastres	1503
Processo de Suporte Citrix	1507
Enviar convites para registro em grupo no XenMobile	1508
Configurar um servidor de atestado de integridade de dispositivo no local	1510
Configurar a autenticação baseada em certificado com o EWS para notificações por push do Secure Mail	1521
Integrar o Gerenciamento de Dispositivos Móveis (MDM) XenMobile com o Cisco Identity Services Engine (ISE)	1525

Notas de versão de patches contínuos

August 20, 2021

Esta seção contém as notas de versão de patches contínuos recentes do XenMobile Server. Clique em um link abaixo para visualizar os problemas corrigidos e conhecidos, as alterações em recursos e as ações necessárias.

O patch contínuo mais recente contém todas as correções dos patches contínuos anteriores para a mesma versão.

Notas de versão de patches para a versão atual	Data de publicação
10.13 Patch contínuo 4	11 de agosto de 2021
10.13 Patch contínuo 3	13 de maio 2021
10.13 Patch contínuo 2	25 de fevereiro 2021
10.13 Patch contínuo 1	8 de janeiro 2021

Notas de versão de patches para versões anteriores	Data de publicação
10.12 Patch contínuo 8	2 de junho 2021
10.12 Patch contínuo 7	29 de março 2021
10.12 Patch contínuo 6	26 de janeiro 2021
10.11 Patch contínuo 7	18 de novembro 2020
10.10 Patch contínuo 6	22 de julho 2020

Notas de versão do Patch contínuo 4 do XenMobile Server 10.13

August 20, 2021

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos no Patch contínuo 4 do XenMobile Server 10.13.

Novidades

Para obter informações sobre patches contínuos anteriores do XenMobile Server 10.13.0, consulte [Notas de versão de patches contínuos](#).

Problemas resolvidos

- A propriedade de servidor `ios.mdm.apns.connectionPoolSize` fica oculta quando você muda para a API baseada em HTTP/2 para APNs. [CXM-95479]
- No XenMobile Server versão 10.12, você não pode modificar as propriedades do VPP em determinados aplicativos. [CXM-96854]
- Os aplicativos da Web necessários não são instalados automaticamente em dispositivos apenas MDM. [CXM-97477]
- No XenMobile Server versão 10.13, quando você configura o servidor proxy sob a **CLI**, não é possível enviar notificações para o Secure Hub em execução em dispositivos iOS. [CXM-97807]
- No XenMobile Server versão 10.13, você recebe um erro ao acessar os **detalhes do dispositivo**. Esse erro ocorre quando a propriedade do dispositivo tem um valor em ”“. [CXM-97951]

Notas de versão do Patch contínuo 8 do XenMobile Server 10.12

June 15, 2021

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos no Patch contínuo 8 do XenMobile Server 10.12.

Novidades

Renovação de certificado APNs do Secure Hub. O certificado APNs (Apple Push Notification Service) do Secure Hub para XenMobile Server 10.12 expira em 17 de junho de 2021. Esta atualização renova o certificado APNs do Secure Hub, que expirará em 7 de maio de 2022. [CXM-94513]

Problemas resolvidos

- Logo após registrar um dispositivo executando o macOS 10.14+, as propriedades do dispositivo nem sempre são preenchidas no console XenMobile Server. Depois que o dispositivo reiniciar, as propriedades do dispositivo aparecem como esperado. [CXM-94221]
- No XenMobile Server 10.12, o ShareFile falha intermitentemente ao estabelecer uma conexão. [CXM-95419]

Notas de versão do Patch contínuo 3 do XenMobile Server 10.13

May 24, 2021

Estas notas de versão descrevem aprimoramentos e problemas corrigidos e conhecidos no Patch contínuo 3 do XenMobile Server 10.13.

Novidades

Renovação de certificado APNs do Secure Hub. O certificado APNs (Apple Push Notification Service) do Secure Hub para XenMobile Server 10.13 expira em 17 de junho de 2021. Esta atualização renova o certificado APNs do Secure Hub, que expirará em 7 de maio de 2022. [CXM-94070]

Porta alternativa para notificações APNs. O XenMobile Server agora é compatível com o uso da porta 2197 como alternativa à porta 443. Você usa a porta 2197 para enviar notificações APNs e recebe feedback de `api.push.apple.com`. A porta usa a API do provedor APNs baseada em HTTP/2. O valor padrão da propriedade do servidor `apns.http2.alternate.port.enabled` é **false**. Para usar a porta alternativa, atualize a propriedade do servidor e reinicie o servidor. [CXM-93911]

Problemas resolvidos

Logo após registrar um dispositivo executando o macOS 10.14+, as propriedades do dispositivo nem sempre são preenchidas no console XenMobile Server. Depois que o dispositivo reiniciar, as propriedades do dispositivo aparecem como esperado. [CXM-94150]

Se você ativar as configurações **Ativar aplicativos do sistema** e **Desativar aplicativos** para o mesmo aplicativo na política de Restrições, o aplicativo aparece no perfil de trabalho. [CXM-94097]

Quando você adiciona usuários SNMP ao console XenMobile Server, os usuários não aparecem na lista **Usuários de monitoramento SNMP**, ou os agentes de SNMP ficam inativos. [CXM-93199]

No XenMobile Server, as verificações de conectividade do NetScaler Gateway não exibem um resultado. [CXM-93134]

No console XenMobile Server, a data de expiração correta do certificado raiz não é exibida. [CXM-93133]

Novidades no XenMobile Server 10.13

August 20, 2021

Suporte continuado para as políticas clássicas preterido do Citrix ADC

A Citrix anunciou recentemente a substituição de alguns recursos baseados em políticas clássicas, começando com o Citrix ADC 12.0 compilação 56.20. Os avisos de substituição do Citrix ADC não têm impacto nas integrações existentes do XenMobile Server com o Citrix Gateway. O XenMobile Server continua a oferecer suporte às políticas clássicas e nenhuma ação é necessária.

Serviço de migração do XenMobile

Se você estiver usando o XenMobile Server no local, nosso Serviço de Migração do XenMobile gratuito pode ajudá-lo a começar a usar o Endpoint Management. A migração do XenMobile Server para o Citrix Endpoint Management não exige que você registre novamente os dispositivos.

Para iniciar a migração, entre em contato com um fornecedor Citrix local ou um parceiro Citrix. Consulte [Serviço de migração do XenMobile](#).

Anúncios de substituição

Para receber um aviso prévio dos recursos do Citrix XenMobile que estão sendo eliminados, consulte [Substituição](#).

Antes de atualizar endpoints para iOS 14.5

A Citrix recomenda que antes de atualizar qualquer endpoint para o iOS 14.5, você execute as seguintes ações para mitigar falhas no aplicativo:

- Atualize o Citrix Secure Mail e o Secure Web para 21.2.X ou superior. Consulte [Atualizar aplicativos MDX ou empresariais](#).
- Se você usar o MDX Toolkit, prepare todos os aplicativos iOS de terceiros com o MDX Toolkit 21.3.X ou superior. Verifique a [página de download](#) do MDX Toolkit para a versão mais recente.

Antes de atualizar um Citrix ADC no local

A atualização de um Citrix ADC local para determinadas versões pode resultar em um erro de logon único. O logon único no Citrix Files ou na URL do domínio ShareFile em um navegador com a opção **Logon de funcionário da empresa** resulta em um erro. O usuário não consegue fazer logon.

Para dar uma solução temporária, se você ainda não tiver executado o seguinte comando da CLI do ADC no Citrix Gateway, execute-o para habilitar o logon único global:

```
1 `set vpn parameter SS0 ON`  
2 `bind vpn vs <vsName> -portalTheme X1`
```

Para obter mais informações, consulte:

- [Citrix ADC Release \(Feature Phase\) 13.0 Build 67.39/67.43](#)
- [Configurações de logon único impactadas](#)

Depois de concluir a solução alternativa, os usuários podem se autenticar no Citrix Files ou no URL do domínio do ShareFile usando o SSO em um navegador com a opção Login de funcionário da empresa. [CXM-88400]

Antes de atualizar para o XenMobile 10.13 (no local)

Alguns requisitos de sistemas mudaram. Para obter informações, consulte [Requisitos do sistema e compatibilidade](#) e [Compatibilidade do XenMobile](#).

1. Se a máquina virtual que executa o XenMobile Server que deve ser atualizado tiver menos de 8 GB de RAM, recomendamos aumentar a RAM para pelo menos 8 GB.
2. Atualize o seu Citrix License Server para 11.16 ou posterior antes de atualizar para a versão mais recente do XenMobile Server 10.13.

A versão mais recente do XenMobile exige o Citrix License Server 11.16 (versão mínima).

Nota:

A data do Customer Success Services (anteriormente, data de Subscription Advantage) no XenMobile 10.13 é 29 de setembro de 2020. A data do Customer Success Services na sua licença Citrix deve ser posterior a essa data.

Você pode ver a data ao lado da licença do servidor de licenças. Se você conectar a versão mais recente do XenMobile a um ambiente de servidor de licenças mais antigo, a verificação de conectividade falhará e você não poderá configurar o servidor de licenças.

Para renovar a data na sua licença, baixe o último arquivo de licença do Portal Citrix e carregue o arquivo para o Servidor de Licença. Consulte [Customer Success Services](#).

3. Para um ambiente em cluster: as implantações de aplicativos e políticas do iOS para dispositivos que executam o iOS 11 e posterior têm o seguinte requisito. Se o Citrix Gateway estiver configurado para persistência de SSL, você deve abrir a porta 80 em todos os nós do XenMobile Server.
4. Recomendação: Antes de instalar uma atualização do XenMobile, use a funcionalidade na sua VM para tirar um instantâneo do seu sistema. Além disso, faça backup do seu banco de dados de configuração do sistema. Se tiver problemas durante uma atualização, backups completos permitirão fazer uma recuperação.

Para atualizar

Com esta versão, o XenMobile oferece suporte ao VMware ESXi 7.0. Certifique-se de atualizar para 10.13 antes de instalar ou atualizar para ESXi 7.0.

Você pode atualizar diretamente do XenMobile 10.11.x ou 10.12.x para o XenMobile 10.13. Para realizar a atualização, baixe o binário mais recente disponível: acesse <https://www.citrix.com/downloads>. Navegue para **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**. No bloco do software XenMobile Server, para o seu hipervisor, clique em **Download File**.

Use a página **Gerenciamento de versão** no console XenMobile. Consulte [Para atualizar usando a página Gerenciamento de versão](#).

Depois de atualizar

Se a funcionalidade que envolve as conexões de saída deixar de funcionar e você não alterou a configuração de suas conexões, verifique os erros no log do XenMobile Server, como os seguintes: “Não é possível se conectar ao servidor VPP: o nome do host ‘192.0.2.0’ não corresponde à entidade do certificado fornecido pelo par”.

- O erro de validação do certificado significa que você deve desabilitar a verificação do nome do host no XenMobile Server.
- Como padrão, a verificação do nome do host está ativada nas conexões de saída, exceto para o servidor Microsoft PKI.
- Se a verificação do nome do host interromper sua implantação, altere a propriedade do servidor `disable.hostname.validation` para **true**. O valor padrão dessa propriedade é **false**.

Atualizações de suporte a plataformas

- **iOS 14:** os aplicativos móveis de produtividade Citrix e o XenMobile Server são compatíveis com o iOS 14, mas atualmente não são compatíveis com nenhum dos novos recursos do iOS 14. O MDX Service não suporta preparar aplicativos iOS para iOS 14. Use o MDX Toolkit 20.8.5 ou posterior.
- **Android 11:** o XenMobile Server suporta o Android 11. Para obter informações sobre como a substituição das APIs do Google Device Administration afeta dispositivos que executam o Android 10+, consulte [Migrar do Device Administration para o Android Enterprise](#). Veja também este [blog da Citrix](#).

Configurar vários modos de gerenciamento de dispositivos e aplicativos em um único ambiente

Agora você pode configurar um único site do XenMobile para oferecer suporte a várias configurações de registro. A função dos perfis de registro foi expandida para incluir configurações de registro para o gerenciamento de dispositivos e aplicativos.

Os perfis de registro oferecem suporte a vários casos de uso e caminhos de migração de dispositivos em um único console XenMobile. Os casos de uso incluem:

- Gerenciamento de Dispositivos Móveis (somente MDM)
- MDM+Gerenciamento de Aplicativos Móveis (MAM)
- Somente MAM
- Registros de propriedade da empresa
- Registros BYOD (a capacidade de cancelar o registro no MDM)
- Migração de registros do Android Device Administrator para registros do Android Enterprise (totalmente gerenciado, perfil de trabalho, dispositivo dedicado)

Os perfis de registro substituem a propriedade de servidor agora preterida, `xms.server.mode`. Essa alteração não afeta os grupos de entrega existentes e os dispositivos registrados.

Se você não precisar registrar dispositivos dedicados, poderá desativar esse recurso definindo a propriedade do servidor `enable.multimode.xms` como **false**. Consulte [Propriedades do servidor](#).

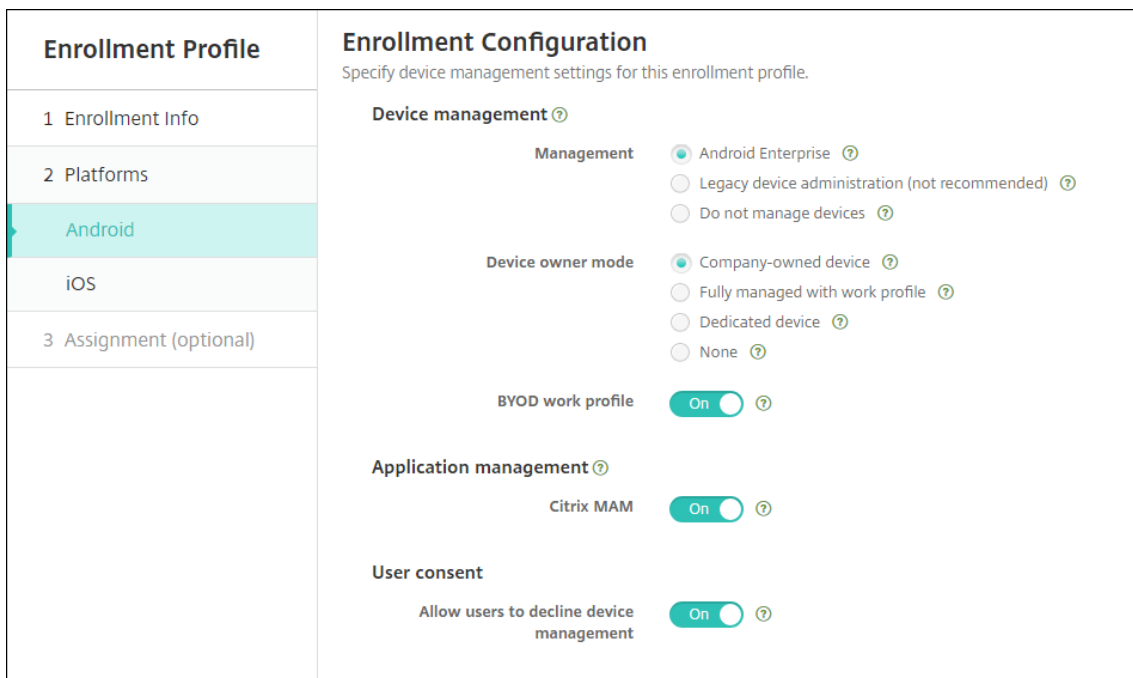
A tabela a seguir mostra o caminho de migração automatizada do modo de propriedade do servidor existente para o novo recurso de perfil de registro:

Propriedade do servidor existente	Novo modo de gerenciamento
Modo ENT (iOS)	Registro de dispositivo Apple com Citrix MAM
Modo ENT (Android)	Administrador de dispositivos legado com Citrix MAM
Modo ENT (Android Enterprise)	Perfil de trabalho totalmente gerenciado (anteriormente COPE), com Citrix MAM
Modo MAM (iOS e Android)	Citrix MAM
Modo MDM (iOS)	Registro de dispositivo Apple
Modo MDM (Android)	Administrador de dispositivo legado
Modo MDM (Android Enterprise)	Perfil de trabalho totalmente gerenciado

Ao criar um grupo de entrega, você pode anexar um perfil de registro ao grupo. Se você não anexar um perfil de registro, o XenMobile anexará o perfil de registro Global.

Os perfis de registro fornecem os seguintes recursos de gerenciamento de dispositivos:

- **Migração mais fácil do modo de administrador de dispositivo Android (DA) para Android Enterprise.** Para dispositivos Android Enterprise, as configurações incluem um modo proprietário de dispositivo, como: totalmente gerenciado, perfil de trabalho totalmente gerenciado ou dedicado. Consulte [Android Enterprise](#).



Para essa atualização, suas configurações atuais do XenMobile para o modo servidor e **Configurações > Android Enterprise** são mapeadas para as novas configurações de perfil de registro da seguinte maneira.

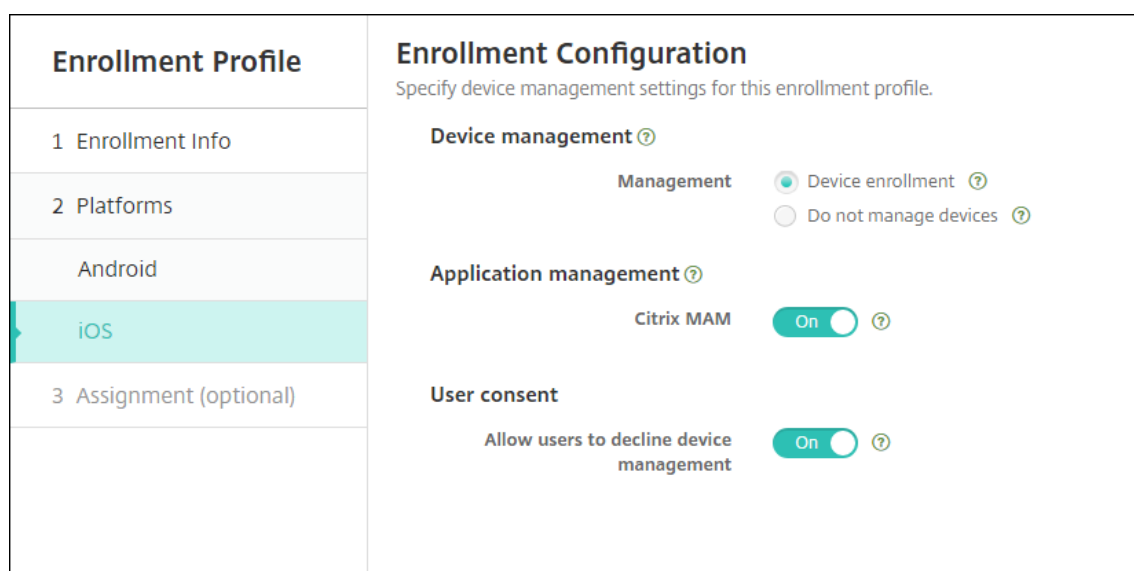
Configuração atual	Configuração de gerenciamento	Configuração do modo proprietário do dispositivo	Configuração do Citrix MAM
MDM. Google Play gerenciado (Android Enterprise)	Android Enterprise	Perfil de trabalho totalmente gerenciado	Desativado
MDM; G Suite (DA legado)	DA legado	não aplicável	Desativado
MAM	Não gerenciar dispositivos	não aplicável	Ativado
MDM+MAM. Google Play gerenciado (Android Enterprise)	Android Enterprise*	Perfil de trabalho totalmente gerenciado	Ativado

Configuração atual	Configuração de gerenciamento	Configuração do modo proprietário do dispositivo	Configuração do Citrix MAM
MDM+MAM; G Suite (DA legado)	DA legado*	não aplicável	Ativado

* Se o registro for necessário, **Permitir que os usuários recusem o gerenciamento de dispositivos** estará **Desativado**.

Após a atualização, seus perfis de registro atuais refletem esses mapeamentos. Considere se você deseja criar outros perfis de registro para lidar com novos casos de uso à medida que você faz a transição do DA legado.

- **Gerenciamento iOS mais fácil.** Para dispositivos iOS, as configurações incluem uma opção de escolha entre registrar dispositivos como gerenciados ou não gerenciados.



Para essa atualização, suas configurações anteriores são mapeadas para as novas configurações de perfil de registro da seguinte maneira.

Modo de servidor	Configuração de gerenciamento	Configuração do Citrix MAM
MDM	Registro do dispositivo	Desativado
MAM	Não gerenciar dispositivos	Ativado
MDM+MAM	Registro do dispositivo	Ativado

Se o registro for necessário, **Permitir que os usuários recusem o gerenciamento de dispositivos** estará **Desativado**.

As seguintes limitações existem para perfis de registro aprimorados:

- O recurso de perfil de registro aprimorado não está disponível para convites de registro de PIN de uso único ou de autenticação de dois fatores.

Consulte [Perfis de registro](#).

Suporte para a API mais recente do provedor de APNs baseada em HTTP/2

O suporte da Apple para o protocolo binário legado do serviço Apple Push Notification termina em 31 de março de 2021. A Apple recomenda que você use a API do provedor de APNs baseada em HTTP/2. O XenMobile Server agora oferece suporte à API baseada em HTTP/2. Para obter mais informações, leia “Apple Push Notification Service Update” em <https://developer.apple.com/>. Para obter ajuda com a verificação da conectividade com APNs, consulte [Verificações de conectividade](#)

As seguintes versões do XenMobile Server permitem o suporte à API baseada em HTTP/2 por padrão:

- XenMobile Server 10.13
- Pacote progressivo 5, XenMobile Server 10.12 e superior

Se você usar as seguintes versões do XenMobile Server, você deve adicionar a propriedade de servidor **apple.apns.http2** para habilitar o suporte:

- Pacotes progressivos 2-4, XenMobile Server 10.12 e superior
- Pacote progressivo 5, XenMobile Server 10.11 e superior

Não oferecemos mais suporte ao XenMobile Server 10.11 e recomendamos que você atualize para a versão mais recente.

Usar uma VPN IPsec baseada em certificado de dispositivo com muitos dispositivos iOS

Em vez de configurar uma política de dispositivo de VPN e uma política de dispositivo de credenciais para cada dispositivo iOS que requer uma VPN IPsec baseada em certificado de dispositivo, automatize o processo.

1. Configure uma política de dispositivo de VPN iOS com o tipo de conexão **AlwaysOn IKEv2**.
2. Selecione **Certificado do dispositivo baseado na identidade do dispositivo** como o método de autenticação do dispositivo.
3. Selecione o **Tipo de identidade do dispositivo** a ser usado.
4. Importe em massa os certificados do dispositivo usando a API REST.

Para obter mais informações sobre como configurar a política de dispositivo de VPN, consulte [Política de dispositivo do VPN](#). Para obter informações sobre como importar certificados em massa, consulte [Carregar certificados em massa usando a API REST](#).

Atualizações automáticas de aplicativos de compra por volume da Apple

Ao adicionar uma conta de compra por volume (**Configurações > Configurações de iOS**), agora você pode ativar atualizações automáticas para todos os aplicativos iOS. Veja a configuração **Atualização automática do aplicativo** em [Compra por volume da Apple](#).

Requisitos de senha para uma conta de usuário local

Ao adicionar ou editar uma conta de usuário local no console XenMobile, certifique-se de estar seguindo os requisitos de senha mais recentes.

Para obter mais informações, consulte [Para adicionar uma conta de usuário local](#).

- **Requisitos de senha:** ao adicionar ou editar uma conta de usuário local no console XenMobile Server, siga os requisitos de senha mais recentes. Consulte [Para adicionar uma conta de usuário local](#).
- **Bloqueio de conta de usuário local:** se um usuário atingir o número máximo de tentativas consecutivas de login inválidas, a conta de usuário local fica bloqueada durante 30 minutos. O sistema nega todas as tentativas de autenticação adicionais até que o período de bloqueio expire. Para desbloquear a conta no console XenMobile Server, vá para **Gerenciar > Usuários**, selecione a conta de usuário e clique em **Desbloquear usuário local**. Consulte [Para desbloquear uma conta de usuário local](#).

Políticas de dispositivo

Novas políticas de dispositivo e configurações de política de dispositivo foram adicionadas para dispositivos Android Enterprise.

Ocultar o ícone da barra da bandeja em dispositivos Android Enterprise

Agora você pode selecionar se o ícone da barra da bandeja fica oculto ou visível nos dispositivos Android Enterprise. Consulte [Políticas de dispositivo das opções de XenMobile](#).

Mais recursos de gerenciamento de certificados para dispositivos Android Enterprise no modo de perfil de trabalho ou modo totalmente gerenciado

Além de instalar autoridades de certificação no keystore gerenciado, agora você pode gerenciar os seguintes recursos:

- **Configurar os certificados usados por aplicativos gerenciados específicos.** A política de dispositivo de Credenciais para Android Enterprise agora inclui a configuração **Aplicativos que devem usar os certificados**. Você pode especificar os aplicativos para usar os certificados de

usuário emitidos pelo provedor de credenciais selecionado nesta política. Os aplicativos recebem, silenciosamente, acesso a certificados durante o tempo de execução. Para usar os certificados para todos os aplicativos, deixe a lista de aplicativos em branco. Consulte [Política de dispositivo de credenciais](#).

- **Remover silenciosamente os certificados do keystore gerenciado ou desinstalar todos os certificados de CA que não são do sistema.** Consulte [Política de dispositivo de credenciais](#).
- **Impedir que os usuários modifiquem as credenciais armazenadas no keystore gerenciado.**

A política de dispositivo de Restrições para Android Enterprise agora inclui a configuração **Permitir que o usuário configure as credenciais do usuário**. Por padrão, essa configuração é **Ativada**. Consulte [Política de dispositivo de restrições](#).

Uso mais fácil do alias de certificado em configurações gerenciadas do Android Enterprise

Use a nova configuração **Alias de certificado** na política de dispositivo de **Credenciais** com a política de dispositivo de **Configurações gerenciadas do Android Enterprise**. Isso permite que os aplicativos sejam autenticados na VPN sem a ação do usuário. Em vez de localizar o alias de credencial nos logs do aplicativo, você cria o alias de credencial. Crie o alias digitando-o no campo **Alias de certificado** da política de dispositivo de **Configurações gerenciadas do Android Enterprise**. Depois, digite o mesmo alias de certificado na configuração **Alias de certificado** na política de dispositivo **Credenciais**. Consulte [Política de configurações gerenciadas do Android Enterprise](#) e [Política de dispositivo de credenciais](#).

Controlar a configuração “Use one lock” em dispositivos Android Enterprise

A nova configuração **Ativar código secreto unificado** na política de dispositivo de **Código secreto** permite controlar se um dispositivo requer um código secreto separado para o dispositivo e o perfil de trabalho. Antes dessa configuração, os usuários controlavam o comportamento com a configuração **Use one lock** no dispositivo. Quando **Ativar código secreto unificado** está **Ativado**, os usuários podem usar o mesmo código secreto para o dispositivo que o do perfil de trabalho. Se **Ativar código secreto unificado** estiver **Desativado**, os usuários não poderão usar o mesmo código secreto para o dispositivo que o do perfil de trabalho. O padrão é **Off**. A configuração **Ativar bloqueio unificado** está disponível para dispositivos Android Enterprise executando o Android 9.0 ou posterior. Consulte [Política de dispositivo de código secreto](#).

Mostrar os aplicativos e atalhos em dispositivos Android Enterprise que não estão em conformidade

A política de dispositivo de Código Secreto para Android Enterprise tem uma nova configuração, **Mostrar aplicativos e atalhos mesmo que o código secreto não esteja em conformidade**. Ative a configuração para fazer com que os aplicativos e atalhos permaneçam visíveis quando o código

secreto do dispositivo não estiver mais em conformidade. A Citrix recomenda que você crie uma ação automatizada para marcar o dispositivo como sem conformidade quando o código secreto não estiver em conformidade. Consulte [Política de dispositivo de código secreto](#).

Desative a capacidade de imprimir em dispositivos totalmente gerenciados ou dispositivos de perfil de trabalho do Android Enterprise

Na política de dispositivo de Restrições, a configuração **Não permitir impressão** permite especificar se os usuários podem imprimir em qualquer impressora acessível a partir do dispositivo Android Enterprise. Consulte [Configurações do Android Enterprise](#).

Permitir aplicativos em dispositivos dedicados adicionando o nome do pacote na política de quiosque

Agora você pode inserir o nome do pacote que deseja permitir na plataforma Android Enterprise. Consulte [Configurações do Android Enterprise](#).

Gerenciar recursos de proteção do teclado para o perfil de trabalho Android Enterprise e dispositivos totalmente gerenciados

O Android keyguard gerencia as telas de bloqueio de dispositivo e de Work Challenge. Use a política de dispositivos de Gerenciamento de proteção do teclado para controlar:

- Gerenciamento de proteção do teclado em dispositivos de perfil de trabalho. Você pode especificar os recursos disponíveis para os usuários antes que eles desbloqueiem a proteção do teclado do dispositivo e o keyguard do Work Challenge. Por exemplo, por padrão, os usuários podem usar o desbloqueio por impressão digital e exibir notificações não editadas na tela de bloqueio. Você também pode usar a política de gerenciamento de proteção do teclado para desativar toda a autenticação biométrica para dispositivos que executam o Android 9.0 e posterior.
- Gerenciamento de proteção do teclado em dispositivos totalmente gerenciados e dedicados. Você pode especificar os recursos disponíveis, como agentes de confiança e câmera segura, antes que desbloqueiem a tela de proteção do teclado. Ou, você pode optar por desativar todos os recursos de proteção do teclado.

Consulte [Política de dispositivo de gerenciamento de keyguard](#).

Publicar aplicativos empresariais para Android Enterprise no console XenMobile

Você não precisa mais se registrar para uma conta de desenvolvedor do Google Play ao adicionar um aplicativo privado do Android Enterprise. O console XenMobile abre uma interface de usuário da

loja gerenciada do Google Play para que você carregue e publique o arquivo APK. Para obter mais informações, consulte [Acrescentar um aplicativo empresarial](#).

Publicar aplicativos web para Android Enterprise no console XenMobile

Você não precisa mais acessar o Google Play gerenciado ou o portal do Google Developer para publicar aplicativos Web do Android Enterprise para XenMobile. Quando você clica em **Carregar** em **Configurar > Aplicativos > Link da Web**, uma interface de usuário da loja gerenciada do Google Play é aberta para que você carregue e salve o arquivo. A aprovação e a publicação do aplicativo podem levar cerca de 10 minutos. Para obter mais informações, consulte [Adicionar um link da Web](#).

Carregar certificados para dispositivos iOS em massa com a API REST do XenMobile Server

Se o carregamento individual de certificados não for prático, use a API REST do XenMobile Server para carregar os certificados em massa para dispositivos iOS.

1. Configure uma política de dispositivo de VPN iOS com o tipo de conexão **AlwaysOn IKEv2**.
2. Selecione **Certificado do dispositivo baseado na identidade do dispositivo** como o método de autenticação do dispositivo.
3. Selecione o **Tipo de identidade do dispositivo** a ser usado.
4. Importe em massa os certificados do dispositivo com a API REST.

Para obter informações sobre como configurar a política de dispositivo de VPN, consulte [Política de dispositivo do VPN](#). Para obter informações sobre como importar certificados em massa, consulte [Carregar certificados para dispositivos iOS em massa com a API REST](#).

Atualizar chaves de criptografia

A opção **Refresh encryption keys** é adicionada às configurações avançadas da CLI do XenMobile. Você pode usar essa opção para atualizar as chaves de criptografia um nó de cada vez. Consulte [Opções do sistema](#).

Suporte a ESXi 7.0

Com esta versão, o XenMobile oferece suporte ao VMware ESXi 7.0. Certifique-se de atualizar para 10.13 antes de instalar ou atualizar para ESXi 7.0.

Novas propriedades do servidor

As seguintes propriedades do servidor agora estão disponíveis:

- **Permitir nomes de host para links da App Store do iOS:** para adicionar aplicativos da loja de aplicativos pública para iOS usando as APIs públicas em vez do console, configure uma lista de nomes de host permitidos, se desejar.
- **Limite de bloqueio de conta de usuário local:** configure o número de tentativas de login que um usuário local tem antes de a sua conta ser bloqueada.
- **Tempo de bloqueio de conta de usuário local:** configure por quanto tempo um usuário local fica bloqueado após muitas tentativas de login malsucedidas.
- **Tamanho máximo da restrição de carregamento de arquivos ativada:** habilite a restrição de tamanho máximo de arquivo para os arquivos carregados.
- **Tamanho máximo de carregamento de arquivo permitido:** defina o tamanho máximo de arquivo para arquivos carregados.

Para obter informações mais detalhadas sobre essas propriedades, consulte [Propriedades do servidor](#).

Limpeza de disco self-service

Uma nova opção de interface de linha de comando chamada **Disk Usage** está disponível no **Troubleshooting Menu**. Esta opção permite que você veja uma lista de arquivos de despejo core e arquivos de pacote de suporte. Depois de ver a lista, você pode optar por excluir todos os arquivos através da linha de comando. Para obter mais informações sobre as ferramentas de interface de linha de comando, consulte [Opções da interface de linha de comando](#).

Novidades no XenMobile Server 10.12

April 8, 2021

[XenMobile Server 10.12](#) (download em PDF)

Serviço de migração do XenMobile

Se você estiver usando o XenMobile Server no local, nosso Serviço de Migração do XenMobile gratuito pode ajudá-lo a começar a usar o Endpoint Management. A migração do XenMobile Server para o Citrix Endpoint Management não exige que você registre novamente os dispositivos.

Para iniciar a migração, entre em contato com um fornecedor Citrix local ou um parceiro Citrix. Para obter mais informações, consulte [Serviço de migração do XenMobile](#).

Anúncios de substituição

Para receber um aviso prévio dos recursos do Citrix XenMobile que estão sendo eliminados, consulte [Substituição](#).

Prepare seus dispositivos Android para mudanças futuras

Essas substituições anunciadas anteriormente afetam seus dispositivos Android e Android Enterprise:

- Registros de Administração do Dispositivo (DA) para Android 10
 - **31 de julho de 2020:** a Citrix substitui novos registros para o modo de administração de dispositivo Android legado.
 - **1 de novembro de 2020:** o Google substitui a API de administração de dispositivo legado. Os dispositivos Android 10 executados no modo de administração de dispositivo legado não funcionarão mais.
- Criptografia MDX:
 - **1 de agosto de 2020:** a Citrix começa a impor a migração da criptografia MDX para a criptografia de plataforma para os aplicativos móveis de produtividade Citrix e aplicativos MDX de terceiros.
 - **1 de setembro de 2020:** a criptografia MDX atinge o fim da vida útil.

Para dispositivos registrados no DA legado

- Se você não usa criptografia MDX, nenhuma ação é necessária.
- Se você usa a criptografia MDX, migre os dispositivos Android para o Android Enterprise antes de 31 de julho de 2020. Os dispositivos com Android 10 devem se registrar ou se registrar novamente usando o Android Enterprise. Este requisito inclui dispositivos Android no modo somente MAM. Consulte [Migrar do Device Administration para o Android Enterprise](#).

Para dispositivos já registrados no Android Enterprise em 31 de julho

- Se você publicou os aplicativos usando a plataforma Android Enterprise, a criptografia já está sendo tratada através do Android Enterprise. Nenhuma ação é necessária.
- Se você publicou os aplicativos usando a plataforma Android legada, publique novamente os aplicativos usando o Android Enterprise antes de 31 de julho de 2020.

Antes de atualizar para o XenMobile 10.12 (no local)

Alguns requisitos de sistemas mudaram. Para obter informações, consulte [Requisitos do sistema e compatibilidade](#) e [Compatibilidade do XenMobile](#).

1. Atualize o seu Citrix License Server para 11.16 ou posterior antes de atualizar para a versão mais recente do XenMobile Server 10.12.

A versão mais recente do XenMobile exige o Citrix License Server 11.16 (versão mínima).

Nota:

Se você quiser usar sua própria licença para a Visualização, saiba que a data do Customer Success Services (anteriormente, data de Subscription Advantage) no XenMobile 10.12 é 20 de janeiro de 2020. A data do Customer Success Services na sua licença Citrix deve ser posterior a essa data.

Você pode ver a data ao lado da licença do servidor de licenças. Se você conectar a versão mais recente do XenMobile a um ambiente de servidor de licenças mais antigo, a verificação de conectividade falhará e você não poderá configurar o servidor de licenças.

Para renovar a data na sua licença, baixe o último arquivo de licença do Portal Citrix e carregue o arquivo para o Servidor de Licença. Para obter mais informações, consulte [Customer Success Services](#).

2. Para um ambiente em cluster: as implantações de aplicativos e políticas do iOS para dispositivos que executam o iOS 11 e posterior têm o seguinte requisito. Se o Citrix Gateway estiver configurado para persistência de SSL, você deve abrir a porta 80 em todos os nós do XenMobile Server.
3. Se a máquina virtual que executa o XenMobile Server que deve ser atualizado tiver menos de 4 GB de RAM, aumente a RAM para pelo menos 4 GB. Lembre-se de que a quantidade mínima de RAM recomendada é de 8 GB para ambientes de produção.
4. Recomendação: Antes de instalar uma atualização do XenMobile, use a funcionalidade na sua VM para tirar um instantâneo do seu sistema. Além disso, faça backup do seu banco de dados de configuração do sistema. Se tiver problemas durante uma atualização, backups completos permitirão fazer uma recuperação.

Para atualizar

Você pode atualizar diretamente do XenMobile 10.11.x ou 10.10.x para o XenMobile 10.12. Para realizar a atualização, baixe o binário mais recente disponível: acesse <https://www.citrix.com/downloads>. Navegue para **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**. No bloco do software XenMobile Server, para o seu hipervisor, clique em **Download File**.

Use a página **Gerenciamento de versão** no console XenMobile. Para obter mais informações, consulte [Para atualizar usando a página Gerenciamento de versão](#).

Depois de atualizar

Após atualizar para o XenMobile 10.12 (no local):

Se a funcionalidade que envolve as conexões de saída deixar de funcionar e você não alterou a configuração de suas conexões, verifique os erros no log do XenMobile Server, como os seguintes: “Não é possível se conectar ao servidor VPP: o nome do host ‘192.0.2.0’ não corresponde à entidade do certificado fornecido pelo par”.

O erro de validação do certificado indica que você precisa desabilitar a verificação do nome do host no XenMobile Server. Como padrão, a verificação do nome do host está ativada nas conexões de saída, exceto para o servidor Microsoft PKI. Se a verificação do nome do host interromper sua implantação, altere a propriedade do servidor `disable.hostname.validation` para `true`. O valor padrão dessa propriedade é `false`.

Suporte adicional para iOS 13

O XenMobile Server suporta dispositivos atualizados para iOS 13. A atualização afeta seus usuários da seguinte forma:

- Durante o registro, algumas novas telas de Opções do assistente de configuração iOS são exibidas. A Apple adicionou novas telas de Opções do assistente de configuração iOS ao iOS 13. As novas opções estão incluídas na página **Configurações > Programa de registro de dispositivo (DEP) da Apple** desta versão. Você pode configurar o XenMobile Server para ignorar essas telas. Essas páginas aparecem para usuários com dispositivos iOS 13.
- Algumas configurações da política de dispositivo Restrições que estavam disponíveis em dispositivos supervisionados ou não supervisionados com versões anteriores do iOS estão disponíveis apenas em dispositivos supervisionados para iOS 13+. As dicas atuais da ferramenta do console XenMobile Server ainda não indicam que essas configurações são apenas para dispositivos supervisionados com iOS 13+.
 - Permitir controles de hardware:
 - * FaceTime
 - * Instalação de aplicativos
 - Permitir aplicativos:
 - * iTunes Store
 - * Safari
 - * Safari > Preenchimento automático
 - Rede - Permitir ações do iCloud:
 - * Documentos e dados do iCloud
 - Apenas configurações supervisionadas - Permitir:
 - * Game Center > Adicionar amigos

- * Game Center > Jogos multiplayer
- Conteúdo de mídia - Permitir:
 - * Música, podcasts e material do iTunes U explícitos

Essas restrições se aplicam da seguinte forma:

- Se um dispositivo iOS 12 (ou inferior) já estiver registrado no XenMobile Server e, depois, for atualizado para o iOS 13, as restrições anteriores se aplicarão a dispositivos não supervisionados e supervisionados.
- Se um dispositivo iOS 13+ não supervisionado for registrado no XenMobile Server, as restrições anteriores se aplicam apenas aos dispositivos supervisionados.
- Se um dispositivo iOS 13+ supervisionado for registrado no XenMobile Server, as restrições anteriores se aplicam apenas aos dispositivos supervisionados.

Migração do Apple Volume Purchase Program para Apple Business Manager (ABM) e Apple School Manager (ASM)

As empresas e instituições que usam o Apple Volume Purchase Program (VPP) precisam migrar para Apps e Livros no Apple Business Manager ou Apple School Manager antes de 1º de dezembro de 2019.

Antes de migrar contas VPP no XenMobile, veja isso, [Artigo de suporte da Apple](#).

Se a sua organização ou escola usar apenas o Volume Purchase Program (VPP), você poderá se inscrever no ABM/ASM e convidar Compradores de VPP existentes para a sua nova conta ABM/ASM. Para ASM, navegue até <https://school.apple.com>. Para ABM, navegue até <https://business.apple.com>.

Para atualizar sua conta VPP no XenMobile:

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida.
2. Clique em **Configurações de iOS**. A página de configuração **Programa de Compra por Volume** é exibida.
3. Certifique-se de que sua conta ABM ou ASM tenha a mesma configuração de aplicativo que sua conta VPP anterior.
4. No portal ABM ou ASM, baixe um token atualizado.
5. No console XenMobile, faça o seguinte:
 - a) Edite a conta de compra de volume existente com as informações de token atualizadas para o local.
 - b) Edite suas credenciais ABM ou ASM. Não mude o sufixo.
 - c) Clique em **Salvar** duas vezes.

Para obter mais informações, consulte:

- [Programa de implantação da Apple](#)
- [Registro em massa de dispositivos Apple](#)

Suporte para dispositivos COPE Android Enterprise

O XenMobile Server suporta dispositivos Android Enterprise totalmente gerenciados com perfis de trabalho, anteriormente conhecidos como dispositivos COPE (Propriedade da empresa, habilitado pessoalmente). Esses dispositivos são um tipo de dispositivo Android Enterprise totalmente gerenciado que também possui um perfil de trabalho. Você pode aplicar definições de política separadas ao dispositivo e ao perfil de trabalho. Para esta versão:

- Você pode aplicar configurações separadas ao dispositivo e ao perfil de trabalho usando estas políticas de dispositivo: Credenciais, Código secreto e Restrições.
- Você pode aplicar a configuração do modo de localização da política de dispositivo de Localização ao próprio dispositivo COPE, mas não ao perfil de trabalho do dispositivo COPE. Outras configurações na política de dispositivo de Localização não estão disponíveis para dispositivos COPE.
- Você pode aplicar a ação de segurança Bloquear separadamente ao dispositivo ou ao perfil de trabalho.

Políticas de dispositivo

Para dispositivos Android Enterprise totalmente gerenciados com perfis de trabalho (dispositivos COPE), algumas políticas de dispositivo podem aplicar configurações separadas a todo o dispositivo e ao perfil de trabalho. No console XenMobile Server, algumas políticas de dispositivo permitem que você aplique as configurações separadas. Você pode usar outras políticas de dispositivo para aplicar configurações apenas para o dispositivo todo ou apenas para o perfil de trabalho de dispositivos totalmente gerenciados com perfis de trabalho.

Ações de segurança

Para dispositivos Android Enterprise totalmente gerenciados com perfis de trabalho (dispositivos COPE), você pode aplicar:

- A ação de segurança Bloquear separadamente para o dispositivo ou o perfil de trabalho.
- Todas as outras ações de segurança para o dispositivo.

Perfis de registro controlam as opções de registro para dispositivos Android

Os perfis de registro agora controlam como os dispositivos Android são registrados se o Android Enterprise estiver habilitado para a sua implantação XenMobile. Os perfis de registro determinam se

os dispositivos Android estão registrados no modo padrão Android Enterprise (totalmente gerenciado ou perfil de trabalho) ou no modo legado (administrador de dispositivo).

Por padrão, o perfil de registro Global registra dispositivos Android Enterprise novos e com redefinição de fábrica como dispositivos totalmente gerenciados e registra dispositivos Android Enterprise BYOD como dispositivos de perfil de trabalho. Para obter mais informações, consulte [Android Enterprise](#).

Preparando dispositivos Android legados para Android Enterprise como registro padrão

O Google está descontinuando o modo administrador do dispositivo de gerenciamento de dispositivos e incentivando os clientes a gerenciar todos os dispositivos Android no modo proprietário do dispositivo ou no modo proprietário do perfil. (Consulte [Device admin deprecation](#) nos guias do desenvolvedor do Google Android Enterprise.) Para suportar essa alteração, o Android Enterprise é agora a opção de registro padrão para dispositivos Android.

Essa alteração significa que, se o Android Enterprise estiver habilitado para sua implantação do XenMobile, todos os dispositivos Android recém-registrados ou registrados novamente serão registrados como dispositivos Android Enterprise.

Para se preparar para essa mudança, o XenMobile agora permite que você crie perfis de registro que controlam como os dispositivos Android são registrados.

Sua organização pode não estar pronta para começar a gerenciar dispositivos Android legados no modo proprietário do dispositivo ou no modo proprietário do perfil. Nesse caso, você pode continuar gerenciando-os no modo de administrador do dispositivo. Crie um perfil de registro para dispositivos legados e registre novamente todos os dispositivos legados registrados.

Para criar um perfil de registro para dispositivos legados:

1. No console XenMobile, vá para **Configurar > Perfis de registro**.
2. Para adicionar um perfil de registro, clique em **Adicionar**. Na página de Informações de registro, digite um nome para o perfil de registro.
3. Clique em **Avançar** ou selecione **Android Enterprise** em **Plataformas**. A página de configuração de registro é exibida.
4. Defina **Gerenciamento** como **Legado (administrador do dispositivos)**. Clique em **Avançar** ou selecione **Atribuição (opções)**. A tela Atribuição de grupo de entrega é exibida.

Enrollment Profile	Enrollment Type
1 Enrollment Info	Select the enrollment type for Android devices
2 Platforms	<input type="radio"/> Fully managed/Work profile <input type="radio"/> COPE/Work profile <input checked="" type="radio"/> Legacy (device administrator)
Android Enterprise	
3 Assignment (optional)	

- Escolha um grupo de entrega ou grupos de entrega contendo os administradores que registram dispositivos dedicados. Em seguida, clique em **Salvar**.

Para continuar a gerenciar o dispositivo legado no modo de administrador de dispositivos, registre-os ou registre-os novamente utilizando este perfil. Você registra dispositivos de administrador de dispositivos de modo similar aos dispositivos de perfil de trabalho, fazendo com que os usuários baixem o Secure Hub e fornecendo um URL do servidor de registro.

Para obter mais informações sobre o suporte do Endpoint Management para a transição para o Android Enterprise, consulte o blog sobre o [Android Enterprise como padrão para o serviço Citrix Endpoint Management](#).

Gerenciamento simplificado de aplicativos para Android Enterprise

Você não precisa mais acessar o Google Play gerenciado ou o portal do Google Developer para aprovar ou publicar aplicativos para o XenMobile Server. Como resultado, a aprovação e a publicação de aplicativos demoram cerca de 10 minutos em vez de horas.

Aprovar aplicativos Android Enterprise para a loja de aplicativos pública no console XenMobile Server. Agora você pode aprovar aplicativos gerenciados da loja Google Play sem sair do console XenMobile Server. Depois de inserir um nome de aplicativo no campo de pesquisa, a interface do usuário gerenciada da loja Google Play abre com as instruções para você aprovar e salvar o aplicativo. Seu aplicativo preenche os resultados, permitindo que você configure os detalhes. Consulte [Acrescentar um aplicativo de loja de aplicativos pública](#).

Adicione aplicativos MDX para Android Enterprise. O console XenMobile Server agora oferece suporte ao Android Enterprise como uma plataforma para implantação do aplicativo MDX. Consulte [Acrescentar um aplicativo MDX](#).

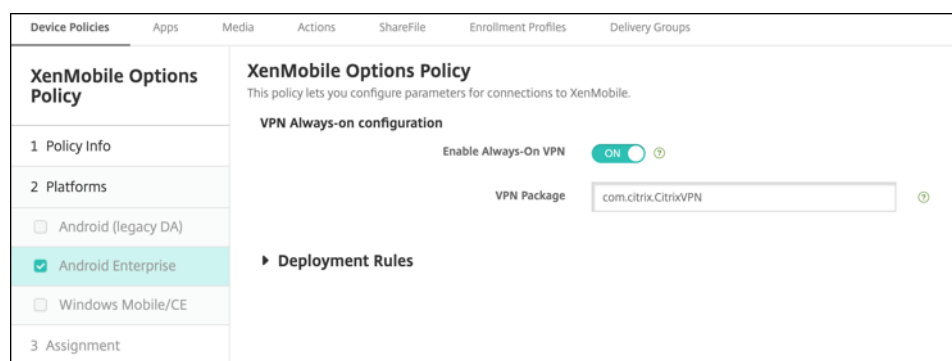
Aprovar aplicativos MDX para Android Enterprise no console XenMobile Server. Agora você pode aprovar aplicativos gerenciados da loja Google Play para Android Enterprise sem sair do console Xen-

Mobile Server. Depois de carregar um arquivo MDX, a interface de usuário gerenciada da loja Google Play é aberta com as instruções para você aprovar e salvar o aplicativo. Consulte [Acrescentar um aplicativo MDX](#).

Suporte para VPN sempre ativa para Android Enterprise

A política de dispositivo de opções do XenMobile Server agora permite habilitar a VPN sempre ativa para Android Enterprise.

Quando você configurar perfis VPN para Android Enterprise, no **perfil VPN padrão**, digite o nome do perfil VPN. O XenMobile usa esse perfil quando os usuários tocam no switch de conexão na interface do usuário do aplicativo Citrix SSO em vez de tocarem em um perfil específico. Se esse campo for deixado vazio, o perfil principal será usado para conexão. Se apenas um perfil estiver configurado, ele será marcado como perfil padrão. Para VPN sempre conectada, esse campo deve ser definido como o nome do perfil VPN a ser usado para estabelecer VPN sempre conectada.



Configurar o rastreamento de produtos para seus aplicativos Android Enterprise

Ao adicionar um aplicativo da loja pública ou um aplicativo MDX para Android Enterprise, configure o rastreamento de produtos que você deseja enviar para os dispositivos do usuário. Por exemplo, se você tiver um rastreamento projetado para testes, poderá selecioná-lo e atribuí-lo a um grupo de entrega específico. Para saber mais sobre como implantar sua versão, consulte a [Central de Ajuda do Google Play](#). Para obter informações sobre como configurar o rastreamento de produtos, consulte [Acrescentar um aplicativo MDX](#) ou [Acrescentar um aplicativo de loja de aplicativos pública](#).

Forçar uma redefinição de código secreto para usuários do macOS

Quando um dispositivo macOS recebe um perfil de configuração com uma política de senha, os usuários devem fornecer um código secreto que atenda às configurações da política. Agora você pode forçar a redefinição do código secreto na próxima vez que um usuário se autentica. Na política de dispositivo de código secreto para macOS (10.13 e posterior), ative a nova configuração **Forçar**

redefinição do código secreto. Para obter mais informações sobre a política, consulte [Política de dispositivo de código secreto](#).

Novidades no XenMobile Server 10.11

December 10, 2020

[XenMobile Server 10.11](#) (download em PDF)

Serviço de migração do XenMobile

Se você estiver usando o XenMobile Server no local, nosso Serviço de Migração do XenMobile gratuito pode ajudá-lo a começar a usar o Endpoint Management. A migração do XenMobile Server para o Citrix Endpoint Management não exige que você registre novamente os dispositivos.

Para iniciar a migração, entre em contato com um fornecedor Citrix local ou um parceiro Citrix. Para obter mais informações, consulte [Serviço de migração do XenMobile](#).

Migração do Apple Volume Purchase Program para Apple Business Manager (ABM) e Apple School Manager (ASM)

As empresas e instituições que usam o Apple Volume Purchase Program (VPP) devem migrar para Apps e Livros no Apple Business Manager ou Apple School Manager antes de 1º de dezembro de 2019.

Antes de migrar contas VPP no XenMobile, veja isso, [Artigo de suporte da Apple](#).

Se a sua organização ou escola usar apenas o Volume Purchase Program (VPP), você poderá se inscrever no ABM/ASM e convidar Compradores de VPP existentes para a sua nova conta ABM/ASM. Para ASM, navegue até <https://school.apple.com>. Para ABM, navegue até <https://business.apple.com>.

Para atualizar sua conta de compra por volume (anteriormente VPP) no XenMobile:

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida.
2. Clique em **Volume Purchase**. A página de configuração **Volume Purchase** é exibida.
3. Certifique-se de que sua conta ABM ou ASM tenha a mesma configuração de aplicativo que sua conta VPP anterior.
4. No portal ABM ou ASM, baixe um token atualizado.
5. No console XenMobile, faça o seguinte:
 - a) Edite a conta de compra de volume existente com as informações de token atualizadas para o local.

- b) Edite suas credenciais ABM ou ASM. Não mude o sufixo.
- c) Clique em **Salvar** duas vezes.

Suporte adicional para iOS 13

Importante:

Para se preparar para atualizações de dispositivos para o iOS 12+: o tipo de conexão Citrix VPN na política de dispositivos VPN para iOS não suporta o iOS 12+. Exclua sua política de dispositivo VPN e crie uma nova política de dispositivo VPN com o tipo de conexão Citrix SSO.

A conexão Citrix VPN continua a operar em dispositivos implantados anteriormente depois que você exclui a política de dispositivo VPN. Sua nova configuração de política de dispositivo VPN entra em vigor no XenMobile Server 10.11, durante o registro do usuário.

O XenMobile Server suporta dispositivos atualizados para iOS 13. A atualização afeta seus usuários da seguinte forma:

- Durante o registro, algumas novas telas de Opções do assistente de configuração iOS são exibidas. A Apple adicionou novas telas de Opções do assistente de configuração iOS ao iOS 13. As novas opções não estão incluídas na página **Configurações > Programa de registro de dispositivo (DEP) da Apple** desta versão. Portanto, você não pode configurar o XenMobile Server para ignorar essas telas. Essas páginas aparecem para usuários com dispositivos iOS 13.
- Algumas configurações da política de dispositivo Restrições que estavam disponíveis em dispositivos supervisionados ou não supervisionados com versões anteriores do iOS estão disponíveis apenas em dispositivos supervisionados para iOS 13+. As dicas atuais da ferramenta do console XenMobile Server ainda não indicam que essas configurações são apenas para dispositivos supervisionados com iOS 13+.
 - Permitir controles de hardware:
 - * FaceTime
 - * Instalação de aplicativos
 - Permitir aplicativos:
 - * iTunes Store
 - * Safari
 - * Safari > Preenchimento automático
 - Rede - Permitir ações do iCloud:
 - * Documentos e dados do iCloud
 - Apenas configurações supervisionadas - Permitir:
 - * Game Center > Adicionar amigos
 - * Game Center > Jogos multiplayer
 - Conteúdo de mídia - Permitir:

- * Música, podcasts e material do iTunes U explícitos

Essas restrições se aplicam da seguinte forma:

- Se um dispositivo iOS 12 (ou inferior) já estiver registrado no XenMobile Server e, depois, for atualizado para o iOS 13, as restrições anteriores se aplicarão a dispositivos não supervisionados e supervisionados.
- Se um dispositivo iOS 13+ não supervisionado for registrado no XenMobile Server, as restrições anteriores se aplicam apenas aos dispositivos supervisionados.
- Se um dispositivo iOS 13+ supervisionado for registrado no XenMobile Server, as restrições anteriores se aplicam apenas aos dispositivos supervisionados.

Requisitos para certificados confiáveis no iOS 13 e macOS 15

A Apple tem novos requisitos para certificados de servidor TLS. Verifique se todos os certificados seguem os novos requisitos da Apple. Consulte a publicação da Apple, <https://support.apple.com/en-us/HT210176>. Para obter ajuda com o gerenciamento de certificados, consulte [Carregando certificados no XenMobile](#).

Atualizar de GCM para FCM

A partir de 10 de abril de 2018, o Google descontinuou o Google Cloud Messaging (GCM). O Google removeu as APIs do servidor e do cliente GCM em 29 de maio de 2019.

Requisitos importantes:

- Atualize para a versão mais recente do XenMobile Server.
- Atualize para a versão mais recente do Secure Hub.

Google recomenda a atualização para o Firebase Cloud Messaging (FCM) imediatamente para começar a aproveitar os novos recursos disponíveis no FCM. Para obter informações do Google, consulte <https://developers.google.com/cloud-messaging/faq> e <https://firebase.googleblog.com/2018/04/time-to-upgrade-from-gcm-to-fcm.html>.

Para continuar a ter suporte para notificações por push para seus dispositivos Android: se você usa o GCM com o XenMobile Server, migre para o FCM. Em seguida, atualize o XenMobile Server com a nova chave FCM disponível no Firebase Cloud Messaging Console.

As etapas a seguir refletem o fluxo de trabalho de registro quando você usa certificados confiáveis.

Etapas de atualização:

1. Siga as informações do Google para atualizar do GCM para o FCM.
2. No Firebase Cloud Messaging Console, copie sua nova chave FCM. Você vai precisar dela na próxima etapa.

3. No console XenMobile Server, vá para **Configurações > Firebase Cloud Messaging** e defina suas configurações.

Os dispositivos alternam para o FCM na próxima vez que fizerem check-in no XenMobile Server e atualizarem a política. Para forçar o Secure Hub a atualizar políticas: no Secure Hub, vá para **Preferências > Informações do Dispositivo** e toque em **Atualizar Política**.

Para obter mais informações sobre como configurar o FCM, consulte [Firebase Cloud Messaging](#).

Serviço de migração do XenMobile

Se você estiver usando o XenMobile Server no local, nosso Serviço de Migração do XenMobile pode ajudá-lo a começar a usar o Endpoint Management. A migração do XenMobile Server para o Citrix Endpoint Management não exige que você registre novamente os dispositivos.

Para obter mais informações, entre em contato com o pessoal de vendas local da Citrix, com um engenheiro de sistemas ou com um parceiro Citrix. Estes blogs discutem o Serviço de Migração do XenMobile:

[Novo serviço de migração do XenMobile](#)

[Criando o cenário para o XenMobile na Nuvem](#)

Antes de atualizar para o XenMobile 10.11 (no local)

Alguns requisitos de sistemas mudaram. Para obter informações, consulte [Requisitos do sistema e compatibilidade](#) e [Compatibilidade do XenMobile](#).

1. Atualize o seu Citrix License Server para 11.15 ou posterior antes de atualizar para a versão mais recente do XenMobile Server 10.11.

A versão mais recente do XenMobile exige o Citrix License Server 11.15 (versão mínima).

Nota:

Se você quiser usar sua própria licença para a Visualização, saiba que a data do Customer Success Services (anteriormente, data de Subscription Advantage) no XenMobile 10.11 é 9 de abril de 2019. A data do Customer Success Services na sua licença Citrix deve ser posterior a essa data.

Você pode ver a data ao lado da licença do servidor de licenças. Se você conectar a versão mais recente do XenMobile a um ambiente de servidor de licenças mais antigo, a verificação de conectividade falhará e você não poderá configurar o servidor de licenças.

Para renovar a data na sua licença, baixe o último arquivo de licença do Portal Citrix e carregue o arquivo para o Servidor de Licença. Para obter mais informações, consulte [Customer Success Services](#).

2. Para um ambiente em cluster: as implantações de aplicativos e políticas do iOS para dispositivos que executam o iOS 11 e posterior têm o seguinte requisito. Se o Citrix Gateway estiver configurado para persistência de SSL, você deve abrir a porta 80 em todos os nós do XenMobile Server.
3. Se a máquina virtual que executa o XenMobile Server que deve ser atualizado tiver menos de 4 GB de RAM, aumente a RAM para pelo menos 4 GB. Lembre-se de que a quantidade mínima de RAM recomendada é de 8 GB para ambientes de produção.
4. Recomendação: Antes de instalar uma atualização do XenMobile, use a funcionalidade na sua VM para tirar um instantâneo do seu sistema. Além disso, faça backup do seu banco de dados de configuração do sistema. Se tiver problemas durante uma atualização, backups completos permitirão fazer uma recuperação.

Para atualizar

Você pode atualizar diretamente do XenMobile 10.10.x ou 10.9.x para o XenMobile 10.11. Para realizar a atualização, baixe o binário mais recente disponível: acesse <https://www.citrix.com/downloads>. Navegue para **Citrix Endpoint Management (e Citrix XenMobile Server) > XenMobile Server (no local) > Product Software > XenMobile Server 10**. No bloco do software XenMobile Server, para o seu hipervisor, clique em **Download File**.

Use a página **Gerenciamento de versão** no console XenMobile. Para obter mais informações, consulte [Para atualizar usando a página Gerenciamento de versão](#).

Depois de atualizar

Após atualizar para o XenMobile 10.11 (no local):

Se a funcionalidade que envolve as conexões de saída deixar de funcionar e você não alterou a configuração de suas conexões, verifique os erros no log do XenMobile Server, como os seguintes: “Não é possível se conectar ao servidor VPP: o nome do host ‘192.0.2.0’ não corresponde à entidade do certificado fornecido pelo par”.

O erro de validação do certificado indica que você precisa desabilitar a verificação do nome do host no XenMobile Server. Como padrão, a verificação do nome do host está ativada nas conexões de saída, exceto para o servidor Microsoft PKI. Se a verificação do nome do host interromper sua implantação, altere a propriedade do servidor `disable.hostname.validation` para **true**. O valor padrão dessa propriedade é **false**.

Configurações de política de dispositivo novas e atualizadas para dispositivos Android Enterprise

Unificação de políticas Samsung Knox e Android Enterprise. Para dispositivos Android Enterprise executando Samsung Knox 3.0 ou posterior e Android 8.0 ou posterior: o Knox e o Android Enterprise são combinados em uma solução unificada de gerenciamento de perfil e dispositivo.

Defina as configurações do Knox na página Android Enterprise das seguintes políticas de dispositivo:

- **Política de dispositivo de atualização de SO.** Inclui configurações para atualizações do Samsung Enterprise FOTA.
- **Política de dispositivo de código secreto.**
- **Política de dispositivo de chave de licença MDM Samsung.** Configura a chave de licença Knox.
- **Configurações da política de dispositivo de restrições.**

The screenshot shows the 'Restrictions Policy' configuration page. The left sidebar lists platforms: iOS, macOS, Android, Android Enterprise (selected), Samsung SAFE, Samsung KNOX, Windows Phone, Windows Desktop/Tablet, Amazon, and Windows Mobile/CE. The main content area is titled 'Restrictions Policy' and includes a description: 'This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.' Below this, there are several sections of settings:

- Allow USB actions:** Debugging (OFF), File transfer (OFF).
- Network:** Allow VPN Configuration (ON), Android beam (ON), Allow configuring location provider (ON).
- Security:** Allow use of the status bar (OFF), Keep the keyguard from locking the device (OFF), Allow Account Management (OFF), Keep the device screen on (OFF), Allow cross profile copy and paste (OFF).

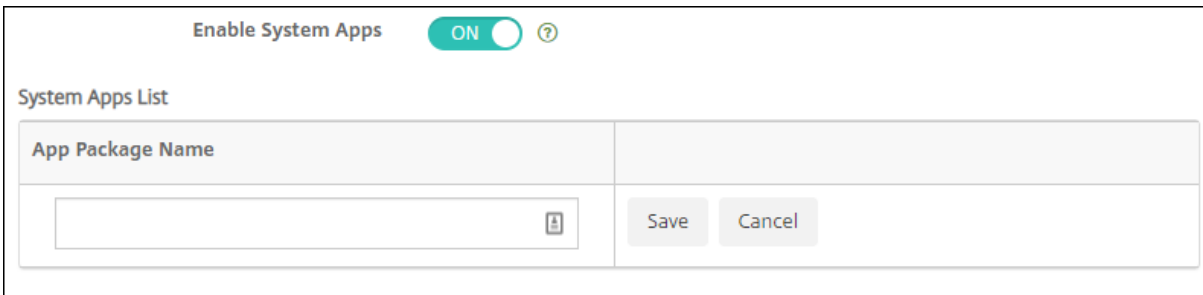
At the bottom right, there are 'Back' and 'Next >' buttons.

Política de dispositivo de inventário de aplicativos para Android Enterprise. Agora você pode coletar um inventário dos aplicativos Android Enterprise em dispositivos gerenciados. Veja [Política de dispositivo de inventário de aplicativos](#).

Acesse todos os aplicativos do Google Play na loja gerenciada do Google Play. A propriedade de servidor **Acesse todos os aplicativos na loja gerenciada do Google Play** torna todos os aplica-

tivos da loja pública do Google Play acessíveis a partir da loja gerenciada do Google Play. Definir esta propriedade como **true** acrescentará os aplicativos da loja pública do Google Play a uma lista de permissão para todos os usuários do Android Enterprise. Os administradores podem usar a [Política de dispositivo de restrições](#) para controlar o acesso a esses aplicativos.

Ativar aplicativos do sistema em dispositivos Android Enterprise. Para permitir que os usuários executem aplicativos de sistema pré-instalados no modo de perfil de trabalho do Android Enterprise ou no modo totalmente gerenciado, configure a [Política de dispositivo de restrições](#). Essa configuração concede ao usuário acesso a aplicativos de dispositivo padrão, como câmera, galeria e outros. Para restringir o acesso a um aplicativo específico, defina permissões de aplicativo usando a [Android Enterprise app permissions device policy](#).



App Package Name
<input type="text"/>

Suporte para dispositivos dedicados Android Enterprise. O XenMobile agora oferece suporte ao gerenciamento de dispositivos dedicados, anteriormente chamados de dispositivos corporativos para uso único (COSU).

Os dispositivos Android Enterprise dedicados são dispositivos totalmente gerenciados e dedicados a atender a um único caso de uso. Você restringe esses dispositivos a um aplicativo ou a um pequeno conjunto de aplicativos necessários para executar as tarefas necessárias para o caso de uso. Você também impede que os usuários habilitem outros aplicativos ou executem outras ações no dispositivo.

Para obter informações sobre como provisionar dispositivos Android Enterprise, consulte [Provisionamento de dispositivos Android Enterprise dedicados](#).

Política renomeada. Para alinhar com a terminologia do Google, a política de dispositivo de restrição de aplicativos Android Enterprise agora é chamada de configurações gerenciadas do Android Enterprise. Veja [Política de dispositivo de configurações gerenciadas do Android Enterprise](#).

Bloquear e redefinir senha para o Android Enterprise

O XenMobile agora suporta a ação de segurança Bloquear e Redefinir senha para dispositivos Android Enterprise. Esses dispositivos devem ser registrados no modo de perfil de trabalho executando o Android 8.0 e posterior.

- O código secreto enviado bloqueia o perfil de trabalho. O dispositivo não é bloqueado.

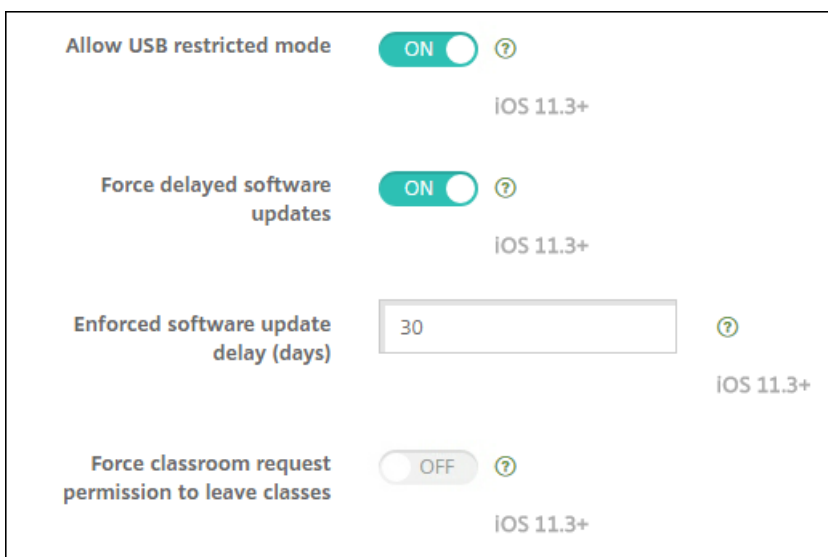
- Se nenhum código secreto for enviado ou se o código secreto enviado não atender aos requisitos de código secreto:
 - E nenhum código secreto estiver definido no perfil de trabalho, o dispositivo será bloqueado.
 - E um código secreto já estiver definido no perfil de trabalho, o perfil de trabalho será bloqueado, mas o dispositivo não será bloqueado.

Para obter mais informações sobre as ações de segurança de bloqueio e redefinição de senha, consulte [Ações de segurança](#).

Novas configurações da política de dispositivo de Restrições para iOS ou macOS

- **Aplicativos não gerenciados leem contatos gerenciados:** Opcional. Disponível somente se **Documentos de aplicativos gerenciados em aplicativos não gerenciados** estiver desativado. Se esta política estiver ativada, os aplicativos não gerenciados poderão ler dados dos contatos das contas gerenciadas. O padrão é **Desativado**. Disponível a partir do iOS 12.
- **Aplicativos gerenciados gravam contatos não gerenciados:** Opcional. Se habilitado, permite que aplicativos gerenciados gravem contatos nos contatos de contas não gerenciadas. Se **Documentos de aplicativos gerenciados em aplicativos não gerenciados** estiver habilitado, essa restrição não terá efeito. O padrão é **Desativado**. Disponível a partir do iOS 12.
- **Preenchimento automático da senha:** opcional. Se desativado, os usuários não poderão usar os recursos Senhas de Preenchimento automático ou Senhas de segurança automáticas. O padrão é **Ativado**. Disponível a partir do iOS 12 e do macOS 10.14.
- **Solicitações de proximidade de senha:** opcional. Se desativado, os dispositivos dos usuários não solicitam senhas de dispositivos próximos. O padrão é **Ativado**. Disponível a partir do iOS 12 e do macOS 10.14.
- **Compartilhamento de senha:** opcional. Se desativado, os usuários não poderão compartilhar suas senhas usando o recurso AirDrop Passwords. O padrão é **Ativado**. Disponível a partir do iOS 12 e do macOS 10.14.
- **Forçar data e hora automáticas:** supervisionado. Se ativado, os usuários não poderão desativar a opção **Geral > Data e hora > Definir automaticamente**. O padrão é **Desativado**. Disponível a partir do iOS 12.
- **Permitir o modo restrito de USB:** disponível apenas para dispositivos supervisionados. Se definido como Desativado, o dispositivo sempre poderá se conectar a acessórios USB enquanto estiver bloqueado. O padrão é **Ativado**. Disponível a partir do iOS 11.3.
- **Forçar atualizações de software atrasadas:** disponível apenas para dispositivos supervisionados. Se definido como **Ativado**, atrasa a visibilidade do usuário das atualizações de software. Com essa restrição em vigor, o usuário não verá uma atualização de software até que o número especificado de dias após a data de lançamento da atualização de software tenha passado. O padrão é **Desativado**. Disponível a partir do iOS 11.3 e do macOS 10.13.4.

- **Atraso forçado de atualização de software (dias):** disponível apenas para dispositivos supervisionados. Essa restrição permite que o administrador defina por quanto tempo adiar uma atualização de software no dispositivo. O máximo é 90 dias e o valor padrão é **30**. Disponível a partir do iOS 11.3 e do macOS 10.13.4.
- **Forçar solicitação de permissão de sala de aula para sair das aulas:** disponível apenas para dispositivos supervisionados. Se definido como **Ativado**, um aluno matriculado em um curso não gerenciado com Sala de aula deve solicitar permissão do professor quando tentar sair do curso. O padrão é **Desativado**. Disponível a partir do iOS 11.3.



Veja [Política de dispositivo de restrições](#).

Atualizações de política de dispositivo do Exchange para iOS ou macOS

Mais configurações de assinatura e criptografia S/MIME Exchange a partir do iOS 12. A política de dispositivo do Exchange agora inclui parâmetros para configurar a assinatura e criptografia S/MIME.

Para assinatura S/MIME:

- **Credencial de identidade de assinatura:** escolha a credencial de assinatura a ser usada.
- **Usuário de assinatura S/MIME substituível:** se definido como **On**, os usuários podem ativar e desativar a assinatura S/MIME nas configurações de seus dispositivos. O padrão é **Off**.
- **UUID de certificado de assinatura S/MIME substituível pelo usuário:** se definido como **On**, os usuários podem selecionar, nas configurações de seus dispositivos, a credencial de assinatura a ser usada. O padrão é **Off**.

Para criptografia S/MIME:

- **Credencial de identidade de criptografia:** escolha a credencial de criptografia a ser usada.
- **Ativar comutador de S/MIME por mensagem:** quando definido como **On**, mostra aos usuários uma opção para ativar ou desativar a criptografia S/MIME para cada mensagem que redigem. O

padrão é **Off**.

- **Criptografia S/MIME como padrão substituível pelo usuário:** se definido como **On**, os usuários podem, nas configurações de seus dispositivos, selecionar se S/MIME permanecerá ativa como padrão. O padrão é **Off**.
- **UUID de certificado de criptografia S/MIME substituível pelo usuário:** se definido como **On**, os usuários podem ativar e desativar a identidade da criptografia de S/MIME e a criptografia nas configurações de seus dispositivos. O padrão é **Off**.

Configurações de OAuth do Exchange a partir do iOS 12. Agora você pode configurar a conexão com o Exchange para usar o OAuth para autenticação.

Configurações de OAuth do Exchange a partir do macOS 10.14. Agora você pode configurar a conexão com o Exchange para usar o OAuth para autenticação. Para a autenticação usando OAuth, você pode especificar o URL de logon para uma configuração que não use a descoberta automática.

Veja [Política de dispositivo do Exchange](#).

Atualizações de política de dispositivo de email para iOS

Mais configurações de assinatura e criptografia S/MIME Exchange a partir do iOS 12. A política de dispositivo de email inclui mais parâmetros para configurar a assinatura e a encriptação S/MIME.

Para assinatura S/MIME:

- **Ativar assinatura S/MIME:** selecione se esta conta suporta ou não a assinatura S/MIME. O padrão é **On**. Quando definido como **On**, os campos abaixo são exibidos.
 - **Usuário de assinatura S/MIME substituível:** se definido como **On**, os usuários podem ativar e desativar a assinatura S/MIME nas configurações de seus dispositivos. O padrão é **Off**. Essa opção se aplica ao iOS 12.0 e posterior.
 - **UUID de certificado de assinatura S/MIME substituível pelo usuário:** se definido como **On**, os usuários podem selecionar, nas configurações de seus dispositivos, a credencial de assinatura a ser usada. O padrão é **Off**. Essa opção se aplica ao iOS 12.0 e posterior.

Para criptografia S/MIME:

- **Ativar criptografia S/MIME:** selecione se essa conta é compatível com a criptografia S/MIME. O padrão é **Off**. Quando definido como **On**, os campos abaixo são exibidos.
 - **Ativar comutador de S/MIME por mensagem:** quando definido como **On**, mostra aos usuários uma opção para ativar ou desativar a criptografia S/MIME para cada mensagem que redigem. O padrão é **Off**.
 - **Criptografia S/MIME como padrão substituível pelo usuário:** se definido como **On**, os usuários podem, nas configurações de seus dispositivos, selecionar se S/MIME permanecerá ativa como padrão. O padrão é **Off**. Essa opção se aplica ao iOS 12.0 e posterior.

- **UUID de certificado de criptografia S/MIME substituível pelo usuário:** se definido como **On**, os usuários podem ativar e desativar a identidade da criptografia de S/MIME e a criptografia nas configurações de seus dispositivos. O padrão é **Off**. Essa opção se aplica ao iOS 12.0 e posterior.

Veja [Política de dispositivo de email](#).

Atualizações da política de dispositivo de notificações de aplicativos para iOS

As seguintes configurações de notificações de aplicativos estão disponíveis a partir do iOS 12.

- **Exibir em Car Play:** se **I**, as notificações serão exibidas no Apple CarPlay. O padrão é **Ativado**.
- **Ativar alerta crítico:** se **I**, um aplicativo pode marcar uma notificação como uma notificação crítica que ignora as configurações de Não Perturbe e de toque. O padrão é **Desativado**.

Consulte [Política de dispositivo de notificações de aplicativo](#)

Suporte para iPads compartilhados usados com o Apple Educação

A integração do XenMobile com os recursos do Apple Educação agora oferece suporte a iPads compartilhados. Vários alunos em uma sala de aula podem compartilhar um iPad para diferentes disciplinas lecionadas por um ou vários instrutores.

Você ou os instrutores registram iPads compartilhados e implantam políticas de dispositivos, aplicativos e mídias nos dispositivos. Depois, os alunos fornecem suas credenciais gerenciadas do ID Apple para se conectar a um iPad compartilhado. Se você implantou anteriormente uma política de Configuração de Educação para estudantes, eles não mais se conectam como “Outro usuário” para compartilhar dispositivos.

Pré-requisitos para iPads compartilhados:

- Qualquer iPad Pro, iPad de 5ª geração, iPad Air 2, ou posterior, e iPad mini 4, ou posterior
- Pelo menos 32 GB de armazenamento
- Supervisionado

Para obter mais informações, consulte [Configurar iPads compartilhados](#).

Alteração de permissões de controle de acesso baseado em função (RBAC)

A permissão RBAC Adicionar/Excluir Usuários Locais agora está dividida em duas permissões: Adicionar usuários locais e Excluir usuários locais.

Para obter mais informações, consulte [Configurar funções com RBAC](#).

Avisos de terceiros

March 6, 2019

Esta versão do XenMobile pode incluir software de terceiros licenciado sob os termos definidos nos seguintes documentos:

[Avisos de terceiros do XenMobile](#)

Substituição

May 24, 2021

Os anúncios neste artigo destinam-se a fornecer um aviso prévio sobre recursos do XenMobile Server que estão sendo eliminados gradualmente. Fornecemos essas informações para que você possa tomar decisões comerciais oportunas. A Citrix monitora o uso e os comentários dos clientes para determinar quando serão eliminados. Os anúncios podem ser alterados em versões subsequentes e nem sempre incluirão todos os recursos ou funcionalidades preteridos. Para obter detalhes sobre o suporte ao ciclo de vida do produto, consulte o artigo [Política de suporte ao ciclo de vida do produto](#).

Substituições e remoções

A lista a seguir mostra os recursos do XenMobile Server que foram preteridos ou removidos.

Itens *preteridos* não são removidos imediatamente. A Citrix continua a oferecer suporte a um item preterido até removê-lo em uma versão futura.

Os itens *removidos* são removidos ou não são mais suportados pelo XenMobile Server.

Para obter informações sobre os aplicativos móveis de produtividade que atingiram o Fim da vida útil, consulte [EOL e aplicativos obsoletos](#).

Item	Descrição	Substituição anunciada	Removido	Alternativa
Knox Mobile Enrollment (DA legado)	Suporte preterido para Knox Mobile Enrollment (KME) no modo Administrador de dispositivo legado em todas as versões do Android.	4 de maio 2021	Meta: 30 de junho 2021	Use o KME para se registrar no modo Android Enterprise. Android 8, 9, 10, 11 suportam Android Enterprise.
Aplicativos de mobilidade Citrix e aplicativos Workspace para Android 7.x e iOS 12.x	Suporte preterido para as versões Android 7.x e iOS 12.x do Secure Hub, Secure Mail, Secure Web e aplicativo Citrix Workspace.	Abril 2021	Meta: junho 2021	No mínimo, use a versão atual e anterior de cada principal plataforma de sistema operacional. Dispositivos mais antigos permanecem registrados. No entanto, a Citrix não testa nem oferece suporte aos dispositivos legados.
Credenciais derivadas	Suporte preterido para credenciais derivadas e o aplicativo Citrix Derived Credentials Manager.	25 de março 2021	Meta: T2 2021	Consulte iOS para obter uma lista de tipos de autenticação compatíveis com iOS.

Item	Descrição	Substituição anunciada	Removido	Alternativa
Internet Explorer 11	Suporte preterido do uso do Internet Explorer com o console XenMobile Server.	Janeiro 2021	Janeiro 2021	Use a versão mais recente destes navegadores: Google Chrome, Mozilla Firefox, Microsoft Edge, Apple Safari
Suporte de token de software de RSA para Android	Suporte preterido para a importação direta de tokens de software de RSA para o Secure Hub para Android.	Janeiro 2021	Fevereiro 2021	Você pode importar o token de software de RSA dentro do aplicativo RSA de ID seguro disponível no Google Play. Depois você pode usar o token para autenticação do Citrix Gateway.
Android - Sony	Suporte preterido para dispositivos Android Sony e políticas específicas da Sony.	Janeiro 2021	Fevereiro 2021	Use o Android Enterprise
Android - HTC	Suporte preterido para dispositivos Android HTC e políticas específicas da HTC.	Janeiro 2021	Fevereiro 2021	Use o Android Enterprise

Item	Descrição	Substituição anunciada	Removido	Alternativa
Componente de terceiros do painel do XenMobile	Vamos substituir um componente de terceiros usado como parte do painel do XenMobile.	Dezembro 2020	Janeiro 2021	Para continuar usando o painel, atualize para o XenMobile 10.12 ou posterior
Aplicativos publicados para o modo Administrador do Dispositivo legado em dispositivos Android Enterprise	Nós não entregamos mais aplicativos publicados para a plataforma DA legada para dispositivos registrados no Android Enterprise.	Outubro 2020	Novembro 2020	Para dispositivos Android Enterprise, publique aplicativos para a plataforma Android Enterprise. Para continuar a publicar aplicativos de DA legados em dispositivos no modo DA, crie um grupo de entrega separado para esses aplicativos.

Item	Descrição	Substituição anunciada	Removido	Alternativa
Portas de saída de APNs	O suporte da Apple para o protocolo binário legado APNs termina em 31 de março de 2021. A Apple recomenda que você use a API do provedor de APNs baseada em HTTP/2. Como parte dessa mudança, estamos preterindo o suporte para as portas 2195 e 2196, usadas para enviar notificações APNs para *.push.apple.com .	Outubro 2020	Meta: abril 2021	Em vez disso, use a porta 443 ou 2197. Consulte Abrir portas do XenMobile para gerenciar dispositivos .
Contêiner Samsung SEAMS	Suporte preterido para o contêiner Samsung SEAMS.	Junho 2020	Agosto 2020	Utilize o aplicativo Samsung Knox Service Plug-in (KSP) para Android Enterprise. Consulte Adicionar o aplicativo Knox Service Plug-in .

Item	Descrição	Substituição anunciada	Removido	Alternativa
Certificados SSL (Secure Sockets Layer) autoassinados	Suporte preterido para certificados SSL autoassinados para todas as plataformas de dispositivos.	Maio 2020		Substitua seu certificado autoassinado existente por um certificado SSL confiável de uma autoridade de certificação (CA) conhecida.
Algoritmos de assinatura de autenticação baseada em certificado (não FIPS e codificação fraca)	Suporte preterido para os seguintes algoritmos de assinatura: SHA1withRSA, SHA224withRSA, SHA1withECDSA, SHA224withECDSA, SHA1withDSA, RIPEMD160withRS, RIPEMD128withRS, RIPEMD256withRS	Maio 2020	Janeiro 2021	Quando você criar um CSR para um provedor de credenciais no console XenMobile (Configurações > Provedores de credenciais > Solicitação de assinatura de certificado), escolha uma codificação mais forte.

Item	Descrição	Substituição anunciada	Removido	Alternativa
Servidores de banco de dados	Suporte preterido para Microsoft SQL Server 2012 R2 e anteriores e Microsoft SQL Server 2012 SP4 e anteriores.	Maio 2020	Agosto 2020	Atualize o sistema para uma das seguintes versões com suporte: Microsoft SQL Server 2014 SP3, Microsoft SQL Server 2016 SP2, Microsoft SQL Server 2017 CU 13 ou Microsoft SQL Server 2019 CTP 3.2. Consulte a lista de servidores suportados em Requisitos do sistema e compatibilidade .

Item	Descrição	Substituição anunciada	Removido	Alternativa
Hipervisores	Suporte preterido para Citrix XenServer 6.5.x e anteriores, VMware ESXi 5.5 Update 3 e anteriores, e Hyper-V 2012.	Maio 2020	Agosto 2020	Atualize o sistema para uma das seguintes versões com suporte: Citrix Hypervisor 8.0 e posterior, Citrix XenServer 7.0 e posterior, VMware (ESXi 6.0, ESXi 6.5.0 Update 3, ESXi 6.7 Update 2 patch 10 ou ESXi 7.0) ou Hyper-V (Windows Server 2016 ou Windows Server 2019).
Citrix Launcher	Suporte preterido para o aplicativo Citrix Launcher.	Maio 2020	Agosto 2020 (remover da loja de aplicativos)	Provisione dispositivos como quiosques (dispositivos dedicados). Para obter mais informações, consulte Substituição do Citrix Launcher .

Item	Descrição	Substituição anunciada	Removido	Alternativa
Aplicativos de mobilidade Citrix e aplicativos Workspace para Android 6.x e iOS 11.x	Suporte preterido para as versões Android 6.x e iOS 11.x do Secure Hub, Secure Mail, Secure Web e aplicativo Citrix Workspace.	Abril 2020	Junho 2020	No mínimo, use a versão atual e anterior de cada principal plataforma de sistema operacional.
MDX Toolkit e MDX Service	Suporte preterido para o MDX Toolkit e MDX Service em favor do SDK de gerenciamento de aplicativos móveis (MAM). Durante o período de transição, você pode usar aplicativos preparados MDX e aplicativos desenvolvidos por SDK MAM.	Março 2020	Meta: setembro 2021	Para continuar gerenciando seus aplicativos empresariais, use o MAM SDK.
MDX: Servidor de gateway alternativo	Autenticação aumentada preterida para dispositivos iOS e Android.	Março 2020	Meta: setembro 2021	Nenhuma alternativa

Item	Descrição	Substituição anunciada	Removido	Alternativa
MDX: micro VPN (modo de túnel completo)	Túnel completo de rede privada virtual (VPN) preterido para dispositivos iOS e Android.	Março 2020	Meta: setembro 2021	Use o modo SSO da Web do MAM SDK ou crie uma política VPN por aplicativo com o tipo de conexão Citrix SSO.
MDX: suporte a arquivos PAC	Suporte preterido a arquivo PAC (configuração automática de proxy) com uma implantação de túnel VPN completo para dispositivos iOS e Android.	Março 2020	Meta: setembro 2021	Use o Citrix Gateway para se conectar por meio de um servidor proxy para acesso a redes internas.
Suporte a dispositivos compartilhados MDX	Suporte a dispositivos compartilhados preterido para aplicativos MDX.	Março 2020	Meta: setembro 2021	Para Android Enterprise, use o suporte de dispositivos compartilhados para MDM. Para iOS, use o Apple School Manager ou o GroundControl.

Item	Descrição	Substituição anunciada	Removido	Alternativa
Novos registros de Administrador do Dispositivo para Android 10	Suporte preterido para novos registros e renovações de registro no modo Administrador do Dispositivo legado em dispositivos Android 10. Os dispositivos já registrados continuam funcionando.	Fevereiro 2020	Setembro 2020	Registre novos dispositivos Android 10+ no Android Enterprise.
Modo Administrador de Dispositivo legado para dispositivos Android 10	Google preteriu algumas APIs do Device Administrator. A Citrix não oferece compatibilidade para dispositivos Android 10 registrados no modo Administrador de Dispositivo a partir da atualização para o Citrix Secure Hub que visa o nível 29 da API Android.	Fevereiro 2020	Novembro 2020	Migrar dispositivos Android 10 para Android Enterprise.

Item	Descrição	Substituição anunciada	Removido	Alternativa
Criptografia MDX	Preterida a criptografia MDX e o recurso de criptografia MDX no console XenMobile.	Outubro 2019	Setembro 2020	Ative a criptografia da plataforma iOS ou Android usando nosso recurso Gerenciamento de Criptografia com verificação de conformidade adicional. Certifique-se de ter testado e planejado a migração da criptografia MDX até julho de 2020.

Item	Descrição	Substituição anunciada	Removido	Alternativa
Política de dispositivo de código secreto: a configuração Sem Restrições para Android Enterprise	Dispositivos Android Enterprise com Android 7 ou superior só oferecem suporte a código secreto criado sem restrições de caracteres. Se você definiu anteriormente Caracteres obrigatórios como Sem restrições , essa atualização altera o valor para Apenas números .	Fevereiro 2019	Abril 2019	Esta alteração não afeta a experiência de logon do usuário atual.
Suporte remoto	Preterido o cliente de suporte remoto para implantações do XenMobile Server em cluster no local.	Janeiro 2019	Agosto 2020	Nenhuma alternativa

Item	Descrição	Substituição anunciada	Removido	Alternativa
Extensões de Rede Secure Hub para iOS	Preterida a estrutura de Extensão de Rede que lhe permitia personalizar funcionalidades de rede para dispositivos iOS, a partir do Secure Hub versão 20.3.0.	Outubro 2018	Março 2020	Nenhuma alternativa
Versões de TLS 1.0 e 1.1	Para melhorar a segurança do XenMobile, a Citrix agora bloqueia qualquer comunicação sobre Transport Layer Security (TLS) 1.0 e 1.1. Como resultado de sua segurança enfraquecida, o PCI Council depreciou o TLS 1.0 e TLS 1.1.	Junho 2018	Março 2019	Atualize para TLS 1.2.
Windows Mobile/CE	Suporte preterido para dispositivos Windows Mobile/CE.	Abril 2018	Setembro 2020	Use computadores e notebooks com Windows 10.

Item	Descrição	Substituição anunciada	Removido	Alternativa
Android TouchDown	A DigiCert parou o suporte para Android TouchDown. A Citrix removerá a página da plataforma Android TouchDown da política de dispositivo Exchange.	Julho 2018	2021	Recomendação: use o Citrix Secure Mail.

Problemas resolvidos

August 20, 2021

O XenMobile 10.13 inclui os seguintes problemas resolvidos:

- O XenMobile Server tem um erro de comunicação com os Programas de Implantação da Apple (anteriormente DEP). Para obter mais informações, consulte <https://support.citrix.com/article/CTX267079>. [CXM-76053]
- Não é possível carregar aplicativos públicos do iOS na App Store usando o URL da App Store. [CXM-76900]
- O ID de usuário em um único dispositivo é mapeado para vários IDs de usuário. [CXM-76915]
- Deadlocks intermitentes no servidor de banco de dados causam falhas de registro. [CXM-77336]
- Os administradores com a permissão RBAC para enviar convites de registro podem exportar convites ilimitados. [CXM-77340]
- Não é possível carregar aplicativos públicos do iOS na App Store usando as APIs públicas para XenMobile. [CXM-77656]
- Para alguns poucos aplicativos instalados, a versão está em branco para o inventário de aplicativos exibido na página **Gerenciar > Dispositivos > Detalhes do dispositivo**. [CXM-79025]
- Você não pode usar o console XenMobile Server para editar a política de dispositivos do Exchange. [CXM-79080]

- Você não pode usar o console XenMobile Server para atualizar a versão de alguns aplicativos VPP. Você recebe o seguinte erro: **Ocorreu um erro de configuração. Tente novamente.** [CXM-79728]
- Os aplicativos de compra por volume do Apple iTunes não podem ser sincronizados com o XenMobile. [CXM-80064]
- Não é possível usar a política de dispositivo de configurações gerenciadas com um aplicativo Knox Service Plug-in. [CXM-80233]
- Não é possível importar o arquivo enterprise.config no XenMobile Server. Você recebe o seguinte erro: **Não foi possível importar o certificado.** [CXM-80737]
- Aplicativos MDX obrigatórios e opcionais adicionados após o registro não são exibidos na Play Store. [CXM-80961]
- Você não pode acessar o console XenMobile Server usando portas personalizadas. [CXM-81841]
- Não é possível configurar vários marcadores devido ao limite de caracteres no campo **Marcadores gerenciados.** [CXM-82524]
- No XenMobile Server, **Verificar se há atualizações** não funciona para Detalhes do aplicativo. [CXM-84259]
- No XenMobile Server, você não pode instalar aplicativos do Google Play gerenciado ao se registrar com **SamAccountName.** [CXM-84973]
- O registro de gerenciamento de dispositivos móveis (MDM) de dispositivos que executam o iOS 14 falha consistentemente quando a propriedade do servidor ios.mdm.enrollment.installRootCalfRequired é definida como true.[CXM-85028]
- Dois certificados PKC12 são criados para o mesmo usuário, resultando em acesso intermitente à rede interna desse usuário. [CXM-87288]
- Para problemas corrigidos relacionados a aplicativos móveis de produtividade, consulte [Secure Hub](#), [Secure Mail](#) e [Secure Web](#).
- Para problemas corrigidos no lançamento do pacote progressivo na versão 10.12.0, consulte:
 - [Pacote progressivo 8, XenMobile Server 10.12.0](#)
 - [Pacote progressivo 7, XenMobile Server 10.12.0](#)
 - [Pacote progressivo 6, XenMobile Server 10.12.0](#)

Informações correlatas

- [Suporte do XenMobile Knowledge Center](#)

Problemas conhecidos

March 5, 2021

No XenMobile 10.13 existem os seguintes problemas conhecidos.

- Depois de importar a imagem do XenMobile Server 10.8 ou 10.9 para o VMware ESXi 6.7 ou 6.5 Atualização 2: após reiniciar a máquina virtual, o aplicativo de configuração não inicia, o XenMobile Server entra no modo de recuperação e as configurações de IP são limpas. Como solução alternativa a esse problema, crie uma nova máquina virtual com uma NIC VMXNET3 e, em seguida, associe essa máquina virtual ao banco de dados da máquina virtual que entrou no modo de recuperação. [CXM-54581]
- Para problemas conhecidos relacionados a aplicativos móveis de produtividade, consulte [Secure Hub](#), [Secure Mail](#) e [Secure Web](#).
- Para problemas conhecidos no mais recente lançamento do pacote progressivo na versão 10.12.0, consulte:
 - [Pacote progressivo 5, XenMobile Server 10.12.0](#)

Informações correlatas

- [Suporte do XenMobile Knowledge Center](#)

Arquitetura

November 30, 2020

Os requisitos de gerenciamento de dispositivo e aplicativo da sua organização determinam os componentes do XenMobile em sua arquitetura XenMobile. Os componentes do XenMobile são modulares e se baseiam uns nos outros. Por exemplo, sua implantação inclui o Citrix Gateway:

- O Citrix Gateway oferece aos usuários acesso remoto a aplicativos móveis e rastreia os tipos de dispositivos de usuários.
- O XenMobile é onde você gerencia esses aplicativos e dispositivos.

Implantando componentes do XenMobile: você pode implantar o XenMobile para permitir que os usuários se conectem aos recursos na sua rede interna das seguintes maneiras:

- Conexões com a rede interna. Se os seus usuários forem remotos, eles poderão se conectar usando uma VPN ou uma conexão micro VPN por meio do Citrix Gateway. Essa conexão fornece acesso a aplicativos e áreas de trabalho na rede interna.

- Registro do dispositivo. Os usuários podem registrar dispositivos móveis no XenMobile para que você possa gerenciá-las no console XenMobile que se conecta aos recursos de rede.
- Aplicativos Web, SaaS e móveis. Os usuários podem acessar aplicativos Web, SaaS e móveis do XenMobile por meio do Secure Hub.
- Aplicativos e áreas de trabalho virtuais baseados no Windows. Os usuários podem se conectar com o Citrix Receiver ou um navegador da Web para acessar aplicativos e áreas de trabalho virtuais baseados no Windows do StoreFront ou na Web Interface.

Para obter algumas dessas capacidades para um XenMobile Server local, a Citrix recomenda a implantação dos componentes do XenMobile na seguinte ordem:

- Citrix Gateway. Você pode definir as configurações do Citrix Gateway para permitir a comunicação com o XenMobile, o StoreFront ou a Web Interface usando o assistente de Configuração Rápida. Antes de usar o assistente de Configuração Rápida no Citrix Gateway, você deve instalar um dos seguintes componentes para configurar as comunicações: XenMobile, StoreFront ou Web Interface.
- XenMobile. Depois de instalar o XenMobile, você poderá definir políticas e configurações no console XenMobile, o que permite que os usuários registrem os dispositivos móveis dele. Você também pode configurar aplicativos móveis, Web e SaaS. Os aplicativos móveis podem incluir aplicativos da Apple App Store ou do Google Play. Os usuários também podem se conectar com aplicativos móveis que você prepara usando o MDX Toolkit e carrega para o console.
- MAM SDK ou MDX Service. A tecnologia de preparação MDX está programada para atingir o fim da vida útil (EOL) em setembro de 2021. Para continuar gerenciando seus aplicativos empresariais, você deve incorporar o SDK MAM.
 - O SDK de Gerenciamento de Aplicativos Móveis (MAM) fornece funcionalidade MDX que não é coberta pelas plataformas iOS e Android. Você pode habilitar com MDX e proteger aplicativos iOS ou Android. Você disponibiliza esses aplicativos em uma loja interna ou em lojas de aplicativos públicas. Veja [MDX App SDK](#).
 - O MDX Service prepara com segurança os aplicativos móveis criados dentro da sua organização ou fora da sua empresa. Para obter mais informações, consulte [MDX Service](#).
- StoreFront (opcional). Você pode fornecer acesso a aplicativos e áreas de trabalho virtuais baseados no Windows do StoreFront por meio de conexões com o Receiver.
- Citrix Files (opcional). Se você implantar o Citrix Files, poderá ativar a integração de diretório empresarial por meio do XenMobile, que atua como um provedor de identidade Security Assertion Markup Language (SAML). Para obter mais informações sobre a configuração de provedores de identidade para o Citrix Content Collaboration, consulte o site de suporte do Content Collaboration.

O XenMobile oferece gerenciamento de dispositivo e de aplicativo por meio do console XenMobile. Esta seção descreve a arquitetura de referência da implantação do XenMobile.

Em um ambiente de produção, a Citrix recomenda a implantação da solução XenMobile em uma configuração de cluster para escalabilidade e redundância de servidor. Além disso, o uso da capacidade de Descarga de SSL do Citrix ADC pode reduzir ainda mais a carga no XenMobile Server e aumentar a taxa de transferência. Para obter mais informações sobre como configurar o clustering para o XenMobile mediante a configuração de dois endereços IP virtuais de balanceamento de carga no Citrix ADC, consulte [Armazenamento em cluster](#).

Para obter mais informações sobre como configurar o XenMobile para uma implantação de recuperação de desastres, consulte o artigo [Recuperação de desastres](#) do manual de implantação. Esse artigo inclui um diagrama da arquitetura.

As seções a seguir descrevem diferentes arquiteturas de referência para a implantação do XenMobile. Para obter um diagrama detalhado da arquitetura de referência, consulte os artigos do XenMobile Deployment Handbook, [Arquitetura de referência para implantações locais](#) e [Arquitetura](#). Para obter uma lista completa de portas, consulte [Requisitos de porta](#) (no local) e [Requisitos de porta](#) (na nuvem).

Modo de gerenciamento de dispositivo móvel (MDM)

Importante:

Se você configurar o modo MDM e depois mudar para o modo ENT, certifique-se de usar a mesma autenticação (Active Directory). O XenMobile não dá suporte à alteração para o modo de autenticação após o registro de usuário. Para obter mais informações, consulte [Atualize do XenMobile MDM Edition para Enterprise Edition](#).

O XenMobile MDM Edition permite o gerenciamento de dispositivos móveis. Para obter suporte à plataforma, consulte [Sistemas operacionais compatíveis de dispositivos](#). Implante o XenMobile no modo MDM se você planejar usar somente os recursos MDM do XenMobile. Por exemplo, se você deseja fazer o seguinte.

- Implantar aplicativos e políticas de dispositivo.
- Recuperar inventários de ativos.
- Executar ações em dispositivos, como um apagamento de dispositivo.

No modelo recomendado, o XenMobile Server é posicionado no DMZ com um Citrix ADC opcional na frente, o que oferece uma proteção adicional ao XenMobile.

Modo de gerenciamento de aplicativos móveis (MAM)

MAM, também chamado de modo somente MAM, oferece gerenciamento de aplicativos móveis. Para obter suporte à plataforma, consulte [Sistemas operacionais compatíveis de dispositivos](#). Implante o XenMobile no modo MAM se você planejar usar somente os recursos MAM do XenMobile sem registrar dispositivos para o MDM. Por exemplo, se você deseja fazer o seguinte.

- Proteger aplicativos e dados em dispositivos móveis BYO.

- Fornecer aplicativos móveis empresariais.
- Bloquear aplicativos e apagar os respectivos dados.

Os dispositivos não podem registrados no MDM.

Nesse modelo de implantação, o XenMobile Server é posicionado com o Citrix Gateway na frente, o que oferece uma proteção adicional ao XenMobile.

Modo MDM+MAM

O uso dos modos MDM e MAM juntos permite o gerenciamento de aplicativos e dados móveis e o gerenciamento de dispositivos móveis. Para obter suporte à plataforma, consulte [Sistemas operacionais compatíveis de dispositivos](#). Implante o XenMobile no modo ENT (empresa) se você planejar usar os recursos do MDM+MAM do XenMobile. Por exemplo, se você desejar:

- Gerenciar um dispositivo emitido pela empresa por meio do MDM
- Implantar aplicativos e políticas de dispositivo
- Recuperar um inventário de ativos
- Apagar dispositivos
- Fornecer aplicativos móveis empresariais
- Bloquear aplicativos e apagar os dados nos dispositivos

No modelo de implantação recomendado, o XenMobile Server é posicionado no DMZ com um Citrix Gateway na frente, o que oferece uma proteção adicional ao XenMobile.

XenMobile na rede interna: outra opção de implantação é posicionar um XenMobile Server local na rede interna, em vez de no DMZ. Essa implantação será usada se a sua política de segurança exigir que somente os dispositivos de rede possam ser colocados no DMZ. Nessa implantação, o XenMobile Server não está na DMZ. Portanto, não há a necessidade de abrir portas no firewall interno para permitir o acesso ao SQL Server e aos servidores PKI do DMZ.

Requisitos do sistema e compatibilidade

April 1, 2021

Nota:

Este artigo aborda os requisitos do sistema e a compatibilidade do XenMobile Server 10.13. Para os requisitos do sistema para o Endpoint Management, consulte [Requisitos do sistema](#).

Para conhecer mais requisitos e informações sobre compatibilidade, consulte os seguintes artigos:

- [Compatibilidade do XenMobile](#)
- [Sistemas operacionais compatíveis de dispositivos](#)

- [Requisitos de porta](#)
- [Escalabilidade](#)
- [Licenciamento](#)
- [Conformidade com FIPS 140-2](#)
- [Suporte a idiomas](#)

Para executar o XenMobile 10.13, você precisa atender aos seguintes requisitos mínimos do sistema:

- Uma das seguintes opções:
 - Citrix Hypervisor 8.1 ou 8.0, ou Citrix XenServer (versões com suporte: 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 8.0, 8.1, 8.2); para obter detalhes, consulte [XenServer](#)
 - VMware (versões com suporte: ESXi 6.0, ESXi 6.5.0 Update 3 ou ESXi 6.7 Update 2 patch 10, ESXi 7.0); para obter detalhes, consulte Solução alternativa ESXi 6.7 e [VMware](#)
 - Hyper-V (versões com suporte: Windows Server 2016 e Windows Server 2019); para obter detalhes, consulte [Hyper-V](#)
- Conector de Endpoint Management para Exchange ActiveSync 10.1.10 ou conector Citrix Gateway para Exchange ActiveSync 8.5.3.19
- Processador dual core
- Quatro CPUs virtuais
- 8 GB de RAM para ambientes de produção; 4 GB de RAM para implantações de prova de conceito e ambientes de teste
- 50 GB de espaço em disco
- Citrix License Server 11.16.

Atualize o seu servidor de licenças antes de atualizar o seu XenMobile Server.

Solução alternativa ESXi 6.7

Para que o ESXi 6.7 funcione, você deve executar a seguinte solução alternativa.

1. Usando a ferramenta OVF fornecida pela VMware, extraia o arquivo OVA baixado do site citrix.com. Obtenha a ferramenta OVF na página da VMware(<https://my.vmware.com/group/vmware/details?downloadGroup=OVFTOOL410&productId=491>).
2. Dos três arquivos extraídos, carregue o arquivo .vmdk no seu armazenamento de dados.
3. Crie uma nova máquina virtual.
 - a) Nomeie a máquina virtual e selecione **Máquina virtual ESX/ESXi 4.x** como a opção de compatibilidade.
 - b) Para a família do SO Convidado, selecione **Linux**.
 - c) Para a versão do SO convidado, selecione **Outro Linux 2.6.x (64 bits)**.
 - d) Para armazenamento de dados, selecione **Padrão**.

- e) Durante a personalização, remova o disco rígido padrão, o controlador USB e a unidade de CD/DVD.
 - f) Em Rede, como o tipo de adaptador, selecione **VMXNET3**.
 - g) No ESXi, se seus discos forem locais, selecione **Controller SCSI** e **LSI Logic Parallel**. Se você estiver usando um disco compartilhado, selecione **VMware Paravirtual**.
 - h) Clique em Avançar para concluir a criação da máquina virtual.
4. Navegue até o seu armazenamento de dados e copie o arquivo .vmdk que você carregou anteriormente. Copie-o para o diretório da máquina virtual que você criou para o XenMobile.
 5. Na interface da Web do ESXi, selecione a máquina virtual e edite as configurações.
 6. Clique em **Adicionar disco rígido**.
 7. Selecione o arquivo .vmdk copiado anteriormente e anexe-o à máquina virtual.
 8. Clique em **Salvar**.
 9. Ligue a sua máquina virtual.

Requisitos do sistema do Citrix Gateway

Para executar o Citrix Gateway com o XenMobile 10.13, você precisa atender aos seguintes requisitos mínimos do sistema.

- Citrix Gateway (local). Versões suportadas: 12.1 ou superior
- Você também precisa ser capaz de se comunicar com o Active Directory, o que requer uma conta de serviço. Você só precisa ter o acesso de consulta e leitura.

Requisitos de banco de dados do XenMobile 10.13

O XenMobile requer um dos seguintes bancos de dados:

- Microsoft SQL Server

O XenMobile dá suporte a um banco de dados do Microsoft SQL Server executando uma das seguintes versões com suporte. Para obter mais informações sobre bancos de dados do Microsoft SQL Server e seus requisitos de hardware, consulte a documentação da Microsoft.

- Microsoft SQL Server 2014 SP3
- Microsoft SQL Server 2016 SP2
- Microsoft SQL Server 2017 CU 21
- Microsoft SQL Server 2019 CU 8

Seus requisitos de banco de dados do Microsoft SQL Server também dependem do tamanho de sua implantação. Para obter mais informações sobre os requisitos de banco de dados do Microsoft SQL Server para o tamanho da sua implantação, consulte [Escalabilidade](#).

O XenMobile dá suporte a Grupos de disponibilidade básicos SQL (Grupos de disponibilidade Always On) e ao Clustering SQL para alta disponibilidade de banco de dados.

A Citrix recomenda usar o Microsoft SQL remotamente.

Para obter informações sobre como atualizar o Microsoft SQL, consulte o artigo da Microsoft [Atualizar o SQL Server](#).

- PostgreSQL (apenas para ambientes de teste). PostgreSQL está incluído no XenMobile. Você pode usá-lo localmente ou remotamente em ambientes de teste. A migração de banco de dados não é compatível. Você não pode mover os bancos de dados criados em um ambiente de teste para um ambiente de produção.

Todas as edições do XenMobile dão suporte ao Remote PostgreSQL 9.5.1 e 9.5.11 para Windows, com as seguintes limitações: não recomendado para ambientes de produção. Suporte para até 300 dispositivos. Uso do SQL Server no local por mais de 300 dispositivos. Sem suporte para clusters.

Requisitos da conta de serviço do SQL Server

Verifique se a conta de serviço do SQL Server a ser usada com o XenMobile tem a permissão de função [DBcreator](#). Registre a senha da conta do SQL Server especificada durante a instalação do XenMobile Server. Essa senha é necessária se você precisar clonar o banco de dados do XenMobile durante a recuperação do XenMobile Server.

Proteja seus bancos de dados do SQL Server usando a criptografia de dados transparente (TDE). Não permita acesso externo às portas do SQL Server, conforme mostrado na arquitetura de referência em [Arquitetura de referência para implantações locais](#).

Para obter mais informações sobre as contas de serviço do SQL Server, consulte as páginas abaixo no site de documentação da Microsoft. Esses links apontam para informações do SQL Server 2014. Se você estiver usando uma versão diferente, escolha sua versão do servidor na lista **Outras versões**:

- [Configurar contas de serviço e permissões do Windows](#)
- [Funções de nível de servidor](#)

Compatibilidade de Áreas de trabalho e aplicativos virtuais

- Virtual Apps and Desktops 7.15 LTSR CU3
- Virtual Apps and Desktops 7.1811
- Virtual Apps and Desktops 7 1906
- Virtual Apps and Desktops 7 1909
- Virtual Apps and Desktops 7 2006

Compatibilidade do StoreFront

- StoreFront 3.12.2

- StoreFront 7 1811
- StoreFront 7 1906
- StoreFront 7 1909
- StoreFront 7 2006

Outra compatibilidade

- Conector Endpoint Management para Exchange ActiveSync 10.1.10
 - Versões mais antigas não são testadas
- Conector Citrix Gateway para Exchange ActiveSync 8.5.3.19
 - Versões mais antigas não são testadas

Compatibilidade do XenMobile

March 5, 2021

Nota:

Este artigo aborda a compatibilidade do XenMobile Server. Para componentes testados com o Endpoint Management, consulte [Compatibilidade do Endpoint Management](#).

Para usar os novos recursos, correções e atualizações de políticas, a Citrix recomenda que você instale a versão mais recente do seguinte:

- A Citrix recomenda que você integre o SDK de Gerenciamento de Aplicativos Móveis (MAM) com aplicativos empresariais iOS e Android para aplicar recursos MDX aos aplicativos.
O MDX Service e o MDX Toolkit estão programados para atingir o fim da vida útil (EOL) em setembro de 2021. Para continuar gerenciando seus aplicativos empresariais, você deve incorporar o SDK MAM.

Este artigo resume as versões dos componentes do XenMobile com suporte que você pode integrar.

Versões com suporte e caminhos de atualização

As versões mais recentes do Secure Hub, do MDX Toolkit e dos aplicativos móveis de produtividade são compatíveis com a versão mais recente, além das duas versões anteriores do XenMobile Server.

A versão mais recente dos aplicativos móveis de produtividade requer a versão mais recente do Secure Hub. As duas versões anteriores dos aplicativos são compatíveis com o Secure Hub mais recente. Para obter detalhes, consulte a [Citrix Product Matrix](#).

A Citrix oferece suporte à distribuição de aplicativos de produtividade XenMobile somente a partir de uma loja de aplicativos pública.

XenMobile Server (no local)

- A Citrix oferece suporte a atualizações das duas últimas versões do XenMobile Server.
- Última versão do XenMobile Server:
 - XenMobile Server 10.13
- Atualizar de:
 - XenMobile Server 10.12.x
 - XenMobile Server 10.11.x

Aplicativos móveis de produtividade

Os usuários obtêm os aplicativos móveis de produtividade da loja de aplicativos pública. A versão mais recente dos aplicativos móveis de produtividade requer a versão mais recente do Secure Hub. As duas versões anteriores dos aplicativos são compatíveis com o Secure Hub mais recente.

Para obter mais informações sobre o período de lançamento em fases de duas semanas dos aplicativos móveis de produtividade, consulte [Cronograma de versão](#). Para obter detalhes de suporte, consulte [Suporte para aplicativos móveis de produtividade](#).

SDK MAM

O SDK MAM fornece funcionalidade MDX que não é coberta pelas plataformas iOS e Android. Você disponibiliza esses aplicativos em uma loja interna ou em lojas de aplicativos públicas. Consulte [MDX App SDK](#).

MDX Toolkit e MDX Service

A tecnologia de preparação MDX está programada para atingir o fim da vida útil (EOL) em setembro de 2021. Para continuar gerenciando seus aplicativos empresariais, você deve incorporar o SDK MAM.

- A Citrix oferece suporte para as três versões mais recentes (n.n.n) do MDX Toolkit. Consulte [Novidades do MDX Toolkit](#).
- Ou, você pode usar o MDX Service para preparar aplicativos. Consulte [MDX Service](#).

Suporte a navegadores

O console XenMobile Server requer um dos seguintes navegadores da Web compatíveis:

- Versão mais recente do Google Chrome
- Versão mais recente de Mozilla Firefox
- Versão mais recente de Microsoft Edge
- Versão mais recente de Apple Safari

Sistemas operacionais compatíveis de dispositivos

April 26, 2021

Nota:

Este artigo aborda os sistemas operacionais de dispositivos compatíveis com o XenMobile Server 10.13. Para sistemas operacionais compatíveis com o Endpoint Management, consulte [Sistemas operacionais compatíveis de dispositivos](#).

O XenMobile é compatível com dispositivos que executam as seguintes plataformas e sistemas operacionais para gerenciamento de mobilidade corporativa, incluindo gerenciamento de aplicativos e dispositivos. Devido a restrições de plataforma e recursos de segurança, o XenMobile não dá suporte a todas as funcionalidades em todas as plataformas.

As informações de plataforma de dispositivo com suporte neste artigo também se aplicam ao conector do XenMobile para Exchange ActiveSync e ao conector Citrix Gateway para Exchange ActiveSync.

Para obter as versões mais recentes dos aplicativos móveis de produtividade, bem como os dispositivos suportados para criptografia MDX, consulte [Suporte para aplicativos móveis de produtividade](#).

Nota:

A Citrix dá suporte pelo menos à versão atual e anterior de cada principal plataforma de sistema operacional. Nem todos os recursos da versão mais recente do Endpoint Management funcionam em versões mais antigas da plataforma.

Para anúncios de substituição, consulte [Substituição](#).

Lista de compatibilidade com o sistema operacional

O Citrix XenMobile suporta os seguintes sistemas operacionais:

Nota:

O suporte para as versões Android 7.x e iOS 12.x do Secure Hub, Secure Mail, Secure Web e aplicativo Citrix Workspace terminou em abril de 2021.

- **Android:** 8.x, 9.x, 10.x, 11.x

Para Android 10+, consulte [Considerações sobre Android](#).

- **iOS:** 13.x, 14.x

O XenMobile e os aplicativos móveis Citrix são compatíveis com o iOS 14.x, mas atualmente não são compatíveis com todos os novos recursos do iOS 14.x. Atualmente, o MDX Service não suporta preparar aplicativos iOS para iOS 14.x. Para preparar aplicativos empresariais internos para iOS 14.x, use o MDX Toolkit 20.8.5 ou posterior.

- **iPadOS:** 13.x, 14.x

O XenMobile e os aplicativos móveis Citrix são compatíveis com o iPadOS 14.x, mas atualmente não são compatíveis com todos os novos recursos do iPadOS 14.x.

- **macOS:** 10.13x, 10.14x, 10.15x, 11.x

O XenMobile e os aplicativos móveis Citrix são compatíveis com o macOS 11, mas atualmente não são compatíveis com todos os novos recursos do iOS macOS11.

- **Desktops e tablets Windows 10:** Windows 10 RS4 e RS5 (somente MDM)

- **Windows Phone:** (somente MDM). Windows Phone 8.1, Windows Phone 10, Windows 10 RS4 e RS5

- **Windows Mobile/CE:** (somente MDM). Desde o segundo trimestre de 2018, o suporte para dispositivos Windows Mobile/CE não está mais disponível.

- **Samsung SAFE e Knox:** em dispositivos Samsung compatíveis, o XenMobile dá suporte às políticas do Samsung for Enterprise (SAFE) e do Samsung Knox e as estende. O XenMobile requer que você habilite as APIs SAFE antes de implantar políticas e restrições SAFE. Para fazer isso, implante a chave interna Samsung Enterprise License Management (ELM) em um dispositivo. Consulte [Política de dispositivo de chave de licença MDM Samsung](#).

Considerações sobre Android

Antes de atualizar para o Android 10 ou posterior, consulte [Migrar do Device Administration para o Android Enterprise](#) para obter informações sobre como a substituição de APIs do Google Device Administration afeta os dispositivos que executam o Android 10.

- A Citrix recomenda que você evite registrar dispositivos Android 10 no modo de administração de dispositivos legados. O Google está substituindo as APIs do Device Administration, o que afeta os dispositivos que executam o Android 10+. Depois que as APIs forem preteridas, o registro de dispositivos Android 10+ no modo de administração de dispositivos legados apresentará falha. A Citrix não oferece suporte ao registro de dispositivos Android 11 no modo de administração de dispositivos.
- A Citrix recomenda o uso do Android Enterprise para dispositivos Android 10. Para obter mais informações, consulte [Migrar do Device Administration para o Android Enterprise](#).
- A alteração da API do Google não afeta os dispositivos registrados no modo somente MAM.

Antes de atualizar:

- Certifique-se de que sua infraestrutura de servidor está em conformidade com os certificados de segurança que tenham um nome de host correspondente na extensão subjectAltName (SAN).

- Para confirmar um nome de host, o servidor deve apresentar um certificado com uma SAN correspondente. A Citrix confia em certificados somente se eles contiverem uma SAN que corresponda ao nome de host.

Requisitos de porta

May 24, 2021

Para ativar a comunicação dos dispositivos e dos aplicativos com o XenMobile, você abre portas específicas nos seus firewalls. As tabelas a seguir listam as portas que devem estar abertas.

Abrir portas para o Citrix Gateway e o XenMobile gerenciarem aplicativos

Abra as seguintes portas para permitir conexões de usuário do Citrix Secure Hub, do Citrix Receiver e do Citrix Gateway Plug-in por meio do Citrix Gateway com os seguintes componentes:

- XenMobile
- StoreFront
- Citrix Virtual Apps and Desktops
- Conector Citrix Gateway para Exchange ActiveSync
- Outros recursos da rede internos, como sites da intranet

Para ativar o tráfego para iniciar Darkly do Citrix ADC, você pode usar os endereços IP anotados neste [artigo do Support Knowledge Center](#).

Para obter mais informações sobre o Citrix Gateway, consulte a documentação do Citrix Gateway. Essa documentação contém informações sobre os endereços IP do Citrix ADC (NSIP), IP de servidor virtual (VIP) e IP de sub-rede (SNIP).

Porta TCP	Descrição	Origem	Destino
21 ou 22	Usada para enviar pacotes de suporte para um servidor FTP ou SCP.	XenMobile	Servidor FTP ou SCP
53 (TCP e UDP)	Usada para conexões DNS.	Citrix Gateway, XenMobile	Servidor DNS

Porta TCP	Descrição	Origem	Destino
80	O Citrix Gateway transmite a conexão VPN para o recurso da rede interna por meio do segundo firewall. Geralmente, essa situação ocorre quando os usuários fazem login com o Citrix Gateway Plug-in.	Citrix Gateway	Sites da Intranet
80 ou 8080; 443	Porta XML e Secure Ticket Authority (STA) usada para enumeração, emissão de tíquetes e autenticação. A Citrix recomenda usar a porta 443.	Tráfego de rede do StoreFront e Web Interface XML; Citrix Gateway STA	Áreas de trabalho e aplicativos virtuais
123 (TCP e UDP)	Usada para os serviços do protocolo NTP.	Citrix Gateway; XenMobile	Servidor NTP
389	Usada para conexões LDAP não seguras	Citrix Gateway; XenMobile	Servidor de autenticação LDAP ou do Microsoft Active Directory
443	Usada para conexões com o StoreFront do Citrix Receiver ou com Receiver para Web para Áreas de trabalho e aplicativos virtuais.	Internet	Citrix Gateway

Porta TCP	Descrição	Origem	Destino
443	Usada para conexões com o XenMobile para entrega Web, móvel e de aplicativo SaaS.	Internet	Citrix Gateway
443	Usada para comunicação geral de dispositivo com o XenMobile Server	XenMobile	XenMobile
443	Usada para conexões de dispositivos móveis com o XenMobile para registro.	Internet	XenMobile
443	Usada para conexões do XenMobile ao conector Citrix Gateway para Exchange ActiveSync.	XenMobile	Conector Citrix Gateway para Exchange ActiveSync
443	Usada para conexões do conector Citrix Gateway do Exchange ActiveSync ao XenMobile.	Conector Citrix Gateway para Exchange ActiveSync	XenMobile
443	Usada para URL de retorno de chamada em implantações sem autenticação de certificado.	XenMobile	Citrix Gateway
514	Usada para conexões entre o XenMobile e um servidor syslog.	XenMobile	Servidor Syslog
636	Usada para conexões LDAP seguras.	Citrix Gateway; XenMobile	Servidor de autenticação LDAP ou do Active Directory

Porta TCP	Descrição	Origem	Destino
1494	Usada para conexões ICA com aplicativos baseados em Windows na rede interna. A Citrix recomenda manter essa porta aberta.	Citrix Gateway	Áreas de trabalho e aplicativos virtuais
1812	Usada para conexões RADIUS.	Citrix Gateway	Servidor de autenticação RADIUS
2598	Usada para conexões com aplicativos baseados em Windows na rede interna usando confiabilidade de sessão. A Citrix recomenda manter essa porta aberta.	Citrix Gateway	Áreas de trabalho e aplicativos virtuais
3268	Usada para conexões LDAP inseguras do Microsoft Global Catalog.	Citrix Gateway; XenMobile	Servidor de autenticação LDAP ou do Active Directory
3269	Usada para conexões LDAP seguras do Microsoft Global Catalog.	Citrix Gateway; XenMobile	Servidor de autenticação LDAP ou do Active Directory
9080	Usada para tráfego HTTP entre o Citrix ADC e o conector Citrix Gateway para Exchange ActiveSync.	Citrix ADC	Conector Citrix Gateway para Exchange ActiveSync
30001	API de gerenciamento para preparação inicial do serviço HTTPS	LAN interna	Servidor XenMobile

Porta TCP	Descrição	Origem	Destino
9443	Usada para tráfego HTTPS entre o Citrix ADC e o conector Citrix Gateway para Exchange ActiveSync.	Citrix ADC	Conector Citrix Gateway para Exchange ActiveSync
45000; 80	Usada para comunicação entre duas VMs do XenMobile quando implantadas em um cluster. A porta 80 é para comunicação entre nós e para descarga de SSL.	XenMobile	XenMobile
8443	Usada para registro, XenMobile Store e gerenciamento de aplicativo móvel (MAM).	XenMobile; Citrix Gateway; Dispositivos; Internet	XenMobile
4443	Usada para acesso ao console XenMobile por um administrador usando o navegador. Usada também para baixar logs e pacotes de suporte para todos os nós de cluster do XenMobile a partir de um nó.	Ponto de acesso (navegador); XenMobile	XenMobile
27000	Porta padrão usada para acessar o Citrix License Server externo.	XenMobile	Citrix License Server

Porta TCP	Descrição	Origem	Destino
7279	Porta padrão usada para fazer check-in e check-out das licenças da Citrix.	XenMobile	Citrix Vendor Daemon
161	Usada para tráfego SNMP usando o protocolo UDP.	SNMP Manager	XenMobile
162	Usada para enviar alertas de interceptação SNMP ao SNMP Manager do XenMobile. A origem é XenMobile e o destino é SNMP Manager.	XenMobile	SNMP Manager

Abrir portas do XenMobile para gerenciar dispositivos

Abra as seguintes portas para permitir que o XenMobile se comunique na sua rede.

Porta TCP	Descrição	Origem	Destino
25	Porta SMTP padrão do serviço de notificação do XenMobile. Se o seu servidor SMTP usar uma porta diferente, verifique se o firewall bloqueia essa porta.	XenMobile	Servidor SMTP

Porta TCP	Descrição	Origem	Destino
80 e 443	Conexão da Loja de Aplicativos da Empresa com Apple iTunes App Store, Google Play (deve usar a porta 80) ou Windows Phone Store. Usado para compra por volume da Apple. Usada para publicar aplicativos das lojas de aplicativos do iOS, Secure Hub para Android ou Secure Hub para Windows Phone.	XenMobile	<code>ax.apps.apple.com</code> <code>e</code> <code>*.mzstatic.com;</code> <code>vpp.itunes.apple.com;</code> <code>login.live.com;</code> <code>*.notify.windows.com;</code> <code>play.google.com,</code> <code>android.clients.google.com,</code> <code>android.l.google.com</code>
80 ou 443	Usada para conexões de saída entre o XenMobile e o Nexmo SMS Notification Relay.	XenMobile	Nexmo SMS Relay Server
389	Usada para conexões LDAP inseguras.	XenMobile	Servidor de autenticação LDAP ou do Active Directory
443	Usada para registro e instalação do agente para Android e Windows Mobile.	Internet	XenMobile
443	Usada para registro e instalação do agente para dispositivos Android e Windows e o Cliente de Suporte Remoto do MDM.	Internet LAN e Wi-Fi	XenMobile

Porta TCP	Descrição	Origem	Destino
1433	Usada como padrão para conexões com um servidor do banco de dados remoto (opcional).	XenMobile	Servidor SQL
443 ou 2197	Usada para enviar notificações de APNs para *.push.apple.com	XenMobile	Internet (hosts APN que usam o endereço IP público 17.0.0.0/8)
5223	Usada para conexões de saída de APNs de dispositivos iOS com *.push.apple.com .	Dispositivos iOS	Internet (hosts APN que usam o endereço IP público 17.0.0.0/8)
8081	Usada para túneis de aplicativo do Cliente de Suporte Remoto do MDM opcional. Usa o padrão 8081.	Cliente de suporte remoto	XenMobile
8443	Usada para registro de dispositivos iOS e Windows Phone.	Internet: LAN e Wi-Fi	XenMobile

Requisito de porta para conectividade do AutoDiscovery Service

Essa configuração de porta garante que os dispositivos Android que se conectam do Secure Hub para Android possam acessar o Citrix AutoDiscovery Service (ADS) na rede interna. Você precisa acessar o ADS para baixar atualizações de segurança disponibilizadas através do ADS.

Nota:

As conexões do ADS podem não dar suporte ao seu servidor proxy. Nesse cenário, permita que a conexão do ADS ignore o servidor proxy.

Se quiser permitir a fixação de certificado, os seguintes pré-requisitos devem ser atendidos:

- **Coletar certificados do XenMobile Server e Citrix ADC.** Os certificados precisam estar no formato PEM e devem ser um certificado público e não a chave privada.
- **Entre em contato com a Citrix Support e faça uma solicitação para permitir a fixação de certificado.** Durante este processo, você será solicitado a fornecer seus certificados.

A fixação de certificado requer que os dispositivos se conectem ao ADS antes que o dispositivo seja registrado. Esse requisito garante que as informações de segurança mais recentes estejam disponíveis para o Secure Hub. Para que o Secure Hub registre um dispositivo, o dispositivo deve atingir o ADS. Portanto, a abertura do acesso ao ADS na rede interna é essencial para possibilitar que os dispositivos sejam registrados.

Para permitir o acesso ao ADS para o Secure Hub para Android, abra a porta 443 para os seguintes endereços IP e FQDN:

FQDN	Endereço IP	Porta	Uso de IP e porta
ads.xm.cloud.com	34.194.83.188	443	Secure Hub - ADS Communication
ads.xm.cloud.com	34.193.202.23	443	Secure Hub - ADS Communication

Nota:

Para versões do Secure Hub anteriores a 10.6.15, o FQDN é [discovery.mdm.zenprise.com](#). Abra a porta 443 para os endereços IP 52.5.138.94 e 52.1.30.122.

Requisitos de rede do Android Enterprise

Para obter informações sobre as conexões de saída a serem consideradas ao configurar ambientes de rede para o Android Enterprise, consulte o artigo de suporte do Google, [Android Enterprise Network Requirements](#).

Requisitos de porta para o XenMobile

Os seguintes hosts de destino deverão estar acessíveis a partir da rede para criar um Google Play Enterprise gerenciado e para acessar o [Google Play iFrame gerenciado](#). A Google disponibilizou o Play iFrame gerenciado para os desenvolvedores de EMM para simplificar a pesquisa e a aprovação de aplicativos. Para usar o Play iFrame gerenciado, o navegador a partir do qual você acessa o console XenMobile deve ter acesso ao Google Play.

Host de destino	Porta	Descrição
play.google.com	TCP/443	Usada para entrar na loja Google Play, Play Enterprise

Host de destino	Porta	Descrição
*.googleapis.com	TCP/443	Usada para o gerenciamento de dispositivos móveis do Google, APIs do Google, APIs da loja do Google Play
accounts.youtube.com, accounts.google.com	TCP/443	Usada para a autenticação da conta
apis.google.com	TCP/443	Usada para GCM e outros serviços da Web do Google
ogs.google.com	TCP/443	Usada para elementos IFrame IU
notifications.google.com	TCP/443	Usada para notificações de desktop e móveis
fonts.googleapis.com, *.gstatic.com, *. googleusercontent.com	TCP/443	Usada para conteúdo gerado pelo usuário do Google Fonts. Por exemplo, os ícones do aplicativo na loja
cri.pki.goog, ocsp.pki.goog	TCP/443	Usada para a validação do certificado

Escalabilidade e desempenho

April 23, 2020

Entender a escala da sua infraestrutura do XenMobile desempenha um papel importante em como você decide implantar e configurar o XenMobile. Este artigo contém dados de testes de escalabilidade e orientação sobre como determinar requisitos de infraestrutura para desempenho e escalabilidade para implantações locais empresariais do XenMobile de pequena a larga escala.

A escalabilidade é definida aqui em termos da capacidade dos dispositivos já registrados na implantação de se reconectar à implantação ao mesmo tempo.

- *A Escalabilidade* é definida como o número máximo de dispositivos registrados na implantação.
- *Taxa de Login* é definida como a taxa máxima com que os dispositivos existentes podem se reconectar à implantação.

Os dados contidos neste artigo são derivados de testes nas implantações com tamanhos que vão de

10.000 a 75.000 dispositivos. Os testes abrangeram dispositivos móveis que usavam cargas de trabalho.

Todos os testes foram realizados com o XenMobile Enterprise Edition.

Os testes foram realizados usando o Citrix Gateway 8200. Do dispositivo Citrix ADC com capacidade semelhante ou superior pode-se esperar que produza escalabilidade semelhante ou maior.

Segue um resumo dos resultados dos testes de escalabilidade.

Resumo dos resultados do teste de escalabilidade para implantações de até 75.000 dispositivos

Taxa de login (taxa de reconexão de usuários existentes) - Até 9.375 dispositivos por hora

Configuração usada:

- Citrix Gateway
- MPX 8200
- XenMobile Enterprise Edition
- Cluster de 7 nós do XenMobile Server
- Banco de dados: banco de dados Microsoft SQL Server externo

Os resultados de teste por população de dispositivos e configuração de hardware

Número de dispositivos em operação	12.500	30.000	60.000	75.000
Taxa de reconexão de dispositivos existentes por hora	1.250	3.750	7.500	9.375
XenMobile Server – modo	Autônomo	Cluster	Cluster	Cluster
XenMobile Server – cluster	N/D	3	5	7
XenMobile Server – dispositivo virtual	Memória = 8 GB de RAM; vCPUs = 4	Memória = 16 GB de RAM; vCPUs = 6	Memória = 24 GB de RAM; vCPUs = 8	Memória = 24 GB de RAM; vCPUs = 8

Número de dispositivos em operação	12.500	30.000	60.000	75.000
Active Directory	Memória = 4 GB de RAM; vCPUs = 2	Memória = 8 GB de RAM; vCPUs = 4	Memória = 16 GB de RAM; vCPUs = 4	Memória = 16 GB de RAM; vCPUs = 4
Banco de dados Microsoft SQL Server externo	Memória = 8 GB de RAM; vCPUs = 4	Memória = 16 GB de RAM; vCPUs = 8	Memória = 24 GB de RAM; vCPUs = 16	Memória = 24 GB de RAM; vCPUs = 16

Perfil de escalabilidade

Configuração do Active Directory	Perfil usado
Usuários	100.000
Grupos	200.000
Níveis de aninhamento	5

Configuração do XenMobile Server		
Server	Total	Por usuário
Políticas	20	20
Aplicativos	270	50
Aplicativo público	200	0
MDX	50	30
Web e SaaS.	20	20
Ações	50	
Grupos de entrega	20	
Grupos do Active Directory por grupo de entrega	10	
SQL		
Número de bancos de dados	1	

Conexões de dispositivos e atividades de aplicativo

Estes testes de escalabilidade coletaram dados sobre a capacidade de dispositivos registrados em uma implantação para reconectar por um período de oito horas.

Os testes simularam um intervalo de reconexão durante o qual os dispositivos que estão sendo reconectados obtêm todas as políticas de segurança autorizadas, fazendo com que os nós do XenMobile Server fiquem sujeitos a condições de carga mais altas do que o normal. Durante as reconexões subsequentes, somente as políticas alteradas ou novas são enviadas para dispositivos iOS, diminuindo a carga nos nós do XenMobile Server.

Estes testes usaram uma mistura de 50% dispositivos iOS e 50% dispositivos Android.

Nesses testes, presume-se que os dispositivos Android que se reconectam receberam notificações GCM prévias.

Durante o intervalo de teste de 8 horas, ocorreram as seguintes atividades relativas a aplicativos:

- O Secure Hub foi aberto uma vez para enumerar os aplicativos com direito
- 2 aplicativos Web SAML foram abertos
- 4 aplicativos MAM foram baixados
- 1 STA foi gerada para uso pelo Secure Mail
- 240 validações de ticket STA, uma para cada evento de Secure Mail reconectado através de uma micro VPN, foram executadas.

Arquitetura de referência

Para obter a arquitetura de referência para implantações usadas nesses testes de escalabilidade, consulte “Core MAM+MDM Reference Architecture” em [Arquitetura de referência para implantações locais](#).

Restrições e limitações

Observe o seguinte ao considerar os resultados do teste de escalabilidade neste artigo:

- A plataforma Windows não foi testada.
- O envio por push de política foi testado para dispositivos iOS e Android.
- Cada nó do XenMobile Server é compatível com um máximo de 12.000 dispositivos simultaneamente.

Licenciamento

December 22, 2020

Importante:

O processo de devolução e modificação de licenças Citrix mudou a partir de 4 de novembro de 2020. Para obter informações sobre as alterações no portal “Manage Licenses” no Citrix.com e em “My Licensing Tools” no Partner Central, consulte o artigo de suporte Citrix, <https://support.citrix.com/article/CTX285157>.

O XenMobile usa o Citrix Licensing para gerenciar licenças. O XenMobile Server e o Citrix Gateway requerem licenças.

Para obter mais informações sobre o licenciamento de Citrix Gateway, consulte a documentação do Citrix Gateway. Para obter mais informações sobre o Citrix Licensing, consulte [O sistema Citrix Licensing](#).

Quando você adquire o XenMobile Server, recebe uma mensagem de email de confirmação de pedido que contém instruções para a ativação das suas licenças. Os novos clientes devem se registrar em um programa de licença antes de fazer um pedido. Para obter mais informações sobre os programas e os modelos de licenciamento do XenMobile, consulte [Licenciamento do XenMobile](#).

Requisitos

- Atualize o seu Citrix License Server para 11.16.x ou posterior antes de atualizar para a versão mais recente do XenMobile Server. Versões mais antigas de servidor de licenças não são compatíveis com a versão mais recente do XenMobile.
- Você deve instalar o Citrix Licensing antes de baixar as suas licenças do XenMobile. O nome do servidor no qual você instalou o Citrix Licensing é necessário para gerar o arquivo de licença. Quando você instala o XenMobile, o Citrix Licensing é instalado no servidor por padrão. Como alternativa, você pode usar uma implantação existente do Citrix Licensing para gerenciar as suas licenças do XenMobile. Para obter mais informações sobre como instalar, implantar e gerenciar o Citrix Licensing, consulte [Como Licenciar o seu Produto](#).
- Se você pretende usar nós de cluster ou instâncias do XenMobile, terá de usar o Citrix Licensing em um servidor remoto.
- A Citrix recomenda que você mantenha cópias locais de todos os arquivos de licença que receber. Quando você salva uma cópia de backup do arquivo de configuração, todos os arquivos de licença são incluídos nesse backup. Se, no entanto, você reinstalar o XenMobile sem primeiro fazer backup do arquivo de configuração, precisará dos arquivos de licença originais.

Considerações sobre o licenciamento do XenMobile

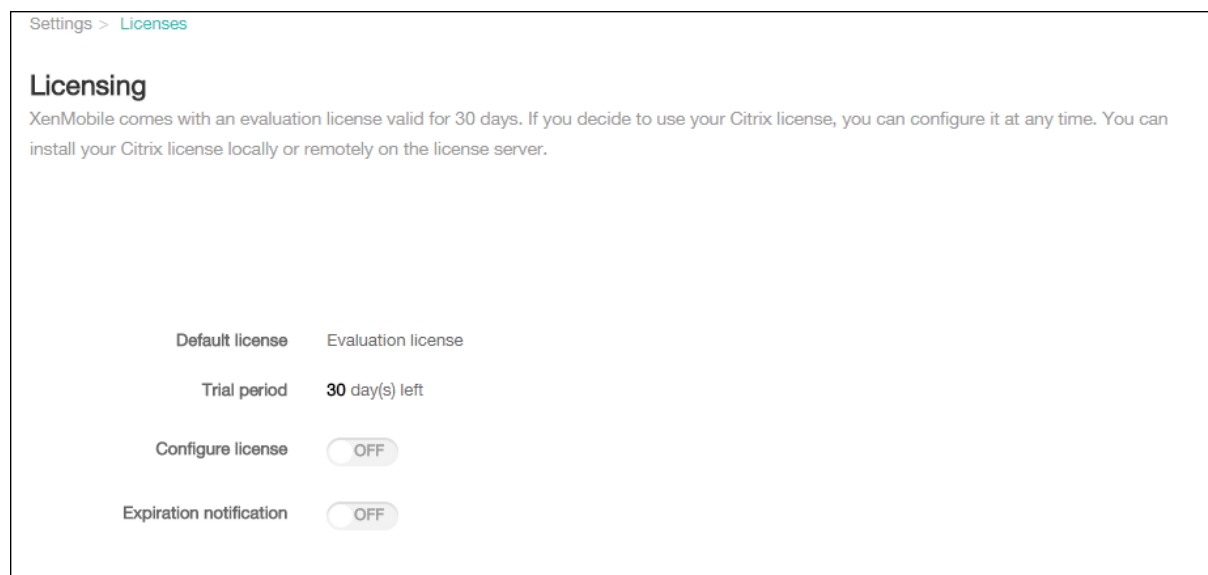
Na ausência de uma licença, o XenMobile funciona com todos os recursos no modo de avaliação por um período de tolerância de 30 dias. Esse modo de avaliação pode ser usado somente uma vez, e o período de 30 dias é iniciado quando você instala o XenMobile. O acesso ao console da Web XenMobile nunca é bloqueado, quer uma licença válida do XenMobile esteja disponível ou não. No console XenMobile, você pode ver quantos dias restam do período de avaliação.

Embora o XenMobile permita que você carregue várias licenças, somente uma licença pode ser ativada por vez.

Quando uma licença do XenMobile expira, você não pode mais executar qualquer função de gerenciamento de dispositivo. Por exemplo, novos usuários ou dispositivos não podem ser registrados, e aplicativos e configurações implantados em dispositivos registrados não podem ser atualizados. Para obter mais informações sobre os programas e os modelos de licenciamento do XenMobile, consulte [Licenciamento do XenMobile](#).

Para localizar a página Licenciamento no console XenMobile

Quando a página **Licenciamento** é exibida pela primeira vez depois que você instala o XenMobile, a licença é definida para o modo de avaliação de 30 dias padrão e ainda não está configurada. Você pode adicionar e configurar licenças nessa página.



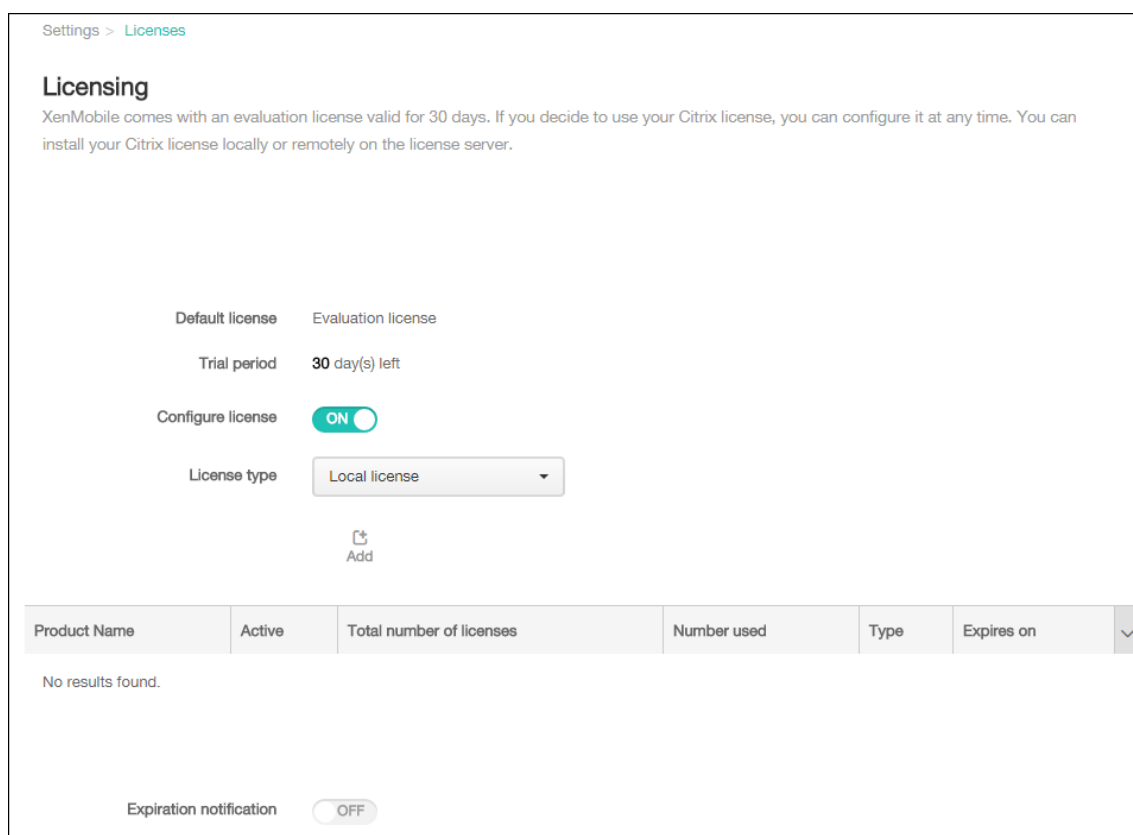
1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida.
2. Clique em **Licenciamento**. A página **Licenciamento** é exibida.

Para adicionar uma licença local

Quando você adiciona novas licenças, elas são exibidas na tabela. A primeira licença adicionada é ativada automaticamente. Se você adicionar várias licenças da mesma categoria, como Empresa, e tipo, essas licenças aparecem em uma única linha da tabela. Nesses casos, o **Número total de licenças** e o **Número usado** refletem a quantidade combinada das licenças comuns. A data **Expira em** mostra a data de expiração mais recente entre as licenças comuns.

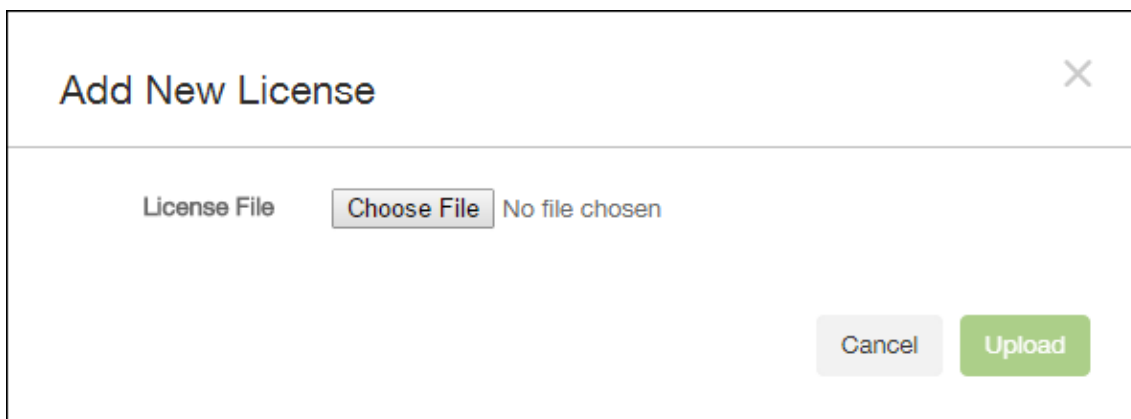
Gerencie todas as licenças locais usando o console XenMobile.

1. Obtenha um arquivo de licença do Simple License Service por meio do License Administration Console ou diretamente da sua conta em Citrix.com. Para obter detalhes, consulte a documentação do Citrix Licensing.
2. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida.
3. Clique em **Licenciamento**. A página **Licenciamento** é exibida.
4. Defina **Configurar licença** como **Ativada**. Aparecem a lista **Tipo de licença**, o botão **Adicionar** e a tabela **Licenciamento**. A tabela **Licenciamento** contém as licenças que você usou com o XenMobile. Se você ainda não tiver adicionado uma licença Citrix ainda, a tabela estará vazia.

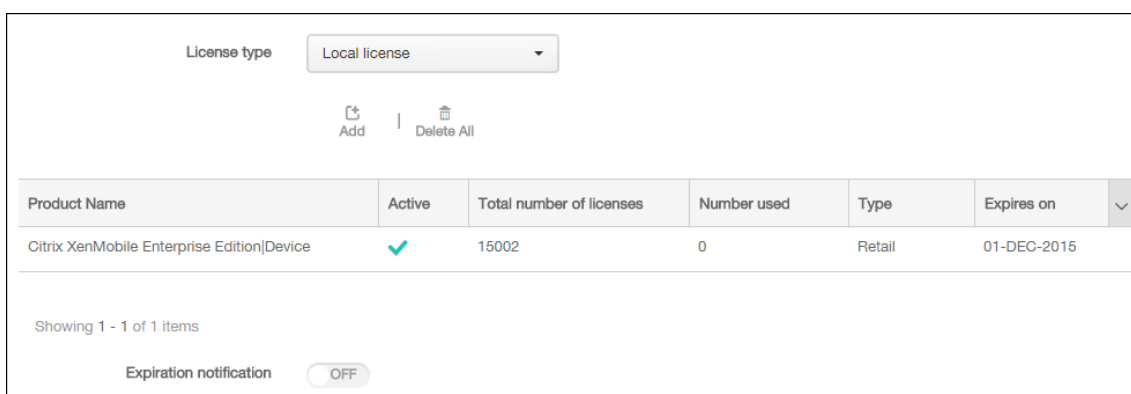


5. Verifique se **Tipo de licença** está definido como **Licença local** e clique em **Adicionar**. A caixa

de diálogo **Adicionar nova licença** é exibida.



6. Na caixa de diálogo **Adicionar nova licença**, clique em **Escolher arquivo** e navegue até a localização do seu arquivo de licença.
7. Clique em **Carregar**. A licença é carregada localmente e é exibida na tabela.



8. Quando a licença for exibida na tabela na página **Licenciamento**, ative-a. Se for a primeira licença na tabela, essa licença será ativada automaticamente.

Para adicionar uma licença remota

Se você estiver usando o servidor Citrix Licensing remoto, use-o para gerenciar *todas* as atividades de licenciamento. Para obter detalhes, consulte [Como Licenciar o seu Produto](#).

1. Importe o certificado do servidor de licença para o XenMobile Server (**Configurações > Certificados**).
2. Como padrão, a verificação do nome do host está ativada nas conexões de saída, exceto para o servidor Microsoft PKI. Se a verificação do nome do host interromper sua implantação, altere a propriedade do servidor **disable.hostname.verification** para **true**. O valor padrão desta propriedade é **false**.

Quando a verificação de nome de host falha, o log do servidor inclui erros como: “Não é possível conectar com o servidor de compra por volume: o nome de host ‘192.0.2.0’ não corresponde à entidade do certificado fornecida pelo par correspondente”

- Na página **Licenciamento**, defina **Configurar licença** como **Ativada**. Aparecem a lista **Tipo de licença**, o botão **Adicionar** e a tabela **Licenciamento**. A tabela **Licenciamento** contém as licenças que você usou com o XenMobile. Se você ainda não tiver adicionado uma licença Citrix ainda, a tabela estará vazia.
- Defina **Tipo de licença** como **Licença remota**. Os campos **Servidor de licença** e **Porta** e o botão **Testar conexão** substituem o botão **Adicionar**.

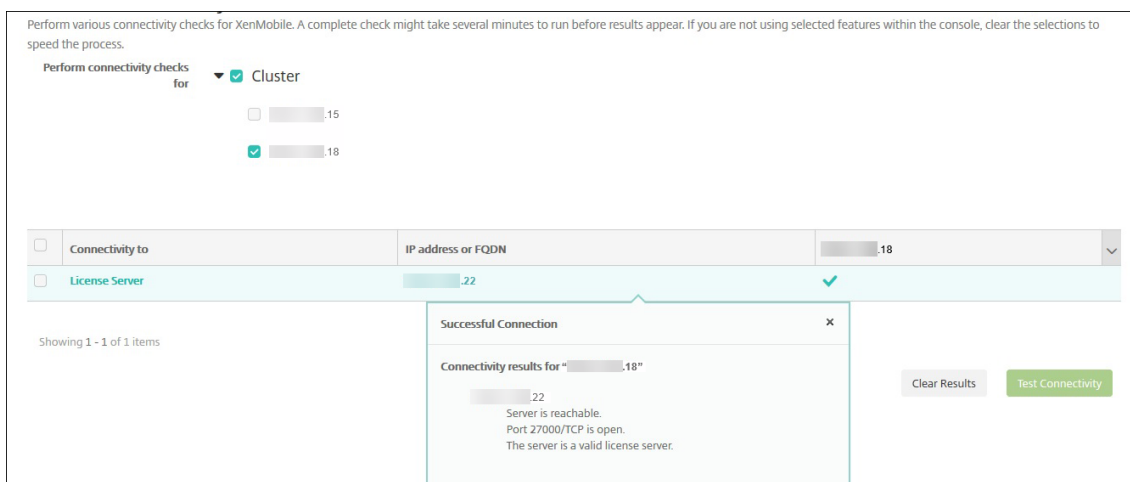
Product name	Active	Total number of licenses	Number used	Type	Expires on
		1001	0	Retail	01-DEC-2015

- Defina estas configurações:
 - Servidor de licenças:** digite o endereço IP ou nome de domínio totalmente qualificado (FQDN) do seu servidor remoto de licenciamento.
 - Porta:** aceite a porta padrão ou digite o número da porta usada para comunicação com o servidor de licenciamento.
- Clique em **Testar conexão**. Se a conexão for bem-sucedida, o XenMobile se conectar com o servidor de Licenciamento e a tabela Licenciamento é preenchida com licenças disponíveis. Se houver apenas uma licença, essa será ativada automaticamente.

Quando você clica em **Testar conexão**, o XenMobile confirma o seguinte:

- Que o XenMobile consegue se comunicar com o servidor de licenças.
- Que as licenças no servidor de licenças são válidas.
- Que o servidor de licenças é compatível com o XenMobile.

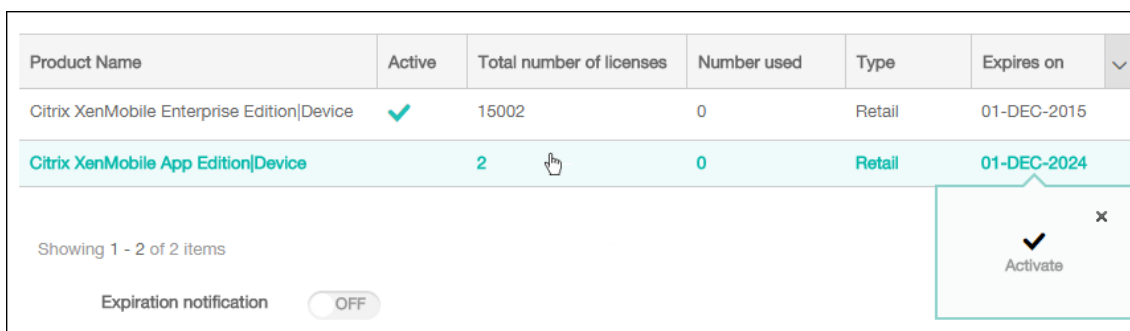
Se a conexão não for bem-sucedida, revise a mensagem de erro exibida, faça as correções necessárias e clique em **Testar conexão**.



Para ativar uma licença diferente

Se você tiver várias licenças, poderá escolher a licença que deseja ativar. No entanto, somente uma licença pode estar ativa por vez.

1. Na página **Licenciamento**, na tabela **Licenciamento**, clique na linha da licença que você deseja ativar. Uma janela de confirmação **Ativar** é exibida ao lado da linha.



2. Clique em **Ativar**. A caixa de diálogo **Ativar** é exibida.
3. Clique em **Ativar**. A licença selecionada é ativada.

Importante:

Se você ativar a licença selecionada, a licença ativa no momento será desativada.

Para automatizar uma notificação de expiração

Depois de ativar licenças locais ou remotas, você poderá configurar o XenMobile para notificar você ou uma pessoa designada quando a data de expiração da licença estiver próxima.

1. Na página **Licenciamento**, defina **Notificação de expiração** como **Ativada**. Novos campos relacionados a notificação são exibidos.

Expiration notification

Notify every* day(s) day(s) before expiration

Recipient*

Content*

2. Defina estas configurações:

- **Notificar a cada:** digite:
 - A frequência com a qual as notificações são enviadas, como a cada **7** dias.
 - Quando começar a enviar notificações, como 60 dias antes da expiração da licença.
- **Destinatário:** digite o seu endereço de email ou o endereço de email da pessoa responsável pela licença.
- **Conteúdo:** digite uma mensagem de notificação de expiração que o destinatário verá na notificação.

3. Clique em **Salvar**. Com base nas suas configurações, o XenMobile começa a enviar mensagens de email que contêm o texto que você digitou em **Conteúdo** ao destinatário inserido em **Destinatário**. As notificações são enviadas com a frequência que você definir.

Conformidade com FIPS 140-2

November 30, 2020

O Federal Information Processing Standard (FIPS), emitido pelo US National Institute of Standards and Technologies (NIST). O FIPS especifica os requisitos de segurança para módulos criptográficos usados em sistemas de segurança. FIPS 140-2 é a segunda versão desse padrão. Para obter mais informações sobre os módulos FIPS 140 validados pelo NIST, consulte o [NIST Computer Security Resource Center](#).

Importante:

- Você pode ativar o modo FIPS do XenMobile somente durante a instalação inicial.
- O gerenciamento somente de dispositivo móvel do XenMobile, o gerenciamento somente de aplicativo móvel do XenMobile e o XenMobile MDM+MAM são compatíveis com FIPS, desde que nenhum aplicativo HDX seja usado.

Todas as operações de criptografia de dados em repouso e dados em trânsito no iOS usam módulos criptográficos validados pelo FIPS e fornecidos pela Citrix e pela Apple. No Android, todas as

operações de criptografia de dados em repouso usam módulos criptográficos validados pelo FIPS e fornecidos pela Citrix ou os módulos de criptografia da plataforma fornecidos pelo fabricante do dispositivo. Entre em contato com seu representante Citrix para obter mais informações sobre os módulos dos fabricantes de dispositivos.

Todas as operações de criptografia de dados em repouso e dados em trânsito para Gerenciamento de dispositivo móvel (MDM) em dispositivos Windows com suporte usam módulos criptográficos validados pelo FIPS e fornecidos pela Microsoft.

Todas as operações de criptografia de dados em repouso e dados em trânsito no XenMobile MDM usam módulos criptográficos validados pelo FIPS e fornecidos pela Citrix. Todos os dados em repouso e dados em trânsito para fluxos MDM usam módulos criptográficos compatíveis com FIPS de ponta a ponta. Essa segurança inclui as operações criptográficas descritas acima para dispositivos móveis, além das operações criptográficas entre dispositivos móveis e o Citrix Gateway.

O MDX Vault criptografa os aplicativos preparados com MDX e os dados em repouso associados em dispositivos iOS e Android usando módulos criptográficos validados pelo FIPS e fornecidos pela Citrix.

Suporte a idiomas

November 30, 2020

Os aplicativos móveis de produtividade e o console XenMobile são adaptados para o uso em idiomas além do inglês. O suporte inclui caracteres e entradas de teclado de idiomas além do inglês, mesmo quando o aplicativo não está localizado no idioma preferencial dos usuários. Para obter mais informações sobre suporte à globalização de todos os produtos Citrix, consulte <https://support.citrix.com/article/CTX119253>.

Este artigo lista os idiomas com suporte na versão mais recente do XenMobile.

Console XenMobile e portal de autoajuda

- Francês
- Alemão
- Espanhol
- Japonês
- Coreano
- Português
- Chinês simplificado

Aplicativos móveis de produtividade

Um X indica que o aplicativo está disponível neste determinado idioma.

iOS e Android

Idioma	Secure Hub	Secure Mail	Secure Web	QuickEdit
Japonês	X	X	X	X
Chinês simplificado	X	X	X	X
Chinês tradicional	X	X	X	X
Francês	X	X	X	X
Alemão	X	X	X	X
Espanhol	X	X	X	X
Coreano	X	X	X	X
Português	X	X	X	X
Holandês	X	X	X	X
Italiano	X	X	X	X
Dinamarquês	X	X	X	X
Sueco	X	X	X	X
Hebraico	X	X	X	iOS somente
Árabe	X	X	X	X
Russo	X	X	X	X
Turco	X	X	Somente Android	-
Polonês	X	X	X	-

Windows

Idioma	Secure Hub	Secure Mail	Secure Web
Francês	X	X	X
Alemão	X	X	X

Idioma	Secure Hub	Secure Mail	Secure Web
Espanhol	X	X	X
Italiano	X	X	X
Dinamarquês	X	X	X
Sueco	X	X	X

Suporte a idioma da direita para a esquerda

A tabela a seguir resume o suporte para texto em idiomas do Oriente Médio de cada aplicativo. Um X indica que o recurso está disponível para a plataforma. O suporte a idiomas da direita para a esquerda não está disponível para dispositivos do Windows.

Aplicativo	iOS	Android
Secure Hub	X	X
Secure Mail	X	X
Secure Web	X	X
QuickEdit	X	X

Instalar e configurar

December 22, 2020

Antes de começar

Você pode usar a seguinte lista de verificação de pré-instalação para conhecer os pré-requisitos e configurações da instalação do XenMobile no local. Cada tarefa ou observação inclui uma coluna que indica o componente ou a função à qual o requisito se aplica.

O planejamento de uma implementação do XenMobile envolve muitas considerações. Para ver recomendações, perguntas comuns e casos de uso para o seu ambiente XenMobile completo, consulte o [Manual de implantação do XenMobile](#).

Para conhecer as etapas de instalação, consulte a seção [Instalar o XenMobile](#) mais adiante neste artigo.

A lista de verificação da pré-instalação

Conectividade básica de rede

Estas são as configurações de rede que você precisa para a solução XenMobile.

| Pré-requisito ou configuração | Componente ou função | Anote a configuração |

| ----- | ----- | ---- |

| Anote o nome de domínio totalmente qualificado (FQDN) ao qual os usuários remotos se conectam.

| XenMobile e Citrix Gateway |

| Anote o endereço IP público e local. |

| Você precisa desses endereços IP para configurar o firewall para configurar a conversão de endereços de rede (NAT). | XenMobile e Citrix Gateway | |

| Anote a máscara de sub-rede. | XenMobile e Citrix Gateway | |

| Anote os endereços IP do DNS. | XenMobile e Citrix Gateway | |

| Anote os endereços IP do servidor WINS (se aplicável). | Citrix Gateway | |

| Identifique e anote o nome do host do Citrix Gateway. | Citrix Gateway | Este item não é o FQDN. O FQDN é contido no certificado de servidor assinado que é vinculado ao servidor virtual e ao qual os usuários se conectam. Você pode configurar o nome do host usando o Assistente de Instalação no Citrix Gateway. | Citrix Gateway | |

| Anote o endereço IP do XenMobile. Reserve um endereço IP se você instalar uma instância do XenMobile. Se você configurar um cluster, anote todos os endereços IP necessários. | XenMobile | |

| Um endereço IP público configurado no Citrix Gateway | Citrix Gateway | |

| Uma entrada de DNS externa para o Citrix Gateway | Citrix Gateway |

| Anote o endereço IP do servidor proxy da Web, a porta, a lista de hosts do proxy e o nome de usuário e senha do administrador. Essas configurações são opcionais se você implantar um servidor proxy em sua rede (se aplicável). | Citrix Gateway | Você pode usar o sAMAccountName ou o nome principal do usuário (UPN) ao configurar o nome de usuário para o proxy da web. | XenMobile e Citrix Gateway | |

| Anote o endereço IP do gateway padrão. | XenMobile e Citrix Gateway | |

| Anote o endereço IP do sistema (NSIP) e a máscara de sub-rede. | Citrix Gateway | |

| Anote o endereço IP de sub-rede (SNIP) e a máscara de sub-rede. | Citrix Gateway | |

| Anote o endereço IP do servidor virtual do Citrix Gateway e o FQDN do certificado. Para configurar vários servidores virtuais, anote todos os endereços IP virtuais e FQDNs dos certificados. | Citrix Gateway | |

| Anote as redes internas que os usuários podem acessar através do Citrix Gateway. Exemplo: 10.10.0.0/24. Insira todas as redes internas e segmentos de rede aos quais os usuários precisam acessar nesses casos: quando os usuários se conectam ao Secure Hub ou ao Citrix Gateway Plug-in quando o túnel dividido está definido como Ativado. | Citrix Gateway | |

| Certifique-se de que a conectividade de rede entre o XenMobile Server, o Citrix Gateway, o Microsoft SQL Server externo e o servidor DNS esteja acessível. | XenMobile e Citrix Gateway | |

Licenciamento

O XenMobile exige a compra de opções de licenciamento para o Citrix Gateway e o XenMobile. Para obter mais informações sobre o Citrix Licensing, consulte [O sistema Citrix Licensing](#).

Pré-requisito	Componente	Anote a localização
Obtenha licenças universais no site da Citrix. Para obter detalhes, consulte Licenciamanento na documentação do Citrix Gateway.	Citrix Gateway, XenMobile e Citrix License Server	

Certificados

O XenMobile e Citrix Gateway exigem certificados para permitir conexões com outros produtos e aplicativos Citrix e de dispositivos de usuário. Para obter detalhes, consulte a seção [Certificados e autenticação](#) na documentação do XenMobile.

| Pré-requisito | Componente | Observações |

| ————— | ———— | — |

| Obtenha e instale os certificados necessários. | XenMobile e Citrix Gateway |

Portas

Abra as portas para permitir a comunicação com os componentes do XenMobile.

Pré-requisito	Componente	Observações
Portas abertas para o XenMobile	XenMobile e Citrix Gateway	

Banco de dados

O XenMobile exige a configuração de conexão de banco de dados. O repositório do XenMobile requer um banco de dados do Microsoft SQL Server em execução em uma das seguintes versões com suporte mencionadas em [Requisitos do sistema e compatibilidade](#). A Citrix recomenda usar o Microsoft SQL remotamente. PostgreSQL está incluído no XenMobile. Use o PostgreSQL local ou remotamente *apenas* em ambientes de teste.

Por padrão, o XenMobile usa o driver do banco de dados jTDS. Para usar o driver Microsoft JDBC para instalações do XenMobile Server no local, consulte [Drivers do SQL Server](#).

Pré-requisito	Componente	Observações
Endereço IP e porta Microsoft SQL Server. Verifique se a conta de serviço do SQL Server a ser usada no XenMobile tem a permissão de função DBcreator.	XenMobile	

Configurações do Active Directory

| Pré-requisito | Componente | Observações |

| ----- | ---- | ----- |

| Anote o endereço IP e a porta do Active Directory para os servidores primários e secundários. Se você usar a porta 636, instale um certificado raiz de uma AC no XenMobile e altere a opção Use secure connections para Yes. | XenMobile e Citrix Gateway |

| Anote o nome de domínio do Active Directory. | XenMobile e Citrix Gateway |

| Anote a conta de serviço do Active Directory, que requer um ID de usuário, senha e alias de domínio.

|

| A conta de serviço do Active Directory é a conta que o XenMobile usa para consultar o Active Directory. | XenMobile e Citrix Gateway | |

| Anote o DN da Base do Usuário, que é o nível do diretório sob o qual os usuários estão localizados. Por exemplo: `cn=users,dc=ace,dc=com`. Citrix Gateway and XenMobile use the User Base DN to query Active Directory. | XenMobile and Citrix Gateway | |

| Note the Group Base DN, which is the directory level under which groups are located. O Citrix Gateway e o XenMobile usam esse DN para consultar o Active Directory. | XenMobile e Citrix Gateway |

|

Conexões entre o XenMobile e o Citrix Gateway

Pré-requisito	Componente	Anote a configuração
Anote o nome de host do XenMobile.	XenMobile	
Anote o endereço IP ou o FQDN do XenMobile.	XenMobile	

Pré-requisito	Componente	Anote a configuração
Identifique os aplicativos que os usuários podem acessar.	Citrix Gateway	
Anote a URL de Retorno de Chamada.	XenMobile	

Conexões de usuário: acesso a Citrix Virtual Apps and Desktops e Citrix Secure Hub

A Citrix recomenda que você use o assistente Quick Configuration no Citrix ADC para definir as configurações de conexão entre o XenMobile e o Citrix Gateway, e entre o XenMobile e o Secure Hub. Você deve criar um segundo servidor virtual para habilitar conexões de usuário do Citrix Receiver e navegadores da Web. Essas conexões são para aplicativos baseados no Windows e áreas de trabalho virtuais no Virtual Apps and Desktops. A Citrix recomenda que você também use o assistente Quick Configuration no Citrix ADC para definir essas configurações.

Pré-requisito	Componente	Anote a configuração
Anote o nome de host e a URL externa do Citrix Gateway. A URL externa é o endereço da Web ao qual os usuários se conectam.	XenMobile	
Anote a URL de retorno de chamada do Citrix Gateway.	XenMobile	
Anote os endereços IP e as máscaras de sub-rede do servidor virtual.	Citrix Gateway	
Anote o caminho do Program Neighborhood Agent ou de um site do Virtual Apps and Desktops.	Citrix Gateway e XenMobile	
Anote o endereço IP ou o FQDN do servidor Citrix Virtual Apps and Desktops que executa a Secure Ticket Authority (STA) (somente para conexões ICA).	Citrix Gateway	

Pré-requisito	Componente	Anote a configuração
Anote o FQDN público do XenMobile.	Citrix Gateway	
Note o FQDN público do Secure Hub.	Citrix Gateway	

Fluxograma para implantação do XenMobile

Você pode usar este fluxograma para guiá-lo pelas etapas principais de implantação do XenMobile. Links para os tópicos sobre cada etapa encontram-se próximos à figura.

- 1: [Requisitos do sistema e compatibilidade](#)
- 2: [Instalar e configurar](#)
- 3 e 4: Lista de verificação pré-instalação (este artigo)
- 5: Configurar o XenMobile na janela do prompt de comando (este artigo)
- 6: Configurar o XenMobile em um navegador da Web (este artigo)
- 7: [Definição das configurações do seu ambiente do XenMobile](#)
- 8: [Requisitos de porta](#)

Instalar o XenMobile

A máquina virtual (VM) do XenMobile é executada no Citrix XenServer, VMware ESXi ou Microsoft Hyper-V. Você pode usar os consoles de gerenciamento do XenCenter ou do vSphere para instalar o XenMobile.

Nota:

Verifique se o hipervisor está configurado com o horário correto, seja usando um servidor NTP ou uma configuração manual, pois o XenMobile usa esse horário. Se você tiver problemas de fuso horário ao sincronizar o horário do XenMobile com um hipervisor, você pode evitar esses problemas apontando o XenMobile para um servidor NTP. Para fazer isso, use a CLI do XenMobile, conforme descrito em [Opções da interface de linha de comando](#).

Pré-requisitos do XenServer ou do VMware ESXi. Antes de instalar o XenMobile no XenServer ou no VMware ESXi, você deve fazer o seguinte. Para obter detalhes, consulte a documentação do [XenServer](#) ou [VMware](#).

- Instale o XenServer ou o VMware ESXi em um computador com os recursos de hardware adequados.

- Instale o XenCenter ou o vSphere em um computador separado. O computador que hospeda o XenCenter ou o vSphere se conecta ao host do XenServer ou do VMware ESXi por meio da rede.

Pré-requisitos do Hyper-V. Antes de instalar o XenMobile no Hyper-V, você deve fazer o seguinte. Para obter detalhes, consulte a documentação do [Hyper-V](#).

- Instale o Windows Server 2008 R2, o Windows Server 2012 ou o Windows Server 2012 R2 ativado para Hyper-V e funções em um computador com os recursos de sistema adequados. Ao instalar a função Hyper-V, certifique-se de especificar as NICs no servidor que o Hyper-V usa para criar as redes virtuais. É possível reservar alguns NICs para o host.
- Exclua o arquivo Virtual Machines/<UUID específico da compilação>.xml
- Mova o arquivo Legacy/<UUID específico da compilação>.exp para Máquinas Virtuais

Se você instalar o Windows Server 2008 R2 ou o Windows Server 2012, faça o seguinte:

Essas etapas são necessárias porque há duas versões diferentes do arquivo de manifesto do Hyper-V que representa a configuração da VM (.exp e .xml). As versões Windows Server 2008 R2 e Windows Server 2012 são compatíveis somente com .exp. Para essas versões, somente o arquivo de manifesto .exp deve estar em vigor antes da instalação.

O Windows Server 2012 R2 não exige essas etapas extras.

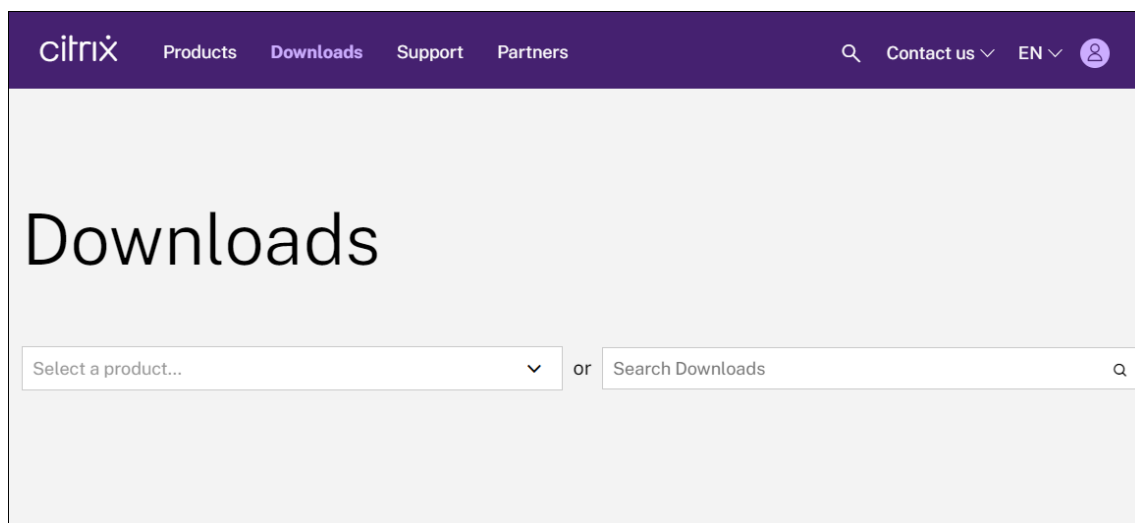
Modo FIPS 140-2. Para instalar o XenMobile Server no modo FIPS, conclua um grupo de pré-requisitos, conforme discutido em [Configurar o modo FIPS com o XenMobile](#).

Baixar o software do produto XenMobile

Você pode baixar o software do produto no [Site da Citrix](#). Faça login no site e use o link de Downloads para navegar até a página que contém o software que você deseja baixar.

Para baixar o software do XenMobile

1. Vá para o [Site da Citrix](#).
2. Ao lado da caixa Pesquisar, clique em **Login** e faça login na sua conta.
3. Clique na guia **Downloads**.
4. Na página Downloads, na lista **Selecionar um produto**, clique em **Citrix Endpoint Management (and Citrix XenMobile Server)**. A página Citrix Endpoint Management (and Citrix XenMobile Server) é exibida automaticamente.



5. Expanda **XenMobile Server (on-premises)**.
6. Expanda **Product Software**.
7. Clique em **XenMobile Server 10**.
8. Clique no menu **Ir para Download** e escolha a imagem virtual apropriada para usar para instalar o XenMobile. Alternativamente, role a página para localizar o botão **Download do arquivo** da imagem que deseja instalar.
9. Siga as instruções na tela para baixar o software.

Para baixar o software do Citrix Gateway

Você pode usar este procedimento para baixar o dispositivo virtual do Citrix Gateway ou as atualizações de software para seu dispositivo existente do Citrix Gateway.

1. Vá para o [Site da Citrix](#).
2. Se você ainda não tiver feito login no site da Citrix, ao lado da caixa Pesquisar, clique em **Login** e faça login na sua conta.
3. Clique na guia **Downloads**.
4. Na página Downloads, na lista Seleccionar um produto, clique em **Citrix Gateway**.
5. Clique em **Ir**. A página do Citrix Gateway é exibida.
6. Na página Citrix Gateway, expanda a versão do Citrix Gateway que você está executando.
7. Em **Firmware**, clique na versão do software do dispositivo que você deseja baixar.

Nota:

Você também pode clicar em **Dispositivos virtuais** para baixar o Citrix ADC VPX. Quando

Se você seleciona essa opção, recebe uma lista de softwares para a máquina virtual de cada hipervisor.

8. Clique na versão do software do dispositivo que você deseja baixar.
9. Na página do software do dispositivo da versão que você deseja baixar, clique na opção **Download** do dispositivo virtual adequado.
10. Siga as instruções na tela para baixar o software.

Configurar o XenMobile para a primeira utilização

1. Para configurar o endereço IP e a máscara de sub-rede, o gateway padrão, os servidores DNS e outros detalhes do XenMobile, use o console de linha de comando do XenCenter ou do vSphere.

Nota:

Quando você usa um cliente vSphere Web, recomendamos que você não configure as propriedades de rede durante o período em que implanta o modelo OVF na página **Personalizar modelo**. Agindo assim, em uma configuração de alta disponibilidade, você evita um problema com o endereço IP que ocorre quando você clona e depois reinicia a segunda máquina virtual do XenMobile.

2. Acesse o console de gerenciamento do XenMobile apenas com o nome de domínio totalmente qualificado do XenMobile Server ou dos endereços IP do nó.
3. Faça login e siga as etapas nas telas de login iniciais.

Configurar o XenMobile na janela do prompt de comando

1. Importe a máquina virtual do XenMobile para o Citrix XenServer, o Microsoft Hyper-V ou o VMware ESXi. Para obter detalhes, consulte a documentação do [XenServer](#), [Hyper-V](#) ou [VMware](#).
2. No seu hipervisor, selecione a máquina virtual do XenMobile importada e inicie a exibição do prompt de comando. Para obter detalhes, consulte a documentação do hipervisor.
3. Na página do console do hipervisor, crie uma conta de administrador para o XenMobile na janela do prompt de comando digitando o nome do usuário e a senha de administrador.

Quando você cria ou altera as senhas da conta do administrador do prompt de comando, dos certificados de servidor de Infraestrutura de Chave Pública (PKI) e do modo FIPS, o XenMobile impõe as seguintes regras a todos os usuários, exceto os usuários do Active Directory cujas senhas são gerenciadas fora do XenMobile.

- A senha deve ter pelo menos oito caracteres.
- A senha deve atender a pelo menos três dos seguintes critérios de complexidade:

- Letras maiúsculas (A a Z)
- Letras minúsculas (a a z)
- Numerais (0 a 9)
- Caracteres especiais (como ! ## \$ %)

```
Welcome to the XenMobile First Time Use wizard. This wizard guides you through the initial configuration of XenMobile. Accept options offered by pressing Enter/Return or type your own response and then press Enter/Return.

Command prompt window administrator account:
This is the user name and password you use when logging on to XenMobile at the command prompt.
Username: admin
New password: █
```

Nenhum caractere (como asteriscos) é exibido quando você digita a nova senha.

4. Forneça as seguintes informações da rede e, em seguida, digite **y** para confirmar as configurações:
 - a) Endereço IP do XenMobile Server
 - b) Máscara de rede
 - c) Gateway padrão, que é o endereço IP do gateway padrão no DMZ
 - d) Servidor DNS principal, que é o endereço IP do servidor DNS
 - e) Servidor DNS secundário (opcional)

```
Network settings:
IP address: 192.0.2.0
Netmask: 225.225.225.128
Default gateway: 203.0.113.3
Primary DNS server: 192.0.2.4
Secondary DNS server [optional]: 192.0.2.5

Commit settings [y/n]: y█
```

Nota:

Os endereços mostrados nesta e nas imagens a seguir são não funcionais e fornecidos somente como exemplo.

5. Digite **y** para aumentar a segurança gerando uma senha de criptografia aleatória ou **n** para fornecer sua própria senha. A Citrix recomenda digitar **y** para gerar uma senha aleatória.

A senha é usada como parte da proteção das chaves de criptografia usadas para proteger os seus dados confidenciais. Um hash da senha, armazenado no sistema de arquivos do servidor, é usado para recuperar as chaves durante a criptografia e decodificação de dados. A senha não pode ser exibida.

Nota:

Se você pretende estender o seu ambiente e configurar mais servidores, forneça sua própria senha. Se você selecionar uma senha aleatória, não poderá visualizá-la.

```
Encryption passphrase:  
Generate a random passphrase to secure the server data? [y/n]: y
```

6. Opcionalmente, ative o Federal Information Processing Standard (FIPS). Para obter detalhes sobre o FIPS, consulte [FIPS](#). Além disso, é preciso atender a um grupo de pré-requisitos, conforme discutido em [Configurar o modo FIPS com o XenMobile](#).

```
Federal Information Processing Standard (FIPS) mode:  
Enable (y/n) [n]:
```

7. Forneça as seguintes informações para configurar a conexão do banco de dados.

```
Database connection:  
Local or remote [l/r]: r  
Type (Microsoft SQL, PostgreSQL or MySQL) [mi/p/my]: mi  
Use SSL [y/n]: n  
Server: .10  
Port: 5432  
Username: postgres  
Password:
```

- O seu banco de dados pode ser local ou remoto. Digite **l** para local ou **r** para remoto.
- Selecione o tipo do banco de dados. Digite **mi** para o Microsoft SQL ou digite **p** para o PostgreSQL.

Importante:

- A Citrix recomenda usar o Microsoft SQL remotamente. PostgreSQL está incluído no XenMobile. Use o PostgreSQL local ou remotamente *apenas* em ambientes de teste.
 - A migração de banco de dados não é compatível. Os bancos de dados criados em um ambiente de teste não podem ser movidos para um ambiente de produção.
- Opcionalmente, digite **y** para usar a autenticação do SSL no seu banco de dados.
 - Forneça o nome de domínio totalmente qualificado (FQDN) do servidor que hospeda o XenMobile. Esse servidor de host fornece os serviços de gerenciamento de dispositivo e gerenciamento de aplicativo.

- Digite o seu número da porta do banco de dados se ele for diferente do número de porta padrão. A porta padrão do Microsoft SQL é 1433 e a porta padrão do PostgreSQL é 5432.
- Digite o nome de usuário do seu administrador de banco de dados.
- Digite a senha do seu administrador de banco de dados.
- Digite o nome do banco de dados.
- Pressione **Enter** para confirmar as configurações do banco de dados.

8. Opcionalmente, digite **y** para ativar o clustering de nós ou instâncias do XenMobile.

Importante:

Se você ativar um cluster do XenMobile, depois de concluir a configuração do sistema, abra a porta 80 para ativar a comunicação em tempo real entre os membros de cluster. Conclua a instalação em todos os nós de cluster.

9. Digite o nome de domínio totalmente qualificado (FQDN) do XenMobile Server.

```
XenMobile hostname:  
Hostname: justan.example.com
```

10. Pressione **Enter** para confirmar as configurações.
11. Identifique as portas de comunicação. Para obter detalhes sobre portas e seus respectivos usos, consulte [Requisitos de porta](#).

Nota:

Aceite as portas padrão pressionando **Enter** (Return em um Mac).

```
HTTP [80]: 80  
HTTPS with certificate authentication [443]: 443  
HTTPS with no certificate authentication [8443]: 8443  
HTTPS for management [4443]: 4443
```

12. Ignore a próxima pergunta sobre atualização de uma versão anterior do XenMobile, pois você está instalando o XenMobile pela primeira vez.
13. Digite **y** se você desejar usar a mesma senha para todos os certificados de Infraestrutura de Chave Pública (PKI). Para obter detalhes sobre o recurso de PKI do XenMobile, consulte [Carregando certificados](#).

```
The wizard will now generate an internal Public Key Infrastructure (PKI):
- A root certificate
- An intermediate certificate to issue device certificates during enrollment
- An intermediate certificate to issue an SSL certificate
- An SSL certificate for your connectors
Do you want to use the same password for all the certificates of the PKI [y]:
New password:
Re-enter new password:
```

Importante:

Se você pretende agrupar em cluster os nós, ou instâncias, do XenMobile, forneça senhas idênticas para os nós subsequentes.

14. Digite a nova senha e, em seguida, redigite-a para confirmá-la.

Nenhum caractere (como asteriscos) é exibido quando você digita a nova senha.

15. Pressione **Enter** para confirmar as configurações.
16. Crie uma conta de administrador para fazer login no console XenMobile usando um navegador da Web. Certifique-se de anotar essas credenciais para uso posterior.

```
XenMobile console administrator account:
This is the user name and password you use when logging on to the XenMobile console through a web browser.
Username [administrator]: administrator
Password:
Re-enter new password:
```

Nota:

Nenhum caractere (como asteriscos) é exibido quando você digita a nova senha.

17. Pressione **Enter** para confirmar as configurações. A configuração inicial do sistema é salva.
18. Quando perguntado se você está atualizando, digite **n** porque é uma nova instalação.
19. Copie a URL completa exibida na tela e continue essa configuração inicial do XenMobile no seu navegador da Web.


```
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!

Upgrade:
  Upgrade from previous release (y/n) [n]:

Stopping configuration app... [ OK ]
Starting configuration app...
  application started successfully [ OK ]
Stopping main app... [ OK ]
Starting main app...
  this may take a few minutes.....
.....
  application started successfully [ OK ]

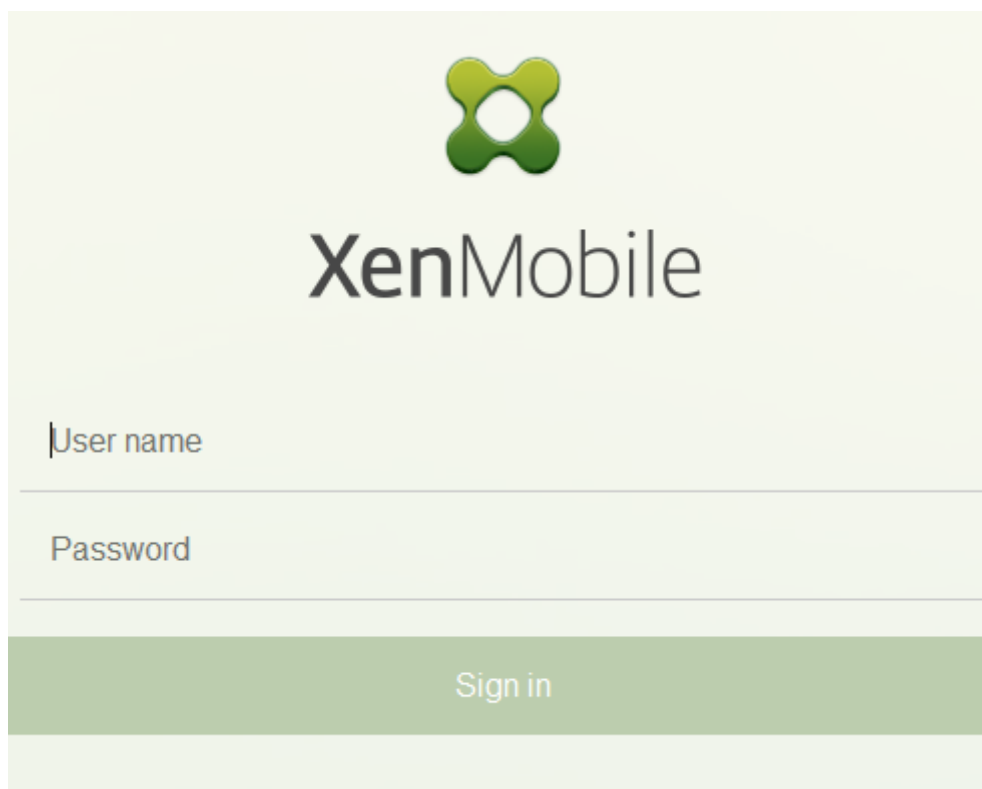
To access the console, from a web browser, go to the following location and
log on with your console credentials:
  https://203.0.113.8:4443/

Starting monitoring... [ OK ]
```

Configurar o XenMobile em um navegador da Web

Depois de concluir a parte inicial da configuração do XenMobile na janela do prompt de comando do hipervisor, conclua o processo no navegador da Web.

1. No navegador da Web, navegue até o local fornecido na conclusão da configuração da janela do prompt de comando.
2. Digite o nome do usuário e a senha da conta do administrador do console XenMobile que você criou na janela do prompt de comando.

The image shows the XenMobile login interface. At the top center is the XenMobile logo, a green four-lobed shape. Below the logo is the text "XenMobile" in a large, dark font. Underneath the logo and text are two input fields: "User name" and "Password". Below these fields is a green button with the text "Sign in". The background is a light green gradient.

3. Na página Introdução, clique em **Iniciar**. A página **Licenciamento** é exibida.
4. Configure a licença. Se você não carregar uma licença, usará uma licença de avaliação válida por 30 dias. Para obter detalhes sobre como adicionar e configurar licenças, além de como configurar notificações de expiração, consulte [Licenciamento](#).

Importante:

Se você pretende usar clustering do XenMobile mediante a adição de nós de cluster, ou instâncias, do XenMobile, precisará usar o Citrix Licensing em um servidor remoto.

5. Na página **Certificados**, clique em **Importar**. A caixa de diálogo Importar é exibida.
6. Importe seu certificado de APNs e de ouvinte SSL. O gerenciamento de dispositivos iOS requer um certificado de APNs. Para obter detalhes sobre como trabalhar com certificados, consulte [Certificados](#).

Nota:

Essa etapa exige a reinicialização do servidor.

7. Se for adequado para o ambiente, configure o Citrix Gateway. Para obter detalhes sobre como configurar o Citrix Gateway, consulte [Citrix Gateway e XenMobile](#) e [Definição das configurações do seu ambiente do XenMobile](#).

Nota:

- Você pode implantar o Citrix Gateway no perímetro da sua rede interna (ou intranet). Essa implantação oferece um ponto único e seguro de acesso para os servidores, aplicativos e outros recursos de rede que residem na rede interna. Nessa implantação, todos os usuários remotos devem se conectar ao Citrix Gateway antes que possam acessar qualquer recurso da rede interna.
- Embora o Citrix Gateway seja uma configuração opcional, depois que você inserir os dados na página, deverá limpar ou preencher os campos obrigatórios antes que possa sair da página.

8. Conclua a configuração do LDAP para acessar usuários e grupos do Active Directory. Para obter detalhes sobre como configurar a conexão LDAP, consulte [Configuração de LDAP](#).
9. Configure o servidor de notificação para que ele seja capaz de enviar mensagens aos usuários. Para obter detalhes sobre como configurar o servidor de notificação, consulte [Notificações](#).

Pós-requisito. Reinicie o XenMobile Server para ativar seus certificados.

Configurar o modo FIPS com o XenMobile

March 5, 2021

O modo FIPS (Federal Information Processing Standards) no XenMobile dá suporte a clientes do governo federal dos EUA, usando somente bibliotecas de certificado FIPS 140-2 para todas as operações de criptografia. Instalar o XenMobile Server com o modo FIPS garante que todos os dados do cliente e do servidor XenMobile sejam totalmente compatíveis com o FIPS 140-2. Essa conformidade se aplica aos dados em repouso e aos dados em trânsito.

Antes de instalar um XenMobile Server no modo FIPS, conclua os pré-requisitos a seguir.

- Use um SQL Server 2014 externo para o banco de dados do XenMobile. O SQL Server também deve ser configurado para comunicação SSL segura. Para obter instruções sobre como configurar a comunicação SSL segura com o SQL Server, consulte [Habilitar conexões criptografadas para o mecanismo de banco de dados \(SQL Server Configuration Manager\)](#).
- A comunicação SSL segura requer que você instale um certificado SSL confiável de uma autoridade de certificação (CA) de renome no SQL Server. Atenção, o SQL Server 2014 não pode aceitar um certificado curinga. A Citrix recomenda, portanto, que você solicite um certificado SSL com o FQDN do SQL Server.

Configuração do modo FIPS

Você pode ativar o modo FIPS somente durante a instalação inicial do XenMobile Server. Não é possível ativar o modo FIPS após a conclusão da instalação. Portanto, se você planeja usar o modo FIPS, deverá instalar o XenMobile Server com o modo FIPS do início. Além disso, para clusters do XenMobile, todos os nós do cluster devem ter o FIPS ativado. Você não pode ter uma combinação de XenMobile Servers FIPS e não FIPS no mesmo cluster.

Há uma opção **Toggle FIPS mode** na interface de linha de comando do XenMobile que não se destina ao uso em produção. Essa opção se destina ao uso diagnóstico e não de produção, e não é compatível em um XenMobile Server de produção.

1. Durante a instalação inicial, ative **FIPS mode**.
2. Carregue o certificado de AC raiz para o SQL Server.
3. Especifique o nome do servidor e a porta do SQL Server, as credenciais de login no SQL Server e o nome do banco de dados a ser criado para o XenMobile.

Nota:

Você pode usar um login SQL ou uma conta do Active Directory para acessar o SQL Server, mas o login usado deve ter a função DBcreator.

4. Para usar uma conta do Active Directory, insira as credenciais no formato domínio\nome do usuário.
5. Depois de concluir essas etapas, prossiga com a instalação inicial do XenMobile.

Para confirmar que a configuração do modo FIPS foi bem-sucedida, faça login na interface de linha de comando do XenMobile. A frase **In FIPS Compliant Mode** é exibida na faixa de login.

Importando certificados

O procedimento a seguir descreve como configurar o modo FIPS no XenMobile importando o certificado, que é necessário quando você usa um hipervisor VMware.

Pré-requisitos do SQL

1. A conexão com a instância do SQL do XenMobile precisa ser segura, e a versão do SQL Server deve ser 2012 ou 2014. Para proteger a conexão, consulte [Como ativar a criptografia SSL de uma instância do SQL Server usando o Console de Gerenciamento Microsoft](#).
2. Se o serviço não for reiniciado corretamente, verifique o seguinte: abra **Services.msc**.
 - a) Copie as informações de conta de login usadas para o serviço do SQL Server.
 - b) Abra MMC.exe no SQL Server.

- c) Vá até **File > Add/Remove Snap-in** e clique duas vezes no item de certificados para adicionar o snap-in dos certificados. Selecione a conta de computador e o computador local nas duas páginas do assistente.
 - d) Clique em **OK**.
 - e) Expanda **Certificates (Local Computer) > Personal > Certificados** e localize o certificado SSL importado.
 - f) Clique com o botão direito do mouse no certificado importado (selecionado no SQL Server Configuration Manager) e clique em **All Tasks > Manage Private Keys**.
 - g) Em **Group or User names**, clique em **Add**.
 - h) Insira o nome da conta de serviço do SQL que você copiou na etapa anterior.
 - i) Limpe a opção **Allow Full Control**. Por padrão, as permissões Controle total e Leitura serão fornecidas à conta de serviço, mas ela precisa somente conseguir ler a chave privada.
 - j) Feche o **MMC** e inicie o serviço SQL.
3. Verifique se o serviço SQL foi iniciado corretamente.

Pré-requisitos dos Serviços de Informações da Internet (IIS)

1. Baixe o certificado raiz (base 64).
2. Copie o certificado raiz para o site padrão no servidor IIS, C:\inetpub\wwwroot.
3. Marque a caixa de seleção **Authentication** do site padrão.
4. Defina **Anonymous** como **enabled**.
5. Marque a caixa de seleção de regras **Failed Request Tracking**.
6. O arquivo .cer não pode estar bloqueado.
7. Navegue até o local do .cer em um navegador da Web a partir do servidor local, <https://localhost/certname.cer>. O texto do certificado raiz é exibido no navegador.
8. Se o certificado raiz não for exibido no navegador da Web, verifique se o ASP está ativado no servidor IIS como se segue.
 - a) Abra o Gerenciador de Servidores.
 - b) Navegue até o assistente em **Gerenciar > Adicionar Funções e Recursos**.
 - c) Nas funções de servidor, expanda **Servidor Web (IIS)**, expanda **Servidor Web**, expanda **Desenvolvimento de aplicativo** e selecione **ASP**.
 - d) Clique em **Avançar** até a conclusão da instalação.

9. Navegue até <https://localhost/cert.cer>.

Para obter mais informações, consulte [Web Server \(IIS\)](#).

Nota:

Você pode usar a instância do IIS da CA para este procedimento.

Importando o certificado raiz durante configuração inicial do modo FIPS

Quando você concluir as etapas para configurar o XenMobile pela primeira vez no console de linha de comando, deverá concluir estas configurações para importar o certificado raiz. Para obter detalhes sobre as etapas de instalação, consulte [Instalação do XenMobile](#).

- Ativar FIPS: Sim
- Carregar certificado raiz: Sim
- Copiar(c) ou Importar(i): i
- Digite a URL HTTP para importar: <https://<FQDN of IIS server>/cert.cer>
- Server: *FQDN do SQL Server*
- Port: 1433
- User name: a conta de serviço que pode criar o banco de dados (*domain\username*).
- Password: a senha da conta de serviço.
- Database: um nome de sua escolha.

Ativar o modo FIPS em dispositivos móveis

Por padrão, o modo FIPS está desativado em dispositivos móveis. Para ativar o modo FIPS, vá para **Configurações > Propriedades do cliente**, edite a propriedade **Ativar o modo FIPS** e defina o valor como **true**. Para obter mais informações, consulte [Propriedades do cliente](#).

Configurar o clustering

December 22, 2020

Para configurar o clustering, configure os dois endereços IP virtuais de balanceamento de carga a seguir no Citrix ADC.

- **Endereço IP virtual de balanceamento de carga do gerenciamento de dispositivo móvel (MDM):** Um endereço IP virtual de balanceamento de carga MDM é necessário para comunicação com os nós do XenMobile que estão configurados em um cluster. O balanceamento de carga é realizado no modo SSL Bridge.

- **Endereço IP virtual de balanceamento de carga do gerenciamento de aplicativo móvel (MAM):** Os endereços IP virtuais de balanceamento de carga MAM são necessários para que o Citrix Gateway se comunique com os nós do XenMobile que estão configurados em um cluster. No XenMobile, por padrão, todo o tráfego do Citrix Gateway é roteado para o endereço IP virtual do balanceamento de carga na porta 8443.

Os procedimentos deste artigo explicam como criar uma nova máquina virtual (VM) XenMobile e vincular a nova VM a uma VM existente. Essas etapas criam uma configuração de cluster.

Pré-requisitos

- O nó do XenMobile necessário está totalmente configurado.
- Configure o NTP em todos os nós do cluster e no banco de dados do XenMobile. Para que o armazenamento em cluster funcione corretamente, todos esses servidores devem ter o mesmo horário.
- Um endereço IP público para balanceador de carga MDM e um endereço IP privado para MAM.
- Certificados de servidor.
- Um IP livre para o endereço IP virtual do Citrix Gateway.
- Com o XenMobile implantado em uma configuração de cluster e no modo somente MDM ou Enterprise (MDM+MAM): modifique a configuração do balanceador de carga do Citrix ADC para usar a **Persistência do endereço IP de origem** para todos os balanceadores de carga do Citrix ADC MDM, ou seja, servidores virtuais configurados para as portas 8443 e 443. Conclua essa configuração antes de dispositivos de usuários atualizarem para o iOS 11. Para obter mais informações, consulte este artigo do Citrix Knowledge Center: <https://support.citrix.com/article/CTX227406>.
- Para instalar aplicativos da XenMobile Store em dispositivos iOS 11, você deve habilitar a porta 80 no XenMobile Server.

Para ver os diagramas de arquitetura de referência para o XenMobile 10.x nas configurações de cluster, consulte [Arquitetura](#).

Instalando os nós de cluster do XenMobile

Com base no número de nós que você exigir, crie VMs do XenMobile. Aponte as novas VMs para o mesmo banco de dados e forneça as mesmas senhas do certificado PKI.

1. Abra o console da linha de comando da nova VM e insira a nova senha da conta de administrador.
2. Forneça os detalhes de configuração de rede, conforme mostrado na figura a seguir.

```
Network settings:
IP address []: 10.147.75.51
Netmask []: 255.255.255.0
Default gateway []: 10.147.75.1
Primary DNS server []: 10.147.75.240
Secondary DNS server (optional) []:

Commit settings (y/n) [y]:
Applying network settings...
eth0: intr type 3, mode 0, 3 vectors allocated
eth0: NIC Link is Up 10000 Mbps
```

3. Se você desejar usar a senha padrão para proteção de dados, digite **y**; ou digite **n** e insira uma nova senha.

```
Encryption passphrase:
Generate a random passphrase to secure the server data (y/n) [y]:
```

4. Se você desejar usar o modo FIPS, digite **y**; caso contrário, **n**.

```
Federal Information Processing Standard (FIPS) mode:
Enable (y/n) [n]:
```

5. Configure o banco de dados para que você aponte para o mesmo banco de dados que a VM totalmente configurada anterior aponta. Você verá a mensagem: O banco de dados já existe.

```
Database connection:
Local or remote (l/r) [r]:
Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
Use SSL (y/n) [n]:

Server []: sql2012.wg.lab
Port [1433]:
Username [sa]:
Password:
Database name [DB_service1]: DB_51

Commit settings (y/n) [y]:

Checking database status...
Database already exists.

To enable realtime communication between cluster members please open port 80 using Firewall menu option in CLI menu once the system configuration is complete

Saving server and client certificate passwords..
```

6. Insira as mesmas senhas dos certificados que você forneceu para a primeira VM.


```
Database connection:
Local or remote (l/r) [r]:
Type (mi=Microsoft SQL, p=PostgreSQL) [mi]:
Use SSL (y/n) [n]:

Server []: sql2012.wg.lab
Port [1433]:
Username [sa]:
Password:
Database name [DB_service1]: DB_51

Commit settings (y/n) [y]:

Checking database status...
Database already exists.
To enable realtime communication between cluster members please open port 80 using Firewall menu option in CLI menu once the system configuration is complete

Saving server and client certificate passwords..

WARNING: Please enter the same passwords used to generate internal Public Key Infrastructure (PKI) in first node
Do you want to use the same password for all the certificates of the PKI [y]:
```

Depois que você tiver inserido a senha, a configuração inicial do segundo nó será concluída.

```
Saving server and client certificate passwords..

WARNING: Please enter the same passwords used to generate internal Public Key Infrastructure (PKI) in first node
Do you want to use the same password for all the certificates of the PKI [y]:
y
New password:
Re-enter new password:
Saving server and client certs password...

Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!
Stopping configuration app... [ OK ]
Starting configuration app...
this may take a few seconds.....
application started [ OK ]
Stopping main app... [ OK ]
Starting main app...
this may take a few minutes....._
```

7. Quando a configuração for concluída, o servidor será reiniciado e a caixa de diálogo de login será exibida.

```
Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...

Initial system configuration complete!
Stopping configuration app... [ OK ]
Starting configuration app...
  this may take a few seconds.....
  application started [ OK ]
Stopping main app... [ OK ]
Starting main app...
  this may take a few minutes.....^I.....
.....
  application started [ OK ]

To access the console, from a web browser, go to the following location and
log on with your console credentials:
  https://10.147.75.59:4443/

Starting monitoring... [ OK ]
xms51.wg.lab login: █
```

Nota:

A caixa de diálogo de login é idêntica à caixa de diálogo de login da primeira VM. A correspondência é uma maneira de confirmar que ambas as VMs usam o mesmo servidor do banco de dados.

8. Use o nome de domínio totalmente qualificado (FQDN) do XenMobile para abrir o console XenMobile em um navegador da Web.
9. No console XenMobile, clique no ícone de chave de boca no canto superior direito do console.



A página **Suporte** é aberta.

10. Em **Avançado**, clique em **Informações de Cluster**.

Support

<p>Diagnostics</p> <p>NetScaler Gateway Connectivity Checks</p> <p>XenMobile Connectivity Checks</p>	<p>Support Bundle</p> <p>Create Support Bundles</p>	<p>Links</p> <p>Citrix Product Documentation</p> <p>Citrix Knowledge Center</p>
<p>Log Operations</p> <p>Logs</p> <p>Log Settings</p>	<p>Advanced</p> <p>Cluster Information</p> <p>Garbage Collection</p> <p>Java Memory Properties</p> <p>Macros</p> <p>PKI Configuration</p> <p>Anonymization and De-anonymization</p>	<p>Tools</p> <p>APNs Signing Utility</p> <p>Citrix Insight Services</p> <p>Device NetScaler Connector Status</p>

Todas as informações sobre o cluster, incluindo o membro do cluster, as informações de conexão do dispositivo, as tarefas e assim por diante, são exibidas. O novo nó agora é um membro do cluster.

Support > Cluster Information

Cluster Information

Provides information about each of the nodes in the cluster.

▼ Cluster Members

Node ID	Node name	Status	Role	First check-in	Next check-in
177425211		ACTIVE	null	2019-04-22 14:40:34.677	2019-04-22 01:52:56.293
177425200		ACTIVE	OLDEST	2019-04-22 14:30:08.47	2019-04-22 02:09:02.61

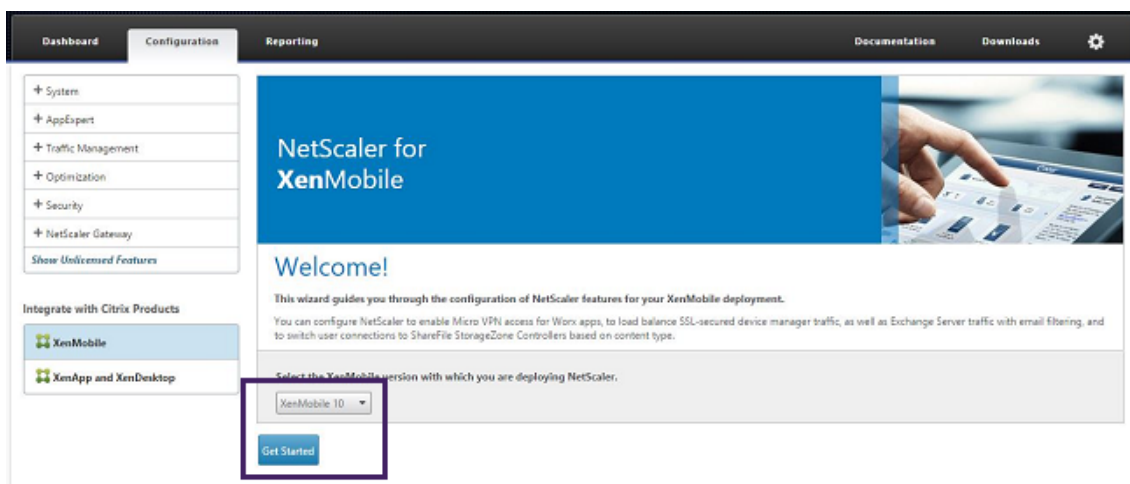
Showing 1 - 2 of 2 items

Você pode adicionar outros nós seguindo as mesmas etapas. O primeiro nó adicionado ao cluster tem uma Função de **MAIS ANTIGO**. Nós adicionados depois disso mostrarão uma Função de **NENHUM** ou **nulo**.

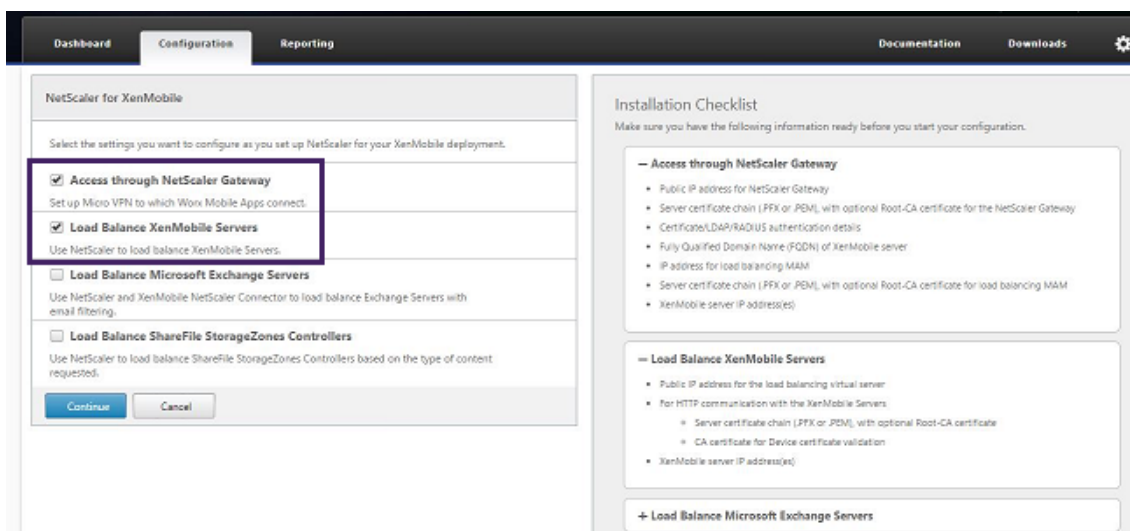
Para configurar o balanceamento de carga do cluster do XenMobile no Citrix ADC

Depois de adicionar os nós como membros do cluster do XenMobile, balanceie a carga dos nós para poder acessar os clusters. O balanceamento de carga é realizado por meio da execução do Assistente do XenMobile disponível no Citrix ADC. As etapas a seguir descrevem como balancear a carga do XenMobile executando o assistente.

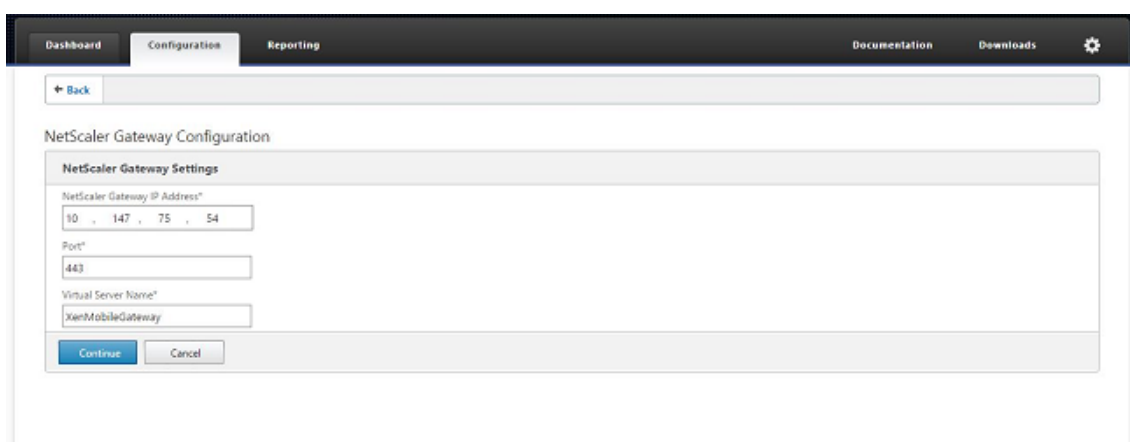
1. Faça login no Citrix ADC.
2. Na guia Configuration, clique em **XenMobile** e em **Get Started**.



3. Marque as caixas de seleção **Access through Citrix Gateway** e **Load Balance XenMobile Servers** e clique em **Continue**.



4. Insira o endereço IP do Citrix Gateway e clique em **Continue**.



5. Associe o certificado de servidor ao endereço IP virtual do Citrix Gateway executando uma das

opções a seguir e clique em **Continue**.

- Em **Use existing certificate**, selecione o certificado do servidor na lista.
- Clique na guia **Install Certificate** para carregar um novo certificado de servidor.

The screenshot shows the NetScaler Gateway Configuration page. At the top, there are navigation tabs: Dashboard, Configuration (selected), and Reporting. On the right, there are links for Documentation and Downloads, and a settings icon. Below the navigation is a 'Back' button. The main content area is titled 'NetScaler Gateway Configuration'. Underneath, there's a 'NetScaler Gateway Settings' section with a table showing 'Virtual Server Name' as 'XenMobileGateway', 'IP Address' as '10.147.75.54', and 'Port' as '443'. Below this is the 'Server Certificate for NetScaler Gateway' section. It contains a paragraph explaining that a server certificate is used for authentication in an SSL handshake. There are two radio buttons: 'Use existing certificate' (selected) and 'Install Certificate'. Below the radio buttons is a dropdown menu for 'Server Certificate*' with the value 'wildcert-wg-lab.pfx_CERT_KEY'. At the bottom of this section are 'Continue' and 'Do It Later' buttons.

6. Insira os detalhes do servidor de Autenticação e clique em **Continue**.

The screenshot shows the 'Authentication Settings' page. It starts with a heading 'Authentication Settings' and a paragraph explaining that a primary authentication method should be selected for client connections. Below this is a dropdown menu for 'Primary authentication method*' set to 'Active Directory/LDAP'. There are several input fields: 'IP Address*' with the value '10 . 147 . 75 . 240' and an unchecked 'IPv6' checkbox; 'Port*' with the value '389'; 'Base DN*' with the value 'dc=wg,dc=lab'; 'Service account*' with the value 'administrator@wg.lab'; 'Password*' and 'Confirm Password*' fields with masked characters; 'Time out (seconds)*' with the value '3'; and 'Server Logon Name Attribute*' with the value 'userPrincipalName'. At the bottom, there is a dropdown for 'Secondary authentication method*' set to 'None'. 'Continue' and 'Cancel' buttons are at the bottom.

Nota:

Confirme que o Server Logon Name Attribute seja o mesmo que você forneceu na configuração LDAP do XenMobile.

7. Nas configurações do XenMobile, insira o Load Balancing FQDN for MAM e clique em **Continue**.

The screenshot shows the 'XenMobile Settings' configuration window. It includes fields for 'Load Balancing FQDN for MAM*' (xms51.wg.lab), 'Load Balancing IP address for MAM*' (10.147.75.55), and 'Port*' (8443). Under 'SSL Traffic Configuration*', the 'HTTPS communication to XenMobile Server' radio button is selected. The 'Split DNS mode for Micro VPN*' is set to 'BOTH'. There is an unchecked checkbox for 'Enable split tunneling' and 'Continue' and 'Cancel' buttons at the bottom.

Nota:

Confirme que o FQDN do endereço IP virtual de balanceamento de carga MAM e o FQDN do XenMobile sejam os mesmos.

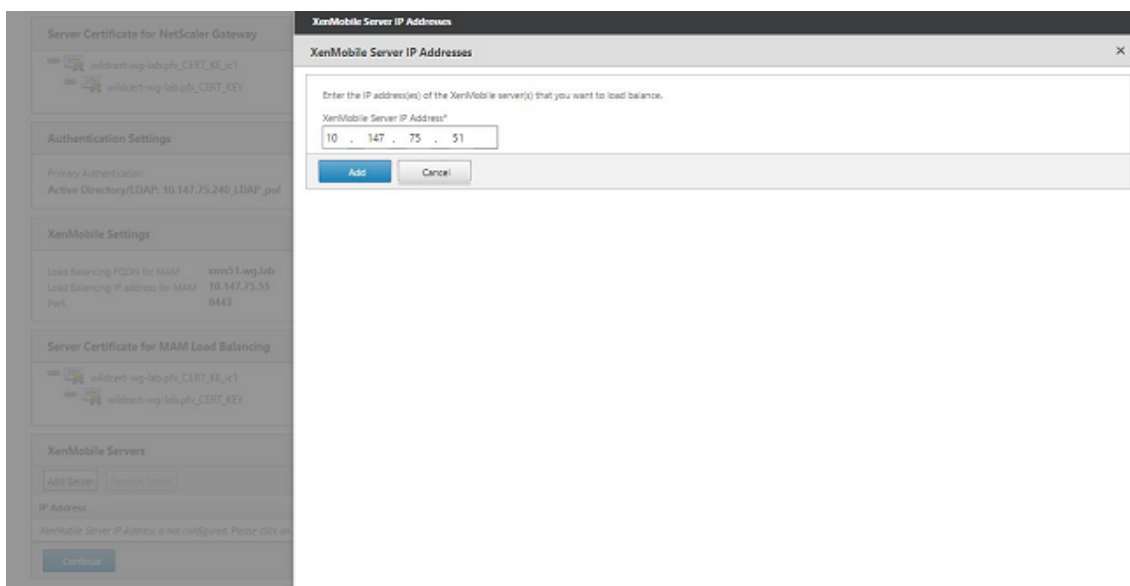
- 8. Se você desejar usar o modo SSL Bridge (HTTPS), selecione **HTTPS communication to XenMobile Server**. No entanto, se você desejar usar a descarga de SSL, selecione **HTTP communication to XenMobile Server**, conforme mostrado na figura anterior. Para este artigo, a opção é o modo SSL Bridge (HTTPS).
- 9. Associe o certificado de servidor do endereço IP virtual de balanceamento de carga MAM e clique em Continue.

This block contains two screenshots. The top one is a summary of the 'XenMobile Settings' configuration, showing the FQDN (xms51.wg.lab), IP (10.147.75.55), port (8443), and SSL configuration (HTTPS communication to XMS Server, Split Tunnel: OFF, Split DNS: BOTH). The bottom screenshot is the 'Server Certificate for MAM Load Balancing' screen, where the 'Use existing certificate' radio button is selected and the 'Server Certificate*' dropdown is set to 'wildcert-wg-lab.pfx_CERT_KEY'. 'Continue' and 'Do It Later' buttons are at the bottom.

- 10. Em XenMobile Servers, clique em **Add Server** para adicionar os nós do XenMobile.

This block contains two screenshots. The top one shows the 'Server Certificate for MAM Load Balancing' screen with two certificates listed: 'wildcert-wg-lab.pfx_CERT_KEY_1' and 'wildcert-wg-lab.pfx_CERT_KEY'. The bottom screenshot is the 'XenMobile Servers' screen, which has an 'Add Server' button and a table with columns for 'IP Address' and 'Port'. A message below the table says 'XenMobile Server IP Address is not configured. Please click on Add Server to configure.' and there is a 'Continue' button at the bottom.

- 11. Insira o endereço IP do nó do XenMobile e clique em Add.



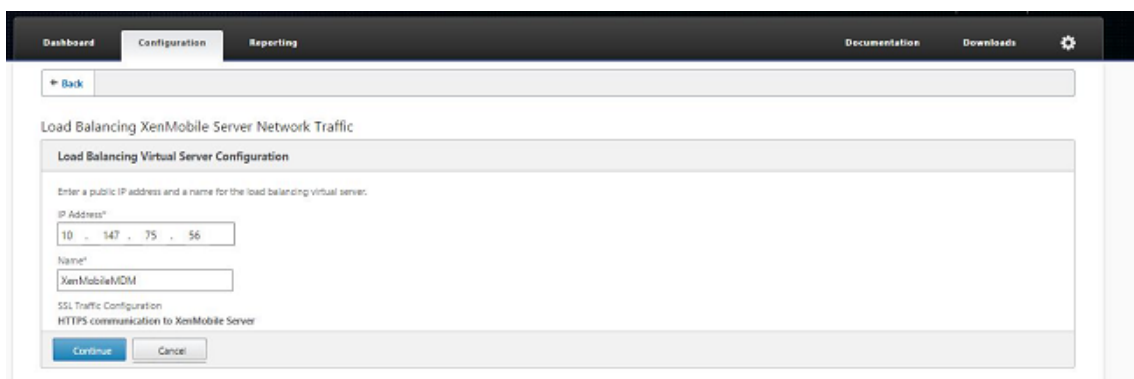
12. Repita as etapas 10 e 11 para adicionar mais nós do XenMobile que fazem parte do cluster do XenMobile. Você verá todos os nós do XenMobile que adicionou. Clique em Continue.



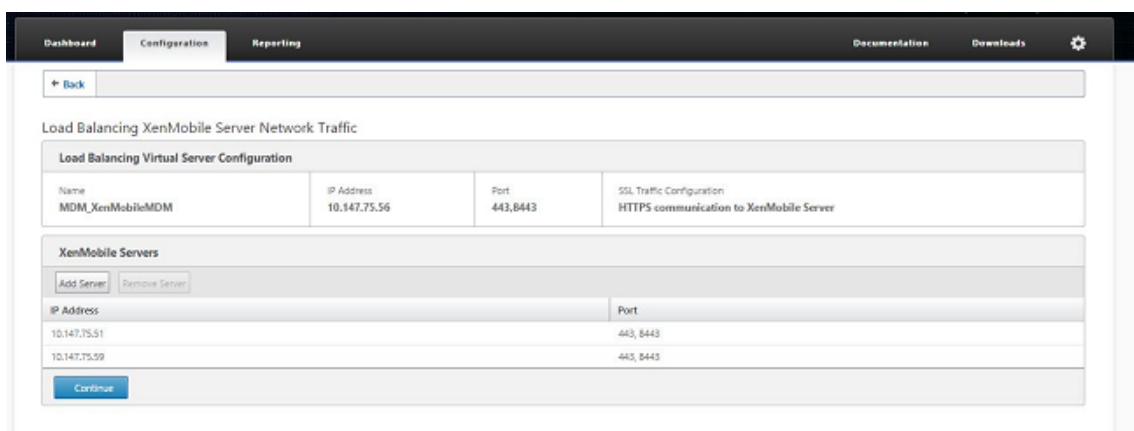
13. Clique em **Load Balance Device Manager Servers** para continuar com a configuração do balanceamento de carga MDM.



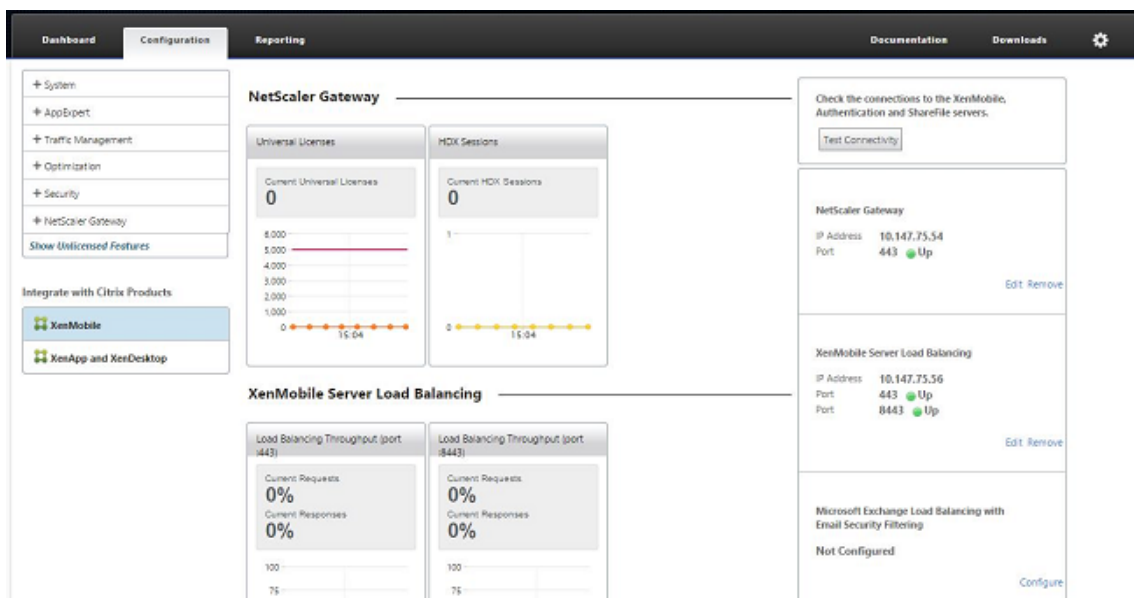
14. Insira o endereço IP a ser usado para o endereço IP de balanceamento de carga MDM e, em seguida, clique em **Continue**.



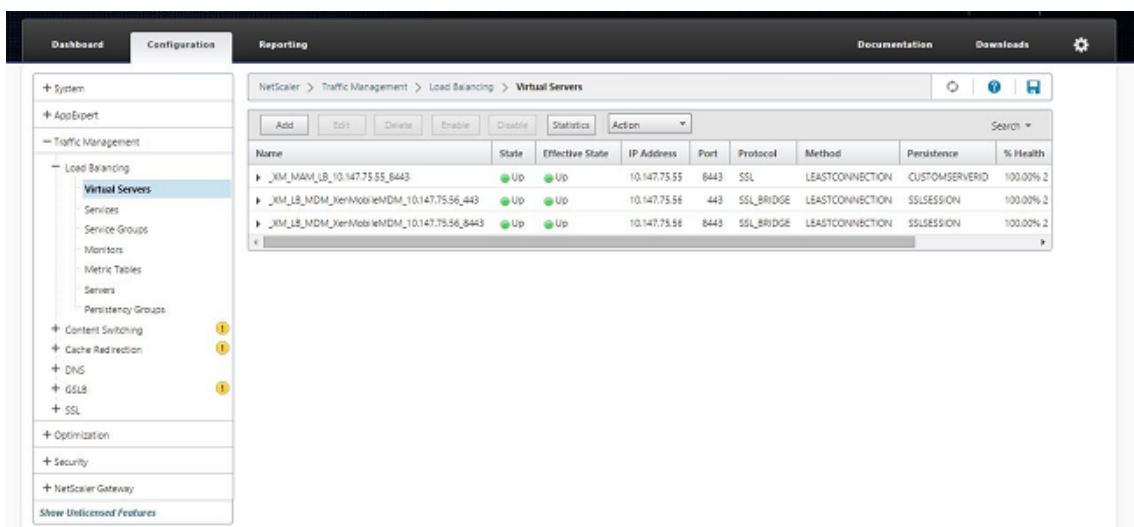
15. Depois que você vir os nós do XenMobile na lista, clique em **Continue** e, em seguida, clique em Done para concluir o processo.



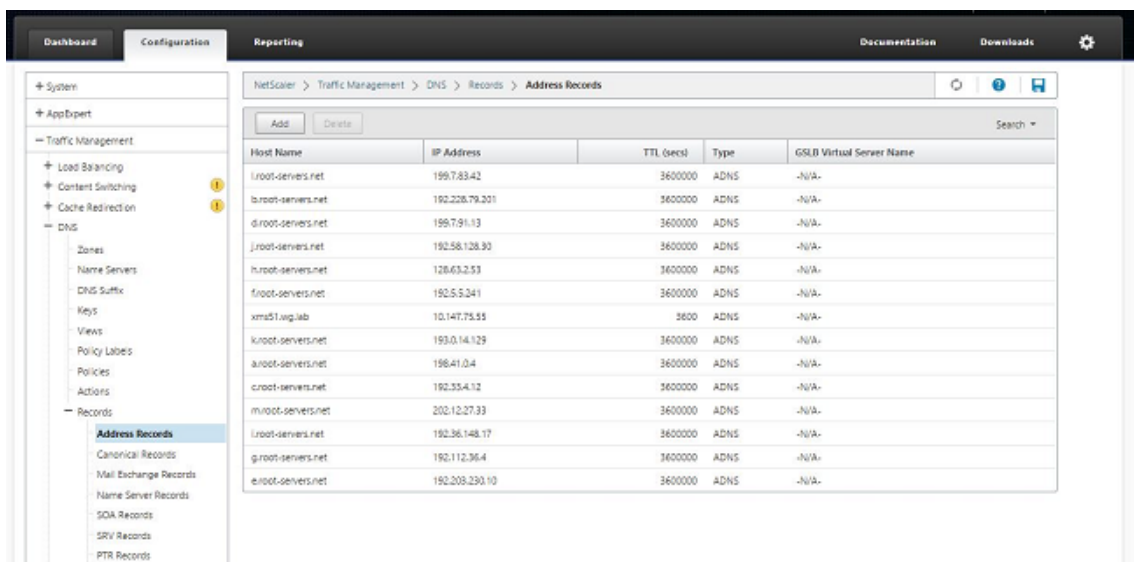
Você verá o status do endereço IP virtual na página XenMobile.



16. Para confirmar se os endereços IP virtuais estão em execução, clique na guia Configuration e navegue até **Traffic Management > Load Balancing > Virtual Servers**.



Você também verá que a entrada DNS no Citrix ADC aponta para o endereço IP virtual do balanceamento de carga MAM.



Guia de recuperação de desastres

April 23, 2020

Você pode desenvolver e configurar implantações do XenMobile que incluem vários locais de recuperação de desastres usando uma estratégia de failover ativo-passivo. Para obter detalhes, consulte o artigo sobre [Recuperação de desastres](#) no manual de implantação do XenMobile.

Ativar servidores proxy

January 8, 2020

Para controlar o tráfego de saída da Internet, você pode configurar um servidor proxy no XenMobile para transportar o tráfego. Você configura um servidor proxy por meio da interface de linha de comando (CLI). Configurar o servidor proxy exige que você reinicie o sistema.

1. No menu principal da CLI do XenMobile, digite **2** para selecionar o menu System.
2. No menu System, digite **6** para selecionar o menu Proxy Server.

```
[2] System
[3] Troubleshooting
[4] Help
[5] Log Out
-----
Choice: [0 - 5] 2
-----
System Menu
-----
[0] Back to Main Menu
[1] Display System Date
[2] Set Time Zone
[3] Display System Disk Usage
[4] Update Hosts File
[5] Display Device Management Instance Name
[6] Proxy Server
[7] HAdmin (CLI) Password
[8] Restart Server
[9] Shutdown Server
[10] Advanced Settings
-----
```

3. No menu Proxy Configuration, digite **1** para selecionar SOCKS.

Antes de salvar essa configuração, você também deve configurar HTTPS. O proxy não funcionará a menos que você salve as configurações SOCKS e HTTPS na mesma configuração.

```
-----  
Choice: [0 - 10] 6  
-----  
Proxy Configuration Menu  
-----  
[0] Back to System Menu  
[1] SOCKS  
[2] HTTPS  
[3] HTTP  
[4] Exclusion List  
[5] Display Configuration  
[6] Delete Proxy Configuration  
-----
```

4. Digite o endereço IP, o número de porta e o destino do seu servidor proxy. Consulte a tabela a seguir para conhecer os tipos de destino compatíveis com cada tipo de servidor proxy.

Tipo de proxy	Destinos compatíveis
SOCKS	APNS
HTTP	APNS, Web, PKI
HTTPS	Web, PKI
HTTP com autenticação	Web, PKI
HTTPS com autenticação	Web, PKI

```
-----  
Proxy Configuration Menu  
-----  
[0] Back to System Menu  
[1] SOCKS  
[2] HTTPS  
[3] HTTP  
[4] Exclusion List  
[5] Display Configuration  
[6] Delete Proxy Configuration  
-----  
Choice: [0 - 6] 1  
  
Enter socks proxy information  
Address [1]: 203.0.113.23  
Port[]: 1080  
Target - APNS  
Proxy configuration updated successfully.  
Please restart all nodes in the cluster for the changes to take effect  
Are you sure to restart the system? [y/n]: █
```

5. Digite **n**, digite **2** para selecionar HTTPS e digite o endereço IP, o número da porta e o destino do seu servidor proxy.
6. Se você optar por configurar um nome do usuário e uma senha para autenticação no servidor proxy, digite **y** e, em seguida, digite o nome do usuário e a senha.

```
[0] Back to System Menu  
[1] SOCKS  
[2] HTTPS  
[3] HTTP  
[4] Exclusion List  
[5] Display Configuration  
[6] Delete Proxy Configuration  
-----  
Choice: [0 - 6] 2  
  
Enter https proxy information  
Address [1]: 203.0.113.23  
Port[]: 4443  
Configure username & password [y/n]: y  
Username: Justaname  
Password:  
Target - WEB  
WEB proxy configured. Override proxy settings?[y/n]: █
```

7. Digite **y** para salvar a configuração.

Configurar SQL Server

April 23, 2020

Para conexões com o SQL Server a partir de um XenMobile Server local, você pode usar qualquer um dos seguintes drivers:

- O driver padrão
- jTDS
- Driver Microsoft Java Database Connectivity (JDBC)

O driver jTDS é o driver padrão quando você:

- Instala o XenMobile Server no local.
- Atualize de um XenMobile Server configurado para usar o driver jTDS.

Para ambos os drivers, o XenMobile é compatível com a autenticação do SQL Server ou com a autenticação do Windows. Para essas combinações de autenticação e driver, o SSL pode estar ligado ou desligado.

Quando você usa a autenticação do Windows com o driver Microsoft JDBC, o driver usa a autenticação integrada com o Kerberos. O XenMobile contata o Kerberos para obter os detalhes do Centro de Distribuição de Chave (KDC) Kerberos. Se os detalhes necessários não estiverem disponíveis, a CLI do XenMobile solicita o endereço IP do servidor do Active Directory.

Para mudar do driver jTDS para o driver JDBC, use SSH para todos os nós do XenMobile Server e use o CLI do XenMobile para a configuração. As etapas variam acordo com a sua configuração do driver jTDS atual, da seguinte maneira.

Mudar para Microsoft JDBC (autenticação do SQL Server)

Para concluir essas etapas, você precisa do nome de usuário do SQL Server e da senha.

1. Use SSH para todos os nós do XenMobile Server.
2. No menu principal da CLI do XenMobile, digite **2** para selecionar o **System Menu**.
3. Digite **12** para selecionar as configurações avançadas.
4. Digite **7** para selecionar mudar o driver JDBC e digite **m** para Microsoft.

```
[12] Advanced Settings
-----
Choice: [0 - 12] 12

***** WARNING *****
Please only modify these options if you are
in contact with Citrix Support
*****

-----
Advanced Settings
-----
[0] Back to System Menu
[1] Toggle FIPS mode
[2] Custom Ciphers
[3] SSL protocols
[4] Reset SSL Certificate
[5] Reset pki.xml
[6] Server Tuning
[7] Switch JDBC driver
-----
Choice: [0 - 7] 7
JDBC driver type (JTDS or Microsoft) []: |
```

5. Quando solicitado, digite **y** para escolher a autenticação SQL e, em seguida, digite o nome de usuário do SQL Server e a senha.
6. Repita as etapas para cada nó do XenMobile Server.
7. Reinicie cada nó do XenMobile Server.

Mudar para Microsoft JDBC (SSL está desativado; autenticação Windows)

Para concluir estas etapas, você precisa do nome e da senha do usuário do Active Directory, do realm Kerberos KDC e do nome de usuário KDC.

1. Use SSH para todos os nós do XenMobile Server.
2. No menu principal da CLI do XenMobile, digite **2** para selecionar o **System Menu**.
3. Digite **12** para selecionar as configurações avançadas.
4. Digite **7** para selecionar mudar o driver JDBC e digite **m**.
5. Quando solicitado se deseja usar a autenticação do SQL Server, digite **n**.
6. Quando solicitado, digite o nome de usuário e a senha do Active Directory configurados para o SQL Server.
7. Se o XenMobile não detectar automaticamente o realm Kerberos KDC, ele solicitará os detalhes KDC, incluindo o FQDN do SQL Server.

8. Quando solicitado se deseja usar SSL, digite **n**. XenMobile salva a configuração. Se o XenMobile não conseguir salvar a configuração devido a erros, ele mostra uma mensagem de erro e os detalhes que você inseriu.
9. Repita as etapas para cada nó do XenMobile Server.
10. Reinicie cada nó do XenMobile Server.

Para alterar a senha do banco de dados XenMobile

Siga esta orientação para alterar a senha do banco de dados XenMobile, por exemplo, quando o Suporte Citrix direciona você para fazer uma alteração de senha.

Se o seu SQL Server usar a autenticação do Windows, faça alterações de senha do banco de dados no Windows Active Directory. Em seguida, atualize a conta de administrador do banco de dados no servidor de banco de dados para sincronizar a alteração de senha. Depois você pode alterar a senha no XenMobile, da seguinte forma.

Importante:

- Planeje uma janela de manutenção para alterar a senha do banco de dados no XenMobile. Uma alteração de senha deve ocorrer durante o tempo de inatividade do sistema.
- Quando você alterar a senha, confirme que todos os nós do XenMobile estão conectados à rede. Depois de alterar a senha, reinicie o XenMobile.

Se você não reiniciar o XenMobile após uma alteração de senha, o XenMobile entrará no modo de recuperação. Nesse caso, reverta para a senha antiga no SQL Server, reinicie o XenMobile e altere a senha novamente.

1. Verifique se todos os nós do XenMobile Server estão em execução. Para um ambiente em cluster, coloque todos os nós em operação.
2. Bloqueie o tráfego de entrada de dispositivos para o XenMobile no balanceador de carga Citrix ADC desativando os servidores virtuais.
3. Para alterar a senha do banco de dados no SQL Server: faça login na CLI do XenMobile, navegue até **Configuração > Banco de dados** e insira a senha alterada quando solicitado:

```
1 Server []: <ipAddress>
2 Port [1433]: 1433
3 Username [sa]: <userName>
4 Password: <*****>
5 <!--NeedCopy-->
```

4. Escolha **Y** para reiniciar o servidor.
5. Repita as etapas 3 e 4 para todos os outros nós no cluster.

6. Desbloqueie o tráfego de entrada dos dispositivos ativando os servidores virtuais no balanceador de carga do Citrix ADC.

Propriedades do servidor

November 30, 2020

O XenMobile apresenta muitas propriedades que se aplicam a operações de todo o servidor. Este artigo descreve muitas das propriedades do servidor e detalha como adicionar, editar ou excluir propriedades do servidor.

Algumas propriedades são chaves personalizadas. Para adicionar uma chave personalizada, clique em **Adicionar** e, em seguida, em **Chave**, escolha **Chave personalizada**.

Para obter informações sobre as propriedades configuradas com mais frequência, consulte [Propriedades do servidor](#) no manual virtual do XenMobile.

Definições de propriedade de servidor

Adicionar dispositivo sempre

- Se **true**, o XenMobile adiciona um dispositivo ao console XenMobile, mesmo que o processo de registro falhe, para que você possa ver quais dispositivos tentaram se registrar. O padrão é **false**.

Intervalo de limitação de emissão de certificado do cliente AG

- O período de tolerância entre a geração de certificados. Esse intervalo impede que o XenMobile gere vários certificados para um dispositivo em um curto período. A Citrix recomenda não alterar esse valor. O padrão é **30** minutos.

Tempo de execução de limpeza do log de auditoria

- A hora do início da limpeza do log de auditoria, formatado como HH:MM AM/PM. Exemplo: 04:00 AM. O padrão é **02:00 AM**.

Intervalo de limpeza de log de auditoria (em dias)

- O número de dias durante os quais o XenMobile mantém o log de auditoria. O padrão é **1**.

Agente de log de auditoria

- Se for **False**, a propriedade não registrará os eventos da interface do usuário (IU). O padrão é **false**.

Retenção de log de auditoria (em dias)

- O número de dias durante os quais o XenMobile mantém o log de auditoria. O padrão é **7**.

auth.ldap.connect.timeout e auth.ldap.read.timeout

- Para compensar lentas respostas LDAP, a Citrix recomenda que você adicione as propriedades do servidor para as seguintes chaves personalizadas.
 - Chave: **chave personalizada**
 - Chave: **auth.ldap.connect.timeout**
 - Valor: **60000**
 - Nome de exibição: **auth.ldap.connect.timeout**
 - Descrição: **tempo limite da conexão LDAP**
 - Chave: **chave personalizada**
 - Chave: **auth.ldap.read.timeout**
 - Valor: **60000**
 - Nome de exibição: **auth.ldap.read.timeout**
 - Descrição: **tempo limite de leitura do LDAP**

Renovação de certificado em segundos

- O número de segundos antes que um certificado expire quais o XenMobile começa a renovar os certificados. Por exemplo, se um certificado expirará 30 de dezembro e esta propriedade é se 30 dias: se o dispositivo se conecta entre 1 de dezembro e 30 de dezembro, o XenMobile tenta renovar o certificado. O padrão é **2592000** segundos (30 dias).

Tempo limite de conexão

- O limite de inatividade de sessão, em minutos, após o qual o XenMobile fecha a conexão TCP a um dispositivo. A sessão permanece aberta. Aplica-se aos dispositivos Android e Windows CE e suporte remoto. O padrão é **5** minutos.

Tempo limite de conexão ao servidor de certificação Microsoft

- O número de segundos durante o qual o XenMobile espera por uma resposta do servidor de certificado. Se o servidor de certificados for lento e tiver uma grande quantidade de tráfego, você poderá aumentar esse valor para 60 segundos ou mais. Um servidor de certificado que não responde após 120 segundos precisa de manutenção. Padrão é **15000** milissegundos (15 segundos).

Canal de implantação padrão

- Determina como o XenMobile implanta um recurso com um dispositivo: no nível do usuário (**DEFAULT_TO_USER**) ou no nível de dispositivo. O padrão é **DEFAULT_TO_DEVICE**.

Implantar limpeza de log (em dias)

- O número de dias durante os quais o XenMobile deve manter o log de implantação. O padrão é **7**.

Desativar verificação de nome de host

- Como padrão, a verificação do nome do host está ativada nas conexões de saída, exceto para o servidor Microsoft PKI. Quando a verificação de nome de host falha, o log do servidor inclui erros como: “Não é possível conectar com o servidor de compra por volume: o nome de host ‘192.0.2.0’ não corresponde à entidade do certificado fornecida pelo par correspondente” Se a verificação do nome do host interromper sua implantação, altere essa propriedade para **true**. O padrão é **false**.

Desativar verificação do servidor SSL

- Se o valor for **True**, desativará a validação de certificado de servidor SSL quando todas as seguintes condições forem atendidas:
 - Você ativou a autenticação baseada em certificado no seu XenMobile Server
 - O servidor Microsoft CA é o emissor do certificado
 - Uma AC interna, em cuja raiz o XenMobile Server não confia, assinou o seu certificado.

O padrão é **true**.

Ativar console

- Se for **true**, permitirá o acesso do usuário ao console do Portal de autoajuda. O padrão é **true**.

Ativar relatórios de falhas

- Se for **true**, a Citrix coletará relatórios e diagnósticos de falhas para ajudar a solucionar problemas com o Secure Hub para iOS e Android. Se for **false**, não haverá coleta de dados. O valor padrão é **true**.

Ativar/desativar registro em log de estatísticas da hibernação para diagnóstico

- Se **true**, ativará o registro em log de estatísticas de Hibernação para ajudar na resolução de problemas de desempenho de aplicativos. A Hibernação é um componente usado para conexões do XenMobile com o Microsoft SQL Server. Por padrão, o registro em log está desativado porque ele afeta o desempenho do aplicativo. Ative o registro em log por pouco tempo somente para evitar a criação de um arquivo de log enorme. O XenMobile grava os logs em `/opt/sas/logs/hibernate_stats.log`. O padrão é **false**.

Ativar OTAE do macOS

- Se for **false**, impedirá o uso de um link de registro para dispositivos macOS, o que significa que os usuários do macOS só podem se registrar usando um convite para registro. O padrão é **true**.

Ativar notificação gatilho

- Ativa ou desativa as notificações de cliente do Secure Hub. O valor **true** ativa notificações. O padrão é **true**.

`force.server.push.required.apps`

- Permite a implantação forçada dos aplicativos necessários em dispositivos Android e iOS em situações como as seguintes:
 - Carregue um novo aplicativo e marque-o conforme necessário.
 - Marque um aplicativo existente conforme necessário.
 - Quando o usuário exclui um aplicativo necessário.
 - Está disponível uma atualização do Secure Hub.

A implantação forçada de aplicativos obrigatórios é **false** por padrão. Crie a chave personalizada e defina **Valor** como **true** para ativar a implantação forçada. Durante a implantação forçada, os aplicativos obrigatórios habilitados para MDX, incluindo aplicativos corporativos e aplicativos da loja de aplicativos pública, são atualizados imediatamente. A atualização ocorre mesmo se você configurar uma política MDX para um período de tolerância de atualização do aplicativo e o usuário optar por atualizar o aplicativo posteriormente.

- Chave: **chave personalizada**

- Chave: **force.server.push.required.apps**
- Valor: **false**
- Nome de exibição: **force.server.push.required.apps**
- Descrição: **forçar a implantação dos aplicativos obrigatórios**

Recepção completa de usuários do ActiveSync permitidos e negados

- O intervalo (em segundos) em que o XenMobile recebe uma lista completa (linha de base) dos usuários do ActiveSync permitidos e negados. O padrão é **28800** segundos.

hibernate.c3p0.idle_test_period

- Essa propriedade do XenMobile Server, uma chave personalizada, determina o tempo ocioso em segundos antes de uma conexão ser validada automaticamente. Configure a chave da seguinte maneira. O padrão é **30**.
- Chave: **chave personalizada**
- Chave: **hibernate.c3p0.idle_test_period**
- Valor: **30**
- Nome de exibição: **hibernate.c3p0.idle_test_period =nnn**
- Descrição: **período de teste de inatividade de hibernação**

hibernate.c3p0.max_size

- Essa chave personalizada determina o número máximo de conexões que o XenMobile pode abrir no banco de dados do SQL Server. O XenMobile usa o valor especificado para esta chave personalizada como um limite superior. As conexões abrem somente se você precisar delas. Baseie suas configurações na capacidade do seu servidor de banco de dados. Para obter mais informações, consulte [Ajuste das operações do XenMobile](#). Configure a chave da seguinte maneira. O padrão é **1000**.
- Chave: **hibernate.c3p0.max_size**
- Valor: **1000**
- Nome de exibição: **hibernate.c3p0.max_size**
- Descrição: **conexões de banco de dados ao SQL**

hibernate.c3p0.min_size

- Essa chave personalizada determina o número mínimo de conexões que o XenMobile abre no banco de dados do SQL Server. Configure a chave da seguinte maneira. O padrão é **100**.
- Chave: **hibernate.c3p0.min_size**
- Valor: **100**
- Nome de exibição: **hibernate.c3p0.min_size**
- Descrição: **conexões de banco de dados ao SQL**

hibernate.c3p0.timeout

- Essa chave personalizada determina o tempo limite de ociosidade, em segundos. O padrão é **120**.
- Chave: **chave personalizada**
- Chave: **hibernate.c3p0.timeout**
- Valor: **120**
- Nome de exibição: **hibernate.c3p0.timeout**
- Descrição: **tempo limite de inatividade do banco de dados**

Identifica se a telemetria está ativada ou não

- Identifica se a telemetria (Programa de melhoria da experiência do cliente ou CEIP) está ativada. Você pode optar por participar do CEIP ao instalar ou atualizar o XenMobile. Se o XenMobile tiver 15 uploads com falha consecutivos, ele desativará a telemetria. O padrão é **false**.

Tempo limite de inatividade em minutos

- Se a propriedade **Tipo de tempo limite de WebServices** for **INACTIVITY_TIMEOUT**: essa propriedade define o número de minutos após os quais o XenMobile faz logut de um administrador inativo que fez o seguinte:
 - Usou a API pública do XenMobile para serviços REST para acessar o console XenMobile.
 - Usou a API pública do XenMobile para serviços REST para acessar os aplicativos de terceiros. Um tempo limite de **0** significa que um usuário inativo permanece conectado.

O padrão é **5**.

Instalação automática de registro de gerenciamento de dispositivo iOS ativada

- Se for true, essa propriedade reduzirá a quantidade de interação do usuário durante o registro do dispositivo. Os usuários precisam clicar em **Instalação de autoridade de certificação raiz** (se necessário) e em **Instalação do perfil MDM**.

Primeira etapa do registro de gerenciamento de dispositivos iOS em atraso

- Depois que um usuário insere suas credenciais durante o registro de dispositivo, este especifica o período de tempo a aguardar antes de avisar para instalar a AC de raiz. A Citrix recomenda que você edite essa propriedade apenas se você tiver problemas de latência ou velocidade de rede. Nesse caso, não defina o valor para mais de 5000 milissegundos (5 segundos). O padrão é **1000** milissegundos (1 segundo).

Última etapa do registro de gerenciamento de dispositivos iOS em atraso

- Durante o registro de dispositivo, este valor da propriedade especifica o período de tempo de espera entre instalar o perfil MDM e iniciar o agente no dispositivo. A Citrix recomenda que você edite essa propriedade apenas se você tiver problemas de latência ou velocidade de rede. Nesse caso, não defina o valor para mais de 5000 milissegundos (5 segundos). O padrão é **1000** milissegundos (1 segundo).

Modo de entrega de identidade de gerenciamento de dispositivo iOS

- Especifica se o XenMobile distribui o certificado do MDM para dispositivos usando **SCEP** (recomendado por motivos de segurança) ou **PKCS12**. No modo de PKCS12, o par de chaves é gerado no servidor e nenhuma negociação é realizada. O padrão é **SCEP**.

Gerenciamento de dispositivo iOS tamanho de chave de identidade

- Define o tamanho das chaves privadas para identidades MDM, o serviço de perfil de iOS e identidades de agente do XenMobile iOS. O padrão é **1024**.

Gerenciamento de dispositivo iOS dias de renovação de identidade

- Especifica o número de dias antes da expiração do certificado que o XenMobile começa a renovação de certificados. Por exemplo: se um certificado expirar em 10 dias e esta propriedade for **10** dias, se um dispositivo se conectar 9 dias antes da expiração, o XenMobile emitirá um novo certificado. O padrão é **30** dias.

Senha da chave privada de iOS MDM APNS

- Essa propriedade contém a senha de APNs, que é necessária para o XenMobile para notificações por push para os servidores da Apple.

Período de inatividade antes que o dispositivo seja desconectado

- Especifica o tempo que um dispositivo pode permanecer inativo, incluindo a última autenticação, antes que o XenMobile o desconecte. O padrão é **7** dias.

Máximo de dispositivos somente MAM

- Essa chave personalizada limita o número de dispositivos somente MAM que cada usuário pode registrar. Configure a chave da seguinte maneira. Um **Valor** de **0** permite registros ilimitados de dispositivos.
- Chave = **number.of.mam.devices.per.user**
- Valor = **5**
- Nome para exibição = **MAM Only Device Max**
- Descrição = **limita o número de dispositivos MAM que cada usuário pode registrar.**

MaxNumberOfWorker

- O número de threads utilizados ao importar várias licenças de compra por volume. O padrão é **3**. Se precisar de mais otimização, você pode aumentar o número de threads. No entanto, com um número maior de threads, como 6, uma importação de compra por volume resulta em uso de CPU alto.

Logon único do Citrix ADC

- Se for **false**, desativará o recurso de retorno de chamada do XenMobile durante o logon único do Citrix ADC para XenMobile. Se a configuração de Citrix Gateway incluir uma URL de retorno de chamada, o XenMobile usa o recurso de retorno de chamada para verificar o ID da sessão do Citrix Gateway. O padrão é **false**.

Número de uploads com falha consecutivos

- Exibe o número de falhas consecutivas durante uploads do Programa de aperfeiçoamento da experiência do cliente (CEIP). O XenMobile incrementa o valor quando um upload falha. Após 15 falhas de upload, o XenMobile desativa o CEIP, também conhecido como telemetria. Para obter

mais informações, consulte a propriedade de servidor **Identifica se a telemetria está ativada ou não**. O XenMobile redefine o valor como **0** quando o upload é bem-sucedido.

Número de usuários por dispositivo

- O número máximo de usuários que podem registrar o mesmo dispositivo no MDM. O valor **0** significa que um número ilimitado de usuários pode registrar o mesmo dispositivo. O padrão é **0**.

Recepção de alteração Incremental dos usuários permitidos e negados

- O número de segundos durante o qual o XenMobile espera por uma resposta do domínio ao executar um comando do PowerShell para obter um delta de dispositivos do ActiveSync. O padrão é **60** segundos.

Tempo limite de leitura para o servidor de certificação Microsoft

- O número de segundos durante o qual o XenMobile espera por uma resposta do servidor de certificado ao executar uma leitura. Caso o servidor de certificados seja lento e tenha uma grande quantidade de tráfego, você pode aumentar esse valor para 60 segundos ou mais. Um servidor de certificado que não responde após 120 segundos precisa de manutenção. Padrão é **15000** milissegundos (15 segundos).

Serviços Web REST

- Ativa o serviço Web REST. O padrão é **true**.

Recupera informações de dispositivos em blocos de tamanho especificado

- Este valor é usado internamente para multithreading durante exportações de dispositivo. Se o valor for maior, um único thread analisa mais dispositivos. Se o valor for menor, mais threads buscam os dispositivos. Reduzir o valor pode aumentar o desempenho de exportações e buscas da lista de dispositivos, mas pode reduzir a memória disponível. O padrão é **1000**.

Limpeza do log de sessões (em dias)

- O número de dias durante os quais o XenMobile deve manter o log de sessão. O padrão é **7**.

Modo de servidor

- Determina se o XenMobile é executado no modo MAM, MDM ou ENT (Enterprise), correspondente ao gerenciamento de aplicativo, gerenciamento de dispositivo ou gerenciamento de aplicativo e dispositivo. Defina a propriedade Modo de Servidor de acordo com a forma como você deseja que os dispositivos sejam registrados, conforme indicado na tabela abaixo. O padrão do Modo de Servidor é **ENT**, independentemente do tipo de licença.

Se você tiver uma licença XenMobile MDM Edition, o modo de servidor efetivo é sempre MDM, independentemente da forma como você definir o modo de servidor em Propriedades do servidor. Se você tiver uma licença do MDM Edition, não poderá ativar o gerenciamento de aplicativo definindo o modo de servidor como MAM ou ENT.

Suas licenças são desta edição	Você deseja que os dispositivos se registrem neste modo	Defina a propriedade Modo de Servidor como
Enterprise / Advanced	Modo MDM	MDM
Enterprise / Advanced	Modo MDM+MAM	ENT
MDM	Modo MDM	MDM

O modo de servidor efetivo é uma combinação do tipo de licença e do modo de servidor. Para obter uma licença de MDM, o modo de servidor efetivo é sempre MDM, independentemente da configuração do modo de servidor. Para as licenças Enterprise e Advanced, o modo de servidor efetivo corresponde ao modo de servidor, se o modo de servidor é **ENT** ou **MDM**. Se o modo de servidor é **MAM**, o modo de servidor efetivo é ENT.

O XenMobile adiciona o modo de servidor ao log do servidor para cada uma dessas atividades: uma licença é ativada ou excluída, e quando você altera o modo de servidor nas Propriedades do Servidor. Para obter informações sobre como criar e exibir arquivos de log, consulte [Logs](#) e [Exibir e analisar arquivos de log no XenMobile](#).

Tipo de configuração do Content Collaboration

- Especifica o tipo de armazenamento do Citrix Files. **ENTERPRISE** ativa o modo Citrix Files Enterprise. **CONNECTORS** fornece acesso somente para conectores de zona de armazenamento que você cria por meio do console XenMobile. O padrão é **NONE**, que mostra a exibição inicial da tela **Configurar > ShareFile** em que você escolhe entre Citrix Files Enterprise e Connectors. O padrão é **NONE**.

Tempo limite estático em minutos

- Se a propriedade **Tipo de tempo limite de WebServices** for **STATIC_TIMEOUT**: essa propriedade define o número de minutos após os quais o XenMobile faz logout de um administrador depois de usar o seguinte:
 - A API pública do XenMobile para serviços REST para acessar o console XenMobile.
 - A API pública do XenMobile para serviços REST para acessar qualquer aplicativo de terceiro.

O padrão é **60**.

Disparar supressão de mensagem de agente

- Ativa ou desativa as mensagens de cliente do Secure Hub. O valor **false** ativa as mensagens. O padrão é **true**.

Disparar supressão de som de agente

- Ativa ou desativa os sons de cliente do Secure Hub. O valor **false** ativa os sons. O padrão é **true**.

Download de aplicativo não autenticado para dispositivos Android

- Se for **true**, você poderá baixar aplicativos auto-hospedados para dispositivos Android que executam o Android Enterprise. O XenMobile precisa dessa propriedade se a opção do Android Enterprise para fornecer estaticamente uma URL de download na Google Play Store estiver ativada. Nesse caso, as URLs de download não poderão incluir um tíquete de uso único (definido pela propriedade **XAM One-Time Ticket server**) que possua o token de autenticação. O padrão é **false**.

Download de aplicativo não autenticado para dispositivos Windows

- Usada somente para as versões mais antigas do Secure Hub que não validam tíquetes de uso único. Se for **false**, você poderá baixar aplicativos não autenticados do XenMobile para dispositivos Windows. O padrão é **false**.

Usar ID do ActiveSync para realizar um exclusão de dispositivo ActiveSync

- Se for **true**, o conector Endpoint Management para Exchange ActiveSync usará o identificador do ActiveSync como argumento para o método `asWipeDevice`. O padrão é **false**.

Propriedades do dispositivo definidas pelo usuário N

- Usada somente em dispositivos Windows CE. Essa chave personalizada permite obter as propriedades que você cria no Registro de dispositivos Windows CE. Depois que essas propriedades estiverem no banco de dados do XenMobile, você poderá criar regras de implantação com base em seus valores.
- Chave: **chave personalizada**
- Chave: **device.properties.userDefinedN**
- Valor: *definido pelo administrador*
- Nome de exibição: *definido pelo administrador*
- Descrição: *definida pelo administrador*

Usuários somente do Exchange

- Se for **true**, desativará a autenticação de usuário para usuários do ActiveSync Exchange. O padrão é **false**.

Intervalo de linha de base do VP

- O intervalo mínimo em que o XenMobile reimporta licenças de compra por volume da Apple. A atualização de informações de licença garante que o XenMobile reflita todas as alterações, como quando você exclui manualmente um aplicativo importado da compra por volume. Por padrão, o XenMobile atualiza a linha de base da licença de compra por volume no mínimo a cada **720** minutos.

Se você tem muitas licenças de compra por volume instaladas (por exemplo, mais de 50.000), a Citrix recomenda que você aumente o intervalo da linha de base para reduzir a frequência e a sobrecarga de importação de licenças. Se você espera mudanças frequentes de licenças de compra por volume da Apple, a Citrix recomenda reduzir o valor para manter o XenMobile atualizado com essas mudanças. O intervalo mínimo entre duas linhas de base é de 60 minutos. Além disso, o XenMobile realiza uma importação delta a cada 60 minutos para capturar as alterações desde a última importação. Portanto, se o intervalo de linha de base da compra por volume for de 60 minutos, o intervalo entre linhas de base poderá ser atrasado até 119 minutos.

Tipo de tempo limite do WebServices

- Especifica a expiração de um token de autenticação obtido na API pública. Se **STATIC_TIMEOUT**, o XenMobile considerará um token de autenticação como expirado após o valor especificado na propriedade de servidor **Static Timeout in Minutes**.

Se **INACTIVITY_TIMEOUT**, o XenMobile considerará um token de autenticação como expirado após o valor especificado na propriedade de servidor **InactivityTimeout in Minutes**. O padrão é **STATIC_TIMEOUT**.

Validade estendida (5 anos) de certificado do Windows Phone MDM Windows Phone certificado do MDM

- O período de validade do certificado do dispositivo emitido por MDM para Windows Phone e Tablet. Os dispositivos usam um certificado de dispositivo para se autenticar no servidor MDM durante o gerenciamento de dispositivo. Se o valor for **true**, o período de validade será de cinco anos. Se o valor for **false**, o período de validade será de dois anos. O padrão é **true**.

Canal Windows WNS - Número de dias antes da renovação

- A frequência de renovação para ChannelURI. O padrão é **10** dias.

Intervalo de pulsação do Windows WNS

- O tempo de espera do XenMobile antes de se conectar a um dispositivo, depois de se conectar a ele a cada três minutos cinco vezes. O padrão é **6** horas.

Tíquete de uso único XAM

- O número de milissegundos durante os quais um token de autenticação de uso único (OTT) é válido para baixar um aplicativo. Essa propriedade funciona com as propriedades **Unauthenticated App download for Android** e **Unauthenticated App download for Windows**. Essas propriedades especificam se devem ser permitidos downloads de aplicativos não autenticados. O padrão é **3600000**.

Intervalo inativo máximo de console do portal de autoajuda XenMobile MDM (minutos)

- O número de minutos após os quais o XenMobile faz logoff de um usuário inativo do portal de autoajuda XenMobile. Um tempo limite de **0** significa que um usuário inativo permanece conectado. O padrão é **30**.

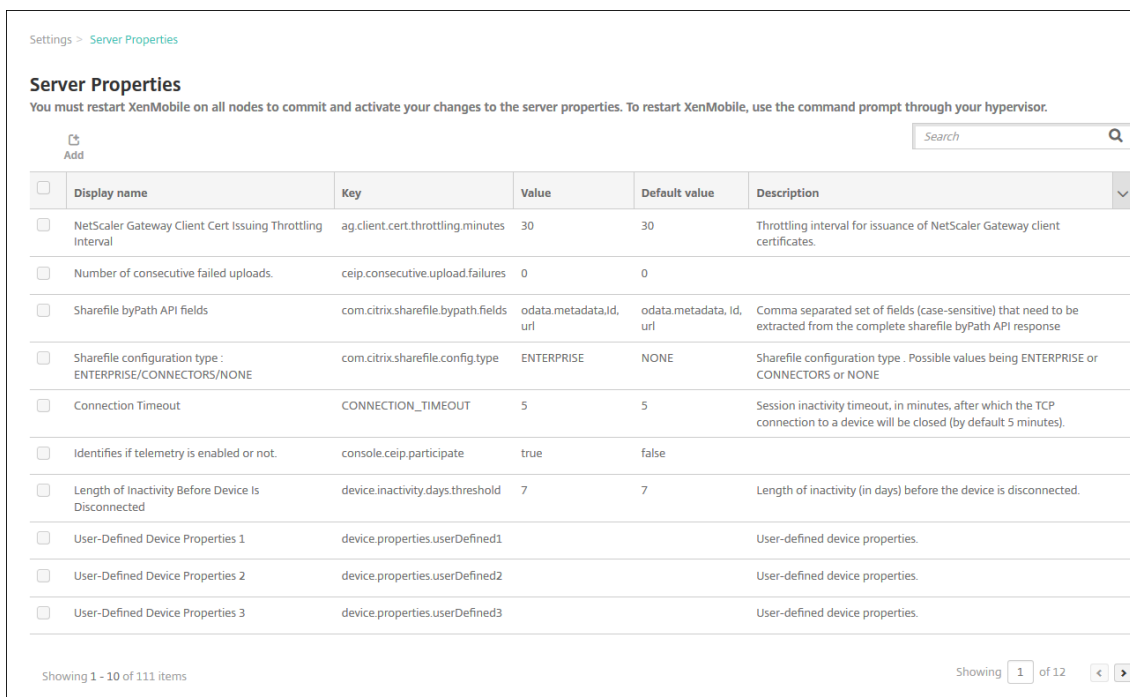
Adição, edição ou exclusão de propriedades do servidor

No XenMobile, você pode aplicar propriedades ao servidor. Depois de fazer alterações, você deverá reiniciar o XenMobile em todos os nós para confirmar e ativar as alterações.

Nota:

Para reiniciar o XenMobile, use o prompt de comando por meio do seu hipervisor.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida.
2. Em **Servidor**, clique em **Propriedades do servidor**. A página **Propriedades do servidor** é exibida. Você pode adicionar, editar ou excluir propriedades do servidor nessa página.



Para adicionar uma propriedade de servidor

1. Clique em **Adicionar**. A página **Adicionar Nova Propriedade de Servidor** é exibida.

Settings > Server Properties > Add New Server Property

Add New Server Property

Key ?

Value*

Display name*

Description

2. Defina estas configurações:

- Chave: na lista, selecione a chave adequada. As chaves diferenciam maiúsculas de minúsculas. Entre em contato com o suporte da Citrix antes de editar os valores de propriedade ou para solicitar uma chave especial.
- Valor: insira um valor de acordo com a chave selecionada.
- Nome para exibição: insira um nome para o valor da nova propriedade que é exibido na tabela **Propriedades do servidor**.
- Descrição: opcionalmente, digite uma descrição para a nova propriedade de servidor.

3. Clique em **Salvar**.

Para editar uma propriedade de servidor

1. Na tabela **Propriedades do servidor**, selecione a propriedade de servidor que você deseja editar.

Quando você marca a caixa de seleção ao lado de uma propriedade de servidor, o menu de opções é exibido acima da lista de propriedades do servidor. Clique em qualquer outro lugar na lista para abrir o menu de opções no lado direito da listagem.

2. Clique em **Edit**. A página **Editar nova propriedade de servidor** é exibida.

Settings > Server Properties > Edit New Server Property

Edit New Server Property

Key ag.client.cert.throttling.mi

Value* 30

Display name* NetScaler Gateway Client

Description Throttling interval for issuance of NetScaler Gateway client certificates.

3. Altere as seguintes informações conforme apropriado:
 - Chave: você não pode alterar esse campo.
 - Valor: o valor da propriedade.
 - Nome de exibição: o nome da propriedade.
 - Descrição: a descrição da propriedade.
4. Clique em **Salvar** para salvar suas alterações ou em **Cancelar** para deixar a propriedade inalterada.

Para excluir uma propriedade de servidor

1. Na tabela **Propriedades do servidor**, selecione a propriedade de servidor que você deseja excluir.

Você pode selecionar mais de uma propriedade para excluir marcando a caixa de seleção ao lado de cada propriedade.
2. Clique em **Excluir**. Uma caixa de diálogo de confirmação é exibida. Clique em **Excluir** novamente.

Opções da interface de linha de comando

November 30, 2020

Para uma instalação no local do XenMobile Server, você pode acessar as opções de CLI da seguinte maneira:

- **No hipervisor em que você instalou o XenMobile:** No seu hipervisor, selecione a máquina virtual XenMobile importada, inicie a exibição do prompt de comando e faça login na sua conta de administrador para o XenMobile. Para obter detalhes, consulte a documentação do hipervisor.
- **Se o SSH estiver habilitado no seu firewall, usando SSH:** Faça login na sua conta de administrador para o XenMobile.

Você pode executar uma variedade de tarefas de configuração e resolução de problemas por meio do CLI. A figura a seguir mostra o menu de nível superior da CLI .

```
Main Menu
-----
[0] Configuration
[1] Clustering
[2] System
[3] Troubleshooting
[4] Help
[5] Log Out
-----
```

Opções de configuração

Veja a seguir exemplos do **Menu Configuration** e as configurações exibidas para cada opção.

```
Configuration Menu
-----
[0] Back to Main Menu
[1] Network
[2] Firewall
[3] Database
[4] Listener Ports
-----
```


[1] Network

```
Reboot is required to save the changes.
Do you want to proceed? (y/n) [y]: y
IP address [10.207.87.75]: 10.200.87.75
Netmask [255.255.254.0]: 255.255.254.0
Default gateway [10.207.86.1]: 10.200.86.1
Primary DNS server [10.207.86.50]: 10.200.86.50
Secondary DNS server (optional) []:

Applying network settings...

Are you sure to restart the system? [y/n]: █
```

[2] Firewall

```
Configure which services are enabled through the firewall.

Can optionally configure allow access white lists:
- comma separated list of hosts or networks
- e.g. 10.20.5.3, 10.20.6.0/24
- an empty value means no access restriction
- enter c as value to clear list

HTTP service
Port: 80
Enable access (y/n) [y]: y
Access white list []:

Management HTTPS service
Port: 4443
Enable access (y/n) [y]:
Access white list []:

SSH service
Port [22]:
Enable access (y/n) [y]:
Access white list []:

Management API (for initial staging) HTTPS service
Port [30001]:
Enable access (y/n) [n]:

Remote support tunnel
Port [8081]:
Enable access (y/n) [n]:

Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...
```

[3] Database

```
Type: [mi]
Use SSL (y/n) [n]:
Server [10.207.86.64]:
Port [1433]:
Username [sa]:
Password:
Database name [RC]:

Reboot is required to save the changes.
Do you want to proceed? (y/n) [y]: █
```

[4] Listener Ports

```
Reboot is required to save the changes.
Do you want to proceed? (y/n) [y]: y
HTTP [80]:
HTTPS with certificate authentication [443]:
HTTPS with no certificate authentication [8443]:
HTTPS for management [4443]:
Applying port listener configuration...
Applying firewall settings ...
Writing iptables configuration...
Restarting iptables...
Are you sure to restart the system? [y/n]: █
```

Opções de clustering

Veja a seguir exemplos do **Menu Clustering** e as configurações exibidas para cada opção.

```
-----
Clustering Menu
-----
[0] Back to Main Menu
[1] Show Cluster Status
[2] Enable/Disable cluster
[3] Cluster member white list
[4] Enable or Disable SSL offload
[5] Display Hazelcast Cluster
-----
```

[1] Show Cluster Status

```
Current Node ID: 181360459

Cluster Members:
node: 10.207.87.75 status: ACTIVE role: OLDEST
node: 10.207.87.77 status: ACTIVE role: NONE
node: 10.207.87.88 status: ACTIVE role: NONE
```

[2] Enable/Disable cluster

Quando você opta por ativar clusters, a seguinte mensagem é exibida:

```
To enable real-time communication between cluster members, please open port 80 using the Firewall menu option in CLI menu. Also configure Access white list under Firewall settings for restricted access.
```

Quando você opta por desativar clusters, a seguinte mensagem é exibida:

```
You have chosen to disable clustering. Access to port 80 is not needed. Please disable it.
```

[3] Cluster member white list

```
Current White List:
- comma separated list of hosts or networks
- e.g. 10.20.5.3, 10.20.6.0/24
- an empty value means no access restriction

Please enter hosts or networks to be white listed:
```

[4] Enable or disable SSL offload

Quando você seleciona ativar ou desativar a descarga de SSL, a seguinte mensagem é exibida:

```
Enabling SSL offload opens port 80 for everyone. Please configure Access white list under Firewall settings for restricted access.
```

[5] Display Hazelcast Cluster

Quando você seleciona exibir o Hazelcast Cluster, as seguintes opções são exibidas:

Membros do cluster Hazelcast:

[[Endereços IP listados]]

Nota:

Se um nó configurado não fizer parte do cluster, reinicie o nó.

Opções do sistema

No **Menu System**, você pode exibir ou definir informações no nível do sistema, reiniciar ou desligar o servidor, ou acessar o menu **Advanced Settings**.

```
-----  
System Menu  
-----  
[0] Back to Main Menu  
[1] Display System Date  
[2] Set Time Zone  
[3] Set NTP Server  
[4] Display NTP Status  
[5] Display System Disk Usage  
[6] Update Hosts File  
[7] Display Device Management Instance Name  
[8] Proxy Server  
[9] Admin (CLI) Password  
[10] Restart Server  
[11] Shutdown Server  
[12] Advanced Settings  
-----
```

Set NTP Server permite que você especifique as informações do servidor NTP. Se você tiver problemas de fuso horário ao sincronizar o horário do XenMobile com um hipervisor, você pode evitar esses problemas apontando o XenMobile para um servidor NTP. Reinicie todos os servidores de cluster após alterar essa opção.

Você também pode verificar o espaço em disco exibindo o item de menu **[5]Display System Disk Usage**.

Sobre o encerramento de nós de servidor

Quando você encerra um único nó de servidor em um cluster, outros nós geralmente podem lidar com a carga de trabalho se atenderem aos requisitos documentados em [Escalabilidade e desempenho](#). O impacto pode variar dependendo de quantos nós estão inativos ao mesmo tempo, do número total de usuários e de quanto tempo os nós estão inativos.

- Os usuários ainda podem acessar o Secure Hub e a loja.
- Os usuários ainda podem acessar e iniciar aplicativos gerenciados implantados, se um nó disponível puder lidar com o número de usuários. As conexões podem ser mais lentas, resultando em check-ins de dispositivos mais lentos.
- As políticas de dispositivo continuam a funcionar, a menos que todos os nós estejam inativos. Dependendo dos recursos e do número de dispositivos, as políticas podem ser implantadas mais lentamente.

[12] Advanced Settings

```
-----  
Advanced Settings  
-----  
[0] Back to System Menu  
[1] Toggle FIPS mode  
[2] Custom Ciphers  
[3] SSL protocols  
[4] Reset CA Certs Password  
[5] Reset SSL Certificate  
[6] Reset pki.xml  
[7] Server Tuning  
[8] Switch JDBC driver  
[9] Cloud Migration Credential Check  
[10] Refresh encryption keys  
-----  
Choice: [0 - 10] █
```

As opções de **Protocolos SSL** definem como padrão todos os protocolos permitidos. Após o aviso de ativação **New SSL protocols to enable**, digite os protocolos que deseja ativar. O XenMobile desativará todos os protocolos que você não incluir na sua resposta. Por exemplo: para desativar TLSv1, digite `TLSv1.2`, `TLSv1.1` e digite **y** para reiniciar o XenMobile Server.

As opções de **Server Tuning** incluem o tempo limite de conexão do servidor, o máximo de conexões (pela porta) e o máximo de threads (pela porta).

As opções de **Switch JDBC driver** são JDBC **jTDS** e **Microsoft**. O driver padrão é jTDS. Para obter informações sobre como alternar para o driver Microsoft JDBC, consulte [Drivers do SQL Server](#).

Opções de solução de problemas

Veja a seguir é exemplos do **Menu Troubleshooting** e as configurações exibidas para cada opção.

```
-----  
Troubleshooting Menu  
-----
```

- [0] Back to Main Menu
- [1] Network Utilities
- [2] Logs
- [3] Support Bundle
- [4] Disk Usage

```
-----  
Choice: [0 - 4] 4
```

[1] Network Utilities

```
-----  
Network Menu  
-----
```

- [0] Back to Troubleshooting Menu
- [1] Network Information
- [2] Show Routing Table
- [3] Show Address Resolution Protocol (ARP) Table
- [4] PING
- [5] Traceroute
- [6] DNS Lookup
- [7] Network Trace

[2] Logs

```
-----  
Logs Menu  
-----
```

- [0] Back to Troubleshooting Menu
- [1] Display Log File

[3] Support Bundle

```
-----  
Support Bundle Menu  
-----
```

- [0] Back to Troubleshooting Menu
- [1] Generate Support Bundle
- [2] Upload Support Bundle by Using SCP
- [3] Upload Support Bundle by Using FTP

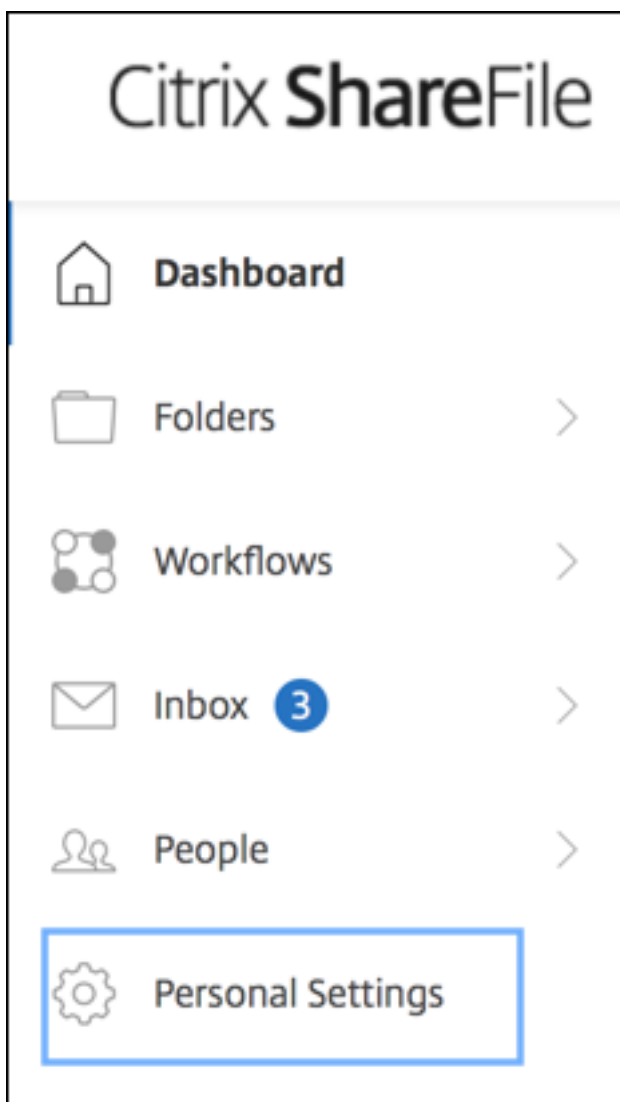
[4] Disk Usage

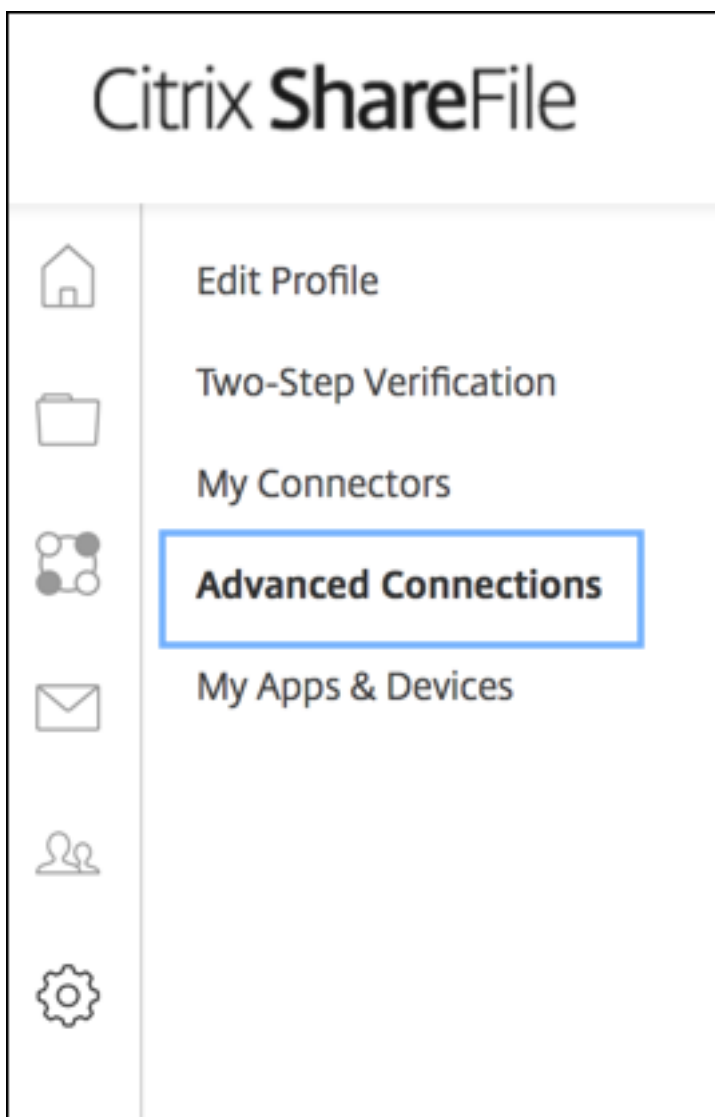
```
-----  
Troubleshooting Menu  
-----  
[0] Back to Main Menu  
[1] Network Utilities  
[2] Logs  
[3] Support Bundle  
[4] Disk Usage  
-----  
Choice: [0 - 4] 4
```

Para carregar um pacote de suporte usando o Citrix Files como o site FTP

Antes de iniciar o carregamento de um pacote de suporte, configure os pré-requisitos a seguir no Citrix Files:

1. Verifique os detalhes do login do FTP.
 - a. Em um navegador da Web, abra <https://citrix.sharefile.com>.
 - b. Clique em **Configurações pessoais** e depois clique em **Conexões avançadas**.





- c. Nas informações do servidor FTP, em Nome do usuário, verifique se um ID de usuário alfanumérico é exibido, juntamente com os detalhes de subdomínio/nome de usuário padrão.

You can connect to your account using an FTP client such as WS-FTP or FileZilla. To connect using an FTP client, use the settings below.

Your FTP user name includes your account's subdomain to the left of your e-mail address. If you are unable to log in, or your FTP client does not allow you to enter the / and @ characters as part of your user name, you can use the shorter, alternate form to the right of your full user name.

[Detailed Set-up Instructions](#)

FTP Server Information

Security: Standard (Port 21) or Implicit SSL/TLS (Port 990)

FTP Server: citrite.sharefileftp.com

User name: [redacted].com or [redacted]

Password: (your ShareFile password)

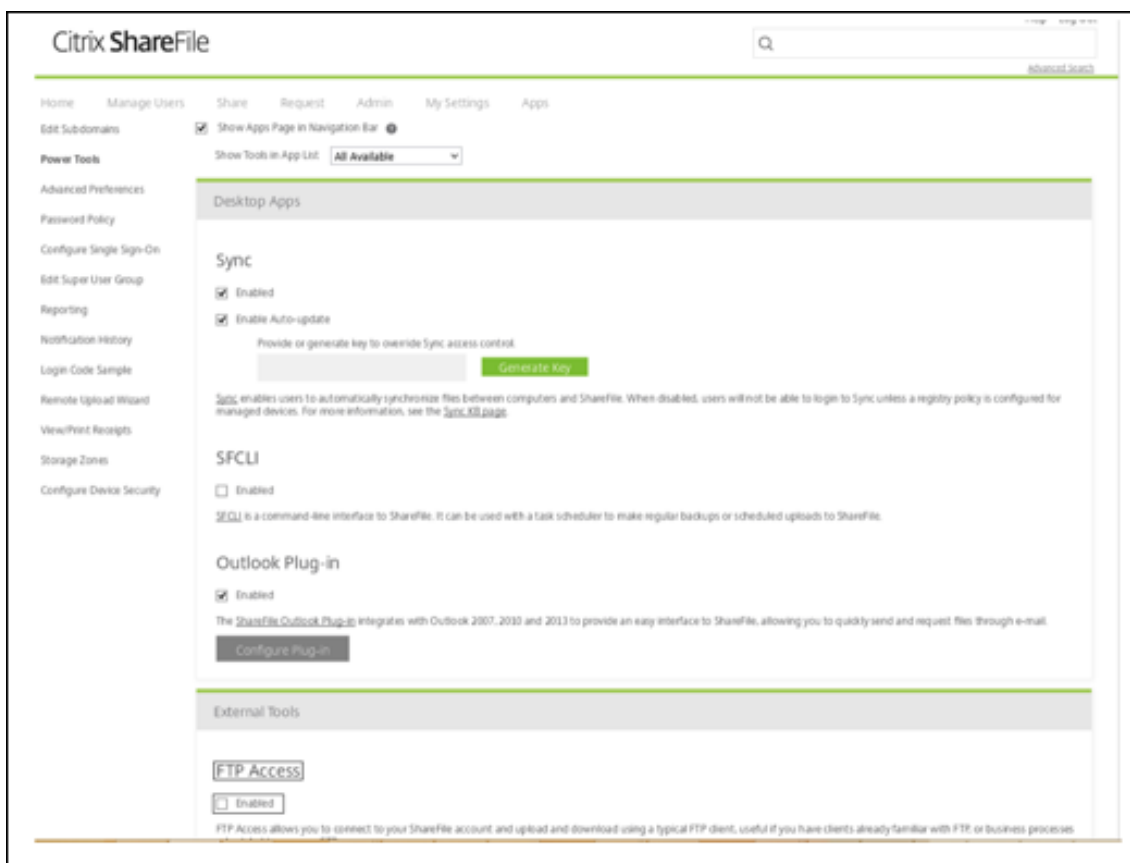
Both secure and standard FTP are enabled for your account.

Notas:

- O arquivo que você está carregando do XenMobile é um cliente FTP baseado em Linux CLI. Como resultado, você não pode usar barra invertida () e arroba (@) como parte do seu nome de usuário.
- Se você não vir o ID de usuário alfanumérico, poderá solicitar esse ID de usuário ao administrador do Content Collaboration ou ao suporte do Content Collaboration.

2. Verifique se o servidor Citrix Files está habilitado para comunicação por FTP juntamente com FTPS. Idealmente, os administradores do Content Collaboration permitem que uma conta de usuário seja aberta para comunicação por FTP. Às vezes, no entanto, apenas a comunicação por FTPS é permitida.

Um usuário com direitos de administrador pode verificar e ativar essa configuração clicando em **Configurações, Configurações de administrador, Preferências avançadas** e, depois, em **Ativar ferramentas do ShareFile**. Em **Aplicativos externos, Acesso por FTP**, verifique se a caixa de seleção **Ativar** está selecionada.



3. Crie uma pasta compartilhada para o cliente FTP usar como um diretório para o carregamento de arquivos. Clique em **Página inicial, Pastas** e depois clique em **Pastas pessoais**.
4. No canto direito, clique no ícone de sinal de adição (+), clique em **Criar pasta** e insira um nome para a pasta.

Create Folder [X]

* Required

Name: *

Description:

Add Users: Add People to Folder

Storage Zone: [v] [?]

5. Na CLI do XenMobile Server, no **Menu principal**, selecione **Solução de problemas > Pacote de suporte**. Em **Support Bundle Menu**, selecione **Generate Support Bundle**.



Nota:

Se existir um pacote de suporte, quando solicitado, digite **y** para substituir o pacote.

6. Carregue o pacote de suporte para o servidor FTP:
 - a. Selecione **Upload Support Bundle by using FTP**.
 - b. **Digitar o nome de host:** Quando solicitado, digite o nome do seu servidor FTP. Quando o Citrix Files for usado como servidor FTP, digite o nome da empresa seguido pelo nome do site FTP do Citrix Files. Por exemplo, citrix.sharefileftp.com.

- c. **Digitar o nome do usuário remoto:** Quando solicitado, digite o ID do usuário alfanumérico.
- d. **Digitar a senha do usuário remoto:** Quando solicitado, digite a sua senha.
- e. **Digitar o diretório remoto:** Quando solicitado, insira o nome da pasta compartilhada que você criou no Citrix Files e pressione **Enter**.

```
-----
Support Bundle Menu
-----
[0] Back to Troubleshooting Menu
[1] Generate Support Bundle
[2] Upload Support Bundle by Using SCP
[3] Upload Support Bundle by Using FTP
-----
Choice: [0 - 3] 3

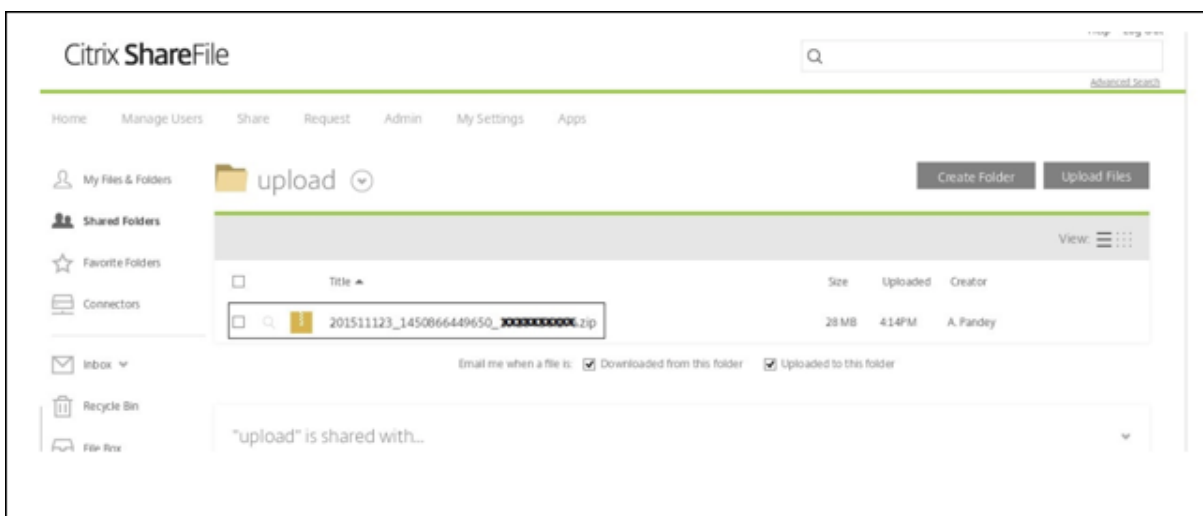
Current support bundle: 201511123_1450866449650_      zip

Enter remote host:      .sharefileftp.com
Enter remote user name:
Enter remote user password:
Enter remote directory
(Note: Do not use ftp://, http:// or host name. Path should be relative to ftp root location.):/upload

-----

Connected to ec      eu-west-1.compute.      .com.
Remote system type is UNIX.
230-Connection established from (unknown) [      ]
230-You are connected as (      ) (      Citrix
.com).
230 Welcome to the      Test Account FTP site.
250 "/upload" is the current directory.
125 Data connection open; transfer starting.
226-Received 29050517 bytes.
226 Transfer Complete.
29050517 bytes sent in 16.3 seconds (1779137 bytes/s)
221-Sent: 550 bytes  Rcvd: 29,050,639 bytes  Billable: 1 operations  Time: 27
s
```

Você pode visualizar o pacote de suporte carregado na pasta compartilhada que você criou no Citrix Files.



Para obter mais informações sobre o Citrix Files FTP, consulte este [artigo do Citrix Support Knowledge Center](#).

Para verificar o espaço em disco

Você pode verificar o espaço em disco do sistema na CLI da seguinte forma:

1. No menu principal, selecione o menu **System**.
2. No menu **System**, selecione a opção **Display System Disk Usage**.

As informações do sistema de arquivos são exibidas.

```
-----
System Menu
-----
[0] Back to Main Menu
[1] Display System Date
[2] Set Time Zone
[3] Set NTP Server
[4] Display NTP Status
[5] Display System Disk Usage
[6] Update Hosts File
[7] Display Device Management Instance Name
[8] Proxy Server
[9] Admin (CLI) Password
[10] Restart Server
[11] Shutdown Server
[12] Advanced Settings
-----
Choice: [0 - 12] 5

filesystem 1K-blocks  Used Available Use% Mounted on
dev/      49431012 3786556  43133500  9% /
mpfs      8191176   156    8191020  1% /run
levtmpfs  8190888   0     8190888  0% /dev
dev/      101086    10094   85773   11% /boot
```

Para executar a limpeza de disco self-service

Você pode limpar o disco na CLI da seguinte maneira:

1. No **Troubleshooting Menu**, selecione **Disk Usage**. O **Disk Usage Menu** tem as seguintes opções:

```
-----  
Disk Usage Menu (Core dump and Support Bundle)  
-----  
[0] Back to Troubleshooting Menu  
[1] Display Disk Usage  
[2] Clean  
-----  
[Choice: [0 - 2] 1  
  
No core dump and support bundle found.
```

2. Digite 1 para listar o arquivo de despejo core e os tipos de arquivos de pacotes de suporte. Se não houver arquivos, você receberá a seguinte mensagem: **No core dump and support bundles found**.
3. Digite 2 para limpar a varredura do arquivo de despejo core e do arquivo de pacote de suporte.

Introdução aos fluxos de trabalho para o console XenMobile

August 20, 2021

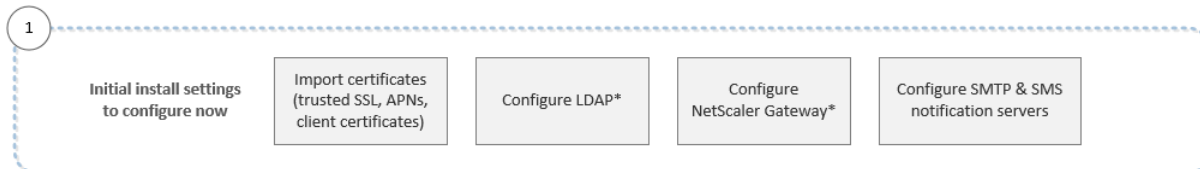
O console XenMobile é a ferramenta de gerenciamento unificado no XenMobile. Este artigo baseia-se no pressuposto de que você tenha instalado o XenMobile e esteja pronto para trabalhar no console. Se ainda for necessário instalar o XenMobile, consulte [Instalação do XenMobile](#). Para obter mais detalhes sobre o suporte de navegador ao console XenMobile, consulte o artigo [Compatibilidade do XenMobile](#).

Fluxo de trabalho das configurações iniciais

Depois que você terminar de configurar o XenMobile primeiro no console da linha de comando e, em seguida, no console XenMobile, o painel será aberto. Você não pode retornar para as telas de configuração inicial. Se você tiver deixado de lado algumas configurações de instalação, poderá configurar as seguintes configurações no console. Antes de iniciar a adição de usuários, aplicativos e dispositivos, conclua estas configurações de instalação. Para iniciar, clique no ícone de engrenagem no canto superior direito do console.

Nota:

Os itens com um asterisco são opcionais.



Para obter mais informações sobre cada configuração, juntamente com procedimentos passo a passo, consulte os seguintes artigos e seções da Documentação de Produtos Citrix:

- [Authentication](#)
- [Citrix Gateway e XenMobile](#)
- [Notificações](#)

Para dar suporte a plataformas Windows, iOS e Android, você deve ter a seguinte configuração de conta.

Android

- Crie credenciais do Google Play. Para obter detalhes, consulte [Launch](#) do Google Play.
- Crie uma conta de administrador do Android Enterprise. Para obter detalhes, consulte [Android Enterprise](#).
- Verifique o seu nome de domínio junto ao Google. Para obter detalhes, consulte [Verify your domain for Google Workspace](#).
- Ative APIs e crie uma conta de serviço para o Android Enterprise. Para obter detalhes, consulte [Android for Work Help](#).

iOS

- Crie um ID Apple e uma conta de desenvolvedor. Para obter detalhes, consulte o site [Apple Developer Program](#).
- Crie um certificado Apple Push Notification Service (APNs). Se você planeja gerenciar dispositivos iOS com a sua implantação do XenMobile Server, precisará de um certificado Apple APNs. Se usar notificações por push para a implantação do Secure Mail, você também precisa de um certificado APNs da Apple. Para obter detalhes sobre como obter certificados de APNs da Apple, consulte o [Apple Push Certificates Portal](#). Para obter mais informações sobre o XenMobile e APNs, consulte [Certificados APNs](#) e [Notificações por push para o Secure Mail para iOS](#).
- Crie um token de empresa de compra por volume. Para obter detalhes, consulte o [Apple Volume Purchase Program](#).

Windows

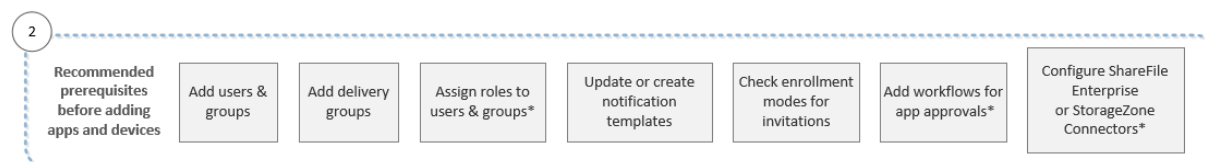
- Crie uma conta de desenvolvedor da Microsoft Windows Store. Para obter detalhes, consulte [Tipos de conta, localizações e taxas](#).
- Obtenha um ID de Publicador da Microsoft Windows Store. Para obter detalhes, consulte [Manage account settings and profile info](#).
- Adquira um certificado empresarial da DigiCert. Para obter detalhes, consulte [Company app distribution for Windows Phone](#).
- Você deverá ter um certificado SSL público disponível se planeja usar a descoberta automática do XenMobile para o registro do Windows Phone. Para obter mais informações, consulte o [XenMobile AutoDiscovery Service](#).
- Crie um Application Enrollment Token (AET). Para obter detalhes, consulte [How to generate an application enrollment token for Windows Phone](#).

Fluxo de trabalho dos pré-requisitos do console

Este fluxo de trabalho mostra os pré-requisitos que você deve configurar antes de adicionar aplicativos e dispositivos.

Nota:

Os itens com um asterisco são opcionais.



Para obter mais informações sobre cada configuração, juntamente com procedimentos passo a passo, consulte os seguintes artigos e seções da Documentação de Produtos Citrix:

- [Contas de usuário, funções e registro](#)
- [Implantar recursos](#)
- [Configurar funções com RBAC](#)
- [Notificações](#)
- [Aplicar fluxos de trabalho](#)
- [Usar Citrix Content Collaboration com XenMobile](#)

Adicionar fluxo de trabalho de aplicativos

Este fluxo de trabalho mostra uma ordem recomendada a ser seguida quando você adiciona aplicativos ao XenMobile.

Nota:

Os itens com um asterisco são opcionais.



Para obter mais informações sobre cada configuração, juntamente com procedimentos passo a passo, consulte os seguintes artigos e seções da Documentação de Produtos Citrix:

- [Sobre o MDX Toolkit](#)
- [Adicionar aplicativos](#)
- [Resumo das políticas do MDX](#)
- [Aplicar fluxos de trabalho](#)
- [Implantar recursos](#)

Adicionar fluxo de trabalho de dispositivos

Este fluxo de trabalho mostra uma ordem recomendada a ser seguida durante a adição e o registro de dispositivos no XenMobile.

Nota:

Os itens com um asterisco são opcionais.

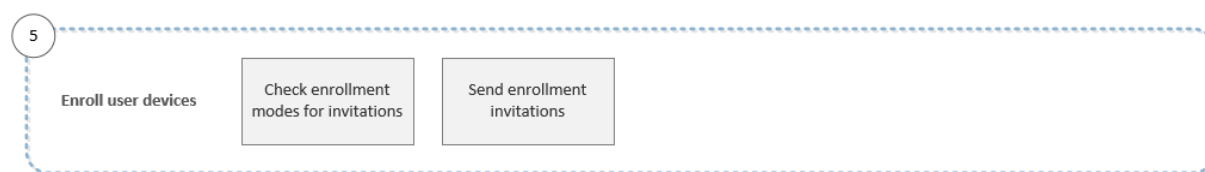


Para obter mais informações sobre cada configuração, juntamente com procedimentos passo a passo, consulte os seguintes artigos e seções da Documentação de Produtos Citrix:

- [Dispositivos](#)
- [Sistemas operacionais compatíveis de dispositivos](#)
- [Implantar recursos](#)
- [Monitoração e suporte](#)
- [Ações automatizadas](#)

Registrar o fluxo de trabalho de dispositivos do usuário

Este fluxo de trabalho mostra uma ordem recomendada de registro de dispositivos de usuário no XenMobile.



Para obter mais informações sobre cada configuração, juntamente com procedimentos passo a passo, consulte os seguintes artigos da Documentação de Produtos Citrix:

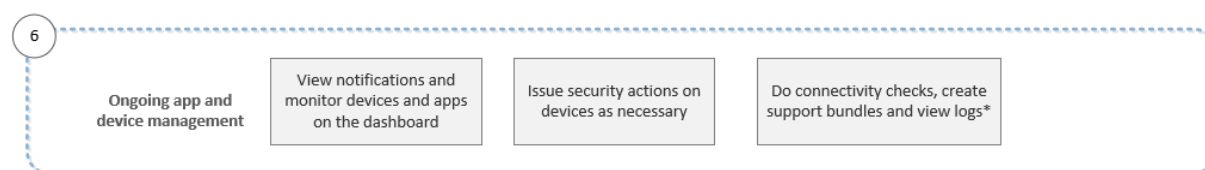
- [Contas de usuário, funções e registro](#)
- [Notificações](#)

Fluxo de trabalho contínuo de gerenciamento de aplicativos e dispositivos

Este fluxo de trabalho mostra atividades de gerenciamento de aplicativo e dispositivo que você pode realizar no console.

Nota:

Os itens com um asterisco são opcionais.



Para obter mais informações sobre as opções de suporte encontradas ao clicar no ícone de chave inglesa no canto superior direito do console, consulte [Monitoramento e suporte](#).

Certificados e autenticação

March 5, 2021

Componentes têm uma função na autenticação durante operações do XenMobile:

- **XenMobile Server:** o XenMobile Server é o local em que você define a segurança do registro e a experiência do registro. Opções para a integração de usuários incluem:
 - Tornar o registro aberto para todos ou apenas por convite.
 - Exigir autenticação de dois fatores ou autenticação de três fatores. Através das propriedades do cliente no XenMobile, você pode ativar Autenticação do PIN da Citrix e configurar a complexidade e o período de vencimento do PIN.
- **Citrix ADC:** o Citrix ADC fornece terminação para sessões SSL micro VPN. O Citrix ADC também oferece segurança em trânsito de rede e permite que você defina a experiência de autenticação usada cada vez que um usuário acessa um aplicativo.

- **Secure Hub:** o Secure Hub e o XenMobile Server trabalham em conjunto nas operações de registro. O Secure Hub é a entidade em um dispositivo que se comunica com o Citrix ADC: quando uma sessão expira, o Secure Hub obtém um tíquete de autenticação do Citrix ADC e passa o tíquete para os aplicativos MDX. A Citrix recomenda o certificate pinning, o que impede ataques de intermediários. Para obter mais informações, consulte esta seção no artigo do Secure Hub: [Fixação de certificado](#).

O Secure Hub também facilita o contêiner de segurança MDX contêiner: o Secure Hub envia as políticas, cria uma sessão com o Citrix ADC quando um aplicativo atinge o tempo limite e define o tempo limite de autenticação do MDX e a experiência de autenticação. O Secure Hub também é responsável por detecção de jailbreak, verificações de localização geográfica e as políticas que você aplicar.

- **Políticas de MDX:** as políticas de MDX criam o cofre de dados no dispositivo. As políticas de MDX conexões direcionam conexões de micro VPN de volta para o Citrix ADC, impõem restrições de modo offline como tempos limite.

Para obter mais informações sobre a configuração de autenticação, incluindo uma visão geral dos métodos de autenticação de fator único e dois fatores, consulte o artigo sobre [Autenticação](#) do manual de implantação.

Você pode usar certificados no XenMobile para criar conexões seguras e autenticar usuários. O restante deste artigo aborda certificados. Para obter outros detalhes de configuração, consulte os seguintes artigos:

- [Configure autenticação de domínio ou de domínio de segurança](#)
- [Autenticação de certificado cliente ou certificado e domínio](#)
- [Entidades PKI](#)
- [Provedores de credenciais](#)
- [Certificados APNs](#)
- [SAML para logon único com Citrix Files](#)
- [Configurações do servidor do Active Directory do Microsoft Azure](#)
- Para enviar um certificado a dispositivos para autenticar no servidor Wi-Fi: [Política de dispositivo Wi-Fi](#)
- Para enviar um certificado exclusivo não usado para autenticação, como um certificado de autoridade de certificação (CA) raiz interna ou uma política específica: [Política de dispositivo de credenciais](#)

Certificados

O XenMobile gera um certificado de Protocolo SSL durante a instalação para proteger os fluxos de comunicação com o servidor. Você deverá substituir o certificado SSL por um certificado SSL confiável de uma CA conhecida.

O XenMobile também usa o seu próprio serviço de Infraestrutura de Chave Pública (PKI) ou obtém certificados da CA dos certificados cliente. Todos os produtos Citrix são compatíveis com certificados curinga e Nome Alternativo da Entidade (SAN). Para a maioria das implementações, você precisa somente de dois certificados curinga ou SAN.

A autenticação de certificado cliente fornece uma camada extra de segurança para os aplicativos móveis e permite aos usuários acessar facilmente aplicativos HDX. Quando a autenticação de certificado de cliente está configurada, os usuários digitam o PIN da Citrix para acesso com logon único (SSO) a aplicativos compatíveis com o XenMobile. O PIN da Citrix também simplifica o processo de autenticação do usuário. O PIN da Citrix é usado para proteger um certificado de cliente ou salvar credenciais do Active Directory localmente no dispositivo.

Para registrar e gerenciar dispositivos iOS com o XenMobile, configure e crie um certificado de serviço de Notificação por Push da Apple (APNs) da Apple. Para ver as etapas, consulte [Certificados APNs](#).

A seguinte tabela mostra o formato e o tipo de certificado para cada componente do XenMobile:

Componente do XenMobile	Formato do certificado	Tipo de certificado exigido
Citrix Gateway	PEM (BASE64), PFX (PKCS #12)	SSL, Root (o Citrix Gateway converte PFX em PEM automaticamente)
Servidor XenMobile	.p12 (.pfx em computadores baseados no Windows)	SSL, SAML, APNs (o XenMobile também gera uma PKI completa durante o processo de instalação). Importante: o XenMobile Server não suporta certificados com a extensão .pem. Para usar um certificado .pem, divida o arquivo .pem em um certificado e uma chave e importe cada um deles para o XenMobile Server.
StoreFront	PFX (PKCS #12)	SSL, Raiz

O XenMobile dá suporte a certificados de ouvinte SSL e certificados de cliente com comprimentos de 4096, 2048 e 1024 bits. Os certificados de 1024 bits ficam facilmente comprometidos.

Para o Citrix Gateway e o XenMobile Server, a Citrix recomenda a obtenção de certificados de servidor de uma AC pública, como Verisign, DigiCert ou Thawte. Você pode criar uma Solicitação de Assinatura

de Certificado (CSR) do Citrix Gateway ou do utilitário de configuração do XenMobile. Depois de criar a CSR, você a envia para a AC assinar. Quando a AC retorna o certificado assinado, você pode instalá-lo no Citrix Gateway ou no XenMobile.

Importante: Requisitos para certificados confiáveis no iOS, iPadOS e macOS

A Apple tem novos requisitos para certificados de servidor TLS. Verifique se todos os certificados seguem os novos requisitos da Apple. Consulte a publicação da Apple, <https://support.apple.com/en-us/HT210176>.

A Apple está reduzindo a duração máxima permitida dos certificados de servidor TLS. Essa alteração afeta somente certificados de servidor emitidos após setembro de 2020. Consulte a publicação da Apple, <https://support.apple.com/en-us/HT211025>.

Carregando certificados no XenMobile

Cada certificado que você carrega tem uma entrada na tabela de Certificados, incluindo um resumo do seu conteúdo. Quando você configura os componentes de integração PKI que exigem um certificado, escolha um certificado de servidor que satisfaça os critérios dependentes de contexto. Por exemplo, você pode querer configurar o XenMobile para integrá-lo à sua Autoridade de Certificação (CA) da Microsoft. A conexão com a CA da Microsoft deve ser autenticada usando um certificado cliente.

Esta seção fornece procedimentos gerais para carregar certificados. Para obter detalhes sobre como criar, carregar e configurar certificados cliente, consulte [Autenticação de certificado cliente ou certificado e domínio](#).

Requisitos de chave privada

O XenMobile pode ou não possuir a chave privada de um determinado certificado. Da mesma forma, o XenMobile pode ou não exigir uma chave privada para os certificados carregados.

Carregando certificados

Você tem duas opções para carregar certificados:

- Carregar os certificados para o console individualmente.
- Executar um carregamento em massa de certificados para dispositivos iOS com a API REST.

Ao carregar certificados para o console, você tem duas opções principais:

- Clicar para importar um keystore. Em seguida, você deve identificar a entrada no repositório keystore que deseja instalar, a menos que você esteja carregando um formato PKCS #12.
- Clicar para importar um certificado.

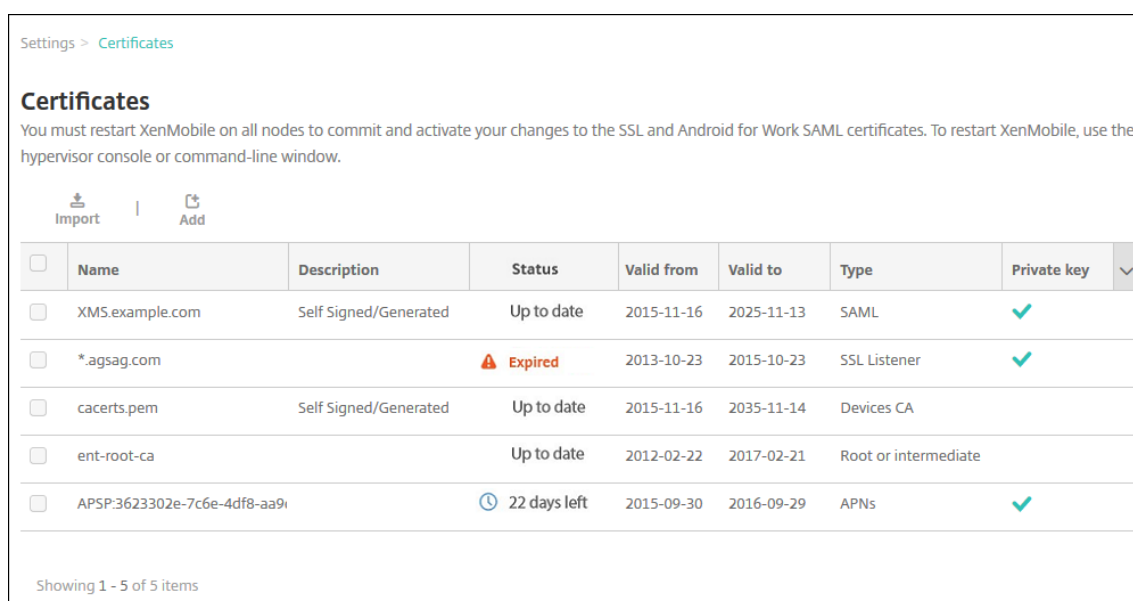
Você pode carregar o certificado de CA (sem a chave privada) que o CA usa para assinar solicitações. Você também pode carregar um certificado de cliente SSL (com a chave privada) para autenticação de cliente.

Quando você configura a entidade CA da Microsoft, você pode especificar o certificado de autoridade de certificação. Você pode selecionar o certificado de CA de uma lista de todos os certificados de servidor são certificados de CA. Da mesma forma, ao configurar a autenticação de cliente, você pode selecionar em uma lista de todos os certificados de servidor para os quais o XenMobile tem a chave privada.

Para importar um keystore

Por natureza, os keystores, que são os repositórios de certificados de segurança, podem conter várias entradas. Quando você carrega de um keystore, precisa especificar o alias de entrada que identifica a entrada que deseja carregar. Se você não especificar um alias, a primeira entrada da loja será carregada. Como os arquivos PKCS #12 geralmente contêm apenas uma entrada, o campo de alias não é exibido quando você seleciona PKCS #12 como o tipo de keystore.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Settings** é exibida.
2. Clique em **Certificados**. A página **Certificados** é exibida.



Settings > Certificates

Certificates

You must restart XenMobile on all nodes to commit and activate your changes to the SSL and Android for Work SAML certificates. To restart XenMobile, use the hypervisor console or command-line window.

Import | Add

<input type="checkbox"/>	Name	Description	Status	Valid from	Valid to	Type	Private key
<input type="checkbox"/>	XMS.example.com	Self Signed/Generated	Up to date	2015-11-16	2025-11-13	SAML	✓
<input type="checkbox"/>	*agsag.com		⚠ Expired	2013-10-23	2015-10-23	SSL Listener	✓
<input type="checkbox"/>	cacerts.pem	Self Signed/Generated	Up to date	2015-11-16	2035-11-14	Devices CA	
<input type="checkbox"/>	ent-root-ca		Up to date	2012-02-22	2017-02-21	Root or intermediate	
<input type="checkbox"/>	APSP:3623302e-7c6e-4df8-aa91		🕒 22 days left	2015-09-30	2016-09-29	APNs	✓

Showing 1 - 5 of 5 items

3. Clique em **Importar**. A caixa de diálogo **Importar** é exibida.
4. Defina estas configurações:
 - **Importar:** na lista, clique em **Keystore**. A caixa de diálogo **Importar** é alterada para refletir as opções de keystore disponíveis.

Import ✕

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import Keystore ▾

Keystore type PKCS#12 ▾

Use as Server ▾

Keystore file* Browse

Password*

Description

Cancel
Import

- **Tipo de keystore:** na lista, clique em **PKCS #12**.
- **Usar como:** na lista, clique em como você pretende usar o certificado. As opções disponíveis são:
 - **Servidor.** Os certificados de servidor são certificados usados funcionalmente pelo XenMobile Server que é carregado para o console da Web do XenMobile. Eles incluem certificados AC, certificados RA e certificados para autenticação de cliente com outros componentes da sua infraestrutura. Além disso, você pode usar os certificados de servidor como um armazenamento dos certificados que você deseja implantar em dispositivos. Esse uso se aplica especialmente a CAs usadas para estabelecer a confiança no dispositivo.
 - **SAML.** A certificação Security Assertion Markup Language (SAML) permite que você forneça o acesso de SSO a servidores, sites e aplicativos.
 - **APNs.** Os certificados de APNs da Apple permitem o gerenciamento de dispositivo móvel por meio da Rede Push da Apple.
 - **Ouvinte SSL.** O Ouvinte do protocolo SSL notifica o XenMobile sobre as atividades de criptografia SSL.
- **Arquivo keystore:** navegue para localizar o keystore que você deseja importar do tipo de

arquivo .p12 (ou .pfx nos computadores baseados em Windows).

- **Senha:** digite a senha atribuída ao certificado.
- **Descrição:** opcionalmente, digite uma descrição para o keystore para ajudá-lo a distingui-lo de outros keystores.

5. Clique em **Importar**. O keystore é adicionado à tabela Certificados.

Para importar um certificado

Ao importar um certificado, seja de um arquivo ou de uma entrada de keystore, o XenMobile tenta construir uma cadeia de certificados a partir da entrada. O XenMobile importa todos os certificados nessa cadeia para criar uma entrada de certificado do servidor para cada um. Essa operação só funcionará se os certificados na entrada do arquivo ou repositório de chaves formarem uma cadeia. Por exemplo, se cada certificado subsequente da cadeia for o emissor do certificado anterior.

Você pode adicionar uma descrição opcional para o certificado importado. A descrição só anexa o primeiro certificado na cadeia. Você pode atualizar a descrição dos certificados restantes mais tarde.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console e clique em **Certificados**.
2. Na página **Certificados**, clique em **Importar**. A caixa de diálogo **Importar** é exibida.
3. Na caixa de diálogo **Importar**, em **Importar**, se já não estiver selecionada, clique em **Certificado**.
4. A caixa de diálogo **Importar** é alterada para refletir as opções de certificado disponíveis. Em **Usar como**, selecione como você planeja usar o keystore. As opções disponíveis são:
 - **Servidor**. Os certificados de servidor são certificados usados funcionalmente pelo XenMobile Server que é carregado para o console da Web do XenMobile. Eles incluem certificados AC, certificados RA e certificados para autenticação de cliente com outros componentes da sua infraestrutura. Além disso, você pode usar os certificados de servidor como um armazenamento dos certificados que você deseja implantar em dispositivos. Essa opção se aplica especialmente a CAs usadas para estabelecer a confiança no dispositivo.
 - **SAML**. A certificação Security Assertion Markup Language (SAML) permite que você forneça o acesso de logon único (SSO) a servidores, sites e aplicativos.
 - **Ouvinte SSL**. O Ouvinte do protocolo SSL notifica o XenMobile sobre as atividades de criptografia SSL.
5. Navegue para localizar o keystore que você deseja importar do tipo de arquivo .p12 (ou .pfx nos computadores baseados em Windows).
6. Procure para localizar um arquivo de chave privada opcional para o certificado. A chave privada é usada para criptografia e descriptografia junto com o certificado.

7. Digite uma descrição para o certificado, opcionalmente, para ajudar a identificá-lo dos outros certificados.
8. Clique em **Importar**. O certificado é adicionado à tabela Certificados.

Carregar certificados para dispositivos iOS em massa com a API REST

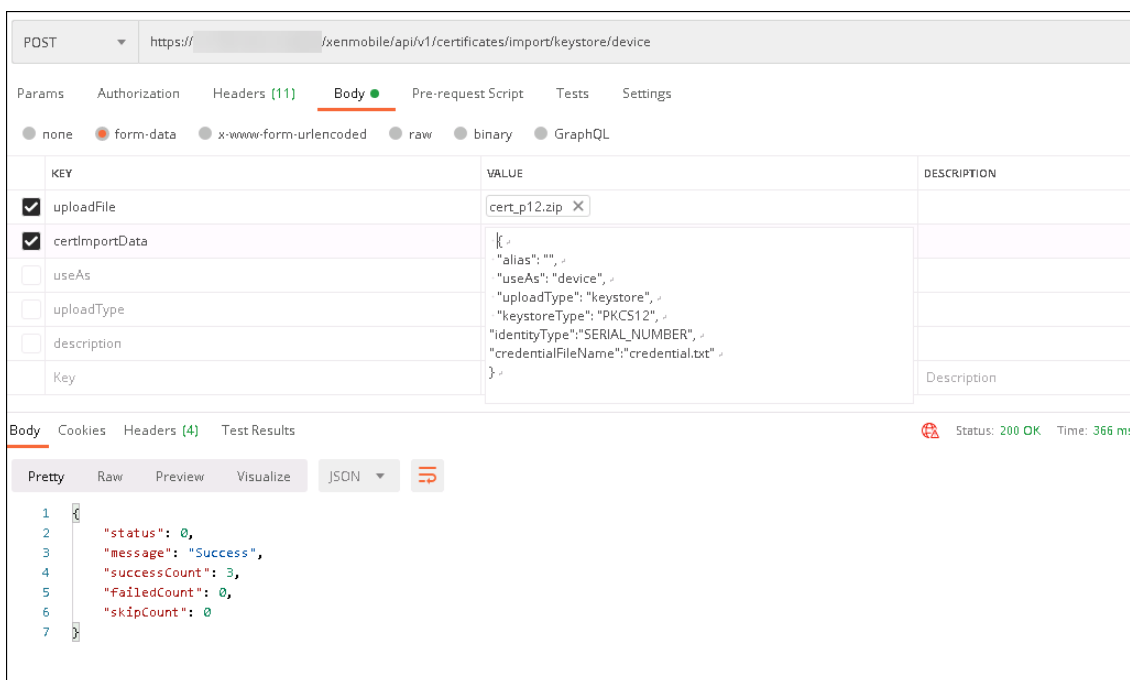
Se o carregamento individual de certificados não for prático, você poderá carregá-los em massa para dispositivos iOS com a API REST. Este método suporta certificados no formato .p12. Para obter mais informações sobre a API REST, consulte [APIs REST](#).

1. Renomeie cada um dos arquivos de certificado no formato `device_identity_value.p12`. O `device_identity_value` pode ser o IMEI, o número de série ou o MEID de cada dispositivo.
Como exemplo, escolhemos usar números de série como o seu método de identificação. Um dispositivo tem um número de série `A12BC3D4EFGH`, então nomeie o arquivo de certificado que você espera instalar nesse dispositivo `A12BC3D4EFGH.p12`.
2. Crie um arquivo de texto para armazenar as senhas para os certificados .p12. Nesse arquivo, digite o identificador de dispositivo e a senha para cada dispositivo em uma nova linha. Use o formato `device_identity_value=password`. Veja abaixo:

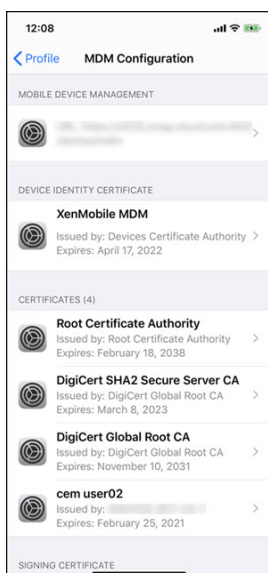
```
1 A12BC3D4EFGH.p12=password1!  
2 A12BC3D4EFIJ.p12=password2@  
3 A12BC3D4EFKL.p12=password3#  
4 <!--NeedCopy-->
```

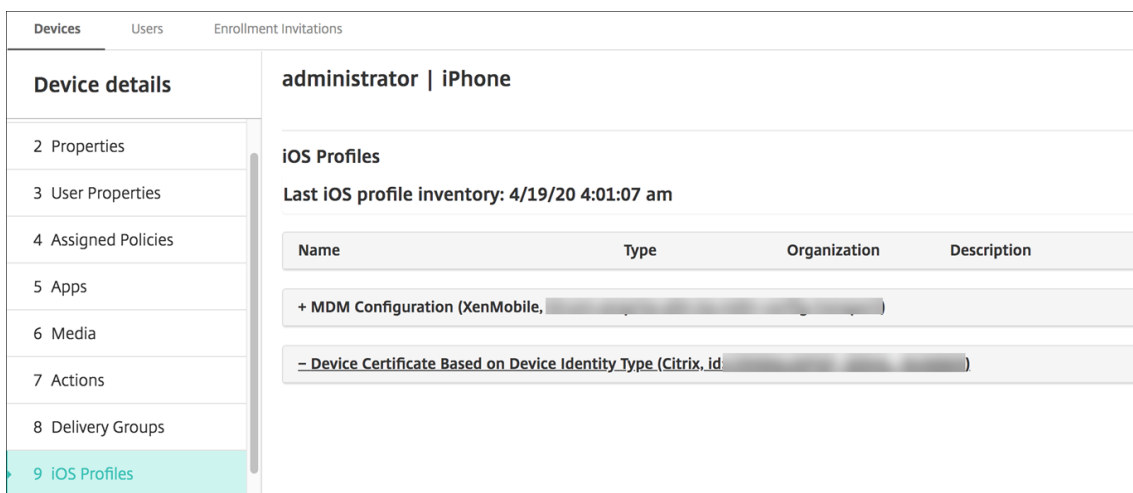
3. Empacote todos os certificados e o arquivo de texto que você criou em um arquivo .zip.
4. Inicie seu cliente de API REST, faça logon no XenMobile e obtenha um token de autenticação.
5. Importe seus certificados, garantindo que você coloque o seguinte no corpo da mensagem:

```
1 {  
2  
3     "alias": "",  
4     "useAs": "device",  
5     "uploadType": "keystore",  
6     "keystoreType": "PKCS12",  
7     "identityType": "SERIAL_NUMBER",           # identity type can be  
8     "credentialFileName": "credential.txt"     # The credential file  
9 }                                               name in .zip  
10  
11 <!--NeedCopy-->
```



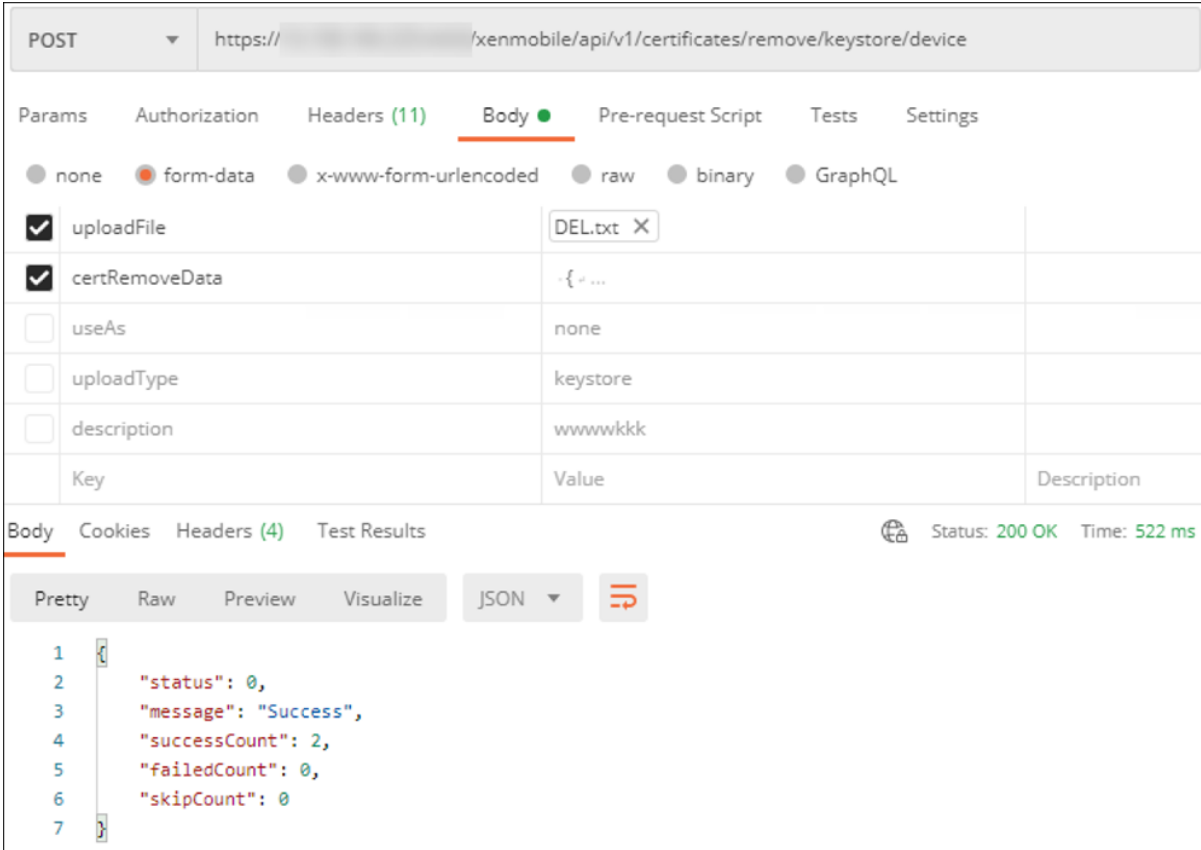
6. Crie uma política de VPN com o tipo de credencial **AlwaysOn IKEv2** e o método de autenticação do dispositivo **Certificado do dispositivo baseado na identidade do dispositivo**. Selecione o **Tipo de identidade do dispositivo** usado nos nomes dos arquivos de certificado. Consulte [Política de dispositivo do VPN](#).
7. Registre um dispositivo iOS e aguarde a implementação da política de VPN. Confirme a instalação do certificado verificando a configuração do MDM no dispositivo. Você também pode verificar os detalhes do dispositivo no console XenMobile.





Você também pode excluir certificados em massa criando um arquivo de texto com o `device_identity_value` listado para cada certificado a ser excluído. Na API REST, chame a API de exclusão e use a seguinte solicitação, substituindo `device_identity_value` pelo identificador apropriado:

```
1  ```\n2  {\n3\n4      "identityType"="device_identity_value"\n5  }\n6\n7  <!--NeedCopy-->  ```\n
```



The screenshot displays a REST client interface for a POST request to the endpoint `https://.../xenmobile/api/v1/certificates/remove/keystore/device`. The request body is a JSON object with the following fields:

Key	Value	Description
<input checked="" type="checkbox"/> uploadFile	DEL.txt X	
<input checked="" type="checkbox"/> certRemoveData	{ ...	
<input type="checkbox"/> useAs	none	
<input type="checkbox"/> uploadType	keystore	
<input type="checkbox"/> description	wwwkkk	

The response is a JSON object with the following fields:

```
1 {
2   "status": 0,
3   "message": "Success",
4   "successCount": 2,
5   "failedCount": 0,
6   "skipCount": 0
7 }
```

The status is 200 OK and the time taken is 522 ms.

Atualizando um certificado

O XenMobile permite que somente um certificado por chave pública exista no sistema a qualquer momento. Se você tentar importar um certificado para o mesmo par de chaves como um certificado já importado, poderá substituir a entrada existente ou excluir a entrada.

Para atualizar de forma eficaz os certificados, no console XenMobile, faça o seguinte: Clique no ícone de engrenagem no canto superior direito do console para abrir a página **Configurações** e clique em **Certificados**. Na caixa de diálogo **Importar**, importe o novo certificado.

Quando você atualiza um certificado de servidor, os componentes que estavam usando o certificado anterior passam automaticamente a usar o novo certificado. Da mesma forma, se você tiver implantado o certificado do servidor em dispositivos, o certificado será atualizado automaticamente na próxima implantação.

Renovação de um certificado

O XenMobile Server usa as seguintes autoridades de certificação internamente para PKI: CA raiz, CA do dispositivo e CA do servidor. Essas CAs são classificadas como um grupo lógico e recebem um nome de grupo. Quando uma nova instância do XenMobile Server é provisionada, as três CAs são geradas e recebem o nome de grupo “padrão”.

Você pode renovar as CAs para dispositivos iOS, macOS e Android suportados usando o console do XenMobile Server ou a API REST pública. Para dispositivos Windows registrados, os usuários devem registrar novamente os seus dispositivos para receber uma nova CA de dispositivo.

As seguintes APIs estão disponíveis para renovar ou regenerar as CAs de PKI internas no XenMobile Server e renovar os certificados de dispositivo emitidos por essas autoridades de certificação.

- Criar autoridades de certificação (CAs) de grupo.
- Ativar novas CAs e desative CAs antigas.
- Renovar o certificado do dispositivo em uma lista de dispositivos configurada. Os dispositivos já registrados continuam a funcionar sem interrupções. Um certificado de dispositivo é emitido quando um dispositivo se reconecta ao servidor.
- Retornar uma lista de dispositivos que ainda usam a CA antiga.
- Excluir a CA antiga depois que todos os dispositivos tiverem a nova CA.

Para obter mais informações, consulte as seguintes seções no arquivo PDF [Public API for REST Services](#):

- Seção 3.16.58, Renew Device Certificate
- Section 3.23, Internal PKI CA Groups

O console **Gerenciar dispositivos** inclui a ação de segurança, **Renovação de Certificado**, usada para renovar o certificado de registro em um dispositivo.

Pré-requisitos

- Por padrão, esse recurso de atualização de certificado está desativado. Para ativar os recursos de atualização de certificado, defina o valor para a propriedade do servidor **refresh.internal.ca** para **True**.

Importante:

Se o seu Citrix ADC estiver configurado para Descarga de SSL, quando você gerar um novo certificado, assegure-se de atualizar seu balanceador de carga com o novo cacert.perm. Para obter mais informações sobre a configuração do Citrix Gateway, consulte [Para usar o modo Descarga de SSL para VIPs Citrix ADC](#).

Opção de CLI para redefinir a senha do certificado de autoridade de certificação do servidor para nós do cluster

Depois de gerar um certificado de CA do servidor em um nó do XenMobile Server, use a CLI do XenMobile para redefinir a senha do certificado em outros nós do cluster. No menu principal da CLI, escolha **Sistema > Configurações avançadas > Redefinir senha de certificados de CA**. Se você redefinir a senha quando não houver um novo certificado de CA, o XenMobile não redefinirá a senha.

```
-----  
Advanced Settings  
-----  
[0] Back to System Menu  
[1] Toggle FIPS mode  
[2] Custom Ciphers  
[3] SSL protocols  
[4] Reset CA Certs Password  
[5] Reset SSL Certificate  
[6] Reset pki.xml  
[7] Server Tuning  
[8] Switch JDBC driver  
[9] Cloud Migration Credential Check  
[10] Refresh encryption keys  
-----  
Choice: [0 - 10] █
```

Administração de certificado do XenMobile

Recomendamos que você liste os certificados que usar na implantação do XenMobile, especialmente quanto às suas datas de expiração e senhas associadas. Esta seção destina-se a ajudá-lo a facilitar a administração de certificados no XenMobile.

Seu ambiente pode incluir alguns dos seguintes certificados ou todos eles:

- Servidor XenMobile
 - Certificado SSL para MDM FQDN
 - Certificado SAML (para Citrix Files)
 - Certificados raiz e de AC intermediários para os certificados acima e quaisquer outros recursos internos (StoreFront/Proxy etc.)
 - Certificado de APNs para gerenciamento de dispositivo iOS
 - Certificados de APNs internos para notificações do Secure Hub do XenMobile Server
 - Certificado de usuário PKI para conectividade com PKI

- MDX Toolkit
 - Certificado de desenvolvedor Apple
 - Perfil de provisionamento da Apple (por aplicativo)
 - Certificado Apple APNs (para uso com o Citrix Secure Mail)
 - Arquivo Android KeyStore
 - Windows Phone — Certificado DigiCert

O MAM SDK não prepara aplicativos, portanto, ele não requer um certificado.

- Citrix ADC
 - Certificado SSL para MDM FQDN
 - Certificado SSL para FQDN de Gateway
 - Certificado SSL para o FQDN do ShareFile SZC
 - Certificado SSL para o balanceamento de carga do Exchange (configuração de descarregamento)
 - Certificado SSL para balanceamento de carga de StoreFront
 - Certificados raiz e de AC intermediários para os precedentes acima

Política de expiração de certificado do XenMobile

Se você permitir um certificado expire, o certificado se torna inválido. Você não pode mais executar transações seguras no seu ambiente e não poderá acessar recursos do XenMobile.

Nota:

A Autoridade de Certificação (AC) exibe um aviso para você renovar seu certificado SSL antes da data de expiração.

Certificado de APNs para o Citrix Secure Mail

Os certificados do Apple Push Notification Service (APNs) expiram todo ano. Lembre-se de criar um certificado SSL de APNs e atualizá-lo no portal da Citrix antes que o certificado expire. Se o certificado expirar, os usuários verão discrepâncias com as notificações por push do Secure Mail. Além disso, você não poderá mais enviar notificações por push relativas aos seus aplicativos.

Certificado de APNs para gerenciamento de dispositivo iOS

Para registrar e gerenciar dispositivos iOS com o XenMobile, configure e crie um certificado de serviço de APNs da Apple. Se o certificado expirar, os usuários não podem se registrar no XenMobile e você não pode gerenciar os respectivos dispositivos iOS. Para obter detalhes, consulte [Certificados APNs](#).

Você pode exibir o status do certificado de APNs e data de vencimento fazendo logon no Apple Push Certificates Portal. Faça login como o mesmo usuário que criou o certificado.

Você também recebe uma notificação por e-mail da Apple 30 e 10 dias antes da data de expiração. A notificação inclui as seguintes informações:

```
1 The following Apple Push Notification Service certificate, created for
  Apple ID CustomerID will expire on Date. Revoking or allowing this
  certificate to expire will require existing devices to be re-
  enrolled with a new push certificate.
2
3 Please contact your vendor to generate a new request (a signed CSR),
  then visit https://identity.apple.com/pushcert to renew your Apple
  Push Notification Service certificate.
4
5 Thank You,
6
7 Apple Push Notification Service
8 <!--NeedCopy-->
```

MDX Toolkit (certificado de distribuição do iOS)

Um aplicativo que é executado em um dispositivo iOS físico (diferente de aplicativos na Apple App Store) tem esses requisitos de assinatura:

- Atribua ao aplicativo um perfil de provisionamento.
- Atribua ao aplicativo um certificado de distribuição correspondente.

Para verificar se você tem um certificado de distribuição do iOS válido, faça o seguinte:

1. No portal Apple Enterprise Developer, crie uma ID de Aplicativo explícita para cada aplicativo que deseja preparar com o MDX Toolkit. Um exemplo de ID de aplicativo aceitável é: `com.CompanyName.ProductName`.
2. No portal Apple Enterprise Developer, vá para **Provisioning Profiles > Distribution** e crie um perfil de provisionamento interno. Repita esta etapa para cada ID de Aplicativo criada na etapa anterior.
3. Baixe todos os perfis de provisionamento. Para obter detalhes, consulte [Preparação de aplicativos móveis iOS](#).

Para confirmar que todos os certificados de XenMobile Server são válidos, faça o seguinte:

1. No console XenMobile, clique em **Configurações > Certificados**.
2. Verifique se todos os certificados de APNs, incluindo os certificados de ouvinte SSL, raiz e intermediário são válidos.

Android KeyStore

O KeyStore é um arquivo que contém os certificados usados para assinar o aplicativo Android. Quando o período de validade da sua chave expira, os usuários não poderão mais atualizar em interrupções para novas versões do seu aplicativo.

Certificado empresarial da DigiCert para Windows Phones

A DigiCert é o provedor exclusivo de certificados de assinatura para o serviço Hub de Aplicativos Microsoft. Os desenvolvedores e editores de software entram no Hub de Aplicativos para distribuir aplicativos Windows Phone e Xbox 360 para download através do Windows Marketplace. Para obter detalhes, consulte [DigiCert Code Signing Certificates for Windows Phone](#) na documentação da DigiCert.

Se o certificado expirar, os usuários do Windows Phone não podem se registrar. Os usuários do Windows Phone não podem registrar, instalar um aplicativo publicado e assinado pela empresa, nem iniciar um aplicativo da empresa que foi instalada no telefone.

Citrix ADC

Para obter detalhes sobre como tratar de expiração do certificado do Citrix ADC, consulte [How to handle certificate expiry on NetScaler](#) no Citrix Support Knowledge Center.

Um certificado do Citrix ADC expirado impede que os usuários se registrem e acessem a Loja. O certificado expirado também impede que os usuários se conectem ao Exchange Server ao usar o Secure Mail. Além disso, os usuários não podem enumerar e abrir aplicativos HDX (dependendo de qual certificado expirou).

O Expiry Monitor e o Command Center podem ajudar você a acompanhar seus certificados do Citrix ADC. O Centro notificará você quando o certificado expirar. Essas ferramentas auxiliam na monitoração dos seguintes certificados do Citrix ADC:

- Certificado SSL para MDM FQDN
- Certificado SSL para FQDN de Gateway
- Certificado SSL para o FQDN do ShareFile SZC
- Certificado SSL para o balanceamento de carga do Exchange (configuração de descarregamento)
- Certificado SSL para balanceamento de carga de StoreFront
- Certificados raiz e de AC intermediários para os certificados acima

Citrix Gateway e XenMobile

November 30, 2020

Quando você configura o Citrix Gateway usando o XenMobile, estabelece o mecanismo de autenticação para o acesso remoto do dispositivo à rede interna. Essa funcionalidade permite que os aplicativos em um dispositivo móvel acessem servidores corporativos localizados na intranet. O XenMobile cria uma micro VPN entre os aplicativos no dispositivo e o Citrix Gateway.

Você configura o Citrix Gateway para uso com o XenMobile exportando um script do XenMobile executado no Citrix Gateway.

Pré-requisitos para usar o script de configuração do Citrix Gateway

Requisitos do Citrix ADC:

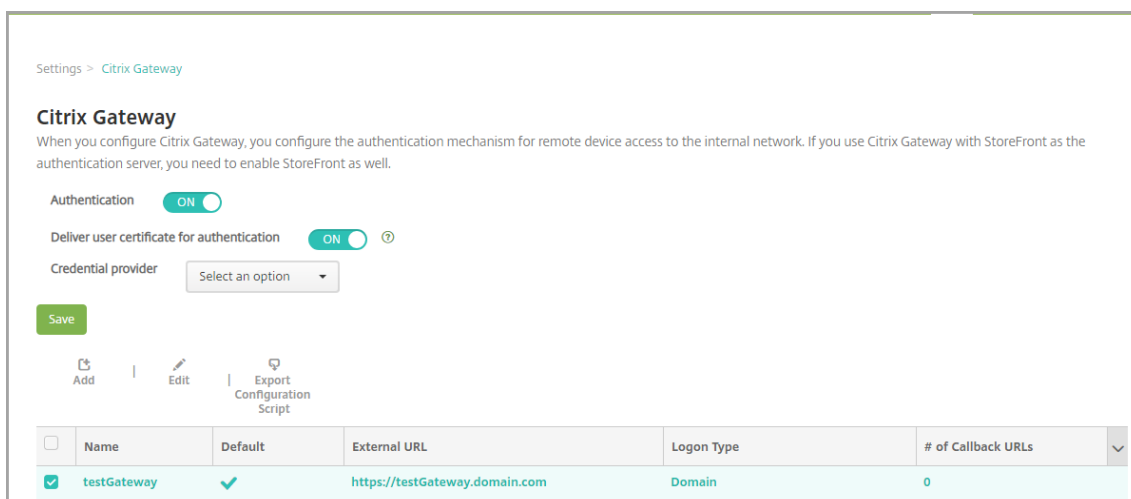
- Citrix ADC (versão mínima 11.0, Compilação 70.12).
- O endereço IP do Citrix ADC deve estar configurado e ter conectividade com o servidor LDAP, a menos que o LDAP tenha balanceamento de carga.
- O endereço IP do Citrix ADC Subnet (SNIP) deve estar configurado, ter conectividade com os servidores back-end necessários e ter acesso à rede pública por meio da porta 8443/TCP.
- O DNS deve poder resolver domínios públicos.
- O Citrix ADC deve estar licenciado com licenças de Plataforma/Universais ou de Avaliação. Para obter informações, consulte <https://support.citrix.com/article/CTX126049>.
- Um certificado SSL do Citrix Gateway é carregado e instalado no Citrix ADC. Para obter informações, consulte <https://support.citrix.com/article/CTX136023>.

Requisitos do XenMobile:

- XenMobile Server (versão mínima 10.6).
- O servidor LDAP deve estar configurado.

Configurar a autenticação para o acesso de dispositivos remotos à rede interna

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Settings** é exibida.
2. Em **Servidor**, clique em **Citrix Gateway**. A página do **Citrix Gateway** é exibida. No exemplo a seguir, existe uma instância do Citrix Gateway.



3. Defina estas configurações:

- **Autenticação:** selecione se a autenticação deve ser ativada. O padrão é **I**.
- **Entregar certificado de usuário para autenticação:** selecione se o XenMobile deve compartilhar o certificado de autenticação com o Secure Hub, para habilitar o Citrix Gateway para manipular a autenticação de certificado cliente. O padrão é **O**.
- **Provedor de credenciais:** na lista, clique no provedor de credenciais a ser usado. Para obter mais informações, consulte [Provedores de credenciais](#).

4. Clique em **Salvar**.

Adicionar uma instância do Citrix Gateway

Depois de salvar as configurações de autenticação, adicione uma instância do Citrix Gateway ao XenMobile.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é aberta.
2. Em **Servidor**, clique em **Citrix Gateway**. A página do **Citrix Gateway** é exibida.
3. Clique em **Adicionar**. A página **Adicionar novo Citrix Gateway** é exibida.

Settings > Citrix Gateway > Add New Citrix Gateway

Add New Citrix Gateway

Name *

Alias

External URL *

Logon Type

Password Required ON

Set as Default OFF

[Export Configuration Script](#) ⓘ

Callback URL * Virtual IP * [Add](#)

4. Defina estas configurações:

- **Nome:** digite um nome para a instância do Citrix Gateway.
- **Alias:** inclua opcionalmente um nome de alias para o Citrix Gateway.
- **URL externa:** digite a URL acessível publicamente do Citrix Gateway. Por exemplo, <https://receiver.com>.
- **Tipo de login:** escolha um tipo de login. Os tipos incluem **Somente domínio**, **Somente token de segurança**, **Domínio e token de segurança**, **Certificado**, **Certificado e domínio** e **Certificado e token de segurança**. A configuração padrão para o campo **Senha obrigatória** muda com base no **Tipo de login** selecionado. O padrão é **Somente domínio**.

Se você tiver vários domínios, use **Certificado e domínio**. Para obter mais informações sobre como configurar a autenticação de vários domínios com o XenMobile e o Citrix Gateway, consulte [Configurar a autenticação para vários domínios](#).

Se você usar **Certificado e token de segurança**, não necessárias configurações adicionais no Citrix Gateway para dar suporte ao Secure Hub. Para obter informações, consulte [Configuração do XenMobile para autenticação de certificado e token de segurança](#).

Para obter mais informações, consulte [Autenticação](#) no Manual de implantação.

- **Senha obrigatória:** selecione se a autenticação de senha deve ser exigida. O padrão varia de acordo com o **Tipo de login** escolhido.
- **Definir como padrão:** selecione se esse Citrix Gateway deve ser usado como padrão. O padrão é **O**.
- **Exportar script de configuração:** clique no botão para exportar um pacote de configuração carregado no Citrix Gateway para defini-lo com as configurações do XenMobile. Para obter informações, consulte “Configurar um Citrix Gateway local para uso com o XenMobile Server”, após estas etapas.

- **URL de retorno de chamada e IP virtual:** salve suas configurações antes de adicionar esses campos. Para obter informações, consulte Adicionar uma URL de retorno de chamada ao IP virtual da VPN do Citrix Gateway neste artigo.

5. Clique em **Salvar**.

O novo Citrix Gateway é adicionado e exibido na tabela. Para editar ou excluir uma instância, clique no nome na lista.

Configurar um Citrix Gateway para uso com o XenMobile Server

Para configurar um Citrix Gateway local para uso com o XenMobile, realize as seguintes etapas gerais, detalhadas neste artigo:

1. Baixe um script e os arquivos relacionados do XenMobile Server. Consulte o arquivo leia-me fornecido com o script para obter as instruções detalhadas mais recentes.
2. Verifique se o seu ambiente atende aos pré-requisitos.
3. Atualize o script do seu ambiente.
4. Execute o script no Citrix ADC.
5. Teste a configuração.

O script configura essas configurações do Citrix Gateway exigidas pelo XenMobile:

- Servidores Citrix Gateway necessários para MDM e MAM
- Políticas de sessão para os servidores virtuais do Citrix Gateway
- Detalhes do XenMobile Server
- Políticas de autenticação e ações para o servidor virtual Citrix Gateway.
O script descreve as definições de configuração de LDAP.
- Ações e políticas de tráfego para o servidor proxy
- Perfil de acesso sem cliente
- Registro DNS local estático no Citrix ADC
- Outras associações: política de serviço, certificado de CA

O script não manipula a seguinte configuração:

- Balanceamento de carga do Exchange
- Balanceamento de carga do Citrix Files
- Configuração de proxy ICA
- Descarga de SSL

Para baixar, atualizar e executar o script

1. Se estiver adicionando um Citrix Gateway, clique em **Exportar script de configuração** na página **Adicionar novo Citrix Gateway**.

Settings > Citrix Gateway > Add New Citrix Gateway

Add New Citrix Gateway

Name *

Alias

External URL *

Logon Type

Password Required ON

Set as Default OFF

[Export Configuration Script](#) ⓘ

Callback URL * Virtual IP * [Add](#)

Ou, se você adicionar uma instância do Citrix Gateway e clicar em **Salvar** antes de exportar o script, retorne à página **Configurações > Citrix Gateway**, selecione o Citrix ADC, clique em **Exportar script de configuração** e, em seguida, clique em **Download**.

Settings > Citrix Gateway

Citrix Gateway

When you configure Citrix Gateway, you configure the authentication mechanism for remote device access to the internal network. If you use Citrix Gateway with StoreFront as the authentication server, you need to enable StoreFront as well.

Authentication ON

Deliver user certificate for authentication ON ⓘ

Credential provider

[Save](#)

[Add](#) | [Edit](#) | [Export Configuration Script](#)

<input type="checkbox"/>	Name	Default	External URL	Logon Type	# of Callback URLs
<input checked="" type="checkbox"/>	testGateway	<input checked="" type="checkbox"/>	https://testGateway.domain.com	Domain	0

Depois de clicar em **Exportar script de configuração**, o XenMobile criará um pacote de script .tar.gz. O pacote de script inclui:

- Arquivo Leiamme com instruções detalhadas
- Script que contém comandos da CLI do Citrix ADC usados para configurar os componentes necessários no Citrix ADC
- Certificado de CA de raiz pública e o certificado de CA intermediária do XenMobile Server (esses certificados, para descarga de SSL, não são necessários para a versão atual)

- Script que contém os comandos da CLI do Citrix ADC para remover a configuração do Citrix ADC
2. Edite o script (NSGConfigBundle_CREATESCRIPT.txt) para substituir todos os espaços reservados por detalhes do seu ambiente.

```
# <LDAP_SECURE_PORT> -- LDAP Server Secure Port.
# <MSG_ROOT_CA_CERT_TAG> -- NetScaler ROOT CA Tag.
# <RADIUS_KEY> -- Radius Key.
# <XMS_CERT_TAG> -- XenMobile Certificate Tag.
# <MAM_LB_IP> -- Virtual IP Address to be assigned for MAM Load-Balancer and this IP must follow the RFC 1918 standard of private IP addresses.
# <MDM_LB_IP> -- Virtual IP Address to be assigned for MDM Load-Balancer and this IP must follow the RFC 1918 standard of private IP addresses.
# <RADIUS_SERVER_IP> -- Radius Server IP Address.
# <LDAP_PASSWORD> -- LDAP Service Account Password.
# <NS_SERVER_CERT_TAG> -- NetScaler Server Certificate Tag.
# <MSG_VIP> -- Virtual IP Address to be assigned to the NetScaler Gateway virtual server. This IP address must be reachable from your devices either directly or via a NAT.
```

3. Execute o script editado no bash shell do Citrix ADC, conforme descrito no arquivo leia-me incluído no pacote de script. Por exemplo:

```
/netscaler/nscli -U :<NetScaler Management Username>:<NetScaler Management Password> batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"
```

```
login as: nsroot
#####
#
#      WARNING: Access to this system is for authorized users only      #
#      Disconnect IMMEDIATELY if you are not an authorized user!      #
#
#####

Using keyboard-interactive authentication.
Password:
Last login: Thu Feb 16 10:10:29 2017 from 10.0.1.121
Done
> shell
Copyright (c) 1992-2013 The FreeBSD Project.
Copyright (c) 1979, 1980, 1983, 1986, 1988, 1989, 1991, 1992, 1993, 1994
    The Regents of the University of California. All rights reserved.

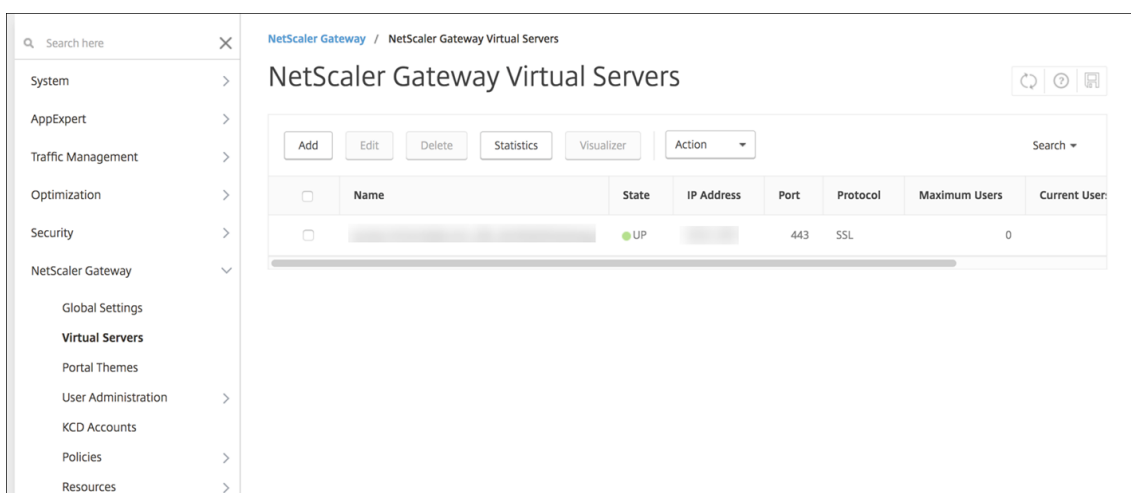
root@ns# /netscaler/nscli -U :nsroot:nsroot batch -f "/var/NSGConfigBundle_CREATESCRIPT.txt"
```

Quando o script for concluído, as seguintes linhas aparecerão.

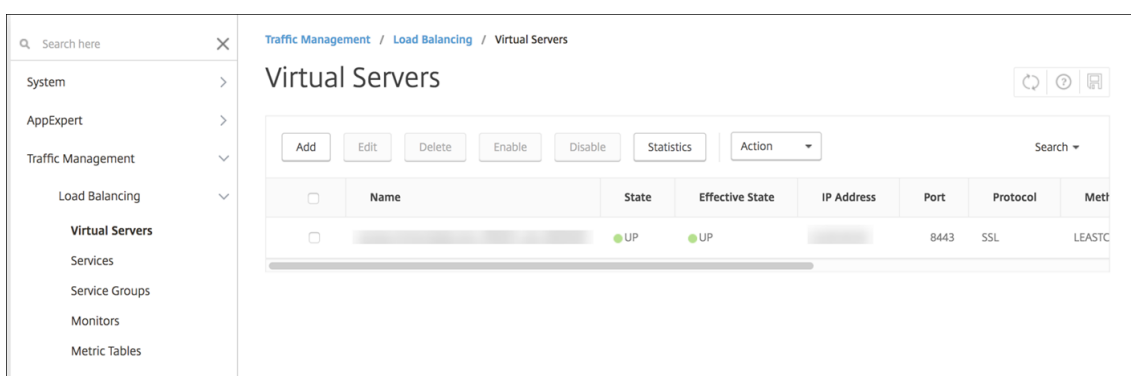
```
exec: save ns config
Done
Done
root@ns#
```

Testar a configuração

1. Valide que o servidor virtual do Citrix Gateway mostra um estado de **UP**.



2. Valide que o servidor virtual de balanceamento de carga proxy mostra um estado de **UP**.



3. Abra um navegador da Web, conecte-se à URL do Citrix Gateway e tente autenticar. Se a autenticação falhar, esta mensagem será exibida: HTTP Status 404 - Não encontrado
4. Registre um dispositivo e verifique se ele obtém os registros de MDM e MAM.

Adicionar uma URL de retorno de chamada ao IP virtual da VPN do Citrix Gateway

Depois de adicionar a instância do Citrix Gateway, você poderá adicionar uma URL de retorno de chamada e especificar um endereço IP virtual do Citrix Gateway. Essas configurações são opcionais, mas podem ser definidas para obter segurança extra, especialmente quando o XenMobile Server está na DMZ.

1. Em **Configurações > Citrix Gateway**, selecione o Citrix Gateway e clique em **Editar**.
 2. Na tabela, clique em **Adicionar**.
 3. Para **URL de retorno de chamada**, digite o nome de domínio totalmente qualificado (FQDN). A URL de retorno de chamada verifica se uma solicitação é proveniente do Citrix Gateway.
- Certifique-se de que a URL de retorno de chamada seja resolvida para um endereço IP acessível

no XenMobile Server. A URL de retorno de chamada pode ser uma URL externa do Citrix Gateway ou alguma outra URL.

4. Digite o endereço **IP virtual** do Citrix Gateway e clique em **Salvar**.

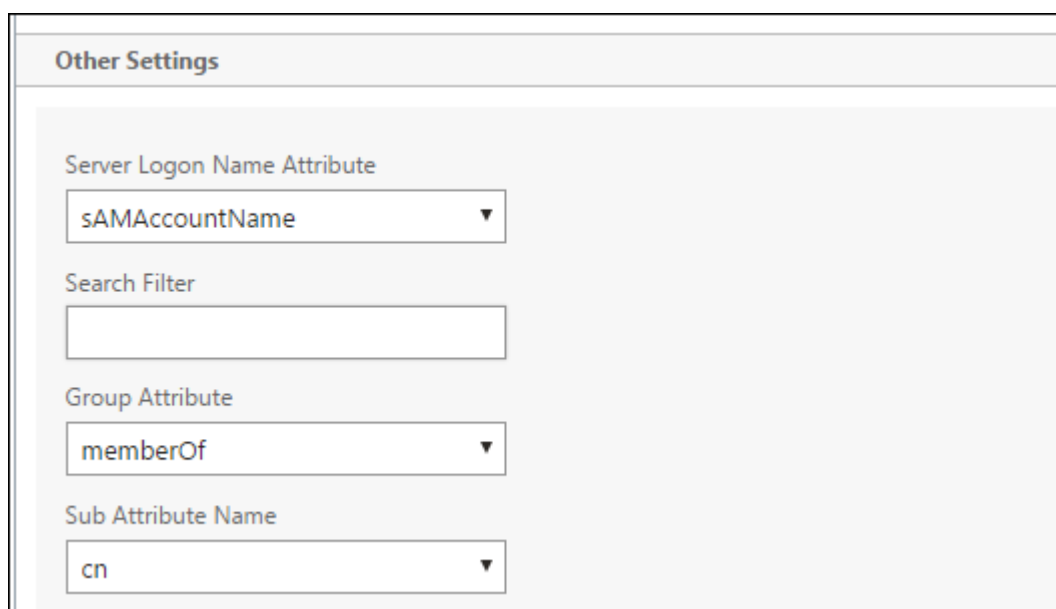
Configurar a autenticação para vários domínios

Se você tiver várias instâncias do XenMobile Server, como ambientes de teste, desenvolvimento e produção, deverá configurar o Citrix Gateway para os ambientes adicionais manualmente. (Você pode usar o assistente Citrix ADC for XenMobile apenas uma vez.)

Configuração do Citrix Gateway

Para configurar políticas de autenticação do Citrix Gateway e uma política de sessão para um ambiente de vários domínios:

1. No utilitário de configuração do Citrix Gateway, na guia **Configuration**, expanda **Citrix Gateway > Policies > Authentication**.
2. No painel de navegação, clique em **LDAP**.
3. Clique para editar o perfil LDAP. Mude o **Server Logon Name Attribute** para **userPrincipalName** ou para o atributo que você deseja usar para pesquisas. Anote o atributo especificado para que você o tenha ao definir as configurações de LDAP no console XenMobile.



The screenshot shows a configuration window titled "Other Settings" with the following fields:

- Server Logon Name Attribute:** A dropdown menu with "sAMAccountName" selected.
- Search Filter:** An empty text input field.
- Group Attribute:** A dropdown menu with "memberOf" selected.
- Sub Attribute Name:** A dropdown menu with "cn" selected.

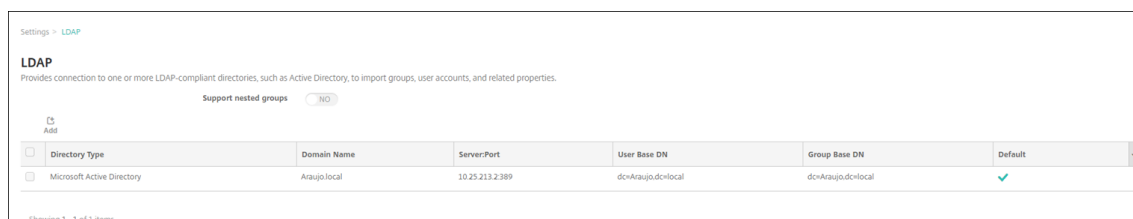
4. Repita essas etapas para cada política LDAP. Uma política LDAP separada é necessária para cada domínio.

5. Na política de sessão associada ao servidor virtual Citrix Gateway, navegue até **Edit session profile > Published Applications**. Certifique-se de que **Single Sign-On Domain** esteja em branco.

Configuração do XenMobile Server

Para configurar o LDAP para um ambiente XenMobile de vários domínios:

1. No console XenMobile, vá para **Configurações > LDAP** e adicione ou edite um diretório.



2. Forneça as informações.

- Em **Alias de domínio**, especifique cada domínio a ser usado para autenticação de usuário. Separe os domínios com uma vírgula e não use espaços entre os domínios. Por exemplo: `domain1.com, domain2.com, domain3.com`
- Certifique-se de que o campo **Pesquisa de usuário por** corresponde ao **Server Logon Name Attribute** especificado na política LDAP do Citrix Gateway.

Directory type*	Microsoft Active Directory	
Primary server*	10.████████	
Secondary server	IP Address or FQDN	
Port*	389	
Domain name*	Araujo.local	
User base DN*	dc=Araujo,dc=local	?
Group base DN*	dc=Araujo,dc=local	?
User ID*	Administrator@Araujo.local	
Password*		
Domain alias*	Araujo.local,Araujo.com,Araujo.net	
XenMobile Lockout Limit	0	?
XenMobile Lockout Time	1	?
Global Catalog TCP Port	3268	?
Global Catalog Root Context	dc=example,dc=com	?
User search by	userPrincipalName	
Use secure connection	<input type="checkbox"/> NO	

Suprimir solicitações de conexão de entrada para URLs específicas

Se o Gateway Citrix em seu ambiente estiver configurado para descarga de SSL, você talvez prefira que o gateway suprima solicitações de conexão de entrada para URLs específicas.

Se preferir manter essa segurança extra, configure os dois servidores virtuais do balanceador de carga MDM (um para a porta 443 e outro para a porta 8443) no Citrix Gateway. Use as seguintes informações como um modelo para suas configurações.

Importante:

As atualizações a seguir são apenas para um Citrix Gateway configurado para descarga de SSL.

1. Crie um conjunto de padrões com o nome `XMS_DropURLs`.

```
1 add policy patset XMS_DropURLs
2 <!--NeedCopy-->
```

2. Adicione as seguintes URLs ao novo conjunto de padrões. Personalize a lista conforme necessário.

```
1 bind policy patset XMS_DropURLs /zdm/shp/console -index 6
2
3 bind policy patset XMS_DropURLs /zdm/login_xdm_uc.jsp -index 5
4
5 bind policy patset XMS_DropURLs /zdm/helper.jsp -index 4
6
7 bind policy patset XMS_DropURLs /zdm/log.jsp -index 3
8
9 bind policy patset XMS_DropURLs /zdm/login.jsp -index 2
10
11 bind policy patset XMS_DropURLs /zdm/console -index 1
12 <!--NeedCopy-->
```

3. Crie uma política para suprimir todo o tráfego para essas URLs, a menos que a solicitação de conexão se origine da sub-rede especificada.

```
1 add responder policy XMS_DROP_pol "CLIENT.IP.SRC.IN_SUBNET
  (192.168.0.0/24).NOT &&
2 HTTP.REQ.URL.CONTAINS_ANY(" XMS_DropURLs ") " DROP -comment "Allow
  only subnet 192.168.0.0/24 to access these URLs. All other
  connections are DROPEd"
3 <!--NeedCopy-->
```

4. Vincule a nova política aos dois servidores virtuais do balanceador de carga MDM (portas 443 e 8443).

```
1 bind lb vserver _XM_LB_MDM_XenMobileMDM_443 -policyName
  XMS_DROP_pol -priority 100 -gotoPriorityExpression END -type
  REQUEST
2
3 bind lb vserver _XM_LB_MDM_XenMobileMDM_8443 -policyName
  XMS_DROP_pol -priority 100 -gotoPriorityExpression END -type
  REQUEST
4 <!--NeedCopy-->
```

Configure autenticação de domínio ou de domínio de segurança

March 5, 2021

O XenMobile dá suporte a autenticação baseada em domínio com relação a um ou mais diretórios que estão em conformidade com o protocolo LDAP. Você pode configurar uma conexão XenMobile para um ou mais diretórios e depois usar a configuração de LDAP para importar grupos, contas de usuários e propriedades correlatas.

O LDAP é um protocolo de aplicativo neutro quanto ao fornecedor e de software livre para acesso e manutenção de serviços de informações de diretório distribuído sobre uma rede Protocolo IP. Os serviços de informações de diretório são usados para compartilhar informações sobre os usuários, os sistemas, as redes, os serviços e os aplicativos disponíveis em toda a rede.

Um uso comum do LDAP é fornecer logon único (SSO, Single Sign-on) para usuários, em que uma única senha (por usuário) é compartilhada entre vários serviços. O logon único permite que um usuário faça logon uma vez em um site da empresa, para acesso autenticado à intranet corporativa.

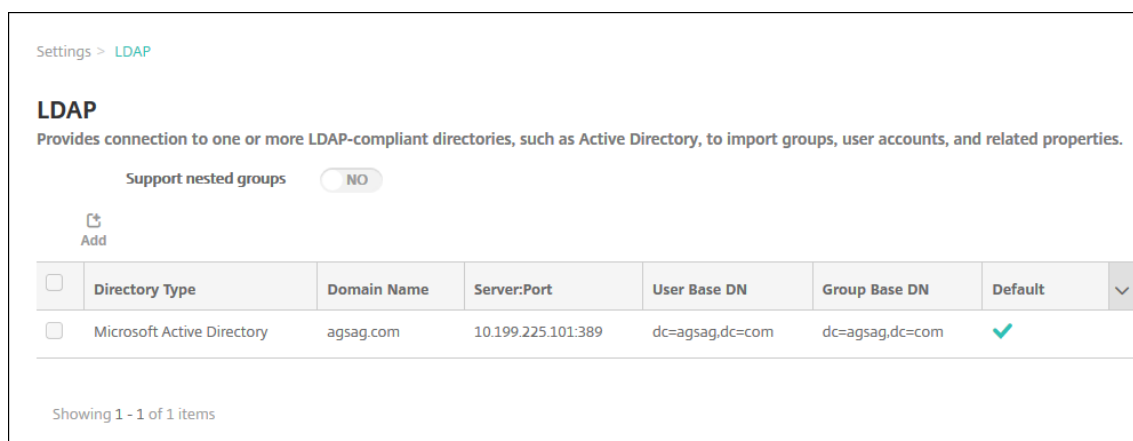
Um cliente inicia uma sessão do LDAP conectando-se a um servidor LDAP, chamado de Directory System Agent (DSA). O cliente envia uma solicitação de operação para o servidor, e o servidor responde com a autenticação adequada.

Importante:

O XenMobile não dá suporte à alteração do modo de autenticação, de autenticação de domínio para um modo de autenticação diferente, depois que os usuários registram dispositivos no XenMobile.

Para adicionar conexões LDAP no XenMobile

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Settings** é exibida.
2. Em **Servidor**, clique em **LDAP**. A página **LDAP** é exibida. Você pode adicionar, editar ou excluir diretórios compatíveis com LDAP, conforme descrito neste artigo.



Para adicionar um diretório compatível com LDAP

1. Na página **LDAP**, clique em **Adicionar**. A página **Adicionar LDAP** é exibida.

Settings > LDAP > Add LDAP

Add LDAP

Provides connection to one or more LDAP-compliant directories, such as Active Directory, to import groups, user accounts, and related properties.

Directory type*	Microsoft Active Directory	
Primary server*	IP Address or FQDN	
Secondary server	IP Address or FQDN	
Port*	389	
Domain name*		
User base DN*	dc=example,dc=com	?
Group base DN*	dc=example,dc=com	?
User ID*		
Password*		
Domain alias*		
XenMobile Lockout Limit	0	?
XenMobile Lockout Time	1	?
Global Catalog TCP Port	3268	?
Global Catalog Root Context	dc=example,dc=com	?
User search by	userPrincipalName	
Use secure connection	<input type="radio"/> NO	

Cancel Save

2. Defina estas configurações:

- **Tipo de diretório:** na lista, clique no tipo de diretório adequado. O padrão é **Microsoft Active Directory**.
- **Servidor primário:** digite o servidor primário usado para o LDAP; você pode inserir o endereço IP ou o nome de domínio totalmente qualificado (FQDN).
- **Servidor secundário:** opcionalmente, se um servidor secundário tiver sido configurado, digite o endereço IP ou o FQDN do servidor secundário. Esse servidor é um failover usado se o servidor primário não pode ser acessado.
- **Porta:** digite o número da porta usada pelo servidor LDAP. Por padrão, o número da porta é definido como **389** para conexões LDAP não seguras. Use o número de porta **636** para

conexões LDAP seguras, **3268** para conexões LDAP não seguras da Microsoft ou **3269** para conexões LDAP seguras da Microsoft.

- **Nome de domínio:** digite o nome de domínio.
- **DN base de usuário:** digite a localização dos usuários no Active Directory por meio de um identificador exclusivo. Exemplos de sintaxe incluem: `ou=users,dc=example` ou `dc=com`.
- **DN base de grupo:** digite a localização dos grupos no Active Directory. Por exemplo, `cn=users,dc=domain,dc=net`, onde `cn=users` representa o nome do contêiner dos grupos e `dc` representa o componente de domínio do Active Directory.
- **ID do usuário:** digite o ID de usuário associado à conta do Active Directory.
- **Senha:** digite a senha associada ao usuário.
- **Alias de domínio:** digite um alias para o nome de domínio. Se você alterar a configuração do **alias do domínio** após o registro, os usuários deverão se registrar novamente.
- **Limite de bloqueio do XenMobile:** digite um número entre **0** e **999** para ser o número de tentativas de login com falha. Um valor **0** significa que o XenMobile nunca bloqueia o usuário com base em tentativas de login com falha.
- **Tempo de bloqueio do XenMobile:** digite um número entre **0** e **99999** para representar o número de minutos que um usuário deve esperar depois de ultrapassar o limite de bloqueio. Um valor **0** significa que o usuário não é forçado a esperar após um bloqueio.
- **Porta TCP do catálogo global:** digite o número da porta TCP do servidor do Catálogo Global. Por padrão, o número da porta TCP é definido como **3268**; para conexões SSL, use o número de porta **3269**.
- **Contexto raiz do catálogo global:** opcionalmente, digite o valor do Contexto Raiz Global usado para ativar uma pesquisa do catálogo global no Active Directory. Essa pesquisa é adicional à pesquisa LDAP padrão, em qualquer domínio, sem a necessidade de especificar o nome de domínio real.
- **Pesquisa de usuário por:** na lista, clique em `userPrincipalName` ou `sAMAccountName`. O padrão é `userPrincipalName`. Se você alterar a configuração de **Pesquisa de usuário por** após o registro, os usuários deverão se registrar novamente.
- **Usar conexão segura:** selecione se devem ou não ser usadas conexões seguras. O padrão é **NÃO**.

3. Clique em **Salvar**.

Para editar um diretório compatível com LDAP

1. Na tabela **LDAP**, selecione o diretório a editar.

Quando você marca a caixa de seleção ao lado de um diretório, o menu de opções é exibido acima da lista LDAP. Clique em qualquer outro lugar na lista e o menu de opções é exibido no lado direito da listagem.

2. Clique em **Edit**. A página **Editar LDAP** é exibida.

The screenshot shows the 'Editar LDAP' configuration page. The fields are as follows:

- Directory type*: Microsoft Active Directory (dropdown)
- Primary server*: 10.61. (text input)
- Secondary server: IP Address or FQDN (text input)
- Port*: 389 (text input)
- Domain name*: .net (text input)
- User base DN*: dc=.dc=.net (text input)
- Group base DN*: dc=.dc=.net (text input)
- User ID*: administrator@.net (text input)
- Password*: (password field)
- Domain alias*: .net (text input)
- XenMobile Lockout Limit: 0 (text input)
- XenMobile Lockout Time: 1 (text input)
- Global Catalog TCP Port: 3268 (text input)
- Global Catalog Root Context: dc=example.dc=com (text input)
- User search by: userPrincipalName (dropdown)
- Use secure connection: NO (radio button)

3. Altere as seguintes informações conforme apropriado:

- **Tipo de diretório:** na lista, clique no tipo de diretório adequado.
- **Servidor primário:** digite o servidor primário usado para o LDAP; você pode inserir o endereço IP ou o nome de domínio totalmente qualificado (FQDN).
- **Servidor secundário:** opcionalmente, digite o endereço IP ou o FQDN do servidor secundário (se um tiver sido configurado).
- **Porta:** digite o número da porta usada pelo servidor LDAP. Por padrão, o número da porta é definido como **389** para conexões LDAP não seguras. Use o número de porta **636** para conexões LDAP seguras, **3268** para conexões LDAP não seguras da Microsoft ou **3269** para conexões LDAP seguras da Microsoft.
- **Nome de domínio:** você não pode alterar esse campo.
- **DN base de usuário:** digite a localização dos usuários no Active Directory por meio de um identificador exclusivo. Exemplos de sintaxe incluem: `ou=users`, `dc=example` ou `dc=com`.
- **DN base de grupo:** digite o nome de grupo DN base de grupo especificado como `cn=groupname`. Por exemplo, `cn=users`, `dc=servername`, `dc=net`, onde `cn=users` é o nome do grupo. `DN` e `servername` representam o nome do servidor que executa o Active Directory.
- **ID do usuário:** digite o ID de usuário associado à conta do Active Directory.

- **Senha:** digite a senha associada ao usuário.
 - **Alias de domínio:** digite um alias para o nome de domínio. Se você alterar a configuração do **Alias de domínio** após o registro, os usuários deverão se registrar novamente.
 - **Limite de bloqueio do XenMobile:** digite um número entre **0** e **999** para ser o número de tentativas de login com falha. Um valor **0** significa que o XenMobile nunca bloqueia o usuário com base em tentativas de login com falha.
 - **Tempo de bloqueio do XenMobile:** digite um número entre **0** e **99999** para representar o número de minutos que um usuário deve esperar depois de ultrapassar o limite de bloqueio. Um valor **0** significa que o usuário não é forçado a esperar após um bloqueio.
 - **Porta TCP do catálogo global:** digite o número da porta TCP do servidor do Catálogo Global. Por padrão, o número da porta TCP é definido como **3268**; para conexões SSL, use o número de porta **3269**.
 - **Contexto raiz do catálogo global:** opcionalmente, digite o valor do Contexto Raiz Global usado para ativar uma pesquisa do catálogo global no Active Directory. Essa pesquisa é adicional à pesquisa LDAP padrão, em qualquer domínio, sem a necessidade de especificar o nome de domínio real.
 - **Pesquisa de usuário por:** na lista, clique em **userPrincipalName** ou **sAMAccountName**. Se você alterar a configuração de **Pesquisa de usuário por** após o registro, os usuários deverão se registrar novamente.
 - **Usar conexão segura:** selecione se devem ou não ser usadas conexões seguras.
4. Clique em **Salvar** para salvar suas alterações ou em **Cancelar** para deixar a propriedade inalterada.

Para excluir um diretório compatível com LDAP

1. Na tabela **LDAP**, selecione o diretório que você deseja excluir.

Você pode selecionar mais de uma propriedade para excluir marcando a caixa de seleção ao lado de cada propriedade.
2. Clique em **Excluir**. Uma caixa de diálogo de confirmação é exibida. Clique em **Excluir** novamente.

Configurar a autenticação para vários domínios

Para configurar o XenMobile Server para usar vários sufixos de domínio em uma configuração LDAP, consulte o procedimento na documentação do Citrix Endpoint Management, [Configurar a autenticação para vários domínios](#). As etapas são as mesmas na versão local do XenMobile Server e na versão na nuvem do Endpoint Management.

Configurar autenticação de domínio e de token de segurança

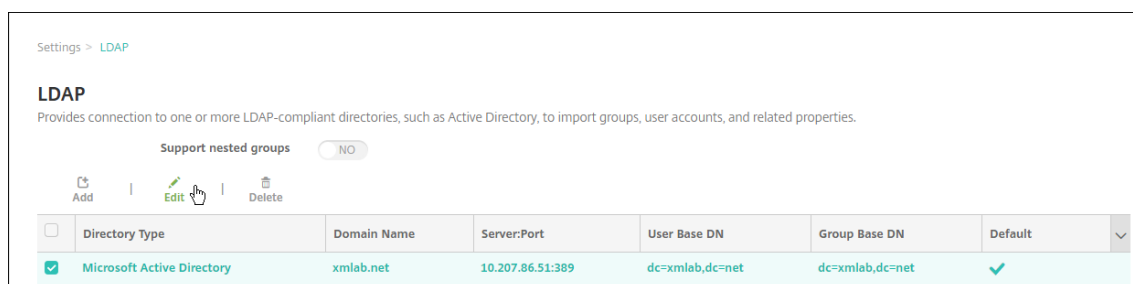
Você pode configurar o XenMobile para exigir que os usuários autentiquem com as suas credenciais LDAP mais uma senha de uso único, usando o protocolo RADIUS.

Para melhor usabilidade, você pode combinar essa configuração com o Citrix PIN e armazenamento em cache de senha do Active Directory. Com essa configuração, os usuários não precisam digitar seus nomes de usuário e senhas LDAP repetidamente. Os usuários inserem seus nomes de usuário e senhas para registro, expiração de senha e bloqueio de conta.

Definir as configurações do LDAP

O uso de LDAP para autenticação requer que você instale um certificado SSL de uma Autoridade de Certificação no XenMobile. Para obter informações, consulte [Carregando certificados no XenMobile](#).

1. Em **Configurações**, clique em **LDAP**.
2. Selecione **Microsoft Active Directory** e, em seguida, clique em **Editar**.



3. Verifique se a Porta é **636**, que é para conexões LDAP seguras, ou **3269**, para conexões LDAP seguras da Microsoft.
4. Altere **Usar conexão segura** para **Sim**.

Port* 636

Domain name* net

User base DN* dc=dc-net ⓘ

Group base DN* dc=dc-net ⓘ

User ID* administrator@net

Password*

Domain alias* net

XenMobile Lockout Limit 0 ⓘ

XenMobile Lockout Time 1 ⓘ

Global Catalog TCP Port 3269 ⓘ

Global Catalog Root Context dc=example.dc=com ⓘ

User search by userPrincipalName

Use secure connection YES

Cancel Save

Definir configurações do Citrix Gateway

As seguintes etapas pressupõem que você já tenha adicionado uma instância do Citrix Gateway ao XenMobile. Para adicionar uma instância do Citrix Gateway, consulte [Adicionar uma instância do Citrix Gateway](#).

1. Em **Configurações**, clique em **Citrix Gateway**.
2. Selecione o **Citrix Gateway** e clique em **Editar**.
3. Em **Tipo de logon**, selecione **Domínio e token de segurança**.

Settings > NetScaler Gateway > Add New NetScaler Gateway

Add New NetScaler Gateway

Name* THAG

Alias

External URL*

Logon Type Domain and security token

Password Required ON

Set as Default ON

Callback URL* Virtual IP* Add

Cancel Save

Ativar o PIN da Citrix e o cache de senha de usuário

Para ativar o PIN da Citrix e a senha do usuário em cache, vá para **Configurações > Propriedades do Cliente** e assinale as caixas de seleção para **Ativar PIN da Citrix** e **Ativar armazenamento em cache da senha do usuário**. Para obter mais informações, consulte [Propriedades do cliente](#).

Configurar o Citrix Gateway para autenticação de domínio e de token de segurança

Configure perfis de sessão do Citrix Gateway e as políticas de seus servidores virtuais usados com o XenMobile. Para obter mais informações, consulte a documentação do Citrix Gateway.

Autenticação de certificado cliente ou certificado de domínio

August 20, 2021

A configuração padrão para o XenMobile é autenticação de nome de usuário e senha. Para adicionar outra camada de segurança para registro e acesso ao ambiente do XenMobile, considere usar a autenticação baseada em certificado. No ambiente XenMobile, essa configuração é a melhor combinação de segurança e experiência do usuário. O certificado mais a autenticação de domínio tem as melhores possibilidades de SSO, juntamente com a segurança fornecida pela autenticação de dois fatores no Citrix ADC.

Para melhor usabilidade, você pode combinar autenticação de certificado mais domínio com o Citrix PIN e a senha em cache do Active Directory. Como resultado, os usuários não precisam digitar seus nomes de usuário e senhas LDAP repetidamente. Os usuários inserem seus nomes de usuário e senhas para registro, expiração de senha e bloqueio de conta.

Importante:

O XenMobile não dá suporte à alteração do modo de autenticação, de autenticação de domínio para algum outro modo de autenticação, depois que os usuários registram dispositivos no XenMobile.

Se você não permitir LDAP e usar cartões inteligentes ou similar métodos, a configuração de certificados permite a você representar um cartão inteligente para o XenMobile. Em seguida, os usuários se registram usando um PIN exclusivo que o XenMobile gera para eles. Depois que o usuário pode acessar, o XenMobile cria e implanta o certificado usado para autenticar no ambiente XenMobile.

Você pode usar o assistente Citrix ADC for XenMobile para executar a configuração necessária para o XenMobile ao usar autenticação de NetScaler de certificado apenas ou autenticação de certificado mais domínio. Você pode executar o assistente Citrix ADC for XenMobile apenas uma vez.

Em ambientes altamente seguros, o uso de credenciais LDAP fora de uma organização em redes públicas ou inseguras é considerado uma grande ameaça à segurança da organização. Para ambientes altamente seguros, uma opção é a autenticação de dois fatores que usa um certificado de cliente e um token de segurança. Para obter informações, consulte [Configuração do XenMobile para autenticação de certificado e token de segurança](#).

Autenticação de certificado de cliente está disponível para o modo MAM do XenMobile (somente MAM) e o modo ENT (quando os usuários se registram no MDM). A autenticação de certificado cliente não está disponível para o modo ENT do XenMobile quando os usuários se registram no modo MAM legado. Para usar a autenticação de certificado de cliente para os modos ENT e MAM do XenMobile, você deve configurar o servidor Microsoft, o XenMobile Server e o Citrix Gateway. Siga os seguintes procedimentos gerais, como detalhado neste artigo.

No servidor Microsoft:

1. Adicione um snap-in de certificado ao Console de Gerenciamento Microsoft.
2. Adicione o modelo à Autoridade de Certificação (AC).
3. Crie um certificado PFX do servidor de AC.

No XenMobile Server:

1. Carregue o certificado no XenMobile.
2. Crie a entidade PKI de autenticação baseada em certificado.
3. Configure os provedores de credenciais.
4. Configure o Citrix Gateway para fornecer um certificado de usuário para autenticação.

Para obter informações sobre a configuração do Citrix Gateway, consulte estes artigos na documentação do Citrix ADC:

- [Autenticação de cliente](#)
- [Infraestrutura de perfil SSL](#)
- [Configuração e vinculação de uma política de autenticação de certificado cliente](#)

Pré-requisitos

- Ao criar um modelo de Entidade de Serviços de Certificado Microsoft, evite possíveis problemas de autenticação com dispositivos registrados excluindo caracteres especiais. Por exemplo, não use esses caracteres no nome do modelo: : ! \$ () ## % + * ~ ? | { } []
- Para dispositivos Windows Phone 8.1 que usam autenticação de certificado e Descarga de SSL, desabilite a reutilização de sessão SSL da porta 443 nos dois servidores virtuais de balanceamento de carga no Citrix ADC. Para fazer isso, execute o seguinte comando nos servidores virtuais para a porta 443:

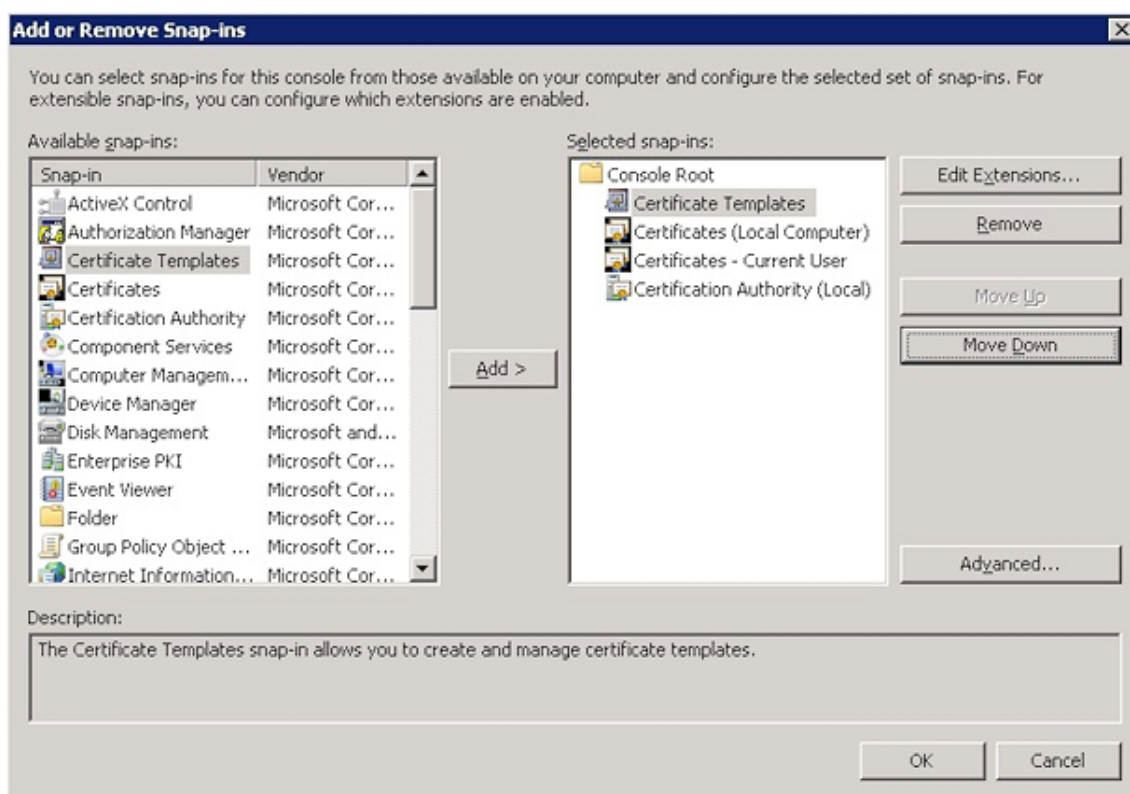
```
set ssl vserver <ssl lb vserver> sessReuse DISABLE
```

A desativação da reutilização da sessão SSL desativa algumas das otimizações que o Citrix ADC oferece, o que pode resultar em uma redução no desempenho no Citrix ADC.

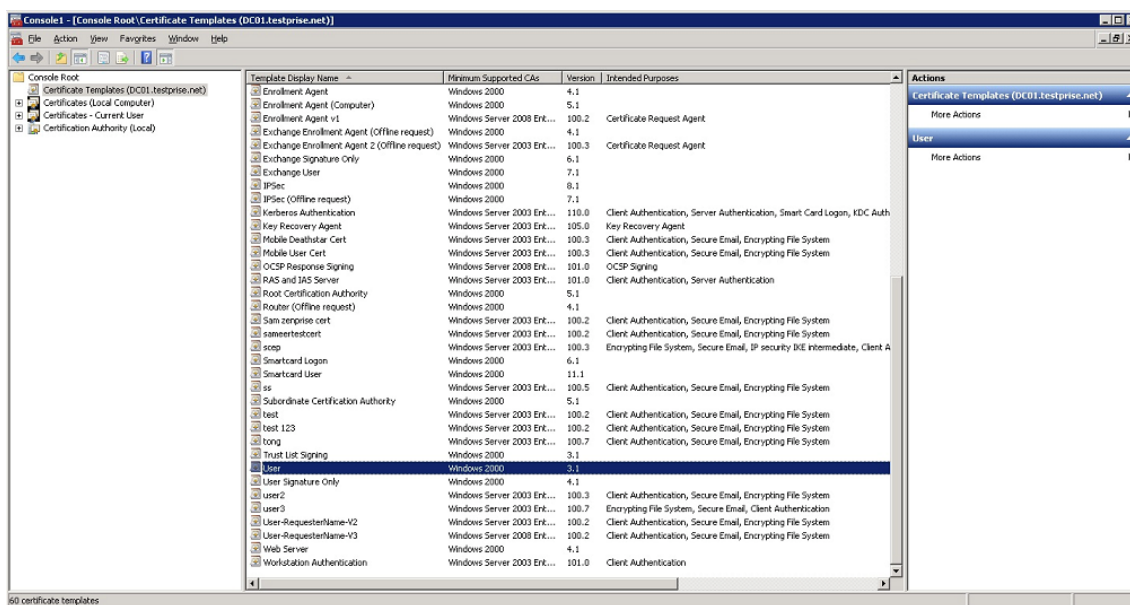
- Para configurar a autenticação baseada em certificado para o Exchange ActiveSync, consulte este [Blog da Microsoft](#). Configure o site do servidor da autoridade de certificação (AC) para o Exchange ActiveSync para exigir certificados cliente.
- Se você usa certificados de servidor privados para proteger o tráfego do ActiveSync ao Exchange Server, verifique se os dispositivos móveis têm todos os certificados raiz e intermediários necessários. Caso contrário, a autenticação baseada em certificado não ocorrerá durante a instalação da caixa de correio no Secure Mail. No console do IIS do Exchange, você deve:
 - Adicione um site para uso do XenMobile com o Exchange e associe o certificado de servidor Web.
 - Use a porta 9443.
 - Para esse site, você deve adicionar dois aplicativos, um para “Microsoft-Server-ActiveSync” e um para “EWS”. Por ambos os aplicativos, em **Configurações de SSL**, selecione **Exigir SSL**.

Adicionar um snap-in de certificado ao Console de Gerenciamento Microsoft

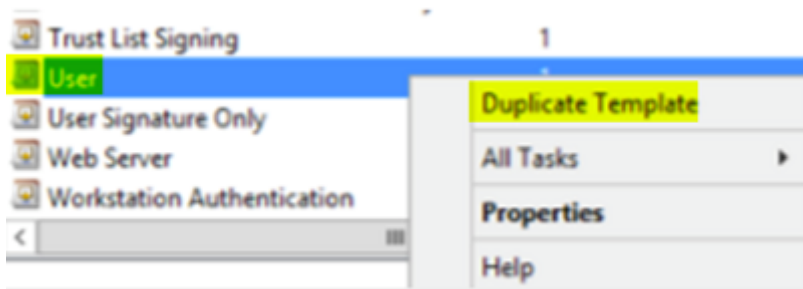
1. Abra o console e, em seguida, clique em **Adicionar ou remover snap-ins**.
2. Adicione os seguintes snap-ins:
 - Modelos de Certificado
 - Certificados (Computador Local)
 - Certificados - Usuário Atual
 - Autoridade de Certificação (Local)



3. Expanda **Modelos de certificado**.



4. Selecione o modelo **Usuário** e **Modelo Duplicado**.

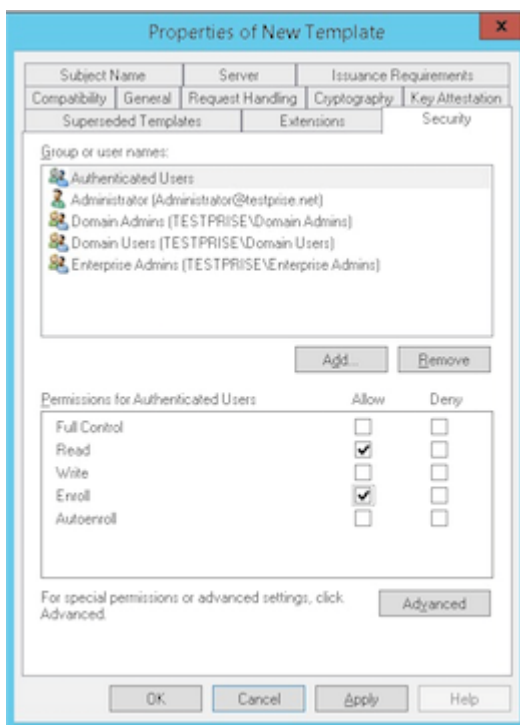


5. Forneça o nome para exibição do Modelo.

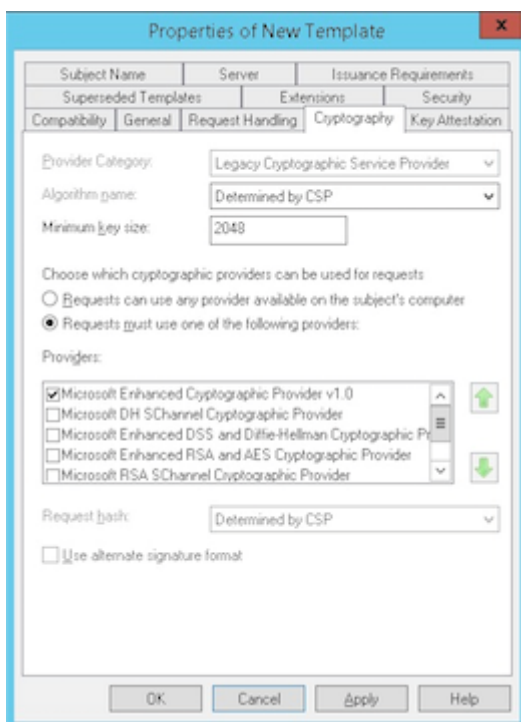
Importante:

Marque a caixa de seleção **Publicar certificado no Active Directory** somente se necessário. Se essa opção estiver marcada, todos os certificados cliente do usuário serão criados no Active Directory, o que pode travancar o banco de dados do Active Directory.

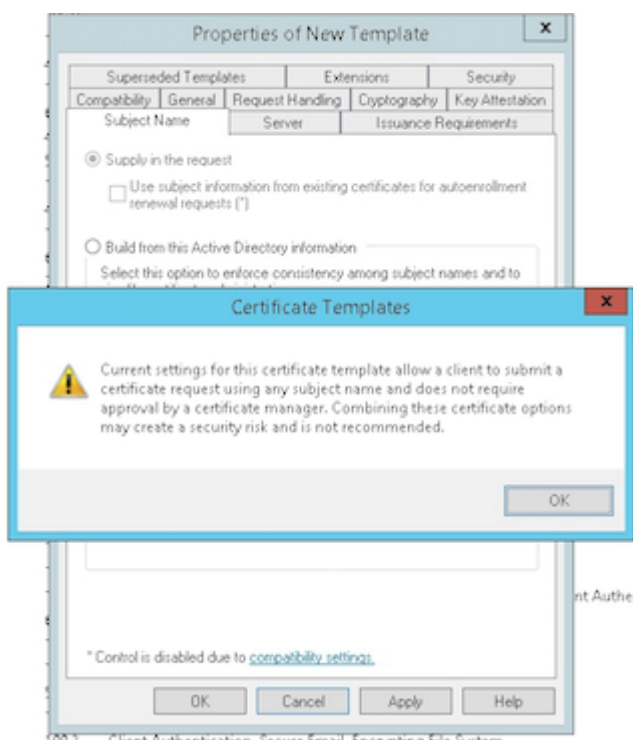
6. Selecione **Windows 2003 Server** como o tipo de modelo. No servidor Windows 2012 R2, em **Compatibilidade**, selecione **Autoridade de certificação** e defina o destinatário como **Windows 2003**.
7. Em **Segurança**, selecione a opção **Registrar** na coluna **Permitir** dos usuários autenticados.



8. Em **Criptografia**, assegure-se de fornecer o tamanho da chave. Mais tarde, você insere o tamanho da chave ao configurar o XenMobile.

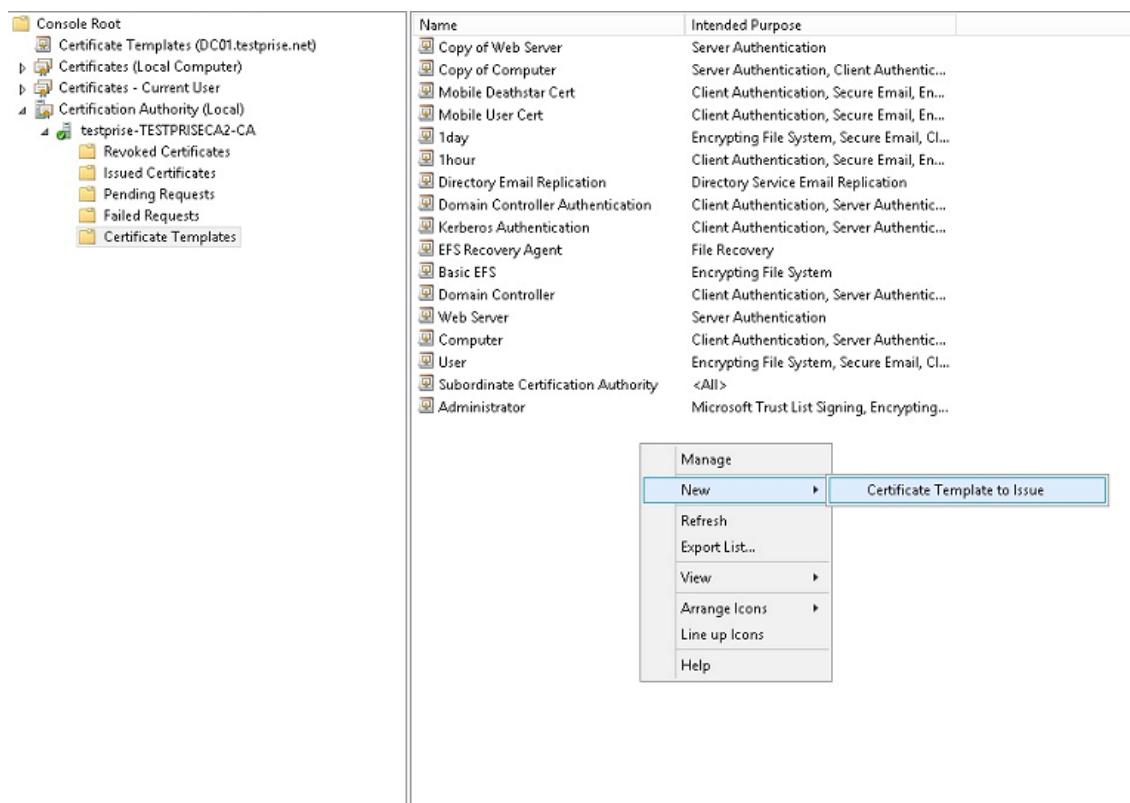


9. Em **Nome da entidade**, selecione **Fornecer na solicitação**. Aplique as alterações e, em seguida, salve.

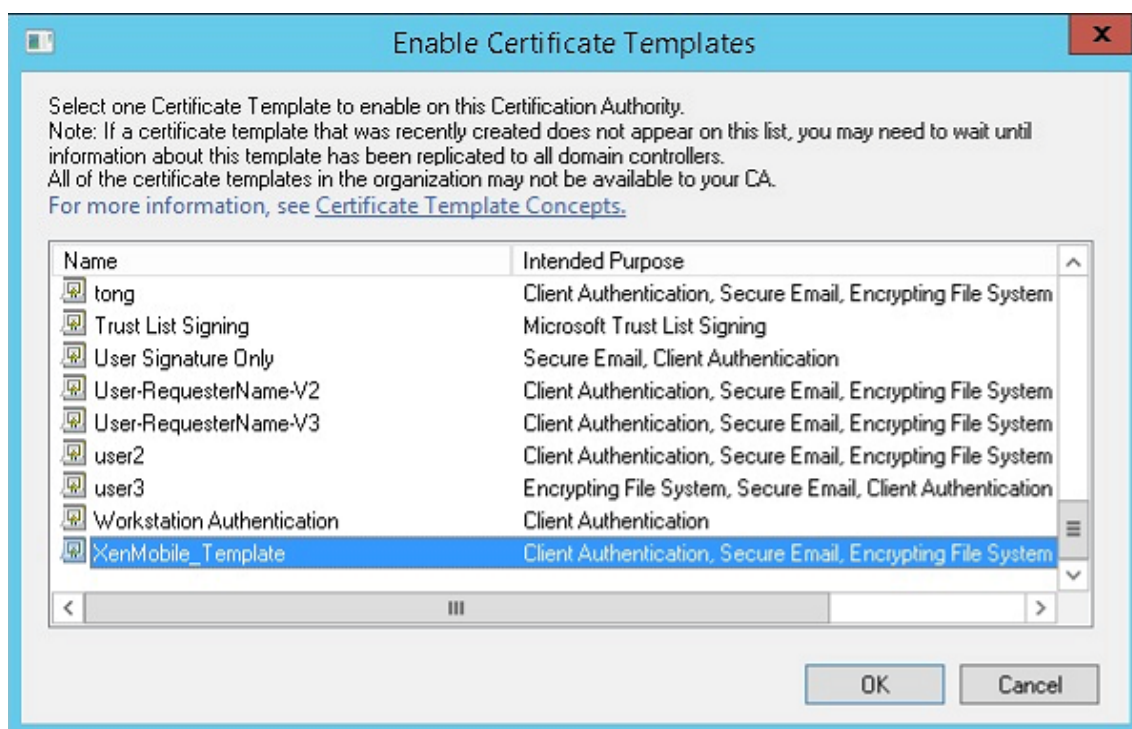


Adição de um modelo à Autoridade de Certificação

1. Vá para **Autoridade de certificação** e selecione **Modelos de certificado**.
2. Clique com o botão direito do mouse no painel direito e selecione **Novo > Modelo de certificado a ser emitido**.

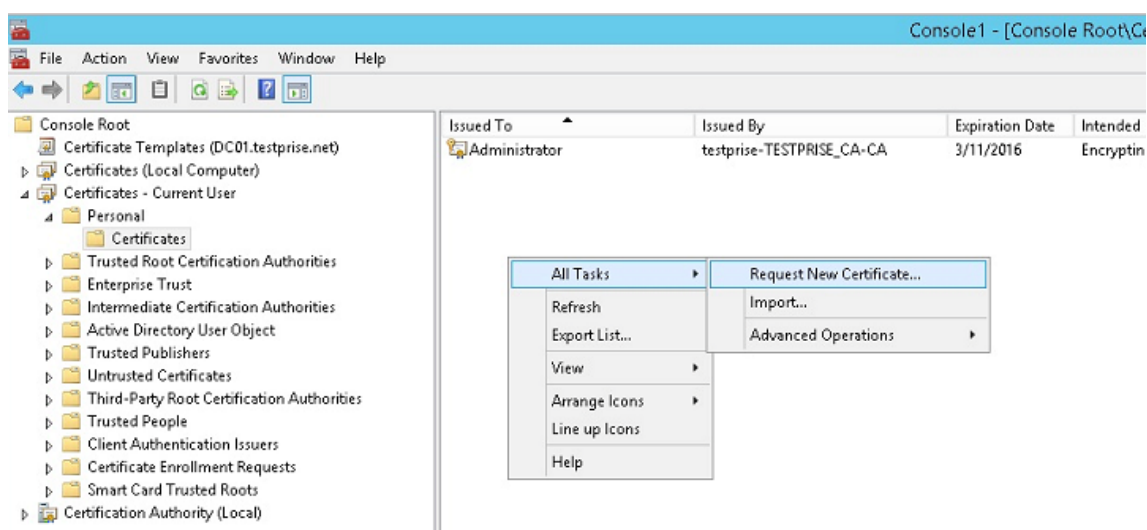


3. Selecione o modelo que você criou na etapa anterior e clique em **OK** para adicioná-lo à **Autoridade de certificação**.

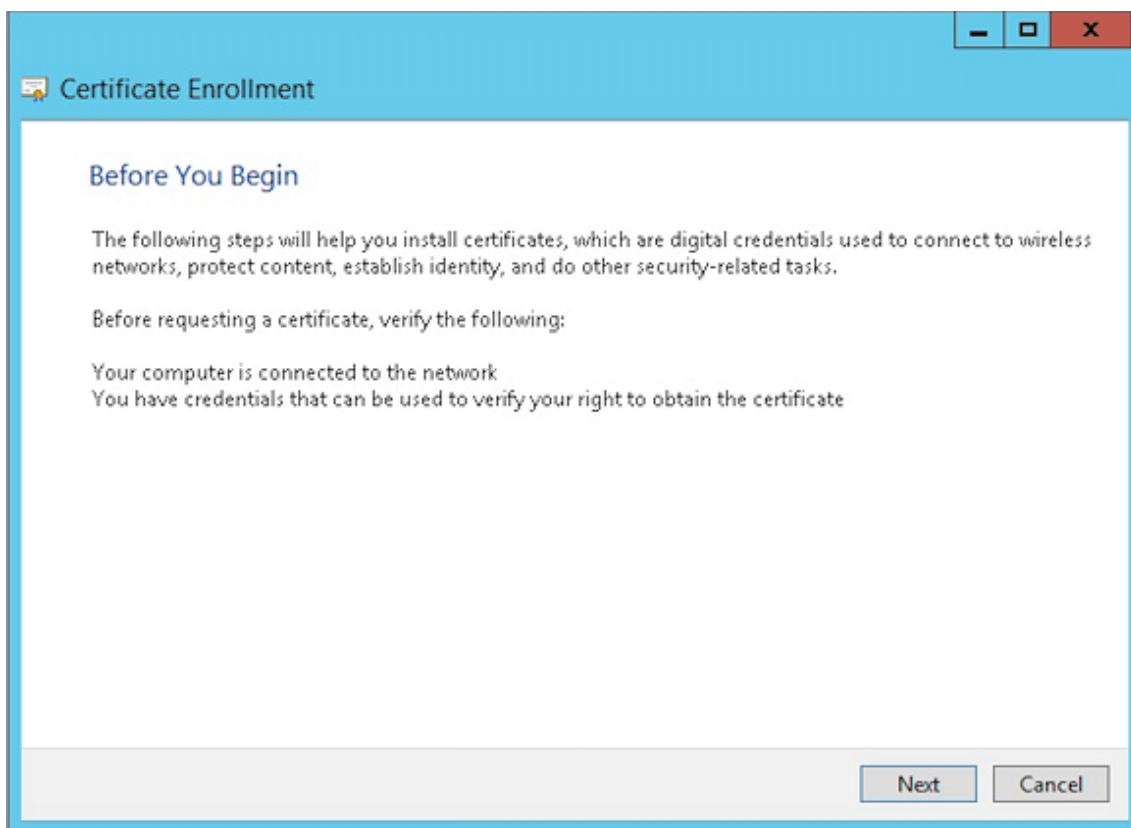


Criação de um certificado PFX do servidor de AC

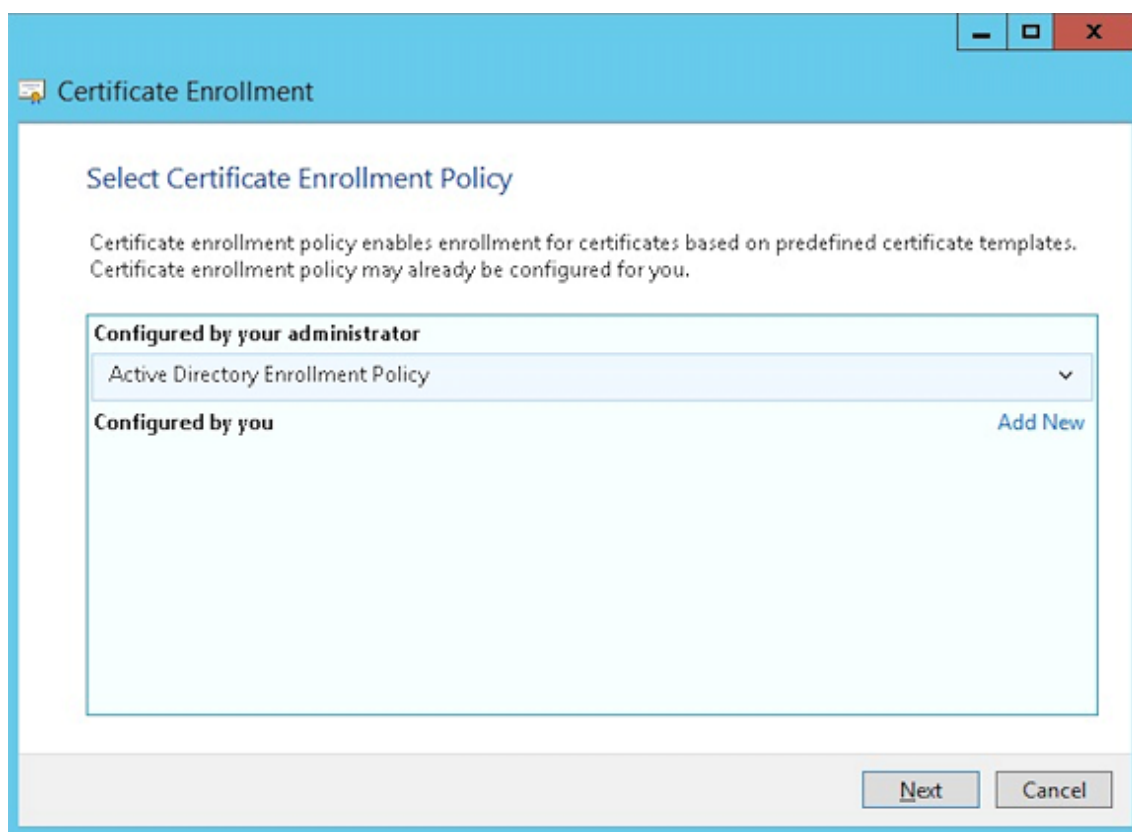
1. Crie um certificado .pfx de usuário usando a conta de serviço com a qual você fez login. O .pfx é carregado no XenMobile, que solicita um certificado de usuário em nome dos usuários que registram seus dispositivos.
2. Em **Usuário atual**, expanda **Certificados**.
3. Clique com o botão direito do mouse no painel direito e clique em **Solicitar novo certificado**.



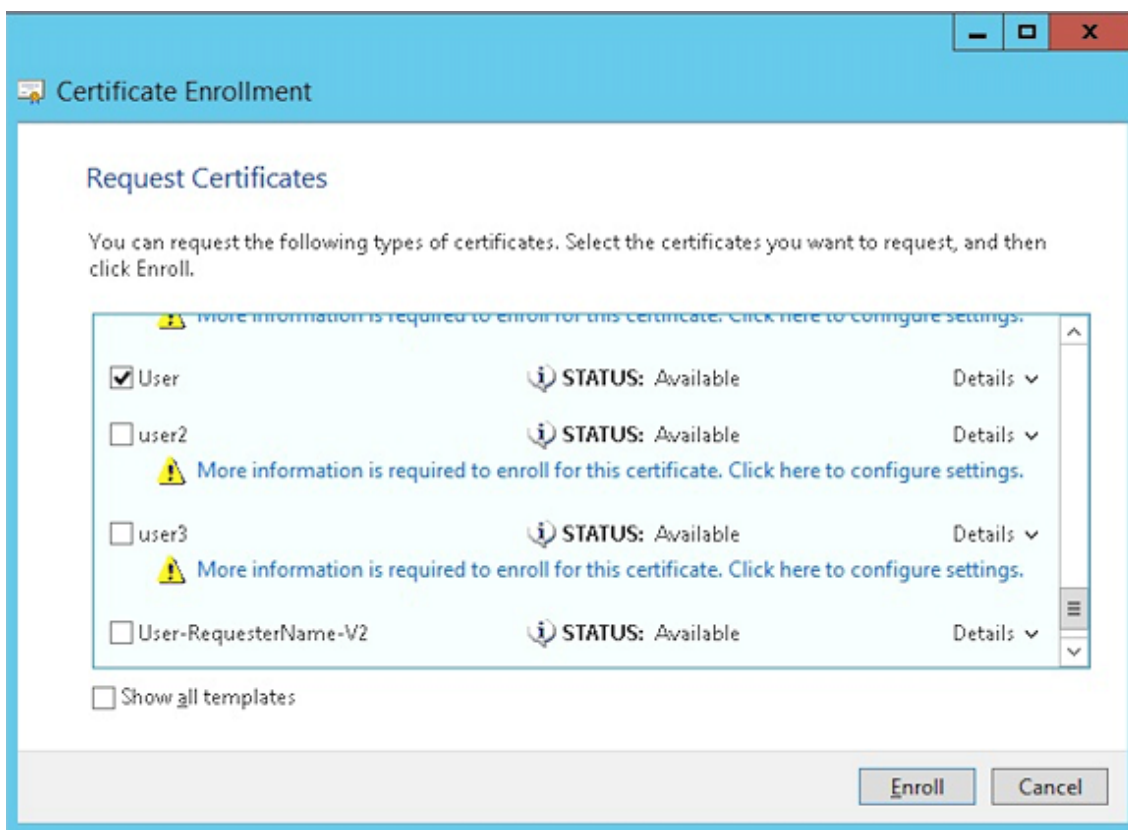
4. A tela **Registro de certificado** é exibida. Clique em **Next**.



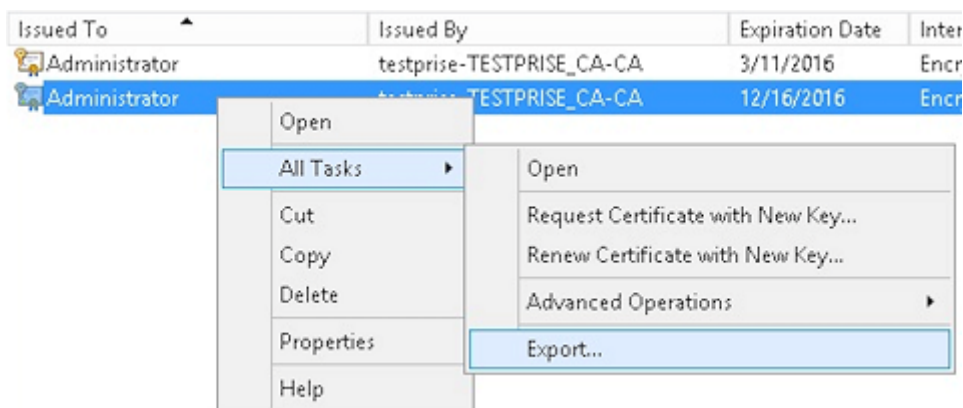
5. Selecione **Política de registro do Active Directory** e clique em **Avançar**.



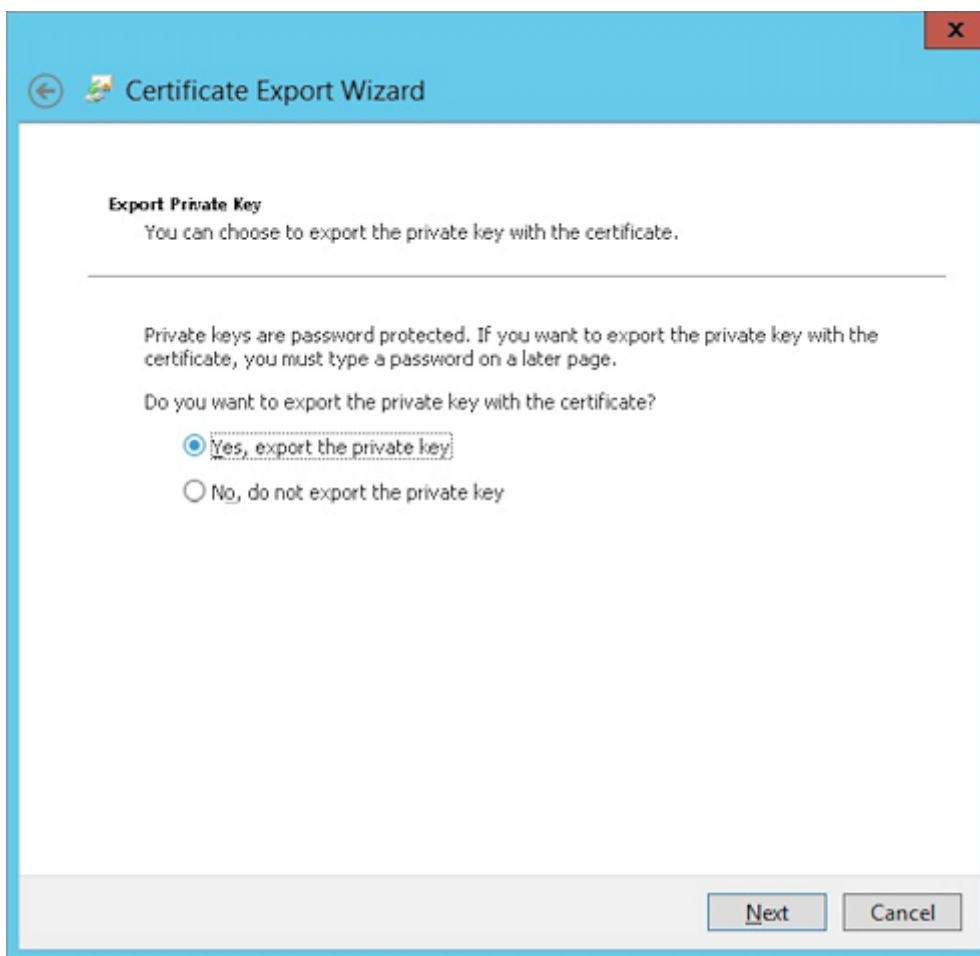
6. Selecione o modelo **Usuário** e clique em **Registrar**.



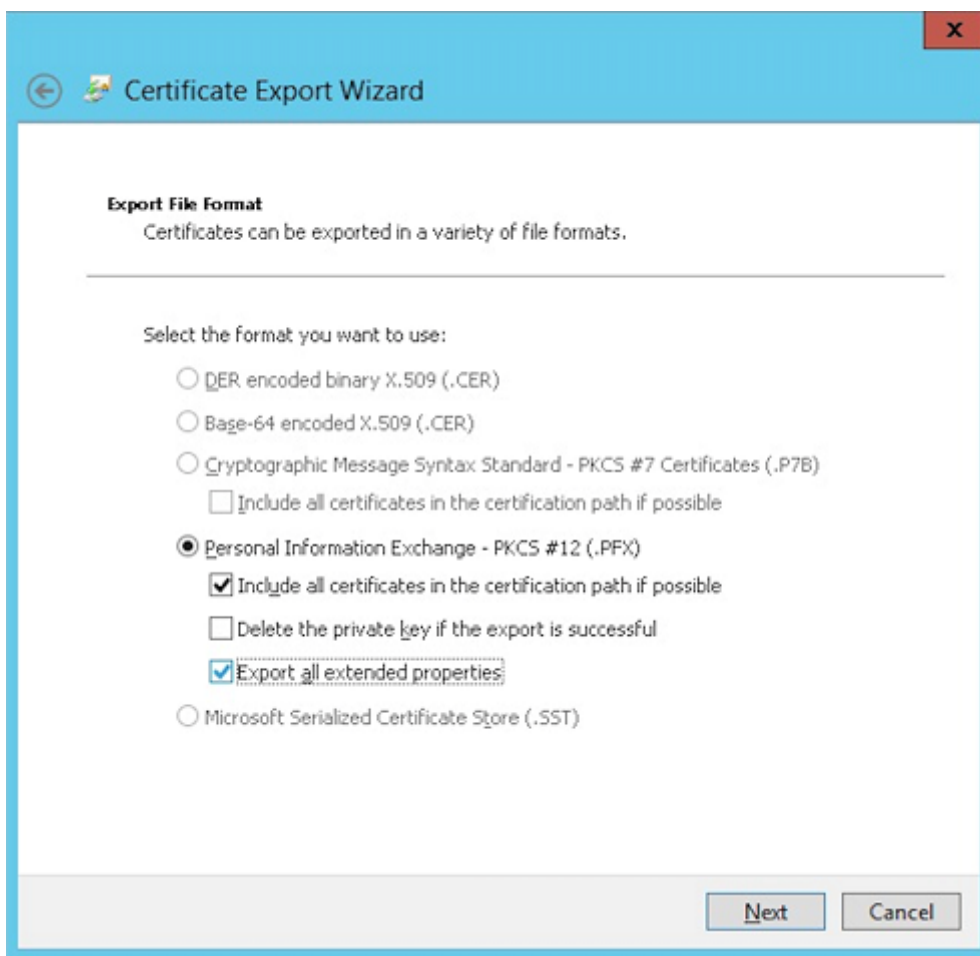
7. Exporte o arquivo .pfx criado na etapa anterior.



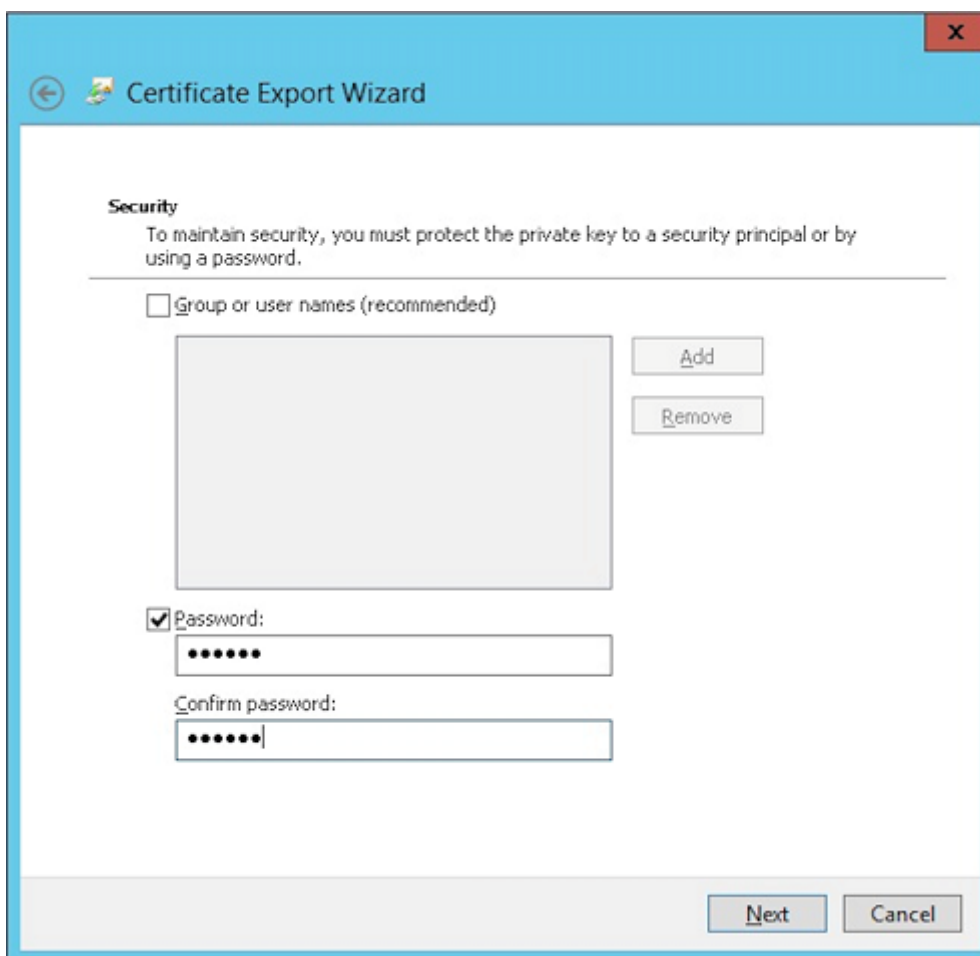
8. Clique em **Sim, exportar a chave privada.**



9. Selecione **Incluir todos os certificados no caminho de certificação, se possível** e marque a caixa de seleção **Exportar todas as propriedades estendidas**.



10. Defina uma senha para usar quando carregar o certificado para o XenMobile.



11. Salve o certificado no seu disco rígido.

Upload do certificado no XenMobile

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A tela **Configurações** é exibida.
2. Clique em **Certificados** e em **Importar**.
3. Insira os seguintes parâmetros:
 - **Importar:** Keystore
 - **Tipo de Keystore:** PKCS #12
 - **Usar como:** Servidor
 - **Arquivo de keystore:** clique em **Procurar** para selecionar o certificado `.pfx` que você criou.
 - **Senha:** insira a senha criada para esse certificado.

Import ×

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import Keystore

Keystore type PKCS#12

Use as Server

Keystore file* **Browse**

Password*

Description

Cancel **Import**

4. Clique em **Importar**.
5. Verifique se o certificado foi instalado corretamente. Um certificado instalado corretamente é exibido como um certificado de usuário.

Criação da entidade PKI de autenticação baseada em certificado

1. Em **Configurações**, vá para **Mais > Gerenciamento de certificados > Entidades PKI**.
2. Clique em **Adicionar** e em **Entidade de serviços de certificado da Microsoft**. A tela **Entidade de serviços de certificado da Microsoft: informações gerais** é exibida.
3. Insira os seguintes parâmetros:
 - **Nome:** digite qualquer nome.
 - **URL raiz do serviço de registro na Web:** <https://RootCA-URL/certsrv/> (Lembre-se de adicionar a última barra (/) ao caminho da URL.)
 - **Nome da página certnew.cer:** certnew.cer (valor padrão)
 - **certfnsh.asp:** certfnsh.asp (valor padrão)
 - **Tipo de autenticação:** certificado cliente

- **Certificado de cliente SSL:** Selecione o certificado de usuário a ser usado para emitir o certificado cliente do XenMobile.

Settings > PKI Entities > Microsoft Certificate Services Entity

Microsoft Certificate Services Entity

1 General
2 Templates
3 HTTP Parameters
4 CA Certificates

Microsoft Certificate Services Entity: General Information

Name* test

Web enrollment service root URL* https:// /certsrv/

certnew.cer page name* certnew.cer ⓘ

certfnsh.asp* certfnsh.asp ⓘ

Authentication type Client certificate ⓘ

SSL client certificate Select an option

Import SSL certificate

4. Em **Modelos**, adicione o modelo que você criou ao configurar o certificado da Microsoft. Não adicione espaços.

Microsoft Certificate Services Entity

1 General
2 Templates
3 HTTP Parameters
4 CA Certificates

Microsoft Certificate Services Entity: Templates

Specify the internal names of the templates your Microsoft CA supports. Every Credential Provider using this entity uses exactly one such template. When creating the provider, you will be prompted to select from the list defined here.

Templates

Templates*	Add
XVMTemplate	

5. Ignore os Parâmetros HTTP e, em seguida, clique em **Certificados de CA**.
6. Selecione o nome da AC raiz que corresponde ao seu ambiente. Essa AC raiz é parte da cadeia importada do certificado cliente do XenMobile.

Microsoft Certificate Services Entity

1 General
2 Templates
3 HTTP Parameters
4 CA Certificates

Microsoft Certificate Services Entity: CA Certificates

Indicate the certificates you want to use for this entity by selecting or clearing the check boxes. An entity is only valid when you select at least one certificate. Add all CA certificates that might be signers of certificates returned by this entity. Although entities may return certificates signed by different CAs, all certificates obtained through a given credential provider must be signed by the same CA. Accordingly, you will have to select one of the certificates configured here in the Distribution page of the Credential Provider setting.

<input type="checkbox"/>	Name	Serial number	Valid from	Valid to
<input checked="" type="checkbox"/>	training-AD-CA		02/22/2013	02/22/2023

7. Clique em **Salvar**.

Configuração dos provedores de credenciais

1. Em **Configurações**, vá para **Mais > Gerenciamento de certificados > Provedores de credenciais**.
2. Clique em **Add**.
3. Em **Geral**, insira os seguintes parâmetros:
 - **Nome:** digite qualquer nome.

- **Descrição:** digite uma descrição
- **Entidade de emissão:** selecione a entidade PKI criada anteriormente.
- **Método de emissão:** SIGN
- **Modelos:** selecione o modelo adicionado sob a entidade PKI.

Credential Providers	Credential Providers: General Information
1 General	You can define one or more credential providers for device certificate issuance and lifecycle. The credential providers control the certificate format (subject, key, algorithms) and the conditions for the certificate renewal or revocation, if any.
2 Certificate Signing Request	<p>Name* <input type="text" value="XenMobile_PKI"/></p> <p>Description <input type="text" value="XenMobile PKI Configuration"/></p> <p>Issuing entity <input type="text" value="MS PKI"/></p> <p>Issuing method <input type="text" value="SIGN"/></p> <p>Templates <input type="text" value="XMTemplates"/></p>
3 Distribution	
4 Revocation XenMobile	
5 Revocation PKI	
6 Renewal	

4. Clique em **Solicitação de assinatura de certificado** e insira os seguintes parâmetros:

- **Algoritmo de chave:** RSA
- **Tamanho da chave:** 2048
- **Algoritmo de assinatura:** SHA256withRSA
- **Nome de entidade:** `cn=$user.username`

Para **Nomes de entidade alternativos**, clique em **Adicionar** e insira os seguintes parâmetros:

- **Tipo:** nome UPN
- **Valor:** `$user.userprincipalname`

Credential Providers	Credential Providers: Certificate Signing Request						
1 General	Configure the parameters for the key pair that is created during issuance, as well as the parameters of the new certificate.						
2 Certificate Signing Request	<p>Key algorithm <input type="text" value="RSA"/></p> <p>Key size* <input type="text" value="2048"/></p> <p>Signature algorithm <input type="text" value="SHA1withRSA"/></p> <p>Subject name* <input type="text" value="cn=\$user.username"/></p> <p>Subject alternative names</p> <table border="1"> <thead> <tr> <th>Type</th> <th>Value*</th> <th>Add</th> </tr> </thead> <tbody> <tr> <td>User Principal name</td> <td>\$user.userprincipalname</td> <td><input type="button" value="Add"/></td> </tr> </tbody> </table>	Type	Value*	Add	User Principal name	\$user.userprincipalname	<input type="button" value="Add"/>
Type	Value*	Add					
User Principal name	\$user.userprincipalname	<input type="button" value="Add"/>					
3 Distribution							
4 Revocation XenMobile							
5 Revocation PKI							
6 Renewal							

5. Clique em **Distribuição** e insira os seguintes parâmetros:

- **Emissão de certificado de CA:** selecione a CA emissora que assinou o Certificado cliente do XenMobile.
- **Selecionar modo de distribuição:** selecione **Preferir modo centralizado: geração de chaves do lado do servidor.**

Credential Providers	Credential Providers: Distribution
1 General	Issuing CA certificate: ON-training-AD-CA, Serial: [dropdown]
2 Certificate Signing Request	Select distribution mode: <ul style="list-style-type: none"> <input checked="" type="radio"/> Prefer centralized: Server-side key generation <input type="radio"/> Prefer distributed: Device-side key generation <input type="radio"/> Only distributed: Device-side key generation
3 Distribution	
4 Revocation XenMobile	

6. Para as duas próximas seções, **Revogação XenMobile** e **Revogação PKI**, defina os parâmetros conforme necessário. Neste exemplo, as duas opções são ignoradas.
7. Clique em **Renovação**.
8. Para **Renovar os certificados quando eles expirarem**, selecione **I**.
9. Deixe todas as outras configurações como o padrão ou altere-as conforme necessário.

Credential Providers	Credential Providers: Renewal
1 General	Renew certificates when they expire: <input checked="" type="checkbox"/> ON
2 Certificate Signing Request	Renew when the certificate comes within*: 30 days of expiration
3 Distribution	<input type="checkbox"/> Do not renew certificates that have already expired
4 Revocation XenMobile	Send notification: <input type="checkbox"/> OFF
5 Revocation PKI	Notify when the certificate nears expiration: <input type="checkbox"/> OFF
6 Renewal	

10. Clique em **Salvar**.

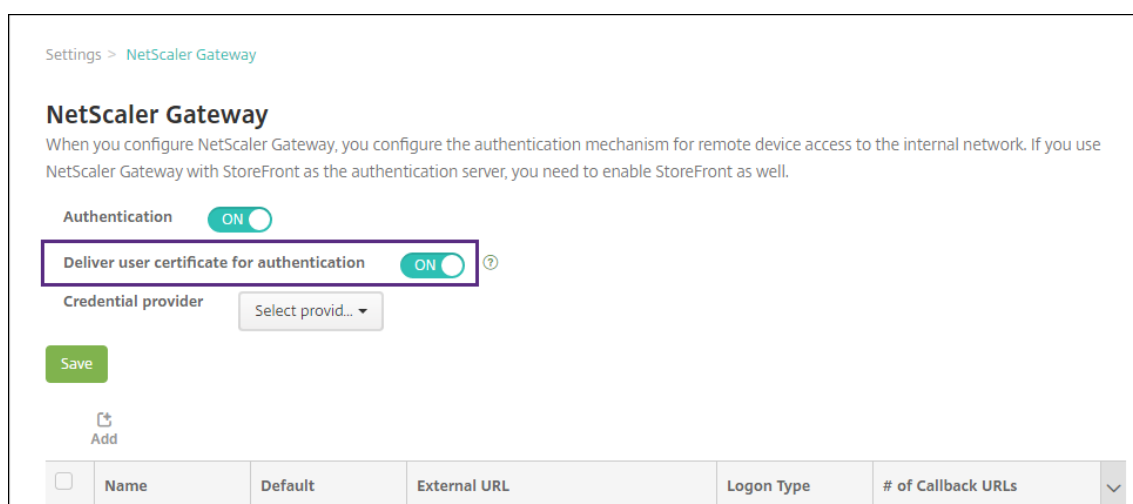
Configuração do Secure Mail para usar a autenticação baseada em certificado

Quando você adicionar o Secure Mail ao XenMobile, defina as configurações do Exchange em **Configurações de Aplicativo**.

MDX	App Interaction	App Settings
1 App Information	Explicit logoff notification: Shared devices only	
2 Platform		WorxMail Exchange Server: mail.testlab.com:9443
<input checked="" type="checkbox"/> iOS		WorxMail user domain: testlab.com
<input checked="" type="checkbox"/> Android		Background network services: mail.testlab.com:443.ap-southeast-1.pushre
<input checked="" type="checkbox"/> Windows Phone		Background services ticket expiration: 168
3 Approvals (optional)		
4 Delivery Group Assignments (optional)		

Configuração da entrega de certificado do Citrix ADC no XenMobile

1. Faça login no console XenMobile e clique no ícone de engrenagem no canto superior direito. A tela **Configurações** é exibida.
2. Em **Servidor**, clique em **Citrix Gateway**.
3. Se o Citrix Gateway ainda não foi adicionado, clique em **Adicionar** e especifique as configurações:
 - **URL externa:** `https://YourCitrixGatewayURL`
 - **Tipo de login:** Certificado e domínio
 - **Senha obrigatória:** desativado
 - **Definir como padrão:** ativado
4. Para **Entregar certificado de usuário para autenticação**, selecione **I**.



5. Para **Provedor de credenciais**, selecione um provedor e clique em **Salvar**.
6. Para usar atributos de sAMAccount nos certificados de usuário como alternativa para o nome UPN, configure o conector LDAP no XenMobile da seguinte maneira: vá para **Configurações > LDAP**, selecione o diretório e clique em **Editar** e selecione **sAMAccountName** em **Pesquisa de usuário por**.

User base DN*	<input type="text"/>	?
Group base DN*	<input type="text"/>	?
User ID*	<input type="text"/>	
Password*	<input type="password"/>	
Domain alias*	<input type="text"/>	
XenMobile Lockout Limit	<input type="text" value="0"/>	?
XenMobile Lockout Time	<input type="text" value="1"/>	?
Global Catalog TCP Port	<input type="text" value="3268"/>	?
Global Catalog Root Context	<input type="text" value="dc=example,dc=com"/>	?
User search by	<input type="text" value="sAMAccountName"/>	
Use secure connection	<input type="checkbox" value="NO"/>	

Ativar o PIN da Citrix e o cache de senha de usuário

Para ativar o PIN da Citrix e a senha do usuário em cache, vá para **Configurações > Propriedades do Cliente** e assinale as caixas de seleção para **Ativar PIN da Citrix** e **Ativar armazenamento em cache da senha do usuário**. Para obter mais informações, consulte [Propriedades do cliente](#).

Criação de uma política de Hub Empresarial para o Windows Phone

Para dispositivos Windows Phone, você deve criar uma política de dispositivo de Hub Empresarial para fornecer o arquivo AETX e o Secure Hub cliente.

Nota:

Certifique-se de que os arquivos AETX e Secure Hub usem:

- O mesmo certificado corporativo do provedor de certificados.
- Mesmo ID de Fornecedor da conta de desenvolvedor da Windows Store.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**.

2. Clique em **Adicionar** e, em **Mais > Agente XenMobile**, clique em **Hub empresarial**.
3. Após atribuir um nome à política, selecione o arquivo **.AETX** correto e o aplicativo Secure Hub assinado para o hub empresarial.

Enterprise Hub Policy	Policy Information
1 Policy Info	To create the Enterprise Hub policy for Windows Phone app distribution through the Enterprise Hub Company store, you need the AET (.aetx) signing certificate from Symantec. You also need to have obtained and signed the Citrix Company Hub app using the Microsoft app signing tool (XapSignTool.exe).
2 Platforms	Upload .aetx file <input type="text"/> <input type="button" value="Browse"/>
<input checked="" type="checkbox"/> Windows Phone	Upload signed Enterprise Hub app <input type="text"/> <input type="button" value="Browse"/>
3 Assignment	

4. Atribua a política a grupos de entrega e salve-a.

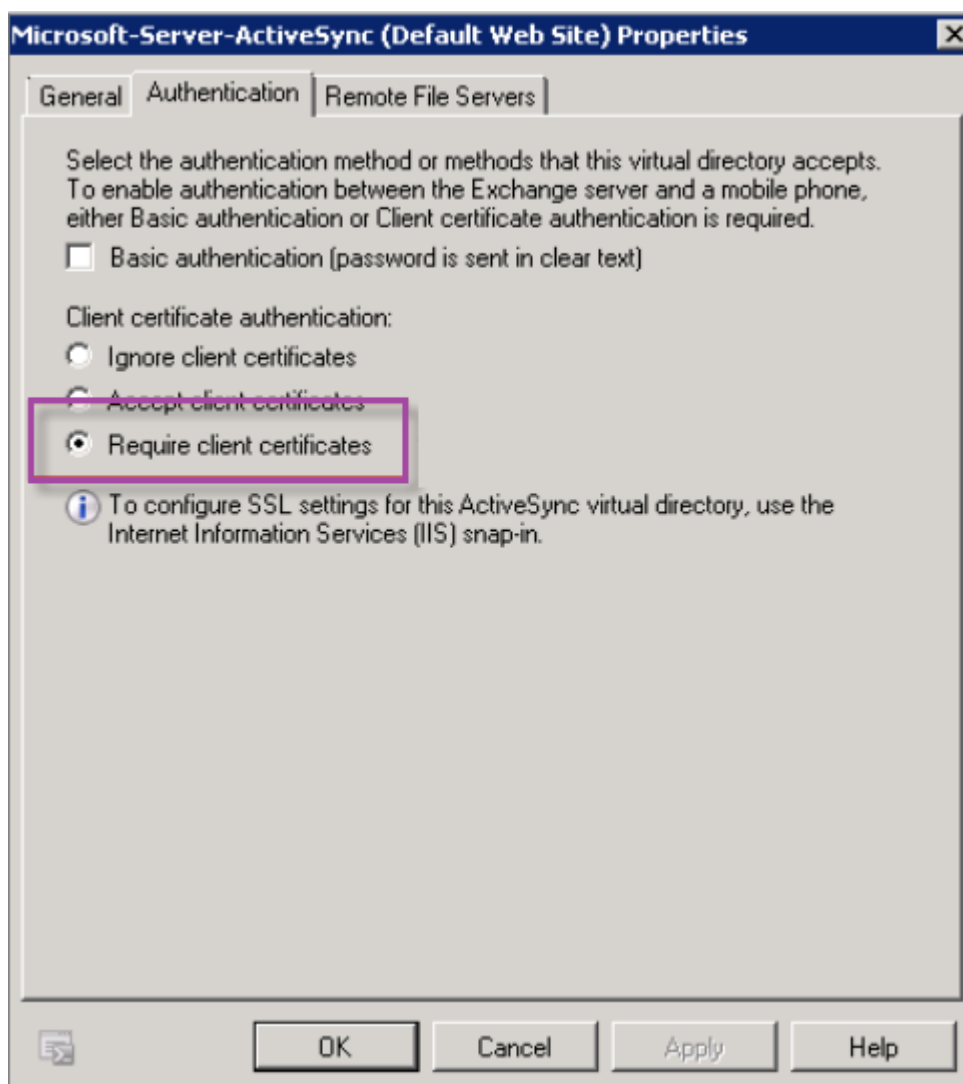
Solução de problemas da sua configuração de certificado cliente

Após uma configuração com êxito da configuração anterior mais a configuração do Citrix Gateway, o usuário fluxo de trabalho é o seguinte:

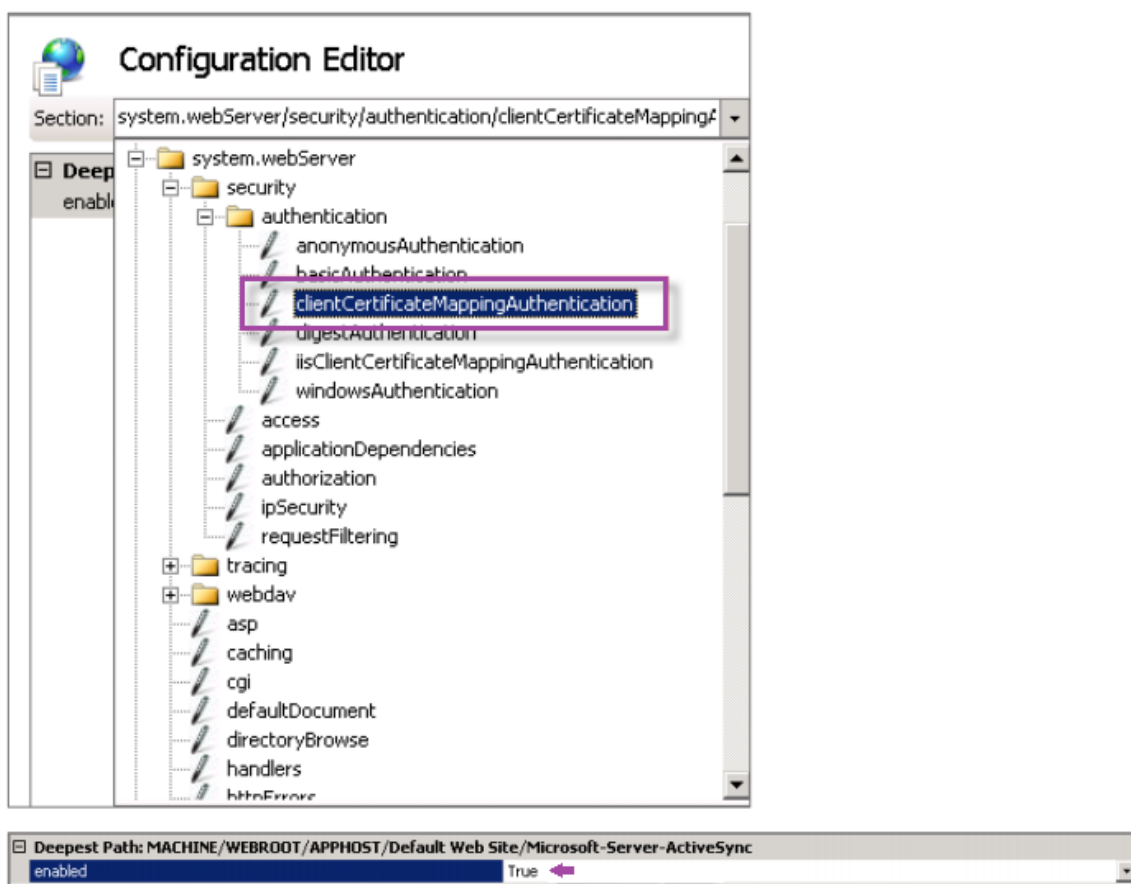
1. Os usuários registram seus dispositivos móveis.
2. O XenMobile solicita que os usuários criem um PIN da Citrix.
3. Os usuários são redirecionados para a XenMobile Store.
4. Quando os usuários iniciam o Secure Mail, o XenMobile não solicita credenciais de usuário para a configuração da caixa de correio. Em vez disso, o Secure Mail solicita o certificado de cliente do Secure Hub e o envia para o Microsoft Exchange Server para autenticação. Se o XenMobile solicitar credenciais quando os usuários iniciarem o Secure Mail verifique a sua configuração.

Se os usuários puderem baixar e instalar o Secure Mail, mas durante a configuração da caixa de correio o Secure Mail não termina a configuração:

1. Se o Microsoft Exchange Server ActiveSync usa certificados de servidor SSL privados para proteger o tráfego, verifique se os certificados raiz/intermediário estão instalados no dispositivo móvel.
2. Verifique se o tipo de autenticação selecionado para o ActiveSync é **Exigir certificados de cliente**.



3. No Microsoft Exchange Server, verifique o site **Microsoft-Server-ActiveSync** para confirmar que a autenticação de mapeamento de certificado de cliente esteja ativada. Por padrão, a autenticação de mapeamento de certificado de cliente está desativada. A opção está sob **Editor de Configurações > Segurança > Autenticação**.



Nota: depois de selecionar **True**, clique em **Aplicar** para que as alterações tenham efeito.

4. Verifique as configurações do Citrix Gateway no console XenMobile: certifique-se de que **Entregar certificado de usuário para autenticação** esteja **Ativado** e que o **Provedor de credenciais** tenha o perfil correto selecionado.

Para determinar se o certificado de cliente foi entregue a um dispositivo móvel

1. No console XenMobile, vá para **Gerenciar > Dispositivos** e selecione o dispositivo.
2. Clique em **Editar** ou **Mostrar mais**.
3. Vá para a seção **Grupos de entrega** e procure esta entrada:

Credenciais do Citrix Gateway: Credencial solicitada, CertId=

Para validar se a negociação do certificado de cliente está habilitada

1. Execute este comando `netsh` para mostrar a configuração de certificado SSL que está vinculada ao website do IIS:

```
netsh http show sslcert
```

2. Se o valor de **Negociar certificado de cliente** for **Desativado**, execute o seguinte comando para ativá-lo:

```
netsh http delete sslcert ipport=0.0.0.0:443
```

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=cert_hash appid={  
  app_id } certstorename=store_name verifyclientcertrevocation=Enable  
  VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable  
  clientcertnegotiation=Enable
```

Por exemplo:

```
netsh http add sslcert ipport=0.0.0.0:443 certhash=609da5df280d1f54a7deb714fb2c54  
  appid={ 4dc3e181-e14b-4a21-b022-59fc669b0914 } certstorename=ExampleCertStoreName  
  verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly  
  =Disable UsageCheck=Enable clientcertnegotiation=Enable
```

Se não for possível fornecer certificados raiz/intermediários a um dispositivo Windows Phone 8.1 por meio do XenMobile:

- Envie arquivos de certificados raiz/intermediário (.cer) por email ao dispositivo Windows Phone 8.1 e instale-os diretamente.

Se o Secure Mail não for instalado com êxito no Windows Phone 8.1, verifique o seguinte:

- O arquivo Application Enrollment Token (.AETX) é entregue por meio do XenMobile usando a política de dispositivo de hub empresarial.
- O arquivo Application Enrollment Token foi criado usando o mesmo certificado empresarial do provedor de certificados usado para preparar o Secure Mail e assinar aplicativos do Secure Hub.
- O mesmo ID de Fornecedor é usado para assinar e preparar o Secure Hub, o Secure Mail e o Application Enrollment Token.

Entidades PKI

April 1, 2021

Uma configuração de entidade Infraestrutura de Chave Pública (PKI) do XenMobile representa um componente que realiza operações reais da PKI (emissão, revogação e informações de status). Esses componentes são internos ou externos ao XenMobile. Os componentes internos são conhecidos como discricionários. Os componentes externos fazem parte da sua infraestrutura corporativa.

O XenMobile é compatível com os seguintes tipos de entidades PKI:

- PKIs Genéricas (GPKIs)

O suporte do XenMobile Server GPKI inclui PKI gerenciada da DigiCert.

- Serviços de Certificado da Microsoft
- Autoridades de Certificação (CAs) Discricionárias

O XenMobile é compatível com os seguintes servidores de AC:

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Conceitos de PKI comuns

Independentemente do tipo, cada entidade PKI tem um subconjunto dos seguintes recursos:

- **Assinar:** emitir um novo certificado com base em uma Solicitação de Assinatura de Certificado (CSR).
- **Obter:** recuperar um certificado e um par de chaves existentes.
- **Revogar:** revogar um certificado cliente.

Sobre certificados AC

Quando você configura uma entidade PKI, indique ao XenMobile qual certificado AC será o signatário dos certificados emitidos por (ou recuperados de) essa entidade. Essa entidade PKI pode retornar certificados (obtidos ou assinados recentemente) assinados por qualquer número de ACs diferentes.

Forneça o certificado de cada uma dessas CAs como parte da configuração da entidade PKI. Para fazer isso, carregue os certificados no XenMobile e faça referência a eles na entidade PKI. Para CAs discricionárias, o certificado é, implicitamente, o certificado de AC de assinatura. Para entidades externas, você deve especificar o certificado manualmente.

Importante:

Quando você cria um modelo de Entidade de Serviços de Certificado Microsoft, evite possíveis problemas de autenticação com dispositivos registrados: não use caracteres especiais no nome do modelo. Por exemplo, não use: ! : \$ () ## % + * ~ ? | { } []

PKI Genérica

O protocolo PKI Genérica (GPKI) é um protocolo proprietário do XenMobile em execução em uma camada do Serviço Web SOAP para fins de interface uniforme com várias soluções de PKI. O protocolo GPKI define as três operações de PKI fundamentais:

- **Assinar:** o adaptador pode receber CSRs, transmiti-las para a PKI e retornar os certificados recém-assinados.

- **Obter:** o adaptador pode recuperar (restaurar) certificados e pares de chaves existentes (dependendo dos parâmetros de entrada) da PKI.
- **Revogar:** o adaptador pode fazer com que a PKI revogue um determinado certificado.

O receptor do protocolo GPKI é o adaptador GPKI. O adaptador converte as operações fundamentais no tipo específico de PKI para o qual foi criado. Por exemplo, há adaptadores GPKI para RSA e Entrust.

O adaptador GPKI, como um ponto de extremidade dos Serviços da Web SOAP, publica uma definição de Linguagem de Descrição de Serviços da Web (WSDL) autodescritiva. Criar uma entidade PKI GPKI equivale a fornecer ao XenMobile essa definição WSDL, por meio de uma URL ou mediante o carregamento do arquivo em si.

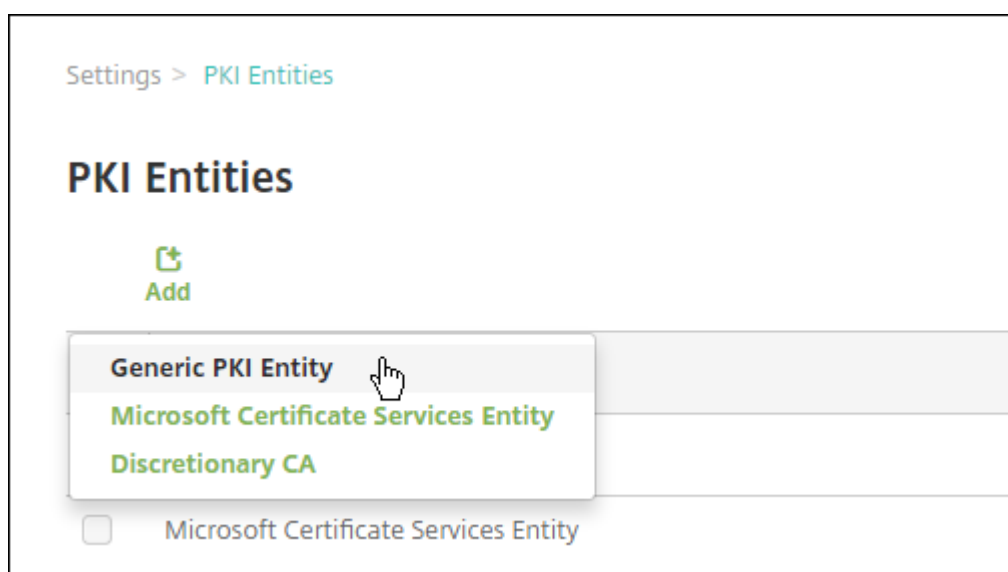
O suporte a cada uma das operações de PKI em um adaptador é opcional. Se um adaptador der suporte a uma determinada operação, considera-se que tem a capacidade correspondente (assinar, obter ou revogar). Cada um desses recursos pode ser associado a um conjunto de parâmetros de usuário.

Os parâmetros de usuário são parâmetros que o adaptador GPKI define para uma operação específica e cujos valores você precisa fornecer ao XenMobile. O XenMobile analisa o arquivo WSDL para determinar quais operações o adaptador tem e quais parâmetros o adaptador exige para cada uma dessas operações. Se você preferir, use a autenticação de cliente SSL para proteger a conexão entre o XenMobile e o adaptador GPKI.

Para adicionar uma PKI genérica

1. No console XenMobile, clique em **Configurações > Entidades PKI**.
2. Na página **Entidades PKI**, clique em **Adicionar**.

É exibido um menu de tipos de entidade PKI.



3. Clique em **Entidade PKI genérica**.

A página Entidade PKI genérica: Informações gerais é exibida.

4. Na página **Entidade PKI genérica: Informações gerais**, faça o seguinte:

- **Nome:** digite um nome descritivo para a entidade PKI.
- **URL WSDL:** digite a localização do WSDL que descreve o adaptador.
- **Tipo de autenticação:** clique no método de autenticação que você deseja usar.
- **Nenhum**
- **HTTP básico:** forneça o nome do usuário e a senha necessários para se conectar ao adaptador.
- **Certificado cliente:** selecione o certificado de cliente SSL correto.

5. Clique em **Avançar**.

A página Entidade PKI genérica: Recursos do adaptador é exibida.

6. Na página **Entidade PKI genérica: Recursos do adaptador**, revise as capacidades e os parâmetros associados ao adaptador e clique em **Avançar**.

A página **Entidade PKI genérica: Emissão de certificados AC** é exibida.

7. Na página Entidade PKI genérica: Emissão de certificados AC, selecione os certificados que você deseja usar para a entidade.

Embora as entidades possam retornar certificados assinados por diferentes ACs, a mesma AC deve assinar todos os certificados obtidos por meio de um determinado provedor de certificados. Da mesma forma, quando você configurar a definição **Provedor de credenciais**, na página **Distribuição**, selecione um dos certificados configurados aqui.

8. Clique em **Salvar**.

A entidade é exibida na tabela Entidades PKI.

PKI gerenciada da DigiCert

O suporte do XenMobile Server GPKI inclui PKI gerenciada da DigiCert, também chamada MPKI. Esta seção descreve como configurar o Windows Server e o XenMobile Server para PKI gerenciada da DigiCert.

Pré-requisitos

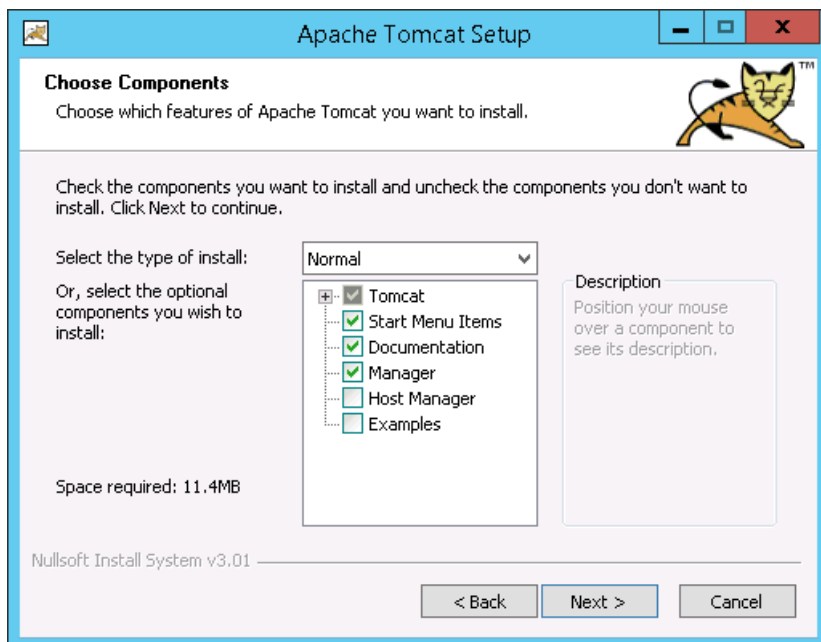
- Acesso a infraestrutura de PKI gerenciada da DigiCert
- Windows Server 2012 R2 com os seguintes componentes instalados, conforme descrito neste artigo:
 - Java
 - Apache Tomcat
 - Cliente PKI DigiCert
 - Portecle
- Acesso ao site de downloads do XenMobile

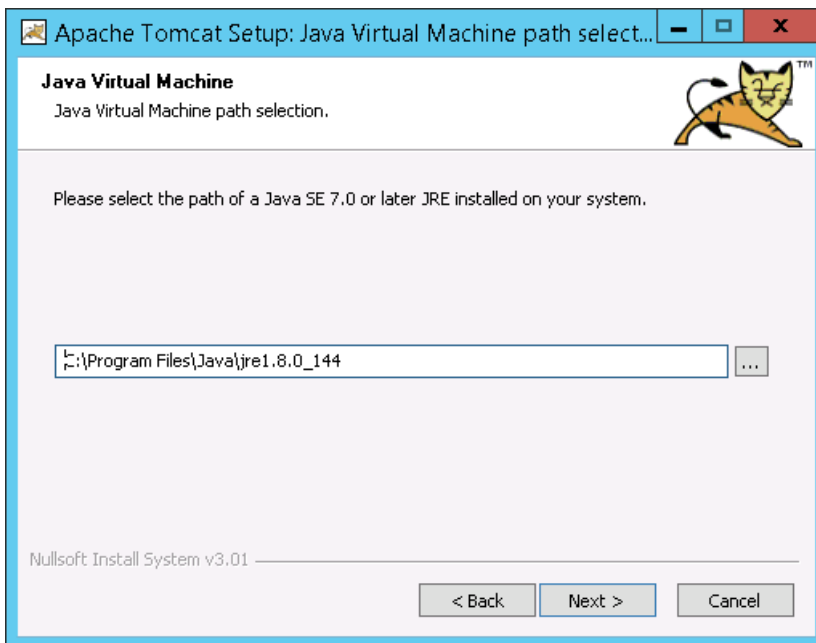
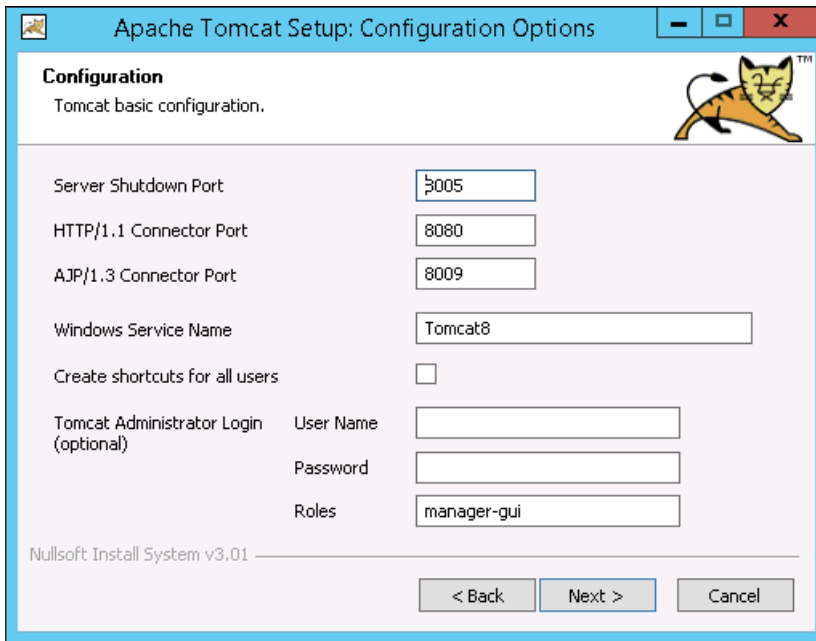
Instalar o Java no Windows Server

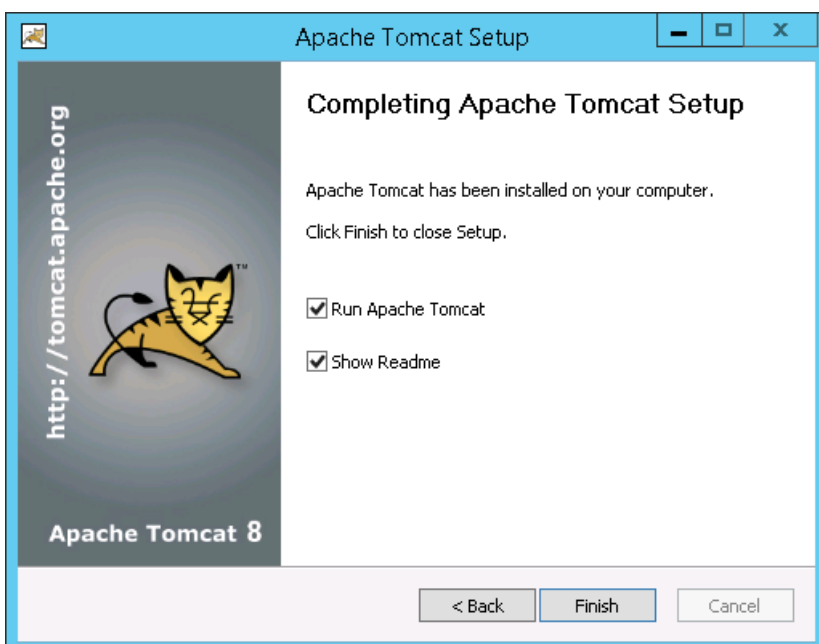
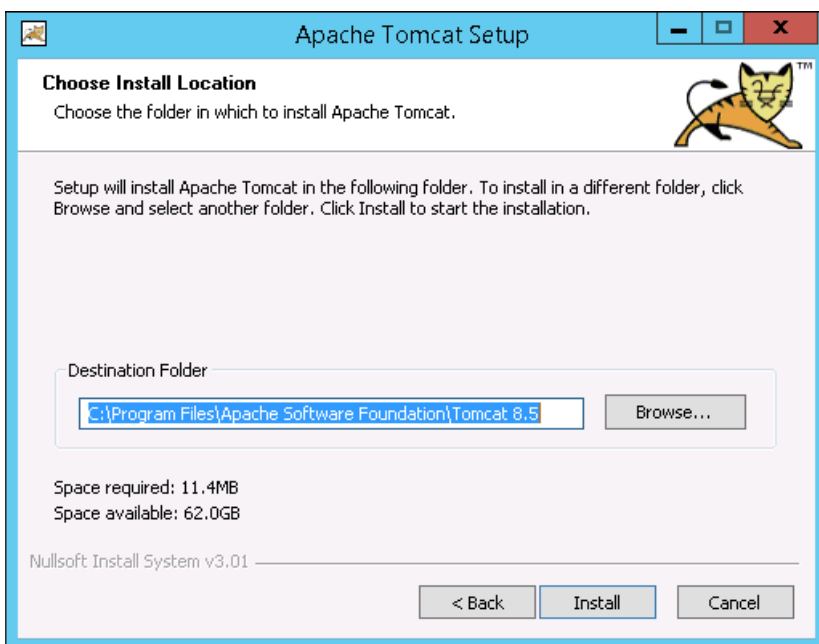
Faça o download do Java em https://java.com/en/download/faq/java_win64bit.xml e instale-o. Na caixa de diálogo Aviso de segurança, clique em **Executar**.

Instalar o Apache Tomcat no Windows Server

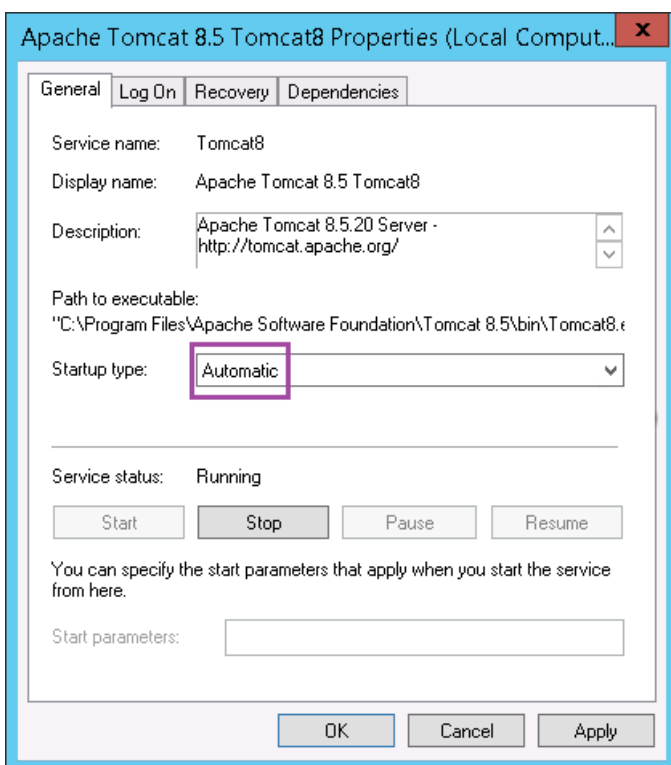
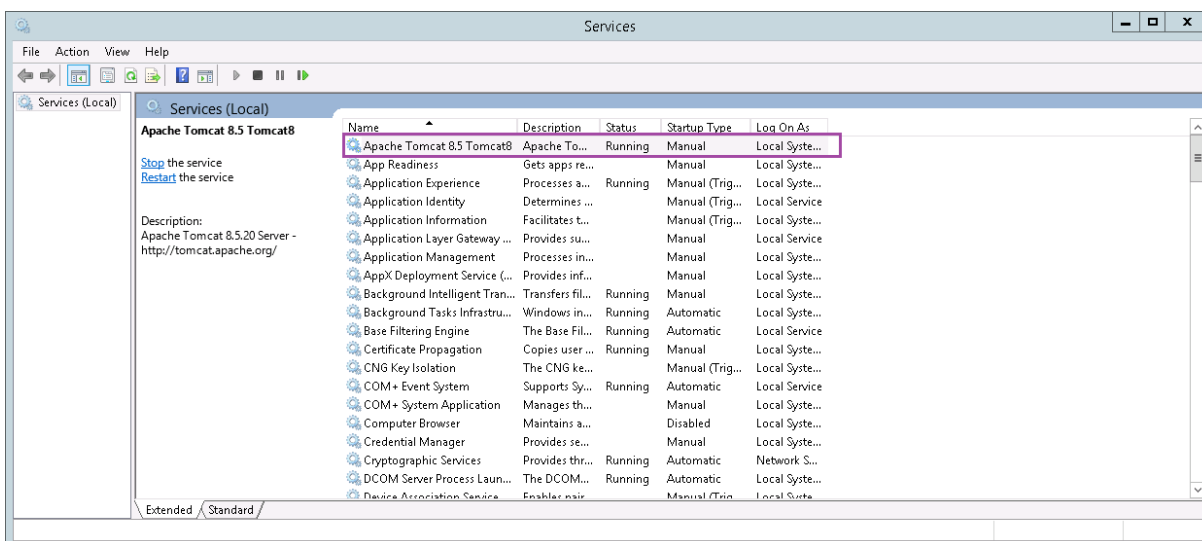
Baixe o instalador de serviços do Windows Apache Tomcat de 32/64 bits em <https://tomcat.apache.org/download-80.cgi> e depois instale-o. Na caixa de diálogo Aviso de segurança, clique em **Executar**. Complete a configuração do Apache Tomcat, usando os seguintes exemplos como um guia.





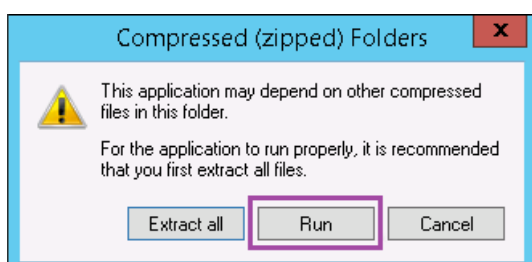
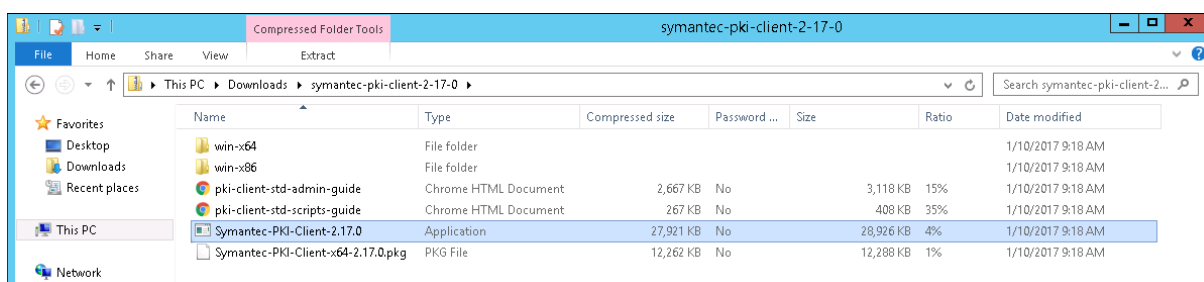


Em seguida, vá até Windows Services e altere o **Tipo de inicialização** de **Manual** para **Automático**.



Instalar o cliente DigiCert PKI no Windows Server

Baixe o instalador a partir do console do PKI Manager. Se você não tem acesso ao console, baixe o instalador a partir da página de suporte da DigiCert [Como baixar o DigiCert PKI Client](#). Descompacte e execute o instalador.



Na caixa de diálogo Aviso de segurança, clique em **Executar**. Siga as instruções no instalador para concluir a instalação. Quando a instalação for concluída, ele solicitará que você reinicie.

Instalar o Portecle no Windows Server

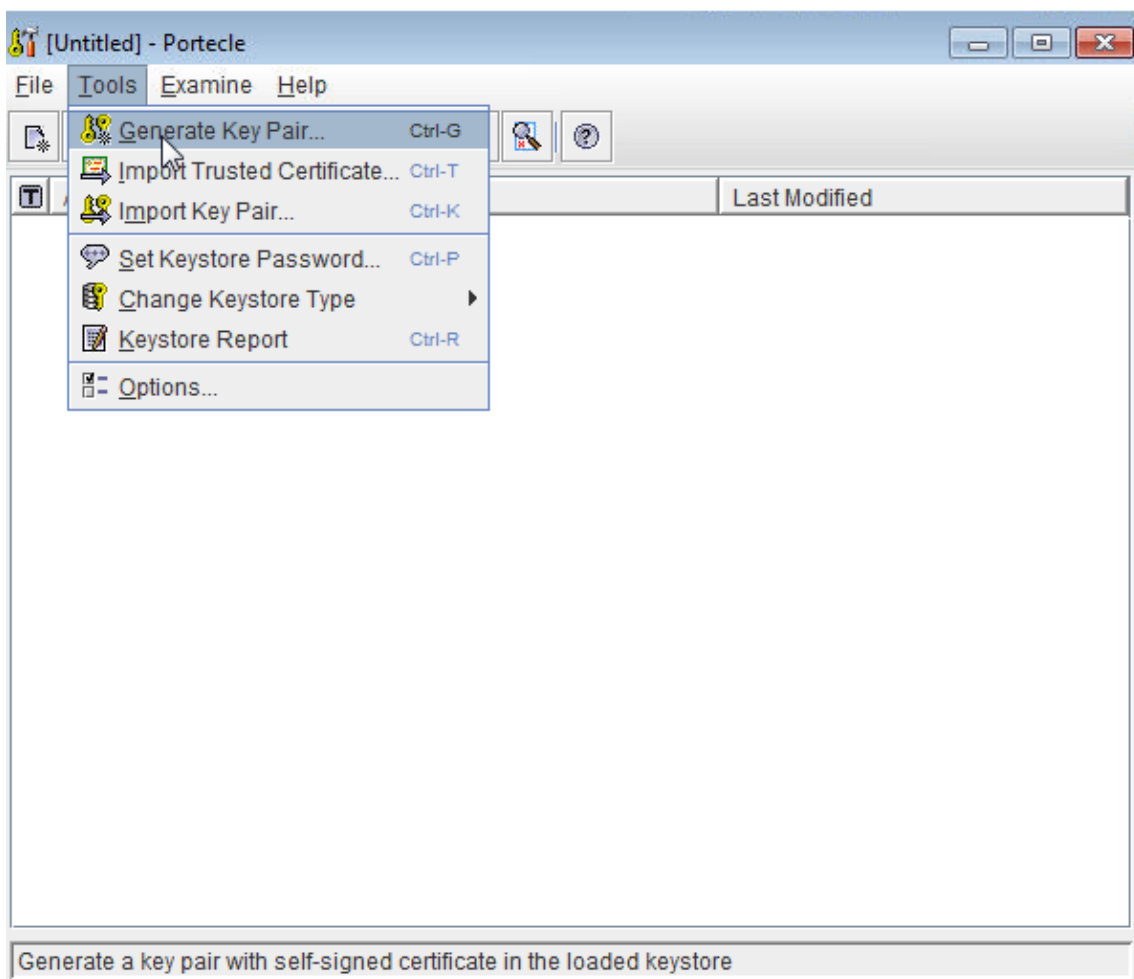
Baixe o instalador de <https://sourceforge.net/projects/portecleinstall/files/> e depois descompacte e execute o instalador.

Gere o certificado de autoridade de registro (RA) para o PKI gerenciado da DigiCert

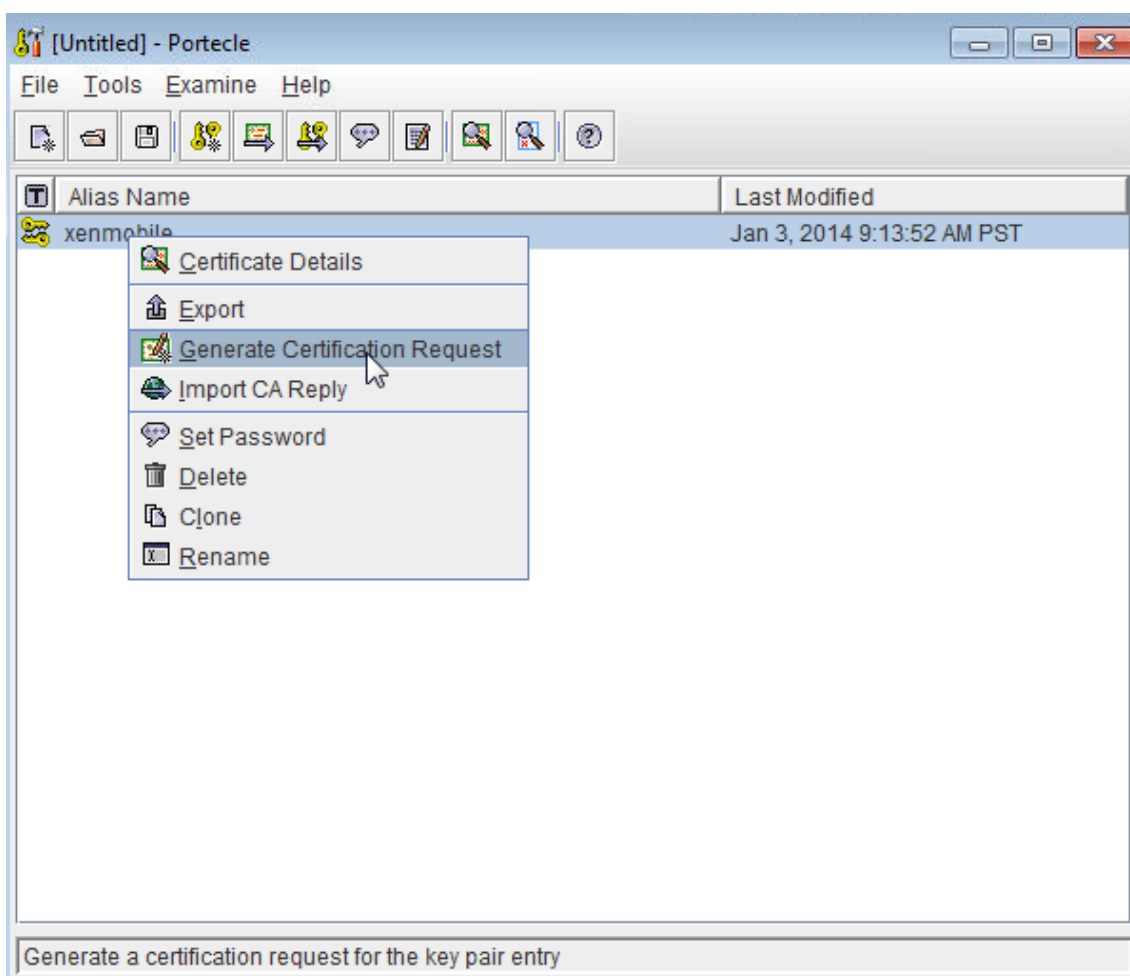
O keystore para autenticação de certificado de cliente está contido em um certificado de autoridade de registro (RA), chamado RA.jks. As etapas a seguir descrevem como gerar esse certificado usando Portecle. Você também pode gerar o certificado de RA usando a interface de linha de comando Java.

Este artigo também descreve como carregar o RA e os certificados públicos.

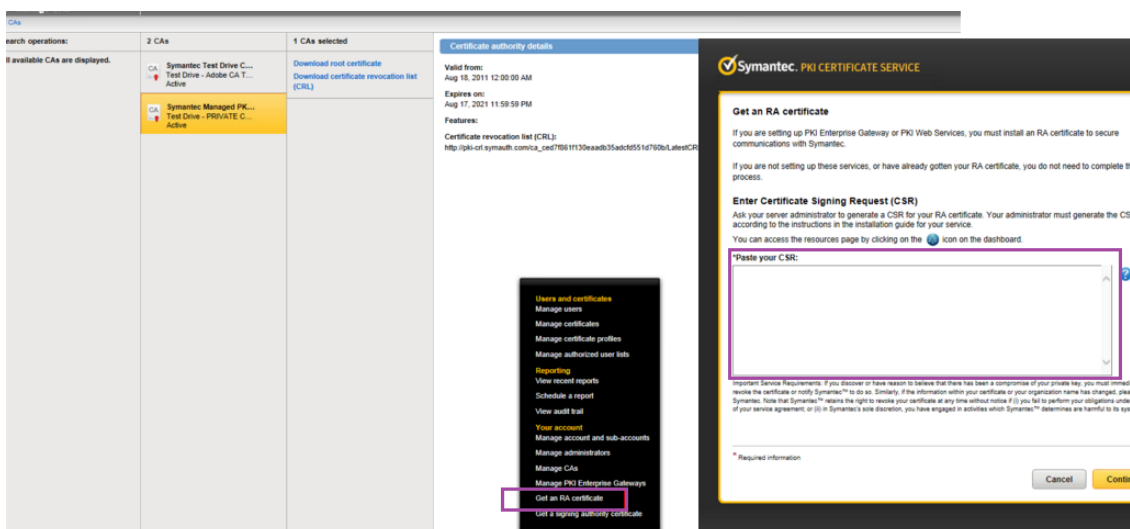
1. No Portecle, vá para **Tools > Generate Key Pair**, forneça as informações necessárias e gere um par de chaves.



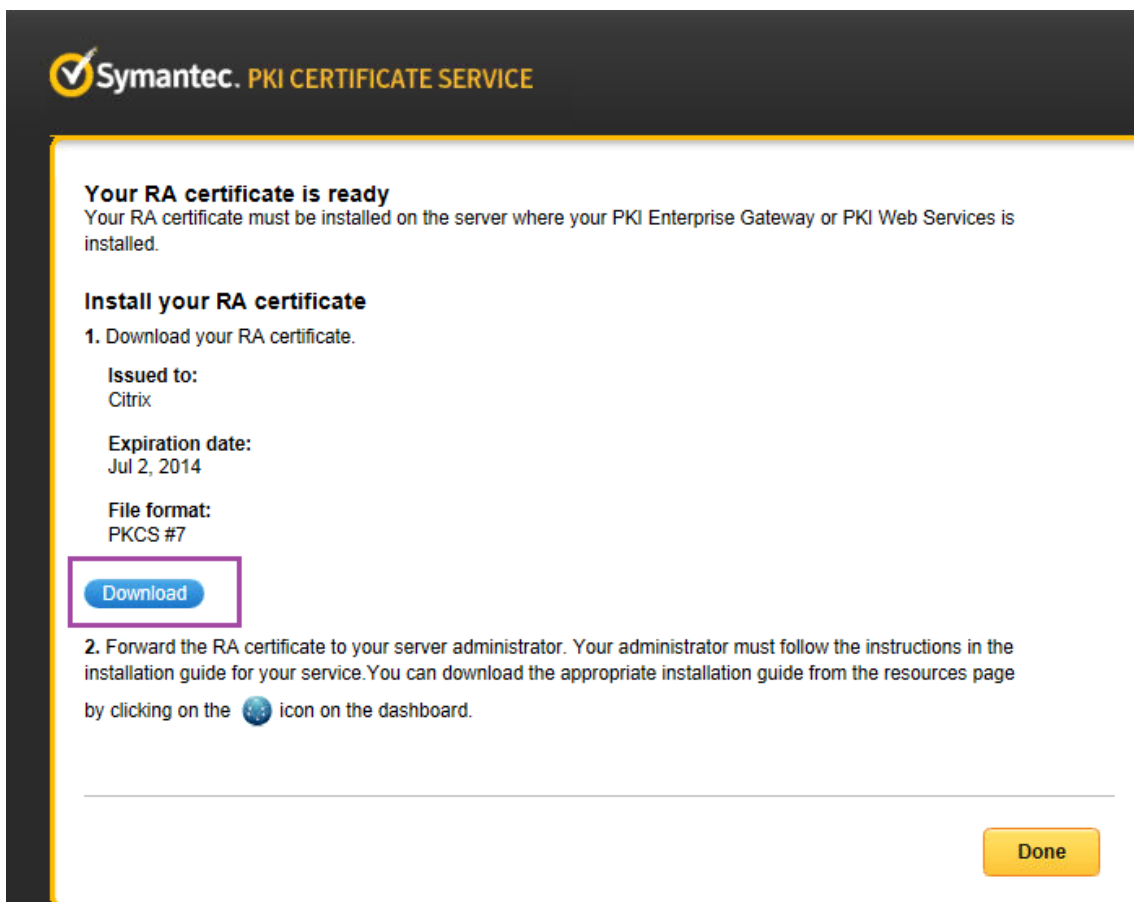
2. Clique com o botão direito do mouse no par de chaves e clique em **Generate Certification Request**.



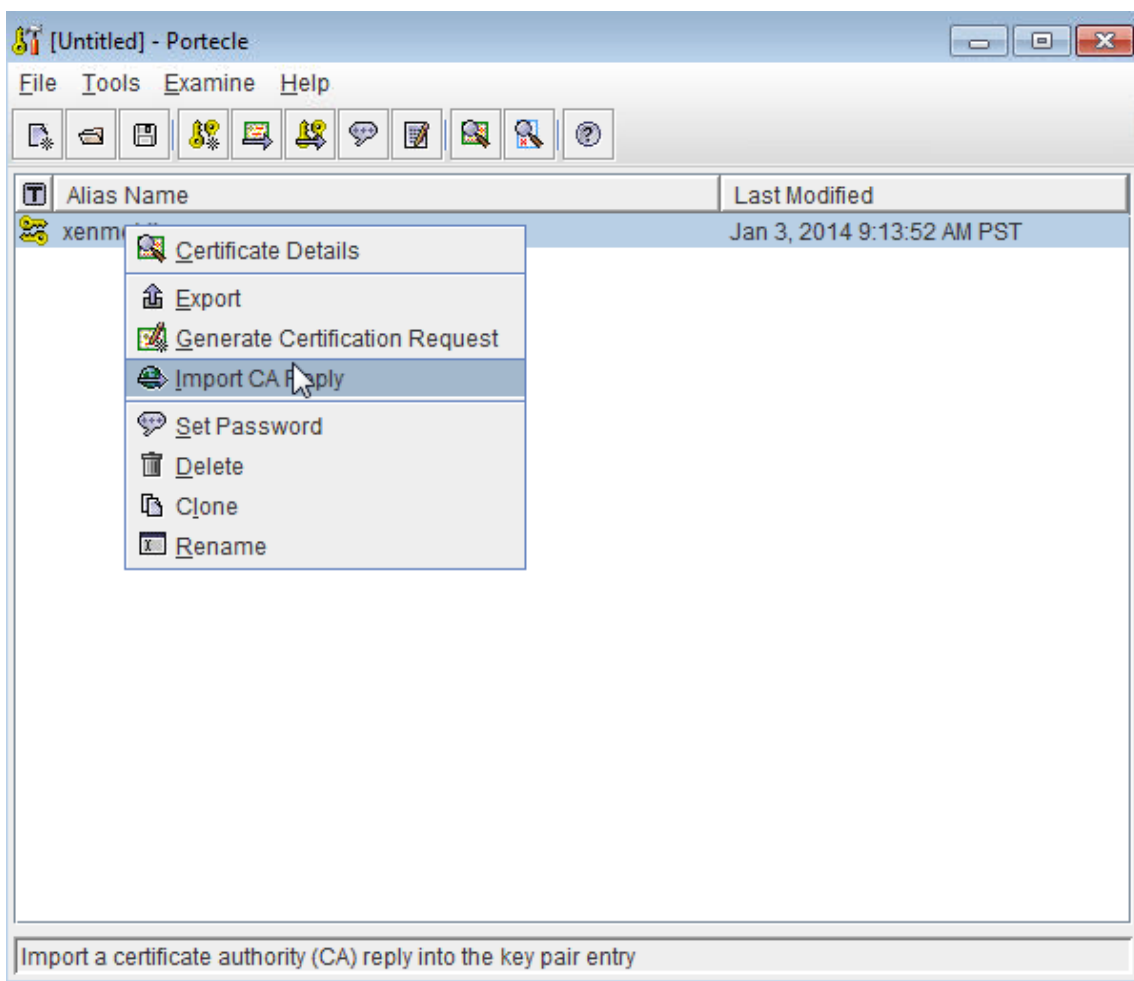
3. Copie o CSR.
4. No DigiCert PKI Manager, gere um certificado de RA: clique em **Settings**, clique em **Get a RA Certificate**, cole a CSR e clique em **Continue**.



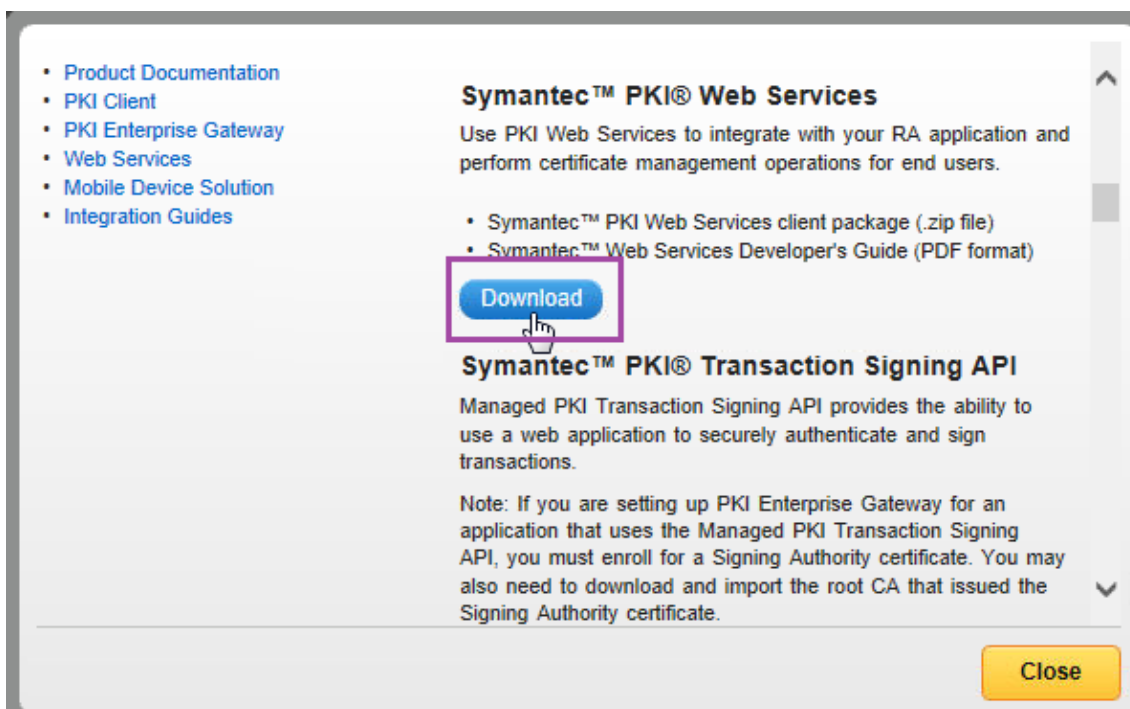
5. Clique em **Download** para baixar o certificado de RA gerado.



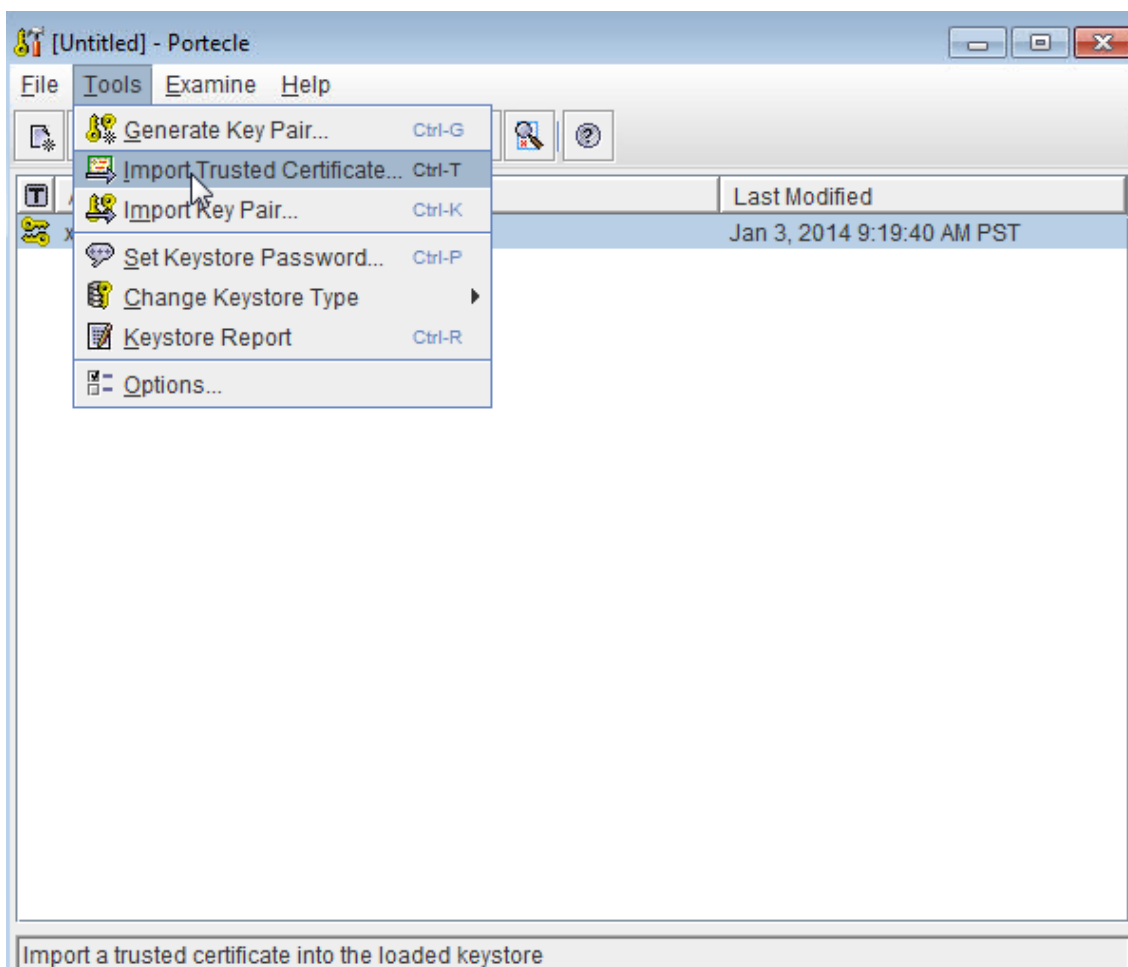
6. No Portecle, importe o certificado RA: clique com o botão direito do mouse no par de chaves e depois clique em **Import CA Reply**.



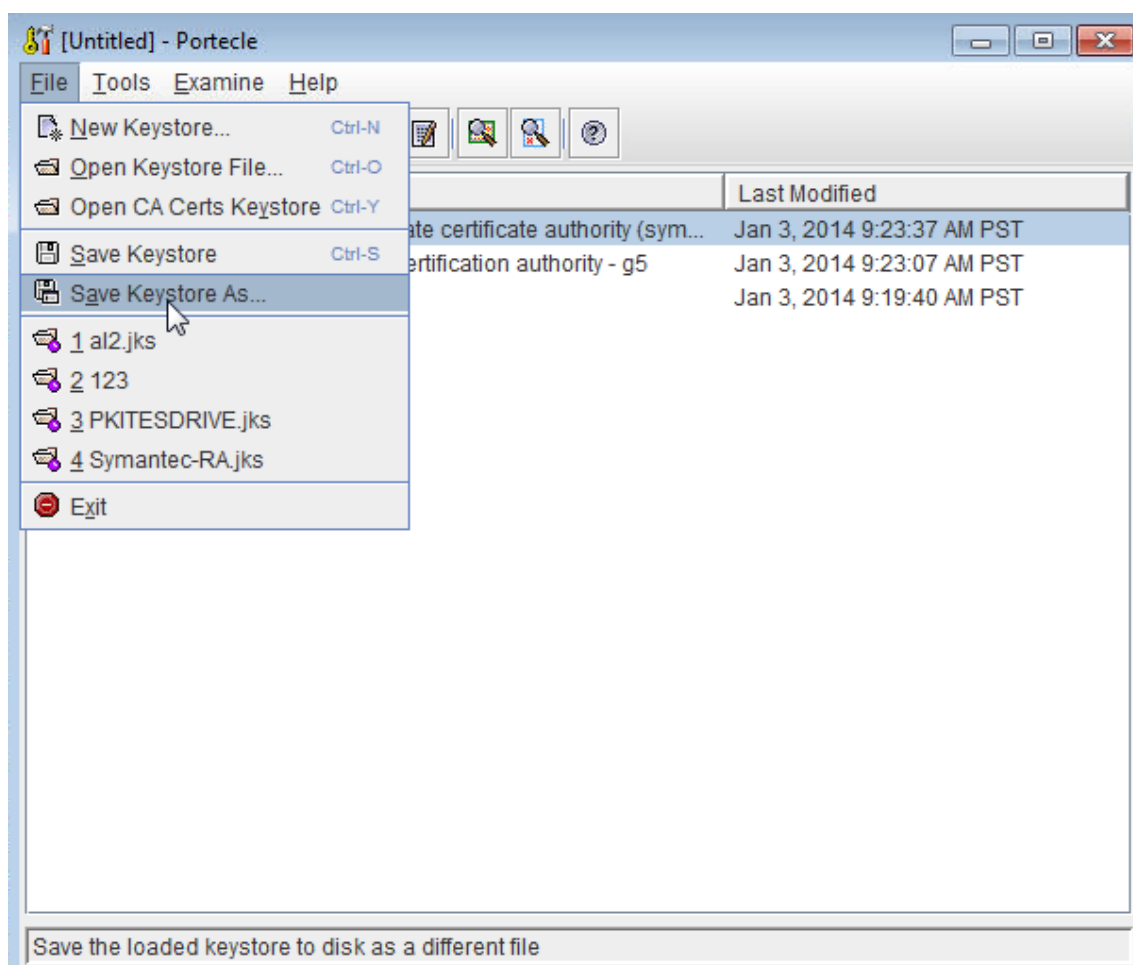
7. No DigiCert PKI Manager: vá para **Resources > Web Services** e, em seguida, baixe os certificados da CA.



8. No Portecle, importe os certificados de RA intermediário e raiz para o keystore: vá para **Tools > Import Trusted Certificates**.



9. Depois de importar os CAs, salve o keystore como RA.jks na pasta C:\DigiCert no Windows Server.



Configurar o DigiCert PKI Adapter no Windows Server

1. Faça login no Windows Server como administrador.
2. Carregue o arquivo RA.jks que você gerou na seção anterior. Carregue também os certificados públicos (cacerts.jks) para o seu servidor Symantec MPKI.
3. Baixe o arquivo do Adaptador Symantec PKI:
 - a) Acesse <https://www.citrix.com/downloads>.
 - b) Navegue para **Citrix Endpoint Management (e Citrix XenMobile Server) > XenMobile Server (no local) > Product Software > XenMobile Server 10 > Tools**.
 - c) No bloco **Symantec PKI Adapter**, clique em **Download File**.
 - d) Descompacte o arquivo .zip e copie os arquivos para a unidade C: do Windows Server:
 - custom_gpki_adapter.properties
 - Symantec.war

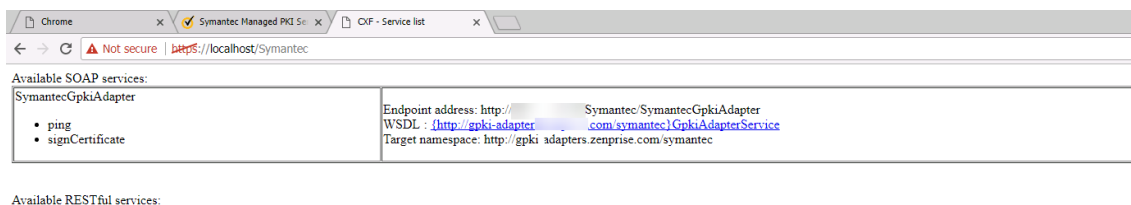
- Abra `custom_gpki_adapter.properties` no Bloco de Notas e edite os seguintes valores:

```

1 Gpki.CaSvc.Url=https://<managed PKI URL>
2
3 # keystore for client-cert auth
4
5 keyStore=C:\Symantec\RA.jks
6
7 # truststore for server with self-signed root CA
8
9 trustStore=C:\Symantec\cacerts.jks
10 <!--NeedCopy-->
    
```

- Copie o `Symantec.war` para a pasta `<tomcat dir>\webapps` e inicie o Tomcat.
- Verifique se o aplicativo foi implantado: abra um navegador da Web e vá até `https://localhost/Symantec`.
- Navegue até a pasta `<tomcat dir>\webapps\Symantec\WEB-INF\classes` e edite `gpki_adapter.properties`. Modifique a propriedade **CustomProperties** para apontar para o arquivo `custom_gpki_adapter` na pasta `C:\Symantec`:

`CustomProperties=C:\\Symantec\\custom_gpki_adapter.properties`
- Reinicie o Tomcat, navegue até `https://localhost/Symantec` e copie o endereço de ponto de extremidade. Na próxima seção, você cola esse endereço ao configurar o adaptador PKI.



Configurar o XenMobile Server para PKI gerenciado da DigiCert

Conclua a instalação do Windows Server antes de executar a configuração de XenMobile Server a seguir.

Para importar os certificados de AC da DigiCert e configurar a entidade PKI

- Importe os certificados de AC da DigiCert que emitem o certificado do usuário final: no console do XenMobile Server, vá para **Configurações > Certificados** e clique em **Importar**.

Settings > Certificates

Certificates

You must restart XenMobile on all nodes to commit and activate your changes to the SSL and Android for Work SAML certificates. To restart XenMobile, use the hypervisor console or command-line window.

Import Add

<input type="checkbox"/>	Name	Description	Status	Valid from	Valid to	Type	Private key
<input type="checkbox"/>	XMS.example.com	Self Signed/Generated	Up to date	2017-04-27	2027-04-25	SAML	✓
<input type="checkbox"/>			Up to date	2017-01-10	2018-12-16	SSL Listener	✓
<input type="checkbox"/>	cacerts.pem	Self Signed/Generated	Up to date	2017-04-27	2037-04-25	Devices CA	
<input type="checkbox"/>			9 days left	2016-09-09	2017-09-09	APNs	✓
<input type="checkbox"/>			Up to date	2011-05-03	2031-05-03	Root or intermediate	
<input type="checkbox"/>	Symantec Managed PKI Online Test Drive Root		Up to date	2009-08-31	2037-12-31	Trusted	

- Adicione e configure a Entidade PKI: vá para **Configurações > Entidades PKI**, clique em **Adicionar** e, em seguida, escolha **Entidade Genérica PKI**. Em **URL WSDL**, cole o endereço do ponto de extremidade que você copiou quando configurou o adaptador PKI na seção anterior e, em seguida, acrescente **?wsdl**, conforme mostrado abaixo.

Settings > PKI Entities > Edit Generic PKI Entity

Generic PKI Entity

Generic PKI Entity: General Information
The Generic PKI (GPKI) protocol is a proprietary XenMobile protocol running over a SOAP Web Service layer to provide uniform interfacing with various PKI solutions. The GPKI adapter, as a SOAP Web Services endpoint, publishes a self-describing Web Services Description Language (WSDL). You can create a GPKI entity to provide XenMobile with the WSDL through a URL.

1 General
2 Capabilities
3 CA Certificates

Name * Symantec

WSDL URL * <http://cip of PKI adapter/Symantec/SymantecGpkiAdapter?wsdl>

Authentication type None

- Clique em **Avançar**. O XenMobile preenche os nomes dos parâmetros do WSDL.

Settings > PKI Entities > Edit Generic PKI Entity

Generic PKI Entity

Generic PKI Entity: Adapter Capabilities
View the capabilities of the adapter this entity operates with, as well as the parameters the adapter defines for each capability.

1 General
2 Capabilities
3 CA Certificates

- Sign certificate: <http://cip of PKI adapter/Symantec/SymantecGpkiAdapter>

certParams

certificateProfileId

- Clique em **Avançar**, selecione o certificado da autoridade de certificação correto e clique em **Salvar**.

Settings > PKI Entities > Edit Generic PKI Entity

Generic PKI Entity

Generic PKI Entity: Issuing CA Certificates
Indicate the certificates you want to use for this entity by selecting or clearing the check boxes. An entity is only valid when you select at least one certificate. Add all CA certificates that might be signers of certificates returned by this entity. Although entities may return certificates signed by different CAs, all certificates obtained through a given credential provider must be signed by the same CA. Accordingly, you will have to select one of the certificates configured here in the Distribution page of the Credential Provider setting.

Import CA certificate

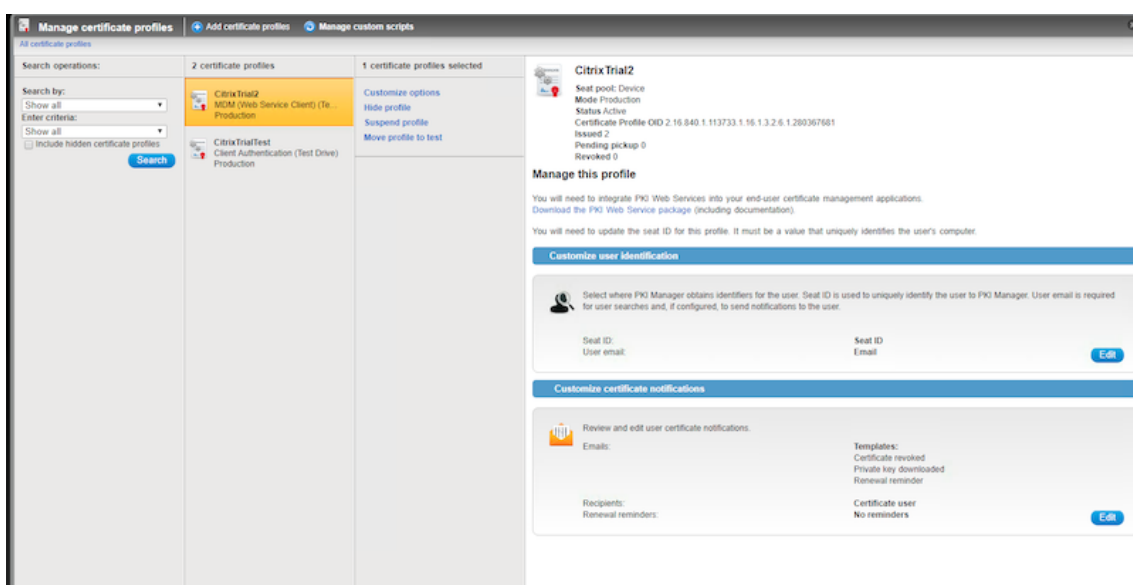
<input type="checkbox"/>	Name	Serial number	Valid from	Valid to
<input type="checkbox"/>			05/02/2016	05/02/2036
<input type="checkbox"/>			08/31/2011	08/31/2021
<input checked="" type="checkbox"/>	Symantec Managed PKI Online Test Drive Root		08/17/2011	08/17/2021

- Na página **Configurações > Entidades de PKI**, verifique se o **Estado** da Entidade PKI que você adicionou é **Válido**.

Name	Type	Capabilities	Description	State
Symantec	GPKI	SIGN	http://[redacted]/Symantec/SymantecGpkiAdapter	Valid

Para criar o provedor de credenciais para PKI gerenciado da DigiCert

- No console do DigiCert PKI Manager, copie o **Certificate Profile OID** em Certificate Template.



- No console do XenMobile Sever, vá para **Configurações > Provedores de credenciais**, clique em **Adicionar** e defina as configurações da seguinte maneira.

- **Nome:** digite um nome exclusivo para a nova configuração do provedor. Este nome é usado para referir-se à configuração em outras partes do console XenMobile.
- **Descrição:** descreva o provedor de credenciais. Embora esse campo seja opcional, uma descrição pode ser útil para quando você precisar de detalhes sobre esse provedor de credenciais.
- **Entidade de emissão:** escolha a entidade de emissão do certificado.
- **Método de emissão:** escolha **Assinar** como o método que o sistema utiliza para obter certificados cliente da entidade configurada.
- **certParams:** Adicione o seguinte valor: **commonName=\${user.mail},otherNameUPN=\${user.userpr**
- **certificateProfileid:** cole o OID de perfil de certificado que você copiou na etapa 1.

Settings > Credential Providers > Edit credential provider

Credential Providers

- 1 General
- 2 Certificate Signing Request
- 3 Distribution
- 4 Revocation XenMobile
- 5 Revocation PKI
- 6 Renewal

Credential Providers: General Information
 You can define one or more credential providers for device certificate issuance and lifecycle. The credential providers control the certificate format (subject, key, algorithms) and the conditions for the certificate renewal or revocation, if any.

Name* Symantec-CP
 Description Symantec-CP
 Issuing entity Symantec
 Issuing method SIGN

Name	Value
certParams	commonName=\$(user.mail), otherNameUPN=\$(user.userprincipalname), mail=\$(user.mail)
certificateProfileId	2.16.840.1.113733.1.16.1.3.2.6.1.250531744

Save Cancel

3. Clique em **Avançar**. Em cada uma das páginas restantes (solicitação de assinatura do certificado por meio de renovação), aceite as configurações padrão. Quando terminar, clique em **Salvar**.

Para testar e solucionar problemas de configuração

1. Criar uma política de dispositivo de credenciais: vá para **Configurar > Políticas de dispositivo**, clique em **Adicionar**, comece a digitar **Credenciais** e clique em **Credenciais**.
2. Especifique o **Nome da Política**.
3. Defina as configurações da plataforma, como se seguem:
 - **Tipo de credencial:** escolha **Provedor de credenciais**.
 - **Provedor de credenciais:** escolha o provedor DigiCert.

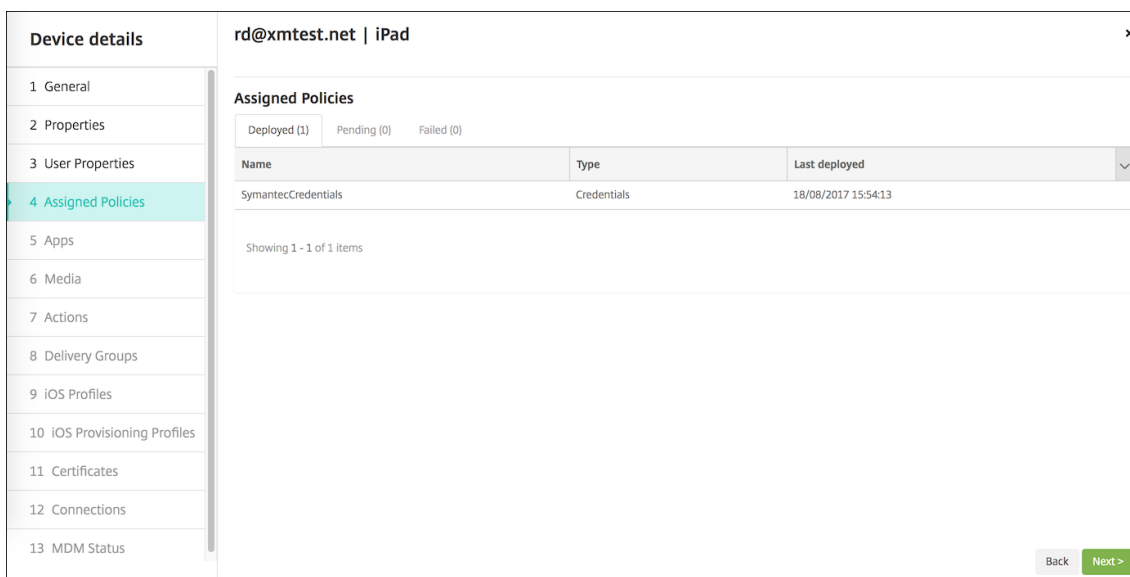
Credentials Policy

1 Policy Info
 2 Platforms
 iOS
 Mac OS X
 Android
 Android for Work
 Windows Phone
 Windows Desktop/Tablet

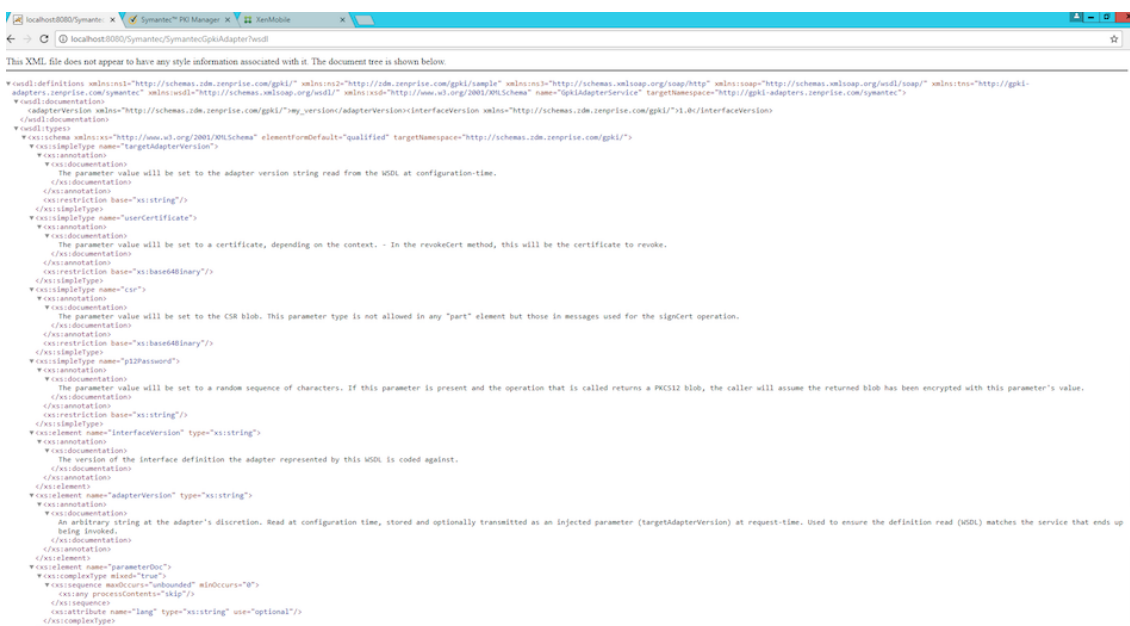
Credentials Policy
 This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Credential type Credential provider
 Credential provider* Symantec-CP
 Remove policy Select date
 Duration until removal (in hours)
 Allow user to remove policy Always

4. Depois de completar as configurações da plataforma, vá para a página **Atribuição**, atribua a política aos grupos de entrega e clique em **Salvar**.
5. Para verificar se a política foi implantada no dispositivo, vá para **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Editar** e clique em **Políticas atribuídas**. O exemplo a seguir mostra uma implantação com êxito de uma política.



Se a política não foi implantada, faça login no Windows Server e verifique se o WSDL está sendo carregado corretamente.



Para mais informações sobre solução de problemas, verifique os logs do Tomcat em `<tomcat dir>\logs\catalina.<current date>`.

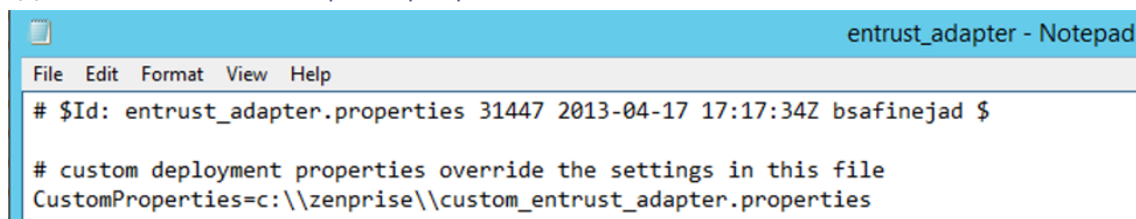
Adaptador PKI Entrust

Como alternativa à PKI gerenciada pela DigiCert, você pode instalar o adaptador Entrust PKI. Antes de instalar o adaptador, consulte as etapas para instalar o Java e o Apache Tomcat no Windows Server na seção PKI gerenciada da DigiCert deste artigo.

Instale o adaptador Entrust PKI

1. Baixe o arquivo do Adaptador Entrust PKI:
 - a) Acesse <https://www.citrix.com/downloads>.
 - b) Navegue para **Citrix Endpoint Management (e Citrix XenMobile Server) > XenMobile Server > Product Software > XenMobile Server 10 > Tools**.
 - c) No bloco **Entrust PKI Adapter**, clique em **Download File**.
 - d) Extraia o arquivo entrust.war file do arquivo .zip baixado e coloque-o no diretório C:\Program Files (x86)\Apache Software Foundation\Tomcat 8.5\webapps.

2. Em C:\Program Files (x86)\Apache Software Foundation\Tomcat 8.5\webapps\Entrust\WEB-INF\classes, edite entrust_adapter.properties e defina CustomProperties como c:\\zenprise\\custom_entrust_adapter.properties.



```
entrust_adapter - Notepad
File Edit Format View Help
# $Id: entrust_adapter.properties 31447 2013-04-17 17:17:34Z bsafinejad $
# custom deployment properties override the settings in this file
CustomProperties=c:\\zenprise\\custom_entrust_adapter.properties
```

3. Na unidade C:, crie um diretório zenprise e um novo arquivo chamado custom_entrust_adapter.properties.
4. Edite o arquivo com o seguinte conteúdo, tomando cuidado ao substituir Entrust.MdmSvc.URL, AdminUserId e AdminPassword apropriadamente.

~

defina o seguinte para a URL apropriada para AS/IG

Entrust.MdmSvc.Url=https://pki.yourcorp.com:19443/mdmws/services/AdminServiceV8

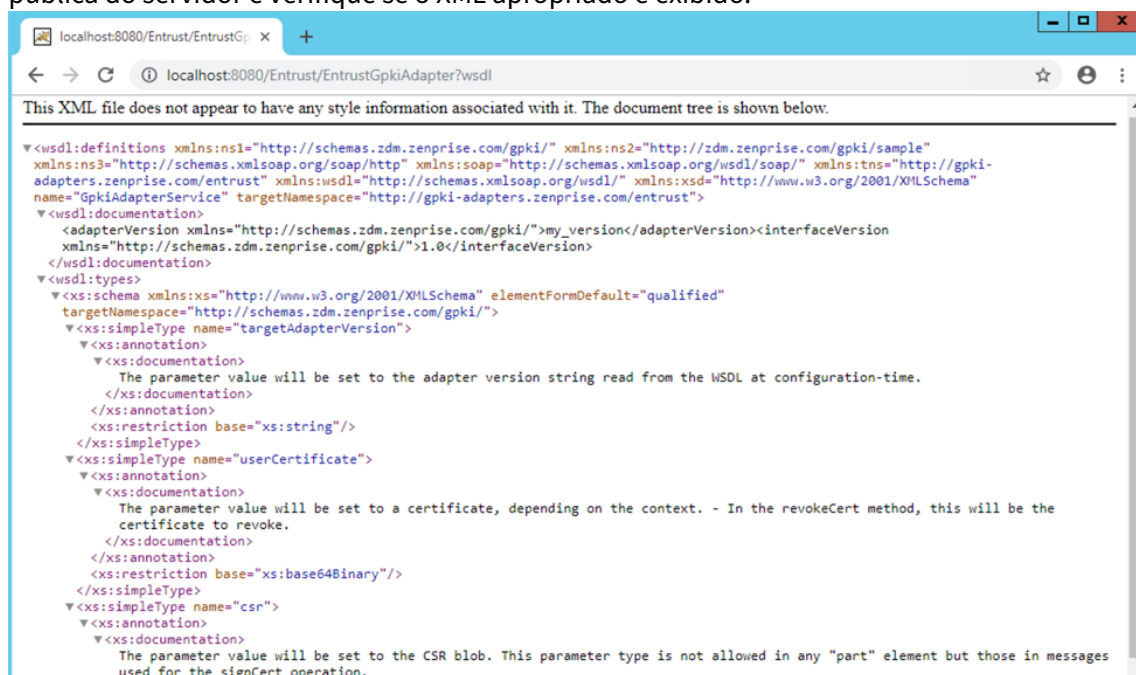
```
1 # definir como 1 ou true para forçar a criação do usuário a partir
   de parâmetros passados de usuário e grupo o IG for utilizado e
   o usuário não existir
2 CreateUser=
3
4 # defina as credenciais para o ponto de extremidade
5 AdminUserId=`[ID do usuário]`
6 AdminPassword=`[senha]`
7
8
9 # keystore para client-cert auth
10 #keyStore=
11 #keyStorePassword=
12 #keyStoreType: JKS, JCEKS e PKCS12 -- não é necessário para
   arquivos .p12 e .jks
13
```

```
14 # truststore para servidor com CA raiz autoassinado
15 #trustStore=
16 #trustStorePassword=
17 #trustStoreType: JKS, JCEKS e PKCS12 -- não é necessário para
    arquivos .p12 e .jks
18 ~
```

5. Reinicie o serviço Tomcat. Navegue até C:\Program Files (x86)\Apache Software Foundation\Tomcat 8.5\logs and open Catalina_201x-MM-DD.log. Confirme que não haja erros e se você vê a seguinte linha:

```
13-Nov-2018 09:02:35.319 INFO [localhost-startStop-1] org.apache.cxf
.endpoint.ServerImpl.initDestination Setting the server's publish
address to be /EntrustGpkiAdapter
```

6. Navegue até <http://localhost:8080/Entrust/EntrustGpkiAdapter?wsdl> ou à URL pública do servidor e verifique se o XML apropriado é exibido.



Configurar o XenMobile para o adaptador Entrust PKI

1. Faça login no console XenMobile e navegue até **Configurações > Entidades PKI**. Clique em **Adicionar > Entidade PKI genérica**.
2. Insira as seguintes informações:
 - **Nome:** - insira um nome para a Entidade PKI.
 - **URL WSDL:** Insira o URL público do servidor.
 - **Tipo de autenticação:** escolha no método de autenticação que você deseja usar.

- **Nenhum**
 - **HTTP básico:** digite o nome do usuário e a senha necessários para se conectar.
 - **Certificado cliente:** escolha o certificado cliente SSL correto.
 - **Local do recurso:** selecione **Meu Local do Recurso**.
 - **Caminhos relativos permitidos:** insira `/Entrust/*`.
3. Quando terminar de configurar a Entidade PKI, volte para a página **Configurações** e adicione um **Provedor de credenciais**.
 4. Na guia **Geral**, selecione sua entidade Entrust como a **Entidade de emissão** e **ASSINAR** como o **Método de emissão**.
 5. Na guia **Solicitação de assinatura de certificado**, defina as configurações da seguinte maneira:
 - **Algoritmo de chave:** **RSA**.
 - **Tamanho da chave:** 2048.
 - **Algoritmo de assinatura** **SHA256withRSA**.
 - **Nome de entidade:** `cd=$user.username`
 - **Nomes alternativos da entidade:** opcional. Recomendamos o seguinte:
 - **Tipo:** **Nome principal do usuário**.
 - **Valor:** `$user.userprincipalname`
- Nota:**
Se você alterar alguma configuração no adaptador, siga estas etapas para reconfigurar o provedor de credenciais.
6. Depois de concluir a configuração do provedor de credenciais, navegue até **Configurar > Políticas de dispositivo** e adicione uma política de Credenciais.
 7. Configure a política para os SOs que você planeja usar. Na página de configuração de cada SO, para **Tipo de credencial**, selecione **Provedor de credenciais**. No menu **Provedor de credenciais**, selecione o provedor de credenciais configurado anteriormente.

Serviços de Certificado da Microsoft

O XenMobile faz interface com os Serviços de Certificado da Microsoft por meio da respectiva interface de registro na Web. O XenMobile é compatível com a emissão de novos certificados somente por meio dessa interface (o equivalente ao recurso assinar da GPKI). Se a AC da Microsoft gerar um certificado de usuário do Citrix Gateway, o Citrix Gateway oferece a renovação e revogação para esses certificados.

Para criar uma entidade PKI da AC da Microsoft no XenMobile, você deve especificar a URL base da interface da Web dos Serviços de Certificado. Se você preferir, use a autenticação de cliente SSL para proteger a conexão entre o XenMobile e a interface da Web dos Serviços de Certificado.

Adicionar uma entidade dos Serviços de Certificado da Microsoft

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console e clique em **Entidades PKI**.

2. Na página **Entidades PKI**, clique em **Adicionar**.

É exibido um menu de tipos de entidade PKI.

3. Clique em **Entidade de serviços de certificado da Microsoft**.

A página **Entidade de serviços de certificado da Microsoft: Informações gerais** é exibida.

4. Na página **Entidade de serviços de certificado da Microsoft: Informações gerais**, defina estas configurações:

- **Nome:** digite um nome para a nova entidade que você usará mais tarde para se referir a ela. Os nomes de entidade devem ser exclusivos.
- **URL raiz do serviço de registro na Web:** digite a URL base do seu serviço de registro na Web da AC da Microsoft, por exemplo, <https://192.0.2.13/certsrv/>. A URL pode usar HTTP simples ou HTTP sobre SSL.
- **certnew.cer page name:** o nome da página certnew.cer. Use o nome padrão a menos que você o tenha renomeado por algum motivo.
- **certfnsh.asp:** o nome da página certfnsh.asp. Use o nome padrão a menos que você o tenha renomeado por algum motivo.
- **Tipo de autenticação:** escolha no método de autenticação que você deseja usar.
 - **Nenhum**
 - **HTTP básico:** digite o nome do usuário e a senha necessários para se conectar.
 - **Certificado cliente:** escolha o certificado cliente SSL correto.

5. Clique em **Testar conexão** para garantir que o servidor esteja acessível. Se ele não estiver acessível, será exibida uma mensagem informando que a conexão falhou. Verifique as definições de configuração.

6. Clique em **Avançar**.

A página **Entidade de serviços de certificado da Microsoft: modelos** é exibida. Nessa página, especifique os nomes internos dos modelos com os quais a sua AC da Microsoft é compatível. Quando você criar provedores de credenciais, selecione um modelo na lista definida aqui. Cada provedor de credenciais que usa essa entidade usa exatamente um desses modelos.

Para os requisitos de modelo dos Serviços de Certificado da Microsoft, consulte a documentação da Microsoft relativa à versão do Microsoft Server. O XenMobile não tem requisitos para os certificados que distribui além dos formatos de certificado indicados em [Certificados](#).

7. Na página **Entidade de serviços de certificado da Microsoft: Modelos** clique em **Adicionar**, digite o nome do modelo e clique em **Salvar**. Repita essa etapa para cada modelo que você desejar adicionar.

8. Clique em **Avançar**.

A página **Entidade de serviços de certificado da Microsoft: parâmetros HTTP** é exibida. Nesta página, você especifica parâmetros personalizados para o XenMobile adicionar à solicitação HTTP para a interface de registro na Web da Microsoft. Parâmetros personalizados são úteis somente para scripts personalizados em execução na autoridade de certificação.

9. Na página **Entidade de serviços de certificado da Microsoft: Parâmetros HTTP**, clique em **Adicionar**, digite o nome e o valor dos parâmetros HTTP que você deseja adicionar e, em seguida, clique em **Avançar**.

É exibida a página **Entidade de serviços de certificado da Microsoft: certificados AC**. Nessa página, você deve informar ao XenMobile sobre os signatários dos certificados que o sistema obtém por meio dessa entidade. Quando seu certificado de CA for renovado, atualize-o no XenMobile. O XenMobile aplica a mudança à entidade de forma transparente.

10. Na página **Entidade de serviços de certificado da Microsoft: Certificados AC**, selecione os certificados que você deseja usar para esta entidade.

11. Clique em **Salvar**.

A entidade é exibida na tabela Entidades PKI.

Lista de certificados revogados (CRL) de Citrix

O XenMobile dá suporte à Lista de revogação de certificados (CRL) somente para uma Autoridade de Certificação terceira. Se você tiver configurado uma AC da Microsoft, o XenMobile usa o Citrix ADC para gerenciar a revogação.

Quando você configurar a autenticação baseada em certificado de cliente, decida se é necessário ou não configurar a opção Lista de revogação de certificados (CRL) do Citrix ADC, **Ativar atualização automática da CRL**. Esta etapa garante que o usuário de um dispositivo no modo somente MAM não possa autenticar usando um certificado existente no dispositivo.

O XenMobile emite novamente um novo certificado porque ele não impede que um usuário gere um certificado de usuário depois que um tiver sido revogado. Essa opção aumenta a segurança de entidades PKI quando a CRL verifica entidades PKI expiradas.

CAs discricionárias

Uma AC discricionária é criada quando você fornece ao XenMobile um certificado de AC e a chave privada associada. O XenMobile manipula a emissão, a revogação e as informações de status do certificado internamente, de acordo com os parâmetros que você especificar.

Quando você configura uma AC discricionária, pode ativar o suporte do Protocolo OCSP (Online Certificate Status Protocol) para essa AC. Se, e somente se, você ativar o suporte do OCSP, a AC adicionará

uma extensão `id-pe-authorityInfoAccess` aos certificados que a AC emitir. A extensão aponta para o respondente OCSP interno do XenMobile na seguinte localização:

`https://<server>/<instance>/ocsp`

Quando você configura o serviço OCSP, especifique um certificado de assinatura OCSP para a entidade discricionária em questão. Você pode usar o próprio certificado de AC como signatário. Para evitar a exposição desnecessária da chave privada de AC (recomendado): crie um certificado de assinatura OCSP assinado pelo certificado de AC e inclua a extensão: `id-kp-OCSPSigning extendedKeyUsage`.

O serviço do respondedor OCSP do XenMobile é compatível com respostas OCSP básicas e com os seguintes algoritmos de hash em solicitações:

- SHA-1
- SHA-224
- SHA-256
- SHA-384
- SHA-512

As respostas são assinadas com SHA-256 e o algoritmo de chave do certificado de assinatura (DSA, RSA ou ECDSA).

Adicionar ACs discricionárias

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console e clique em **Mais > Entidades PKI**.
2. Na página **Entidades PKI**, clique em **Adicionar**.
É exibido um menu de tipos de entidade PKI.
3. Clique em **CA discricionária**.
A página **CA discricionária: Informações gerais** é exibida.
4. Na página **CA discricionária: Informações gerais**, faça o seguinte:
 - **Nome:** digite um nome descritivo para a CA discricionária.
 - **Certificado de AC para assinar solicitações de certificado:** clique no certificado da CA discricionária a ser usado para assinar solicitações de certificado.
Essa lista de certificados é gerada com base nos certificados de AC com chaves privadas que você carregou para o XenMobile em **Configurar > Configurações > Certificados**.
5. Clique em **Avançar**.
A página **CA discricionária: Parâmetros** é exibida.

6. Na página **CA discricionária: Parâmetros**, faça o seguinte:

- **Gerador de número de série:** a CA discricionária gera números de série para os certificados que ela emite. Nessa lista, clique em **Sequencial** ou **Não sequencial** para determinar como os números serão gerados.
- **Próximo número de série:** digite um valor para determinar o próximo número emitido.
- **Certificado válido para:** digite o número de dias durante os quais o certificado é válido.
- **Uso da chave:** identifique o propósito dos certificados emitidos pela CA discricionária definindo as chaves adequadas como **Ativado**. Depois de definida, a AC é limitada a emitir certificados para esses fins.
- **Uso de chave estendido:** para adicionar mais parâmetros, clique em **Adicionar**, escreva o nome da chave e clique em **Salvar**.

7. Clique em **Avançar**.

A página **CA discricionária: Distribuição** é exibida.

8. Na página **CA discricionária: Distribuição**, selecione um modo de distribuição:

- **Centralizado: geração de chave do lado do servidor.** A Citrix recomenda a opção centralizada. As chaves privadas são geradas e armazenadas no servidor e distribuídas para os dispositivos do usuário.
- **Distribuído: geração de chave do lado do dispositivo.** As chaves privadas são geradas nos dispositivos do usuário. Esse modo distribuído usa o SCEP e requer um certificado de criptografia RA com a extensão **keyUsage keyEncryption** e um certificado de assinatura RA com a extensão **keyUsage digitalSignature**. O mesmo certificado pode ser usado para autenticação e criptografia.

9. Clique em **Avançar**.

A página **CA discricionária: Protocolo OCSP (Online Certificate Status Protocol)** é exibida.

Na página **CA discricionária: Protocolo OCSP (Online Certificate Status Protocol)**, faça o seguinte:

- Se você desejar adicionar uma extensão **AuthorityInfoAccess** (RFC2459) aos certificados assinados por essa AC, defina **Ativar suporte a OCSP para esta AC** como **Ativado**. Essa extensão aponta para o respondente OCSP da AC em `https://<server>/<instance>/ocsp`.
- Se você tiver ativado o suporte do OCSP, selecione um certificado de AC de assinatura OSCP. Essa lista de certificados é gerada com base nos certificados de AC que você carregou no XenMobile.

10. Clique em **Salvar**.

A AC discricionária é exibida na tabela Entidades PKI.

Provedores de credenciais

April 1, 2021

Os provedores de credenciais são as configurações reais de certificado que você usa em várias partes do sistema XenMobile. Provedores de credenciais definem as origens, parâmetros e ciclos de vida de seus certificados. Essas operações ocorrem se os certificados fizerem parte das configurações do dispositivo ou se forem independentes (isto é, enviados como estão para o dispositivo).

O registro do dispositivo restringe o ciclo de vida do certificado. Ou seja, o XenMobile não emite certificados antes do registro, embora ele possa emitir alguns certificados como parte do processo de registro. Além disso, os certificados emitidos da PKI interna no contexto de um registro são revogados quando o processo de registro é revogado. Depois que o relacionamento de gerenciamento é encerrado, nenhum certificado válido permanece.

Você pode usar uma configuração de provedor de credenciais em vários locais para que uma configuração possa reger qualquer número de certificados ao mesmo tempo. A unidade está no recurso de implantação e na implantação. Por exemplo, se o provedor de credenciais P for implantado para o dispositivo D como parte da configuração C, as configurações de emissão para P determinam o certificado que é implantado em D. Da mesma forma, as configurações de renovação de D se aplicam quando C é atualizada. E as configurações de revogação de D também se aplicam quando C é excluída ou quando D é revogado.

De acordo com essas regras, a configuração do provedor de credenciais no XenMobile determina o seguinte:

- A origem de certificados.
- O método pelo qual os certificados são obtidos: assinando um novo certificado ou obtendo (recuperando) um certificado e um par de chaves existentes.
- Os parâmetros para emissão ou recuperação. Por exemplo, os parâmetros de CSR (Solicitação de Assinatura de Certificado), como tamanho da chave, algoritmo de chave e extensões de certificado.
- A forma como os certificados são entregues ao dispositivo.
- Condições de revogação. Embora todos os certificados sejam revogados no XenMobile quando o relacionamento de gerenciamento é interrompido, a configuração pode especificar uma revogação anterior. Por exemplo, a configuração pode especificar a revogação de um certificado quando a configuração do dispositivo associado é excluída. Além disso, sob algumas condições, a revogação do certificado associado no XenMobile pode ser enviada para a infraestrutura de chave pública (PKI) de back-end. Ou seja, a revogação de certificados no XenMobile pode causar a revogação de certificados na PKI.
- Configurações de renovação. Os certificados obtidos por meio de um determinado provedor de credenciais podem ser renovados automaticamente quando estão próximos do vencimento.

Ou, separadamente dessa situação, as notificações podem ser emitidas quando essa expiração se aproximar.

A disponibilidade das opções de configuração depende principalmente do tipo de Entidade PKI e do método de emissão que você selecionar para um provedor de credenciais.

Métodos de emissão de certificado

Você pode obter um certificado, conhecido como métodos de emissão, de duas maneiras:

- **Assinar:** Com esse método, a emissão envolve a criação de uma nova chave privada, a criação de uma CSR e o envio da CSR para uma Autoridade de Certificação (CA) para assinatura. O XenMobile é compatível com o método de assinar para as três entidades PKI (Entidade de serviços de certificado da Microsoft, PKI genérica e CA discricionária).
- **Obter:** Com esse método, a emissão, para fins do XenMobile, é a recuperação de um par de chaves existente. O XenMobile é compatível com o método obter somente para PKI Genérica.

Um provedor de credenciais usa o método de emissão Assinar ou Obter. O método selecionado afeta as opções de configuração disponíveis. Em especial, a configuração de CSR e a entrega distribuída estarão disponíveis somente se o método de emissão for assinar. Um certificado obtido é sempre enviado para o dispositivo como um PKCS #12, o equivalente ao modo de entrega centralizado do método de assinatura.

Entrega de certificado

Dois modos de entrega de certificado estão disponíveis no XenMobile: centralizado e distribuído. O modo distribuído usa o Protocolo de Registro de Certificado Simples (SCEP) e está disponível somente nas situações em que o cliente é compatível com o protocolo (somente iOS). O modo distribuído é obrigatório em algumas situações.

Para que um provedor de credenciais seja compatível com a entrega distribuída (assistida por SCEP), é necessária uma etapa de configuração especial: Configurar certificados de Autoridade de Registro (RA). Os certificados de RA são necessários porque, ao usar o protocolo SCEP, o XenMobile age como um representante (um registrador) da AC real. O XenMobile precisa comprovar para o cliente que ele tem autoridade para agir como tal. Essa autoridade é estabelecida fazendo o upload para o XenMobile dos certificados anteriormente mencionados.

São necessárias duas funções de certificado diferentes (embora um único certificado possa atender a ambos os requisitos): assinatura de RA e criptografia de RA. As restrições dessas funções são as seguintes:

- O certificado de assinatura RA deve ter a assinatura digital de uso de chave X.509.
- O certificado de criptografia RA deve ter a codificação de chave de uso de chave X.509.

Para configurar os certificados de RA do provedor de credenciais, você carrega os certificados para o XenMobile e cria links para eles no provedor de credenciais.

Um provedor de credenciais é considerado como compatível com entregas distribuídas somente se ele tiver um certificado configurado para funções de certificado. Você pode configurar cada provedor de credenciais para dar preferência ao modo centralizado, ao modo distribuído ou para exigir o modo distribuído. O resultado real depende do contexto: se o contexto não for compatível com o modo distribuído, mas o provedor de credenciais exigir esse modo, a implantação não será realizada. Da mesma forma, quando o contexto exige o modo distribuído, mas o provedor de credenciais não é compatível com ele, a implantação não é realizada. Em todos os outros casos, a configuração preferencial é respeitada.

A seguinte tabela mostra a distribuição SCEP em todo o XenMobile:

Contexto	SCEP com suporte	SCEP necessário
Serviço de Perfil do iOS	Sim	Sim
Registro do gerenciamento de dispositivo móvel do iOS	Sim	Não
Perfis de configuração do iOS	Sim	Não
Registro SHTTP	Não	Não
Configuração SHTTP	Não	Não
Registro de telefone e tablet com Windows	Não	Não
Configuração de telefone e tablet com Windows	Não, exceto para a política de dispositivo de Wifi, que é compatível com Windows Phone 8.1 e a versão mais recente do Windows 10	Não

Revogação de certificados

Há três tipos de revogação.

- **Revogação interna:** A revogação interna afeta o status do certificado, conforme mantido pelo XenMobile. O XenMobile considera esse status ao avaliar um certificado apresentado ou ao fornecer informações de status OCSP para um certificado. A configuração do provedor de credenciais determina como o status é afetado sob várias condições. Por exemplo, o provedor de credenciais pode especificar para sinalizar certificados como revogados quando os certificados são excluídos do dispositivo.

- **Revogação propagada externamente:** Também conhecido como Revogação XenMobile, esse tipo de revogação se aplica aos certificados obtidos de uma PKI externa. O certificado foi revogado na PKI quando o XenMobile o revogou internamente, sob as condições definidas pela configuração do provedor de credenciais. A chamada para realizar a revogação exige uma entidade PKI Geral (GPKI) com capacidade de revogação.
- **Revogação induzida externamente:** Também conhecida como Revogação PKI, esse tipo de revogação também se aplica somente aos certificados obtidos de uma PKI externa. Sempre que o XenMobile avalia um determinado status de certificado, ele consulta a PKI quanto a esse status. Se o certificado tiver sido revogado, o XenMobile revoga-o internamente. Esse mecanismo usa o protocolo OCSP.

Esses três tipos não são exclusivos, mas aplicam-se juntos. Uma revogação externa ou descoberta independente pode causar uma revogação interna. Uma revogação interna afeta potencialmente uma revogação externa.

Renovação de certificado

A renovação de certificado é a combinação de uma revogação do certificado existente e uma emissão de outro certificado.

O XenMobile primeiro tenta obter o novo certificado antes de revogar o certificado anterior para evitar a descontinuação do serviço quando a emissão falhar. Para entrega distribuída (suportada pelo SCEP), a revogação também ocorre somente após o certificado ter sido instalado com êxito no dispositivo. Caso contrário, a revogação ocorre antes que o novo certificado seja enviado ao dispositivo. Essa revogação é independente do sucesso ou falha da instalação do certificado.

A configuração de revogação exige que você especifique uma determinada duração (em dias). Quando o dispositivo se conecta, o servidor verifica se a data `NotAfter` do certificado é posterior à data atual, menos a duração especificada. Se o certificado atender a essa condição, o XenMobile tentará renovar o certificado.

Criar um provedor de credenciais

Configurar um provedor de credenciais varia principalmente como um fator de qual entidade e método de emissão você seleciona para o provedor de credenciais. Você pode distinguir entre os provedores de credenciais que usam uma entidade interna ou uma entidade externa:

- Uma entidade discricionária, que é interna para o XenMobile, é uma entidade interna. O método de emissão para uma entidade discricionária é sempre Assinar. Assinar significa que, a cada operação de emissão, o XenMobile assina um novo par de chaves com o certificado de CA selecionado para a entidade. A geração do par de chaves no dispositivo ou no servidor depende do método de distribuição selecionado.

- Uma entidade externa, que faz parte de sua infraestrutura corporativa, inclui AC da Microsoft ou uma GPKI.

Para obter informações detalhadas sobre a configuração do PKI gerenciado da DigiCert, incluindo a criação do provedor de credenciais, consulte “DigiCert Managed PKI” em [Entidades PKI](#).

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito e clique em **Configurações > Provedores de credenciais**.

2. Na página **Provedores de credenciais**, clique em **Adicionar**.

A página **Provedores de credenciais: informações gerais** é exibida.

3. Na página **Provedores de credenciais: informações gerais**, faça o seguinte:

- **Nome:** digite um nome exclusivo para a nova configuração do provedor. Este nome é usado mais tarde para identificar a configuração em outras partes do console XenMobile.
- **Descrição:** descreva o provedor de credenciais. Embora esse campo seja opcional, uma descrição pode fornecer detalhes úteis sobre esse provedor de credenciais.
- **Entidade de emissão:** clique na entidade de emissão do certificado.
- **Método de emissão:** clique em **Assinar** ou **Obter** para servir como o método que o sistema utiliza para obter certificados da entidade configurada. Para usar a autenticação de certificado de cliente, **Assinar**.
- Se a lista de **Modelos** estiver disponível, selecione o modelo que você adicionou sob a entidade PKI para o provedor de credenciais.

Esses modelos são disponibilizados quando as Entidades de serviços de certificado da Microsoft são adicionadas em **Configurações > Entidades PKI**.

4. Clique em **Avançar**.

A página **Provedores de credenciais: solicitação de assinatura de certificado** é exibida.

5. Na página **Credenciais de Fornecedores: solicitação de assinatura de certificado**, configure o seguinte de acordo com a configuração do seu certificado:

- **Algoritmo de chave:** escolha o algoritmo de chave para o novo par de chaves. Os valores disponíveis são **RSA**, **DSA** e **ECDSA**.
- **Tamanho da chave:** digite o tamanho, em bits, do par de chaves. Este campo é obrigatório.

Os valores permitidos dependem do tipo de chave. Por exemplo, o tamanho máximo para chaves DSA é de 1024 bits. Para evitar falsos negativos, o que depende do hardware e do software subjacentes, o XenMobile não impõe tamanhos de chave. Sempre teste as configurações do provedor de credenciais em um ambiente de teste antes de ativá-lo em produção.

- **Algoritmo de assinatura:** clique em um valor para o novo certificado. Os valores dependem do algoritmo de chave.
- **Nome de entidade:** necessário. Digite o Nome Diferenciado (DN) da entidade do novo certificado. Por exemplo: `CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } , C=${ user.c } \endquotation`

Por exemplo, para a autenticação de certificado de cliente, use estas configurações:

- **Algoritmo de chave:** RSA
 - **Tamanho da chave:** 2048
 - **Algoritmo de assinatura:** SHA256withRSA
 - **Nome de entidade:** `cn=${user.username}`
- Para adicionar uma entrada à tabela **Nomes alternativos de entidade**, clique em **Adicionar**. Selecione o tipo de nome alternativo e digite um valor na segunda coluna.

Para autenticação de certificado de cliente, especifique:

- **Tipo:** nome UPN
- **Valor:** `${user.userprincipalname}`

Assim como para o nome de entidade, você pode usar macros do XenMobile no campo de valor.

6. Clique em **Avançar**.

A página **Provedores de credenciais: distribuição** é exibida.

7. Na página **Provedores de credenciais: distribuição**, faça o seguinte:

- Na lista **Emissão de certificado de CA**, clique no certificado de CA oferecido. Como o provedor de credenciais usa uma entidade de CA discricionária, o certificado de CA do provedor de credenciais é sempre o certificado de CA configurado na própria entidade. O certificado de CA é apresentado aqui para consistência com configurações que usam entidades externas.
- Em **Selecionar modo de distribuição**, clique em uma das seguintes formas de gerar e distribuir chaves:
 - **Preferir modo centralizado: geração de chaves do lado do servidor:** a Citrix recomenda essa opção centralizada. Ela é compatível com todas as plataformas compatíveis com o XenMobile e é exigida quando a autenticação do Citrix Gateway é usada. As chaves privadas são geradas e armazenadas no servidor e distribuídas para os dispositivos do usuário.
 - **Preferir modo distribuído: geração de chaves do lado do dispositivo:** as chaves privadas são geradas e armazenadas nos dispositivos do usuário. Esse modo distribuído usa SCEP e requer um certificado de criptografia RA com o keyUsage

keyEncryption e um certificado de assinatura RA com o KeyUsage DigitalSignature. O mesmo certificado pode ser usado para autenticação e criptografia.

- **Somente distribuído: geração de chaves do lado do dispositivo:** Essa opção funciona da mesma forma que Preferir modo distribuído: geração de chaves do lado do dispositivo, exceto que, como é “Somente” em vez de “Preferir”, nenhuma opção estará disponível se a geração de chave do lado do dispositivo falhar ou não estiver disponível.

Se você tiver selecionado **Preferir modo distribuído: geração de chaves do lado do dispositivo** ou **Somente distribuído: geração de chaves do lado do dispositivo**, clique no certificado de assinatura RA e no certificado de criptografia RA. O mesmo certificado pode ser usado para ambos. Novos campos são exibidos para esses certificados.

8. Clique em **Avançar**.

A página **Provedores de credenciais: revogação XenMobile** é exibida. Nessa página, você pode configurar as condições sob as quais o XenMobile sinaliza internamente como revogados os certificados emitidos por essa configuração de provedor.

9. Na página **Provedores de credenciais: revogação XenMobile**, faça o seguinte:

- Em **Revogar certificados emitidos**, selecione uma das opções que indicam quando revogar os certificados.
- Para que o XenMobile envie uma notificação quando o certificado for revogado, defina o valor de **Enviar notificação** como **Ativado** e escolha um modelo de notificação.
- Para revogar o certificado na PKI quando ele tiver sido revogado do XenMobile, defina **Revogar certificado na PKI** como **Ativado** e, na **lista Entidade**, clique em um modelo. A lista Entidade mostra todas as entidades GPKI disponíveis com capacidades de revogação. Quando o certificado é revogado do XenMobile, uma chamada de revogação é enviada para a PKI selecionada da lista Entidade.

10. Clique em **Avançar**.

A página **Provedores de credenciais: revogação PKI** é exibida. Nessa página, identifique as ações a serem tomadas na PKI se o certificado for revogado. Você também tem a opção de criar uma mensagem de notificação.

11. Na página **Provedores de credenciais: revogação PKI**, faça o seguinte se você deseja revogar os certificados da PKI:

- Altere a configuração de **Ativar verificações de revogação externa** para **Ativado**. São exibidos mais campos relacionados à revogação PKI.
- Na lista **Certificado de AC do respondedor OCSP**, clique no nome distinto (DN) da entidade do certificado.

Você pode usar macros do XenMobile para os valores de campo de DN. Por exemplo: `CN=${ user.username } , OU=${ user.department } , O=${ user.companyname } , C=${ user.c }`

- Na lista **Quando o certificado for revogado**, clique em uma das seguintes ações a serem tomadas em relação à entidade PKI quando o certificado é revogado:
 - Não fazer nada.
 - Renovar o certificado.
 - Revogar e apagar o dispositivo.
- Para que o XenMobile envie uma notificação quando o certificado for revogado, defina o valor de **Enviar notificação** como **Ativado**.

Você pode escolher entre duas opções de notificação:

- Se você escolher **Selecionar modelo de notificação**, poderá selecionar uma mensagem de notificação previamente escrita que poderá personalizar. Esses modelos estão na lista Modelo de notificação.
- Se você selecionar **Inserir detalhes da notificação**, poderá escrever sua própria mensagem de notificação. Além de fornecer endereço de email do destinatário e a mensagem, você pode definir a frequência com que a notificação é enviada.

12. Clique em **Avançar**.

A página **Provedores de credenciais: renovação** é exibida. Nessa página, você pode configurar o XenMobile para fazer o seguinte:

- Renovar o certificado. Você pode, opcionalmente, enviar uma notificação sobre a renovação e, opcionalmente, excluir certificados já expirados da operação.
- Emitir uma notificação para os certificados que estão perto do vencimento (notificação antes da renovação).

13. Na página **Provedores de Credenciais: renovação**, faça o seguinte se desejar renovar os certificados quando eles expirarem:

Defina **Renovar certificados** quando eles expirarem para **Ativado**. Mais campos aparecem.

- No campo **Renovar quando o certificado expirar em**, digite quantos dias antes da expiração para renovar o certificado.
- Opcionalmente, selecione **Não renovar certificados que já expiraram**. Nesse caso, “já expiraram” significa que a data `NotAfter` está no passado, não que tenha sido revogada. O XenMobile não renova certificados depois que eles são revogados internamente.

Para que o XenMobile envie uma notificação quando o certificado tiver sido renovado, defina **Enviar notificação** como **Ativado**. Para que o XenMobile envie uma notificação quando o certificado estiver prestes a expirar, defina **Notificar quando o certificado estiver prestes a ex-**

pirar como **Ativado**.

Para qualquer uma dessas opções, você pode escolher entre duas opções de notificação:

- **Selecionar modelo de notificação:** selecione uma mensagem de notificação previamente escrita que você pode personalizar. Esses modelos estão na lista Modelo de notificação.
- **Inserir detalhes da notificação:** escreva a sua própria mensagem de notificação. Forneça o endereço de e-mail do destinatário, uma mensagem e uma frequência para enviar a notificação.

No campo **Notificar quando o certificado expira em**, digite quantos dias antes da expiração do certificado a notificação deve ser enviada.

14. Clique em **Salvar**.

O provedor de credenciais é exibido na tabela Provedor de Credenciais.

Certificados APNs

March 5, 2021

Importante:

O suporte da Apple para o protocolo binário legado APNs termina em 31 de março de 2021. A Apple recomenda que você use a API do provedor de APNs baseada em HTTP/2. A partir da versão 10.13.0, o XenMobile Server oferece suporte à API baseada em HTTP/2. Para obter mais informações, leia “Apple Push Notification Service Update” em <https://developer.apple.com/>. Para obter ajuda com a verificação da conectividade com APNs, consulte [Verificações de conectividade](#)

Para registrar e gerenciar dispositivos iOS e macOS no XenMobile, configure um certificado de serviço de Notificação por Push (APNs) da Apple.

Resumo do fluxo de trabalho:

- **Etapa 1:** Criar uma solicitação de assinatura de certificado (CSR) através de um destes métodos:
 - Criar uma CSR usando o Keychain Access no macOS (recomendado pela Citrix)
 - Criar uma CSR usando o Microsoft IIS
 - Criar uma CSR usando o OpenSSL
- **Etapa 2:** Assinar a CSR no XenMobile Tools
- **Etapa 3:** Enviar a CSR assinada para a Apple para obter o certificado de APNs
- **Etapa 4:** Utilizando o mesmo computador utilizado na Etapa 1, Completar a CSR e exportar um arquivo PKCS #12:

- Criar um arquivo PKCS #12 usando o Keychain Access no macOS
- Criar um arquivo PKCS #12 usando o Microsoft IIS
- Criar um arquivo PKCS #12 usando o OpenSSL
- **Etapa 5:** Importar um certificado de APNs para o XenMobile
- **Etapa 6:** Renovar um certificado de APNs

Criar uma solicitação de assinatura de certificado

Recomendamos que você crie uma CSR usando o Keychain Access no macOS. Você também pode criar uma CSR usando o Microsoft IIS ou o OpenSSL.

Importante:

- Para o ID Apple usado para criar o certificado:
 - O ID Apple deve ser um ID corporativo, não um ID pessoal.
 - Registre o ID Apple que você usa para criar o certificado.
 - Para renovar o certificado, use o mesmo nome da organização e o mesmo ID Apple. A utilização de um ID Apple diferente para renovar o certificado requer um novo registro do dispositivo.
- Se você acidentalmente ou intencionalmente revogar o certificado, perderá a capacidade de gerenciar os seus dispositivos.
- Se você usou o iOS Developer Enterprise Program para criar um certificado push do gerenciador de dispositivos móveis, certifique-se de manipular todas as ações para os certificados migrados no Apple Push Certificates Portal.

Criar uma CSR usando o Keychain Access no macOS

1. Em um computador com macOS, em **Aplicativos > Utilitários**, inicie o aplicativo Keychain Access.
2. Abra o menu **Keychain Access** e clique em **Certificate Assistant > Request a Certificate From a Certificate Authority**.
3. O Certificate Assistant solicita que você insira as seguintes informações:
 - **Email Address:** o endereço de email do indivíduo ou da conta de função responsável por gerenciar o certificado.
 - **Common Name:** o nome comum do indivíduo ou da conta de função responsável por gerenciar o certificado.
 - **CA Email Address:** o endereço de email da autoridade de certificação.
4. Selecione as opções **Saved to disk** e **Let me specify key pair information** e clique em **Continue**.

5. Insira um nome para o arquivo da CSR, salve o arquivo no seu computador e depois clique em **Save**.
6. Especifique as informações de par de chaves: selecione o **Key Size** de 2048 bits e o **RSA algorithm** e clique em **Continue**. O arquivo da CSR está pronto para que você o carregue como parte do processo de certificado de APNs.
7. Clique em **Done** quando o Certificate Assistant concluir o processo da CSR.
8. Para continuar, Assinar a CSR.

Criar uma CSR usando o Microsoft IIS

A primeira etapa para gerar uma solicitação de certificado de APNs é criar uma Solicitação de Assinatura de Certificado (CSR). Para Windows, gere uma CSR usando o Microsoft IIS.

1. Abra o Microsoft IIS.
2. Clique duas vezes no ícone Certificados do Servidor do IIS.
3. Na janela **Certificados do Servidor**, clique em **Criar Solicitação de Certificado**.
4. Digite as informações adequadas de Nome Diferenciado (DN) e clique em **Avançar**.
5. Selecione **Microsoft RSA SChannel Cryptographic Provider** como o Provedor de Serviços de Criptografia e **2048** como o comprimento de bit e, em seguida, clique em **Avançar**.
6. Insira um nome do arquivo, especifique uma localização para salvar a CSR e clique em **Concluir**.
7. Para continuar, Assinar a CSR.

Criar uma CSR usando o OpenSSL

Se não puder usar um dispositivo macOS ou o Microsoft IIS para gerar uma CSR, use o OpenSSL. Você pode baixar e instalar o OpenSSL a partir do site OpenSSL.

1. No computador no qual você instalar o OpenSSL, execute o seguinte comando a partir de um prompt de comando ou do shell.

```
openssl req -new -keyout Customer.key.pem -out CompanyAPNScertificate.  
csr -newkey rsa:2048
```

2. A mensagem de informações de nomenclatura de certificado a seguir é exibida. Insira as informações conforme solicitado.

```
1 You are about to be asked to enter information that will be  
   incorporated into your certificate request.  
2 What you are about to enter is what is called a Distinguished Name  
   or a DN.  
3 There are quite a few fields but you can leave some blank  
4 For some fields there will be a default value,  
5 If you enter '.', the field will be left blank.  
6 -----
```

```
7 Country Name (2 letter code) [AU]:US
8 State or Province Name (full name) [Some-State]:CA
9 Locality Name (eg, city) []:RWC
10 Organization Name (eg, company) [Internet Widgits Pty Ltd]:
    Customer
11 Organizational Unit Name (eg, section) [:Marketing
12 Common Name (eg, YOUR name) []:John Doe
13 Email Address []:john.doe@customer.com
14 <!--NeedCopy-->
```

3. Na mensagem seguinte, insira uma senha para a chave privada da CSR.

```
1 Please enter the following 'extra' attributes
2 to be sent with your certificate request
3 A challenge password []:
4 An optional company name []:
5 <!--NeedCopy-->
```

4. Para continuar, assine a CSR conforme descrito na próxima seção.

Assinar a CSR

Para usar um certificado com o XenMobile, envie-o à Citrix para assinatura. A Citrix assina a CSR com o respectivo certificado de assinatura de gerenciamento de dispositivo móvel e retorna o arquivo assinado em um formato `.plist`.

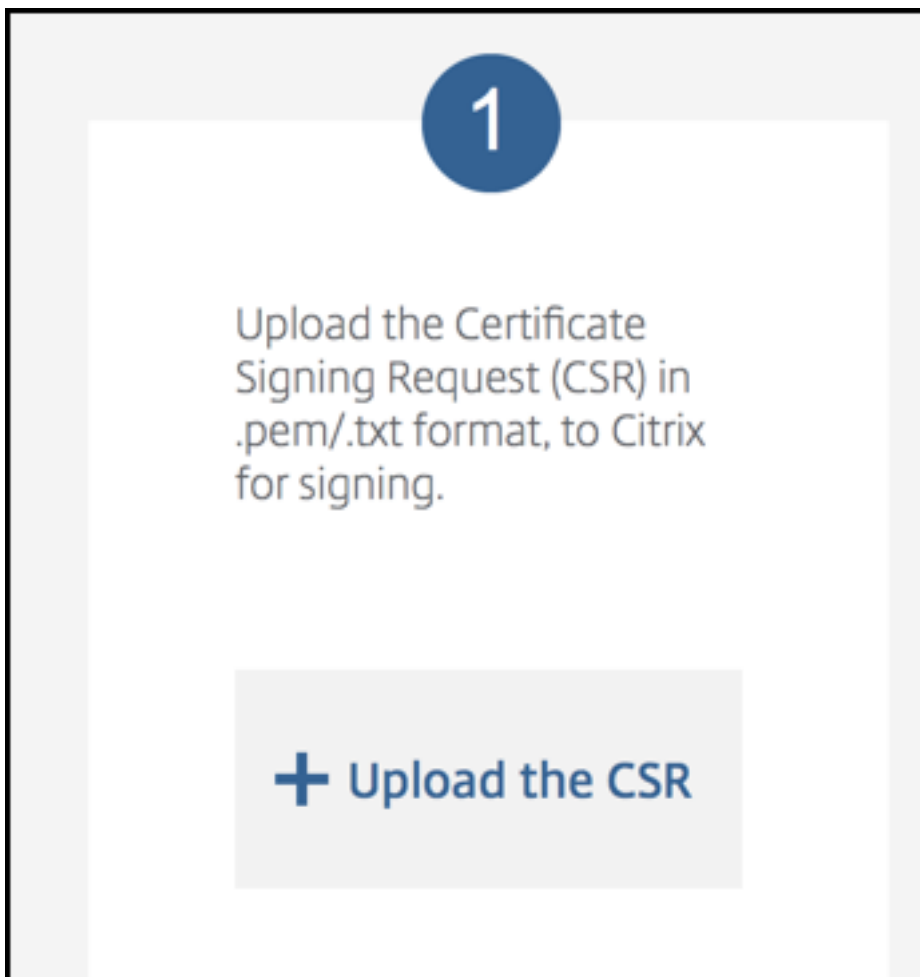
1. No navegador, acesse o site [Ferramentas do Endpoint Management](#) e clique em **Request push notification certificate signature**.

The screenshot shows the 'All Management Tools' page with the heading 'What do you want to do?'. Below the heading is a sub-heading: 'Endpoint Management Tools can help you troubleshoot your Endpoint Management Server set up and enable key features in your Endpoint Management deployment.' There are three main cards:

- Analyze and Troubleshoot my Endpoint Management environment**: Endpoint Management Analyzer. Follow steps to identify and triage potential issues with your deployment.
- Request Auto Discovery**: Auto Discovery Service. Request and Configure Auto Discovery for your domain's Endpoint Management Server.
- Request push notification certificate signature**: Create APNs Certificate. Submit a request to Citrix to sign an APNs certificate, which you then submit to Apple.

The 'Request push notification certificate signature' card is highlighted with a purple border.

2. Na página **Creating a new certificate**, clique em **Upload the CSR**.



3. Procure e selecione o certificado.
O certificado deve estar no formato .pem/.txt.
4. Na página **Endpoint Management APNs CSR Signing**, clique em **Sign**. A CSR é assinada e salva automaticamente na sua pasta configurada de downloads.
5. Para continuar, envie a CSR assinada conforme descrito na próxima seção.

Enviar a CSR assinada para a Apple para obter o certificado de APNs

Depois de receber a sua Solicitação de Assinatura de Certificado (CSR) assinada da Citrix, você precisará enviar a CSR para a Apple para obter o certificado de APNs necessário para importar para o XenMobile.

Nota:

Alguns usuários relataram problemas ao fazer login no Apple Push Portal. Como alternativa, faça

logon no [Apple Developer Portal](#) e siga estes passos.

1. Em um navegador, vá para o [Apple Push Certificates Portal](#).
2. Clique em **Create a Certificate**.
3. Na primeira vez em que você cria um certificado junto à Apple, marque a caixa de seleção **I have read and agree to these terms and conditions** e clique em **Accept**.
4. Clique em **Choose File**, navegue até a CSR assinada no seu computador e clique em **Upload**. Uma mensagem de confirmação indica que o carregamento foi bem-sucedido.
5. Clique em **Download** para recuperar o certificado .pem.
6. Para continuar, conclua a CSR e exporte um arquivo PKCS #12 conforme descrito na próxima seção.

Completar a CSR e exportar um arquivo PKCS #12

Depois de receber o certificado APNs da Apple, volte para o Keychain Access, Microsoft IIS ou OpenSSL para exportar o certificado para um arquivo PCKS #12.

Um arquivo PKCS #12 contém o arquivo de certificado APNs e sua chave privada. Os arquivos PFX geralmente têm a extensão .pfx ou .p12. Você pode usar arquivos .pfx e .p12 de forma intercambiável.

Importante:

A Citrix recomenda que você salve ou exporte as chaves pessoal e pública do sistema local. Você precisa das chaves para acessar os certificados APNs para reutilização. Sem as mesmas chaves, seu certificado é inválido e você deve repetir todo o processo CSR e APNs.

Criar um arquivo PKCS #12 usando o Keychain Access no macOS

Importante:

Para esta tarefa, use o mesmo dispositivo macOS que você usou para gerar a CSR.

1. No dispositivo, localize o certificado de identidade Production (.pem) recebido da Apple.
2. Inicie o aplicativo Keychain Access e navegue até a guia **Login > My Certificates**. Arraste e solte o certificado de identidade do produto na janela aberta.
3. Clique no certificado e expanda a seta à esquerda para verificar se o certificado inclui uma chave privada associada.
4. Para começar a exportar o certificado para um certificado PCKS #12 (.pfx), escolha o certificado e a chave privada, clique com o botão direito do mouse e selecione **Export 2 items**.

5. Dê ao arquivo de certificado um nome exclusivo para uso com o XenMobile. Não inclua espaços no nome. Em seguida, escolha o local da pasta para o certificado salvo, selecione o formato de arquivo .pfx e clique em **Salvar**.
6. Insira uma senha para exportar o certificado. A Citrix recomenda que você use uma senha única e forte. Além disso, mantenha o certificado e a senha protegidos para uso e referência posteriores.
7. O aplicativo Keychain Access solicitará a senha de login ou as chaves selecionadas. Digite a senha e clique em **OK**. O certificado salvo agora está pronto para ser usado com o servidor XenMobile.
8. Para continuar, consulte Importar um certificado de APNs para o XenMobile.

Criar um arquivo PKCS #12 usando o Microsoft IIS

Importante:

Para essa tarefa, use o mesmo servidor IIS que você usou para gerar a CSR.

1. Abra o Microsoft IIS.
2. Clique no ícone **Certificados do Servidor**.
3. Na janela **Certificados do Servidor**, clique em **Concluir Solicitação de Certificado**.
4. Procure o arquivo Certificate.pem da Apple. Em seguida, digite um nome amigável ou o nome do certificado, e clique em **OK**. Não inclua espaços no nome.
5. Selecione o certificado que você identificou na etapa 4 e clique em **Exportar**.
6. Especifique a localização e nome do arquivo de certificado .pfx e uma senha; depois clique em **OK**.
Você precisa da senha do certificado para importá-lo para o XenMobile.
7. Copie o certificado .pfx para o servidor no qual planeja instalar o XenMobile.
8. Para continuar, consulte Importar um certificado de APNs para o XenMobile.

Criar um arquivo PKCS #12 usando o OpenSSL

Se você usar o OpenSSL para criar uma CSR, também poderá usar o OpenSSL para criar um certificado de APNs. pfx.

1. Em um prompt de comando ou shell, execute o seguinte comando. `Customer.privatekey.pem` é a chave privada da sua CSR. `APNs_Certificate.pem` é o certificado que você acabou de receber da Apple.

```
openssl pkcs12 -export -in APNs_Certificate.pem -inkey Customer.privatekey.pem -out apns_identity.pfx
```

2. Insira uma senha para o arquivo de certificado .pfx. Guarde essa senha, pois você a usará novamente quando carregar o certificado para o XenMobile.
3. Anote a localização do arquivo de certificado .pfx. Depois copie o arquivo para o XenMobile Server para que você possa usar o console para carregar o arquivo.
4. Para continuar, importe um certificado APNs para o XenMobile conforme descrito na próxima seção.

Importar um certificado de APNs para o XenMobile

Depois de receber o novo certificado de APNs, importe-o para o XenMobile para adicioná-lo pela primeira vez ou para substituir um certificado existente.

1. No console XenMobile, clique em **Configurações > Certificados**.
2. Clique em **Importar > Keystore**.
3. Em **Usar como**, selecione **APNs**.
4. Navegue até o arquivo .pfx ou .p12 no seu computador.
5. Insira uma senha e clique em **Importar**.

Para obter mais informações sobre certificados no XenMobile, consulte [Certificados e autenticação](#).

Renovar um certificado de APNs

Importante:

Se você utilizar um ID Apple diferente para o processo de renovação, deverá registrar novamente os dispositivos de usuário

Para renovar um certificado APNs, execute as etapas para criar um certificado e, em seguida, vá para o [Apple Push Certificates Portal](#). Use o portal para carregar o novo certificado. Depois de fazer login, o seu certificado existente ou um certificado importado da sua conta anterior do Apple Developers é exibido.

No Certificates Portal, a única diferença para a renovação do certificado é que você clica em **Renew**. Você deve ter uma conta de desenvolvedor no Certificates Portal para acessar o site. Para renovar o certificado, use o mesmo nome da organização e o mesmo ID Apple.

Para determinar quando o seu certificado de APNs expira, no console XenMobile, vá para **Configurações > Certificados**. Se o certificado expirar, não o revogue.

1. Gere uma CSR usando o Microsoft IIS, Keychain Access (macOS) ou OpenSSL. Para obter mais informações sobre como gerar uma CSR, consulte Criar uma solicitação de assinatura de certificado.
2. No seu navegador, vá para [XenMobile Tools](#). Clique em **Request push notification certificate signature**.
3. Clique em **+ Upload the CSR**.
4. Na caixa de diálogo, navegue até a CSR, clique em **Open** e clique em **Login**.
5. Quando você receber um arquivo `.plist`, salve-o.
6. No título da etapa 3, clique em **Apple Push Certificates Portal** e faça login.
7. Selecione o certificado que deseja renovar e clique em **Renew**.
8. Carregue o arquivo `.plist`. Você receberá um arquivo `.pem` como resultado. Salve o arquivo `.pem`.
9. Usando esse arquivo `.pem`, preencha a CSR (de acordo com o método usado para criar a CSR na Etapa 1).
10. Exporte o certificado como um arquivo `.pfx`.

No console XenMobile, importe o arquivo `.pfx` e conclua a configuração da seguinte maneira:

1. Vá para **Configurações > Certificados > Importar**.
2. No **menu Importar**, selecione **Keystore**.
3. No menu **Tipo de keystore**, escolha **PKCS #12**.
4. Em **Usar como**, selecione **APNs**.

Import ✕

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time. Use the [APNs portal](#) on the Endpoint Management Tools page to create the APNs certificate.

Import Keystore

Keystore type PKCS#12

Use as APNs

Keystore file *

Password *

Description

5. Em **Arquivo de keystore**, clique em **Procurar** e navegue até o arquivo.
6. Em **Senha**, digite a senha do certificado.
7. Digite uma **Descrição** opcional.
8. Clique em **Importar**.

O XenMobile redireciona você de volta à página **Certificados**. Os campos **Nome**, **Status**, **Válido de** e **Válido até** são atualizados.

SAML para logon único com Citrix Files

March 5, 2021

Você pode configurar o XenMobile e o Citrix Content Collaboration para usar SAML (Security Assertion Markup Language) para fornecer acesso via logon único (SSO) a aplicativos móveis do Citrix Files. Essa funcionalidade inclui:

- Aplicativos Citrix Files que são habilitados para MAM SDK ou preparados usando o MDX Service ou MDX Toolkit
- Clientes do Citrix Files não preparados, como site, plug-in do Outlook ou clientes de sincronização
- **Para aplicativos Citrix Files preparados.** Os usuários que fazem login no Citrix Files por meio do aplicativo móvel do Citrix Files são redirecionados para o Secure Hub para autenticação do usuário e para obter um token SAML. Após a autenticação bem-sucedida, o aplicativo móvel do Citrix Files envia o token SAML para o Content Collaboration. Após o logon inicial, os usuários podem acessar o aplicativo móvel do Citrix Files por meio de SSO. Eles também podem anexar documentos do Content Collaboration a emails do Secure Mail sem fazer login todas as vezes.
- **Para clientes Citrix Files não preparados.** Os usuários que fazem login no Citrix Files usando um navegador da Web ou outro cliente Citrix Files são redirecionados para o XenMobile. O XenMobile autentica os usuários, que então adquirem um token SAML que é enviado para o Content Collaboration. Após o login inicial, os usuários podem acessar os clientes Citrix Files por meio de SSO sem fazer login toda vez.

Para usar o XenMobile como um provedor de identidade de SAML (IdP) para o Content Collaboration, você deve configurar o XenMobile para usar com contas da empresa, conforme descrito neste artigo. Como alternativa, você pode configurar o XenMobile para funcionar apenas com conectores de zona de armazenamento. Para obter mais informações, consulte [Usar Citrix Content Collaboration com XenMobile](#).

Para um diagrama da arquitetura de referência detalhada, consulte [Arquitetura](#).

Pré-requisitos

Conclua os pré-requisitos antes de configurar o SSO com aplicativos Citrix Files e XenMobile:

- O MAM SDK ou uma versão compatível do MDX Toolkit (para aplicativos móveis do Citrix Files).
Para obter mais informações, consulte [Compatibilidade do XenMobile](#).
- Uma versão compatível de aplicativos móveis do Citrix Files e Secure Hub.
- Conta de administrador do Content Collaboration.
- Conectividade verificada entre o XenMobile e o Content Collaboration.

Configurar acesso ao Content Collaboration

Antes de configurar o SAML para Content Collaboration, forneça as informações de acesso ao Content Collaboration da seguinte forma:

1. No console da Web do XenMobile, clique em **Configurar > ShareFile**. A página de configuração do **ShareFile** é exibida. Seu console pode mostrar o termo Content Collaboration em vez de ShareFile.

Content Collaboration ▾
Configure settings to connect to the Content Collaboration and administrator service accounts for user account management.

Domain *

Assign to delivery groups

AllUsers
 Local Policy
 o87
 Local

Content Collaboration Administrator Account Logon

User name *

Password *

User account provisioning OFF

App Internal name

SAML certificate

Name

Advanced Content Collaboration Configuration

2. Defina estas configurações:
 - **Domínio:** digite o nome do subdomínio do Content Collaboration. Por exemplo: `example.sharefile.com`.
 - **Atribuir a grupos de entrega:** selecione ou pesquise os grupos de entrega nos quais você deseja usar o SSO com o Content Collaboration.
 - **Logon de conta de administrador do ShareFile**
 - **Nome do usuário:** digite o nome de usuário do administrador do Content Collaboration. Esse usuário deve ter privilégios de administrador.
 - **Senha:** digite a senha do administrador do Content Collaboration.
 - **Provisionamento de conta de usuário:** deixe esta configuração desativada. Use a Ferramenta de gerenciamento de usuários do Content Collaboration para o provisionamento do usuário. Consulte [Provisionar contas de usuário e grupos de distribuição](#).
3. Clique em **Testar conexão** para verificar se o nome de usuário e a senha para a conta de administrador do Content Collaboration autenticam a conta especificada do Content Collaboration.

4. Clique em **Salvar**.

- O XenMobile sincroniza com o Content Collaboration e atualiza as configurações do Content Collaboration **Emissor de ShareFile/ID de entidade** e **URL de Login**.
- A página **Configurar > ShareFile** mostra o **Nome interno do aplicativo**. Você precisa desse nome para concluir as etapas descritas posteriormente em Modificar as configurações de SSO do Citrix Files.com.

Configurar SAML para aplicativos Citrix Files MDX preparados

Você não precisa usar o Citrix Gateway para configuração de logon único com aplicativos Citrix Files MDX preparados. Para configurar o acesso para clientes Citrix Files não preparados, como o site, o plug-in do Outlook ou os clientes de sincronização, consulte [Configurar o Citrix Gateway para outros clientes Citrix Gateway](#).

As etapas a seguir se aplicam aos aplicativos e dispositivos iOS e Android. Para configurar SAML para aplicativos Citrix Files MDX preparados:

1. Com o MDX Toolkit, prepare o aplicativo móvel do Citrix Files. Para obter mais informações sobre como preparar aplicativos com o MDX Toolkit, consulte [Preparação de aplicativos com o MDX Toolkit](#).
2. No console XenMobile, carregue o aplicativo móvel preparado do Citrix Files. Para obter informações sobre como carregar aplicativos MDX, consulte [Para adicionar um aplicativo MDX ao XenMobile](#).
3. Verifique as configurações de SAML: faça login no Content Collaboration com o nome de usuário e a senha de administrador que você configurou anteriormente.
4. Verifique se o Content Collaboration e o XenMobile estão configurados para o mesmo fuso horário. Certifique-se de que o XenMobile mostre a hora correta para o fuso horário configurado. Caso contrário, o SSO pode falhar.

Validar o aplicativo móvel do Citrix Files

1. No dispositivo do usuário, instale e configure o Secure Hub.
2. Na XenMobile Store, baixe e instale o aplicativo móvel do Citrix Files.
3. Inicie o aplicativo móvel do Citrix Files. O Citrix Files é iniciado sem solicitar nome de usuário ou senha.

Validar com Secure Mail

1. No dispositivo do usuário, caso ainda não tenha sido feito, instale e configure o Secure Hub.

2. Na XenMobile Store, baixe, instale e configure o Secure Mail.
3. Abra um novo formulário de email e toque em **Anexar do Citrix Files**. Os arquivos disponíveis para serem anexados ao email são mostrados sem a necessidade de informar nome do usuário ou senha.

Configurar o Citrix Gateway para outros clientes Citrix Gateway

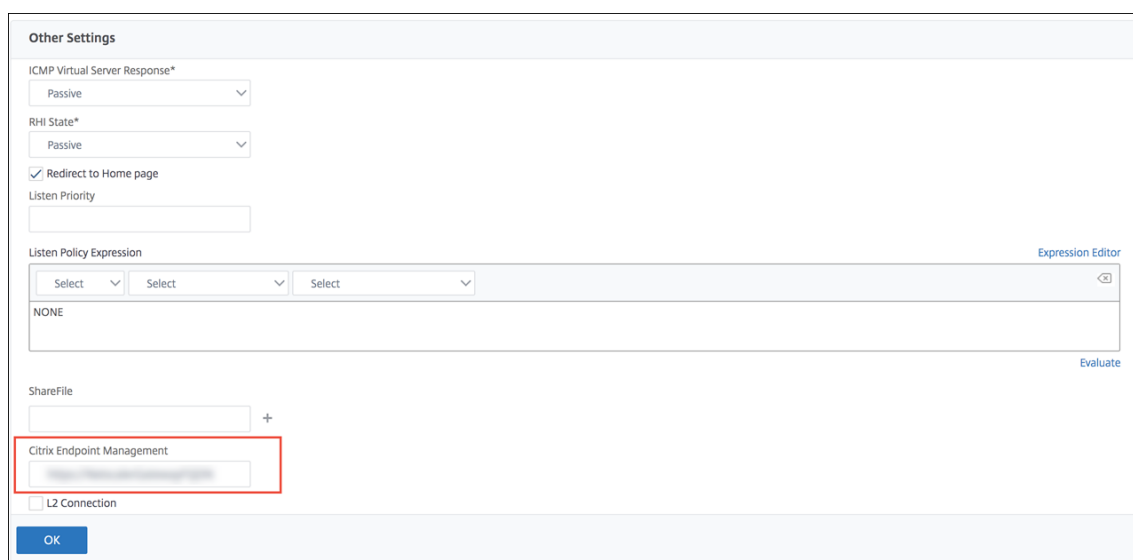
Para configurar o acesso aos clientes do Citrix Files não preparados, como site da Web, plug-in do Outlook ou clientes de sincronização, configure o Citrix Gateway para dar suporte ao uso do XenMobile como um provedor de identidade SAML da maneira a seguir.

- Desative o redirecionamento de página inicial.
- Crie um perfil e uma política de sessão Citrix Files.
- Configure políticas no servidor virtual do Citrix Gateway.

Desative o redirecionamento de página inicial

Desative o comportamento padrão para solicitações que chegam pelo caminho /cginfra. Essa ação permite que os usuários vejam a URL interna solicitada original em vez da página inicial configurada.

1. Edite as configurações do servidor virtual do Citrix Gateway usado para logins no XenMobile. No Citrix ADC, acesse **Other Settings** e desmarque a caixa de seleção **Redirect to Home Page**.



The screenshot shows the 'Other Settings' configuration page in Citrix Gateway. The 'Redirect to Home page' checkbox is checked. The 'Citrix Endpoint Management' field is highlighted with a red box. The 'ShareFile' field is empty. The 'L2 Connection' checkbox is unchecked. The 'OK' button is visible at the bottom.

2. Em **ShareFile** (agora chamado de Content Collaboration), digite o nome e o número da porta do servidor interno do XenMobile.
3. Em **Citrix Endpoint Management**, digite sua URL do XenMobile. Sua versão do Citrix Gateway pode se referir ao nome de produto mais antigo, **App Controller**.

Essa configuração autoriza as solicitações da URL inserida por meio do caminho /cginfra.

Criar uma política de sessão e um perfil de solicitação do Citrix Files

Defina estas configurações para criar uma política de sessão e um perfil de solicitação do Citrix Files:

1. No utilitário de configuração do Citrix Gateway, no painel de navegação esquerdo, clique em **Citrix Gateway > Políticas > Session**.
2. Crie uma política de sessão. Na guia **Políticas**, clique em **Add**.
3. No campo **Name**, digite **ShareFile_Policy**.
4. Crie uma ação clicando no botão **+**. A página **Create Session Profile** é exibida.

Configure NetScaler Gateway Session Profile

Configure NetScaler Gateway Session Profile

Name
Sharefile_Profile

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration Client Experience Security Published Applications

Accounting Policy

Override Global

Display Home Page

Home Page
none

URL for Web-Based Email

Split Tunnel*
OFF

Session Time-out (mins)
1

Client Idle Time-out (mins)

Clientless Access*
Allow

Clientless Access URL Encoding*
Obscure

Clientless Access Persistent Cookie*
DENY

Plug-in Type*
Windows/MAC OS X

Single Sign-on to Web Applications

Credential Index*
PRIMARY

KCD Account

Defina estas configurações:

- **Name:** digite **ShareFile_Profile**.
- Clique na guia **Client Experience** e defina estas configurações:
 - **Home Page:** digite **none**.
 - **Session Time-out (mins):** digite **1**.
 - **Single Sign-on to Web Applications:** selecione esta configuração.

- **Credential Index:** clique em **PRIMARY**.
- Clique na guia **Published Applications**.

The screenshot shows the 'Configure NetScaler Gateway Session Profile' dialog box with the 'Published Applications' tab selected. The 'Name' field contains 'Sharefile_Profile'. Below the name field, a note states: 'Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.' The 'Override Global' section contains the following settings:

- ICA Proxy*:** ON (checked)
- Web Interface Address:** https://xms.citrix.lab:8443 (checked)
- Web Interface Address Type*:** IPV4
- Web Interface Portal Mode*:** NORMAL (unchecked)
- Single Sign-on Domain:** citrix (checked)
- Citrix Receiver Home Page:** (unchecked)
- Account Services Address:** (unchecked)

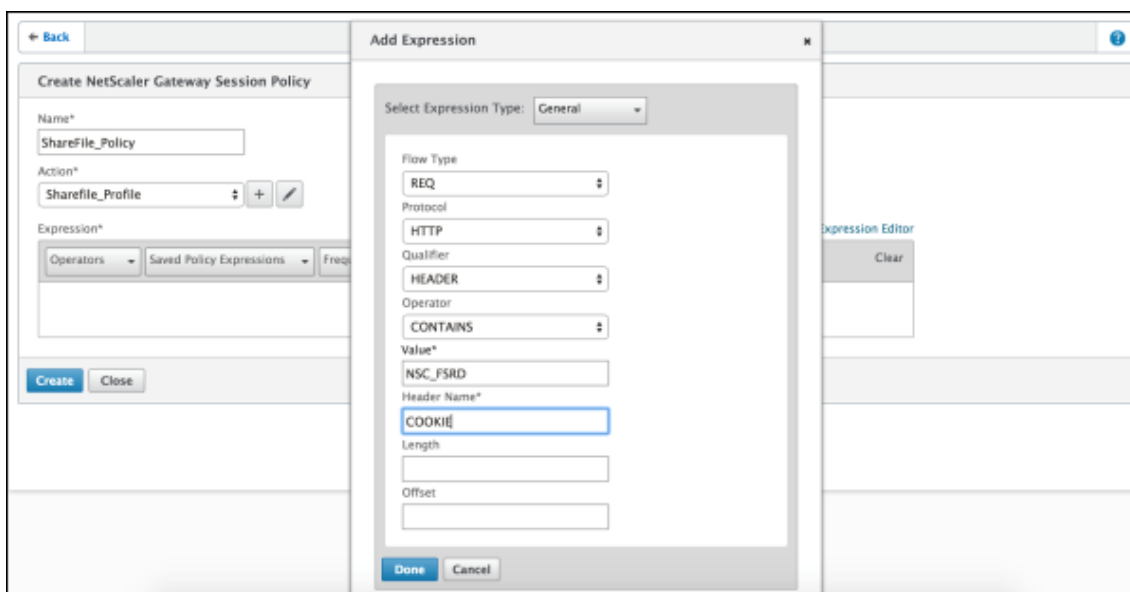
At the bottom of the dialog are 'OK' and 'Close' buttons.

Defina estas configurações:

- **ICA Proxy:** clique em **ON**.
- **Web Interface Address:** digite sua URL do XenMobile Server.
- **Single Sign-on Domain:** digite o nome do domínio do Active Directory.

Durante a configuração do Citrix Gateway Session Profile, o sufixo de domínio para **Single Sign-on Domain** deve corresponder ao alias de domínio do XenMobile definido no LDAP.

5. Clique em **Create** para definir o perfil de sessão.
6. Clique em **Expression Editor**.



Defina estas configurações:

- **Value:** digite **NSC_FSRD**.
- **Header Name:** digite **COOKIE**.

7. Clique em **Create** e em **Close**.



Configurar políticas no servidor virtual do Citrix Gateway

Defina estas configurações no servidor virtual do Citrix Gateway.

1. No utilitário de configuração do Citrix Gateway, no painel de navegação esquerdo, clique em **Citrix Gateway > Virtual Servers**.
2. No painel **Details**, clique em seu servidor virtual do Citrix Gateway.
3. Clique em **Edit**.
4. Clique em **Configured policies > Session policies** e em **Add binding**.

5. Selecione **ShareFile_Policy**.
6. Edite o número de **Priority** gerado automaticamente para a política selecionada, para que ele tenha a prioridade mais alta (o menor número) em relação às outras políticas listadas. Por exemplo:

Priority	Policy Name	Expression	Action
10	ShareFile_Policy	REQ.HTTP.HEADER Cookie CONTAINS NSC_FSRD	Sharefile_Profile
100	PL_OS_10.217.232.36	REQ.HTTP.HEADER User-Agent CONTAINS CitrixR...	AC_OS_10.217.232.36_A_
100	PL_WB_10.217.232.36	REQ.HTTP.HEADER User-Agent NOTCONTAINS Cl...	AC_WB_10.217.232.36_A_
100	PL_AG_PLG_10.217.232.36	REQ.HTTP.HEADER User-Agent NOTCONTAINS Cl...	AC_AG_PLG_10.217.232.36_A_

7. Clique em **Done** e salve a configuração do Citrix ADC em execução.

Modificar as configurações de SSO do Citrix Files.com

Faça as seguintes alterações para aplicativos Citrix Files MDX e não-MDX.

Importante:

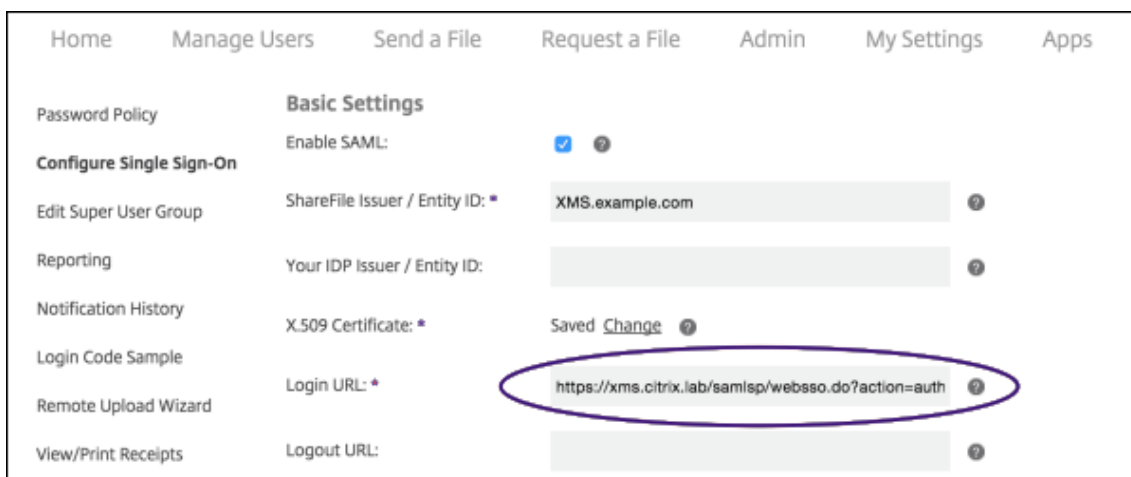
Um novo número é anexado ao nome do aplicativo interno:

- Cada vez que você edita ou recria o aplicativo Citrix Files
- Cada vez que você altera as configurações de Content Collaboration no XenMobile

Como resultado, você também deve atualizar a URL de Login no site do Citrix Files para refletir o nome do aplicativo atualizado.

1. Faça login na sua conta do Content Collaboration (<https://<subdomain>.sharefile.com>) como administrador do Content Collaboration.
2. Na interface da Web do Content Collaboration, clique em **Administrador** e selecione **Configurar logon único**.
3. Edite a **URL de login** da seguinte maneira:

Aqui está um exemplo de **URL de login** antes das edições: https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1.



- Insira o FQDN externo do servidor virtual do Citrix Gateway mais **/cginfra/https/** na frente do FQDN do XenMobile Server e adicione **8443** após o FQDN do XenMobile.

Aqui está uma amostra de um URL editado: https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1

- Altere o parâmetro **&app=ShareFile_SAML_SP** para o nome do aplicativo do Citrix Files interno. O nome interno é **ShareFile_SAML** por padrão. No entanto, toda vez que você altera sua configuração, um número é anexado ao nome interno (**ShareFile_SAML_2**, **ShareFile_SAML_3** e assim por diante). Você pode procurar o **nome interno do aplicativo** na página **Configurar > ShareFile**.

Aqui está uma amostra de um URL editado: https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1

- Adicione **&nssso=true** ao final da URL.

Aqui está uma amostra da URL final: https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1&nssso=true.

4. Em **Configurações opcionais**, marque a caixa de seleção **Ativar autenticação da Web**.

Optional Settings

Require SSO Login: ?

SSO IP Range: ?

SP-Initiated SSO certificate: HTTP Redirect with no signature ?

Enable Web Authentication: ?

SP-Initiated Auth Context: User Name and Password Minimum ?

Active Profile Cookies: ?

Save Cancel

Validar a configuração

Siga os procedimentos a seguir para validar a configuração.

1. Aponte seu navegador para <https://<subdomain>sharefile.com/saml/login>.
Você será redirecionado para o formulário de logon do Citrix Gateway. Se você não for redirecionado, verifique as definições de configuração anteriores.
2. Insira o nome do usuário e a senha do Citrix Gateway e do ambiente do XenMobile configurado.
As suas pastas do Citrix Files no <subdomain>.sharefile.com são exibidas. Se você não vir as pastas do Citrix Files, verifique se inseriu as credenciais de login corretas.

Azure Active Directory como IdP

May 24, 2021

Configurar o Azure Active Directory (AAD) como seu provedor de identidade (IdP) permite que os usuários se registrem no XenMobile usando suas credenciais do Azure.

iOS, Android e Windows 10 dispositivos são compatíveis. Dispositivos iOS e Android são registrados por meio do Secure Hub. Esse método de autenticação está disponível apenas para usuários que se registram no MDM por meio do Citrix Secure Hub. Os dispositivos que se registram no MAM não podem ser autenticados usando as credenciais AAD. Para usar o Secure Hub com MDM+MAM, configure o XenMobile para usar o Citrix Gateway para registro no MAM. Para obter mais informações, consulte [Citrix Gateway e XenMobile](#).

Configure o Azure como o seu IdP em **Configurações > Autenticação > IDP**. A página **IDP** é nova nesta versão do XenMobile. Em versões anteriores do XenMobile, você configurava o Azure em **Configurações > Microsoft Azure**.

Requisitos

- Versões e licenças
 - Para registrar dispositivos Android ou iOS, você precisa do Secure Hub 10.5.5.
 - Para registrar dispositivos Windows 10, você precisa de licenças do Microsoft Azure Premium.
- Serviços e autenticação de diretório
 - O XenMobile Server deve ser configurado para a autenticação baseada em certificado.
 - Se você estiver usando Citrix ADC para autenticação, o Citrix ADC deve ser configurado para autenticação baseada em certificado.
 - A autenticação do Secure Hub usa o Azure AD e respeita o modo de autenticação definido no Azure AD.
 - O XenMobile Server deve se conectar ao Windows Active Directory (AD) usando o LDAP. Configure o servidor LDAP local para sincronizar com o Azure AD.

Fluxo de autenticação

Quando o dispositivo se registra por meio do Secure Hub e o XenMobile está configurado para usar o Azure como seu IdP:

1. Os usuários inserem o nome de usuário e a senha do Active Directory do Azure em seus dispositivos, na tela de logon do Azure AD mostrada no Secure Hub.
2. O Azure AD valida o usuário e envia um token de ID.
3. O Secure Hub compartilha o token de ID com o XenMobile Server.
4. O XenMobile valida o token de ID e as informações do usuário presentes nesse token. O XenMobile retorna um ID de sessão.

Configuração da conta do Azure

Para usar o Azure AD como seu IdP, primeiro faça login na sua conta do Azure e faça estas alterações:

1. Registre o seu domínio personalizado e verifique esse domínio. Para obter detalhes, consulte [Adicionar seu próprio nome de domínio ao Active Directory do Azure](#).
2. Estenda seu diretório local para o Active Directory do Azure usando ferramentas de integração de diretório. Para obter detalhes, consulte [Integração de Diretórios](#).

Para usar o AD do Azure para registrar dispositivos Windows 10, faça as seguintes alterações na sua conta do Azure:

1. Torne o MDM uma parte confiável de AD do Azure. Para fazer isso, clique em **Active Directory do Azure > Aplicativos** e clique em **Adicionar**.
2. Selecione **Adicionar um aplicativo** na galeria. Acesse **MOBILE DEVICE MANAGEMENT** e selecione **Aplicativo MDM no local**. Salve as configurações.

Você escolhe o aplicativo local mesmo se tiver se inscrito na nuvem do Citrix XenMobile. Na terminologia da Microsoft, qualquer aplicativo não multilocatário é um aplicativo MDM local.

3. No aplicativo, configure a descoberta do XenMobile Server, os pontos de extremidade dos termos de uso e a URI do ID de aplicativo, da seguinte forma:

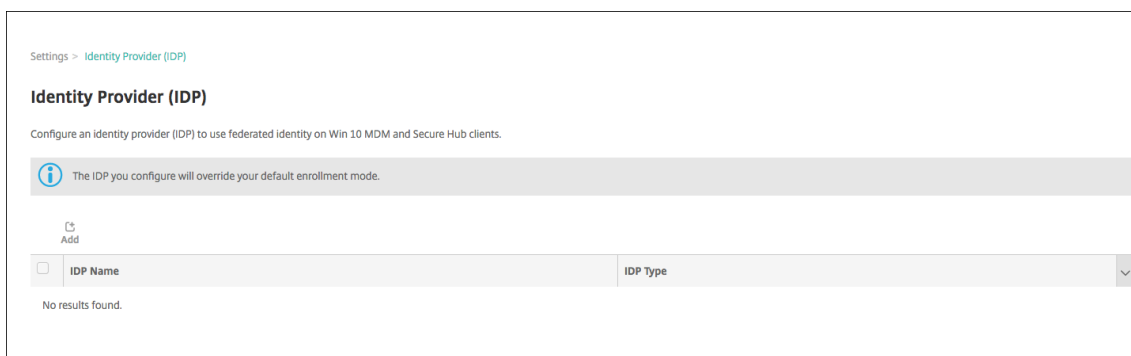
- **URL de descoberta do MDM:** `https://<FQDN>:8443/<instanceName>/wpe`
- **URL dos Termos de Uso do MDM:** `https://<FQDN>:8443/<instanceName>/wpe/tou`
- **URI de ID do aplicativo** `https://<FQDN>:8443/`

4. Selecione o aplicativo MDM local que você criou na etapa 2. Ative a opção **Gerenciar dispositivos para estes usuários** para permitir o gerenciamento de MDM para todos os usuários ou para qualquer grupo específico de usuários.

Para obter mais informações sobre como usar o Azure AD com dispositivos Windows 10, consulte o artigo da Microsoft [Azure Active Directory integration with MDM](#).

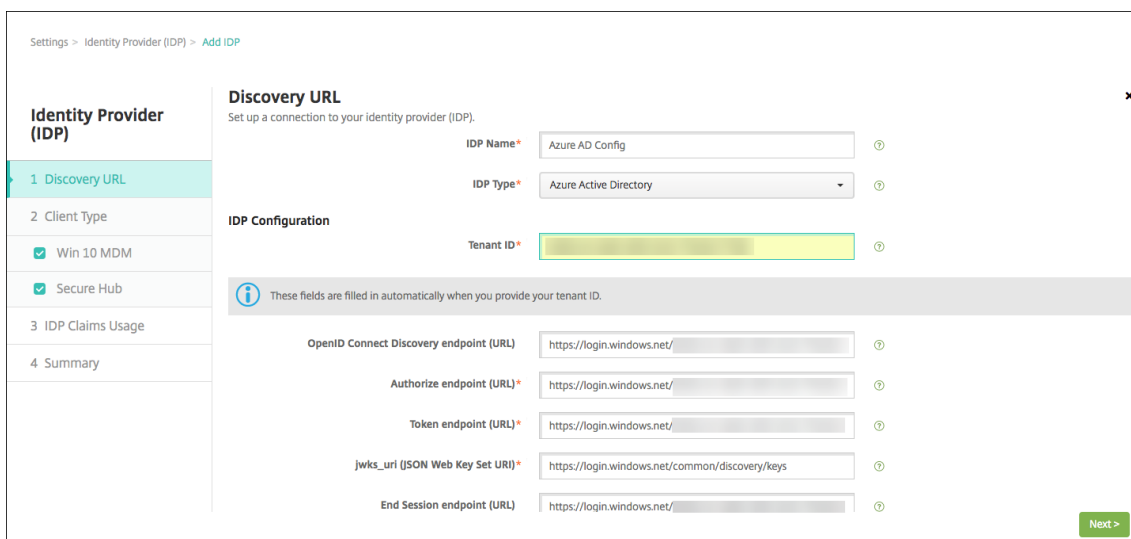
Configurar o AD do Azure como seu IdP

1. Localize ou anote as informações necessárias da sua conta do Azure:
 - ID de locatário, na página de configurações do aplicativo Azure.
 - Se quiser usar o Azure AD para registrar dispositivos Windows 10, você também precisará do seguinte:
 - **URI do ID de aplicativo:** a URL do servidor que executa o XenMobile.
 - **ID do cliente:** o identificador exclusivo do seu aplicativo, na página de configuração do Azure.
 - **Chave:** na página de configurações do aplicativo Azure.
2. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida.
3. Em **Autenticação**, clique em **Provedor de identidade (IDP)**. A página **Provedor de identidade** é exibida.



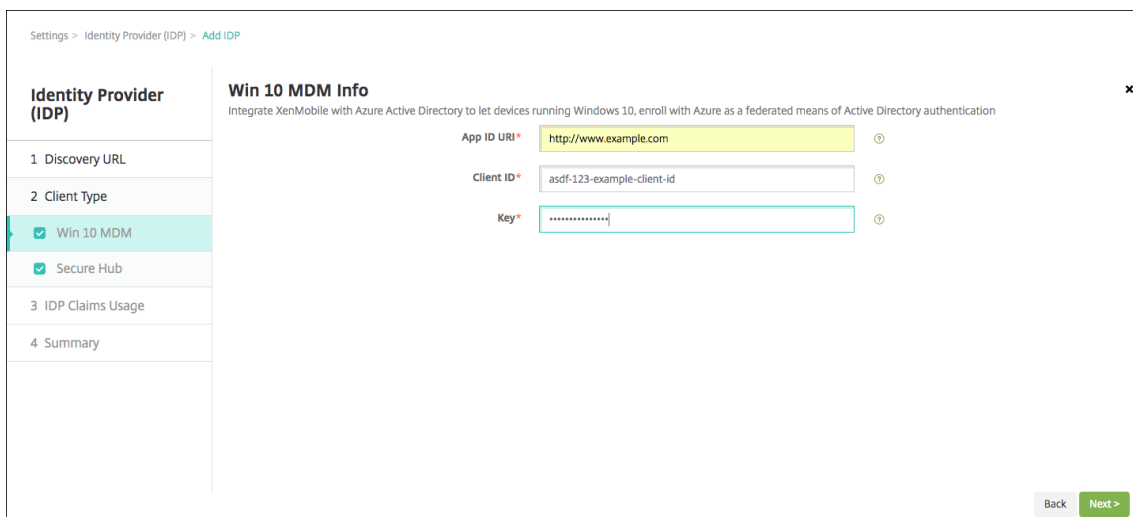
4. Clique em **Add**. A página **Configuração IDP** é exibida.
5. Configure as seguintes informações sobre seu IdP:
 - **Nome do IDP:** digite um nome para a conexão com o IdP que você está criando.
 - **Tipo de IDP:** escolha Azure Active Directory como tipo de IdP.
 - **ID do locatário:** copie esse valor da página de configurações do aplicativo Azure. Na barra de endereços do navegador, copie a seção composta por números e letras.

Por exemplo, em <https://manage.windowsazure.com/acmew.onmicrosoft.com/#workspaces/ActiveDirectoryExtensin/Directory/abc213-abc123-abc123/onprem...>, o ID do locatário é: `abc123-abc123-abc123`.



6. O restante dos campos é preenchido automaticamente. Quando eles estiverem preenchidos, clique em **Avançar**.
7. Para configurar o XenMobile para registrar dispositivos Windows 10 usando o AD do Azure para registro do MDM, defina as seguintes configurações. Para ignorar essa etapa opcional, desmarque **Win 10 MDM**.
 - **URI do ID de aplicativo:** digite a URL do XenMobile Server inserido quando você definiu as configurações do Azure.

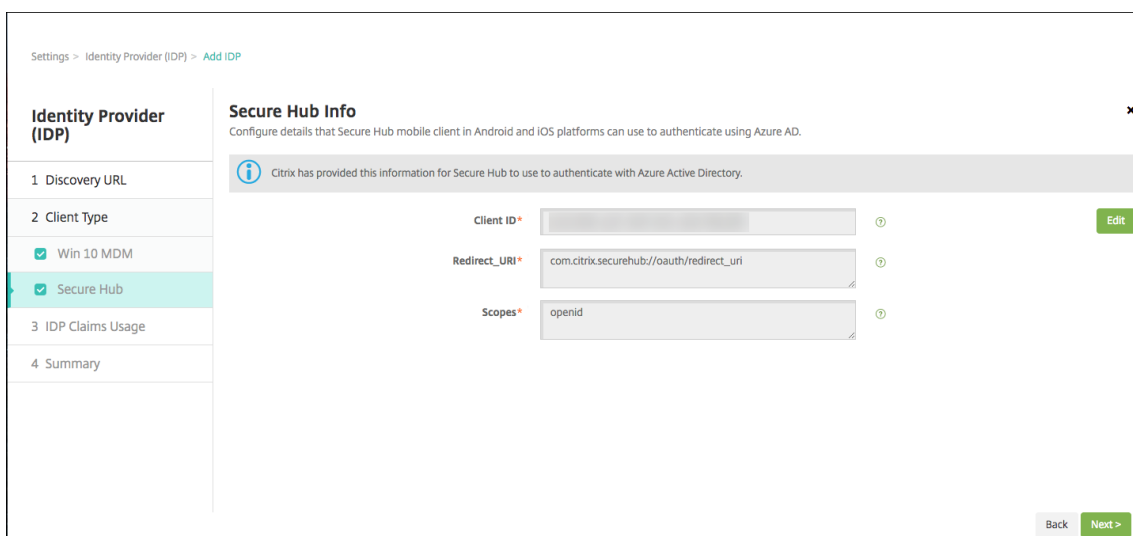
- **ID do cliente:** copie e cole esse valor da página Configurar do Azure. O ID do cliente é o identificador exclusivo do seu aplicativo.
- **Chave:** copie esse valor da página de configurações do aplicativo Azure. Em chaves, selecione uma duração na lista e salve a configuração. Você pode copiar a chave e colá-la nesse campo. Uma chave é necessária para a leitura e a gravação de dados no AD do Microsoft Azure.



8. Clique em **Avançar**.

A Citrix registrou o Secure Hub no Microsoft Azure e mantém as informações. Essa tela mostra os detalhes usado pelo Secure Hub para se comunicar com o Azure Active Directory. Essa página será usada no futuro se essas informações precisarem de alteração. Edite essa página apenas se recomendado pela Citrix.

9. Clique em **Avançar**.



10. Configure o tipo de identificador de usuário que seu IdP fornece:

- **Tipo de identificador do usuário:** escolha **userPrincipalName** na lista.
- **Sequência de caracteres do identificador do usuário:** esse campo é preenchido automaticamente.

11. Clique em **Avançar**.

Settings > Identity Provider (IDP) > Add IDP

Identity Provider (IDP)

- 1 Discovery URL
- 2 Client Type
- Win 10 MDM
- Secure Hub
- 3 IDP Claims Usage**
- 4 Summary

IDP Claims Usage

Choose the type of user identifier that IDP is providing.

XenMobile uses the 'upn' key to retrieve the user information from the jwt token provided by Azure Active Directory.

User Identifier type* userPrincipalName

User Identifier string* \$[id_token].upn

Back Next >

12. Revise a página **Resumo** e clique em **Salvar**.

Identity Provider (IDP)

- 1 Discovery URL
- 2 Client Type
- Win 10 MDM
- Secure Hub
- 3 IDP Claims Usage
- 4 Summary**

Token endpoint (URL) https://login.windows.net/.../oauth2/token

Token endpoint (URL) https://login.windows.net/.../oauth2/token

End Session endpoint (URL) https://login.windows.net/.../oauth2/logout

Win 10 MDM

App ID URI http://www.example.com

Client ID asdf-123-example-client-id

Key *****

Secure Hub Info

Client ID [redacted]

Client Secret (optional) N/A

Redirect_URI com.citrix.securehub://oauth/redirect_uri

Scopes openid

IDP Claims Usage

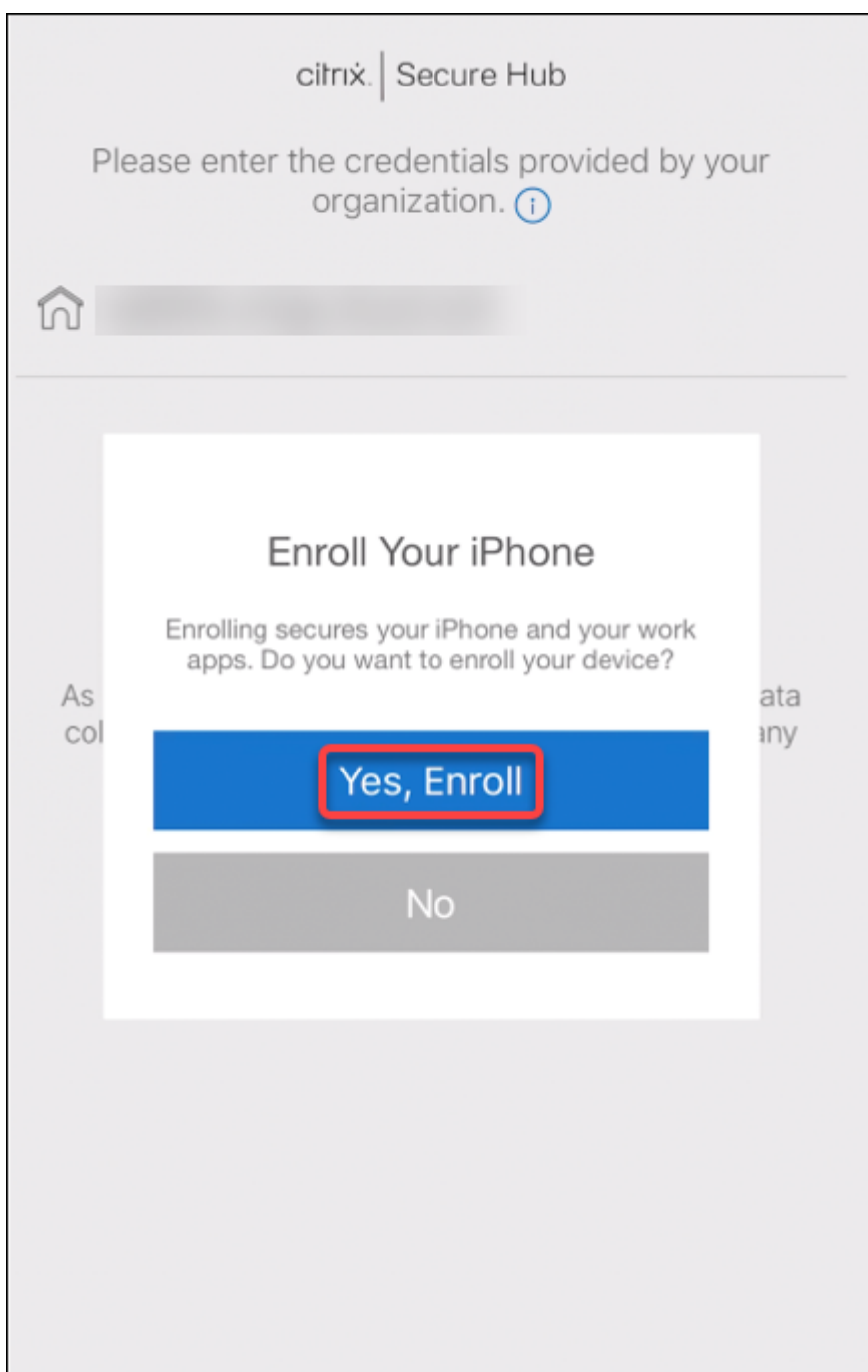
User Identifier type userPrincipalName

User Identifier string \$[id_token].upn

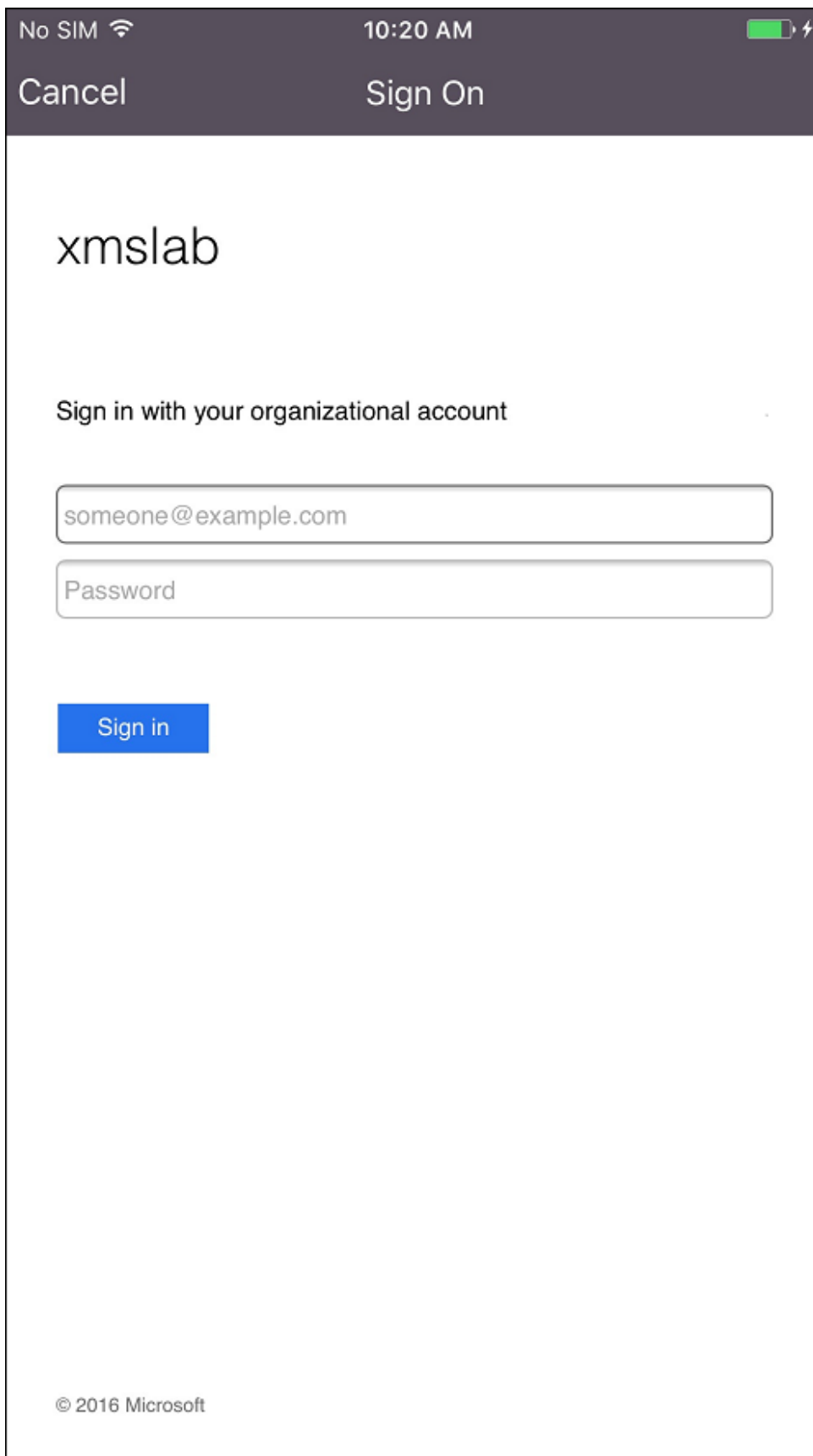
Back Save

Experiência dos usuários

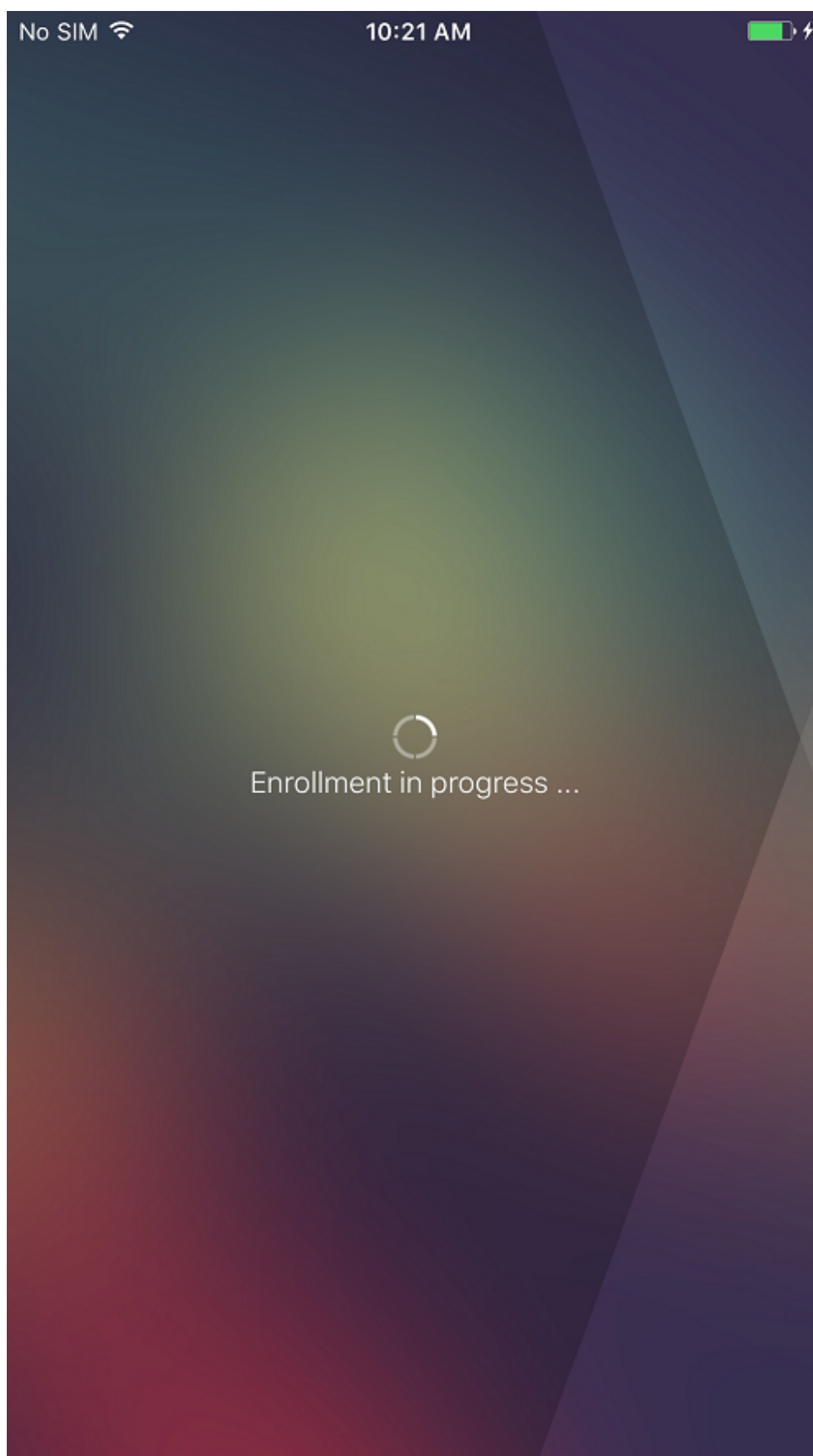
1. Os usuários iniciam o Secure Hub. Em seguida, eles inserem o nome de domínio totalmente qualificado (FQDN) do XenMobile Server, nome UPN ou endereço de email.

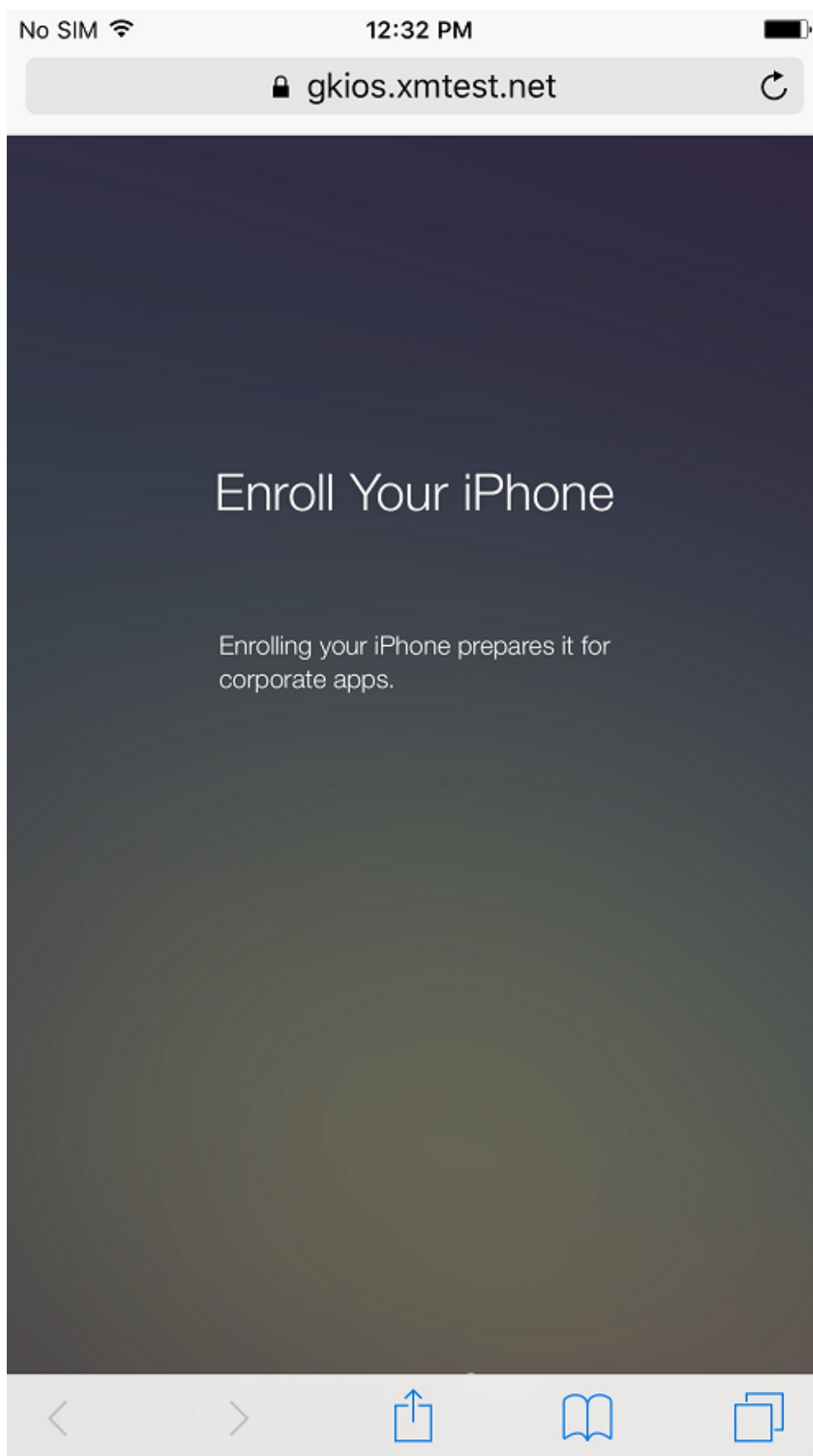


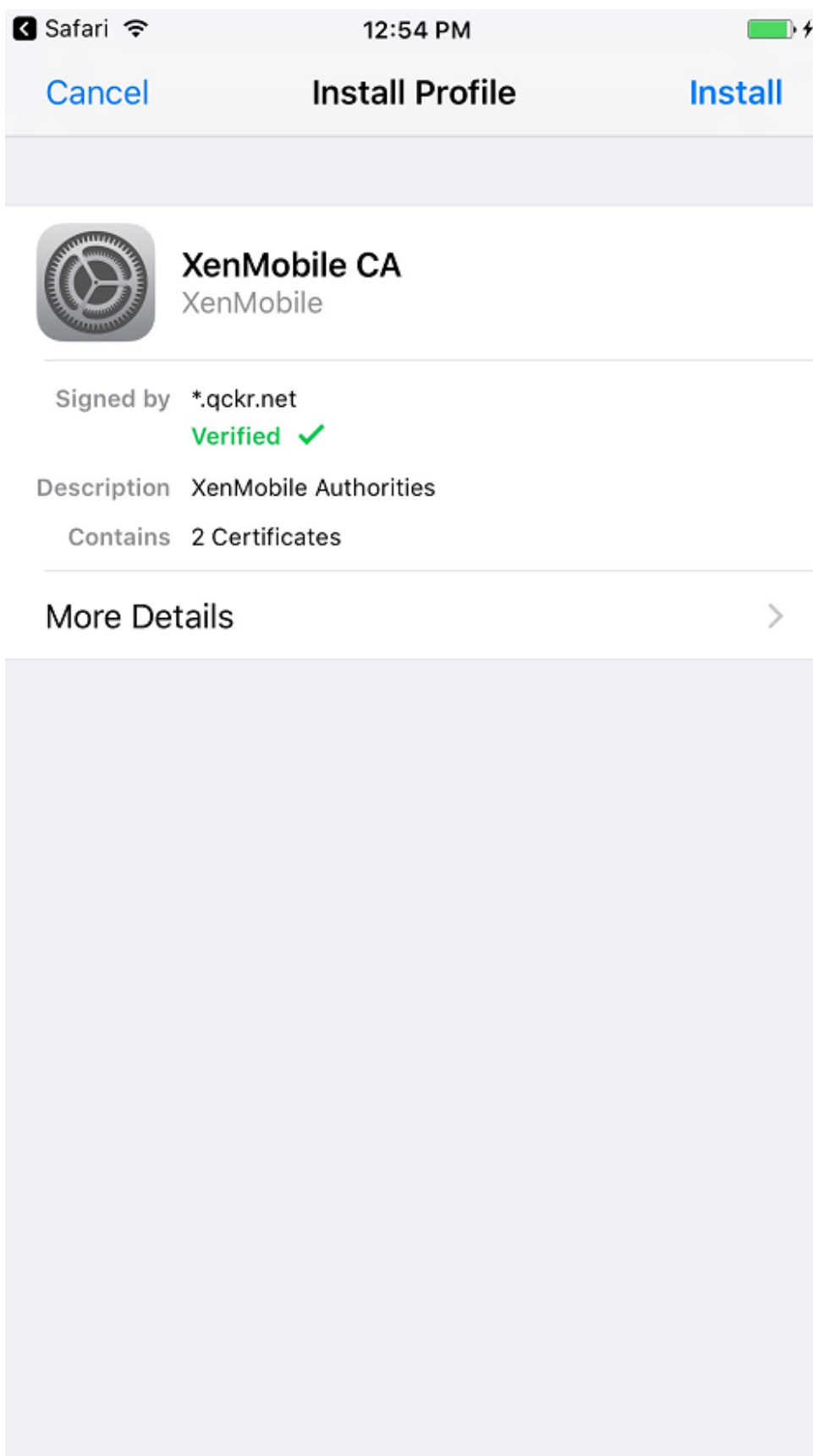
2. Em seguida, os usuários clicam em **Sim, registrar**.



3. Os usuários fazem logon usando suas credenciais do AD do Azure.







- Os usuários concluem as etapas de registro da mesma forma que qualquer outro registro por meio do Secure Hub.

Nota:

O XenMobile não dá suporte à autenticação por meio do AD do Azure a convites para registro. Se você enviar um convite para registro que contém uma URL de registro de usuários, os usuários se autenticarão por meio do LDAP em vez do AD do Azure.

Credenciais derivadas

April 1, 2021

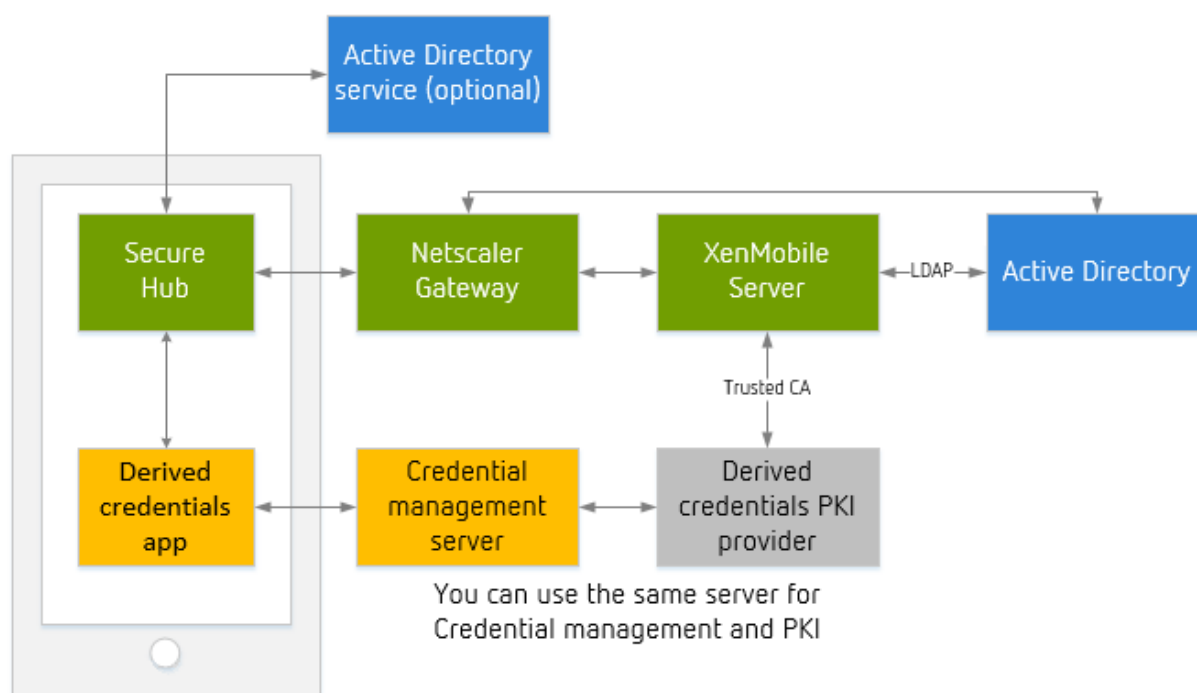
As credenciais derivadas fornecem autenticação forte para dispositivos móveis. Um cartão inteligente fornece as credenciais, que residem em um dispositivo móvel em vez do cartão. Um cartão inteligente é um cartão de verificação de identidade pessoal (Personal Identity Verification - PIV).

As credenciais derivadas são um certificado de registro que contém o identificador de usuário, como UPN. O XenMobile salva as credenciais obtidas do provedor de credenciais em um cofre seguro no dispositivo.

O XenMobile pode usar credenciais derivadas para registro e autenticação do dispositivo. Se configurado para credenciais derivadas, o XenMobile não dá suporte a convites de registro ou outros modos de segurança de registro. A Citrix suporta o uso de um aplicativo de credenciais derivadas durante o registro do iOS.

Arquitetura

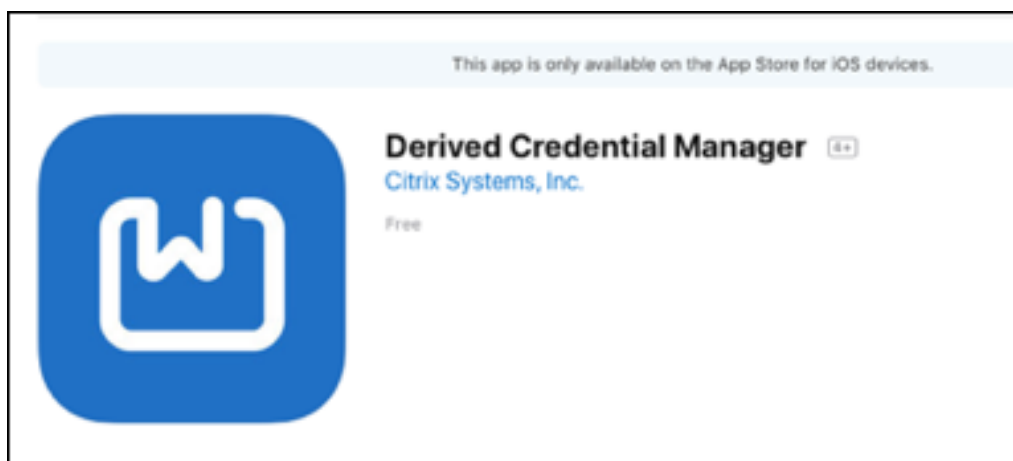
Para o registro, o XenMobile Server se conecta aos componentes, conforme mostrado no diagrama a seguir.



- Durante o registro de dispositivos, o Secure Hub obtém certificados do aplicativo de credenciais derivadas.
- O aplicativo de credenciais derivadas se comunica com o servidor de gerenciamento de credenciais durante o registro.
- Você pode usar o mesmo servidor ou um servidor diferente para o servidor de gerenciamento de credenciais e um provedor de PKI de terceiros.
- O XenMobile Server se conecta ao seu servidor de PKI de terceiros para obter certificados.

Requisitos

- Baixe e instale o Citrix Secure Hub.
- Com base na sua solução de credencial derivada, baixe e configure o aplicativo:
 - **Para Entrust Datacard:**
 - * Baixe e instale o aplicativo Citrix Derived Credential Manager em seus dispositivos *antes* de se registrar no XenMobile. O aplicativo Derived Credentials Manager é o aplicativo provedor de identidade da Citrix. Segue o logotipo desse aplicativo.



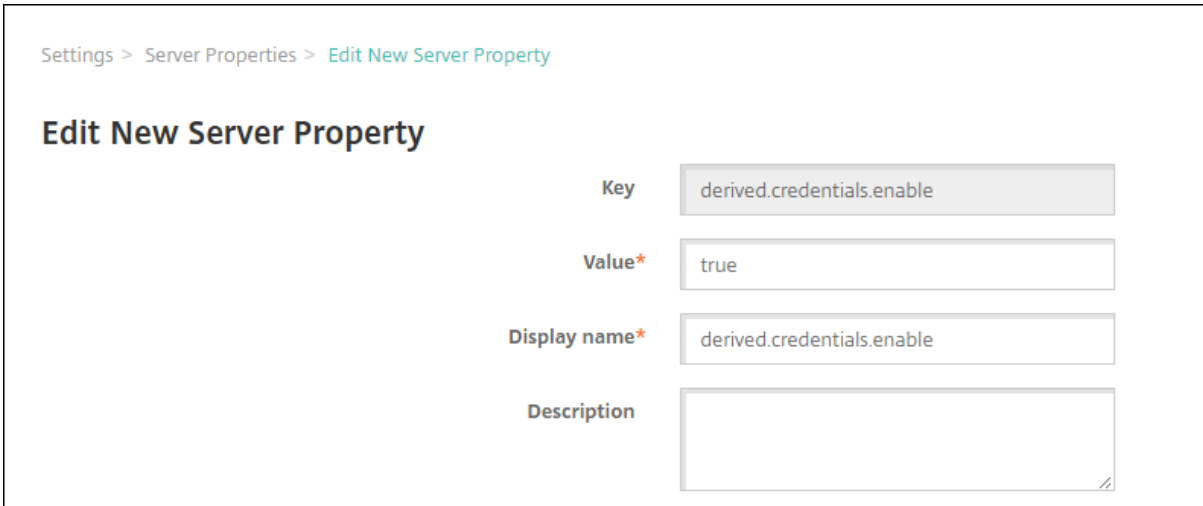
- O aplicativo Citrix Derived Credential Manager suporta apenas novos registros. Os usuários do dispositivo devem se registrar novamente.
 - XenMobile Server versão 10.8 ou posterior.
 - Requer o registro de dispositivo no MDM+MAM.
- **Para outros provedores de credenciais derivadas:** embora seja provável que a maioria das outras soluções de credenciais seja compatível com o XenMobile, teste a integração antes de colocá-la em produção.
- Deve ter o certificado raiz da autoridade que emite certificados ao servidor do Provedor de credenciais. Essa configuração permite que o XenMobile aceite os certificados assinados digitalmente durante o registro. Para obter informações sobre como adicionar certificados, consulte [Certificados e autenticação](#).
 - Se o domínio de email de usuário for diferente do domínio LDAP, inclua o domínio de email na configuração **Alias de domínio**, em **Configurações > LDAP**. Por exemplo, se o domínio de endereços de email for `citrix.com` e o nome do domínio LDAP for `sample.com`, defina **Alias de domínio** como `sample.com`, `citrix.com`.
 - O XenMobile não suporta o uso de credenciais derivadas com dispositivos compartilhados.
- Certificados de identidade de usuário:
 - O nome de usuário no campo Nome de entidade alternativo deve ser formatado como o campo `otherName`, `rfc822Name` ou `dNSName` da extensão `SubjectAltName`. Não há suporte para outros campos. Para obter mais informações sobre o Nome de entidade alternativo, consulte a RFC, <https://www.ietf.org/rfc/rfc5280.txt>.
 - Não há suporte para o campo Entidade em Email ou CN.
- Citrix Gateway configurado para autenticação de certificado ou autenticação de certificado mais token de segurança

Ativar credenciais derivadas

Por padrão, o console XenMobile não inclui a página **Configurações > Credenciais derivadas**.

Para ativar a interface para credenciais derivadas:

- Vá até **Configurações > Propriedades do servidor**, adicione **derived.credentials.enable** como a propriedade de servidor e defina o valor da propriedade como **true**.



Settings > Server Properties > Edit New Server Property

Edit New Server Property

Key	<input type="text" value="derived.credentials.enable"/>
Value*	<input type="text" value="true"/>
Display name*	<input type="text" value="derived.credentials.enable"/>
Description	<input type="text"/>

Configurar credenciais derivadas

Parte-se do pressuposto que você tenha uma configuração funcional para o provedor de credenciais derivadas que planeja integrar com o XenMobile. Você poderá configurar o XenMobile para se comunicar com esse servidor. Você também pode escolher um certificado de CA de credenciais derivadas já adicionado ao XenMobile ou importar o certificado.

É possível ativar o suporte ao protocolo OCSP para esse certificado de CA. Para obter mais informações sobre o protocolo OCSP, consulte “CAs discricionárias”, em [Entidades PKI](#).

1. No console XenMobile, vá até **Configurações > Credenciais derivadas para iOS**.
2. Em **Escolher o provedor de credenciais derivadas**, escolha **Outro** para Entrust Datacard. Digite `dcapp://mode=SecureHub` em **URL de aplicativo (iOS)**.

3. **Parâmetros opcionais:** alguns provedores de credenciais derivadas podem exigir que você forneça parâmetros para a conexão. Por exemplo, um fornecedor pode exigir que você especifique as URLs de um servidor back-end. Clique em **Adicionar** para fornecer parâmetros.
4. Especifique um certificado para credenciais derivadas: se o certificado já estiver carregado no XenMobile, escolha-o em **AC emissora**. Caso contrário, clique em **Importar** para adicionar um certificado. A caixa de diálogo **Importar certificado** é exibida.
5. Na caixa de diálogo **Importar certificado**, clique em **Procurar** para navegar até o certificado. Em seguida, clique em **Procurar** para navegar até o arquivo de chave privada.

Import ×

You can import certificates or keystores used by PKI components. You can import several certificates, but you can only have one certificate active at a time.

Import Certificate ▾

Use as Server ▾

Certificate import* **Browse**

Private key file **Browse**

Description

Cancel **Import**

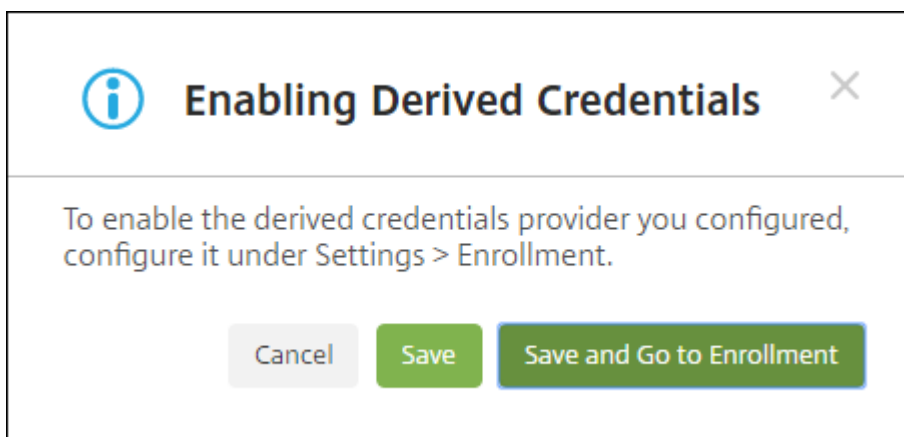
6. Defina as configurações.

- No aplicativo Citrix Derived Credentials Manager: o **Campo de identificador do usuário** é o **Nome de entidade alternativo**, e o **Tipo de identificador do usuário** é **userPrincipalName**.
- Entre em contato com outros provedores de credenciais derivadas para obter suas informações.

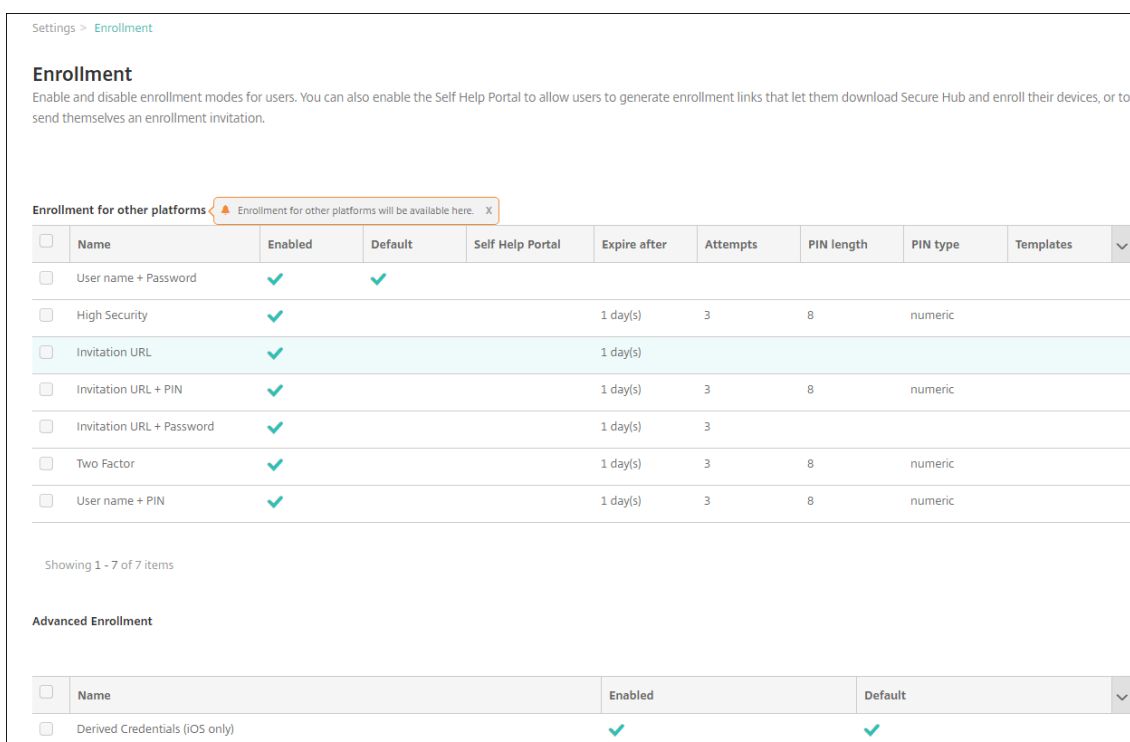
7. Você tem a opção de usar um respondedor OCSP para verificação da revogação de certificados. A Citrix recomenda o uso de um respondedor OCSP para fins de segurança. Por padrão, a verificação OSP é **Desativado**.

- Se você ativar o suporte OCSP para o certificado de CA, escolha uma opção para **Use a URL de OCSP personalizada**. Por padrão, o XenMobile extrai a URL OCSP do certificado (a opção **Usar definição de certificado para revogação**). Para especificar uma URL de respondedor, clique em **Usar definido pelo usuário** e digite a URL.
- **AC respondedora:** em **AC respondedora**, escolha um certificado. Ou clique em **Importar** e use a caixa de diálogo **Importar certificado** para localizar o certificado.

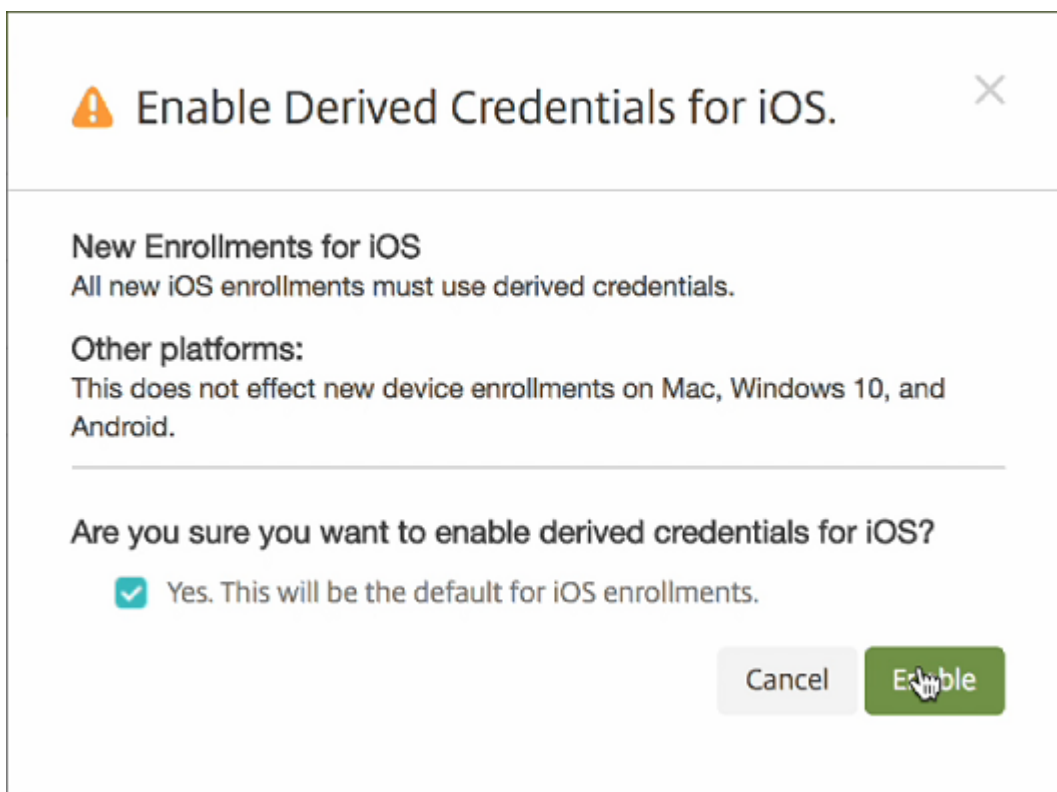
8. Clique em **Salvar**. A caixa de diálogo **Ativação de credenciais derivadas** é exibida.



- Para ativar a configuração de credenciais derivadas, clique em **Salvar**. Para usar credenciais derivadas, você também deve definir as configurações de registro.
 - Para ativar a configuração de credenciais derivadas e ir imediatamente para **Configurações > Registro**, clique em **Salvar e Ir para Registro**.
9. Para ativar credenciais derivadas para registro: na página **Configurações > Registro**, em **Registro avançado**, selecione **Credenciais derivadas** (apenas iOS) e clique em **Ativar**.



10. Uma caixa de diálogo de confirmação é exibida. Para ativar credenciais derivadas, marque a caixa de seleção e clique em **Ativar**.



11. Para editar opções de registro de credenciais derivadas, acesse **Configurações > Registro**, selecione **Credenciais derivadas (apenas iOS)** e clique em **Editar**.

Depois que você ativar credenciais derivadas, no relatório **Registro de dispositivos**, a coluna **Modo de registro** mostrará **derived_credentials**.

Importante:

Depois de adicionar o provedor de credenciais derivadas, reinicie o XenMobile Server.

Configurar o XenMobile Server para Secure Mail

Para que o Secure Mail dê suporte a credenciais derivadas, adicione a propriedade de cliente `SEND_LDAP_ATTRIBUTES`. Para obter informações sobre como adicionar uma propriedade de cliente, consulte [Propriedades do cliente](#).

Use as seguintes informações para a propriedade do cliente:

- **Chave:** `SEND_LDAP_ATTRIBUTES`
- **Valor:** `userPrincipalName=${ user.userprincipalname } ,sAMAccountName=${ user.samaccountname } ,displayName=${ user.displayName } ,mail=${ user.mail }`

Settings > Client Properties > Edit Client Property

Edit Client Property

Key	SEND_LDAP_ATTRIBUTES
Value *	userPrincipalName=\${user.userprincipalname},sAM
Name *	SEND_LDAP_ATTRIBUTES
Description *	SEND_LDAP_ATTRIBUTES

Ativação de credenciais derivadas do Entrust Datacard em dispositivos iOS

Nota:

Quando usar site Entrust, limpe o cache do navegador ao mudar o cartão PIV.

1. Para solicitar novas credenciais inteligentes, utilize um computador ou outro dispositivo para iniciar uma sessão no site da Entrust. Faça login usando o botão em **Smart Credential Log In**, na parte inferior da página. Os usuários inserem o cartão inteligente em um leitor acoplado ao computador.

The screenshot displays the login interface for XenMobile Server, divided into two main sections:

- Log In:** This section features a dropdown menu for "Sign In Using:" with "Corporate Domain Password" selected. Below it are two required fields, marked with a red asterisk: "User Name:" and "Password:". A "Log In" button is positioned below the password field. At the bottom of this section, there are four blue arrow icons pointing to the following links: "Forgot your password?", "Perform SAML login", "Forgot your smart credential PIN?", and "Let me use an OTP to log in."
- Smart Credential Log In:** This section contains the instruction: "Ensure your smart credential can be read by your computer, then click this button to log in." Below this text is a blue "Log In" button, which is highlighted with a red rectangular box. At the bottom of this section, it says "Close your web browser when you are done."

2. Em **Self-Administration Actions**, selecione **I'd like to enroll for a derived mobile smart credential** e clique em **Done**.

Self-Administration Actions

Please select one of the actions below or click Done if you're finished:

- [I'd like to update my personal information.](#)
- [I'd like to change my question and answer pairings.](#)
- [I'd like to request a grid.](#)
- [I'd like to change my Entrust IdentityGuard password.](#)
- [I've forgotten my Entrust IdentityGuard password.](#)
- [I'd like to request a soft token.](#)
- [I'd like to unblock my smart credential.](#)
- [I'd like to activate or update my smart credential.](#)
- [I've permanently lost my smart credential or it has been compromised.](#)
- [I've temporarily forgotten or misplaced my smart credential.](#)
- [I'd like to enroll for a derived mobile smart credential.](#)

Done

3. Na tela **Derived Mobile Smart Credential**, forneça o nome de identidade em **Identity Name**. O usuário pode escolher um nome exclusivo, como um nome de usuário ou números de ID.
4. Selecione **Citrix DCAPP** no menu aplicativo de credenciais derivadas e clique em **Ok**.

Derived Mobile Smart Credential

Enter any name you would like to use to identify your new derived mobile smart credential identity.

* Identity Name:

Choose which app you want to associate with your new derived mobile smart credential.

* Derived Mobile Smart Credential App:

Citrix DCAPP

You will receive an email message, to be opened on your mobile device, that contains a link that will launch the derived mobile smart credential app with the appropriate activation data.

To unlock the activation data, you will be required to enter a password that will be provided on the next page.

The activation email message will be delivered to the account associated with citrix.com.

You will have approximately 60 minutes to complete the activation of your derived mobile smart credential.

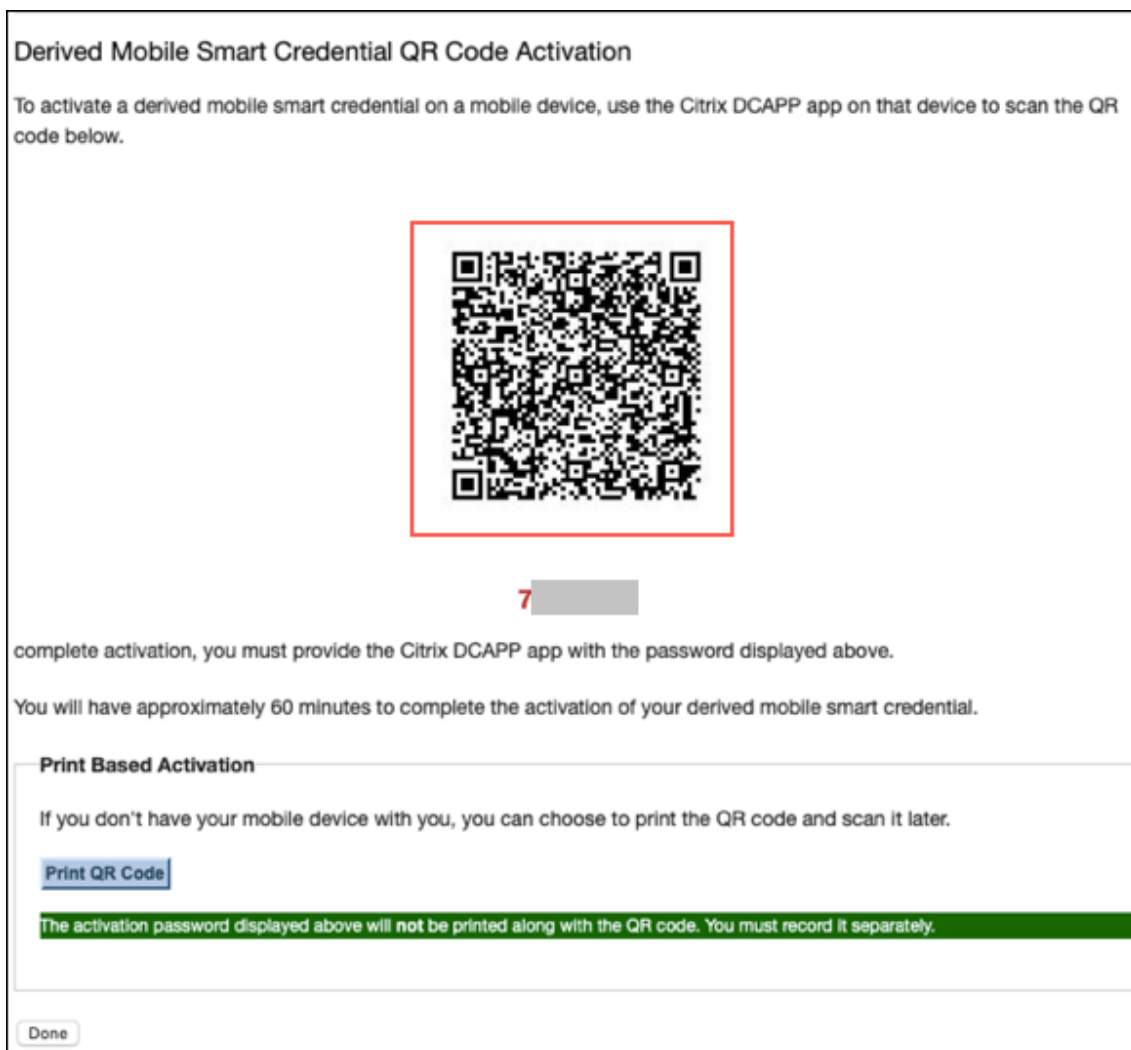
OK Cancel

A tela de ativação de código QR aparece e solicita ao usuário que escaneie o código com o dispositivo móvel.

Nota:

Por padrão, o código QR de credenciais derivadas expira em 3 minutos.

5. Escaneie o código QR usando o aplicativo **Derived Credential Manager** no dispositivo para concluir a ativação.



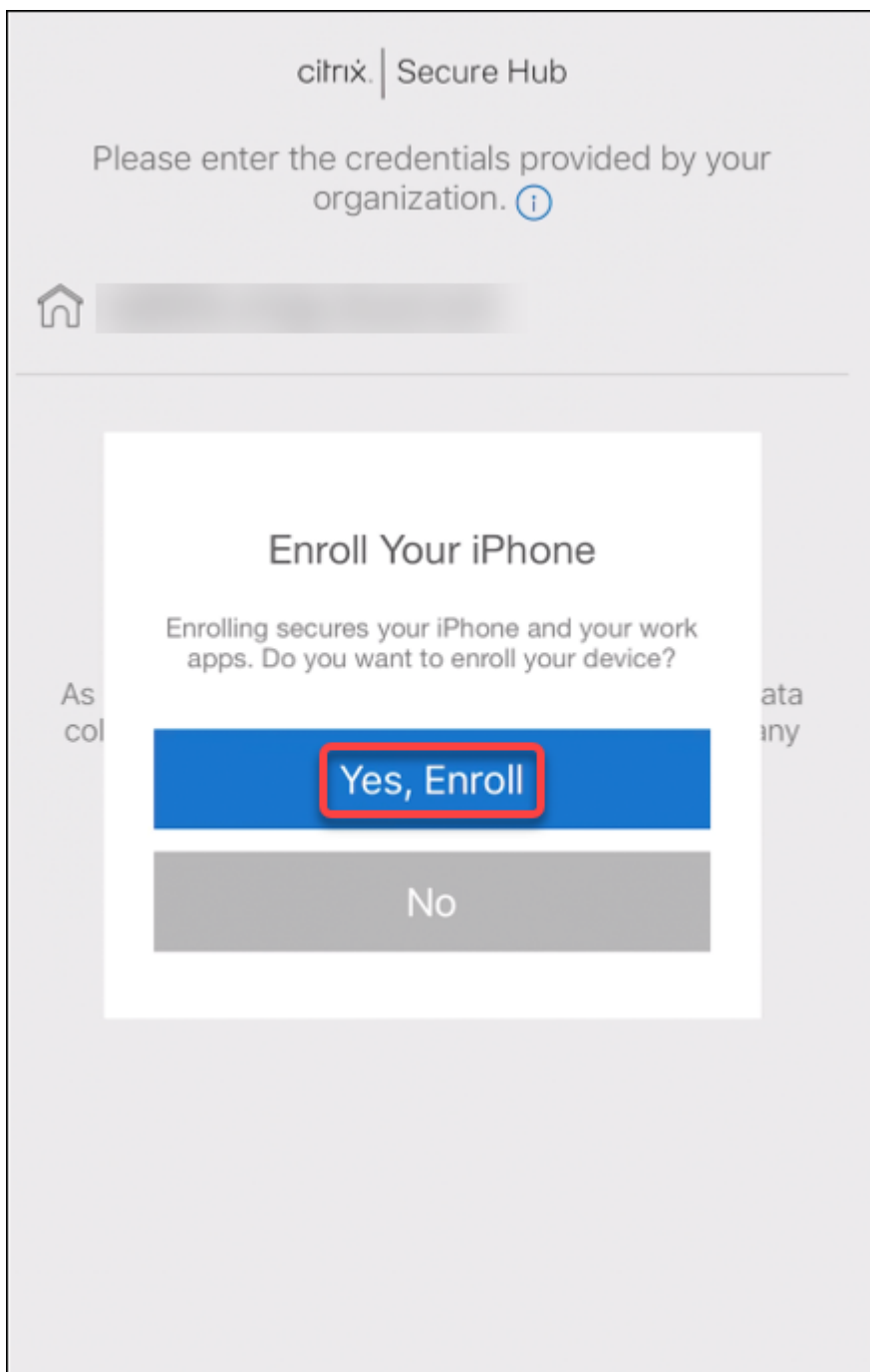
Registro do dispositivo

Depois de concluir a instalação descrita anteriormente neste artigo, os usuários podem registrar seus dispositivos usando credenciais derivadas.

Nota:

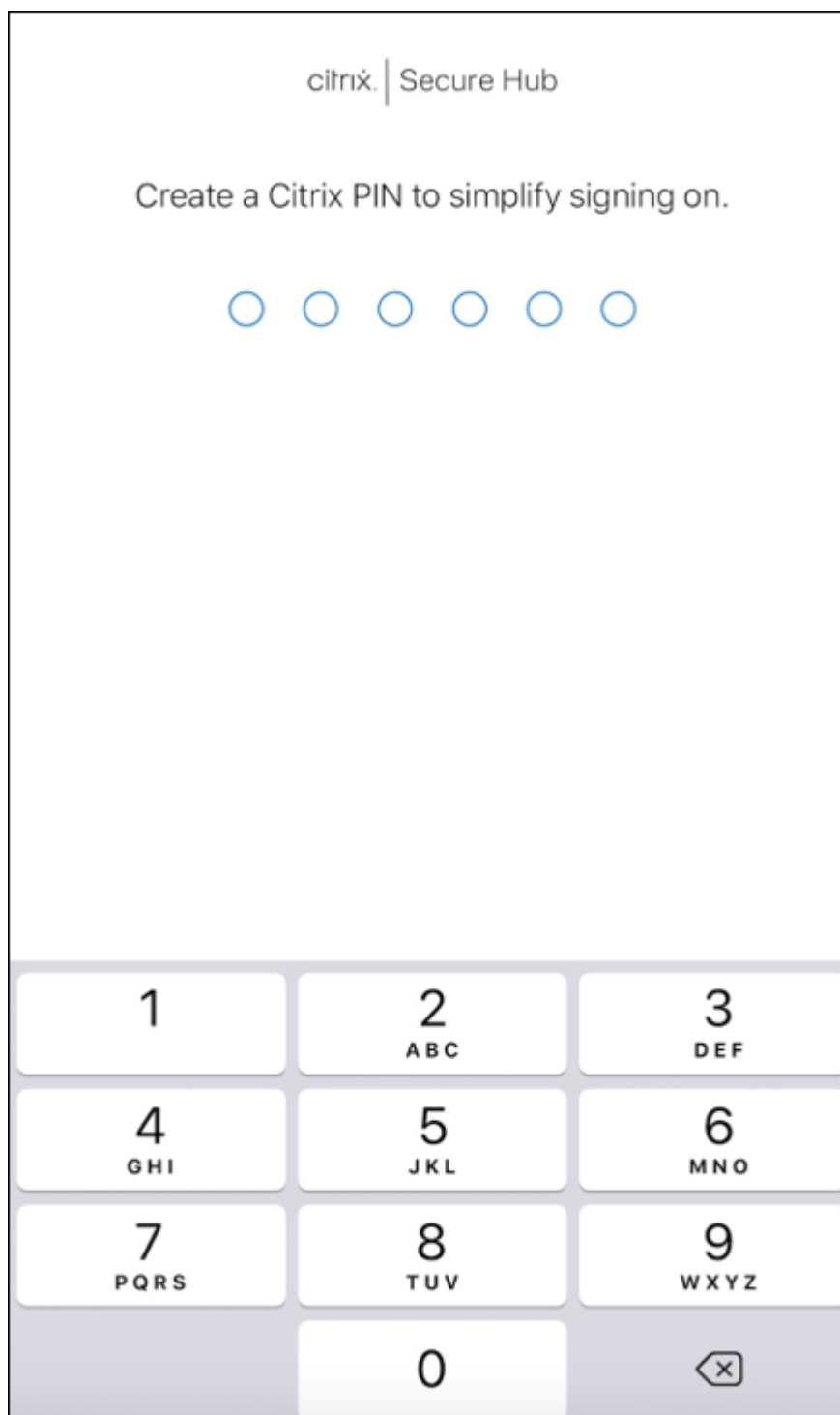
As capturas de tela desta seção usam o Entrust Datacard como exemplo.

1. Toque para abrir o **Secure Hub**. Quando solicitado, digite o nome de domínio totalmente qualificado do XenMobile Server e clique em **Avançar**.
2. Clique em **Sim, registrar**. O registro do dispositivo no Secure Hub é iniciado.



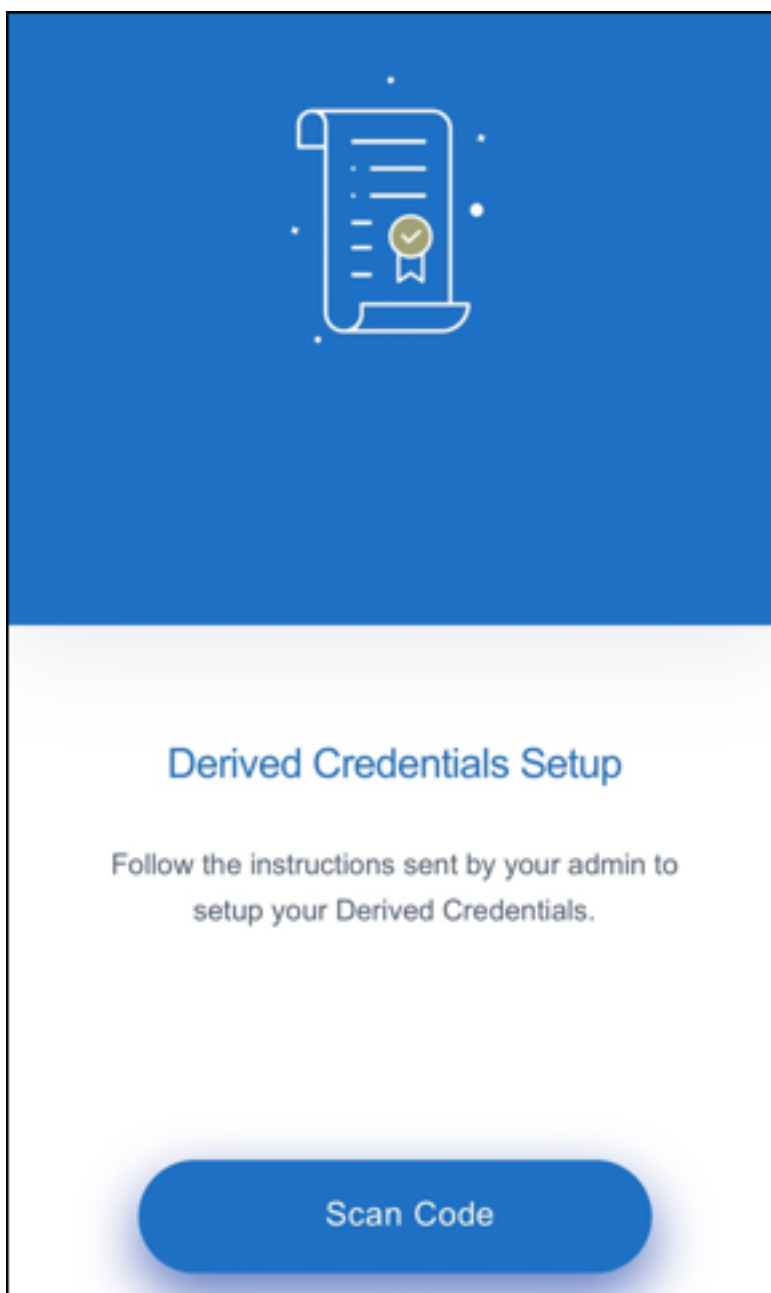
Se o XenMobile Server oferecer suporte a credenciais derivadas, o Secure Hub solicita ao

usuário que crie e confirme o PIN da Citrix.



Depois de confirmar o PIN da Citrix, aparece a tela de abertura de configuração de Credenciais Derivadas. Siga as instruções para ativar as credenciais inteligentes.

3. Toque em **Escanear código**. A câmera do telefone celular é ativada.




Nota:

Para escanear o código QR, certifique-se de que sua câmera e microfone estão ativados e têm as permissões de acesso necessárias.

4. No aplicativo de credenciais derivadas, escaneie o código QR que foi criado em etapas anteriores.

Derived Mobile Smart Credential QR Code Activation

To activate a derived mobile smart credential on a mobile device, use the Citrix DCAPP app on that device to scan the QR code below.



7 [REDACTED]

complete activation, you must provide the Citrix DCAPP app with the password displayed above.

You will have approximately 60 minutes to complete the activation of your derived mobile smart credential.

Print Based Activation

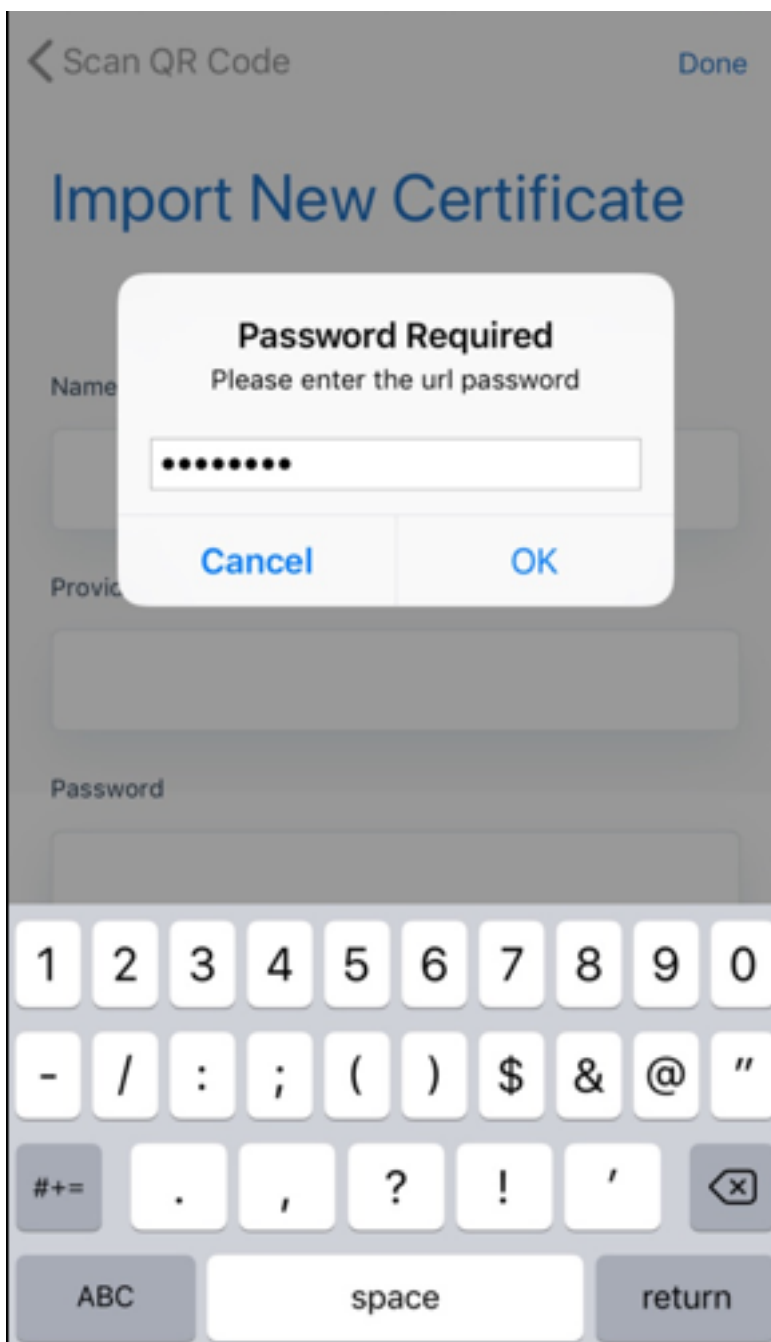
If you don't have your mobile device with you, you can choose to print the QR code and scan it later.

[Print QR Code](#)

The activation password displayed above will not be printed along with the QR code. You must record it separately.

Done

5. Depois de escanear o código QR, na tela **Importar novo certificado** aparece uma caixa de diálogo de senha: digite a senha e clique em **OK**.



A tela **Importar novo certificado** é exibida com os campos preenchidos automaticamente.

Import Certificates

Below are the details of certificate that you are importing into the app. Click done to confirm.

Name

DCDemo

Provider

sede

Credential ID

ET91

Import Certificates

6. Depois que os certificados forem adicionados com êxito, na tela de **Credenciais derivadas**, clique em **Continue to Secure Hub**.

Derived Credentials

You have three authentication and signing certificate for authentication

🕒 23 December 2018

Enrollment Cert

Authentication

🕒 23 December 2018

SMIME Cert

Signing

🕒 23 December 2018

Encryption Cert

Encryption

[Continue to Secure Hub](#)

7. No Secure Hub, insira um novo PIN quando solicitado.

Depois de autenticar o PIN, o Secure Hub baixa os certificados. Siga os prompts para concluir o registro.

Para exibir informações do dispositivo no console XenMobile:

- Vá para **Gerenciar > Dispositivos** e selecione um dispositivo para exibir uma caixa de comando. Clique em **Mostrar mais**.
- Vá para **Analisar > Painel**.

Atualização

November 30, 2020

Dica: Serviço de Migração do XenMobile

Se você estiver usando o XenMobile Server no local, nosso Serviço de Migração do XenMobile gratuito pode ajudá-lo a começar a usar o Endpoint Management. A migração do XenMobile Server para o Citrix Endpoint Management não exige que você registre novamente os dispositivos.

Para obter mais informações, entre em contato com o pessoal de vendas local da Citrix, com um engenheiro de sistemas ou com um parceiro Citrix. Estes blogs discutem o Serviço de Migração do XenMobile:

[Novo serviço de migração do XenMobile](#)

[Criando o cenário para o XenMobile na Nuvem](#)

Antes de atualizar para o XenMobile 10.13

1. Atualize o seu Citrix License Server para 11.16 ou posterior antes de atualizar para a versão mais recente do XenMobile Server 10.13.

A versão mais recente do XenMobile exige o Citrix License Server 11.16 (versão mínima).

A data do Customer Success Services (anteriormente, data de Subscription Advantage) no XenMobile 10.13 é 29 de setembro de 2020. A data do Customer Success Services na sua licença Citrix deve ser posterior a essa data. Você pode ver a data ao lado da licença do servidor de licenças. Se você conectar a versão mais recente do XenMobile a um ambiente de servidor de licenças mais antigo, a verificação de conectividade falhará e você não poderá configurar o servidor de licenças.

Para renovar a data na sua licença, baixe o último arquivo de licença do Portal Citrix e carregue o arquivo para o Servidor de Licença. Para obter mais informações, consulte [Customer Success](#)

Services.

2. Para um ambiente em cluster: as implantações de aplicativos e políticas do iOS para dispositivos que executam o iOS 11 e posterior têm o seguinte requisito. Se o Citrix Gateway estiver configurado para persistência de SSL, você deve abrir a porta 80 em todos os nós do XenMobile Server.
3. Se a máquina virtual que executa o XenMobile Server que deve ser atualizado tiver menos de 8 GB de RAM, recomendamos aumentar a RAM para pelo menos 8 GB.
4. Recomendação: Antes de instalar uma atualização do XenMobile, use a funcionalidade na sua VM para tirar um instantâneo do seu sistema. Além disso, faça backup do seu banco de dados de configuração do sistema. Se tiver problemas durante uma atualização, backups completos permitirão fazer uma recuperação.

Para atualizar

Você pode atualizar diretamente do XenMobile 10.11.x ou 10.12.x para o XenMobile 10.13. Para realizar a atualização, baixe o binário mais recente disponível: acesse <https://www.citrix.com/downloads>. Navegue para **Citrix Endpoint Management (XenMobile) > XenMobile Server > Product Software > XenMobile Server 10**. No bloco do software XenMobile Server, para o seu hipervisor, clique em **Download File**. Use a página **Gerenciamento de versão** no console XenMobile.

Para atualizar usando a página Gerenciamento de versão

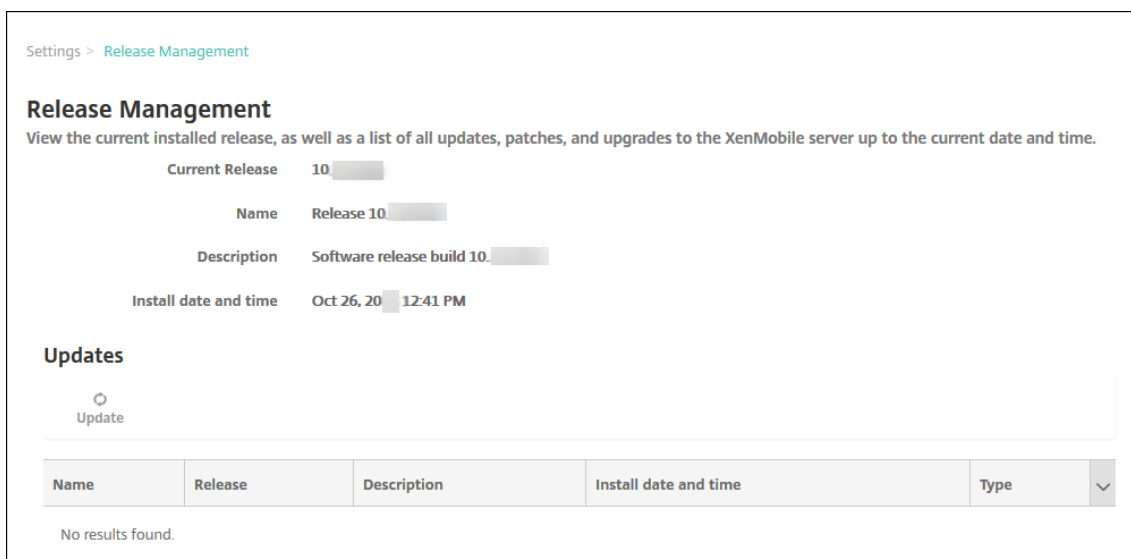
Use a página **Gerenciamento de versão** para atualizar para a versão mais recente do XenMobile Server.

Pré-requisitos:

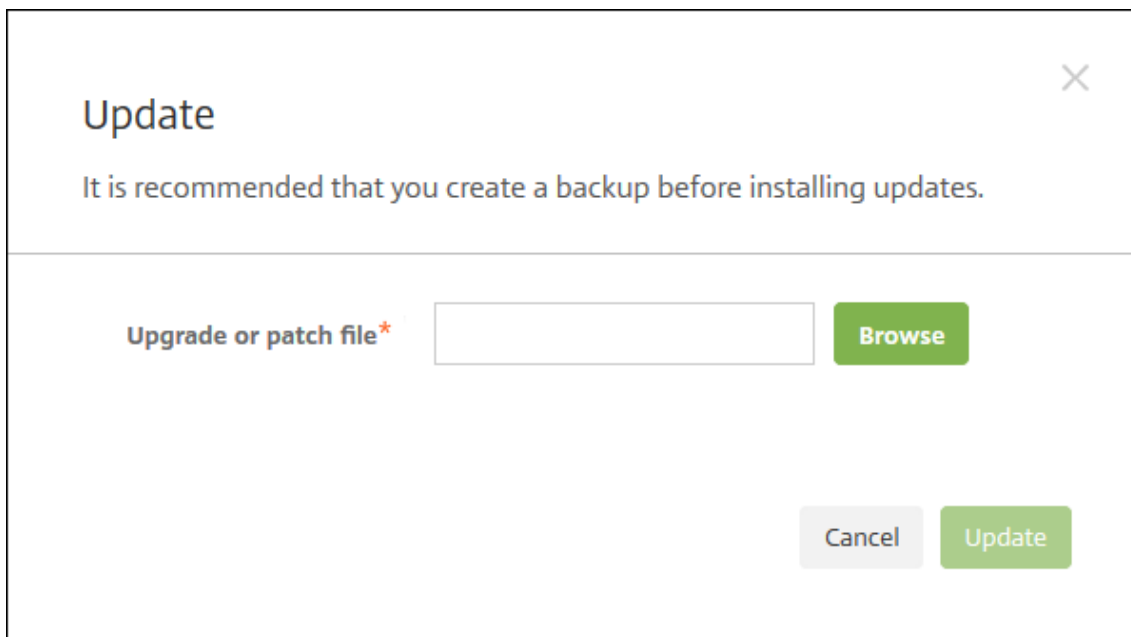
- Leia os [Requisitos do sistema](#).

Se você tem uma implantação em cluster, consulte as instruções no final deste artigo.

1. Baixe o binário mais recente disponível: acesse <https://www.citrix.com/downloads>. Navegue para **Citrix Endpoint Management (e Citrix XenMobile Server) > XenMobile Server (no local) > Product Software > XenMobile Server 10**. No bloco do software XenMobile Server, para o seu hipervisor, clique em **Download File**.
2. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Settings** é exibida.
3. Clique em **Gerenciamento de versão**. A página **Gerenciamento de Versão** é exibida.



4. Em **Atualizações**, clique em **Atualizar**. A caixa de diálogo **Atualizar** é exibida.



5. Selecione o arquivo de atualização do XenMobile que você baixou do site Citrix.com clicando em **Procurar** e navegando até a localização do arquivo.
6. Clique em **Atualizar** e, se solicitado, reinicie o XenMobile.

Se por algum motivo a atualização não puder ser concluída com sucesso, uma mensagem de erro será exibida indicando o problema. O sistema é revertido ao estado anterior à tentativa de atualização.

Depois de atualizar

Após uma atualização, o XenMobile exige a reinicialização. Use a interface de linha de comando do XenMobile para reiniciar o XenMobile Server. É importante que você limpe o cache do navegador depois que o sistema for reiniciado.

Se a funcionalidade que envolve as conexões de saída deixar de funcionar e você não alterou a configuração de suas conexões, verifique os erros no log do XenMobile Server, como os seguintes: “Não é possível se conectar ao servidor VPP: o nome do host ‘192.0.2.0’ não corresponde à entidade do certificado fornecido pelo par”

O erro de validação do certificado indica que você precisa desabilitar a verificação do nome do host no XenMobile Server. Como padrão, a verificação do nome do host está ativada nas conexões de saída, exceto para o servidor Microsoft PKI. Se a verificação do nome do host interromper sua implantação, altere a propriedade do servidor **disable.hostname.verification** para **true**. O valor padrão desta propriedade é **false**.

A Citrix publica novas versões ou atualizações importantes do XenMobile no site Citrix.com. Ao mesmo tempo, uma notificação é enviada ao contato registrado para cada cliente.

Para atualizar implantações XenMobile em cluster

Importante:

Antes de instalar uma atualização do XenMobile, use a funcionalidade na sua máquina virtual (VM) para tirar um instantâneo do seu sistema. Além disso, faça backup do seu banco de dados de configuração do sistema. Se tiver problemas durante uma atualização, backups completos permitirão fazer uma recuperação.

Se o seu sistema estiver configurado no modo de cluster, siga estas etapas para atualizar cada nó de uma versão do XenMobile 10:

1. Carregue o arquivo .bin em todos os nós, acessando **Configurações > Gerenciamento de versão**.
2. Desligue todos os nós no **Menu Sistema** na interface de linha de comando.
3. Ative um único nó, no **Menu Sistema** na interface de linha de comando e verifique se o serviço está em execução.
4. Abra os outros nós, um após o outro.

Se o XenMobile não conseguir concluir a atualização com sucesso, uma mensagem de erro será exibida indicando o problema. O XenMobile reverte o sistema ao seu estado anterior à tentativa de atualização.

Atualize do XenMobile MDM Edition para Enterprise Edition

Você pode atualizar do XenMobile MDM Edition para o XenMobile Enterprise Edition para dispositivos iOS e Android.

Pré-requisitos

- A licença Enterprise correta.
- O Citrix Gateway está configurado.

Para atualizar

1. Vá para **Configurações > Licenciamento** e verifique se o tipo de licença Enterprise Edition correto está carregado.
2. Vá para **Configurações > Propriedades do Servidor** e mude a propriedade do **Modo Servidor** de **MDM** para **ENT**.
3. Vá para **Configurações > Citrix Gateway** e configure os detalhes do Citrix Gateway. Defina o modo de autenticação para o mesmo que o MDM Edition, ou seja, a autenticação de domínio (Active Directory). O XenMobile não dá suporte à alteração para o modo de autenticação após o registro de usuário.
4. Opcional: vá para **Configurações > Propriedades do Cliente** e habilite a autenticação do PIN da Citrix.

Depois de concluir essas etapas, os usuários devem executar as seguintes etapas para alternar um dispositivo para o modo Enterprise.

Usuários do iOS

1. Fechar o Secure Hub: toque no botão de página inicial do dispositivo duas vezes (rapidamente) e deslize no aplicativo Secure Hub.
2. Abra o Secure Hub.

Usuários do Android

1. Abra o Secure Hub.
2. Vá para **Preferências > Informações do dispositivo**.
3. Clique em **Atualizar política**.

Se você ativou a autenticação do PIN da Citrix, o Secure Hub solicita aos usuários que criem um PIN. Depois que um usuário cria um PIN, o XenMobile configura o dispositivo no modo Enterprise. No console XenMobile, a página **Gerenciar > Dispositivos** mostra ambos, MDM e MAM, como ativos para o dispositivo.

Contas de usuário, funções e registro

April 1, 2021

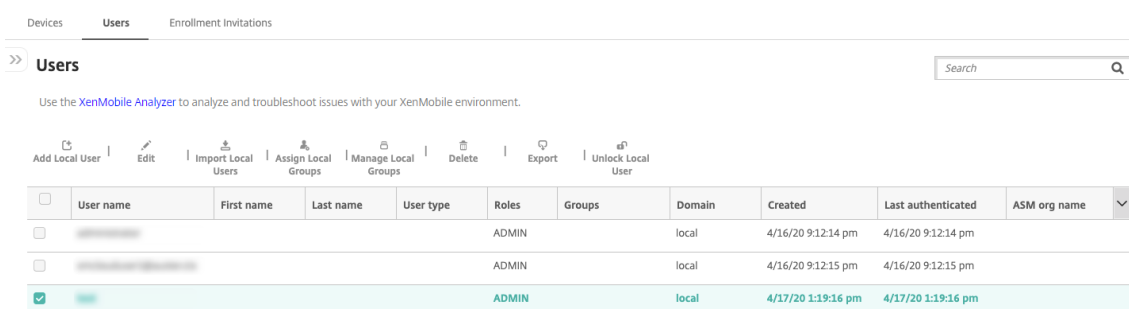
Você configura contas de usuário, funções e inscrições no console XenMobile na guia **Gerenciar** e na página **Configurações**. Salvo indicação em contrário, as etapas para as seguintes tarefas são fornecidas neste artigo.

- Contas de usuário e grupos:
 - Em **Gerenciar > Usuários**, adicione contas de usuário manualmente ou use um arquivo de provisionamento .csv para importar as contas e gerenciar os grupos locais.
 - Em **Configurações > Fluxos de trabalho**, use fluxos de trabalho para gerenciar a criação e a remoção de contas de usuário.
- Funções para contas de usuário e grupos
 - Clique em **Configurações > Controle de acesso baseado em função** para atribuir funções predefinidas ou conjuntos de permissões a usuários e grupos. Essas permissões controlam o nível de acesso que os usuários têm às funções do sistema. Para obter mais informações, consulte [Configurar funções com RBAC](#).
 - Em **Configurações > Modelos de notificação**, para criar ou atualizar modelos de notificação para usar em ações automatizadas, registros e mensagens de notificação padrão enviadas para os usuários. Configure os modelos de notificação para enviar mensagens por três canais diferentes: Secure Hub, SMTP ou SMS. Para obter mais informações, consulte: [Criar e atualizar modelos de notificação](#).
- Modo de segurança de registro e convites
 - Em **Configurações > Registro**, configure até sete modos de segurança de registro e envie convites para registro. Cada modo de segurança de registro tem seu próprio nível de segurança e as etapas que os usuários devem seguir para registrar seus dispositivos.
 - [Ativar AutoDiscovery no XenMobile para o registro de usuário](#)

Para adicionar, editar, desbloquear ou excluir contas de usuários

Você pode adicionar contas de usuário locais ao XenMobile manualmente ou pode usar um arquivo de provisionamento para importar as contas. Para as etapas para importar contas de usuário de um arquivo de provisionamento, consulte [Importar contas de usuário](#).

1. No console XenMobile, clique em **Gerenciar > Usuários**. A página **Usuários** é exibida.



2. Clique em **Mostrar filtro** para filtrar a lista.

Para adicionar uma conta de usuário local

1. Na página **Usuários**, clique em **Adicionar usuário local**. A página **Adicionar usuário local** é exibida.

2. Defina estas configurações:

- **Nome de usuário:** digite o nome, um campo obrigatório. Você pode incluir espaços em nomes, bem como letras maiúsculas e minúsculas.
- **Senha:** digite uma senha de usuário opcional. A senha deve ter pelo menos 14 caracteres e atender a todos os seguintes critérios:
 - Incluir pelo menos dois números
 - Incluir pelo menos uma letra maiúscula e uma letra minúscula
 - Incluir pelo menos um caractere especial

- Não inclua palavras de dicionário ou palavras restritas, como seu nome de usuário ou endereço de e-mail da Citrix
- Não inclua mais de três caracteres sequenciais e repetidos ou padrões de teclado, como 1111, 1234 ou asdf
- **Função:** Na lista, clique na função do usuário. Para obter mais informações sobre as funções, consulte [Configurar funções com RBAC](#). As opções possíveis são:
 - ADMIN
 - DEVICE_PROVISIONING
 - SUPPORT
 - USER
- **Participação:** na lista, clique nos grupos aos quais deseja adicionar o usuário.
- **Propriedades de usuário:** adicione as propriedades de usuário opcionais. Para cada propriedade de usuário que você deseja adicionar, clique em **Adicionar** e siga os procedimentos:
 - **Propriedades de usuário:** Na lista, clique em uma propriedade e digite o atributo de propriedade do usuário no campo ao lado da propriedade.
 - Clique em **Concluído** para salvar a propriedade do usuário ou clique em **Cancelar**.

Para excluir uma propriedade do usuário existente, passe o mouse sobre a linha que contém a propriedade e clique no X à direita. A propriedade é excluída imediatamente.

Para editar uma propriedade do usuário existente, clique na propriedade e faça alterações. Clique em **Concluído** para salvar a listagem alterada ou em **Cancelar** para deixar a listagem inalterada.

3. Clique em **Salvar**.

Para editar uma conta de usuário local

1. Na página **Usuários**, na lista de usuários, clique para selecionar um usuário e clique em **Editar**. A página **Editar usuário local** é exibida.

Edit Local User

User name* administrator

Password Enter new password

Role* ADMIN

Membership

- local\Device Enrollment Program Group
- local\MSP

Manage Groups

- User Properties Add

2. Altere as seguintes informações conforme apropriado:

- **Nome de usuário:** Não é possível alterar o nome do usuário.
- **Senha:** Altere ou adicione uma senha de usuário.
- **Função:** Na lista, clique na função do usuário.
- **Participação:** Na lista, clique nos grupos aos quais deseja adicionar o usuário. Para remover a conta de usuário de um grupo, desmarque a caixa de seleção ao lado do nome do grupo.
- **Propriedade do usuário:** Você pode optar por um dos seguintes procedimentos:
 - Para cada propriedade de usuário que você deseja alterar, clique na propriedade e faça as alterações. Clique em **Concluído** para salvar a listagem alterada ou em **Cancelar** para deixar a listagem inalterada.
 - Para cada propriedade de usuário que você deseja adicionar, clique em **Adicionar** e siga os procedimentos:
 - * **Propriedades de usuário:** Na lista, clique em uma propriedade e digite o atributo de propriedade do usuário no campo ao lado da propriedade.
 - * Clique em **Concluído** para salvar a propriedade do usuário ou clique em **Cancelar**.
 - Para cada propriedade de usuário existente que você deseja excluir, passe o mouse sobre a linha que contém a propriedade e clique no **X** à direita. A propriedade é excluída imediatamente.

3. Clique em **Salvar** para salvar suas alterações ou em **Cancelar** para deixar o usuário inalterado.

Para desbloquear uma conta de usuário local

1. Na página **Usuários**, na lista de contas de usuários, clique para selecionar uma conta de usuário.
2. Clique em **Desbloquear usuário local**. Uma caixa de diálogo de confirmação é exibida.
3. Clique em **Desbloquear** para desbloquear a conta de usuário ou clique em **Cancelar** para deixar o usuário inalterado.

Para excluir uma conta de usuário local

1. Na página **Usuários**, na lista de contas de usuários, clique para selecionar uma conta de usuário. Você pode selecionar mais de um usuário a ser excluído marcando a caixa de seleção ao lado de cada usuário.

1. Clique em **Excluir**. Uma caixa de diálogo de confirmação é exibida.
2. Clique em **Excluir** para excluir o usuário ou em **Cancelar**.

Para excluir usuários do Active Directory

Para excluir um ou mais usuários do Active Directory por vez, selecione os usuários e clique em **Excluir**.

Se um usuário que você excluir tiver os dispositivos registrados e você desejar registrar novamente esses dispositivos, exclua os dispositivos antes de registrá-los. Para excluir um dispositivo, vá até **Gerenciar > Dispositivos**, selecione o dispositivo e, em seguida, clique em **Excluir**.

Importar contas de usuário

Você pode importar contas de usuário locais e propriedades de um arquivo .csv, chamado de arquivo de provisionamento, que pode ser criado manualmente. Para obter mais informações sobre arquivos de provisionamento, consulte Formatos de arquivo de provisionamento.

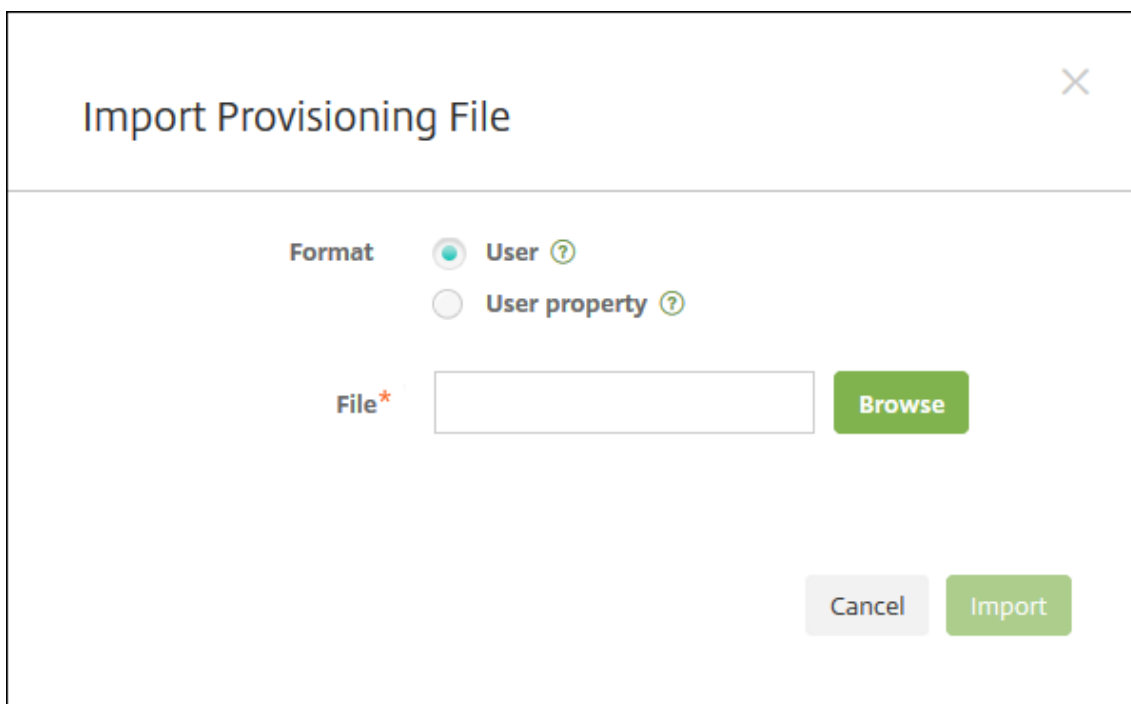
Nota:

- Para usuários locais, use o nome de domínio junto com o nome do usuário no arquivo de importação. Por exemplo, especifique nome_usuario@domínio. Se o usuário local que você criar ou importar for um domínio gerenciado no XenMobile, o usuário não poderá fazer o registro usando as credenciais LDAP correspondentes.
- Se você estiver importando contas de usuários para o diretório de usuário interno do XenMobile, desative o domínio padrão para acelerar o processo de importação. Lembre-se que desativar o domínio afeta os registros, portanto, reative o domínio padrão após a importação de usuários internos ser concluída.

- Os usuários locais podem estar no formato de nome UPN. No entanto, a Citrix recomenda que você não use o domínio gerenciado. Por exemplo, se exemplo.com for gerenciado, não crie um usuário local com este formato de UPN: user@example.com.

Depois que você preparar um arquivo de provisionamento, siga estas etapas para importá-lo para o XenMobile.

1. No console XenMobile, clique em **Gerenciar > Usuários**. A página **Usuários** é exibida.
2. Clique em **Importar usuários locais**. A caixa de diálogo **Importar Arquivo de Provisionamento** é exibida.



The screenshot shows a dialog box titled "Import Provisioning File". It contains a "Format" section with two radio buttons: "User" (selected) and "User property". Below this is a "File*" input field with a "Browse" button to its right. At the bottom right, there are "Cancel" and "Import" buttons.

3. Selecione **Usuário** ou **Propriedade** para o formato do arquivo de provisionamento que você está importando.
4. Selecione o arquivo de provisionamento a ser usada clicando em **Procurar** e navegando até a localização do arquivo.
5. Clique em **Importar**.

Formatos de arquivo de provisionamento

Você pode criar manualmente um arquivo de provisionamento para importar contas e propriedades de usuário para o XenMobile. Os formatos válidos são os seguintes:

- **Campos de arquivo de provisionamento do usuário:** `user;password;role;group1;group2`

- **Campos de arquivo de provisionamento de atributo do usuário:** `user;propertyName1;propertyValue1;propertyName2;propertyValue2`

Nota:

- Separe os campos no arquivo de provisionamento com um ponto e vírgula (;). Se parte de um campo contiver um ponto e vírgula, ele deverá ser antecedido por um caractere de barra invertida (\). Por exemplo, digite a propriedade `propertyV;test;1;2` como `propertyV\;test\;1\;2` no arquivo de provisionamento.
- Os valores válidos para **Função** são as funções predefinidas USER, ADMIN, SUPPORT e DEVICE_PROVISIONING, além outras funções que você definiu.
- Use o caractere de ponto (.) como um separador para criar a hierarquia de grupo. Não use um ponto nos nomes de grupo.
- Use letras minúsculas para atributos de propriedade nos arquivos de provisionamento de atributo. O banco de dados diferencia maiúsculas de minúsculas.

Exemplo de conteúdo de fornecimento de usuário

A entrada `user01;pwd\;01;USER;myGroup.users01;myGroup.users02;myGroup.users.users01` significa:

- **Usuário:** `user01`
- **Senha:** `pwd;01`
- **Função:** `USER`
- **Grupos:**
 - `myGroup.users01`
 - `myGroup.users02`
 - `myGroup.users.users01`

Como outro exemplo, `AUser0;1.password;USER;ActiveDirectory.test.net` significa:

- **Usuário:** `AUser0`
- **Senha:** `1.password`
- **Função:** `USER`
- **Grupo:** `ActiveDirectory.test.net`

Exemplo de conteúdo de fornecimento de atributo do usuário

A entrada `user01;propertyN;propertyV\;test\;1\;2;prop 2;prop2 value` significa:

- **Usuário:** `user01`
- **Propriedade 1**
 - **nome:** `propertyN`
 - **valor:** `propertyV;test;1;2`

- **Propriedade 2:**

- **nome:** `prop 2`
- **valor:** `prop2 value`

Para configurar modos de segurança de registro

Você configura um modo de segurança de registro de dispositivo para especificar um nível de segurança e um modelo de notificação para o registro do dispositivo no XenMobile.

O XenMobile oferece sete modos de segurança de registro, cada um com seu próprio nível de segurança e etapas que os usuários devem seguir para registrar seus dispositivos. Configure modos de segurança de registro no console XenMobile Server da página **Configurações > Registro**.

Você pode disponibilizar alguns modos no Portal de Autoajuda. No portal, os usuários geram links de registro que lhes permitem registrar seus dispositivos. Os usuários de iOS, iPadOS, macOS e Android legado podem optar por enviar a si mesmos um convite para registro a partir do portal. Os convites para registro não estão disponíveis para dispositivos Android Enterprise e Windows.

Envie convites de registro na página **Gerenciar > Convites de registro**. Para obter informações, consulte [Envie um convite para registro](#).

Nota:

Se você planejar usar modelos de notificação personalizados, deverá configurar os modelos antes de você configurar os modos de segurança de registro. Para obter mais informações sobre modelos de notificação, consulte [Criando ou atualizando modelos de notificação](#).

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Settings** é exibida.
2. Clique em **Registro**. A página **Registro** é exibida, contendo uma tabela de todos os modos de segurança de registro disponíveis. Por padrão, todos os modos de segurança de registro estão ativados.
3. Selecione um modo de segurança de registro na lista para editá-lo. Em seguida, defina o modo como padrão, desative o modo ou permita o acesso de usuários ao Portal de Autoajuda.

Nota:

Quando você marca a caixa de seleção ao lado de um modo de segurança de registro, o menu de opções é exibido acima da lista de modos de segurança de registro. Quando você clica em qualquer outro lugar da lista, o menu de opções é exibido no lado direito da listagem.

Settings > Enrollment

Enrollment

Enable and disable enrollment modes for users. You can also enable the Self Help Portal to allow users to generate enrollment links that let them download Work Home and enroll their devices, or to send themselves an enrollment invitation.

<input type="checkbox"/>	Name	Enabled	Default	Self Help Portal	Expire after	Attempts	PIN length	PIN type	Templates	▼
<input type="checkbox"/>	User name + Password	✓	✓							
<input type="checkbox"/>	High Security	✓			1 day(s)	3	8	numeric		
<input type="checkbox"/>	Invitation URL	✓			1 day(s)					
<input type="checkbox"/>	Invitation URL + PIN	✓			1 day(s)	3	8	numeric		
<input type="checkbox"/>	Invitation URL + Password	✓			1 day(s)	3				
<input type="checkbox"/>	Two Factor	✓			1 day(s)	3	8	numeric		
<input type="checkbox"/>	User name + PIN	✓			1 day(s)	3	8	numeric		

Showing 1 - 7 of 7 items

Escolha entre os modos de segurança de registro:

- Nome de usuário + Senha
- Alta Segurança
- URL de Convite
- URL de Convite + PIN
- URL de Convite + Senha
- Autenticação de dois fatores
- Nome de usuário + PIN

Você pode usar convites de registro para restringir o registro para os usuários com apenas um convite.

Você pode usar convites de registro de PIN de uso único (OTP) como uma solução de autenticação de dois fatores. Os convites de registro OTP controlam o número de dispositivos que um usuário pode registrar.

Para ambientes com requisitos de segurança, você pode associar convites de registro a um dispositivo por UDID/SN/EMEI. Uma opção de autenticação de dois fatores também está disponível para exigir uma senha do Active Directory e OTP.

Para editar um modo de segurança de registro

1. Na lista **Registro**, selecione um modo de segurança de registro e clique em **Editar**. A página **Editar Modo de Registro** é exibida. O modo selecionado determina as opções mostradas.

Settings > Enrollment > Edit Enrollment Mode

Edit Enrollment Mode

Name High Security

Expire after* 1 Days ⓘ

Maximum attempts* 3 ⓘ

PIN Length* 8 Numeric ▾

Notification templates

Template for enrollment URL -- SELECT ONE -- ▾

Template for Enrollment PIN -- SELECT ONE -- ▾

Template for enrollment confirmation -- SELECT ONE -- ▾

Cancel Save

2. Altere as seguintes informações conforme apropriado:
 - **Expira após:** digite um prazo de expiração após o qual os usuários não poderão registrar dispositivos. Este valor aparece nas páginas de configuração de convite de registro de usuário e de grupo.
Digite **0** para impedir que o convite expire.
 - **Dias:** na lista, clique em **Dias** ou **Horas** para corresponder ao prazo de expiração inserido em **Expira após**.
 - **Máximo de tentativas:** digite o número de tentativas para registrar que um usuário pode fazer antes que o processo de registro fique bloqueado para ele. Este valor aparece nas páginas de configuração de convite de registro de usuário e de grupo.
Digite **0** para permitir tentativas ilimitadas.
 - **Comprimento do PIN:** digite um numeral para definir o comprimento do PIN gerado.
 - **Numérico:** na lista, clique em **Numérico** ou **Alfanumérico** para o tipo de PIN.
 - **Modelos de notificação:**

- **Modelo de URL de registro:** na lista, clique em um modelo a ser usado para a URL de registro. Por exemplo, o modelo de convite de registro envia aos usuários um email ou SMS. O método depende de como você configurou o modelo que permite registrar seus dispositivos no XenMobile. Para obter mais informações sobre modelos de notificação, consulte [Criando ou atualizando modelos de notificação](#).
- **Modelo de PIN de registro:** na lista, clique em um modelo a ser usado para o PIN de registro.
- **Modelo de confirmação de registro:** na lista, clique em um modelo a ser usado para informar um usuário que ele foi registrado com sucesso.

3. Clique em **Salvar**.

Para definir um modo de segurança de registro como padrão

Quando você define um modo de segurança de registro como padrão, o modo é usado para todas as solicitações de registro de dispositivo, a menos que você selecione um modo de segurança de registro diferente. Se nenhum modo de segurança de registro for definido como padrão, você deverá criar uma solicitação de registro para cada dispositivo.

Nota:

Os únicos modos de segurança de registro que você pode usar como padrão são **Somente nome de usuário + senha**, **Dois fatores** ou **Nome de usuário + PIN**.

1. Selecione o modo de segurança de registro, **Nome de usuário + senha**, **Dois fatores** ou **Nome de usuário + PIN**.

Para usar um modo como padrão, é preciso ativá-lo primeiramente.

2. Clique em **Padrão**. O modo selecionado agora é o padrão. Se qualquer outro modo de segurança de registro tiver sido definido como padrão, o modo não será mais o padrão.

Para desabilitar um modo de segurança de registro

Desativar um modo de segurança de registro o torna indisponível para uso nos convites de registro de grupo e no Portal de Autoajuda. Você pode alterar como os usuários podem registrar seus dispositivos desativando um modo de segurança de registro e permitindo outro.

1. Selecione um modo de segurança de registro.

Você não pode desativar o modo de segurança de registro padrão. Se você desejar desativar o modo de segurança de registro padrão, deverá primeiro remover o status padrão.

2. Clique em **Desativar**. O modo de segurança de registro não está mais ativado.

Para habilitar um modo de segurança de registro no Portal de Autoajuda

Permitir um modo de segurança de registro no Portal de Autoajuda permite que os usuários registrem seus dispositivos no XenMobile individualmente.

Nota:

- O modo de segurança de registro deve ser ativado e estar limitado aos modelos de notificação a serem disponibilizados no Portal de Autoajuda.
- Você só pode ativar um modo de segurança de registro no Portal de Autoajuda por vez.

1. Selecione um modo de segurança de registro.
2. Clique em **Portal de Autoajuda**. O modo de segurança de registro selecionado está disponível para os usuários do Portal de Autoajuda. Qualquer modo que já estiver ativado no Portal de Autoajuda não estará mais disponível para os usuários.

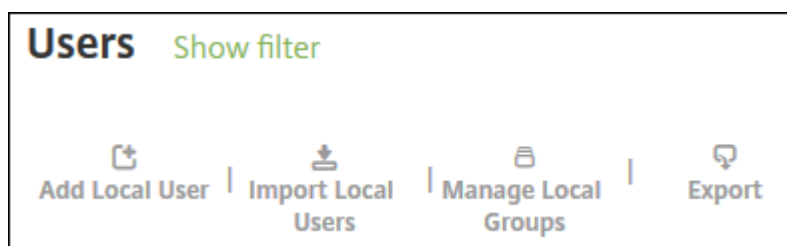
Adição ou remoção de grupos

Gerencie grupos na caixa de diálogo **Gerenciar grupos** no console XenMobile nestas páginas: **Usuários**, **Adicionar usuário local** ou **Editar usuário local**. Não há nenhum comando de edição de grupo.

Se você remover um grupo, esteja ciente de que a remoção do grupo não afeta as contas de usuário. Remover um grupo simplesmente remove a associação dos usuários àquele grupo. Os usuários também perdem acesso aos aplicativos ou aos perfis fornecidos pelos Grupos de Entrega que são associados a esse grupo; todas as outras associações de grupo, no entanto, permanecem intactas. Se os usuários não estiverem associados a nenhum outro grupo local, eles estarão associados ao nível superior.

Para adicionar um grupo local

1. Você pode optar por um dos seguintes procedimentos:
 - Na página **Usuários**, clique em **Gerenciar grupos locais**.

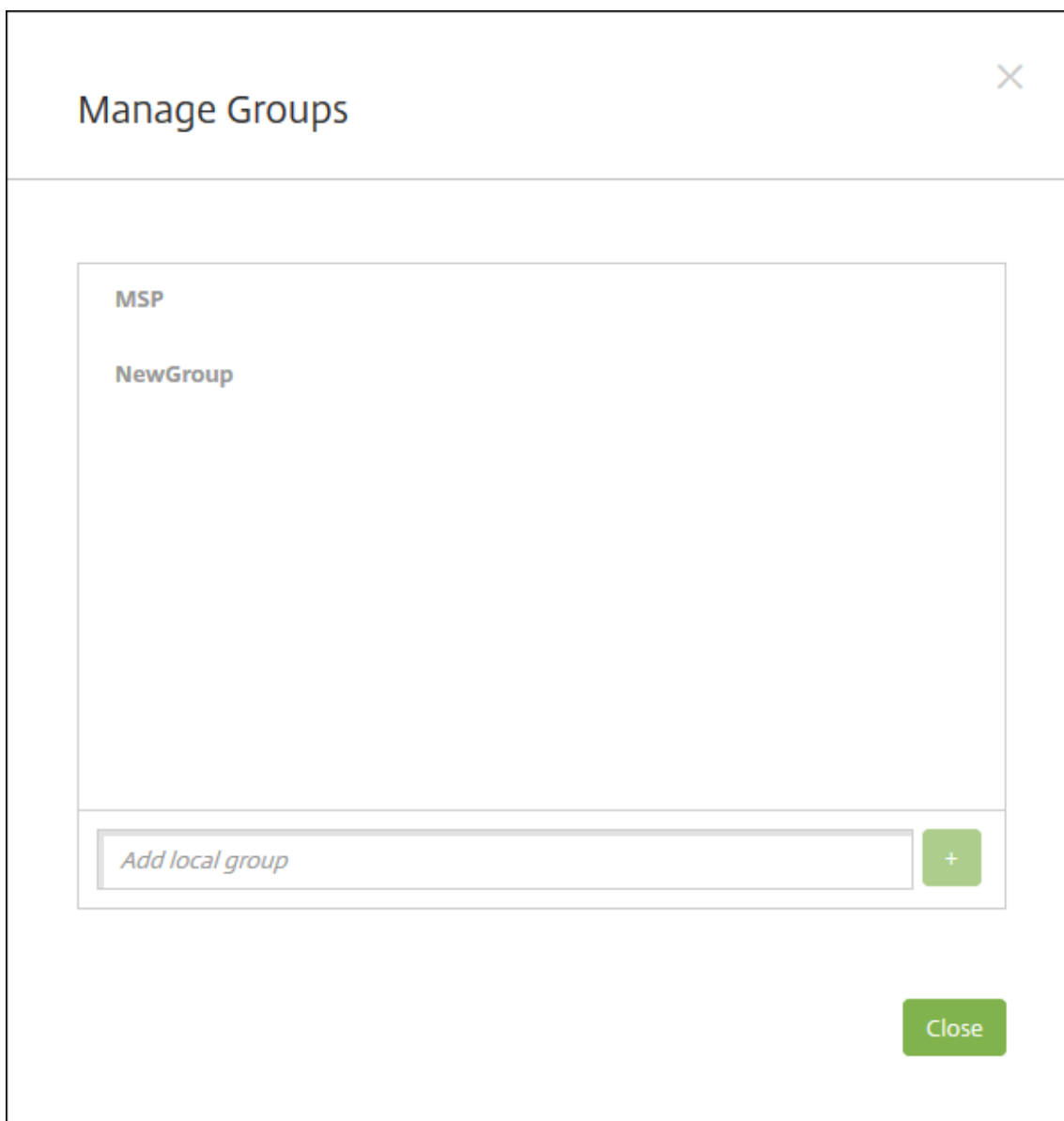


- Na página **Adicionar usuário local** ou na página **Editar usuário local**, clique em **Gerenciar grupos**.

The screenshot shows a configuration dialog box with the following elements:

- User name***: Text input field containing "User01".
- Password**: Text input field containing the placeholder text "Enter new password".
- Role***: Dropdown menu showing "SUPPORT".
- Membership**: List box containing "local\MSP" with a checked checkbox.
- Manage Groups**: A blue button located to the right of the membership list.

A caixa de diálogo **Gerenciar grupo** é exibida.



2. Abaixo da lista de grupos, digite um novo nome de grupo e, em seguida, clique no sinal de mais (+). O grupo de usuário é adicionado à lista.
3. Clique em **Fechar**.

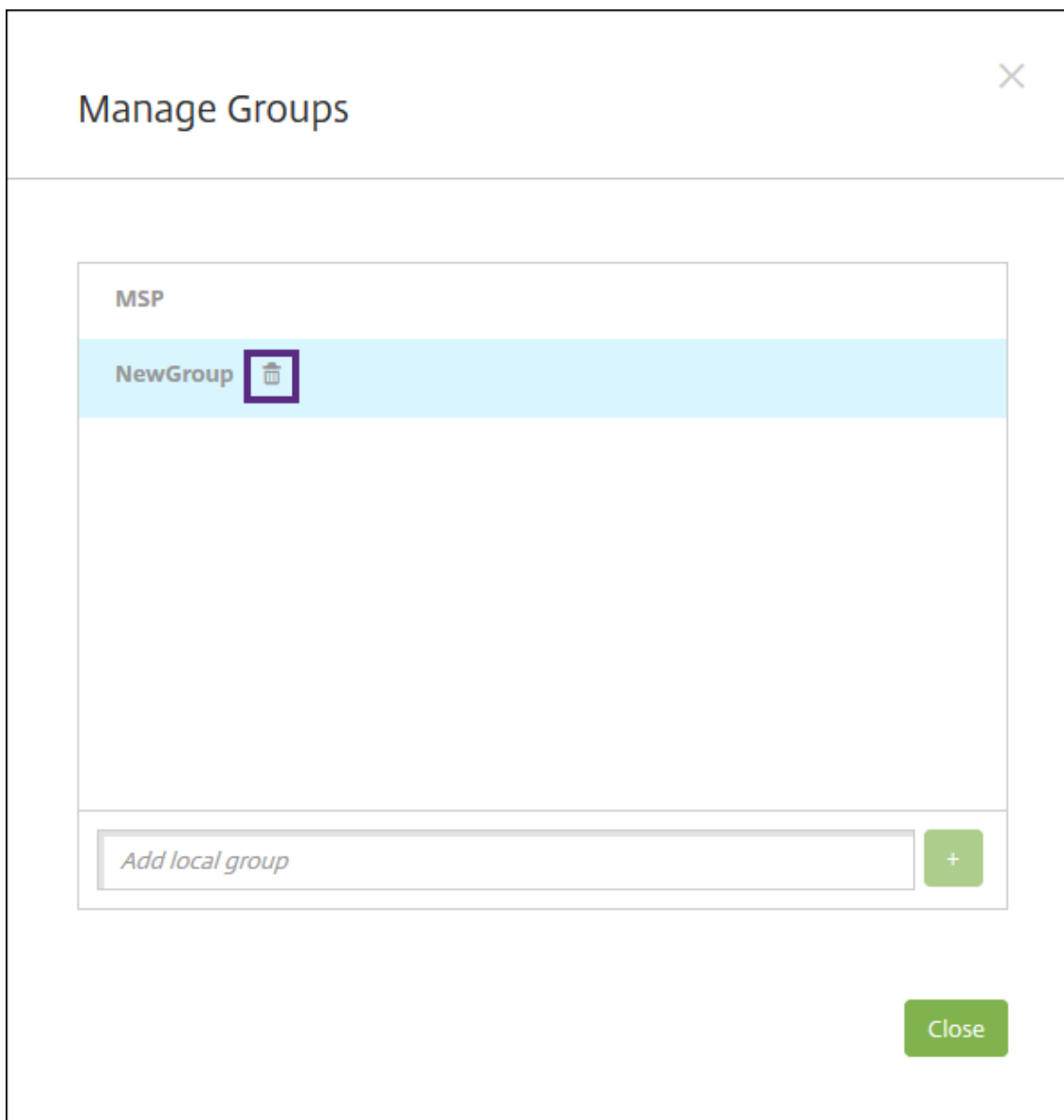
Para remover um grupo

Remover um grupo não afeta as contas de usuário. Remover um grupo simplesmente remove a associação do usuário àquele grupo. Os usuários também perdem acesso aos aplicativos ou aos perfis fornecidos pelos Grupos de Entrega que são associados a esse grupo. No entanto, todas as outras associações de grupo permanecem intactas. Se os usuários não estiverem associados a nenhum outro grupo local, eles estarão associados ao nível superior.

1. Você pode optar por um dos seguintes procedimentos:

- Na página **Usuários**, clique em **Gerenciar grupos locais**.
- Na página **Adicionar usuário local** ou na página **Editar usuário local**, clique em **Gerenciar grupos**.

A caixa de diálogo **Gerenciar grupos** é exibida.



2. Na caixa de diálogo **Gerenciar grupos**, clique no grupo que você deseja excluir.
3. Clique no ícone de lixeira à direita do nome do grupo. Uma caixa de diálogo de confirmação é exibida.
4. Clique em **Excluir** para confirmar a operação e remover o grupo.

Importante:

Você não pode desfazer essa operação.

5. Na caixa de diálogo **Gerenciar Grupos**, clique em **Fechar**.

Criar e gerenciar fluxos de trabalho

Você pode usar fluxos de trabalho para gerenciar a criação e a remoção de contas de usuário. Antes de poder usar um fluxo de trabalho, identifique as pessoas em sua organização que têm a autoridade para aprovar solicitações de conta de usuário. Em seguida, você pode usar o modelo de fluxo de trabalho para criar e aprovar solicitações de conta de usuário.

Quando você configura o XenMobile pela primeira vez, define as configurações de email de fluxo de trabalho, o que deve ocorrer antes de você poder usar os fluxos de trabalho. Você pode alterar as configurações de email de fluxo de trabalho a qualquer momento. Essas configurações incluem o servidor de email, a porta, o endereço de email, e se a solicitação para criar a conta de usuário requer aprovação.

Você pode configurar os fluxos de trabalho em dois lugares no XenMobile:

- Na página **Fluxos de trabalho** no console XenMobile. Na página **Fluxos de trabalho**, você pode configurar vários fluxos de trabalho para serem usados com as configurações do aplicativo. Ao configurar fluxos de trabalho na página Fluxos de trabalho, você pode selecionar o fluxo de trabalho durante a configuração do aplicativo.
- Ao configurar um conector de aplicativo, forneça um nome de fluxo de trabalho e configure os indivíduos que podem aprovar a solicitação de conta de usuário. Consulte [Adição de aplicativos ao XenMobile](#).

Você pode atribuir até três níveis à aprovação do gerente de contas de usuário. Se você precisar que outras pessoas aprovem a conta de usuário, poderá procurar e selecionar essas pessoas usando o respectivo nome ou endereço de email. Quando o XenMobile encontrar a pessoa, adicione-a ao fluxo de trabalho. Todos os indivíduos do fluxo de trabalho recebem emails para aprovar ou negar a nova conta de usuário.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Settings** é exibida.
2. Clique em **Fluxos de trabalho**. A página **Fluxos de trabalho** é exibida.
3. Clique em **Adicionar**. A página **Adicionar fluxo de trabalho** é exibida.

Settings > Workflows > Add Workflow

Add Workflow

Name*

Description

Email Approval Templates Workflow Approval Request

Levels of manager approval 1 level

Select Active Directory domain agsag.com

Find additional required approvers

Selected additional required approvers

4. Defina estas configurações:

- **Nome:** digite um nome exclusivo para o fluxo de trabalho.
- **Descrição:** opcionalmente, digite uma descrição para o fluxo de trabalho.
- **Modelos de aprovação de email:** na lista, selecione o modelo de aprovação a ser atribuído. Você pode criar modelos de emails na seção **Modelos de notificação** sob **Configurações** no console XenMobile. Quando você clica no ícone de olho à direita deste campo, é exibida uma visualização do modelo que você está configurando.
- **Níveis de aprovação do gerente:** na lista, selecione o número de níveis de aprovação do gerente necessários para esse fluxo de trabalho. O padrão é **1 nível**. As opções possíveis são:
 - Não é Necessário
 - 1 nível
 - 2 níveis
 - 3 níveis
- **Selecionar domínio do Active Directory:** na lista, selecione o domínio do Active Directory adequado a ser usado para o fluxo de trabalho.

- **Encontrar aprovadores necessários adicionais:** digite o nome no campo de busca e clique em **Pesquisar**. Os nomes são originários do Active Directory.
- Quando o nome aparece no campo, selecione a caixa de seleção próxima ao nome. O nome e endereço de email da pessoa aparecem na lista **Aprovadores necessários adicionais selecionados**.
 - Para remover um nome da lista, proceda de um dos seguintes modos:
 - * Clique em **Pesquisar** para ver uma lista de todos no domínio selecionado.
 - * Digite um nome parcial ou completo na caixa Pesquisar e clique em **Pesquisar** para limitar os resultados da pesquisa.
 - * As pessoas da lista **Aprovadores necessários adicionais selecionados** têm marcas de seleção ao lado do respectivo nome na lista de resultados de pesquisa. Percorra a lista e desmarque a caixa de seleção ao lado de cada nome que você deseja remover.

5. Clique em **Salvar**. O fluxo de trabalho criado é exibido na página **Fluxos de trabalho**.

Depois de criar o fluxo de trabalho, você pode exibir os detalhes do fluxo de trabalho, exibir os aplicativos associados a ele ou excluí-lo. Você não pode editar um fluxo de trabalho depois de tê-lo criado. Se você precisar de um fluxo de trabalho com níveis diferentes de aprovação ou aprovadores diferentes, crie outro fluxo de trabalho.

Para ver detalhes e excluir um fluxo de trabalho

1. Na página **Fluxos de trabalho**, na lista de fluxos de trabalho existentes, selecione um fluxo de trabalho específico. Para tanto, clique na linha da tabela ou selecione a caixa de seleção ao lado do fluxo de trabalho.
2. Para excluir um fluxo de trabalho, clique em **Excluir**. Uma caixa de diálogo de confirmação é exibida. Clique em **Excluir** novamente.

Importante:

Você não pode desfazer essa operação.

Perfis de registro

May 24, 2021

Um perfil de registro especifica o seguinte:

- Opções de registro de gerenciamento de dispositivo para dispositivos Android e iOS. Para Android, as opções de registro disponíveis para o modo de servidor MDM+MAM (ENT) diferem das opções para o modo MDM.

- Opções de registro de gerenciamento de aplicativo para dispositivos Android e iOS.
- Outras opções de registro:
 - Limitar o número de dispositivos que um usuário pode registrar.
Se o limite do dispositivo for atingido, uma mensagem de erro informa o usuário que ele excedeu o limite de registro do dispositivo.
 - Permitir que um usuário recuse o gerenciamento de dispositivo.

Você pode usar perfis de registro para combinar vários casos de uso e caminhos de migração de dispositivos em um único console XenMobile Server. Alguns casos de uso incluem:

- Gerenciamento de Dispositivos Móveis (somente MDM)
- MDM+Gerenciamento de Aplicativos Móveis (MAM)
- Somente MAM
- Registros de propriedade da empresa
- Registros BYOD (a capacidade de cancelar o registro no MDM)
- Migração de registros do Android Device Administrator para registros do Android Enterprise (totalmente gerenciado, perfil de trabalho, dispositivo dedicado)

Ao criar um grupo de entrega, você pode usar o perfil de registro padrão denominado Global ou especificar um perfil de registro diferente.

Os recursos de perfil de registro por plataforma incluem o seguinte.

- **Para dispositivos Android:** você especifica o modo proprietário do dispositivo. Por exemplo, totalmente gerenciado, totalmente gerenciado com perfil de trabalho e perfil de trabalho BYOD. A opção **Dispositivo dedicado** aparece somente quando você tem uma licença Enterprise ou Advanced para o XenMobile. Os novos dispositivos são registrados no Android Enterprise e no gerenciamento de aplicativos por padrão. Os modos de segurança de registro **Nome de usuário + PIN**, **URL de convite**, **URL de convite + PIN** e **URL de convite + senha** não estão disponíveis para o Android Enterprise.
- **Para dispositivos iOS:** você especifica o tipo de registro do dispositivo: Registro do dispositivo ou dispositivos sem gerenciamento. As configurações do iOS aparecem somente quando você tem uma licença Enterprise ou Advanced para o XenMobile. Os novos dispositivos são registrados no gerenciamento de aplicativos e gerenciamento de dispositivos Apple por padrão.

Se não precisar registrar dispositivos dedicados para dispositivos Android nem precisar do registro somente MAM para dispositivos Android ou iOS, você pode desativar a propriedade do servidor `enable.multimode.xms`. No entanto, manter essa propriedade ativada significa que você precisa de apenas um XenMobile Server para lidar com todos os tipos de perfis de registro. Consulte [Propriedades do servidor](#).

Quando você desabilita `enable.multimode.xms`, apenas as configurações nesta captura de tela ficam disponíveis:

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	Device management ?
Android	<p>Management</p> <p><input checked="" type="radio"/> Android Enterprise ?</p> <p><input type="radio"/> Legacy device administration (not recommended) ?</p> <p>Device owner mode</p> <p><input checked="" type="radio"/> Company-owned device ?</p> <p><input type="radio"/> Fully managed with work profile ?</p> <p>BYOD work profile <input checked="" type="checkbox"/> ?</p>
3 Assignment (optional)	

Para obter mais detalhes sobre essas configurações, consulte [Android Enterprise](#).

Perfil de registro global

O perfil de registro padrão é chamado de Global. O perfil Global é útil para testes até que você tenha a chance de criar perfis de registro.

As capturas de tela a seguir mostram as configurações padrão do perfil de registro Global.

Enrollment Profile	Enrollment Info
1 Enrollment Info	Set the number of devices a user can enroll. The default is unlimited, which lets users enroll an unlimited number of devices.
2 Platforms	<p>Enrollment profile name * <input type="text"/></p> <p>Total number of devices a user can enroll <input type="text" value="unlimited"/></p>
Android	
iOS	
3 Assignment (optional)	

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	
Android	<p>Device management ⓘ</p> <p>Management</p> <p><input checked="" type="radio"/> Android Enterprise ⓘ</p> <p><input type="radio"/> Legacy device administration (not recommended) ⓘ</p> <p><input type="radio"/> Do not manage devices ⓘ</p> <p>Device owner mode</p> <p><input checked="" type="radio"/> Company-owned device ⓘ</p> <p><input type="radio"/> Fully managed with work profile ⓘ</p> <p><input type="radio"/> Dedicated device ⓘ</p> <p><input type="radio"/> None ⓘ</p> <p>BYOD work profile <input checked="" type="checkbox"/> ⓘ</p> <p>Application management ⓘ</p> <p>Citrix MAM <input checked="" type="checkbox"/> ⓘ</p> <p>User consent</p> <p>Allow users to decline device management <input checked="" type="checkbox"/> ⓘ</p>
iOS	
3 Assignment (optional)	

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	
Android	
iOS	<p>Device management ⓘ</p> <p>Management</p> <p><input checked="" type="radio"/> Device enrollment ⓘ</p> <p><input type="radio"/> Do not manage devices ⓘ</p> <p>Application management ⓘ</p> <p>Citrix MAM <input checked="" type="checkbox"/> ⓘ</p> <p>User consent</p> <p>Allow users to decline device management <input checked="" type="checkbox"/> ⓘ</p>
3 Assignment (optional)	

Perfis de registro, grupos de entrega e registro

Os perfis de registro e os grupos de entrega interagem da seguinte forma:

- Você pode anexar um perfil de registro a um ou mais grupos de entrega.
- Se um usuário pertencer a vários grupos de entrega que têm perfis de registro diferentes, o nome do grupo de entrega determinará o perfil de registro usado. O XenMobile Server seleciona o grupo de entrega que aparece por último em uma lista alfabética de grupos de entrega. Por

exemplo, suponha que você tenha o seguinte:

- Dois perfis de registro, chamados “EP1” e “EP2”.
- Dois grupos de entrega, denominados “DG1” e “DG2”.
- “DG1” está associado ao “EP1”.
- “DG2” está associado ao “EP2”.

Se o usuário de registro estiver nos grupos de entrega “DG1” e “DG2”, o XenMobile Server usará o perfil de registro “EP2” para determinar o tipo de registro para o usuário.

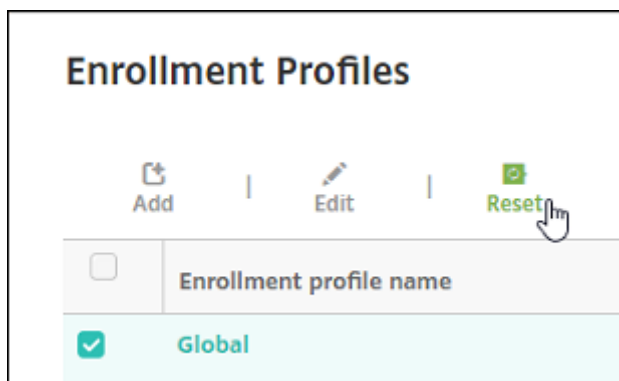
- A ordem de implantação se aplica somente a dispositivos em um grupo de entrega que tenha um perfil de registro configurado para MDM (gerenciamento de dispositivo).
- Após o registro de um dispositivo, algumas alterações ao perfil de registro exigem um novo registro:
 - Adicionar MAM a um perfil de registro configurado para MDM.
 - Mover um dispositivo registrado no MDM para um grupo de entrega configurado para MDM+MAM. Essa mudança afeta apenas os registros de dispositivos novos. Os registros de dispositivos existentes não são afetados.
 - Adicionar MDM a um perfil de registro configurado para MAM.
- Mudar para um perfil de registro diferente não afeta os dispositivos registrados existentes. No entanto, os usuários devem cancelar o registro e registrar novamente os dispositivos para que as alterações entrem em vigor.

Para criar um perfil de registro

1. No console XenMobile Server, vá para **Configurar > Perfis de registro**.
2. Na página de **Informações de registro**, digite um nome descritivo para o perfil. Por padrão, um usuário pode registrar dispositivos ilimitadamente. Selecione um valor para limitar o número de dispositivos por usuário. O limite se aplica à soma de dispositivos Android e iOS gerenciados por MAM ou MDM que um usuário registra.
3. Preencha as páginas de plataforma. Para obter informações sobre configurações de registro específicas para as plataformas, consulte:
 - [Android Enterprise](#)
 - iOS: [Métodos de registro suportados](#)
4. Na página **Atribuição**, anexe um ou mais grupos de entrega ao perfil de registro.

Um usuário pode pertencer a vários grupos de entrega que têm perfis de registro diferentes. Nesse caso, o nome do grupo de entrega determina o perfil de registro usado. O XenMobile seleciona o grupo de entrega que aparece por último em uma lista alfabética de grupos de entrega. Para criar grupos de entrega, vá para **Configurar > Grupos de entrega**.

Uma lista dos perfis de registro é exibida na página **Configurar > Perfis de registro**. Para editar o perfil Global ou redefini-lo para os padrões originais, selecione a linha do perfil Global e clique em **Redefinir**. Não é possível excluir o perfil Global.



Configurar funções com RBAC

August 20, 2021

Cada função de controle de acesso baseado em função (RBAC) predefinida tem acesso a determinados recursos e permissões associados. Este artigo descreve o que cada uma dessas permissões faz. Para obter uma lista completa das permissões padrão de cada função interna, baixe [Padrões de controle de acesso baseado em funções](#).

Quando você *aplica permissões*, você define os grupos de usuários que a função RBAC tem permissão para gerenciar. O administrador padrão não pode alterar as configurações de permissões aplicadas. Como padrão, as permissões aplicadas se aplicam a todos os grupos de usuários.

Quando você faz uma *atribuição*, você atribui a função RBAC a um grupo, de modo que o grupo de usuários detém os direitos de administrador RBAC.

Importante:

Na permissão de Configurações, a permissão RBAC dá aos usuários administradores acesso total, incluindo a capacidade de atribuir suas próprias permissões. Dê esse acesso apenas aos usuários que você pretende dar a capacidade de manipular tudo no sistema Endpoint Management.

Este artigo contém as seguintes seções:

- [Função de Administrador](#)
- [Função de provisionamento de dispositivos](#)
- [Função de suporte](#)
- [Função de Usuário](#)

- [Configurar funções com RBAC](#)

Função de Administrador

Os usuários com a função Administração predefinida têm acesso ou não aos recursos a seguir no XenMobile. Como padrão, **Acesso autorizado** (exceto Portal de Autoajuda), **Recursos do console** e **Aplicar permissões** estão ativados.

Acesso autorizado

Acesso ao console de administração	Os administradores têm acesso a todos os recursos no console XenMobile.
Acesso ao Portal de Autoajuda	Os administradores não têm acesso ao Portal de Autoajuda.
Assistente de registro de dispositivos compartilhados	Os administradores não têm acesso ao assistente de registro de dispositivos compartilhados. Esse recurso é destinado aos usuários que precisam registrar dispositivos compartilhados.
Acesso ao suporte remoto	Os administradores têm acesso ao suporte remoto.*
Acesso à API pública	Os administradores têm acesso à API pública para realizar, de forma programática, ações que estão disponíveis no console XenMobile. As ações incluem administrar certificados, aplicativos, dispositivos, grupos de entrega e usuários locais.
Assistente de registro de dispositivos COSU	Fornecer uma maneira de os administradores registrarem dispositivos Android Enterprise dedicados (também conhecidos como dispositivos COSU) se o recurso não foi configurado usando um perfil de registro.

* O suporte remoto permite que o pessoal da central de ajuda assumo o controle remotamente de dispositivos móveis gerenciados Windows CE e Android. Conversão de tela é compatível somente com dispositivos Samsung Knox. O suporte remoto não está disponível para implantações do XenMobile

| Suporte | A página **Solução de problemas e suporte** é onde você executa atividades de solução de problemas, como executar diagnósticos e gerar logs. |

Dispositivos

Os administradores acessam recursos de dispositivo em todo o console definindo restrições de dispositivo, configurando e enviando notificações para dispositivos, administrando os aplicativos nos dispositivos e assim por diante.

Apagamento completo do dispositivo	Apagar todos os dados e aplicativos de um dispositivo, incluindo cartões de memória, caso o dispositivo os tenha.
Apagar Restrição	Remover uma ou mais restrições de dispositivo.
Apagamento seletivo do dispositivo	Apagar todos os dados e aplicativos corporativos de um dispositivo, deixando dados pessoais e aplicativos no local.
Exibir localizações	Ver a localização de e definir as restrições geográficas em um dispositivo. Inclui: Localizar dispositivo, ver a localização de um dispositivo, rastrear dispositivo, rastrear a localização de um dispositivo ao longo do tempo.
Bloquear dispositivo	Bloquear remotamente o dispositivo, de forma que os usuários não possam usá-lo.
Desbloquear dispositivo	Desbloquear remotamente o dispositivo, de forma que os usuários não possam usá-lo.
Bloquear contêiner	Bloquear remotamente o contêiner corporativo em um dispositivo.
Desbloquear contêiner	Desbloquear remotamente o contêiner corporativo em um dispositivo.
Redefinir senha do contêiner	Redefinir a senha do contêiner corporativo.

Ativar desvio de bloqueio de ativação DEP ASM	Armazene um código de desvio em um dispositivo iOS supervisionado, quando o bloqueio de ativação estiver ativado. Se você precisar apagar o dispositivo, use esse código para limpar o bloqueio de ativação automaticamente.
Chama o dispositivo	Chamar remotamente um dispositivo Windows no volume mais alto durante cinco minutos.
Reinicializar o dispositivo	Reinicie os dispositivos Windows no console XenMobile.
Implantar no dispositivo	Enviar aplicativos, notificações, restrições e assim por diante para um dispositivo.
Editar dispositivo	Alterar as configurações do dispositivo.
Notificação para o dispositivo	Enviar uma notificação para um dispositivo.
Adicionar/excluir dispositivo	Adicionar ou remover dispositivos no XenMobile.
Importação de dispositivos	Importar um grupo de dispositivos de um arquivo para o XenMobile.
Exportar tabela do dispositivo	Coletar informações do dispositivo na página Dispositivo e exportá-las para um arquivo .csv.
Revogar dispositivo	Proibir um dispositivo de se conectar ao XenMobile.
Bloqueio de aplicativo	Negar acesso a todos os aplicativos em um dispositivo. No Android, os usuários não podem fazer login no XenMobile. No iOS, os usuários podem fazer login, mas não podem acessar aplicativos.
Apagamento de aplicativos	No Android, esta ação exclui a conta do XenMobile do usuário. No iOS, essa ação exclui a chave de criptografia de que os usuários precisam para ter acesso aos recursos do XenMobile.
Exibir inventário de software	Ver quais softwares estão instalados em um dispositivo.

Solicitar espelhamento de AirPlay	Solicitar o início do streaming do AirPlay.
Parar espelhamento de AirPlay	Parar o streaming do AirPlay.
Ativar o modo perdido	Em Gerenciar > Dispositivos , você pode colocar um dispositivo supervisionado no modo perdido para bloquear um dispositivo supervisionado na tela de bloqueio. O modo Perdido também permite localizar o dispositivo quando é perdido ou roubado.
Desativar o modo perdido	Em Gerenciar > Dispositivos , você pode desativar o modo perdido para um dispositivo que está configurado para o modo perdido.
Dispositivo de atualização de SO	Você pode implantar uma política de dispositivo de Controle de atualizações de sistema operacional para dispositivos.
Desligar o dispositivo	Desligue os dispositivos iOS no console XenMobile.
Reinicializar o dispositivo	Reinicie os dispositivos iOS no console XenMobile.

Usuários locais e grupos

Os administradores gerenciam usuários locais e grupos de usuários locais na página **Gerenciar > Usuários** no XenMobile.

Adicionar usuários locais
Excluir usuários locais
Editar usuários locais
Importar usuários locais
Exportar usuários locais
Grupos de usuários locais
Obter ID de bloqueio de usuário local
Excluir bloqueio de usuário local

Registro

Os administradores podem adicionar e excluir convites para registro, enviar notificações para os usuários e exportar a tabela de registro para um arquivo .csv.

Adicionar/excluir registro	Adicionar ou remover um convite para registro de um usuário ou um grupo de usuários.
Notificar usuário	Enviar um convite para registro para um usuário ou um grupo de usuários.
Exportar tabela de convites de registro	Coletar informações de registro na página Registro e exportá-las para um arquivo .csv.

Políticas

Adicionar/excluir política	Adicionar ou remover um dispositivo ou uma política de aplicativo.
Editar política	Alterar um dispositivo ou uma política de aplicativo.
Carregar Política	Carregar uma política de dispositivo ou de aplicativo.
Clonar Política	Copiar uma política de dispositivo ou de aplicativo.
Desativar Política	Desativar uma política de aplicativo existente.
Exportar política	Coletar informações de política de dispositivo na página Políticas de dispositivo e exportá-las para um arquivo .csv.
Atribuir política	Atribuir uma política de dispositivo a um ou mais grupos de entrega.

Aplicativo

Os administradores gerenciam aplicativos na página **Configurar > Aplicativos** no XenMobile.

Adicionar/excluir loja de aplicativos ou aplicativo empresarial	Adicionar ou remover um aplicativo da loja de aplicativos pública ou um aplicativo empresarial (não ativado para MDX).
Editar loja de aplicativos ou aplicativo empresarial	Alterar um aplicativo da loja de aplicativos pública ou um aplicativo empresarial (não ativado para MDX).
Adicionar/excluir aplicativo MDX, Web e SaaS	Adicionar ou remover um aplicativo ativado para MDX, um aplicativo da sua rede interna (aplicativo Web) ou um aplicativo de uma rede pública (SaaS) ao/do XenMobile.
Editar aplicativo MDX, Web e SaaS	Alterar um aplicativo ativado para MDX, um aplicativo da sua rede interna (aplicativo Web) ou um aplicativo de uma rede pública (SaaS) para o XenMobile.
Adicionar/excluir categoria	Adicionar ou excluir uma categoria na qual os aplicativos podem aparecer no XenMobile Store.
Atribuir aplicativo público/empresarial ao grupo de entrega	Atribuir um aplicativo de loja de aplicativos pública ou um aplicativo não preparado com MDX a um grupo de entrega para implantação.
Atribuir aplicativo MDX/WebLink/SaaS ao grupo de entrega	Atribuir a um grupo de entrega um aplicativo ativado para MDX, não exige logon único (WebLink), ou que seja de uma rede pública (SaaS).
Exportar tabela de aplicativos	Coletar informações do aplicativo na página Aplicativo e exportá-las para um arquivo .csv.

Mídia

Gerencie mídias obtidas de uma loja de aplicativos pública ou por meio de uma licença de compra por volume.

Adicionar/excluir loja de aplicativos ou livros empresariais

Atribuir livros públicos/empresariais ao grupo de entrega

Editar loja de aplicativos ou livros empresariais

Ação

Adicionar/excluir ação	Adicionar ou remover uma ação definida por um gatilho (evento, propriedade do dispositivo ou usuário, ou nome do aplicativo instalado) e a resposta associada.
Editar ação	Alterar uma ação definida por um gatilho (evento, propriedade do dispositivo ou usuário, ou nome do aplicativo instalado) e a resposta associada.
Atribuir ação ao grupo de entrega	Atribuir uma ação a um grupo de entrega para implantação nos dispositivos do usuário.
Exportar ação	Coletar informações sobre a ação na página Ações e exportá-las para um arquivo .csv.

Grupo de entrega

Os administradores gerenciam grupos de entrega na página **Configurar > Grupos de Entrega**.

Adicionar/excluir grupo de entrega	Criar ou remover um grupo de entrega, que adiciona os usuários especificados e políticas, aplicativos e ações opcionais.
Editar grupo de entrega	Alterar um grupo de entrega, que modifica os usuários e políticas opcionais, aplicativos e ações.
Implantar grupo de entrega	Disponibilizar o grupo de entrega para uso.
Exportar grupo de entrega	Coletar informações de grupo de entrega da página Grupo de Entrega e exportá-las para um arquivo .csv.

Perfil de registro

Gerenciar perfis de registro.

Adicionar/apagar perfil de registro

Editar perfil de registro

Atribuir o perfil de registro para o grupo de entrega

Configurações

Os administradores definem várias configurações nas páginas de **Configurações**.

RBAC	Atribuição de RBAC, atribuir funções. Importante: Essa permissão dá aos administradores acesso total, incluindo a capacidade de atribuir suas próprias permissões. Dê esse acesso apenas aos usuários que você pretende dar a capacidade de manipular tudo no sistema Endpoint Management.
LDAP	Administrar um ou mais diretórios em conformidade com o LDAP, como o Active Directory, para importar grupos, contas de usuário e propriedades relacionadas.
Licença	Para o XenMobile Server local. Administrar as licenças da Citrix.
Registro	Ativar os modos de segurança de registro dos usuários e o Portal de Autoajuda.
Gerenciamento de Versão	Exibir a versão instalada atual. Inclui: atualização do gerenciamento de versões
Certificados	Editar certificado APNS, certificados de ouvinte SSL

Modelos de notificação	Criar modelos de notificação para usar em ações automatizadas, registros e entregas de mensagens de notificação padrão para os usuários.
Fluxos de Trabalho	Gerenciar a criação, a aprovação e a remoção de contas de usuário para uso com as configurações do aplicativo.
Provedores de credenciais	Adicionar um ou mais provedores de credenciais autorizados a emitir certificados do dispositivo. Os provedores de credenciais controlam o formato do e as condições certificado para renová-lo ou revogá-lo.
Entidades PKI	Gerenciar entidades de infraestrutura de chave pública (genéricas, Serviços de Certificado da Microsoft ou AC discricionária).
Testar conexão PKI	Use o botão Testar Conexão na página Configurações > Entidades PKI para garantir que o servidor esteja acessível.
Propriedades do cliente	Gerenciar várias propriedades nos dispositivos do usuário, como o tipo de código secreto, a segurança ou a expiração.
Suporte ao cliente	Defina como os usuários podem entrar em contato com os seus serviços de suporte (email, telefone ou email de tíquete de suporte).
Identidade visual do cliente	Crie um nome de armazenamento personalizado e exibições de armazenamento padrão para o XenMobile Store. Adicione o logotipo personalizado exibido no XenMobile Store ou no Secure Hub.
Gateway de SMS da operadora	Instalar gateways de SMS da operadora para configurar as notificações que o XenMobile envia pelos gateways de SMS da operadora.
Servidor de notificação	Configurar um servidor de gateway SMTP para enviar emails aos usuários.

ActiveSync Gateway	Gerenciar o acesso do usuário aos usuários e dispositivos por meio de regras e propriedades.
Programa de implantação da Apple	Adicione uma conta do Programa de implantação da Apple ao XenMobile.
Registro de dispositivo do Apple Configurator	Definir configurações do Apple Configurator no XenMobile.
Configurações do compra por volume/iOS	Adicionar contas de compra por volume da Apple.
Provedor de serviços móveis	Usar a interface de Provedor de Serviços Móveis para consultar o BlackBerry e outros dispositivos do Exchange ActiveSync e para emitir operações.
Citrix Gateway	Para o XenMobile Server local. Adicione um Citrix Gateway. Escolha se deseja ativar a autenticação e se deseja enviar um certificado de usuário para autenticação. Escolha um provedor de credenciais.
Controle de Acesso da Rede	Definir as condições que determinam que um dispositivo não está em conformidade e, portanto, tem acesso negado à rede.
Samsung Knox	Ativar ou desativar o XenMobile para consultar as APIs REST do servidor de atestado do Samsung Knox.
Propriedades do servidor	Adicionar ou modificar as propriedades do servidor. Exige a reinicialização do XenMobile em todos os nós.
Syslog	Para o XenMobile Server local. Enviar arquivos de log para um servidor de logs do sistema (syslog) usando o nome de host ou o endereço IP do servidor.
XenApp e XenDesktop	Permitir que os usuários adicionem Áreas de trabalho e aplicativos virtuais via Secure Hub.

Citrix Files	Ao usar o XenMobile com contas do Enterprise: defina configurações para conexão com a conta do Content Collaboration e a conta de serviço do administrador para gerenciar contas de usuário. Exige um domínio do Citrix Files existente e credenciais de administrador. Ao usar o XenMobile com conectores de zona de armazenamento: configure o XenMobile para apontar para compartilhamentos de rede e locais do SharePoint definidos nos conectores de zonas de armazenamento.
Programa de melhoria de experiência	Para o XenMobile Server local. Aceitar ou recusar o envio de estatísticas anônimas e informações de uso para a Citrix.
Microsoft Azure	Para o XenMobile Server local. Integre o XenMobile ao Microsoft Azure.
Android Enterprise	Defina as configurações de servidor do Android Enterprise.
Provedor de identidade (IdP)	Configure um provedor de identidade.
XenMobile Tools	Acesse a página do XenMobile Tools.
Configuração de SNMP	Ative SNMP para os nós do XenMobile Server. Edite ou adicione usuários de monitoramento, configure o SNMP Manger onde as notificações de interceptação aparecem e configure intervalos e limites de interceptação.

Suporte

Os administradores podem executar várias tarefas de suporte.

Verificações de conectividade do Citrix Gateway	Executar várias verificações de conectividade do Citrix Gateway por endereço IP. Exige um nome do usuário e uma senha.
---	--

Verificações de conectividade XenMobile	Realizar verificações de conectividade dos recursos selecionados do XenMobile, como o banco de dados, o DNS ou o Google Plan.
Criar pacotes de suporte	Para o XenMobile Server local. Crie um arquivo a ser enviado para o suporte da Citrix para solução de problemas. Contém as informações do sistema, os logs, as informações do banco de dados, as informações de núcleo, arquivos de rastreamento e as informações de configuração mais recentes do XenMobile ou do Citrix Gateway.
Documentação de Produtos Citrix	Acessar o site público de documentação do Citrix XenMobile.
Citrix Knowledge Center	Acessar o site Suporte da Citrix para pesquisar artigos da base de dados de conhecimento.
Logs	Acessar e analisar detalhes dos arquivos de log de depuração, auditoria do administrador e auditoria do usuário.
Informações de cluster	Para o XenMobile Server local. Acessar informações sobre cada um dos nós em um ambiente clusterizado.
Coleta de lixo	Para o XenMobile Server local. Acessar informações sobre objetos de memória que não são mais usados.
Propriedades de memória Java	Para o XenMobile Server local. Acessar um instantâneo do uso da memória, dos detalhes da memória e dos detalhes do pool de memória Java.
Macros	Preencher os dados de propriedade do usuário ou do dispositivo no campo de texto de um perfil, uma política, uma notificação ou um modelo de registro. Configure uma única política, implante-a em uma grande base de usuários e faça com que os valores específicos do usuário sejam exibidos para cada usuário de destino.

Configuração de PKI	Importar e exportar informações de configuração de PKI.
Utilitário de assinatura APNS	Enviar uma solicitação de certificados de assinatura de Apple Push Network (APNs) ou carregar um certificado de APNs do Secure Mail para o iOS.
Citrix Insight Services	Carregar logs para o Citrix Insight Services (CIS) para obter assistência com vários problemas.
Status do dispositivo com o conector Citrix Gateway para Exchange ActiveSync	Consulte o XenMobile para saber o status de um dispositivo conforme enviado ao conector Citrix Gateway para Exchange ActiveSync com base no ID do ActiveSync do dispositivo.
Anonimização e desanonimização	Para o XenMobile Server local. Quando você cria pacotes de suporte no XenMobile, dados confidenciais do usuário, do servidor e da rede são anonimizados por padrão. Você pode alterar esse comportamento em Suporte > Anonimização e desanonimização em Avançado .
Configurações de log	Personalize o nível de log ou adicione um agente de log personalizado.

Restringir Acesso de Grupo

Os usuários administradores podem aplicar permissões a todos os grupos de usuários.

Função de provisionamento de dispositivos

Importante:

A Função de Provisionamento do Dispositivo se aplica somente aos dispositivos Windows CE.

Os usuários com a função de Provisionamento de Dispositivos predefinida têm acesso limitado aos recursos do console. Por padrão, sua permissão é definida para todos os grupos de usuários e eles não podem alterar essa configuração.

Recursos do console

Os usuários de provisionamento de dispositivo têm o acesso restrito a seguir no console XenMobile. Por padrão, cada um dos recursos a seguir está ativado.

Dispositivos

Editar dispositivo	Alterar as configurações do dispositivo.
Adicionar/excluir dispositivo	Adicionar ou remover dispositivos no XenMobile.

Configurações

Os usuários de provisionamento do dispositivo podem acessar a página **Configurações**, mas não têm os direitos para configurar os recursos.

Função de suporte

Os usuários com a função Suporte têm acesso ao suporte remoto. Suas permissões se aplicam a todos os usuários por padrão, e eles não podem editar essa configuração.

Função de Usuário

Os usuários com a função de Usuário têm o acesso limitado a seguir ao XenMobile.

Acesso autorizado

Portal de Autoajuda	Os usuários têm acesso somente ao Portal de Autoajuda no XenMobile.
---------------------	---

Recursos do console

Os usuários têm o acesso restrito a seguir no console XenMobile.

Dispositivos

Apagamento completo do dispositivo	Apagar todos os dados e aplicativos de um dispositivo, incluindo cartões de memória, caso o dispositivo os tenha.
Apagamento seletivo do dispositivo	Apagar todos os dados e aplicativos corporativos de um dispositivo, deixando dados pessoais e aplicativos no local.
Exibir localizações	Ver a localização de e definir as restrições geográficas em um dispositivo. Incluído: Localizar dispositivo, ver a localização de um dispositivo, rastrear dispositivo, rastrear a localização de um dispositivo ao longo do tempo
Bloquear dispositivo	Bloquear remotamente um dispositivo para que ele não possa ser usado.
Desbloquear dispositivo	Desbloquear remotamente um dispositivo para que ele não possa ser usado.
Bloquear contêiner	Bloquear remotamente o contêiner corporativo em um dispositivo.
Desbloquear contêiner	Desbloquear remotamente o contêiner corporativo em um dispositivo.
Redefinir senha do contêiner	Redefinir a senha do contêiner corporativo.
Ativar desvio de bloqueio de ativação DEP ASM	Armazene um código de desvio em um dispositivo iOS supervisionado, quando o bloqueio de ativação estiver ativado. Se você precisar apagar o dispositivo, use esse código para limpar o bloqueio de ativação automaticamente.
Chama o dispositivo	Chamar remotamente um dispositivo Windows no volume mais alto durante cinco minutos.
Reinicializar o dispositivo	Reinicie um dispositivo Windows.
Exibir inventário de software	Ver quais softwares estão instalados em um dispositivo.

Registro

Adicionar/excluir registro	Adicionar ou remover um convite para registro de um usuário ou um grupo de usuários.
Notificar usuário	Enviar um convite para registro para um usuário ou um grupo de usuários.

Restringir Acesso de Grupo

Para todas as quatro funções padrão, essa permissão é definido como padrão e pode ser aplicada a todos os grupos de usuários. Você não pode editar a função.

Configurar funções com RBAC

O recurso Controle de Acesso Baseado em Função (RBAC) no XenMobile permite que você atribua funções predefinidas ou conjuntos de permissões a usuários e grupos. Essas permissões controlam o nível de acesso que os usuários têm às funções do sistema.

O XenMobile implementa quatro funções de usuário padrão para separar logicamente o acesso às funções do sistema:

- **Administrador:** Concede acesso total ao sistema.
- **Provisionamento de dispositivos:** Concede acesso à administração básica de dispositivos para dispositivos Windows CE.
- **Suporte:** Concede acesso ao suporte remoto.
- **Usuário:** Usado pelos usuários que podem registrar dispositivos e acessar o Portal de Autoajuda.

Você também pode usar as funções padrão como modelos que você personaliza para criar funções de usuário. Você pode atribuir as permissões de funções para acessar funções específicas do sistema além das funções definidas pelas funções padrão.

As funções podem ser atribuídas a usuários locais (no nível de usuário) ou a grupos do Active Directory (todos os usuários nesse grupo têm as mesmas permissões). Se um usuário pertencer a vários grupos do Active Directory, todas as permissões serão mescladas para definir as permissões desse usuário. Por exemplo, suponha que os usuários do ADGroupA possam localizar dispositivos gerenciadores e que os usuários do ADGroupB possam apagar dispositivos de funcionários. Nesse caso, um usuário que pertença a ambos os grupos pode localizar e apagar dispositivos de gerentes e funcionários.

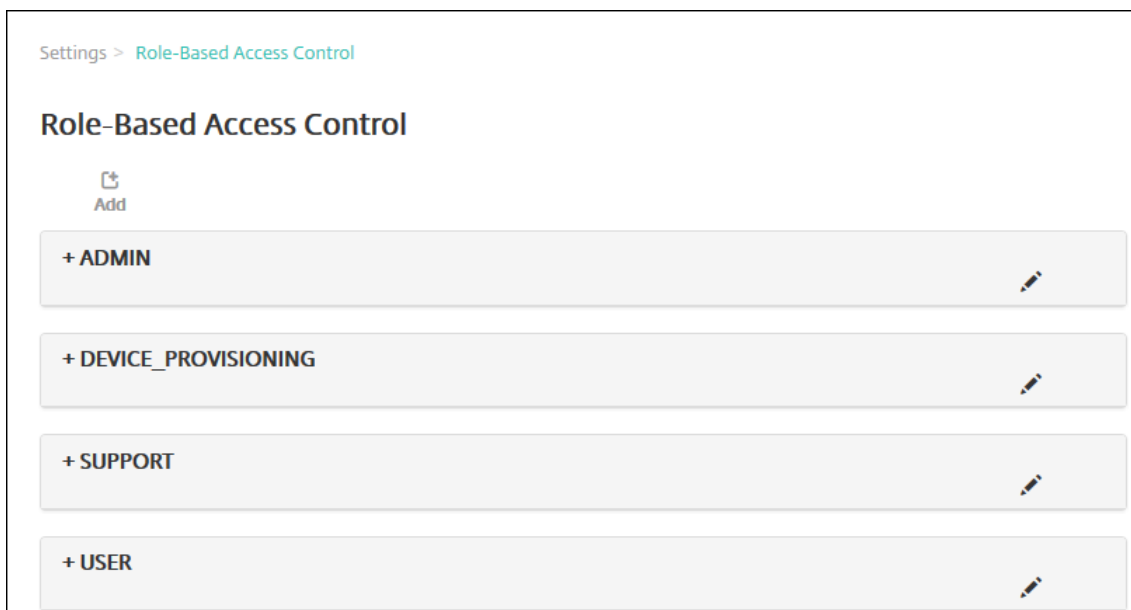
Nota:

Os usuários locais podem ter somente uma função atribuída a eles.

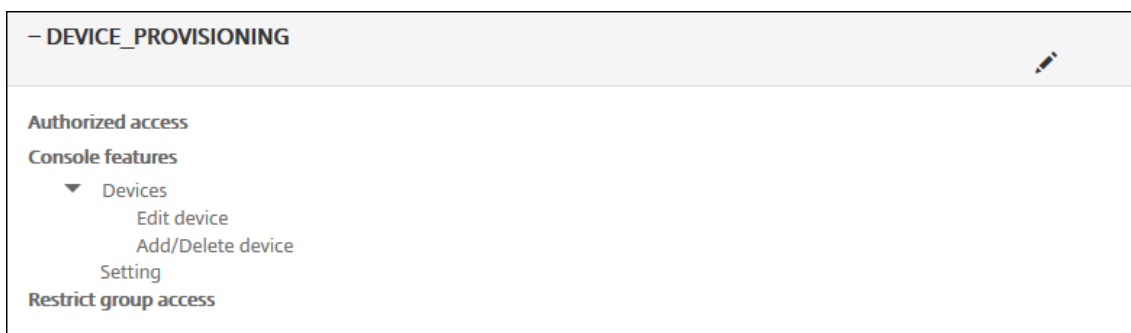
Você pode usar o recurso RBAC no XenMobile para fazer o seguinte:

- Crie uma função.
- Adicionar grupos a uma função.
- Associar os usuários locais a funções.

1. No console XenMobile, vá para **Configurações > Controle de acesso baseado em função**. A página **Controle de acesso baseado em função** é exibida, mostrando as quatro funções de usuário padrão e as funções adicionadas anteriormente.



Se você clicar no sinal de mais (+) ao lado de uma função, a função se expande para mostrar todas as permissões dessa função, conforme mostrado na figura a seguir.



2. Clique em **Adicionar** para adicionar uma nova função de usuário. Para editar a função, clique no ícone de caneta à direita de uma função existente. Para excluir a função, clique no ícone de lixeira à direita de uma função. Você não pode excluir as funções do usuário padrão.

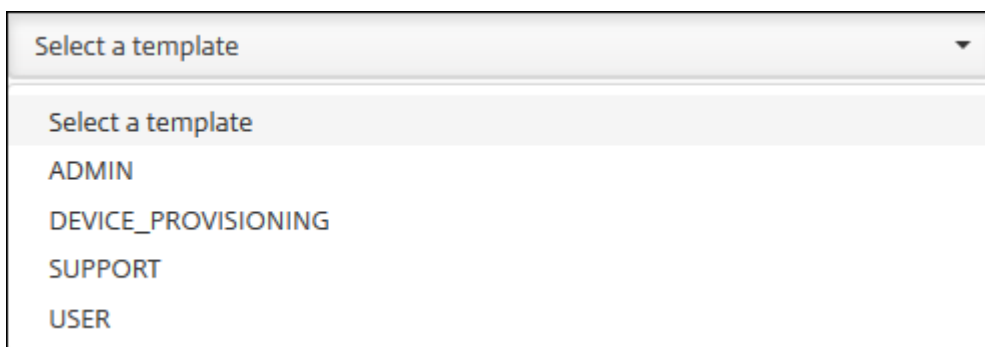
- Quando você clica em **Adicionar** ou no ícone de caneta, a página **Adicionar função** ou **Editar função** é exibida.
- Quando você clica no ícone de lixeira, uma caixa de diálogo de confirmação é exibida.

Clique em **Excluir** para remover a função selecionada.

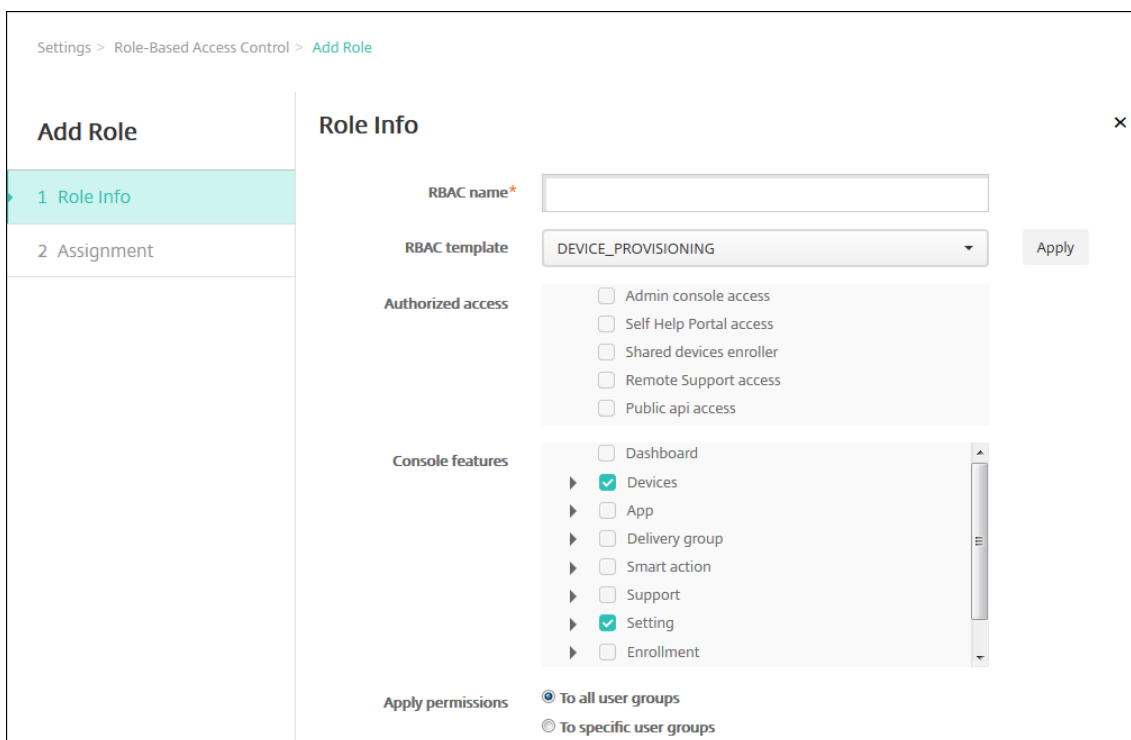
3. Insira as seguintes informações para criar ou editar uma função de usuário:

- **Nome RBAC:** digite um nome descritivo para a nova função do usuário. Você não pode alterar o nome de uma função existente.
- **Modelo RBAC:** opcionalmente, clique em um modelo como o ponto de partida para a nova função. Você não poderá selecionar um modelo se estiver editando uma função existente.

Os modelos RBAC são as funções do usuário padrão. Eles definem o acesso às funções do sistema que usuários associados a essa função têm. Depois de selecionar um modelo RBAC, você poderá ver todas as permissões associadas a essa função nos campos **Acesso autorizado** e **Recursos do console**. O uso de um modelo é opcional. Você pode selecionar diretamente as opções que deseja atribuir a uma função nos campos **Acesso autorizado** e **Recursos do console**.

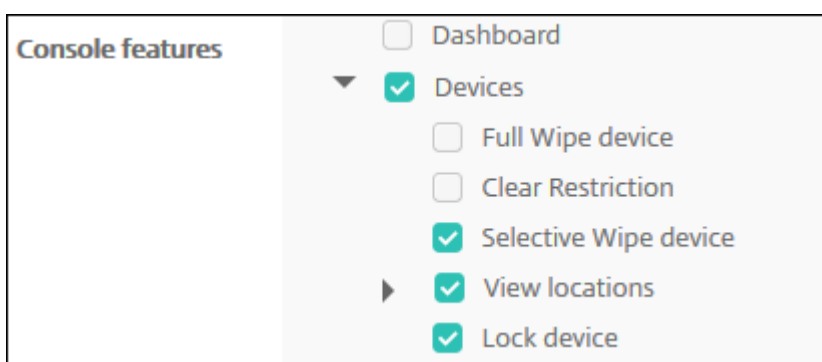


4. Clique em **Aplicar** ao lado do campo **Modelo RBAC** selecionado para preencher **Acesso autorizado** e **Recursos do console** com as permissões predefinidas de acesso e recursos.



5. Marque e desmarque as caixas de seleção em **Acesso autorizado** e **Recursos do console** para personalizar a função.

Se você clicar no triângulo ao lado de um recurso do Console, as permissões específicas desse recurso, que você pode selecionar e limpar, serão exibidas. Clicar na caixa de seleção de nível superior proíbe o acesso a essa área do console. Selecione opções individuais abaixo do nível superior para ativar essas opções. Por exemplo, na figura a seguir, as opções **Apagamento completo do dispositivo** e **Limpar restrições** não aparecem para usuários atribuídos à função. As opções marcadas aparecem.

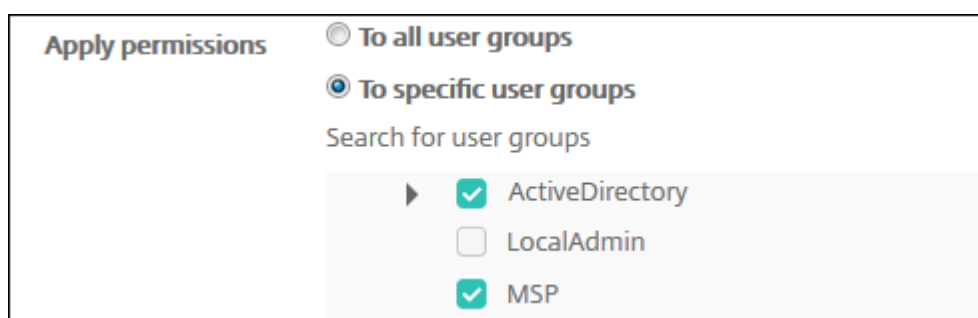


6. **Aplicar permissões:** selecione um ou mais grupos de usuários para limitar quais grupos o administrador pode gerenciar. Se você clicar em **Para grupos de usuários específicos**, será exibida uma lista de grupos a partir da qual você pode selecionar um ou mais grupos.

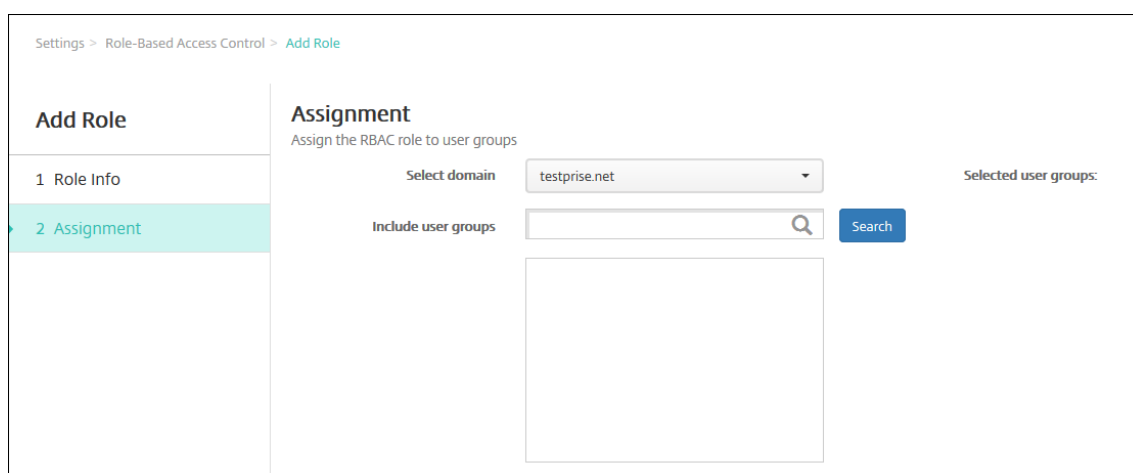
Por exemplo, se um administrador RBAC tiver permissões para os grupos de usuários ActiveDi-

rectory e MSP:

- O administrador pode acessar informações somente para usuários que estejam no grupo ActiveDirectory, no grupo MSP ou em ambos os grupos.
- O administrador não pode exibir nenhum outro usuário local ou AD. O administrador pode exibir usuários que são membros de grupos filhos de qualquer um desses grupos.
- O administrador pode enviar convites para:
 - os grupos de permissão e seus grupos filhos
 - os usuários que são membros de grupos de permissões e seus grupos filhos

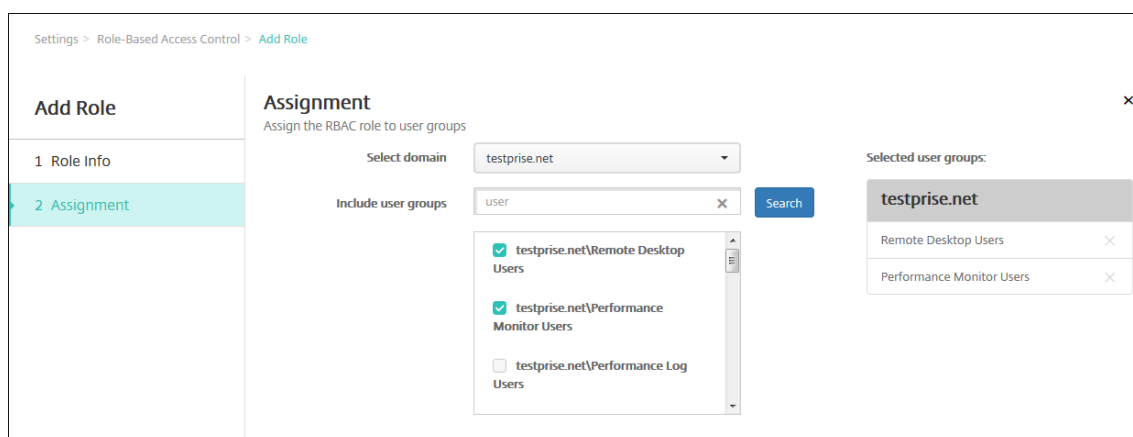


7. Clique em **Next**. A página **Atribuições** é exibida.



8. Insira as informações a seguir para atribuir uma função a grupos de usuários.

- **Selecionar domínio:** na lista, clique em um domínio.
- **Incluir grupos de usuários:** clique em Pesquisar para ver uma lista de todos os grupos disponíveis ou digite um nome de grupo completo ou parcial para limitar a lista a somente grupos com esse nome.
- Na lista exibida, selecione os grupos de usuários aos quais você deseja atribuir a função. Quando você seleciona um grupo de usuários, o grupo aparece na lista **Grupos de usuários selecionados**.



Nota:

Para remover um grupo de usuários da lista **Grupos de usuários selecionados**, clique no X ao lado do nome do grupo de usuários.

9. Clique em **Save**.

Notificações

December 22, 2020

Você pode usar as notificações no XenMobile para os seguintes fins:

- Para se comunicar com grupos selecionados de usuários para uma série de funções relacionadas ao sistema. Você também pode direcionar essas notificações para determinados usuários. Por exemplo, todos os usuários com dispositivos iOS, usuários cujos dispositivos estão fora de conformidade, usuários com dispositivos de propriedade de funcionários etc.
- Para registrar os usuários e os dispositivos deles.
- Para notificar automaticamente os usuários (usando ações automatizadas) quando determinadas condições são atendidas. Por exemplo:
 - Quando o dispositivo de um usuário está prestes a ser bloqueado no domínio corporativo devido a um problema de conformidade.
 - Quando um dispositivo sofreu jailbreak ou root.

Para obter detalhes sobre as ações automatizadas, consulte [Ações automatizadas](#).

Para enviar notificações usando o XenMobile, você deve configurar um gateway e um servidor de notificação. Você pode configurar um servidor de notificação no XenMobile para configurar os servidores de gateway de Protocolo SMTP e SMS para enviar notificações de email e mensagem de texto (SMS) aos usuários. Você pode usar as notificações para enviar mensagens por dois canais diferentes: SMTP ou SMS.

- SMTP é um protocolo orientado para conexão e baseado em texto no qual um remetente de email se comunica com um destinatário de email mediante a emissão de cadeias de caracteres de comando e o fornecimento dos dados necessários, geralmente sobre uma conexão de Protocolo TCP. As sessões SMTP consistem em comandos originados de um cliente SMTP (a pessoa que envia a mensagem) e respostas correspondentes do servidor SMTP.
- SMS é um componente do serviço de mensagem de texto de sistemas de comunicação de telefone, Web ou celular. O SMS usa protocolos padronizados de comunicação para possibilitar que dispositivos de telefone fixo ou celular troquem mensagens de texto breves.

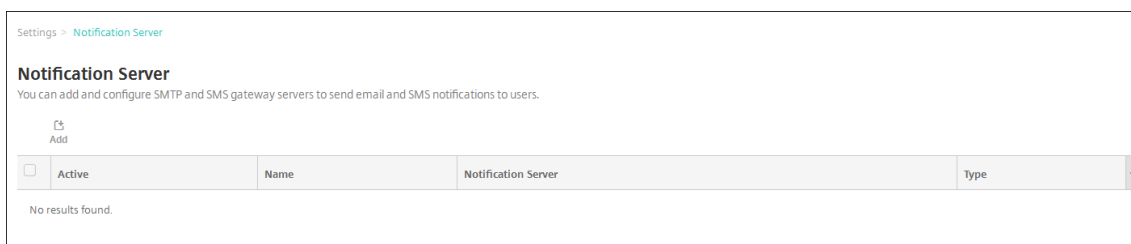
Você também pode instalar um Gateway de SMS de operadora no XenMobile para configurar notificações que são enviadas por meio de um gateway de SMS de uma operadora. As operadoras usam gateways de SMS para enviar ou receber transmissões SMS para ou de uma rede de telecomunicações. Essas mensagens baseadas em texto usam protocolos padronizados de comunicação para permitir que dispositivos de telefone fixo ou celular troquem mensagens de texto breves.

Pré-requisitos

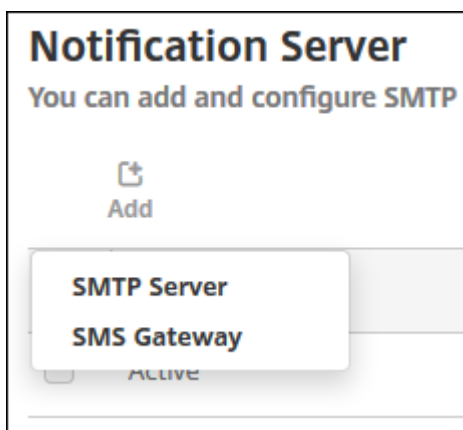
- Antes de configurar o gateway de SMS, consulte o administrador do sistema para determinar as informações do servidor. É importante saber se o servidor SMS está hospedado em um servidor corporativo interno ou se ele faz parte de um serviço de email hospedado. Nesse caso, você precisa de informações do site do provedor de serviços.
- Configure as notificações do servidor SMTP para enviar mensagens aos usuários. Se o servidor estiver hospedado em um servidor interno, entre em contato com o administrador do sistema para obter as informações de configuração. Se o servidor for um serviço de email hospedado, localize as informações de configuração adequadas no site do provedor de serviços.
- Você pode usar um servidor SMTP ativo e um servidor SMS ativo simultaneamente. Ambos os canais de comunicação permitem uma configuração ativa.
- Abra a porta 25 do XenMobile localizado no DMZ da sua rede para apontar de volta para o servidor SMTP na sua rede interna. Isso permite que o XenMobile envie notificações com êxito.

Configurar um servidor SMTP e um gateway de SMS

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Settings** é exibida.
2. Em **Notificações**, clique em **Servidor de notificação**. A página **Servidor de notificação** é exibida.



3. Clique em **Adicionar**. Um menu aparece com opções para configurar um servidor SMTP ou um gateway SMS.



- Para adicionar um servidor SMTP, clique em **Servidor SMTP** e, em seguida, consulte [Para adicionar um servidor SMTP](#) para ver as etapas para definir essa configuração.
- Para um gateway de SMS, clique em **Gateway de SMS** e consulte [Para adicionar um gateway de SMS](#) para ver as etapas para definir essa configuração.

Adicionar um servidor SMTP

Settings > Notification Server > Add SMTP Server

Add SMTP Server

You need to configure the SMTP notifications server to send messages to users. If the SMTP server is hosted on an internal server, you get the server information from your IT department. If the server is a hosted email service, you can find information from the service provider's website. Only one SMTP server is activated at one time.

Name*

Description

SMTP Server*

Secure channel protocol

SMTP server port*

Authentication

Microsoft Secure Password Authentication (SPA)

From name*

From email*

▶ **Advanced Settings**

1. Defina estas configurações:

- **Nome:** digite o nome associado a essa conta do servidor SMTP.
- **Descrição:** opcionalmente, insira uma descrição do servidor.
- **Servidor SMTP:** digite o nome de host do servidor. O nome de host pode ser um nome de domínio totalmente qualificado (FQDN) ou um endereço IP.
- **Protocolo de canal seguro:** na lista, clique em **SSL**, **TLS** ou **Nenhum** para obter o protocolo de canal seguro usado pelo servidor (se o servidor estiver configurado para usar a autenticação segura). O padrão é **Nenhum**.
- **Porta do servidor SMTP:** digite a porta usada pelo servidor SMTP. Por padrão, a porta é definida como 25; se as conexões SMTP usarem o protocolo canal seguro SSL, a porta será

definida como 465.

- **Autenticação:** selecione **I** ou **O**. O padrão é **O**.
 - Se você ativar a **Autenticação**, defina estas configurações:
 - **Nome de usuário:** digite o nome do usuário para autenticação
 - **Senha:** insira a senha do usuário de autenticação.
 - **Autenticação de senha segura (SPA) da Microsoft:** se o servidor SMTP estiver usando o SPA, clique em **I**. O padrão é **O**.
 - **Nome do remetente:** digite o nome exibido na caixa **De** quando um cliente recebe um email de notificação desse servidor. Por exemplo, TI corporativa.
 - **Email do remetente:** digite o endereço de email usado se um destinatário de email responder à notificação enviada pelo servidor SMTP.
2. Clique em **Testar configuração** para enviar uma notificação de email de teste.
 3. Expanda **Configurações avançadas** e defina estas configurações:
 - **Número de novas tentativas de SMTP:** digite o número de novas tentativas para uma mensagem com falha enviada do servidor SMTP. O padrão é 5.
 - **Tempo limite de SMTP:** digite o tempo (em segundos) para aguardar ao enviar uma solicitação SMTP. Aumente esse valor se o envio de mensagens estiver falhando continuamente devido a tempos de espera. Tenha cuidado ao diminuir o valor; ele pode aumentar o número de mensagens não entregues e que atingem o tempo de espera. O padrão é 30 segundos.
 - **Número máximo de destinatários de SMTP:** digite o número máximo de destinatários por mensagem de email enviada pelo servidor SMTP. O padrão é 100.
 4. Clique em **Adicionar**.

Adicionar um gateway SMS

Settings > Notification Server > Add SMS Gateway

Add SMS Gateway

Please consult with your IT department about the server info if the SMS server is hosted on internal corporate server; if this is a hosted email service, the info is available from the service provider's website. Only one SMS server is activated at one time.

Name*

Description

Key*

Secret*

Virtual phone number*

HTTPS OFF

Country code

Use Carrier Gateway ON

Nota:

O XenMobile é compatível somente com mensagens SMS Nexmo. Se você ainda não tiver uma conta para usar as mensagens Nexmo, visite o [site](#) para criar uma.

1. Faça as seguintes configurações:

- **Nome:** digite um nome para a configuração de Gateway de SMS. Este campo é obrigatório.
- **Descrição:** opcionalmente, digite uma descrição da configuração.
- **Chave:** digite o identificador numérico fornecido pelo administrador do sistema ao ativar a conta. Este campo é obrigatório.
- **Segredo:** digite um segredo fornecido pelo administrador do sistema que é usado para acessar sua conta caso uma senha seja perdida ou roubada. Este campo é obrigatório.
- **Número de telefone virtual:** esse campo é usado durante o envio para números de telefone da América do Norte (com o prefixo +1). Você deve digitar um número de telefone virtual Nexmo e você deve usar apenas dígitos neste campo. Você pode comprar números de telefone virtual no site do Nexmo.

- **HTTPS:** selecione se HTTPS deve ser usado para transmitir solicitações SMS para o Nexmo. O padrão é **O**.

Importante:

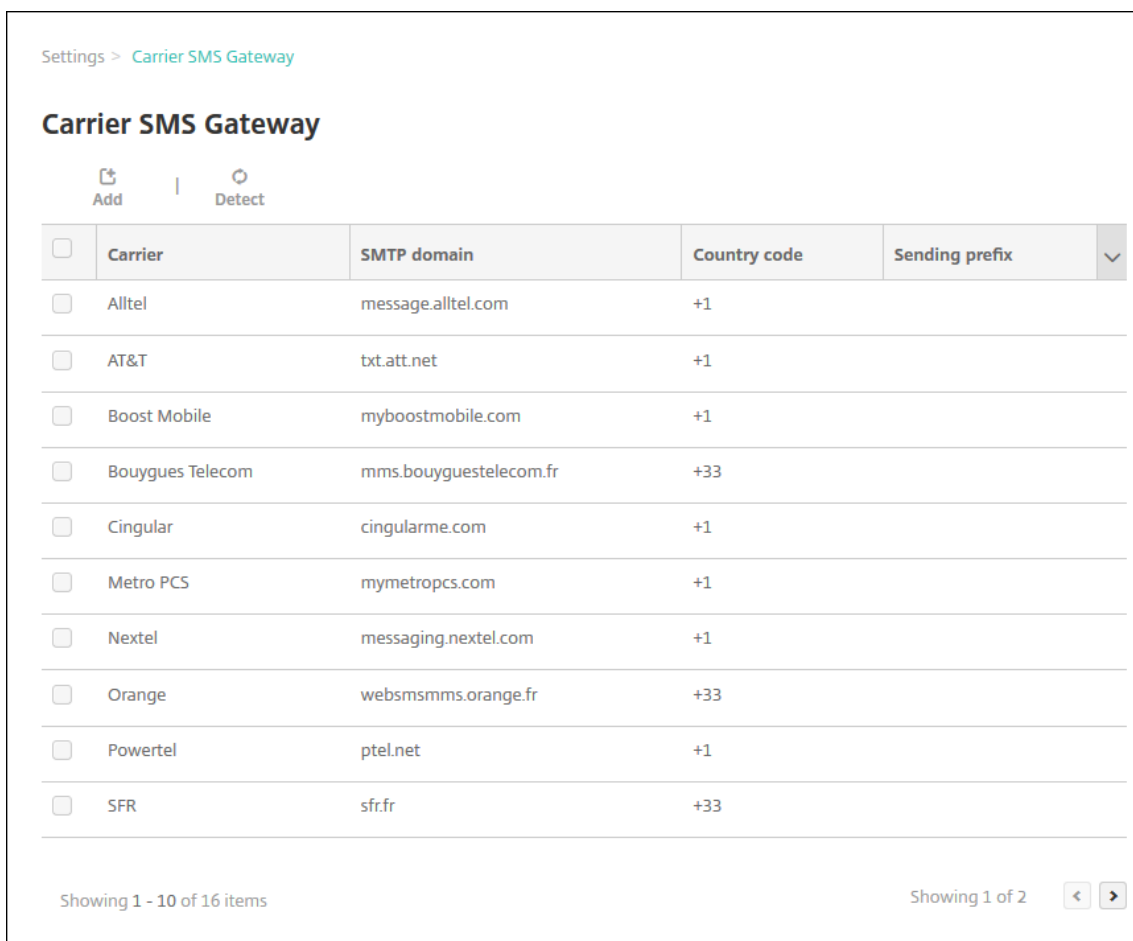
Mantenha o HTTPS definido como **I**, a menos que você receba instruções do Suporte Citrix para mantê-lo como **O**.

- **Código do país:** na lista, clique no prefixo padrão do código de país do SMS para os destinatários na sua organização. Esse campo sempre começa com o símbolo +. O padrão é **Afganistão +93**.
2. Clique em **Testar configuração** para enviar uma mensagem de teste usando a configuração atual. Erros de conexão, como erros de autenticação ou número de telefone virtual, são detectados e exibidos imediatamente. As mensagens são recebidas no mesmo período de tempo que as mensagens enviadas entre celulares.
 3. Clique em **Adicionar**.

Adicionar um gateway SMS de operadora

Você pode configurar um Gateway de SMS da Operadora no XenMobile para configurar notificações enviadas usando um gateway de SMS da operadora. As operadoras usam gateways de SMS para enviar ou receber transmissões SMS para ou de uma rede de telecomunicações. Essas mensagens baseadas em texto usam protocolos padronizados de comunicação para permitir que dispositivos de telefone fixo ou celular troquem mensagens de texto breves.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Settings** é exibida.
2. Em **Notificações**, clique em **Gateway de SMS da operadora**. A página **Gateway de SMS da operadora** é exibida.



3. Você pode optar por um dos seguintes procedimentos:

- Clique em **Detectar** para detectar automaticamente um gateway. Uma caixa de diálogo é exibida para indicar que não há novas operadoras detectadas ou para listar as novas operadoras detectadas entre os dispositivos registrados.
- Clique em **Adicionar**. A caixa de diálogo **Adicionar um Gateway de SMS de operadora** é exibida.

Add a Carrier SMS Gateway ✕

Converts email messages passing through the gateway to a pre-defined format, such as an instant message.

Carrier*

Gateway SMTP domain*

Country code*

Email sending prefix

Nota:

O XenMobile é compatível somente com mensagens SMS Nexmo. Se você ainda não tiver uma conta para usar as mensagens Nexmo, visite o [site](#) para criar uma.

4. Defina estas configurações:
 - **Operadora:** digite o nome da operadora.
 - **Domínio SMTP de gateway:** Digite o domínio associado ao gateway de SMTP.
 - **Código do país:** na lista, clique no código do país da operadora.
 - **Prefixo de envio de email:** opcionalmente, especifique um prefixo de envio de email.
5. Clique em **Adicionar** para adicionar a nova operadora ou em **Cancelar** para não adicionar.

Criar e atualizar modelos de notificação

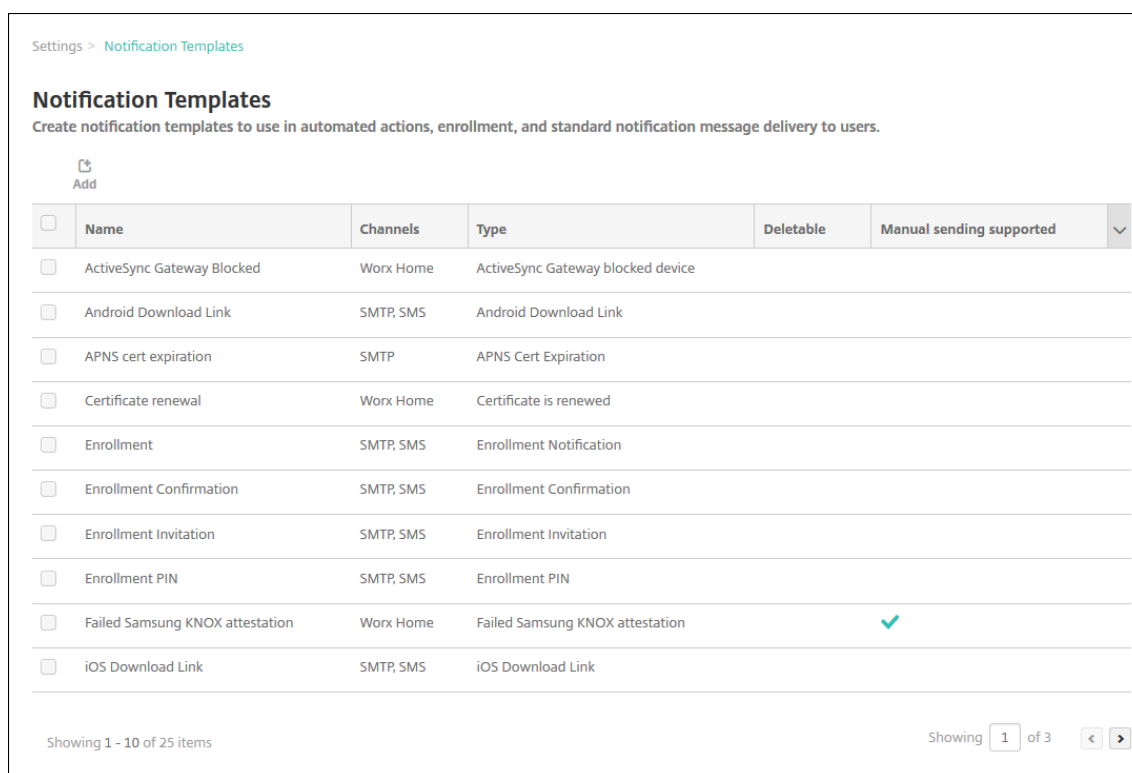
Você pode criar ou atualizar modelos de notificação no XenMobile para que sejam usados em ações automatizadas, registros e mensagens de notificação padrão enviadas para os usuários. Configure os

modelos de notificação para enviar mensagens por três canais diferentes: Secure Hub, SMTP ou SMS. O XenMobile inclui vários modelos de notificação predefinidos que refletem os tipos diferentes de eventos aos quais o XenMobile responde automaticamente para cada dispositivo no sistema.

Nota:

Se planeja usar canais SMTP ou SMS para enviar notificações aos usuários, você deverá configurar os canais antes que possa ativá-los. O XenMobile solicita que você configure os canais ao adicionar modelos de notificação, se eles já não estiverem configurados.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Settings** é exibida.
2. Clique em **Modelos de notificação**. A página **Modelos de notificação** é exibida.



Adicionar modelo de notificação

1. Clique em **Adicionar**. Se nenhum gateway de SMS ou servidor SMTP tiver sido configurado, uma mensagem será exibida em relação ao uso de notificações SMS e SMTP. Você pode optar por configurar o servidor SMTP ou o gateway de SMS agora ou mais tarde.

Se você optar por definir as configurações do servidor SMTP ou SMS agora, será redirecionado para a página **Servidor de notificação** na página **Configurações**. Depois de configurar os

canais que desejar usar, você poderá retornar para a página **Modelo de notificação** para continuar adicionando ou modificando modelos de notificação.

Importante:

Se você optar por definir as configurações do servidor SMTP ou SMS mais tarde, não conseguirá ativar esses canais ao adicionar ou editar um modelo de notificação, o que significa que esses canais não estarão disponíveis para o envio de notificações ao usuário.

2. Defina estas configurações:

- **Nome:** Digite um nome descritivo para o modelo.
- **Descrição:** Digite uma descrição para o modelo.
- **Tipo:** Na lista, clique no tipo de notificação. São exibidos somente os canais para o tipo selecionado. Somente um modelo de tipo de Expiração de certificado APNS é permitido, o que é um modelo predefinido. Isso significa que você não pode adicionar um novo modelo desse tipo.

Nota:

Para alguns tipos de modelo, a frase “Suporte para envio manual” é exibida abaixo do tipo. Isso significa que o modelo está disponível na lista **Notificações** no **Painel** e na página **Dispositivos** para permitir que você envie manualmente a notificação aos usuários. O envio manual não está disponível em nenhum modelo que usa as seguintes macros no campo Assunto ou Mensagem em qualquer canal:

- `{outofcompliance.reason(whitelist_blacklist_apps_name)}`

Nota:

O console XenMobile Server inclui os termos “lista negra” e “lista branca”. Estamos alterando esses termos em uma próxima versão para “lista de bloqueio” e “lista de permissão”.

- `{outofcompliance.reason(smg_block)}`

3. Em **Canais**, configure as informações de cada canal a ser usado com essa notificação. Você pode escolher qualquer um ou todos os canais. Os canais que você escolher dependem de como você desejar enviar as notificações:

- Se você escolher **Secure Hub**, somente os dispositivos Android e iOS receberão as notificações, que serão exibidas na bandeja de notificações do dispositivo.
- Se você escolher **SMTP**, a maioria dos usuários deverá receber a mensagem, pois eles se registraram com os respectivos endereços de email.
- Se você escolher **SMS**, somente os usuários que usam dispositivos com um cartão SIM receberão a notificação.

Secure Hub:

- **Ativar:** clique para ativar o canal de notificação.
- **Mensagem:** digite a mensagem a ser enviada ao usuário. Esse campo será obrigatório se você estiver usando o Secure Hub. Para obter informações sobre como usar macros em uma mensagem, consulte [Macros](#).
- **Arquivo de Som:** na lista, clique no som de notificação que o usuário ouvirá quando a notificação for recebida.

SMTP:

- **Ativar:** clique para ativar o canal de notificação.
Você pode ativar a notificação SMTP somente depois de configurar o servidor SMTP.
- **Remetente:** digite um remetente opcional para a notificação, que pode ser um nome, um endereço de email ou ambos.
- **Destinatário:** esse campo contém uma macro pré-integrada para todas as notificações, exceto Ad-Hoc, para garantir que elas sejam enviadas para o endereço correto do destinatário de SMTP. A Citrix recomenda que você não modifique as macros em modelos. Você também pode acrescentar destinatários (por exemplo, o administrador corporativo), além do usuário mediante a adição dos respectivos endereços separados por um ponto e vírgula (;). Para enviar notificações Ad Hoc, você pode inserir destinatários específicos nessa página ou selecionar dispositivos na página **Gerenciar > Dispositivos** e enviar as notificações de lá. Para obter detalhes, consulte [Dispositivos](#).
- **Assunto:** Digite um assunto descritivo para a notificação. Este campo é obrigatório.
- **Mensagem:** digite a mensagem a ser enviada ao usuário. Para obter informações sobre como usar macros em uma mensagem, consulte [Macros](#).

SMS:

- **Ativar:** clique para ativar o canal de notificação.
Você pode ativar a notificação SMTP somente depois de configurar o servidor SMTP.
- **Destinatário:** esse campo contém uma macro pré-integrada para todas as notificações, exceto Ad-Hoc, para garantir que elas sejam enviadas para o endereço correto do destinatário de SMS. A Citrix recomenda que você não modifique as macros em modelos. Para enviar notificações Ad Hoc, você pode inserir destinatários específicos ou selecionar dispositivos na página **Gerenciar > Dispositivos**.
- **Mensagem:** digite a mensagem a ser enviada ao usuário. Este campo é obrigatório. Para obter informações sobre como usar macros em uma mensagem, consulte [Macros](#).

4. Clique em **Adicionar**. Quando todos os canais estiverem corretamente configurados, eles serão exibidos nesta ordem na página **Modelos de Notificação**: SMTP, SMS e Secure Hub. Todos os

canais que não estiverem configurados corretamente serão exibidos após os canais configurados corretamente.

Editar um modelo de notificação

1. Selecione um modelo de notificação. É exibida a página de edição específica desse modelo, na qual você pode alterar todos os campos, exceto **Tipo**, bem como ativar ou desativar os canais.
2. Clique em **Salvar**.

Excluir um modelo de notificação

Você pode excluir apenas os modelos de notificação que você adicionou. Você não pode excluir modelos de notificação predefinidos.

1. Selecione um modelo de notificação existente.
2. Clique em **Excluir**. Uma caixa de diálogo de confirmação é exibida.
3. Clique em **Excluir** para excluir o modelo de notificação ou em **Cancelar** para cancelar a exclusão.

Dispositivos

March 5, 2021

O Citrix XenMobile pode provisionar, gerenciar, proteger e fazer inventário de uma ampla variedade de tipos de dispositivos em um único console de gerenciamento.

O banco de dados do servidor XenMobile armazena uma lista de dispositivos móveis. Um único número de série ou International Mobile Station Equipment Identity (IMEI)/Mobile Equipment Identifier (MEID) define exclusivamente cada dispositivo móvel. Para preencher o console XenMobile com seus dispositivos, você pode adicioná-los manualmente ou importar uma lista de dispositivos de um arquivo. Para obter mais informações sobre formatos de arquivo de provisionamento de dispositivo, consulte Formatos de arquivo de provisionamento do dispositivo posteriormente neste artigo.

A página **Dispositivos** no console XenMobile lista cada dispositivo e as seguintes informações:

- **Status:** ícones indicam se o dispositivo tiver jailbreak, for gerenciado, se Active Sync Gateway estiver disponível e o estado de implantação.
- **Modo:** se o modo de dispositivo é MDM, MAM ou ambos.

- Outras informações sobre o dispositivo, como **Nome de usuário**, **Plataforma de dispositivo**, **Versão do sistema operacional**, **Modelo de dispositivo**, **Último acesso** e **Dias de inatividade**. Esses títulos são os padrões mostrados.

Para personalizar a tabela **Dispositivos**, clique na seta para baixo no último cabeçalho. Em seguida, selecione os títulos adicionais que você deseja ver na tabela ou desmarque títulos a serem removidos.

Last access	Inactivity days
	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Status <input checked="" type="checkbox"/> Mode <input checked="" type="checkbox"/> User name Serial number IMEI/MEID ActiveSync ID WiFi MAC address Bluetooth MAC address <input checked="" type="checkbox"/> Device platform <input checked="" type="checkbox"/> Operating system version <input checked="" type="checkbox"/> Device model <input checked="" type="checkbox"/> Last access <input checked="" type="checkbox"/> Inactivity days Shareable Shared status DEP registered

Você pode adicionar dispositivos manualmente, importá-los de um arquivo de provisionamento de dispositivo, editar detalhes do dispositivo, executar ações de segurança e enviar notificações para dispositivos. Você também pode exportar todos os dados da tabela do dispositivo para um arquivo .csv para criar um relatório personalizado. O servidor exporta todos os atributos do dispositivo. Se você aplicar filtros, o XenMobile os usará ao criar o arquivo .csv.

Adicionar um dispositivo manualmente

1. No console XenMobile, clique em **Gerenciar > Dispositivos**. A página **Dispositivos** é exibida.

	Status	Mode	User name	Device platform	Operating system version
<input type="checkbox"/>		MDM MAM	[Redacted]	Android	5.0.2
<input type="checkbox"/>		MDM MAM	[Redacted]	iOS	8.4.1

2. Clique em **Adicionar**. A página **Adicionar dispositivo** é exibida.

Add Device

Select Platform

iOS

Android

Serial Number*

3. Defina estas configurações:

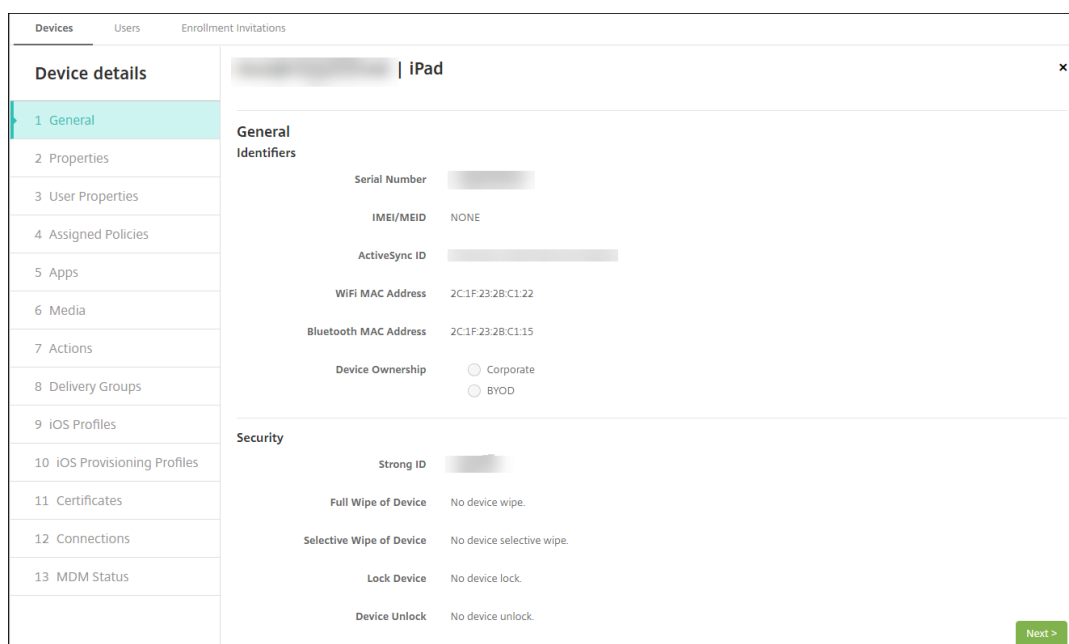
- **Selecionar plataforma:** Clique em **iOS** ou **Android**.
- **Número de série:** digite o número de série do dispositivo.
- **IMEI/MEID:** como opção, somente para dispositivos Android, digite as informações de IMEI/MEID do dispositivo.

4. Clique em **Adicionar**. A tabela **Dispositivos** é exibida com o dispositivo adicionado à parte inferior da lista. Escolha o dispositivo que você adicionou e, no menu exibido, clique em **Editar** para exibir e confirmar os detalhes do dispositivo.

Nota:

Quando você marca a caixa de seleção ao lado de um dispositivo, o menu de opções é exibido acima da lista de dispositivos. Quando você clica em qualquer outro lugar da lista, o menu de opções é exibido no lado direito da listagem.

- XenMobile Server configurado no modo Empresarial (XME) ou MDM
- LDAP configurado
- Se estiver usando grupos locais e usuários locais:
 - Um ou mais grupos locais.
 - Usuários locais atribuídos a grupos locais.
 - Grupos de entrega são associados a grupos locais.
- Se estiver usando o Active Directory:
 - Grupos de entrega são associados a grupos do Active Directory.



5. A página **Geral** lista **identificadores** de dispositivo, como o número de série, ID do ActiveSync e outras informações para o tipo de plataforma. Para **Propriedade do dispositivo**, selecione **Corporativo** ou **BYOD**.

A página **Geral** também lista propriedades de **segurança**, como ID forte, Bloquear dispositivo, Ignorar bloqueio de ativação e outras informações, para o tipo de plataforma. O campo de **apagamento completo do dispositivo** inclui o código PIN do usuário. O usuário deve digitar o código depois que o dispositivo for apagado. Se o usuário esquecer o código, você pode procurá-lo aqui.

6. A página **Propriedades** lista as propriedades de dispositivo que o XenMobile provisionará. Esta lista mostra as propriedades de dispositivo incluídas no arquivo de provisionamento usado para adicionar o dispositivo. Para adicionar uma propriedade, clique em **Adicionar** e, em seguida, selecione uma propriedade na lista. Para obter os valores válidos para cada propriedade, consulte o PDF [Nomes de propriedade do dispositivo e os valores](#).

Quando você adicionar uma propriedade, ela inicialmente aparece na categoria em que você adicionou. Depois de clicar em **Avançar** e voltar para a página **Propriedades**, a propriedade aparece na lista apropriada.

Para excluir uma propriedade, passe o mouse sobre a listagem e clique no **X** à direita. XenMobile exclui o item imediatamente.

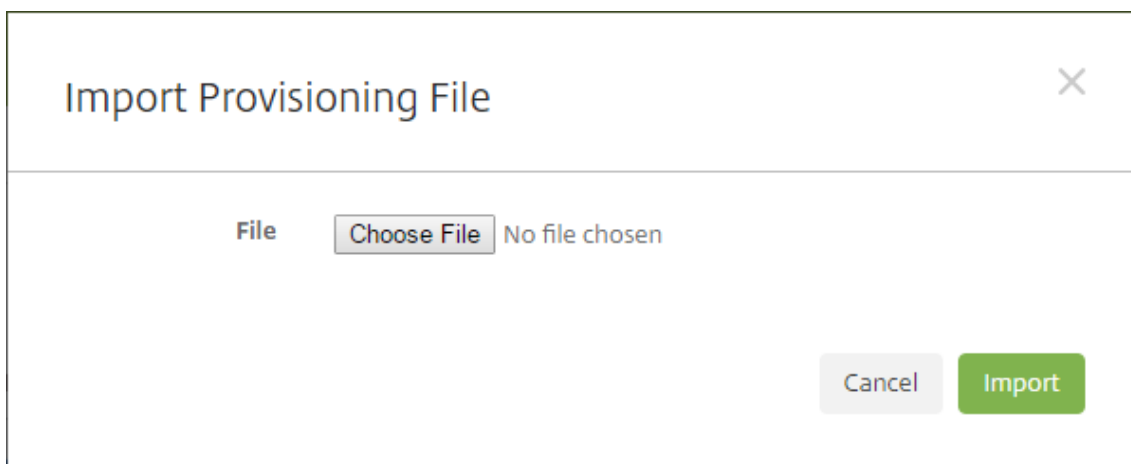
7. As seções restantes de **Detalhes do dispositivo** contêm informações resumidas do dispositivo.
- **Propriedades do usuário:** exibe funções RBAC, associações de grupo, contas de compra por volume e propriedades do usuário. Você pode desativar uma conta de compra por volume nesta página.

- **Políticas atribuídas:** exibe o número de políticas atribuídas, incluindo o número de políticas implantadas, pendentes e com falha. Fornece o nome da política, tipo e últimas informações de implantação de cada política.
- **Aplicativos:** exibe, para o último inventário, o número de implementações de aplicativo instaladas, pendentes e com falha. Fornece o nome do aplicativo, identificador, tipo e outras informações.
- **Mídia:** exibe, para o último inventário, o número de implementações de mídia implantadas, pendentes e com falha.
- **Ações:** exibe o número de ações implantadas, pendentes e com falha. Fornece o nome da ação e a hora da última implantação.
- **Grupos de entrega:** exibe o número de grupos de entrega bem-sucedidos, pendentes e com falha. Para cada implantação fornece o tempo nome e a implantação do grupo de entrega. Selecione um grupo de entrega para exibir informações mais detalhadas, incluindo status, ação e canal ou usuário.
- **Perfis de iOS:** exibe o último inventário de perfil de iOS, incluindo nome, tipo, organização e descrição.
- **Perfis de provisionamento do iOS:** informações de perfil, como o UUID de provisionamento para distribuição empresarial mostra a data de expiração, e se ele é gerenciado.
- **Certificados:** exibe, para certificados válidos, expirados ou revogados, informações como o tipo, provedor, emissor, número de série e o número de dias restantes antes da expiração.
- **Conexões:** exibe o status da primeira conexão e o status da última conexão. Fornece para cada conexão, o nome do usuário, penúltimo (próxima ao último) tempo de autenticação e última vez de autenticação.
- **Status de MDM:** exibe informações como o status do MDM, o último envio por push e a hora da última resposta do dispositivo.

Importar dispositivos de um arquivo de provisionamento

Você pode importar um arquivo fornecido por operadoras móveis ou fabricantes de dispositivos, ou pode criar seus próprios arquivos de provisionamento de dispositivo. Para obter detalhes, consulte Formatos de arquivo de provisionamento do dispositivo mais abaixo.

1. Vá até **Gerenciar > Dispositivos** e clique em **Importar**. A caixa de diálogo **Importar Arquivo de Provisionamento** é exibida.



2. Clique em **Escolher Arquivo** e, em seguida, navegue até o arquivo a ser importado.
3. Clique em **Importar**. A tabela de **Dispositivos** contém o arquivo importado.
4. Para editar as informações do dispositivo, selecione-o e, em seguida, clique em **Editar**. Para obter informações sobre as páginas de **Detalhes do dispositivo**, consulte Adicionar um dispositivo manualmente.

Enviar uma notificação para dispositivos

Você pode enviar notificações para os dispositivos da página Dispositivos. Para obter mais informações sobre as notificações, consulte [Notificações](#).

1. Na página **Gerenciar > Dispositivos**, selecione o dispositivo ou os dispositivos para os quais você deseja enviar uma notificação.
2. Clique em **Notificar**. A caixa de diálogo **Notificação** é exibida. O campo **Destinatários** lista todos os dispositivos que devem receber a notificação.

The screenshot shows a 'Notification' dialog box with a close button (X) in the top right corner. The dialog is divided into several sections:

- Recipients:** A text input field containing 'CMVVXKX06J6A'.
- Templates:** A dropdown menu currently set to 'Ad Hoc'.
- Channels:** Two checkboxes, 'SMTP' and 'SMS', both of which are checked.
- Channel Selection:** Below the channels, there are two tabs: 'SMTP' (which is selected) and 'SMS'.
- Form Fields:** Under the 'SMTP' tab, there are three input fields: 'Sender', 'Subject', and 'Message'. The 'Message' field is a larger text area.
- Buttons:** At the bottom right, there are two buttons: 'Cancel' (disabled) and 'Notify' (active).

3. Defina estas configurações:

- **Modelos:** na lista, clique no tipo de notificação que você deseja enviar. Para cada modelo exceto **Ad Hoc**, os campos **Assunto** e **Mensagem** mostram o texto configurado para o modelo que você escolher.
- **Canais:** selecione como enviar a mensagem. O padrão é **SMTP** e **SMS**. Clique nas guias para ver o formato de mensagem de cada canal.
- **Remetente:** insira um remetente opcional.
- **Assunto:** Insira um assunto para uma mensagem **Ad Hoc**.
- **Mensagem:** insira a mensagem para uma mensagem **Ad Hoc**.

4. Clique em **Notificar**.

Exportar a tabela Dispositivos

1. Filtre a tabela de **Dispositivos** de acordo com o que você deseja exibir no arquivo de exportação.
2. Clique no botão **Exportar** acima da tabela **Dispositivos**. O XenMobile extrai as informações da tabela **Dispositivos** filtrada e converte-as em um arquivo .csv.
3. Quando avisado, abra ou salve o arquivo .csv.

Marcar os dispositivos de usuário manualmente

Você pode marcar manualmente um dispositivo no XenMobile das seguintes maneiras:

- Durante o processo de registro baseado em convite.
- Durante o processo de registro do Portal de Autoajuda.
- Adicionando a propriedade do dispositivo como uma propriedade do dispositivo

Você tem a opção de marcar o dispositivo como de propriedade também da empresa ou do funcionário. Ao usar o Portal de Autoajuda para autorregistrar um dispositivo, você pode marcar o dispositivo como pertencente à empresa ou ao funcionário. Você também pode marcar um dispositivo manualmente, da seguinte maneira.

1. Adicione uma propriedade ao dispositivo da guia **Dispositivos** no console XenMobile.
2. Adicione a propriedade chamada **Propriedade de** e escolha **Empresa** ou **BYOD** (propriedade do funcionário).

Devices	Users	Enrollment Invitations
Device details iPhone		
1 General	Properties	
2 Properties	+ Battery Add	
3 User Properties	+ Location information Add	
4 Assigned Policies	+ Network information Add	
5 Apps	+ Security information Add	
6 Media	+ Storage space Add	
7 Actions	- System information Add	
8 Delivery Groups	Owned by: Corporate (selected) BYOD Done Cancel	
9 iOS Profiles	Active iTunes account: Yes	
10 iOS Provisioning Profiles	Baseband firmware version: 2.16.00	
11 Certificates	Cloud backup enabled: No	
12 Connections	Color: BLACK	
13 MDM Status	DEP account name: DEP	
	DEP profile assigned: 01/08/2017 06:47:15	

Formatos de arquivo de provisionamento do dispositivo

Muitas operadoras móveis ou fabricantes de dispositivos fornecem listas de dispositivos móveis autorizados. Você pode usar essas listas para evitar a necessidade de inserir manualmente uma longa lista de dispositivos móveis. O XenMobile é compatível com um formato de arquivo de importação que é comum a todos os três tipos de dispositivos compatíveis: Android, iOS e Windows.

Um arquivo de provisionamento que você cria manualmente e usa para importar dispositivos para o XenMobile deve estar no seguinte formato:

```
SerialNumber; IMEI; OperatingSystemFamily; propertyName1; propertyValue1; propertyName2;
propertyValue2; ... propertyNameN; propertyValueN
```

Tenha em mente o seguinte:

- Para obter os valores válidos para cada propriedade, consulte o PDF [Nomes de propriedade do dispositivo e os valores](#).
- Use o conjunto de caracteres UTF-8.
- Use um ponto e vírgula (;) para separar os campos no arquivo de provisionamento. Se parte de um campo contiver um ponto e vírgula, ele deverá ser antecedido por um caractere de barra invertida (\).

Por exemplo, para esta propriedade:

```
propertyV;test;1;2
```

Faça da seguinte maneira:

```
propertyV\;test\;1\;2
```

- O número de série é necessário para dispositivos iOS porque ele é o identificador do dispositivo iOS.
- Para outras plataformas de dispositivo, você deve incluir o número de série ou o IMEI.
- Os valores válidos para **OperatingSystemFamily** são **WINDOWS**, **ANDROID** ou **iOS**.

Exemplo de um arquivo de provisionamento do dispositivo:

```
1 `1050BF3F517301081610065510590391;15244201625379901;WINDOWS;propertyName;
   propertyV\;test\;1\;2;prop 2
2 2050BF3F517301081610065510590392;25244201625379902;ANDROID;propertyName;
   propertyV$*&&ééétest
3 3050BF3F517301081610065510590393;35244201625379903;iOS;test;
4 4050BF3F517301081610065510590393;;iOS;test;
5 ;55244201625379903;ANDROID;test.testé;value;`
```

Cada linha no arquivo descreve um dispositivo. A primeira entrada no exemplo acima significa o seguinte:

- SerialNumber: 1050BF3F517301081610065510590391
- IMEI: 15244201625379901
- OperatingSystemFamily: WINDOWS
- PropertyName: propertyN
- PropertyValue: propertyV\;test\;1\;2;prop 2

ActiveSync Gateway

November 30, 2020

O ActiveSync é um protocolo de sincronização de dados móveis desenvolvido pela Microsoft. O ActiveSync sincroniza dados com dispositivos portáteis e computadores desktop (ou laptop).

Você pode configurar as regras do ActiveSync Gateway no XenMobile. Com base nessas regras, você pode permitir ou negar o acesso dos dispositivos a dados do ActiveSync. Por exemplo, se você ativar a regra Aplicativos Obrigatórios Ausentes, o XenMobile verificará a Política de acesso aos aplicativos dos aplicativos obrigatórios e negará o acesso aos dados do ActiveSync se eles estiverem ausentes. Para cada regra, você poderá escolher a **Permitir** ou **Negar**. A configuração padrão é **Permitir**.

Para obter mais informações sobre a política de dispositivo de Acesso aos aplicativos, consulte [Política de dispositivo de acesso aos aplicativos](#).

O XenMobile é compatível com as seguintes regras:

Dispositivos Anônimos: verifica se um dispositivo está no modo anônimo. Essa verificação estará disponível se o XenMobile não conseguir autenticar novamente o usuário quando um dispositivo tentar se reconectar.

Erro de atestado de Samsung KNOX: verifica se um dispositivo falhou em uma consulta do servidor de atestado do Samsung KNOX.

Aplicativos proibidos: verifica se um dispositivo tem aplicativos proibidos, conforme definido em uma política de Acesso aos Aplicativos.

Permissão e negação implícitas: essa ação é o padrão para o ActiveSync Gateway. O gateway cria uma Lista de dispositivos de todos os dispositivos que não atendem a qualquer um dos outros critérios de regra do filtro e permite ou nega conexões com base nessa lista. Se nenhuma regra corresponder, o padrão será Permissão Implícita.

Dispositivos inativos: verifica se um dispositivo está inativo conforme definido pela configuração Limite de Dias de Inatividade do dispositivo em Propriedades do Servidor.

Aplicativos obrigatórios ausentes: verifica se um dispositivo não tem os aplicativos obrigatórios, conforme definido em uma política de Acesso aos aplicativos.

Aplicativos não sugeridos: verifica se um dispositivo tem aplicativos não sugeridos, conforme definido em uma Política de acesso aos aplicativos.

Senha não compatível: verifica se a senha de usuário está em conformidade. Nos dispositivos Android e iOS, o XenMobile pode determinar se a senha no dispositivo no momento está em conformidade com a política de código secreto enviada para o dispositivo. Por exemplo, no iOS, o usuário tem 60 minutos para definir uma senha se o XenMobile enviar uma política de código secreto para o dispositivo. Antes que o usuário defina a senha, o código secreto pode não estar em conformidade.

Dispositivos sem conformidade: verifica se um dispositivo está fora de conformidade, com base na propriedade de dispositivo Sem Conformidade. Essa propriedade normalmente é alterada pelas ações automatizadas ou por um terceiro que aproveita as APIs do XenMobile.

Status revogado: verifica se o certificado do dispositivo foi revogado. Um dispositivo revogado não pode se registrar novamente até que tenha autorização novamente.

Dispositivos Android com root e iOS com jailbreak: verifica se um dispositivo Android ou iOS tem root ou jailbreak.

Dispositivos não gerenciados: verifica se um dispositivo ainda está em um estado gerenciado, sob o controle do XenMobile. Por exemplo, um dispositivo registrado no MAM ou um dispositivo não registrado não é gerenciado.

Enviar usuários de domínio do Android para o ActiveSync Gateway: clique em **SIM** para garantir que o XenMobile envie as informações do dispositivo Android para o ActiveSync Gateway.

Para definir as configurações do ActiveSync Gateway

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida.
2. Em **Servidor**, clique em **ActiveSync Gateway**. A página **ActiveSync Gateway** é exibida.

Settings > ActiveSync Gateway

ActiveSync Gateway

Allows or denies access to devices and users based on rules and properties.

All devices

Activate the following rule(s)

- Anonymous Devices
- Failed Samsung KNOX attestation
- Forbidden Apps
- Implicit Allow and Deny
- Inactive Devices
- Missing Required Apps
- Non-Suggested Apps
- Noncompliant Password
- Out of Compliance Devices
- Revoked Status
- Rooted Android and Jailbroken iOS Devices
- Unmanaged Devices

Android only

Send Android domain users to ActiveSync Gateway YES ?

1. Em **Ativar as regras a seguir**, selecione uma ou mais regras que você deseja ativar.
2. Em **Somente Android**, em **Enviar usuários de domínio do Android para o ActiveSync Gateway**, clique em **SIM** para garantir que o XenMobile envie as informações do dispositivo Android para o ActiveSync Gateway.
3. Clique em **Salvar**.

Migrar do Device Administration para o Android Enterprise

April 23, 2020

Este artigo discute considerações e recomendações para migrar do Android Device Administration legado para o Android Enterprise. O Google descontinuará a API Android Device Administration. Essa API suportava aplicativos empresariais em dispositivos Android. Android Enterprise é a solução de gerenciamento moderna recomendada pela Google e Citrix.

O XenMobile está mudando para o Android Enterprise como o método de registro padrão para dispositivos Android. Depois que o Google substituir as APIs, o registro irá falhar nos dispositivos Android Q no modo Device Administration.

O Android Enterprise inclui suporte aos modos de dispositivo totalmente gerenciado e de perfil de trabalho. A publicação do Google, [Android Enterprise Migration Bluebook](#), explica, em detalhes, as diferenças entre o Device Administration legado e o Android Enterprise. Recomendamos que você leia as informações de migração do Google.

Essa publicação também descreve as quatro fases da migração do Device Administration e inclui o diagrama a seguir. Esse artigo inclui recomendações específicas para as fases de migração ao XenMobile.

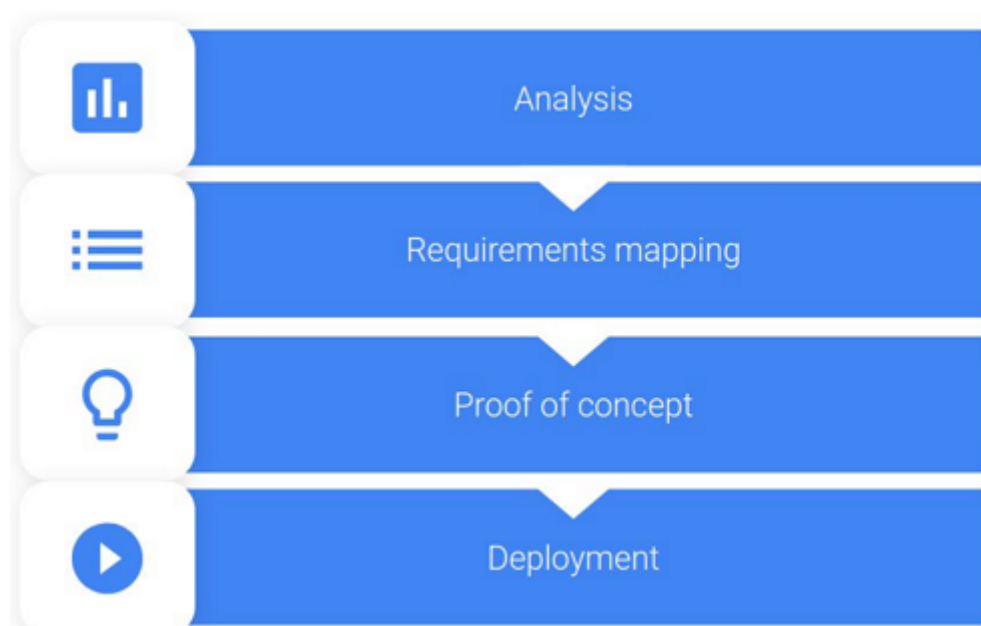


Diagrama do [Android Enterprise Migration Bluebook](#).

Republicado com a permissão do Google.

Impacto da substituição do Device Administration

O Google substituirá as seguintes APIs do Device Administration. Essas APIs não funcionarão em dispositivos que executam o Android Q depois que você atualizar o Secure Hub para direcionar-se ao nível da API do Android Q:

- Desativar câmera: controla o acesso às câmeras do dispositivo.
- Expirar senha: força os usuários a alterarem suas senhas após um período de tempo configurável.
- Limitar senha: define requisitos restritivos de senha.

As APIs obsoletas não têm impacto nos dispositivos registrados no modo Citrix somente MAM.

Recomendações

As recomendações a seguir são para dispositivos já registrados no modo Device Administration do Android legado, dispositivos não registrados e dispositivos registrados no modo Citrix somente MAM.

Status do registro do dispositivo	Ação recomendada
O dispositivo existente está registrado no modo Device Administration e pode ser atualizado para o Android Q.	Antes de atualizar o dispositivo para Android Q, migre do modo Device Administration para o Android Enterprise.
O dispositivo existente está registrado no modo Device Administration. O dispositivo não pode ser atualizado para o Android Q.	O dispositivo pode permanecer no modo Device Administration. No entanto, planeje mudar o dispositivo para o Android Enterprise ao atualizar o dispositivo.
O dispositivo existente está registrado no modo Device Administration e foi atualizado para o Android Q.	Migre do modo Device Administration para o Android Enterprise antes que o Google substitua as APIs. Uma mensagem de aviso para esses dispositivos é exibida no console XenMobile.
Novo dispositivo entregue com Android Q e registrado no modo Device Administration.	Migre do modo Device Administration para o Android Enterprise antes que o Google substitua as APIs. Uma mensagem de aviso para esses dispositivos é exibida no console XenMobile.
Novo dispositivo entregue com Android Q ou atualizável. O dispositivo não está registrado.	Use o Android Enterprise nos dispositivos novos.

Status do registro do dispositivo	Ação recomendada
O dispositivo novo ou existente no Android Q é registrado no modo Device Administration depois que o Google substituir as APIs.	Para evitar o impacto de APIs do Google obsoletas, a Citrix recomenda migrar para o Android Enterprise antes que o Google substitua as APIs. Após essa data, o registro desses dispositivos irá falhar.
Dispositivos novos ou existentes registrados no modo Citrix somente MAM.	Nenhuma ação necessária. As APIs do Google obsoletas não têm impacto nos dispositivos no modo somente MAM.

Analysis

A fase Analysis da migração consiste em:

- Informações da configuração do Android legada
- Documentar a configuração legada para que você possa mapear recursos legados para recursos do Android Enterprise

Análise recomendada

1. Avaliar o Android Enterprise no XenMobile: totalmente gerenciado, totalmente gerenciado com perfil de trabalho, dispositivo dedicado, perfil de trabalho (BYOD).
2. Analise seus recursos atuais do Device Administration em relação ao Android Enterprise.
3. Documente os casos de uso do Device Administration.

Para documentar os casos de uso do Device Administration:

1. Crie uma planilha e liste os grupos de políticas atuais no console XenMobile.
2. Crie casos de uso separados com base nos grupos de políticas existentes.
3. Para cada caso de uso, documente o seguinte:
 - Nome
 - Proprietário da empresa
 - Modelo de identidade do usuário
 - Requisitos de dispositivo
 - Segurança
 - Gerência
 - Usabilidade
 - Inventário de dispositivos

- Marca e modelo
 - Versão de SO
 - Aplicativos
4. Para cada aplicativo, liste:
- Nome do aplicativo
 - Nome do pacote
 - Método de hospedagem
 - Se o aplicativo é público ou privado
 - Se o aplicativo é obrigatório (true/false)

Requirements mapping

Com base na análise concluída, determine os requisitos dos recursos do seu Android Enterprise.

Mapeamento de requisitos recomendado

1. Determine o modo de gerenciamento e o método de registro:
 - Perfil de trabalho (BYOD): requer novo registro. Não é necessário redefinição de fábrica.
 - Totalmente gerenciado: requer redefinição de fábrica. Registre os dispositivos usando código QR, bump NFC (comunicação a curta distância), identificador DPC (controlador de política de dispositivo), registro sem toque.
2. Crie uma estratégia de migração de aplicativos.
3. Mapeie os requisitos de caso de uso para os recursos do Android Enterprise. Documente o recurso para cada requisito de dispositivo que mais se aproxime do requisito e sua versão Android correspondente.
4. Determine o sistema operacional Android mínimo com base nos requisitos do recurso (7.0, 8.0, 9.0).
5. Escolha um modelo de identidade:
 - Recomendado: conta do Google Play gerenciado
 - Use as contas do Google G-Suite somente se você for um cliente do Google Cloud Identity
6. Crie uma estratégia de dispositivo:
 - Nenhuma ação: se os dispositivos atenderem ao nível mínimo de SO
 - Atualizar: se os dispositivos suportarem e puderem ser atualizados para o SO suportado
 - Substituir: se os dispositivos não puderem ser atualizados para o nível de SO suportado

Estratégia de migração de aplicativos recomendada

Depois de concluir o mapeamento de requisitos, mova os aplicativos da plataforma Android para a plataforma Android Enterprise. Para obter detalhes sobre a publicação de aplicativos, consulte [Adicionar aplicativos](#).

- Aplicativos da loja pública
 1. Selecione os aplicativos a serem migrados e edite os aplicativos para limpar a configuração do Google Play e selecionar **Android Enterprise** como plataforma.
 2. Selecione o grupo de entrega. Se um aplicativo for obrigatório, mova o aplicativo para a lista **Aplicativos obrigatórios** no grupo de entrega.

Depois de salvar um aplicativo, ele será exibido na Google Play Store. Se você tiver um perfil de trabalho, os aplicativos serão exibidos na Google Play Store no perfil de trabalho.

- Aplicativos (empresariais) privados

Aplicativos privados são desenvolvidos internamente ou por um desenvolvedor terceirizado. Recomendamos que você publique aplicativos privados usando o Google Play.

1. Selecione os aplicativos a serem migrados e edite os aplicativos para selecionar o **Android Enterprise** como plataforma.
2. Carregue o arquivo APK e defina as configurações do aplicativo.
3. Publique o aplicativo no grupo de entrega necessário.

- Aplicativos MDX

1. Selecione os aplicativos a serem migrados e edite os aplicativos para selecionar o **Android Enterprise** como plataforma.
2. Carregue o arquivo MDX. Siga o processo de aprovação do aplicativo.
3. Selecione as políticas MDX.

Para aplicativos Enterprise MDX, recomendamos alterá-los para aplicativos preparados no modo MDX SDK:

- Opção 1: hospede o APK no Google Play com uma conta de desenvolvedor atribuída de modo privado à sua organização. Publique o arquivo MDX no XenMobile.
- Opção 2: publique o aplicativo do XenMobile como um aplicativo empresarial. Publique o APK no XenMobile e selecione a plataforma **Android Enterprise** para o arquivo MDX.

Migração da política de dispositivo Citrix

Para políticas que estão disponíveis para as plataformas Android e Android Enterprise: edite a política e selecione a plataforma **Android Enterprise**.

Para o Android Enterprise, considere o modo de registro. Algumas opções de política estão disponíveis apenas para dispositivos no modo de perfil de trabalho ou no modo totalmente gerenciado.

Proof of concept

Depois de migrar os aplicativos para o Android Enterprise, você pode configurar um teste de migração para verificar se os recursos estão funcionando conforme esperado.

Configuração recomendada para a prova de conceito

1. Configure a infraestrutura de implantação:
 - Crie um grupo de entrega para os seus testes do Android Enterprise.
 - Configure o Android Enterprise no XenMobile.
2. Configure os aplicativos do usuário.
3. Configure os recursos do Android Enterprise.
4. Atribua políticas ao grupo de entrega do Android Enterprise.
5. Teste e confirme os recursos.
6. Conclua o processo passo a passo de configuração do dispositivo para cada caso de uso.
7. Documente as etapas de configuração do usuário.

Deployment

Agora você pode implantar sua configuração do Android Enterprise e preparar os seus usuários para a migração.

Estratégia de implantação recomendada

A estratégia de implantação recomendada pela Citrix é testar todos os seus sistemas de produção no Android Enterprise e concluir a migração de dispositivos posteriormente.

- Nesse cenário, os usuários continuam a usar dispositivos legados com a configuração atual. Você configura novos dispositivos para o gerenciamento do Android Enterprise.
- Migre os dispositivos existentes somente quando uma atualização ou substituição for necessária.
- Migre os dispositivos existentes para o gerenciamento Android Enterprise no final de seu ciclo de vida habitual. Ou migre esses dispositivos quando precisarem de substituição devido a perda ou quebra.

Android Enterprise

August 20, 2021

Android Enterprise é um conjunto de ferramentas e serviços fornecidos pelo Google como uma solução de gerenciamento corporativo para dispositivos Android. Com o Android Enterprise:

- Você usa o XenMobile para gerenciar dispositivos Android de propriedade da empresa e dispositivos Android BYOD (o seu próprio).
- Você pode gerenciar todo o dispositivo ou um perfil separado no dispositivo. O perfil separado isola contas, aplicativos e dados comerciais de contas, aplicativos e dados pessoais.
- Você também pode gerenciar dispositivos dedicados a um único uso, como gerenciamento de inventário. Para obter uma visão geral dos recursos do Android Enterprise do Google, consulte [Android Enterprise Management](#).

Recursos:

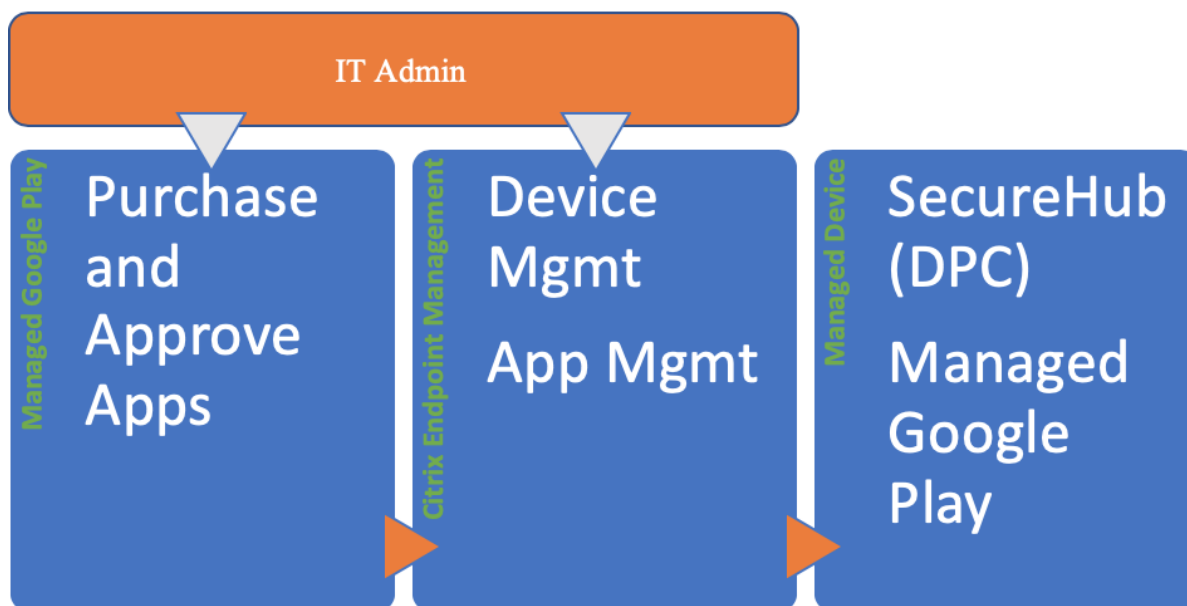
- Para obter uma lista de termos e definições relacionados ao Android Enterprise, consulte a [terminologia do Android Enterprise](#) no guia de desenvolvedores do Google Android Enterprise. O Google atualiza estes termos com frequência.
- Para sistemas operacionais Android compatíveis com o XenMobile, consulte [Sistemas operacionais compatíveis de dispositivos](#).
- Para obter informações sobre as conexões de saída a serem consideradas ao configurar ambientes de rede para o Android Enterprise, consulte o artigo de suporte do Google, [Android Enterprise Network Requirements](#).

Ao integrar o XenMobile com o Google Play gerenciado para usar o Android Enterprise, você cria uma empresa. O Google define uma empresa como um vínculo entre a organização e sua solução de gerenciamento móvel corporativo (EMM). Todos os usuários e dispositivos que a organização gerencia através de sua solução pertencem à sua empresa.

Uma empresa para Android Enterprise tem três componentes: uma solução EMM, um aplicativo DPC (Device Policy Controller) e uma plataforma de aplicativos empresariais do Google. Quando você integra o XenMobile com o Android Enterprise, a solução completa possui os seguintes componentes:

- **XenMobile:** o Citrix EMM. O XenMobile é a solução XenMobile unificada para um espaço de trabalho digital seguro. O XenMobile fornece os meios para que os administradores de TI gerenciem dispositivos e aplicativos para suas organizações.
- **Citrix Secure Hub:** o aplicativo Citrix DPC. O Secure Hub é a plataforma de lançamento para XenMobile. O Secure Hub impõe políticas no dispositivo.
- **Google Play gerenciado:** uma plataforma de aplicativos empresariais do Google que se integra ao XenMobile. A API EMM do Google Play define políticas de aplicativo e distribui o aplicativo.

Esta ilustração mostra como os administradores interagem com esses componentes e como os componentes interagem entre si:



Usar o Google Play gerenciado com o XenMobile

Nota:

Você pode usar o Google Play gerenciado ou o Google Workspace para registrar o Citrix como seu provedor de EMM. Este artigo aborda o uso do Android Enterprise com o Google Play gerenciado. Se a sua organização usa o Google Workspace para fornecer acesso a aplicativos, você pode usá-lo com o Android Enterprise. Consulte [Clientes do Android Enterprise herdado para Google Workspace \(anteriormente G Suite\)](#).

Quando você usa o Google Play gerenciado, você provisiona contas do Google Play gerenciado para dispositivos e usuários finais. As contas do Google Play gerenciado fornecem acesso ao Google Play gerenciado, permitindo que os usuários instalem e usem os aplicativos que você disponibilizar. Se a sua organização usa um serviço de identidade de terceiros, você pode vincular contas do Google Play gerenciado às suas contas de identidade existentes.

Como esse tipo de empresa não está vinculado a um domínio, você pode criar mais de uma empresa para uma única organização. Por exemplo, cada departamento ou região de uma organização pode se registrar como uma empresa diferente para gerenciar conjuntos separados de dispositivos e aplicativos.

Para administradores XenMobile, o Google Play gerenciado combina a experiência do usuário e os recursos da loja de aplicativos do Google Play com um conjunto de recursos de gerenciamento projetados para empresas. Você pode usar o Google Play gerenciado para adicionar, comprar e aprovar

aplicativos para implantação no espaço de trabalho do Android Enterprise em um dispositivo. Você pode usar o Google Play para implantar aplicativos públicos, aplicativos privados e aplicativos de terceiros.

Para usuários de dispositivos gerenciados, o Google Play gerenciado é a loja de aplicativos empresariais. Os usuários podem procurar aplicativos, visualizar detalhes do aplicativo e instalá-los. Ao contrário da versão pública do Google Play, os usuários só podem instalar aplicativos do Google Play gerenciado que você disponibilizar para eles.

Cenários de implantação de dispositivos e modos de operação

O cenário de implantação do dispositivo refere-se a quem possui os dispositivos implantados e como você os gerencia. Os perfis de dispositivos referem-se a como o DPC gerencia e impõe políticas aos dispositivos.

Um perfil de trabalho isola contas, aplicativos e dados comerciais de contas, aplicativos e dados pessoais. Para obter mais detalhes sobre perfis de trabalho, consulte o tópico de ajuda do Google Android Enterprise, [What is a work profile](#).

Importante:

Quando os dispositivos Android Enterprise atualizam para o Android 11, o Google migrará os dispositivos gerenciados como “totalmente gerenciados com um perfil de trabalho” para uma nova experiência de perfil de trabalho com segurança aprimorada. Para obter mais informações, consulte [Alterações à frente para o perfil de trabalho totalmente gerenciado com o Android Enterprise](#).

Gerenciamento de dispositivos	Casos de uso	Perfil de trabalho	Perfil pessoal	Observações
Dispositivos de propriedade da empresa (totalmente gerenciados)	Dispositivos de propriedade da empresa destinados apenas ao trabalho	Não	Sim. O DPC pode executar ações em todo o dispositivo, como configurar conectividade em todo o dispositivo, configurar configurações globais e executar uma redefinição de fábrica.	Apenas para dispositivos novos ou com redefinição de fábrica.
Totalmente gerenciado com um perfil de trabalho	Dispositivos de propriedade da empresa destinados a uso pessoal e profissional	Sim	Sim. Duas cópias do DPC são executadas nesses dispositivos: uma gerencia o dispositivo no modo proprietário do dispositivo e a outra gerencia o perfil de trabalho no modo proprietário do perfil. Você pode aplicar políticas separadas ao dispositivo e ao perfil de trabalho.	Anteriormente conhecidos como dispositivos corporativos, habilitados pessoalmente (COPE).

Gerenciamento de dispositivos	Casos de uso	Perfil de trabalho	Perfil pessoal	Observações
Dispositivos dedicados*	Dispositivos de propriedade da empresa configurados para um único caso de uso, como sinalização digital ou impressão de tíquetes	Não	Sim. Você fornece apenas os aplicativos necessários e impede que os usuários adicionem outros aplicativos.	Anteriormente conhecidos como dispositivos corporativos para uso único (COSU).
Perfil de trabalho BYOD**	Dispositivos pessoais registrados no modo de perfil de trabalho (também conhecido como modo de proprietário do perfil)	Sim	Sim. O DPC gerencia apenas o perfil de trabalho, não o dispositivo inteiro.	Esses dispositivos não precisam ser novos ou com redefinição de fábrica.

* Os usuários podem compartilhar um dispositivo dedicado. Quando um usuário faz logon em um aplicativo em um dispositivo dedicado, o estado do trabalho fica com o aplicativo, não com o dispositivo.

** O XenMobile não suporta dispositivos Zebra como no modo de perfil de trabalho BYOD. O XenMobile suporta dispositivos Zebra como dispositivos totalmente gerenciados e no modo legado do dispositivo (também chamado de modo de administração do dispositivo).

Para obter informações sobre como migrar do modo legado para o modo de proprietário do dispositivo ou de proprietário do perfil, consulte [Migrar do Device Administration para o Android Enterprise](#).

Métodos de autenticação

Os perfis de registro determinam se os dispositivos Android se registram ou não no MAM, MDM ou MDM+MAM, com uma opção para que os usuários optem para não ter MDM.

Os modos de segurança de registro **Nome de usuário + PIN**, **URL de convite**, **URL de convite + PIN** e **URL de convite + senha** não estão disponíveis para o Android Enterprise. Para obter informações sobre como especificar o nível de segurança e as etapas de registro necessárias, consulte [Para configurar modos de segurança de registro](#).

O XenMobile suporta os seguintes métodos de autenticação para dispositivos Android registrados no MDM+MAM. Para obter informações, consulte os artigos em [Certificados e autenticação](#).

- Domínio
- Domínio mais token de segurança
- Certificado de cliente
- Certificado de cliente mais domínio
- Provedores de identidade:
 - Azure Active Directory
 - Provedor de identidade Citrix

Outro método de autenticação raramente usado é certificado de cliente mais token de segurança. Para obter informações, consulte <https://support.citrix.com/article/CTX215200>.

Requisitos

Antes de começar a usar o Android Enterprise, você precisa:

- Contas e credenciais:
 - Para configurar o Android Enterprise com o Google Play gerenciado, uma conta corporativa do Google
 - Para baixar os arquivos MDX mais recentes, uma conta de cliente Citrix
 - Para implantar aplicativos privados (opcional), uma conta de desenvolvedor do Google
- Firebase Cloud Messaging (FCM) configurado para XenMobile. Consulte [Firebase Cloud Messaging](#) para obter instruções.
- Para Samsung Knox Mobile Enrollment (opcional), licenças premium Knox

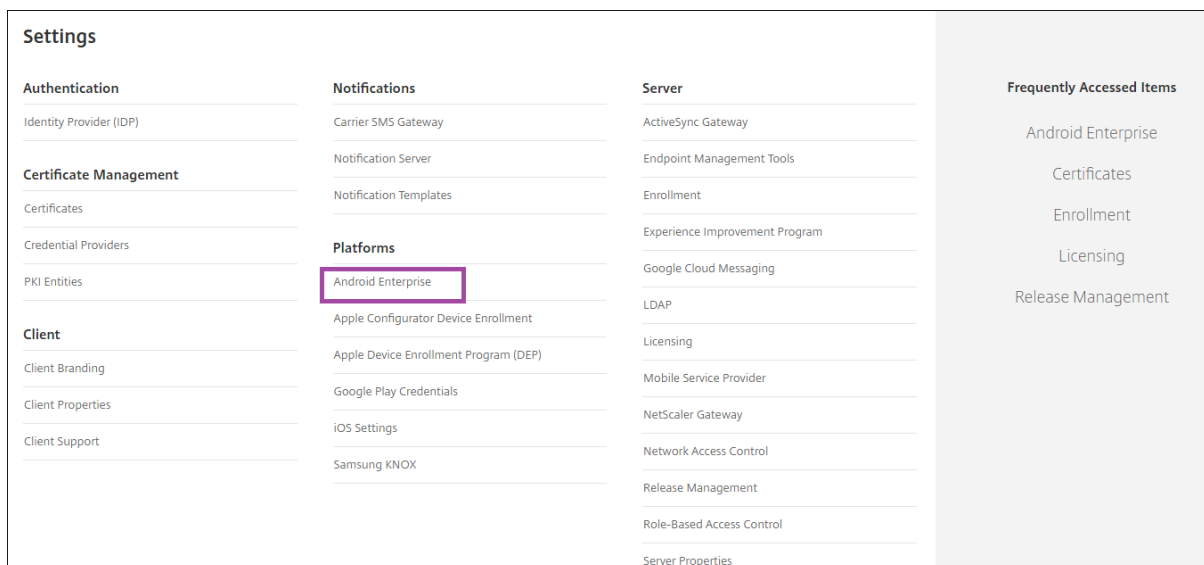
Conectar o XenMobile ao Google Play

Para configurar o Android Enterprise para a sua organização, registre o Citrix como seu provedor de EMM por meio do Google Play gerenciado. Essa configuração conecta o Google Play gerenciado ao XenMobile e cria uma empresa para Android Enterprise no XenMobile.

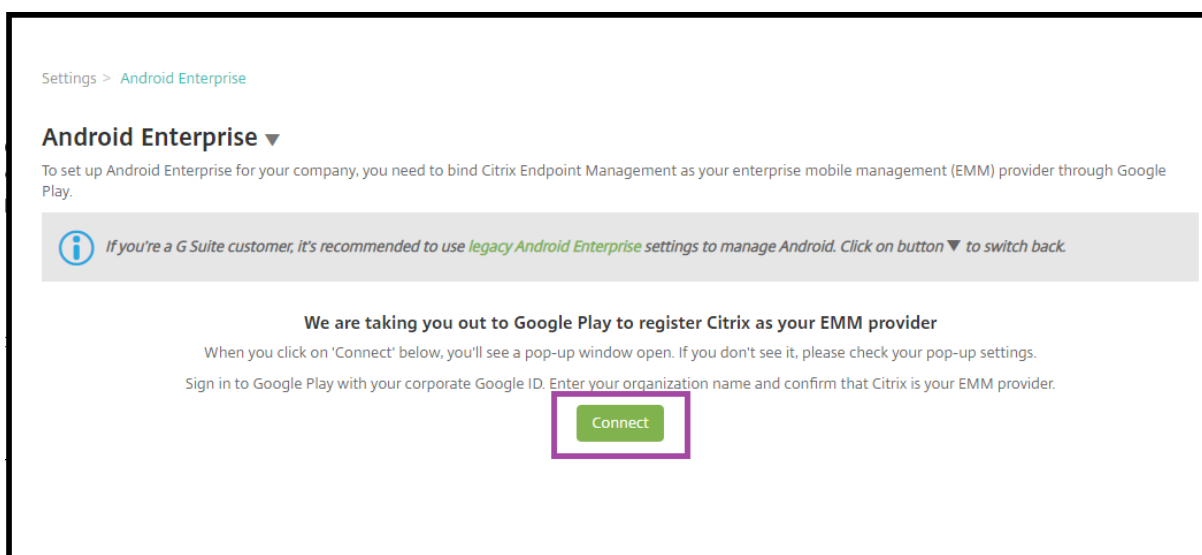
Você precisará de uma conta corporativa do Google para entrar no Google Play.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida.

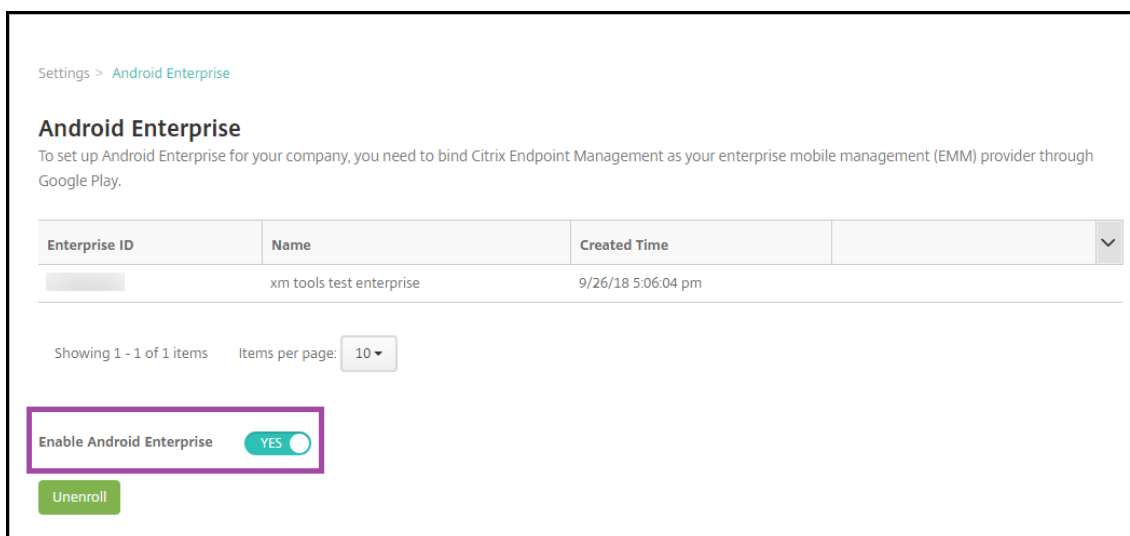
2. Vá para **Configurações > Android Enterprise**.



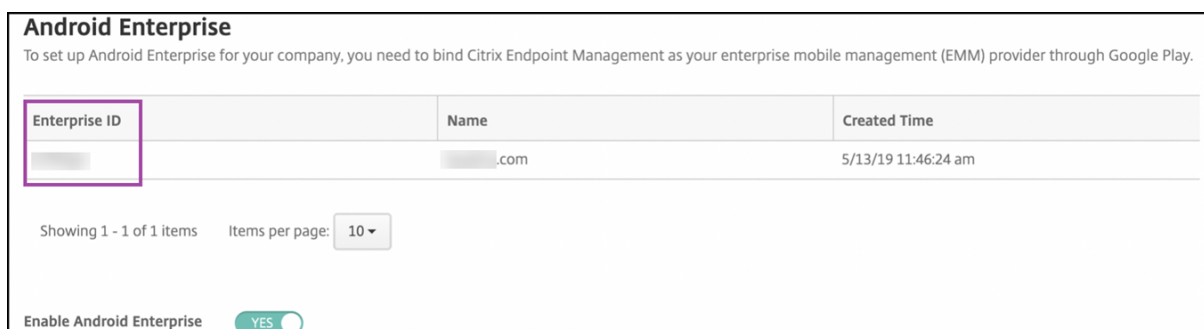
1. Clique em **Connect**. O Google Play é aberto.



1. Inicie a sessão no Google Play com as credenciais da sua conta corporativa do Google. Insira o nome da sua organização e confirme que a Citrix é seu provedor de EMM.
2. Um ID empresarial é adicionado ao Android Enterprise. Para ativar o Android Enterprise, deslize **Ativar Android Enterprise** para **Sim**.



Seu ID corporativo aparece no console XenMobile.



Seu ambiente está conectado ao Google e está pronto para gerenciar dispositivos. Agora você pode fornecer aplicativos para usuários.

O XenMobile pode ser usado para fornecer aos usuários aplicativos móveis de produtividade da Citrix, aplicativos MDX, aplicativos da loja de aplicativos pública, aplicativos Web e SaaS, aplicativos empresariais e links da Web. Para obter mais informações sobre esses tipos de aplicativos e fornecê-los aos usuários, consulte [Adicionar aplicativos](#).

A seção a seguir mostra como fornecer aplicativos móveis de produtividade.

Fornecer aplicativos móveis de produtividade da Citrix para usuários do Android Enterprise

Fornecer aplicativos móveis de produtividade da Citrix para usuários do Android Enterprise requer estas etapas.

1. Publique os aplicativos como aplicativos MDX. Consulte Configurar aplicativos como aplicativos MDX.

2. Configure as regras para o desafio de segurança que seus usuários usam para acessar os perfis de trabalho em seus dispositivos. Consulte Configurar política de desafio de segurança.

Os aplicativos que você publica estão disponíveis para dispositivos registrados no seu enterprise do Android Enterprise.

Nota:

Quando você implanta um aplicativo da loja de aplicativos pública do Android Enterprise em um usuário Android, esse usuário é automaticamente registrado no Android Enterprise.

Configurar aplicativos como aplicativos MDX

Para configurar um aplicativo de produtividade Citrix como um aplicativo MDX para Android Enterprise:

1. No console XenMobile, clique em **Configurar > Aplicativos**. A página **Aplicativos** é exibida.

Icon	App Name	Type	Category	Created On	Last Updated	Disable
	Citrix Secure Web - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	<input type="checkbox"/>
	Citrix Secure Hub - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	<input type="checkbox"/>
	Classroom - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	<input type="checkbox"/>
	MRF Android Enterprise TD	Enterprise	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	<input type="checkbox"/>

2. Clique em **Add**. A caixa de diálogo **Adicionar Aplicativo** é exibida.

Add App ✕

Click an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

MDX

Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.

Example: WorxMail

Public App Store

Free or paid apps available in a public app store, such as iTunes or Google Play, for download.

Example: GoToMeeting

Web & SaaS

Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.

Example: GoogleApps_SAML

Enterprise

Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.

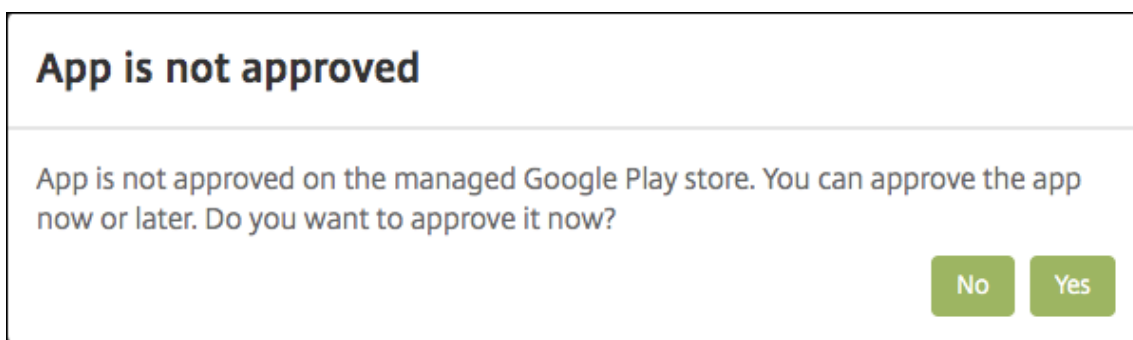
Example: Quick-iLaunch

Web Link

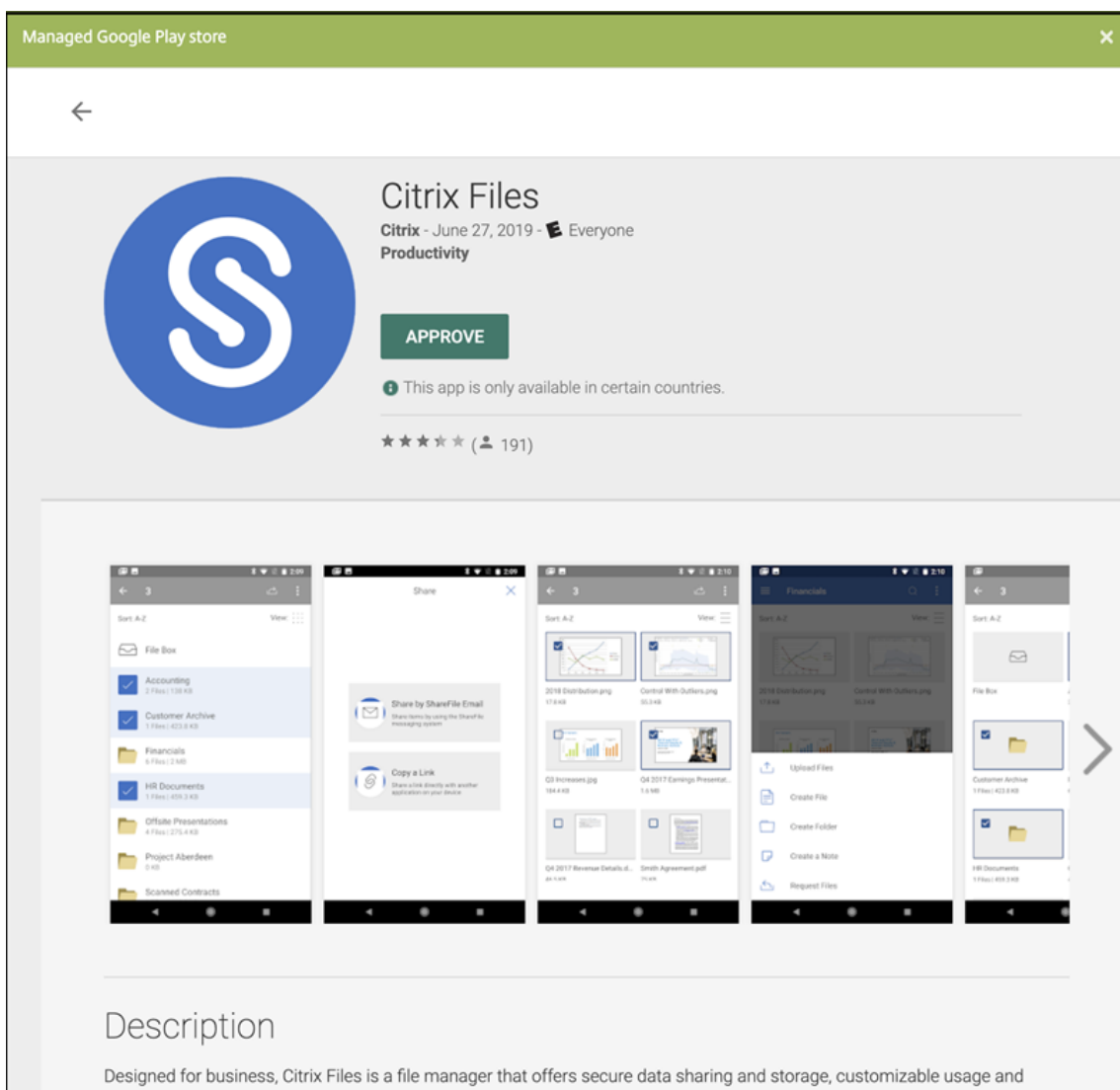
A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. Clique em **MDX**. A página **Informações do Aplicativo** é exibida.

4. No lado esquerdo da página, selecione **Android Enterprise** como plataforma.
5. Na página **Informações do aplicativo**, digite as seguintes informações:
 - **Nome:** digite um nome descritivo para o aplicativo. Esse nome aparecerá em **Nome do aplicativo** na tabela **Aplicativos**.
 - **Descrição:** digite uma descrição opcional para o aplicativo.
 - **Categoria do aplicativo:** opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte [Sobre categorias de aplicativos](#).
6. Clique em **Next**. A página do **Aplicativo MDX Android Enterprise** é exibida.
7. Clique em **Carregar** e navegue até o local dos arquivos .mdx do aplicativo. Selecione o arquivo e clique em **Abrir**.
8. A interface do usuário notificará você se o aplicativo anexado exigir aprovação da loja gerenciada do Google Play. Para aprovar o aplicativo sem sair do console XenMobile, clique em **Sim**.




9. Quando a página da loja gerenciada do Google Play for aberta, clique em **Aprovar**.



10. Clique em **Aprovar** novamente.
11. Selecione **Manter aprovado quando o aplicativo solicitar novas permissões**. Clique em **Save**.

APPROVAL SETTINGS NOTIFICATIONS

 **Citrix Files**
Citrix

How would you like to handle new app permission requests?

Keep approved when app requests new permissions.
Users will be able to install the updated app.

Revoke app approval when this app requests new permissions.
App will be removed from the store until it is reapproved.

CANCEL SAVE

12. Quando o aplicativo é aprovado e salvo, mais configurações aparecem na página. Defina estas configurações:
 - **Nome do arquivo:** digite o nome de arquivo associado ao aplicativo.
 - **Descrição do aplicativo:** digite uma descrição para o aplicativo.
 - **Rastreamento de produtos:** especifique qual rastreamento de produto você deseja enviar para os dispositivos do usuário. Se você tiver um rastreamento projetado para testes, poderá selecioná-lo e atribuí-lo aos seus usuários. O padrão é Produção.
 - **Versão do aplicativo:** opcionalmente, digite o número da versão do aplicativo.
 - **ID de pacote:** o URL do aplicativo na loja Google Play.
 - **Versão do SO mínima:** opcionalmente, digite a versão mais antiga do sistema operacional que o dispositivo pode executar para usar o aplicativo.
 - **Versão do SO máxima:** opcionalmente, digite a versão mais recente do sistema operacional que o dispositivo deve executar para usar o aplicativo.
 - **Dispositivos excluídos:** opcionalmente, digite o fabricante ou os modelos de dispositivos que não podem executar o aplicativo.
13. Configure as **Políticas de MDX**. Para obter mais informações sobre políticas de aplicativos para aplicativos MDX, consulte [Resumo das políticas do MDX](#) e [Visão geral do MAM SDK](#).
14. Configure as regras de implantação. Para obter informações, consulte [Implantar recursos](#).
15. Expanda **Configuração da loja**. Essa configuração não se aplica aos aplicativos Android Enterprise, que aparecem somente no Google Play gerenciado.

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings

Allow app comments

Opcionalmente, você pode adicionar ao aplicativo perguntas frequentes ou capturas de tela que são exibidas na loja de aplicativos. Você também pode definir se os usuários podem classificar ou comentar no aplicativo.

- Defina estas configurações:
 - **Perguntas frequentes sobre o aplicativo:** adicione perguntas frequentes e respostas para o aplicativo.
 - **Instantâneos do aplicativo:** adicione capturas de tela para ajudar a classificar o aplicativo na loja de aplicativos. O gráfico que você carregar deve ser um PNG. Você não pode carregar uma imagem GIF ou JPEG.
 - **Permitir classificações do aplicativo:** selecione se um usuário tem permissão para classificar o aplicativo. O padrão é **I**.
 - **Permitir comentários do aplicativo:** selecione se os usuários têm permissão para comentar sobre o aplicativo selecionado. O padrão é **I**.

16. Clique em **Next**. A página **Aprovações** é exibida.

MDX	Approvals (optional) ×
1 App Information	Apply an existing workflow or create a new workflow to require approval before allowing users to access the app. Workflow to Use <input type="text" value="None"/>
2 Platform	
<input type="checkbox"/> iOS	
<input type="checkbox"/> Android	
<input checked="" type="checkbox"/> Windows Phone	
<input checked="" type="checkbox"/> Windows Desktop/Tablet	
3 Approvals (optional)	
4 Delivery Group Assignments (optional)	

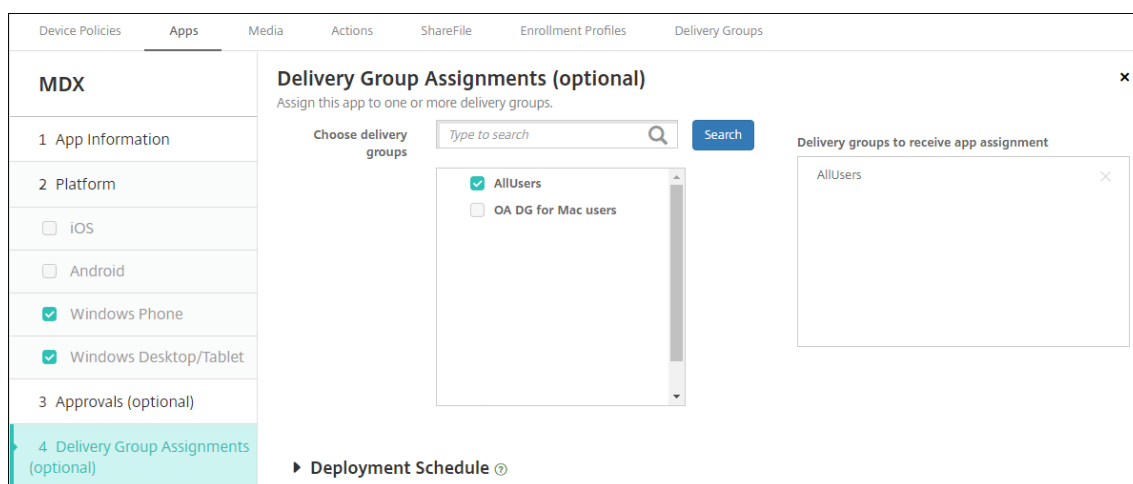
Use fluxos de trabalho quando precisar de aprovação ao criar contas de usuário. Se você não quiser configurar fluxos de trabalho de aprovação, pule para a Etapa 15.

Configure estas definições para atribuir ou criar um fluxo de trabalho:

- **Fluxo de trabalho a ser usado:** na lista, clique em um fluxo de trabalho existente ou clique em **Criar um novo fluxo de trabalho**. O padrão é **Nenhum**.
- Se você selecionar **Criar um novo fluxo de trabalho**, defina essas configurações. Para obter mais informações, consulte [Aplicar fluxos de trabalho](#).
- **Nome:** digite um nome exclusivo para o fluxo de trabalho.
- **Descrição:** opcionalmente, digite uma descrição para o fluxo de trabalho.
- **Modelos de aprovação de email:** na lista, selecione o modelo de aprovação a ser atribuído. Quando você clica no ícone de olho à direita deste campo, uma caixa de diálogo é exibida na qual você pode visualizar o modelo.
- **Níveis de aprovação do gerente:** na lista, selecione o número de níveis de aprovação do gerente necessários para esse fluxo de trabalho. O padrão é 1 nível. As opções possíveis são:
 - Não é Necessário
 - 1 nível
 - 2 níveis
 - 3 níveis
- **Selecionar domínio do Active Directory:** na lista, selecione o domínio do Active Directory adequado a ser usado para o fluxo de trabalho.
- **Encontrar aprovadores necessários adicionais:** digite o nome adicional da pessoa no campo de pesquisa e clique em **Pesquisar**. Os nomes são originários do Active Directory.
- Quando o nome aparece no campo, selecione a caixa de seleção próxima ao nome. O nome e endereço de email da pessoa aparecem na lista **Aprovadores necessários adicionais selecionados**.
 - Para remover uma pessoa da lista **Aprovadores necessários adicionais selecionados**, você pode optar por um dos seguintes procedimentos:

- * Clique em **Pesquisar** para ver uma lista de todas as pessoas do domínio selecionado.
- * Digite um nome parcial ou completo na caixa Pesquisar e clique em **Pesquisar** para limitar os resultados da pesquisa.
- * As pessoas da lista **Aprovadores necessários adicionais selecionados** têm marcas de seleção ao lado do respectivo nome na lista de resultados de pesquisa. Percorra a lista e desmarque a caixa de seleção ao lado de cada nome que você deseja remover.

17. Clique em **Next**. A página **Atribuição de grupo de entrega** é exibida.



18. Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega ou selecione um ou mais grupos. Os grupos que você selecionar aparecerão na lista **Grupos de entrega que receberão a atribuição de aplicativos**.

19. Expanda **Cronograma de implantação** e defina estas configurações:

- Ao lado de **Implantar**, clique em **I** para agendar a implantação ou em **O** para impedi-la. A opção padrão é **I**.
- Ao lado do Cronograma de implantação, clique em **Agora** ou **Mais tarde**. A opção padrão é **Agora**.
- Se você clicar em **Mais tarde**, clique no ícone de calendário e selecione a data e a hora da implantação.
- Ao lado de **Condição de implantação**, clique em **Em cada conexão** ou em **Somente quando a implantação anterior tiver falhado**. A opção padrão é **Em cada conexão**.
- Ao lado de **Implantar para conexões permanentes**, verifique se **O** está selecionado. A opção padrão é **O**. As conexões sempre ativas AlwaysOn não estão disponíveis para o Android Enterprise se você começou a usar o XenMobile com a versão 10.18.19 ou posterior. Não recomendamos as conexões para clientes que começaram a usar o XenMobile antes

da versão 10.18.19.

Essa opção será aplicável quando você tiver configurado a chave de implantação em segundo plano do cronograma em **Configurações > Propriedades do servidor**.

O cronograma de implantação que você configura é o mesmo para todas as plataformas. Todas as alterações feitas se aplicam a todas as plataformas, exceto **Implantar para conexões permanentes**.

20. Clique em **Save**.

Repita as etapas para configurar um aplicativo MDX para cada aplicativo móvel de produtividade.

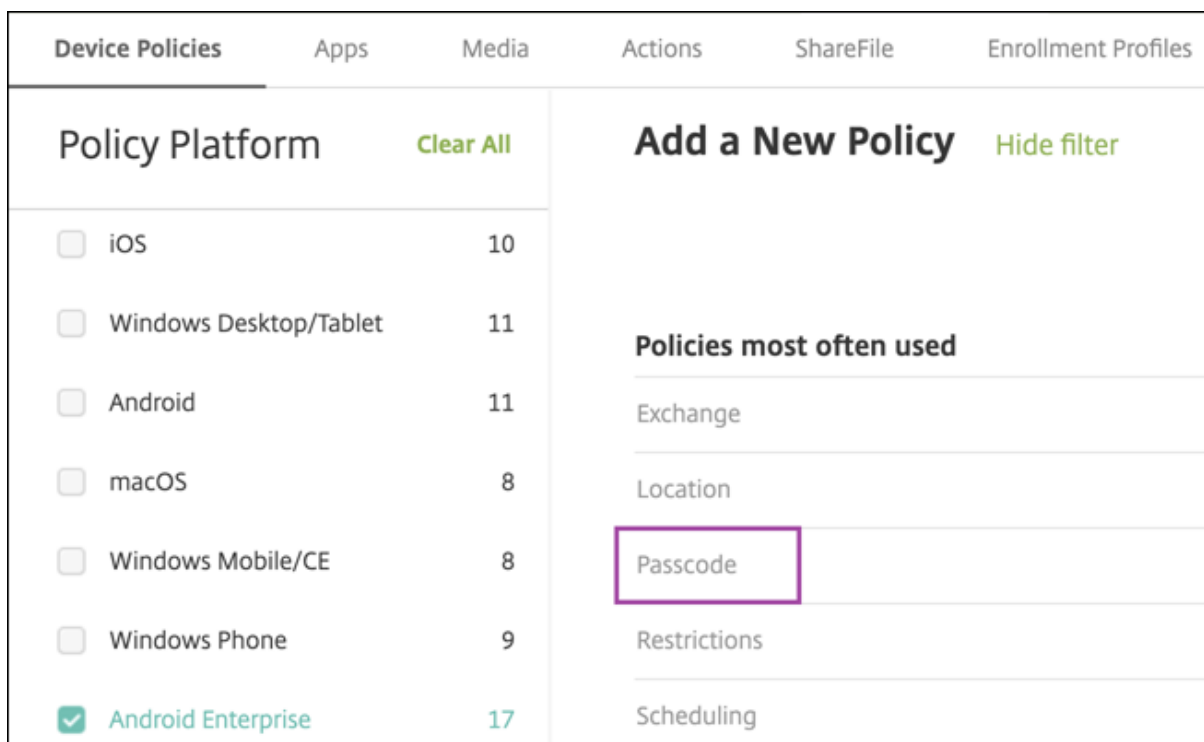
Configurar política de desafio de segurança

A política de dispositivo de código secreto XenMobile configura o conjunto de regras para que os usuários de desafios de segurança acessem seus dispositivos ou os perfis de trabalho Android Enterprise em seus dispositivos. Um desafio de segurança pode ser um código secreto ou reconhecimento biométrico. Para obter mais informações sobre a política de código secreto, consulte [Políticas de dispositivo de código secreto](#).

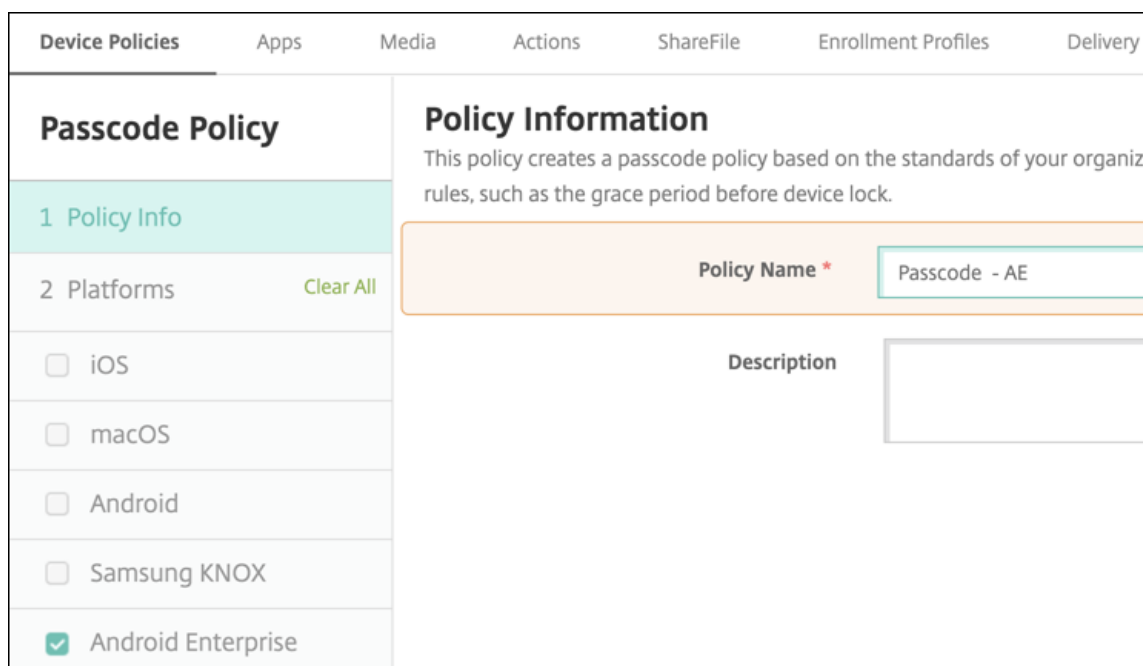
- Se a implantação do Android Enterprise incluir dispositivos BYOD, configure a política de código secreto para o perfil de trabalho.
- Se sua implantação incluir dispositivos totalmente gerenciados de propriedade da empresa, configure a política de código secreto para o próprio dispositivo.
- Se a sua implantação incluir ambos os tipos de dispositivos, configure os dois tipos de política de código secreto.

Para configurar a política de código secreto:

1. No console XenMobile, vá para **Configurar > Políticas de dispositivo**.
2. Clique em **Add**.
3. Clique em **Mostrar filtro** para mostrar o painel **Plataforma de política**. No painel **Plataforma de política**, selecione **Android Enterprise**.
4. Clique em **Código secreto** no painel direito.



1. Digite o **Nome da política**. Clique em **Next**.



2. Defina as configurações de política de código secreto.

- Defina **Código secreto do dispositivo obrigatório** para **Ativado** para ver as definições disponíveis para os desafios de segurança do dispositivo.
- Defina **Desafio de segurança no perfil de trabalho** como **Ativado** para ver as definições

disponíveis para os desafios de segurança do perfil de trabalho.

3. Clique em **Next**.
4. Atribua a política a um ou mais grupos de entrega.
5. Clique em **Save**.

Criar perfis de registro

Os perfis de registro controlam como os dispositivos Android são registrados se o Android Enterprise estiver habilitado para a sua implantação XenMobile. Ao criar um perfil de registro para registrar dispositivos Android Enterprise, você pode configurar o perfil de registro para registrar dispositivos novos e com redefinição de fábrica como:

- Dispositivos totalmente gerenciados
- Dispositivos dedicados (dispositivos COSU)
- Dispositivos totalmente gerenciados com um perfil de trabalho (dispositivos COPE)

Você também pode configurar cada um desses perfis de registro do Android Enterprise para registrar dispositivos Android BYOD como dispositivos de perfil de trabalho.

Se o Android Enterprise estiver habilitado para sua implantação do XenMobile, todos os dispositivos Android recém-registrados ou registrados novamente serão registrados como dispositivos Android Enterprise. Por padrão, o perfil de registro Global registra dispositivos Android novos e com redefinição de fábrica como dispositivos totalmente gerenciados e registra dispositivos Android BYOD como dispositivos de perfil de trabalho.

Ao criar perfis de inscrição, você atribui grupos de entrega a eles. Se um usuário pertencer a vários grupos de entrega que têm perfis de registro diferentes, o nome do grupo de entrega determinará o perfil de registro usado. O XenMobile seleciona o grupo de entrega que aparece por último em uma lista alfabética de grupos de entrega. Para obter mais informações, consulte [Perfis de registro](#).

Você pode usar perfis de registro para combinar vários casos de uso, como somente MDM, MDM+MAM e somente MAM. O tipo de licença do XenMobile Server, refletido na propriedade do servidor `xms.server.mode`, determina as configurações disponíveis em **Configurar > Perfis de registro**.

Adicionar um perfil de registro para dispositivos totalmente gerenciados

O perfil de registro Global registra dispositivos totalmente gerenciados por padrão, mas você pode criar mais perfis de registro para registrar dispositivos totalmente gerenciados.

1. No console XenMobile, vá para **Configurar > Perfis de registro**.
2. Para adicionar um perfil de registro, clique em **Adicionar**. Na página de Informações de registro, digite um nome para o perfil de registro.

3. Defina o número de dispositivos que os membros com este perfil podem registrar.
4. Selecione **Android** em **Plataformas** ou clique em **Avançar**. A página de configuração de registro é exibida.
5. Defina **Gerenciamento** para **Android Enterprise**.
6. Defina **Modo proprietário do dispositivo** como **Dispositivo de propriedade da empresa**.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	Device management ⓘ Management <ul style="list-style-type: none"> <input checked="" type="radio"/> Android Enterprise ⓘ <input type="radio"/> Legacy device administration (not recommended) ⓘ <input type="radio"/> Do not manage devices ⓘ
Android	Device owner mode <ul style="list-style-type: none"> <input checked="" type="radio"/> Company-owned device ⓘ <input type="radio"/> Fully managed with work profile ⓘ <input type="radio"/> Dedicated device ⓘ <input type="radio"/> None ⓘ
iOS	BYOD work profile <input checked="" type="checkbox"/> ⓘ
3 Assignment (optional)	Application management ⓘ Citrix MAM <input checked="" type="checkbox"/> ⓘ
	User consent Allow users to decline device management <input checked="" type="checkbox"/> ⓘ

7. **Perfil de trabalho BYOD** permite configurar o perfil de registro para registrar dispositivos BYOD como dispositivos de perfil de trabalho. Dispositivos novos e com redefinição de fábrica são registrados como dispositivos totalmente gerenciados.
 - Defina **Perfil de trabalho BYOD** como **Ativado** para permitir o registro de dispositivos BYOD como dispositivos de perfil de trabalho. O padrão é **On**.
 - Defina o **perfil de trabalho BYOD** como **Desativado** para restringir o registro a dispositivos totalmente gerenciados.
8. Escolha se deseja registrar dispositivos no Citrix MAM.
9. Se você definir **Perfil de trabalho BYOD** como **Ativado**, configure o consentimento do usuário. Para permitir que os usuários de dispositivos de perfil de trabalho BYOD recusem o gerenciamento do dispositivo ao registrar seus dispositivos, defina **Permitir que os usuários recusem o gerenciamento de dispositivos** como **On**.

Se o **Perfil de trabalho BYOD** estiver definido como **On**, o valor padrão de **Permitir que os usuários recusem o gerenciamento de dispositivos** será **On**. Se o **Perfil de trabalho BYOD** estiver definido como **Off**, **Permitir que os usuários recusem o gerenciamento de dispositivos** será desabilitado.

10. Selecione **Atribuição (opções)**. A tela Atribuição de grupo de entrega é exibida.
11. Escolha um grupo de entrega ou grupos de entrega contendo os administradores que registram dispositivos totalmente gerenciados. Em seguida, clique em **Save**.

A página de Perfil de registro é exibida com o perfil que você adicionou.

<input type="checkbox"/>	Enrollment profile name	Created on	Updated on	Device limit
<input type="checkbox"/>	Fully managed devices	11/19/19 2:19:16 pm	11/19/19 2:19:16 pm	unlimited
<input type="checkbox"/>	Global	3/7/18 4:08:24 pm	3/7/18 4:08:24 pm	unlimited

Showing 1 - 2 of 2 items Items per page: 10

Adicionar um perfil de registro de dispositivo dedicado

Quando a sua implantação do XenMobile inclui dispositivos dedicados, um único administrador XenMobile ou um pequeno grupo de administradores registra vários dispositivos dedicados. Para garantir que esses administradores possam registrar todos os dispositivos necessários, crie um perfil de registro para eles com dispositivos ilimitados permitidos por usuário.

1. No console XenMobile, vá para **Configurar > Perfis de registro**.
2. Para adicionar um perfil de registro, clique em **Adicionar**. Na página de Informações de registro, digite um nome para o perfil de registro. Certifique-se de que o número de dispositivos que os membros com este perfil podem registrar esteja definido como ilimitado.
3. Selecione **Android** em **Plataformas** ou clique em **Avançar**. A página de configuração de registro é exibida.
4. Defina **Gerenciamento** para **Android Enterprise**.
5. Defina **Modo de proprietário do dispositivo** como **Dispositivo dedicado**.

The screenshot displays the 'Enrollment Configuration' page for an Android profile. The left sidebar shows a navigation menu with 'Enrollment Profile' at the top, followed by '1 Enrollment Info', '2 Platforms', 'Android' (highlighted), 'iOS', and '3 Assignment (optional)'. The main content area is titled 'Enrollment Configuration' and includes the instruction 'Specify device management settings for this enrollment profile.' Below this, there are several sections: 'Device management' with radio buttons for 'Android Enterprise' (selected), 'Legacy device administration (not recommended)', and 'Do not manage devices'; 'Device owner mode' with radio buttons for 'Company-owned device', 'Fully managed with work profile', 'Dedicated device' (selected), and 'None'; 'BYOD work profile' with a toggle switch set to 'Off'; 'Application management' with a toggle switch for 'Citrix MAM' set to 'On'; and 'User consent' with a toggle switch for 'Allow users to decline device management' set to 'Off'. Each setting has a help icon (question mark in a circle).

6. **Perfil de trabalho BYOD** permite configurar o perfil de registro para registrar dispositivos BYOD como dispositivos de perfil de trabalho. Dispositivos novos e com redefinição de fábrica são registrados como dispositivos dedicados. Defina **Perfil de trabalho BYOD** como **Ativado** para permitir o registro de dispositivos BYOD como dispositivos de perfil de trabalho. Defina **Perfil de trabalho BYOD** como **Desativado** para restringir o registro a dispositivos de propriedade da empresa. O padrão é **Ativado**.

7. Escolha se deseja registrar dispositivos no Citrix MAM.

8. Se você definir **Perfil de trabalho BYOD** como **Ativado**, configure o consentimento do usuário. Para permitir que os usuários de dispositivos de perfil de trabalho BYOD recusem o gerenciamento do dispositivo ao registrar seus dispositivos, defina **Permitir que os usuários recusem o gerenciamento de dispositivos** como **On**.

Se o **Perfil de trabalho BYOD** estiver definido como **On**, o valor padrão de **Permitir que os usuários recusem o gerenciamento de dispositivos** será **On**. Se o **Perfil de trabalho BYOD** estiver definido como **Off**, **Permitir que os usuários recusem o gerenciamento de dispositivos** será desabilitado.

9. Selecione **Atribuição (opções)**. A tela Atribuição de grupo de entrega é exibida.

10. Escolha um grupo de entrega ou grupos de entrega contendo os administradores que registram dispositivos dedicados. Em seguida, clique em **Save**.

A página de Perfil de registro é exibida com o perfil que você adicionou.

Enrollment profile name	Created on	Updated on	Device limit
Dedicated devices	11/1/19 3:30:36 pm	11/1/19 3:30:36 pm	unlimited
Global	10/28/19 5:30:39 am	10/28/19 5:30:39 am	unlimited

Adicionar um perfil de registro para dispositivos totalmente gerenciados com um perfil de trabalho

1. No console XenMobile, vá para **Configurar > Perfis de registro**.
2. Para adicionar um perfil de registro, clique em **Adicionar**. Na página de Informações de registro, digite um nome para o perfil de registro.
3. Defina o número de dispositivos que os membros com este perfil podem registrar.
4. Selecione **Android** em **Plataformas** ou clique em **Avançar**. A página de configuração de registro é exibida.
5. Defina **Gerenciamento** para **Android Enterprise**. Defina **Modo proprietário do dispositivo** como **Totalmente gerenciado com perfil de trabalho**.

Enrollment Configuration
Specify device management settings for this enrollment profile.

Device management ⓘ

Management

- Android Enterprise ⓘ
- Legacy device administration (not recommended) ⓘ
- Do not manage devices ⓘ

Device owner mode

- Company-owned device ⓘ
- Fully managed with work profile ⓘ
- Dedicated device ⓘ
- None ⓘ

BYOD work profile ⓘ

Application management ⓘ

Citrix MAM ⓘ

User consent

Allow users to decline device management ⓘ

6. **Perfil de trabalho BYOD** permite configurar o perfil de registro para registrar dispositivos BYOD como dispositivos de perfil de trabalho. Dispositivos novos e com redefinição de fábrica são reg-

istrados como dispositivos totalmente gerenciados com um perfil de trabalho. Defina **Perfil de trabalho BYOD** como **Ativado** para permitir o registro de dispositivos BYOD como dispositivos de perfil de trabalho. Defina **Perfil de trabalho BYOD** como **Desativado** para restringir o registro a dispositivos dedicados. O padrão é **Desativado**.

7. Escolha se deseja registrar dispositivos no Citrix MAM.
8. Se você definir **Perfil de trabalho BYOD** como **Ativado**, configure o consentimento do usuário. Para permitir que os usuários de dispositivos de perfil de trabalho BYOD recusem o gerenciamento do dispositivo ao registrar seus dispositivos, defina **Permitir que os usuários recusem o gerenciamento de dispositivos** como **On**.

Se o **Perfil de trabalho BYOD** estiver definido como **On**, o valor padrão de **Permitir que os usuários recusem o gerenciamento de dispositivos** será **On**. Se o **Perfil de trabalho BYOD** estiver definido como **Off**, **Permitir que os usuários recusem o gerenciamento de dispositivos** será desabilitado.
9. Selecione **Atribuição (opções)**. A tela Atribuição de grupo de entrega é exibida.
10. Escolha um grupo de entrega ou grupos de entrega contendo os administradores que registram dispositivos totalmente gerenciados com um perfil de trabalho. Em seguida, clique em **Save**.

A página de Perfil de registro é exibida com o perfil que você adicionou.

Enrollment profile name	Created on	Updated on	Device limit
COPE devices	11/1/19 1:01:51 pm	11/1/19 1:01:51 pm	unlimited
Global	10/28/19 5:30:39 am	10/28/19 5:30:39 am	unlimited

Adicionar um perfil de registro para dispositivos legados

Google preteriu o modo de administrador do dispositivo de gerenciamento de dispositivos. O Google incentiva os clientes a gerenciar todos os dispositivos Android no modo de proprietário do dispositivo ou no modo de proprietário do perfil. (Consulte [Device admin deprecation](#) nos guias do desenvolvedor do Google Android Enterprise.)

Para dar suporte a essa alteração:

- A Citrix torna o Android Enterprise a opção de registro padrão para dispositivos Android.

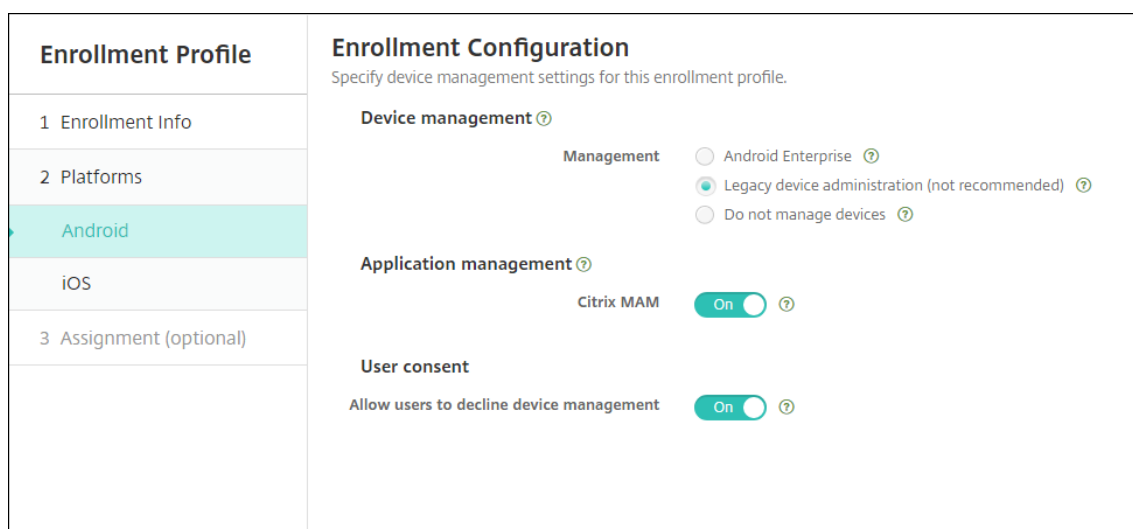
- Se o Android Enterprise estiver habilitado para sua implantação do XenMobile, todos os dispositivos Android recém-registrados ou registrados novamente serão registrados como dispositivos Android Enterprise.

Sua organização pode não estar pronta para começar a gerenciar dispositivos Android legados usando o Android Enterprise. Nesse caso, você pode continuar gerenciando-os no modo de administrador do dispositivo. Para dispositivos já registrados no modo de administrador de dispositivos, o XenMobile continua a gerenciá-los no modo de administrador de dispositivos.

Crie um perfil de registro para dispositivos legados para permitir que novos registros de dispositivos Android usem o modo de administrador de dispositivos.

Para criar um perfil de registro para dispositivos legados:

1. No console XenMobile, vá para **Configurar > Perfis de registro**.
2. Para adicionar um perfil de registro, clique em **Adicionar**. Na página de Informações de registro, digite um nome para o perfil de registro.
3. Defina o número de dispositivos que os membros com este perfil podem registrar.
4. Selecione **Android** em **Plataformas** ou clique em **Avançar**. A página de configuração de registro é exibida.
5. Defina **Gerenciamento** para **Administração de dispositivos herdados (não recomendado)**. Clique em **Next**.



6. Escolha se deseja registrar dispositivos no Citrix MAM.
7. Para permitir que os usuários recusem o gerenciamento do dispositivo ao registrar seus dispositivos, defina **Permitir que os usuários recusem o gerenciamento de dispositivos** como **Ativado**. O padrão é **Ativado**.
8. Selecione **Atribuição (opções)**. A tela Atribuição de grupo de entrega é exibida.

- Escolha um grupo de entrega ou grupos de entrega contendo os administradores que registram dispositivos dedicados. Em seguida, clique em **Save**.

A página de Perfil de registro é exibida com o perfil que você adicionou.

<input type="checkbox"/>	Enrollment profile name	Created on	Updated on	Device limit
<input type="checkbox"/>	Android legacy (DA) devices	11/19/19 1:41:54 pm	11/19/19 1:41:54 pm	unlimited
<input type="checkbox"/>	Global	3/7/18 4:08:24 pm	3/7/18 4:08:24 pm	unlimited

Para continuar a gerenciar um dispositivo legado no modo de administrador de dispositivos, registre-o ou registre-o novamente utilizando este perfil. Você registra dispositivos de administrador de dispositivos de modo similar aos dispositivos de perfil de trabalho, fazendo com que os usuários baixem o Secure Hub e fornecendo um URL do servidor de registro.

Provisionar dispositivos de perfil de trabalho Android Enterprise

Os dispositivos de perfil de trabalho Android Enterprise são registrados no modo de proprietário do perfil. Esses dispositivos não precisam ser novos ou com redefinição de fábrica. Os dispositivos BYOD são registrados como dispositivos de perfil de trabalho. A experiência de registro é semelhante ao registro do Android no XenMobile. Os usuários fazem o download do Secure Hub a partir do Google Play e registram seus dispositivos.

Por padrão, as configurações de **Depuração de USB e Fontes desconhecidas** são desativadas em um dispositivo quando ele é registrado no Android Enterprise como um dispositivo de perfil de trabalho.

Quando for registrar dispositivos no Android Enterprise como dispositivos de perfil de trabalho, sempre vá para o Google Play. A partir dali, habilite o Secure Hub para aparecer no perfil pessoal do usuário.

Provisionamento de dispositivos Android Enterprise totalmente gerenciados

Você pode registrar dispositivos totalmente gerenciados na implantação configurada nas seções anteriores. Dispositivos totalmente gerenciados são dispositivos de propriedade da empresa e estão registrados no modo proprietário do dispositivo. Somente dispositivos novos ou redefinidos de fábrica podem ser registrados no modo proprietário do dispositivo.

Você pode registrar dispositivos no modo proprietário do dispositivo usando qualquer um destes métodos de registro:

- **Token identificador DPC:** com esse método de registro, os usuários inserem os caracteres `afw##xenmobile` ao configurar o dispositivo. `afw##xenmobile` é o token identificador Citrix DPC. Esse token identifica o dispositivo como gerenciado pelo XenMobile e baixa o Secure Hub da loja Google Play. Consulte Registrar dispositivos usando o token identificador Citrix DPC.
- **Near field communication (NFC) bump:** o método de registro de colisão NFC transfere dados entre dois dispositivos usando comunicação a curta distância. Bluetooth, Wi-Fi e outros meios de comunicação estão desativados em um dispositivo que sofreu uma redefinição de fábrica ou novo. O NFC é o único protocolo de comunicação que o dispositivo pode usar nesse estado. Consulte Registrar dispositivos com NFC bump.
- **Código QR:** o registro de código QR pode ser usado para registrar uma frota distribuída de dispositivos que não suportam NFC, como tablets. O método de registro de código QR instala e configura o modo de perfil de dispositivo digitalizando um código QR no Assistente de instalação. Consulte Registrar dispositivos usando um código QR.
- **Sem toque:** o registro sem toque permite que você configure dispositivos para se registrarem automaticamente quando eles são ligados pela primeira vez. O registro sem toque é suportado em alguns dispositivos Android que executam o Android 8.0 ou posterior. Consulte Registro sem toque.
- **Contas do Google:** os usuários inserem suas credenciais da Conta do Google para iniciar o processo de provisionamento. Essa opção é para empresas que usam o Google Workspace.

Registrar dispositivos usando o token identificador Citrix DPC

Os usuários inserem `afw##xenmobile` quando solicitados a inserir uma conta do Google depois de ligarem dispositivos novos ou redefinidos de fábrica para instalação inicial. Essa ação baixa e instala o Secure Hub. Os usuários seguem os prompts de configuração do Secure Hub para concluir o registro.

Esse método de registro é recomendado para a maioria dos clientes, porque a versão mais recente do Secure Hub é baixada da loja Google Play. Ao contrário de outros métodos de registro, você não fornece o Secure Hub para download no servidor XenMobile Server.

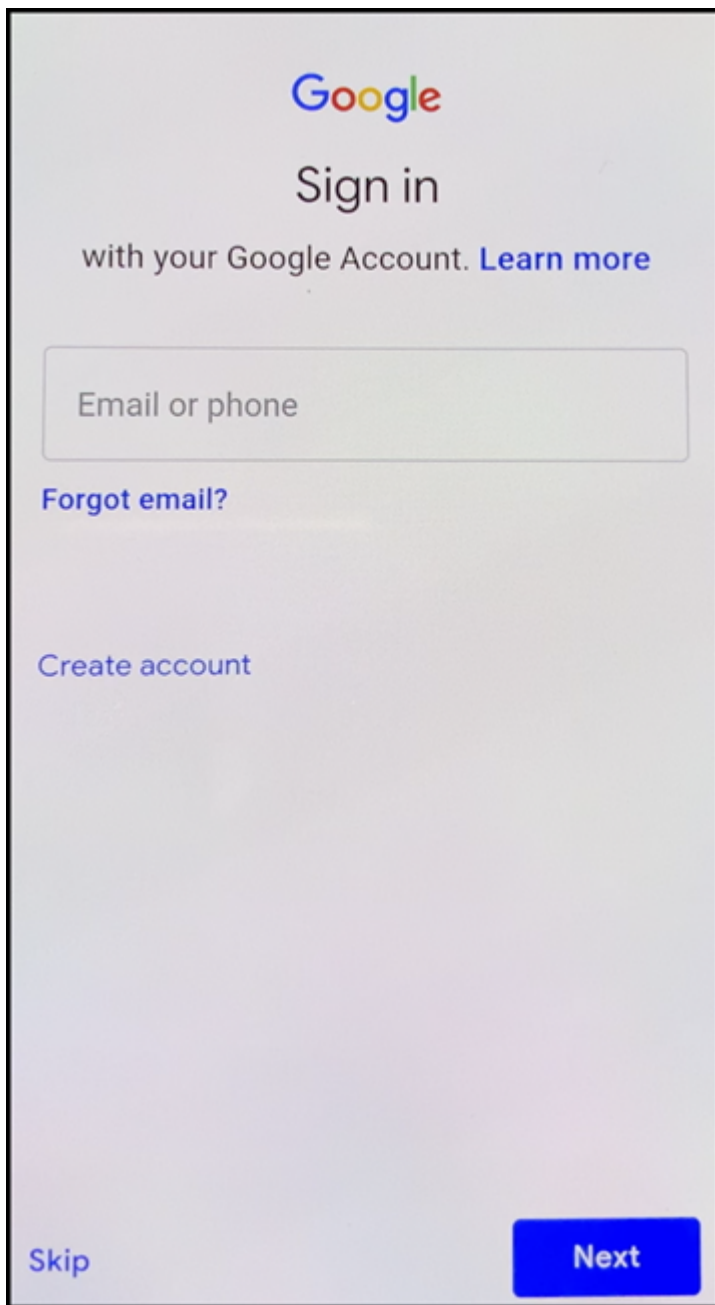
Requisitos do sistema

- Suportado em todos os dispositivos Android que executam o sistema operacional Android.

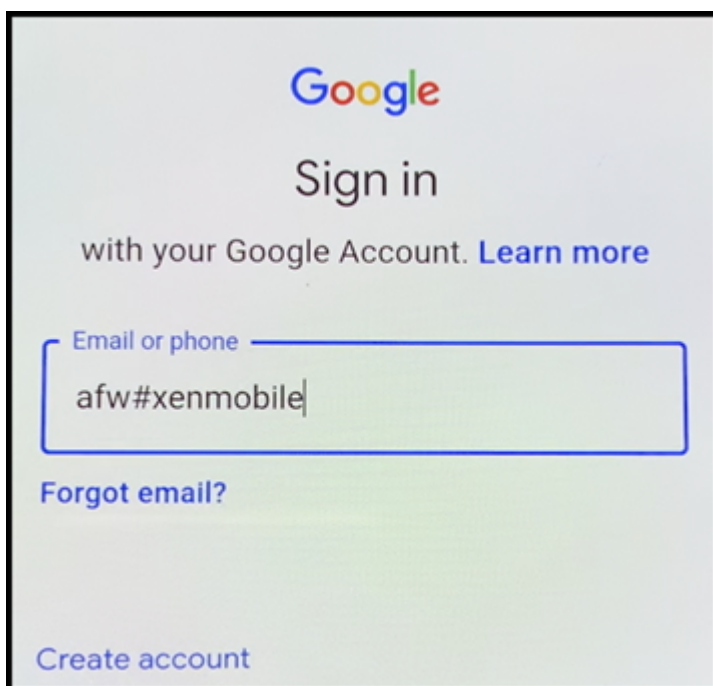
Para registrar o dispositivo

1. Ligue um dispositivo novo ou redefinido de fábrica.

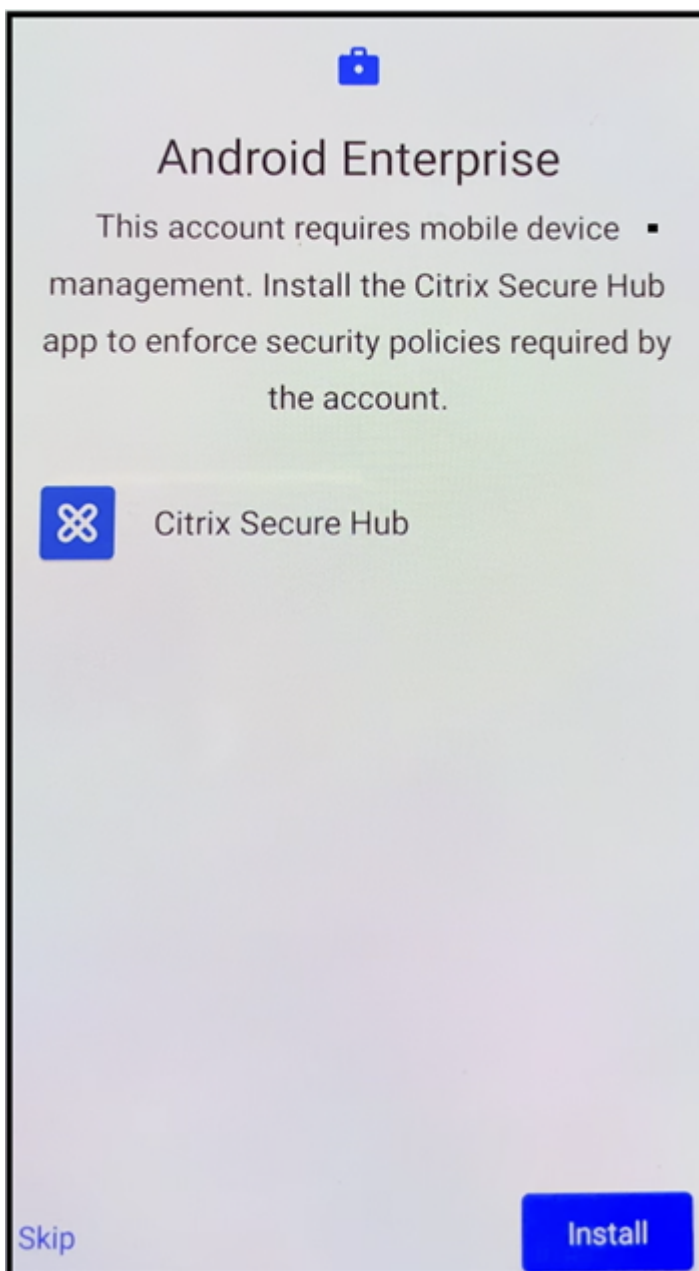
2. A instalação inicial do dispositivo é carregada e solicita uma conta do Google. Se o dispositivo carregar a tela inicial do dispositivo, verifique se há na barra de notificação uma notificação **Concluir instalação**.



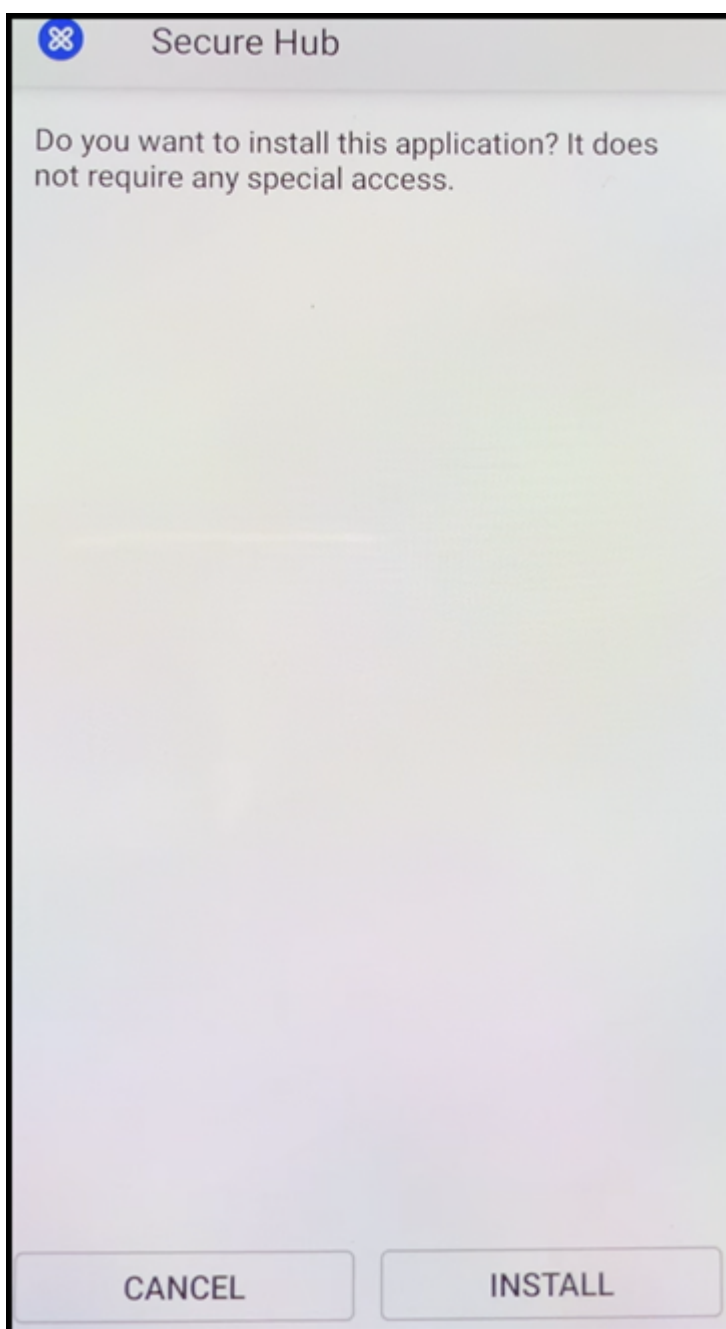
3. Digite `afw##xenmobile` no campo **E-mail ou telefone**.



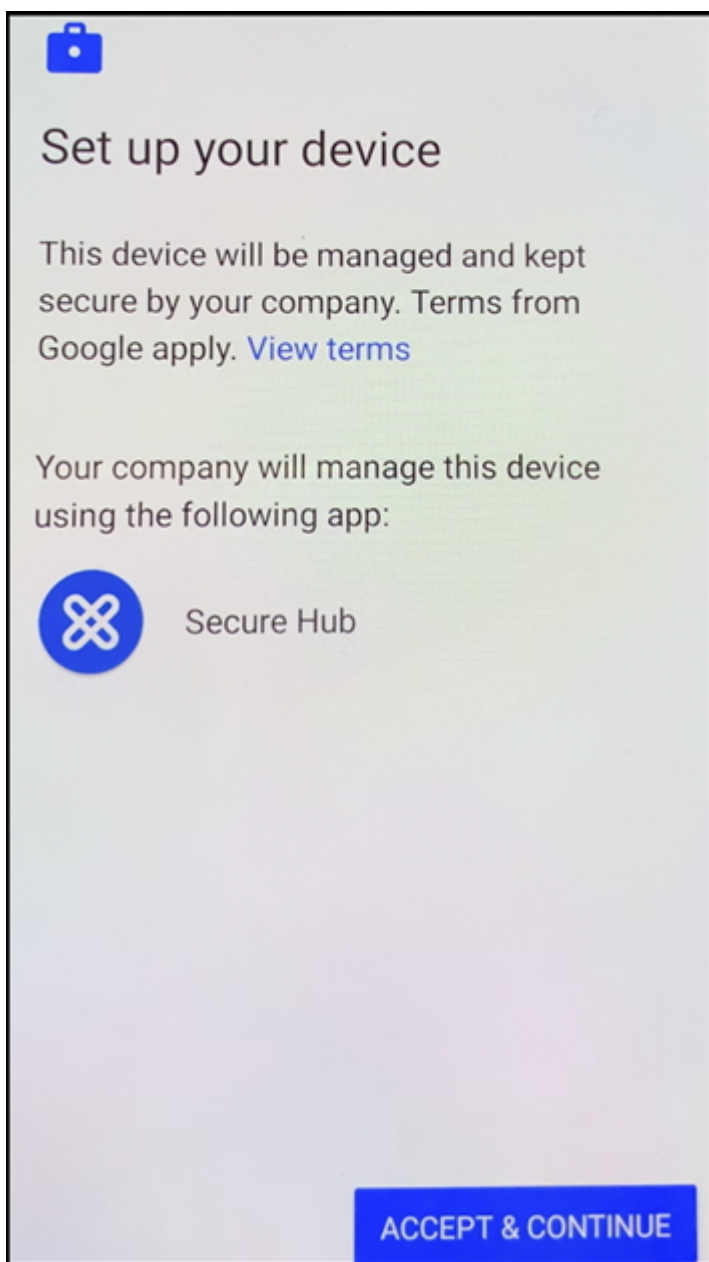
4. Toque em **Instalar** na tela do Android Enterprise solicitando a instalação do Secure Hub.



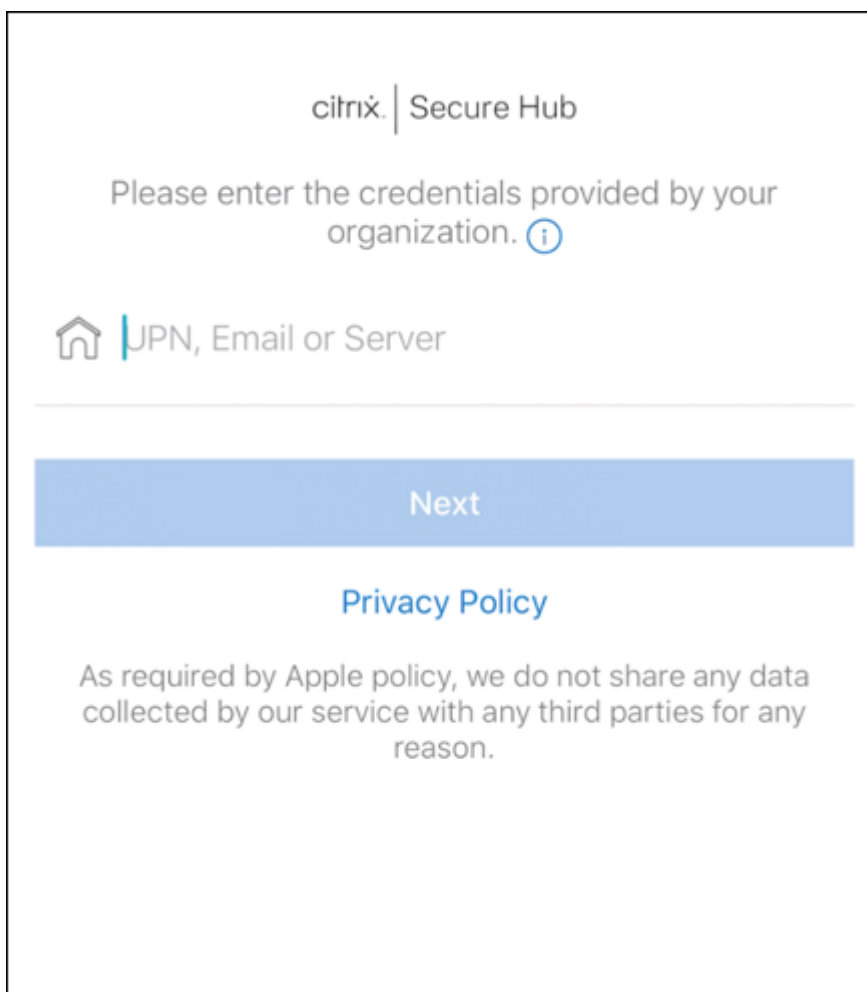
5. Toque em **Instalar** na tela do instalador do Secure Hub.



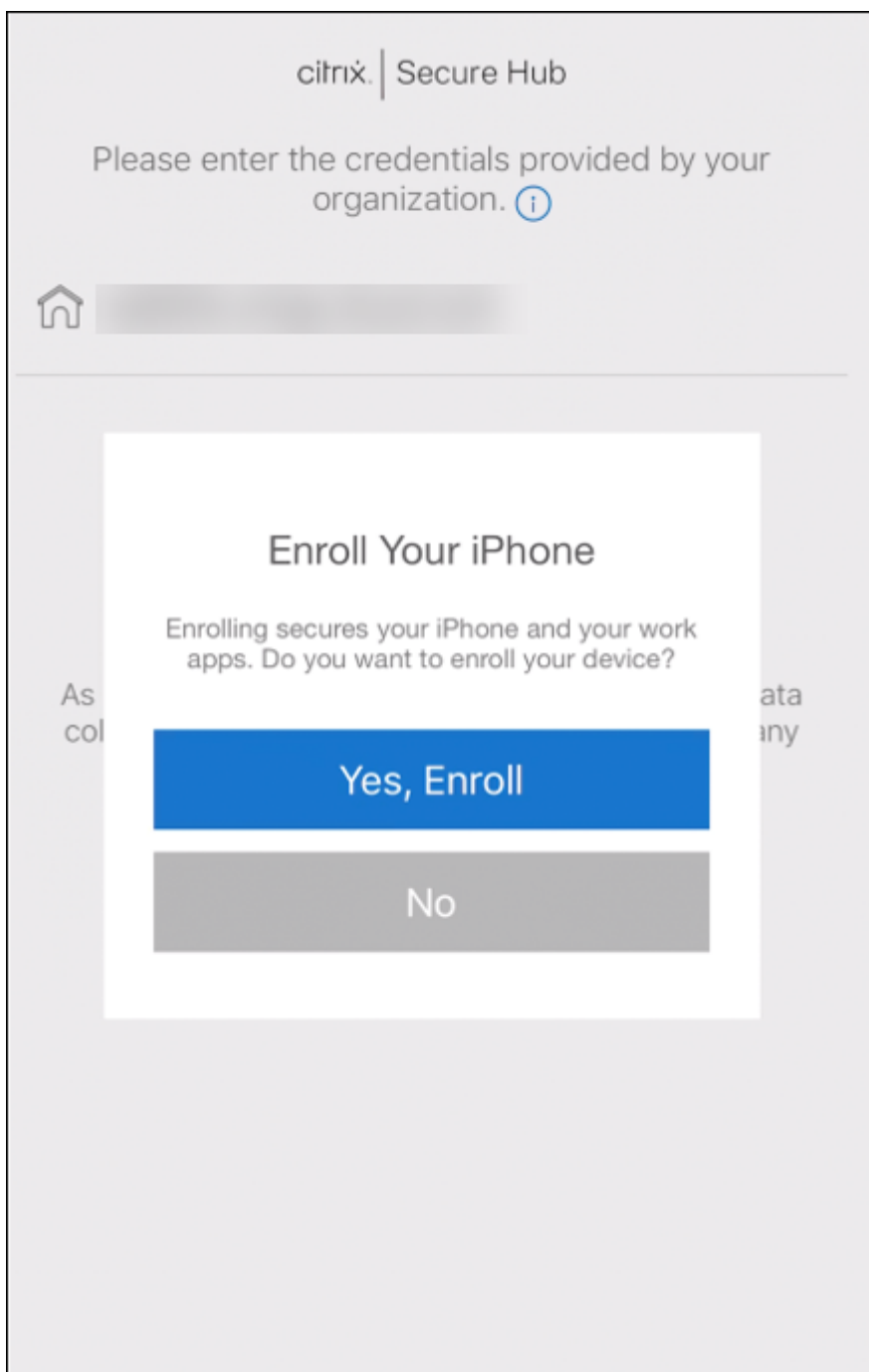
6. Toque em **Permitir** para todas as solicitações de permissão do aplicativo.
7. Toque em **Aceitar e continuar** para instalar o Secure Hub e permitir que ele gerencie o dispositivo.



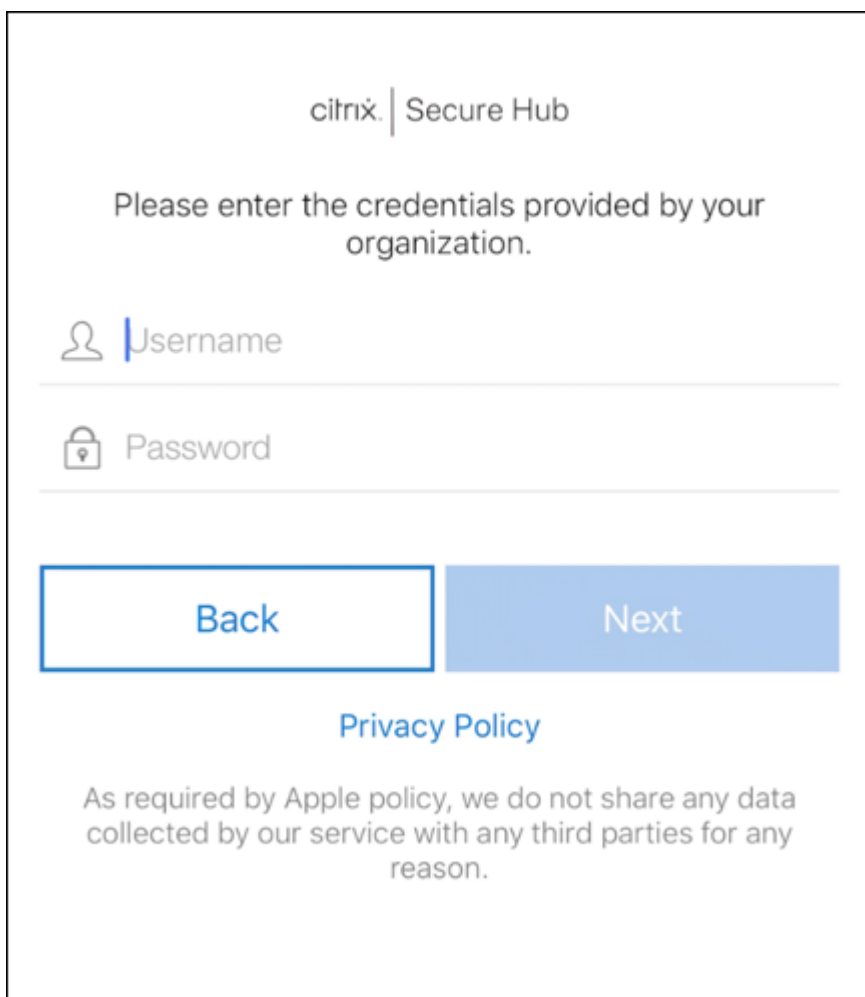
8. O Secure Hub agora está instalado e na tela de registro padrão. Neste exemplo, AutoDiscovery não está configurado. Se estivesse, o usuário poderá inserir seu nome de usuário/e-mail e um servidor será encontrado para ele. Em vez disso, insira a URL de registro do ambiente e toque em **Avançar**.



9. A configuração padrão do XenMobile permite que os usuários escolham se usarão MAM ou MDM+MAM. Se solicitado dessa forma, toque em **Sim, registrar** para escolher MDM+MAM.





10. Insira o nome de usuário e a senha e, em seguida, toque em **Avançar**.



citrix | Secure Hub

Please enter the credentials provided by your organization.

 Username

 Password

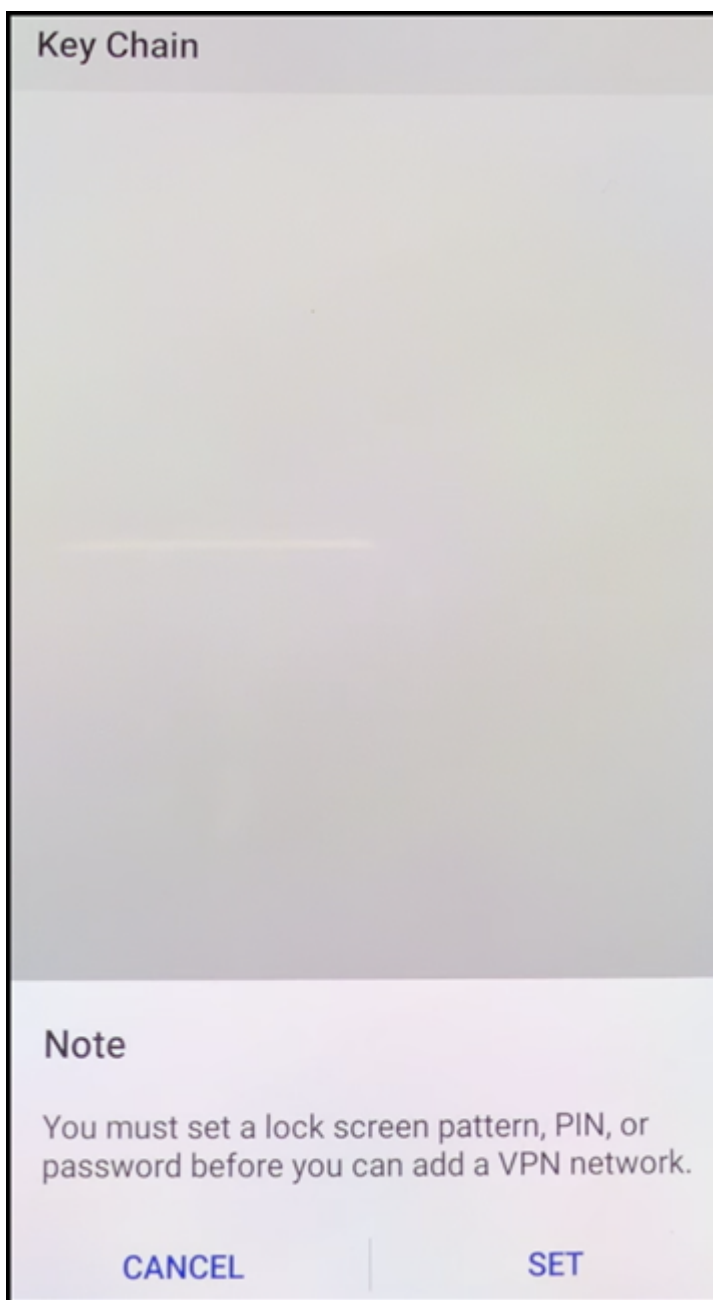
Back

Next

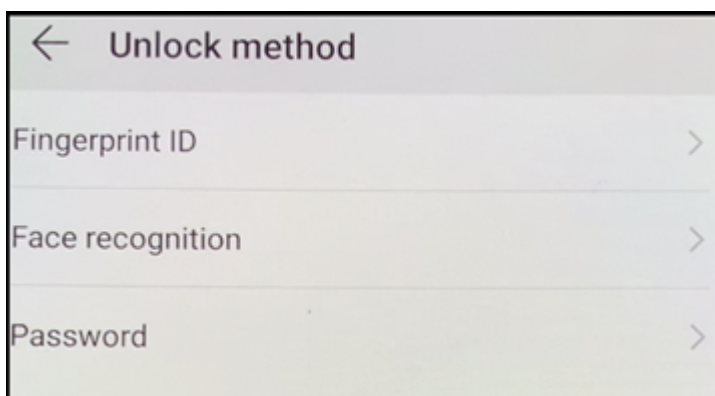
[Privacy Policy](#)

As required by Apple policy, we do not share any data collected by our service with any third parties for any reason.

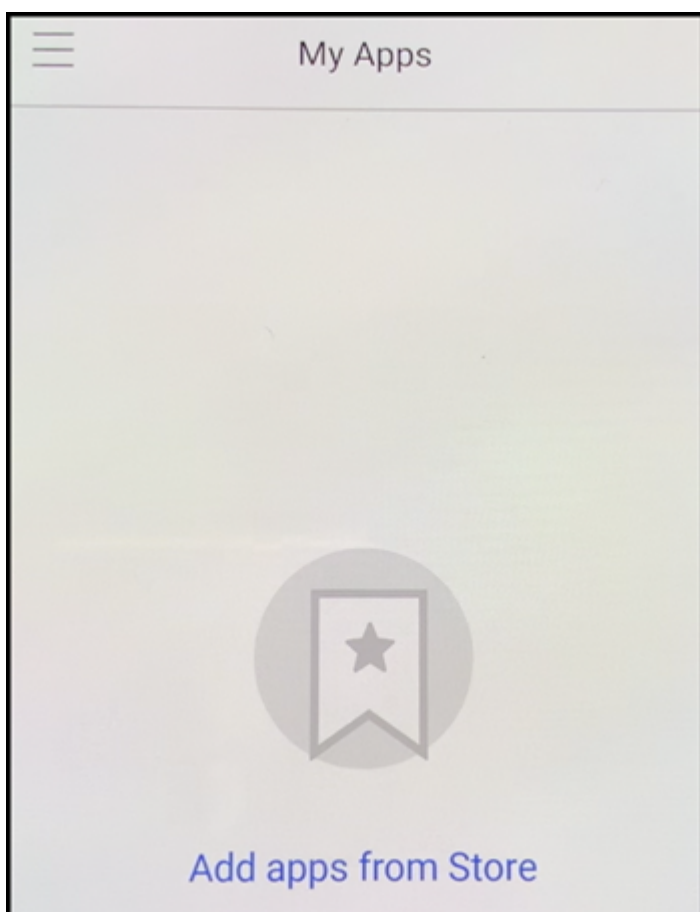
11. O usuário é solicitado a configurar o código secreto do dispositivo. Toque em **Definir** e insira um código secreto.



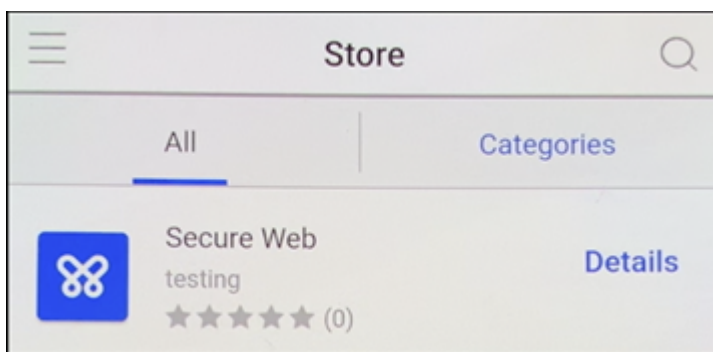
12. O usuário é solicitado a configurar um método de desbloqueio do perfil de trabalho. Para este exemplo, toque em **Senha**, toque em **PIN** e digite um PIN.



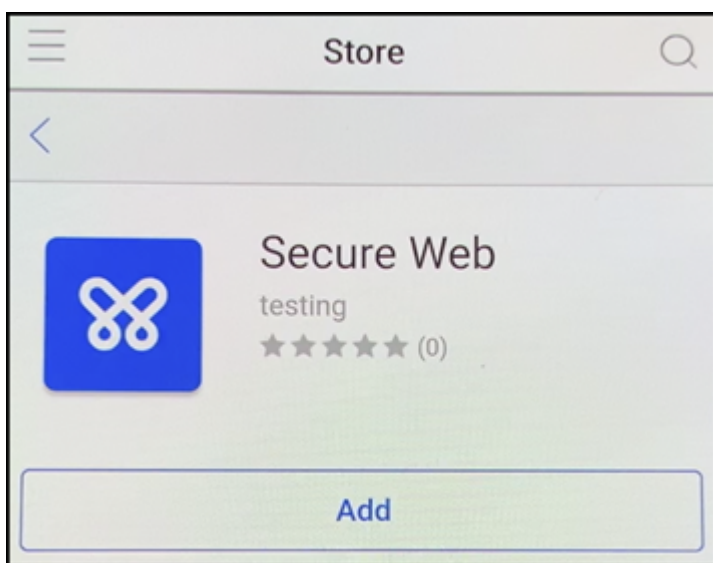
13. O dispositivo está agora na tela inicial **Meus aplicativos** do Secure Hub. Toque em **Adicionar aplicações da loja**.



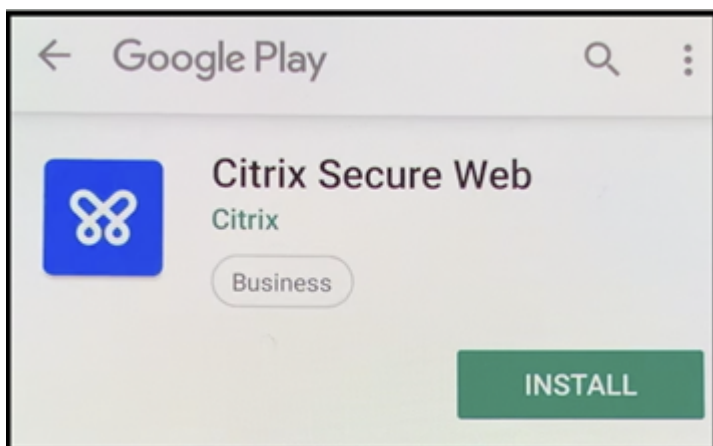
14. Para adicionar o Secure Web, toque em **Secure Web**.



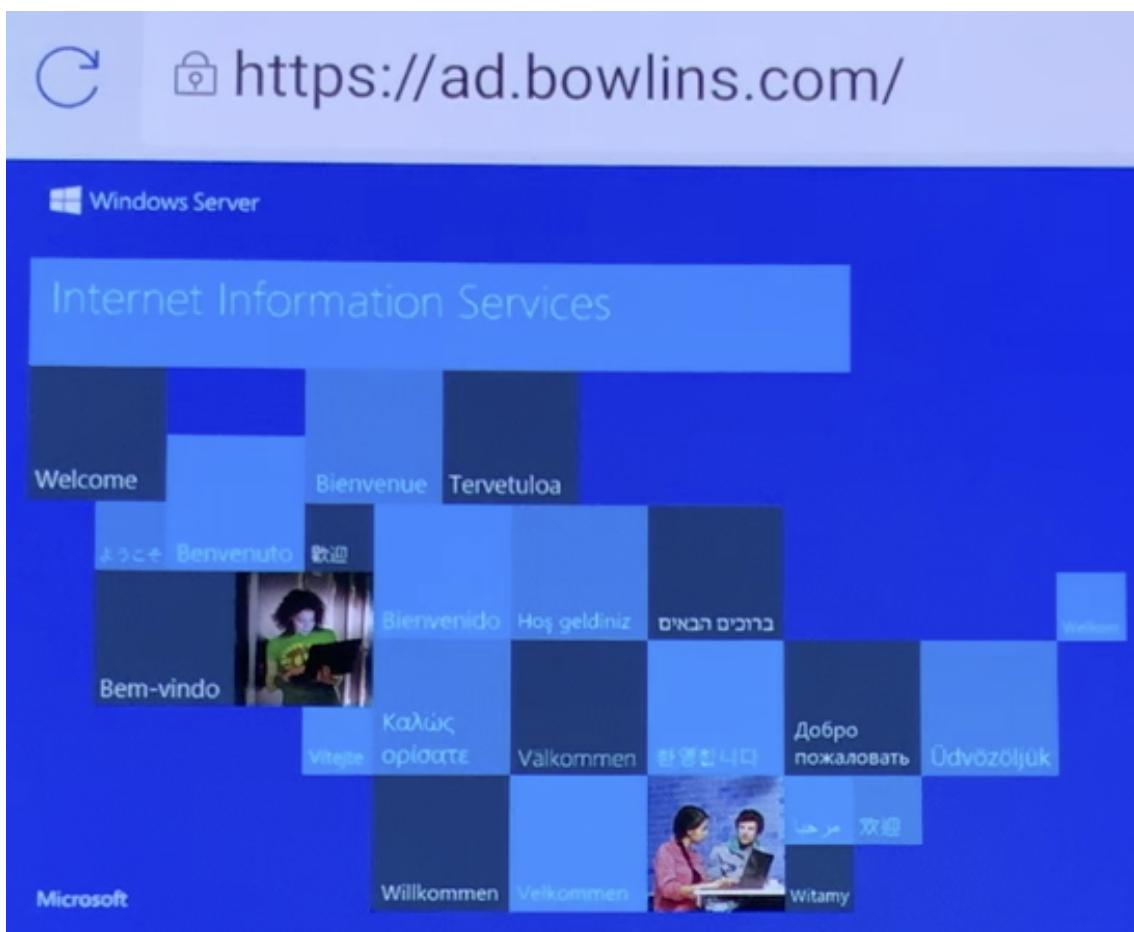
15. Toque em **Adicionar**.



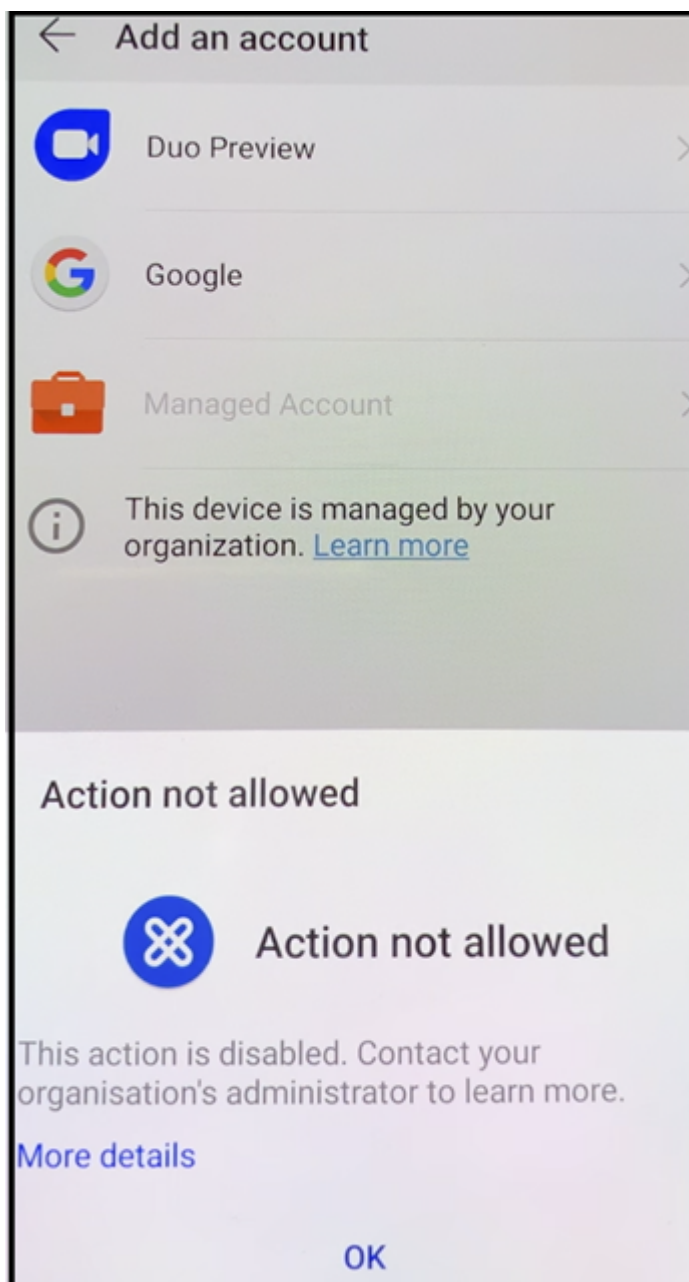
16. O Secure Hub direciona o usuário para o Google Play Store para instalar o Secure Web. Toque em **Instalar**.



17. Depois que o Secure Web for instalado, toque em **Abrir**. Insira a URL de um site interno na barra de endereços e verifique se a página é carregada.



18. Vá para **Configurações > Contas** no dispositivo. Observe que a **conta gerenciada** não pode ser modificada. As opções do desenvolvedor para compartilhamento de tela ou depuração remota também são bloqueadas.



Registrar dispositivos com NFC bump

Registrar um dispositivo como um dispositivo totalmente gerenciado usando compartilhamentos por NFC requer dois dispositivos: um cujas configurações de fábrica sejam redefinidas e um que esteja executando a XenMobile Provisioning Tool.

Requisitos do sistema e pré-requisito

- Dispositivos Android com suporte.

- Um dispositivo novo ou com redefinição de fábrica, provisionado para o Android Enterprise como um dispositivo totalmente gerenciado. Você pode encontrar as etapas para concluir esse pré-requisito neste artigo.
- Outro dispositivo com recursos NFC executando a Provisioning Tool configurada. A Provisioning Tool está disponível no Secure Hub ou na [página de downloads da Citrix](#).

Cada dispositivo pode ter apenas um perfil Android Enterprise gerenciado do Secure Hub. Somente um perfil é permitido em cada dispositivo. A tentativa de adicionar um segundo aplicativo DPC remove o Secure Hub instalado.

Dados transferidos através do aumento de NFC

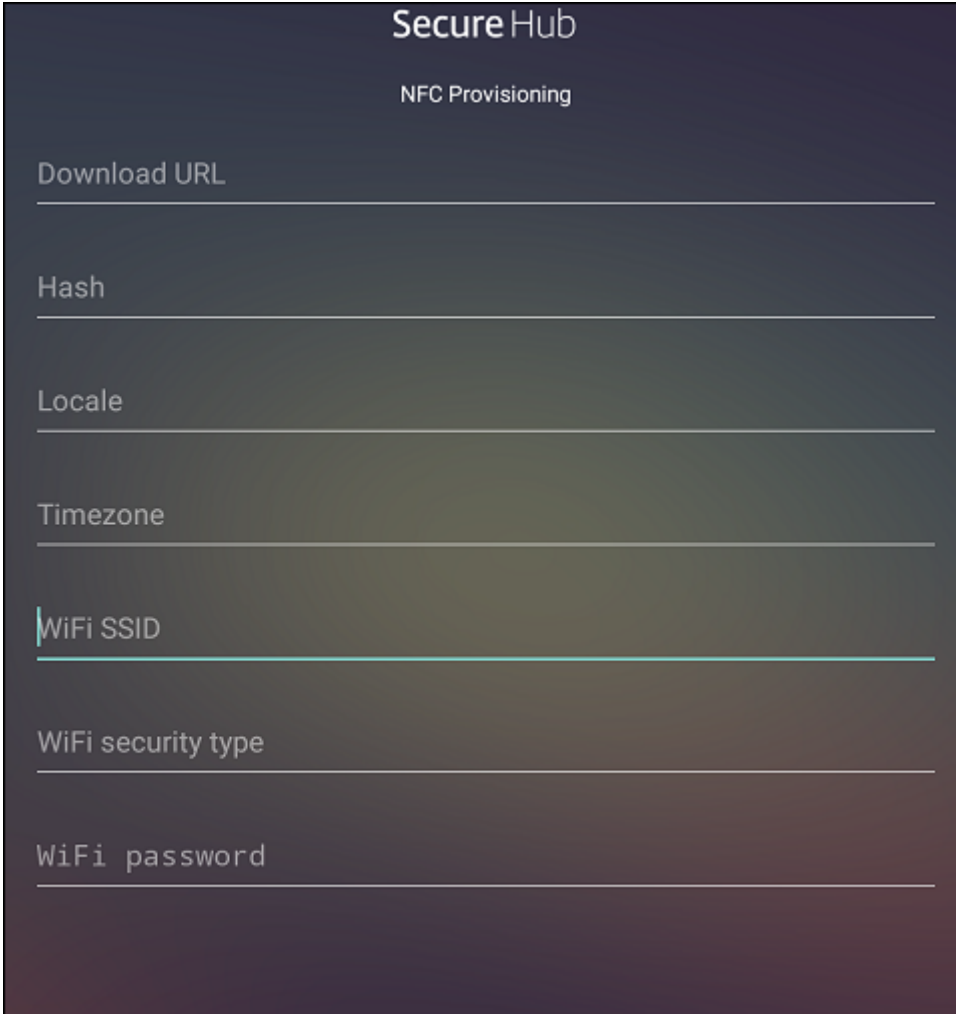
Provisionar um dispositivo com redefinição de fábrica requer que você envie os seguintes dados por meio de um NFC bump para inicializar o Android Enterprise:

- O nome do pacote do aplicativo DPC que atua como o proprietário do dispositivo (neste caso, o Secure Hub).
- A localização de Intranet/Internet da qual o dispositivo pode baixar o aplicativo DPC.
- O hash SHA1 do aplicativo DPC para verificar se o download é bem-sucedido.
- Os detalhes da conexão WiFi para que um dispositivo com redefinição de fábrica possa se conectar e baixar o aplicativo DPC. Nota: no momento, o Android não é compatível com WiFi 802.1x para esta etapa.
- O fuso horário do dispositivo (opcional).
- A localização geográfica do dispositivo (opcional).

Quando os dois dispositivos são aumentados, os dados da Provisioning Tool são enviados para o dispositivo com redefinição de fábrica. Esses dados são usados para baixar o Secure Hub com as configurações do administrador. Se você não inserir os valores de localização e fuso horário, o Android os configura automaticamente no novo dispositivo.

Configuração da XenMobile Provisioning Tool

Antes de realizar um aumento de NFC, você deve configurar a Provisioning Tool. Em seguida, essa configuração é transferida para o dispositivo com redefinição de fábrica durante o aumento de NFC.



The screenshot shows the 'Secure Hub' interface for 'NFC Provisioning'. It features a dark background with white text. The title 'Secure Hub' is at the top, followed by 'NFC Provisioning'. Below are seven input fields, each with a label and a horizontal line for text entry: 'Download URL', 'Hash', 'Locale', 'Timezone', 'WiFi SSID', 'WiFi security type', and 'WiFi password'. The 'WiFi SSID' field has a blue cursor at the start.

Você pode digitar dados nos campos obrigatórios ou preenchê-los usando um arquivo de texto. As etapas no procedimento a seguir descrevem como configurar o arquivo de texto e contém descrições para cada campo. O aplicativo não salva as informações depois que as digitar, portanto, convém criar um arquivo de texto para manter as informações para uso futuro.

Para configurar a Provisioning Tool usando um arquivo de texto

Dê ao arquivo o nome `ncfprovisioning.txt` e coloque-o na pasta `/sdcard/` no cartão SD do dispositivo. Em seguida, o aplicativo poderá ler o arquivo de texto e preencher os valores.

O arquivo de texto deve conter os seguintes dados:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<
download_location>
```

Essa linha é o local da intranet/internet do aplicativo do provedor EMM. Depois que o dispositivo com redefinição de fábrica se conectar a Wi-Fi em seguida ao aumento de NFC, o dispositivo deve ter

acesso a esse local para fazer o download. A URL é uma URL regular, sem necessidade de formatação especial.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA1 hash>
```

Essa linha é a soma de verificação do aplicativo do provedor EMM. Essa soma de verificação é usada para verificar se o download foi bem-sucedido. As etapas para obter a soma de verificação são discutidas neste artigo.

```
android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>
```

Esse é o SSID de Wi-Fi conectado do dispositivo no qual a Provisioning Tool está em execução.

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>
```

Os valores suportados são WEP e WPA2. Se o Wi-Fi for desprotegido, esse campo deverá estar vazio.

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>
```

Se o Wi-Fi for desprotegido, esse campo deverá estar vazio.

```
android.app.extra.PROVISIONING_LOCALE=<locale>
```

Insira os códigos de idioma e país. Os códigos de idioma são códigos de idioma ISO com duas letras minúsculas (por exemplo, en), conforme definido pela [ISO 639-1](#). Os códigos de país são códigos de país ISO com duas letras maiúsculas (por exemplo, US), conforme definido pela [ISO 3166-1](#). Por exemplo, digite en_US para o inglês falado nos Estados Unidos. Se você não digitar nenhum código, o país e o idioma serão preenchidos automaticamente.

```
android.app.extra.PROVISIONING_TIME_ZONE=<timezone>
```

O fuso horário no qual o dispositivo está em execução. Insira um [nome Olson da área/localização do formulário](#). Por exemplo, America/Los_Angeles para o horário do Pacífico. Se você não inserir nenhum nome, o fuso horário será preenchido automaticamente.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>
```

Isso não é necessário, pois o valor é inserido em código fixo no aplicativo, como o Secure Hub. Ele é mencionado aqui somente por uma questão de conclusão.

Se houver um Wi-Fi protegido por WPA2, um arquivo nfcprovisioning.txt preenchido terá a seguinte aparência:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk
```

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFk4Crh\nu003d
```

```
android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name
```

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2
```

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere
```

```
android.app.extra.PROVISIONING_LOCALE=en_US
```

```
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Se houver uma Wi-Fi desprotegida, um arquivo `nfcprovisioning.txt` preenchido terá a seguinte aparência:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk
```

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crh\u003d
```

```
android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name
```

```
android.app.extra.PROVISIONING_LOCALE=en_US
```

```
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Para obter a soma de verificação do Citrix Secure Hub

A soma de verificação do Secure Hub é um valor constante: `qn7oZUtheu3JBAinzZRrjCQv6L006Ll10jcxT3-yKM`. Para baixar um arquivo APK para o Secure Hub, use o seguinte link da loja do Google Play: <https://play.google.com/managed/downloadManagingApp?identifier=xenmobile>.

Para obter uma soma de verificação de aplicativo

Pré-requisitos:

- A ferramenta **apksigner** do Android SDK Build Tools
- Linha de comando OpenSSL

Para obter a soma de verificação de qualquer aplicativo, siga estas etapas:

Baixe o arquivo APK do aplicativo na loja do Google Play.

Na linha de comando OpenSSL, navegue até a ferramenta **apksigner**: `android-sdk/build-tools/<version>/apksigner` e digite o seguinte:

```
1 apksigner verify -print-certs <apk_path> | perl -nle 'print
2
3
4
5
6
7
8
```

9 [Android Enterprise | Versão atual do XenMobile Server](#)

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

[This content has been machine translated dynamically.](#)

54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95

[Give feedback here](#)

[Thank you for the feedback](#)

XenMobile
Versão atual do XenMobile Server

This content has been machine translated dynamically.
Dieser Inhalt ist eine maschinelle Übersetzung, die dynamisch erstellt wurde. (Haftungsausschluss)
Cet article a été traduit automatiquement de manière dynamique. (Clause de non responsabilité)
Este artículo lo ha traducido una máquina de forma dinámica. (Aviso legal)
此内容已动态机器翻译。 放弃
このコンテンツは動的に機械翻訳されています。 免責事項

96 This content has been machine translated dynamically.
97 This content has been machine translated dynamically.
98 This content has been machine translated dynamically.
99
100 This article has been machine translated.
101 Dieser Artikel wurde maschinell übersetzt. (
Haftungsausschluss)
102 Ce article a été traduit automatiquement. (Clause de
non responsabilité)
103 Este artículo ha sido traducido automáticamente. (Aviso
legal)
104 この記事は機械翻訳されています。免責事項
105 이 기사는 기계 번역되었습니다.
106 Este artigo foi traduzido automaticamente.
107 这篇文章已经过机器翻译。放弃
108
109
110
111
112
113
114 Switch to english
115 Auf Englisch anzeigen
116 Lire en anglais
117 Leer en inglés
118 英語に切り替え
119 영어로 전환
120 Mudar para ingles
121 切换到英文
122
123
124
125
126
127
128
129
130 Translation failed!
131
132
133
134
135
136
137

138

139

Android Enterprise

140

141

142

143

144

145

146

August 20, 2021

147

148

Contribuíram por:

149

150

151

152

153

C

154

155

156

157

158

159

G

160

161

162

163

164

165

166

Android Enterprise é um conjunto de ferramentas e serviços fornecidos pelo Google como uma solução de gerenciamento corporativo para dispositivos Android. Com o Android Enterprise:

167

168

169

170

Você usa o XenMobile para gerenciar dispositivos Android de propriedade da empresa e dispositivos Android BYOD (o seu próprio).

171

172

173

Você pode gerenciar todo o dispositivo ou um perfil separado no dispositivo. O perfil separado isola contas, aplicativos e dados comerciais de contas, aplicativos e dados pessoais.

174

175

176 Você também pode gerenciar dispositivos dedicados a um único uso,
 como gerenciamento de inventário. Para obter uma visão geral dos
 recursos do Android Enterprise do Google, consulte [Android
Enterprise Management](#).

177

178

179

180 **Recursos:**

181

182

183

184 Para obter uma lista de termos e definições relacionados ao Android
 Enterprise, consulte a terminologia do Android Enterprise no
 [guia de desenvolvedores do Google Android Enterprise](#). O Google
 atualiza estes termos com frequência.

185

186

187 Para sistemas operacionais Android compatíveis com o XenMobile,
 consulte [Sistemas operacionais compatíveis de dispositivos](#).

188

189

190 Para obter informações sobre as conexões de saída a serem
 consideradas ao configurar ambientes de rede para o Android
 Enterprise, consulte o artigo de suporte do Google, [Android
Enterprise Network Requirements](#).

191

192

193

194 Ao integrar o XenMobile com o Google Play gerenciado para usar o
 Android Enterprise, você cria uma empresa. O Google define uma
 empresa como um vínculo entre a organização e sua solução de
 gerenciamento móvel corporativo (EMM). Todos os usuários e
 dispositivos que a organização gerencia através de sua solução
 pertencem à sua empresa.

195

196 Uma empresa para Android Enterprise tem três componentes: uma solução
 EMM, um aplicativo DPC (Device Policy Controller) e uma plataforma
 de aplicativos empresariais do Google. Quando você integra o
 XenMobile com o Android Enterprise, a solução completa possui os
 seguintes componentes:

197

198

199

200 **XenMobile:** o Citrix EMM. O XenMobile é a solução XenMobile unificada

para um espaço de trabalho digital seguro. O XenMobile fornece os meios para que os administradores de TI gerenciem dispositivos e aplicativos para suas organizações.

201

202 Citrix Secure Hub: o aplicativo Citrix DPC. O Secure Hub é a
plataforma de lançamento para XenMobile. O Secure Hub impõe polí-
ticas no dispositivo.

203

204 Google Play gerenciado: uma plataforma de aplicativos empresariais do
Google que se integra ao XenMobile. A API EMM do Google Play define
políticas de aplicativo e distribui o aplicativo.

205

206

207 Esta ilustração mostra como os administradores interagem com esses
componentes e como os componentes interagem entre si:

208

209

210

211

212 Usar o Google Play gerenciado com o XenMobile

213

214

215 **Nota:**

216

217 Você pode usar o Google Play gerenciado ou o Google Workspace para
registrar o Citrix como seu provedor de EMM. Este artigo aborda o
uso do Android Enterprise com o Google Play gerenciado. Se a sua
organização usa o Google Workspace para fornecer acesso a
aplicativos, você pode usá-lo com o Android Enterprise. Consulte
Clientes do Android Enterprise herdado para Google Workspace (
anteriormente G Suite).

218

219

220 Quando você usa o Google Play gerenciado, você provisiona contas do
Google Play gerenciado para dispositivos e usuários finais. As
contas do Google Play gerenciado fornecem acesso ao Google Play
gerenciado, permitindo que os usuários instalem e usem os
aplicativos que você disponibilizar. Se a sua organização usa um
serviço de identidade de terceiros, você pode vincular contas do
Google Play gerenciado às suas contas de identidade existentes.

221

222 Como esse tipo de empresa não está vinculado a um domínio, você pode
criar mais de uma empresa para uma única organização. Por exemplo,
cada departamento ou região de uma organização pode se registrar
como uma empresa diferente para gerenciar conjuntos separados de

dispositivos e aplicativos.

223

224 Para administradores XenMobile, o Google Play gerenciado combina a experiência do usuário e os recursos da loja de aplicativos do Google Play com um conjunto de recursos de gerenciamento projetados para empresas. Você pode usar o Google Play gerenciado para adicionar, comprar e aprovar aplicativos para implantação no espaço de trabalho do Android Enterprise em um dispositivo. Você pode usar o Google Play para implantar aplicativos públicos, aplicativos privados e aplicativos de terceiros.

225

226 Para usuários de dispositivos gerenciados, o Google Play gerenciado é a loja de aplicativos empresariais. Os usuários podem procurar aplicativos, visualizar detalhes do aplicativo e instalá-los. Ao contrário da versão pública do Google Play, os usuários só podem instalar aplicativos do Google Play gerenciado que você disponibilizar para eles.

227

228

229 Cenários de implantação de dispositivos e modos de operação

230

231 O cenário de implantação do dispositivo refere-se a quem possui os dispositivos implantados e como você os gerencia. Os perfis de dispositivos referem-se a como o DPC gerencia e impõe políticas aos dispositivos.

232

233 Um perfil de trabalho isola contas, aplicativos e dados comerciais de contas, aplicativos e dados pessoais. Para obter mais detalhes sobre perfis de trabalho, consulte o tópico de ajuda do Google Android Enterprise, *What is a work profile*.

234

235

236 **Importante:**

237

238 Quando os dispositivos Android Enterprise atualizam para o Android 11, o Google migrará os dispositivos gerenciados como “totalmente gerenciados com um perfil de trabalho” para uma nova experiência de perfil de trabalho com segurança aprimorada. Para obter mais informações, consulte *Alterações à frente para o perfil de trabalho totalmente gerenciado com o Android Enterprise*.

239

240

241

242

243

Casos de uso

Perfil de trabalho

Perfil pessoal

Observações

Dispositivos de propriedade da empresa (totalmente gerenciados)

Dispositivos de propriedade da empresa destinados apenas ao trabalho

Não

Sim. O DPC pode executar ações em todo o dispositivo, como configurar conectividade em todo o dispositivo, configurar configurações globais e executar uma redefinição de fábrica.

Apenas para dispositivos novos ou com redefinição de fábrica.

Totalmente gerenciado com um perfil de trabalho

Dispositivos de propriedade da empresa destinados a uso pessoal e profissional

Sim

Sim. Duas cópias do DPC são executadas nesses dispositivos: uma gerencia o dispositivo no modo proprietário do dispositivo e a outra gerencia o perfil de trabalho no modo proprietário do perfil. Você pode aplicar políticas separadas ao dispositivo e ao perfil de trabalho.

Anteriormente conhecidos como dispositivos corporativos, habilitados pessoalmente (COPE).

Dispositivos dedicados*

Dispositivos de propriedade da empresa configurados para um único caso de uso, como sinalização digital ou impressão de tíquetes

Não

Sim. Você fornece apenas os aplicativos necessários e impede que os usuários adicionem outros aplicativos.

Anteriormente conhecidos como dispositivos corporativos para uso único (COSU).

Perfil de trabalho BYOD**

Dispositivos pessoais registrados no modo de perfil de trabalho (também conhecido como modo de proprietário do perfil)

Sim

Sim. O DPC gerencia apenas o perfil de trabalho, não o dispositivo inteiro.

Esses dispositivos não precisam ser novos ou com redefinição de fábrica.

* Os usuários podem compartilhar um dispositivo dedicado. Quando um usuário faz login em um aplicativo em um dispositivo dedicado, o estado do trabalho fica com o aplicativo, não com o dispositivo.

** O XenMobile não suporta dispositivos Zebra como no modo de perfil de trabalho BYOD. O XenMobile suporta dispositivos Zebra como dispositivos totalmente gerenciados e no modo legado do dispositivo (também chamado de modo de administração do dispositivo).

Para obter informações sobre como migrar do modo legado para o modo de proprietário do dispositivo ou de proprietário do perfil, consulte [Migrar do Device Administration para o Android Enterprise](#).

Métodos de autenticação

Os perfis de registro determinam se os dispositivos Android se registram ou não no MAM, MDM ou MDM+MAM, com uma opção para que os usuários optem para não ter MDM.

Os modos de segurança de registro **Nome de usuário + PIN**, **URL de convite**, **URL de convite + PIN** e **URL de convite + senha** não estão disponíveis para o Android Enterprise. Para obter informações sobre como especificar o nível de segurança e as etapas de registro necessárias, consulte [Para configurar modos de segurança de registro](#).

O XenMobile suporta os seguintes métodos de autenticação para dispositivos Android registrados no MDM+MAM. Para obter informações, consulte os artigos em [Certificados e autenticação](#).

- Domínio
- Domínio mais token de segurança
- Certificado de cliente
- Certificado de cliente mais domínio
- Provedores de identidade:
 - Azure Active Directory
 - Provedor de identidade Citrix

Outro método de autenticação raramente usado é certificado de cliente mais token de segurança. Para obter informações, consulte <https://support.citrix.com/article/CTX215200>.

Requisitos

Antes de começar a usar o Android Enterprise, você precisa:

- Contas e credenciais:
 - Para configurar o Android Enterprise com o Google Play gerenciado, uma conta corporativa do Google
 - Para baixar os arquivos MDX mais recentes, uma conta de cliente Citrix

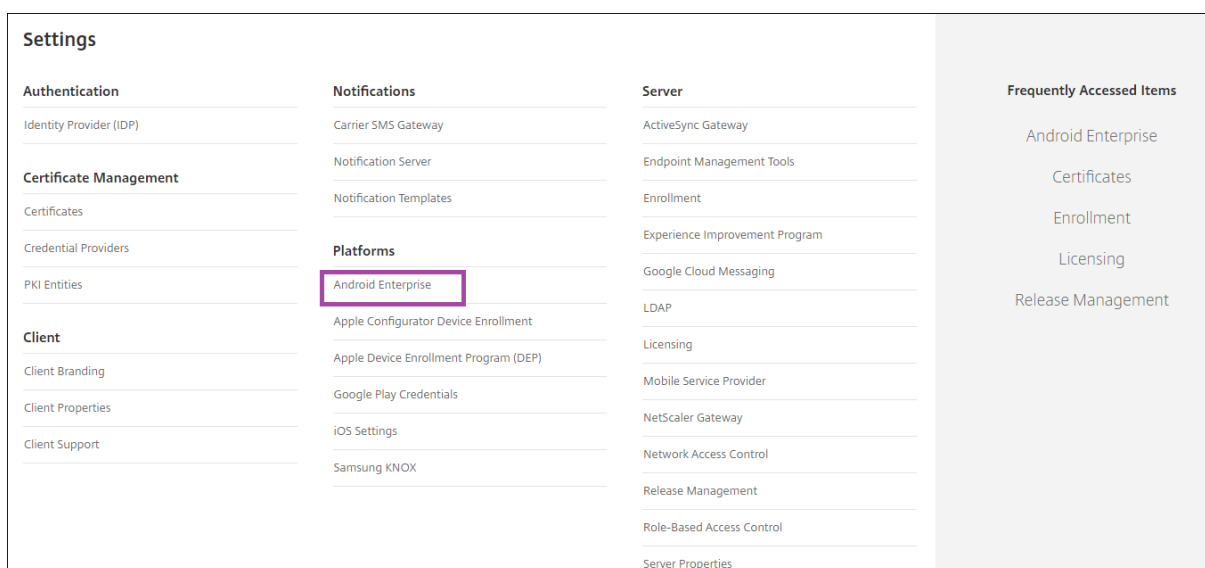
- Para implantar aplicativos privados (opcional), uma conta de desenvolvedor do Google
- Firebase Cloud Messaging (FCM) configurado para XenMobile. Consulte [Firebase Cloud Messaging](#) para obter instruções.
- Para Samsung Knox Mobile Enrollment (opcional), licenças premium Knox

Conectar o XenMobile ao Google Play

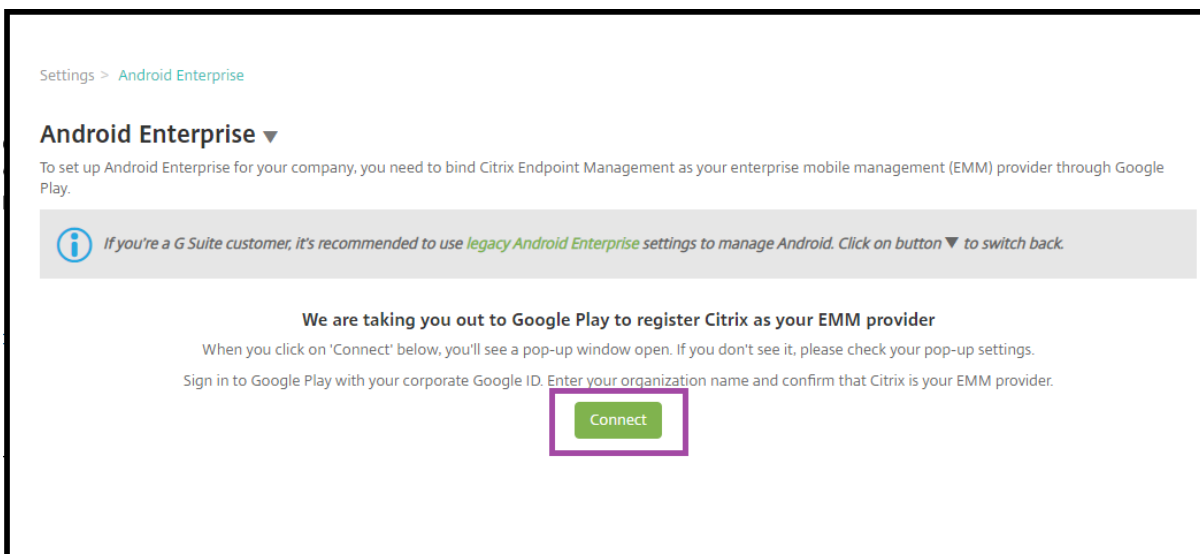
Para configurar o Android Enterprise para a sua organização, registre o Citrix como seu provedor de EMM por meio do Google Play gerenciado. Essa configuração conecta o Google Play gerenciado ao XenMobile e cria uma empresa para Android Enterprise no XenMobile.

Você precisará de uma conta corporativa do Google para entrar no Google Play.

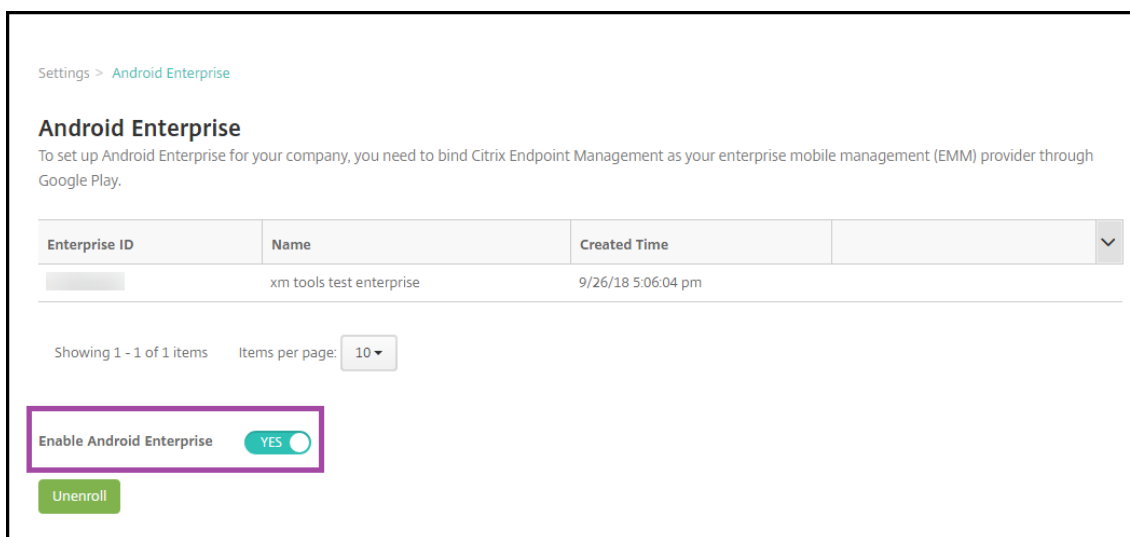
1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida.
2. Vá para **Configurações > Android Enterprise**.



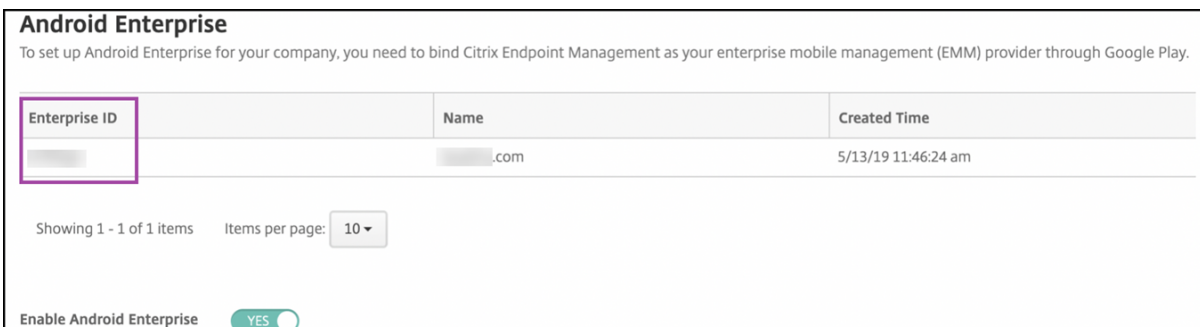
1. Clique em **Connect**. O Google Play é aberto.



1. Inicie a sessão no Google Play com as credenciais da sua conta corporativa do Google. Insira o nome da sua organização e confirme que a Citrix é seu provedor de EMM.
2. Um ID empresarial é adicionado ao Android Enterprise. Para ativar o Android Enterprise, deslize **Ativar Android Enterprise para Sim**.



Seu ID corporativo aparece no console XenMobile.



Seu ambiente está conectado ao Google e está pronto para gerenciar dispositivos. Agora você pode fornecer aplicativos para usuários.

O XenMobile pode ser usado para fornecer aos usuários aplicativos móveis de produtividade da Citrix, aplicativos MDX, aplicativos da loja de aplicativos pública, aplicativos Web e SaaS, aplicativos empresariais e links da Web. Para obter mais informações sobre esses tipos de aplicativos e fornecê-los aos usuários, consulte [Adicionar aplicativos](#).

A seção a seguir mostra como fornecer aplicativos móveis de produtividade.

Fornecer aplicativos móveis de produtividade da Citrix para usuários do Android Enterprise

Fornecer aplicativos móveis de produtividade da Citrix para usuários do Android Enterprise requer estas etapas.

1. Publique os aplicativos como aplicativos MDX. Consulte [Configurar aplicativos como aplicativos MDX](#).
2. Configure as regras para o desafio de segurança que seus usuários usam para acessar os perfis de trabalho em seus dispositivos. Consulte [Configurar política de desafio de segurança](#).

Os aplicativos que você publica estão disponíveis para dispositivos registrados no seu enterprise do Android Enterprise.

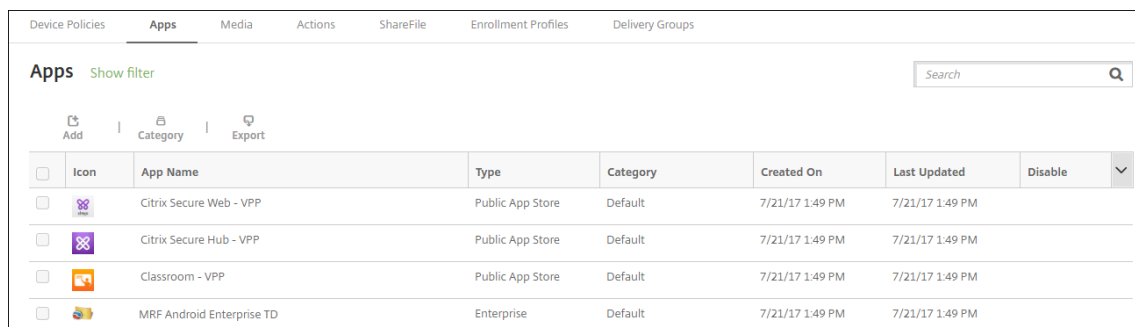
Nota:

Quando você implanta um aplicativo da loja de aplicativos pública do Android Enterprise em um usuário Android, esse usuário é automaticamente registrado no Android Enterprise.

Configurar aplicativos como aplicativos MDX

Para configurar um aplicativo de produtividade Citrix como um aplicativo MDX para Android Enterprise:

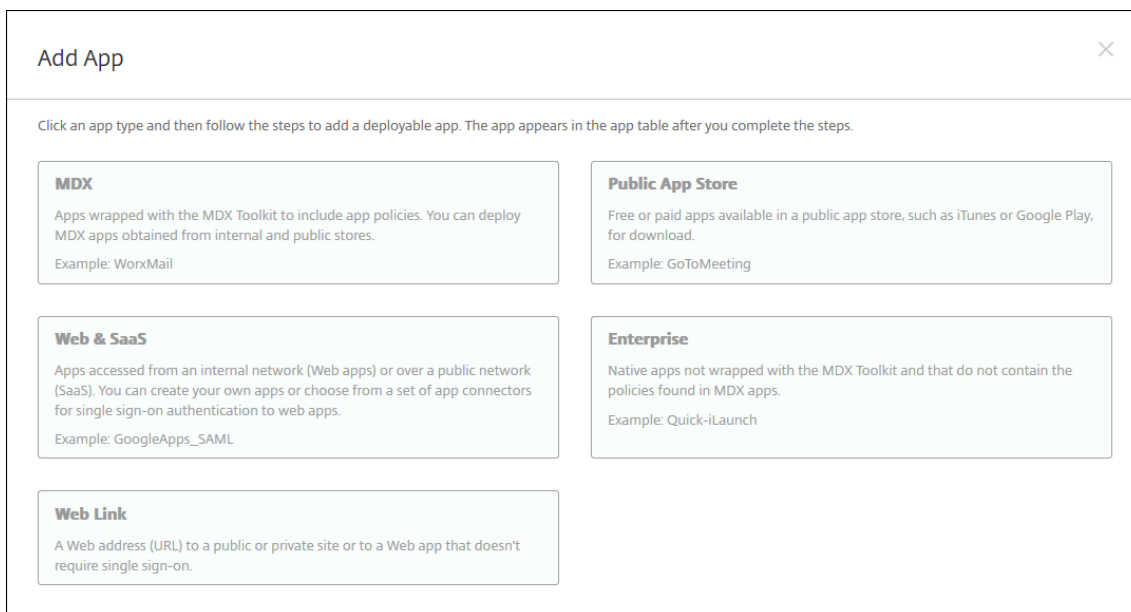
1. No console XenMobile, clique em **Configurar > Aplicativos**. A página **Aplicativos** é exibida.



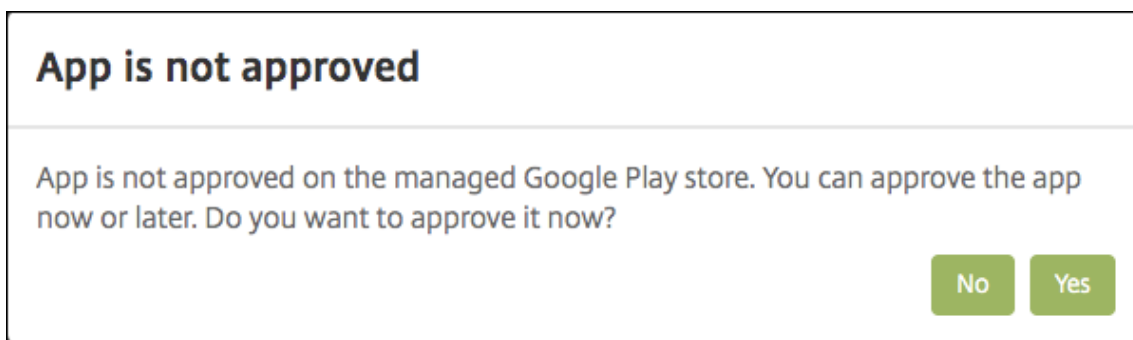
The screenshot shows the 'Apps' management interface in the XenMobile console. At the top, there are navigation tabs: 'Device Policies', 'Apps' (selected), 'Media', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. Below the tabs, there is a search bar and a 'Show filter' link. Underneath, there are three icons: 'Add', 'Category', and 'Export'. The main content is a table with the following columns: 'Icon', 'App Name', 'Type', 'Category', 'Created On', 'Last Updated', and 'Disable'. The table contains four rows of data:

Icon	App Name	Type	Category	Created On	Last Updated	Disable
	Citrix Secure Web - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	<input type="checkbox"/>
	Citrix Secure Hub - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	<input type="checkbox"/>
	Classroom - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	<input type="checkbox"/>
	MRF Android Enterprise TD	Enterprise	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	<input type="checkbox"/>

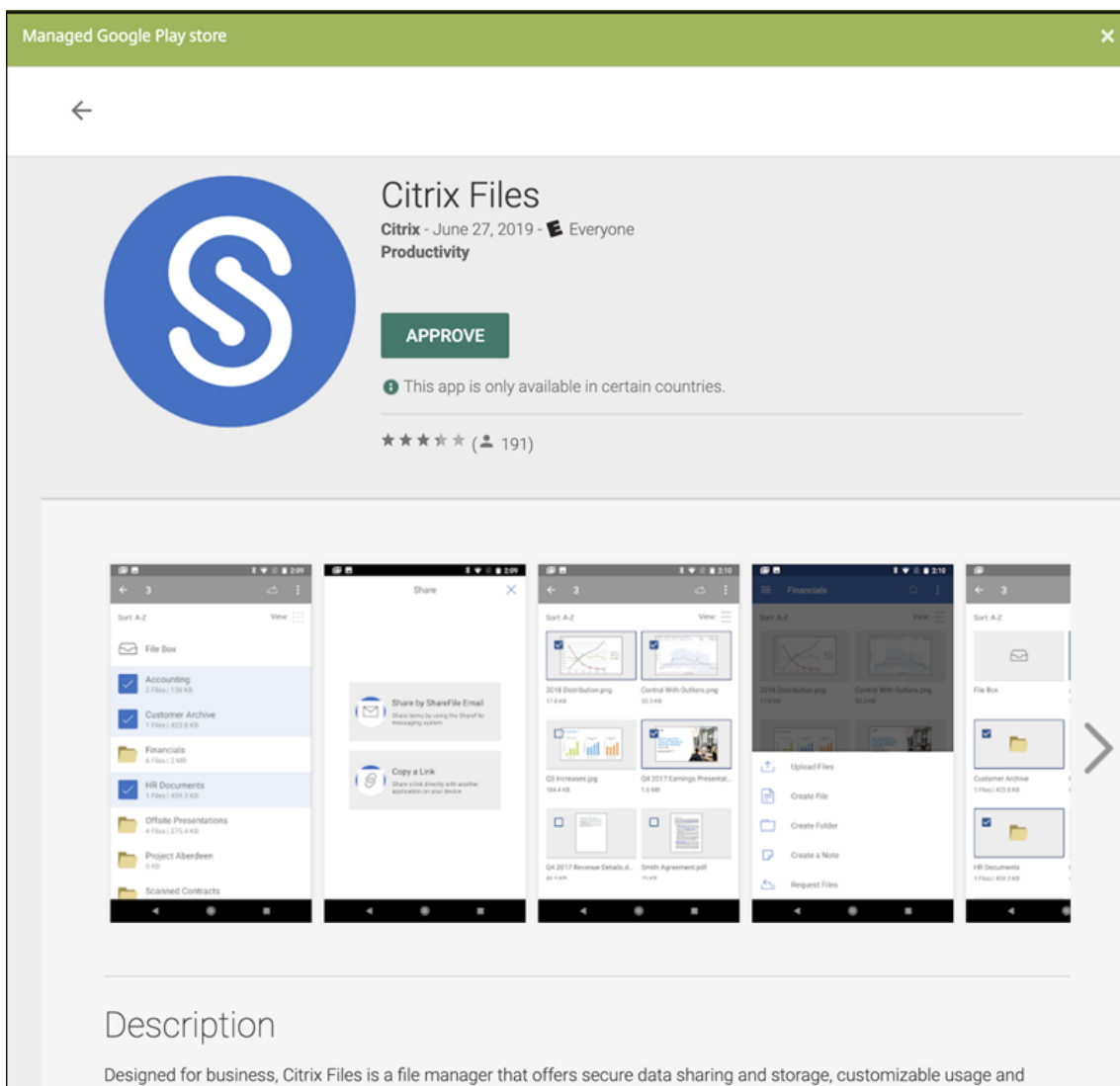
2. Clique em **Add**. A caixa de diálogo **Adicionar Aplicativo** é exibida.



3. Clique em **MDX**. A página **Informações do Aplicativo** é exibida.
4. No lado esquerdo da página, selecione **Android Enterprise** como plataforma.
5. Na página **Informações do aplicativo**, digite as seguintes informações:
 - **Nome:** digite um nome descritivo para o aplicativo. Esse nome aparecerá em **Nome do aplicativo** na tabela **Aplicativos**.
 - **Descrição:** digite uma descrição opcional para o aplicativo.
 - **Categoria do aplicativo:** opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte [Sobre categorias de aplicativos](#).
6. Clique em **Next**. A página do **Aplicativo MDX Android Enterprise** é exibida.
7. Clique em **Carregar** e navegue até o local dos arquivos .mdx do aplicativo. Selecione o arquivo e clique em **Abrir**.
8. A interface do usuário notificará você se o aplicativo anexado exigir aprovação da loja gerenciada do Google Play. Para aprovar o aplicativo sem sair do console XenMobile, clique em **Sim**.




9. Quando a página da loja gerenciada do Google Play for aberta, clique em **Aprovar**.



10. Clique em **Aprovar** novamente.
11. Selezione **Manter aprovado quando o aplicativo solicitar novas permissões**. Clique em **Save**.

APPROVAL SETTINGS NOTIFICATIONS

 **Citrix Files**
Citrix

How would you like to handle new app permission requests?

Keep approved when app requests new permissions.
Users will be able to install the updated app.

Revoke app approval when this app requests new permissions.
App will be removed from the store until it is reapproved.

CANCEL SAVE

12. Quando o aplicativo é aprovado e salvo, mais configurações aparecem na página. Defina estas configurações:
 - **Nome do arquivo:** digite o nome de arquivo associado ao aplicativo.
 - **Descrição do aplicativo:** digite uma descrição para o aplicativo.
 - **Rastreamento de produtos:** especifique qual rastreamento de produto você deseja enviar para os dispositivos do usuário. Se você tiver um rastreamento projetado para testes, poderá selecioná-lo e atribuí-lo aos seus usuários. O padrão é Produção.
 - **Versão do aplicativo:** opcionalmente, digite o número da versão do aplicativo.
 - **ID de pacote:** o URL do aplicativo na loja Google Play.
 - **Versão do SO mínima:** opcionalmente, digite a versão mais antiga do sistema operacional que o dispositivo pode executar para usar o aplicativo.
 - **Versão do SO máxima:** opcionalmente, digite a versão mais recente do sistema operacional que o dispositivo deve executar para usar o aplicativo.
 - **Dispositivos excluídos:** opcionalmente, digite o fabricante ou os modelos de dispositivos que não podem executar o aplicativo.
13. Configure as **Políticas de MDX**. Para obter mais informações sobre políticas de aplicativos para aplicativos MDX, consulte [Resumo das políticas do MDX](#) e [Visão geral do MAM SDK](#).
14. Configure as regras de implantação. Para obter informações, consulte [Implantar recursos](#).
15. Expanda **Configuração da loja**. Essa configuração não se aplica aos aplicativos Android Enterprise, que aparecem somente no Google Play gerenciado.

The screenshot displays the 'Store Configuration' section. It includes an 'App FAQ' section with a button to 'Add a new FAQ question and answer'. Below this is the 'App screenshots' section, which contains five placeholder boxes, each with a 'Choose File' button. At the bottom, there are two toggle switches: 'Allow app ratings' and 'Allow app comments', both of which are currently turned 'ON'.

Opcionalmente, você pode adicionar ao aplicativo perguntas frequentes ou capturas de tela que são exibidas na loja de aplicativos. Você também pode definir se os usuários podem classificar ou comentar no aplicativo.

- Defina estas configurações:
 - **Perguntas frequentes sobre o aplicativo:** adicione perguntas frequentes e respostas para o aplicativo.
 - **Instantâneos do aplicativo:** adicione capturas de tela para ajudar a classificar o aplicativo na loja de aplicativos. O gráfico que você carregar deve ser um PNG. Você não pode carregar uma imagem GIF ou JPEG.
 - **Permitir classificações do aplicativo:** selecione se um usuário tem permissão para classificar o aplicativo. O padrão é **I**.
 - **Permitir comentários do aplicativo:** selecione se os usuários têm permissão para comentar sobre o aplicativo selecionado. O padrão é **I**.

16. Clique em **Next**. A página **Aprovações** é exibida.

MDX	Approvals (optional) ×
1 App Information	Apply an existing workflow or create a new workflow to require approval before allowing users to access the app. Workflow to Use <input type="text" value="None"/>
2 Platform	
<input type="checkbox"/> iOS	
<input type="checkbox"/> Android	
<input checked="" type="checkbox"/> Windows Phone	
<input checked="" type="checkbox"/> Windows Desktop/Tablet	
3 Approvals (optional)	
4 Delivery Group Assignments (optional)	

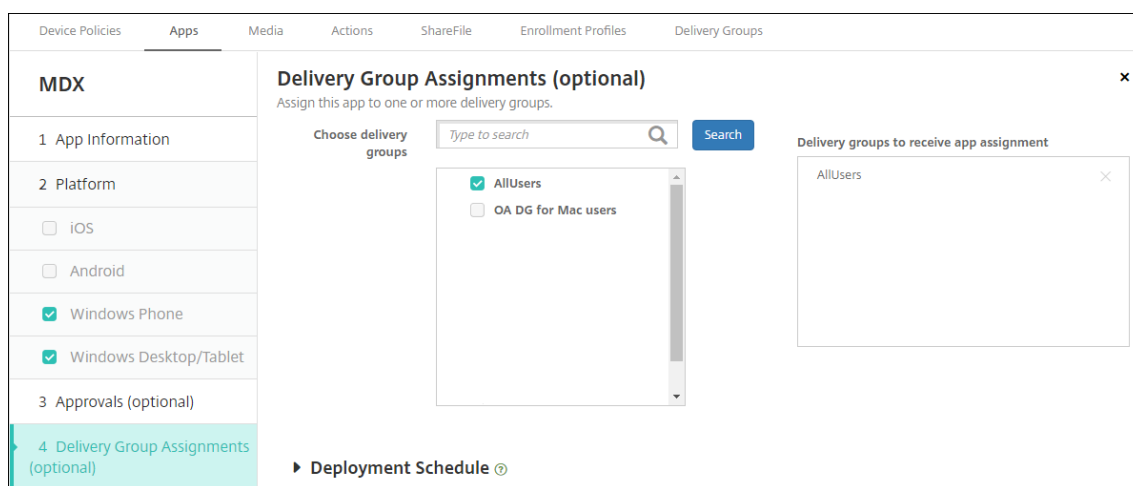
Use fluxos de trabalho quando precisar de aprovação ao criar contas de usuário. Se você não quiser configurar fluxos de trabalho de aprovação, pule para a Etapa 15.

Configure estas definições para atribuir ou criar um fluxo de trabalho:

- **Fluxo de trabalho a ser usado:** na lista, clique em um fluxo de trabalho existente ou clique em **Criar um novo fluxo de trabalho**. O padrão é **Nenhum**.
- Se você selecionar **Criar um novo fluxo de trabalho**, defina essas configurações. Para obter mais informações, consulte [Aplicar fluxos de trabalho](#).
- **Nome:** digite um nome exclusivo para o fluxo de trabalho.
- **Descrição:** opcionalmente, digite uma descrição para o fluxo de trabalho.
- **Modelos de aprovação de email:** na lista, selecione o modelo de aprovação a ser atribuído. Quando você clica no ícone de olho à direita deste campo, uma caixa de diálogo é exibida na qual você pode visualizar o modelo.
- **Níveis de aprovação do gerente:** na lista, selecione o número de níveis de aprovação do gerente necessários para esse fluxo de trabalho. O padrão é 1 nível. As opções possíveis são:
 - Não é Necessário
 - 1 nível
 - 2 níveis
 - 3 níveis
- **Selecionar domínio do Active Directory:** na lista, selecione o domínio do Active Directory adequado a ser usado para o fluxo de trabalho.
- **Encontrar aprovadores necessários adicionais:** digite o nome adicional da pessoa no campo de pesquisa e clique em **Pesquisar**. Os nomes são originários do Active Directory.
- Quando o nome aparece no campo, selecione a caixa de seleção próxima ao nome. O nome e endereço de email da pessoa aparecem na lista **Aprovadores necessários adicionais selecionados**.
 - Para remover uma pessoa da lista **Aprovadores necessários adicionais selecionados**, você pode optar por um dos seguintes procedimentos:

- * Clique em **Pesquisar** para ver uma lista de todas as pessoas do domínio selecionado.
- * Digite um nome parcial ou completo na caixa Pesquisar e clique em **Pesquisar** para limitar os resultados da pesquisa.
- * As pessoas da lista **Aprovadores necessários adicionais selecionados** têm marcas de seleção ao lado do respectivo nome na lista de resultados de pesquisa. Percorra a lista e desmarque a caixa de seleção ao lado de cada nome que você deseja remover.

17. Clique em **Next**. A página **Atribuição de grupo de entrega** é exibida.



18. Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega ou selecione um ou mais grupos. Os grupos que você selecionar aparecerão na lista **Grupos de entrega que receberão a atribuição de aplicativos**.

19. Expanda **Cronograma de implantação** e defina estas configurações:

- Ao lado de **Implantar**, clique em **I** para agendar a implantação ou em **O** para impedi-la. A opção padrão é **I**.
- Ao lado do Cronograma de implantação, clique em **Agora** ou **Mais tarde**. A opção padrão é **Agora**.
- Se você clicar em **Mais tarde**, clique no ícone de calendário e selecione a data e a hora da implantação.
- Ao lado de **Condição de implantação**, clique em **Em cada conexão** ou em **Somente quando a implantação anterior tiver falhado**. A opção padrão é **Em cada conexão**.
- Ao lado de **Implantar para conexões permanentes**, verifique se **O** está selecionado. A opção padrão é **O**. As conexões sempre ativas AlwaysOn não estão disponíveis para o Android Enterprise se você começou a usar o XenMobile com a versão 10.18.19 ou posterior. Não recomendamos as conexões para clientes que começaram a usar o XenMobile antes

da versão 10.18.19.

Essa opção será aplicável quando você tiver configurado a chave de implantação em segundo plano do cronograma em **Configurações > Propriedades do servidor**.

O cronograma de implantação que você configura é o mesmo para todas as plataformas. Todas as alterações feitas se aplicam a todas as plataformas, exceto **Implantar para conexões permanentes**.

20. Clique em **Save**.

Repita as etapas para configurar um aplicativo MDX para cada aplicativo móvel de produtividade.

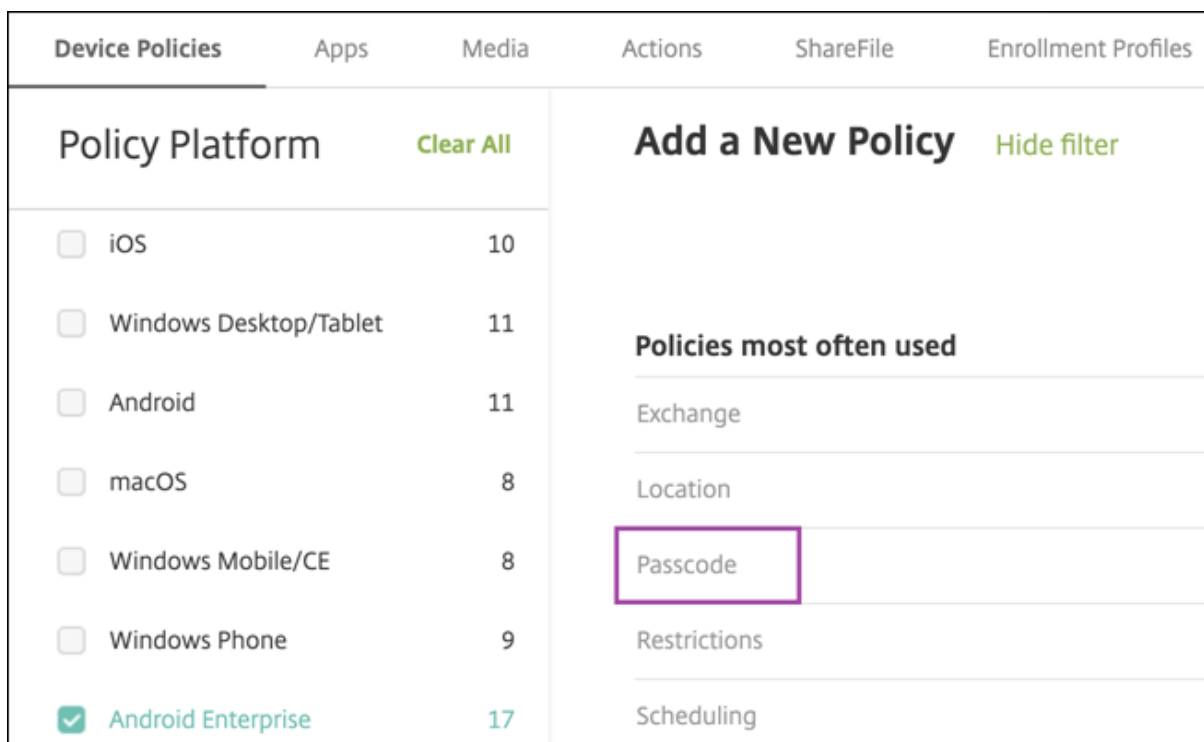
Configurar política de desafio de segurança

A política de dispositivo de código secreto XenMobile configura o conjunto de regras para que os usuários de desafios de segurança acessem seus dispositivos ou os perfis de trabalho Android Enterprise em seus dispositivos. Um desafio de segurança pode ser um código secreto ou reconhecimento biométrico. Para obter mais informações sobre a política de código secreto, consulte [Políticas de dispositivo de código secreto](#).

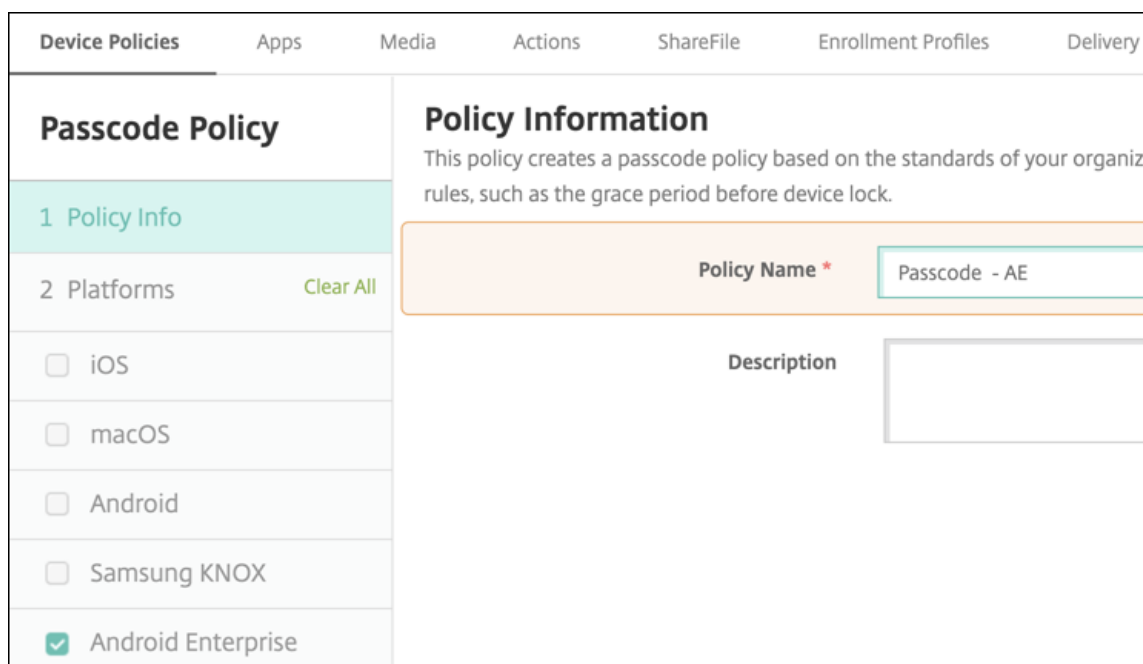
- Se a implantação do Android Enterprise incluir dispositivos BYOD, configure a política de código secreto para o perfil de trabalho.
- Se sua implantação incluir dispositivos totalmente gerenciados de propriedade da empresa, configure a política de código secreto para o próprio dispositivo.
- Se a sua implantação incluir ambos os tipos de dispositivos, configure os dois tipos de política de código secreto.

Para configurar a política de código secreto:

1. No console XenMobile, vá para **Configurar > Políticas de dispositivo**.
2. Clique em **Add**.
3. Clique em **Mostrar filtro** para mostrar o painel **Plataforma de política**. No painel **Plataforma de política**, selecione **Android Enterprise**.
4. Clique em **Código secreto** no painel direito.



1. Digite o **Nome da política**. Clique em **Next**.



2. Defina as configurações de política de código secreto.

- Defina **Código secreto do dispositivo obrigatório** para **Ativado** para ver as definições disponíveis para os desafios de segurança do dispositivo.
- Defina **Desafio de segurança no perfil de trabalho** como **Ativado** para ver as definições

disponíveis para os desafios de segurança do perfil de trabalho.

3. Clique em **Next**.
4. Atribua a política a um ou mais grupos de entrega.
5. Clique em **Save**.

Criar perfis de registro

Os perfis de registro controlam como os dispositivos Android são registrados se o Android Enterprise estiver habilitado para a sua implantação XenMobile. Ao criar um perfil de registro para registrar dispositivos Android Enterprise, você pode configurar o perfil de registro para registrar dispositivos novos e com redefinição de fábrica como:

- Dispositivos totalmente gerenciados
- Dispositivos dedicados (dispositivos COSU)
- Dispositivos totalmente gerenciados com um perfil de trabalho (dispositivos COPE)

Você também pode configurar cada um desses perfis de registro do Android Enterprise para registrar dispositivos Android BYOD como dispositivos de perfil de trabalho.

Se o Android Enterprise estiver habilitado para sua implantação do XenMobile, todos os dispositivos Android recém-registrados ou registrados novamente serão registrados como dispositivos Android Enterprise. Por padrão, o perfil de registro Global registra dispositivos Android novos e com redefinição de fábrica como dispositivos totalmente gerenciados e registra dispositivos Android BYOD como dispositivos de perfil de trabalho.

Ao criar perfis de inscrição, você atribui grupos de entrega a eles. Se um usuário pertencer a vários grupos de entrega que têm perfis de registro diferentes, o nome do grupo de entrega determinará o perfil de registro usado. O XenMobile seleciona o grupo de entrega que aparece por último em uma lista alfabética de grupos de entrega. Para obter mais informações, consulte [Perfis de registro](#).

Você pode usar perfis de registro para combinar vários casos de uso, como somente MDM, MDM+MAM e somente MAM. O tipo de licença do XenMobile Server, refletido na propriedade do servidor `xms.server.mode`, determina as configurações disponíveis em **Configurar > Perfis de registro**.

Adicionar um perfil de registro para dispositivos totalmente gerenciados

O perfil de registro Global registra dispositivos totalmente gerenciados por padrão, mas você pode criar mais perfis de registro para registrar dispositivos totalmente gerenciados.

1. No console XenMobile, vá para **Configurar > Perfis de registro**.
2. Para adicionar um perfil de registro, clique em **Adicionar**. Na página de Informações de registro, digite um nome para o perfil de registro.

3. Defina o número de dispositivos que os membros com este perfil podem registrar.
4. Selecione **Android** em **Plataformas** ou clique em **Avançar**. A página de configuração de registro é exibida.
5. Defina **Gerenciamento** para **Android Enterprise**.
6. Defina **Modo proprietário do dispositivo** como **Dispositivo de propriedade da empresa**.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	Device management ⓘ Management <ul style="list-style-type: none"> <input checked="" type="radio"/> Android Enterprise ⓘ <input type="radio"/> Legacy device administration (not recommended) ⓘ <input type="radio"/> Do not manage devices ⓘ
Android	Device owner mode <ul style="list-style-type: none"> <input checked="" type="radio"/> Company-owned device ⓘ <input type="radio"/> Fully managed with work profile ⓘ <input type="radio"/> Dedicated device ⓘ <input type="radio"/> None ⓘ
iOS	BYOD work profile <input checked="" type="checkbox"/> ⓘ
3 Assignment (optional)	Application management ⓘ Citrix MAM <input checked="" type="checkbox"/> ⓘ
	User consent Allow users to decline device management <input checked="" type="checkbox"/> ⓘ

7. **Perfil de trabalho BYOD** permite configurar o perfil de registro para registrar dispositivos BYOD como dispositivos de perfil de trabalho. Dispositivos novos e com redefinição de fábrica são registrados como dispositivos totalmente gerenciados.
 - Defina **Perfil de trabalho BYOD** como **Ativado** para permitir o registro de dispositivos BYOD como dispositivos de perfil de trabalho. O padrão é **On**.
 - Defina o **perfil de trabalho BYOD** como **Desativado** para restringir o registro a dispositivos totalmente gerenciados.
8. Escolha se deseja registrar dispositivos no Citrix MAM.
9. Se você definir **Perfil de trabalho BYOD** como **Ativado**, configure o consentimento do usuário. Para permitir que os usuários de dispositivos de perfil de trabalho BYOD recusem o gerenciamento do dispositivo ao registrar seus dispositivos, defina **Permitir que os usuários recusem o gerenciamento de dispositivos** como **On**.

Se o **Perfil de trabalho BYOD** estiver definido como **On**, o valor padrão de **Permitir que os usuários recusem o gerenciamento de dispositivos** será **On**. Se o **Perfil de trabalho BYOD** estiver definido como **Off**, **Permitir que os usuários recusem o gerenciamento de dispositivos** será desabilitado.

10. Selecione **Atribuição (opções)**. A tela Atribuição de grupo de entrega é exibida.
11. Escolha um grupo de entrega ou grupos de entrega contendo os administradores que registram dispositivos totalmente gerenciados. Em seguida, clique em **Save**.

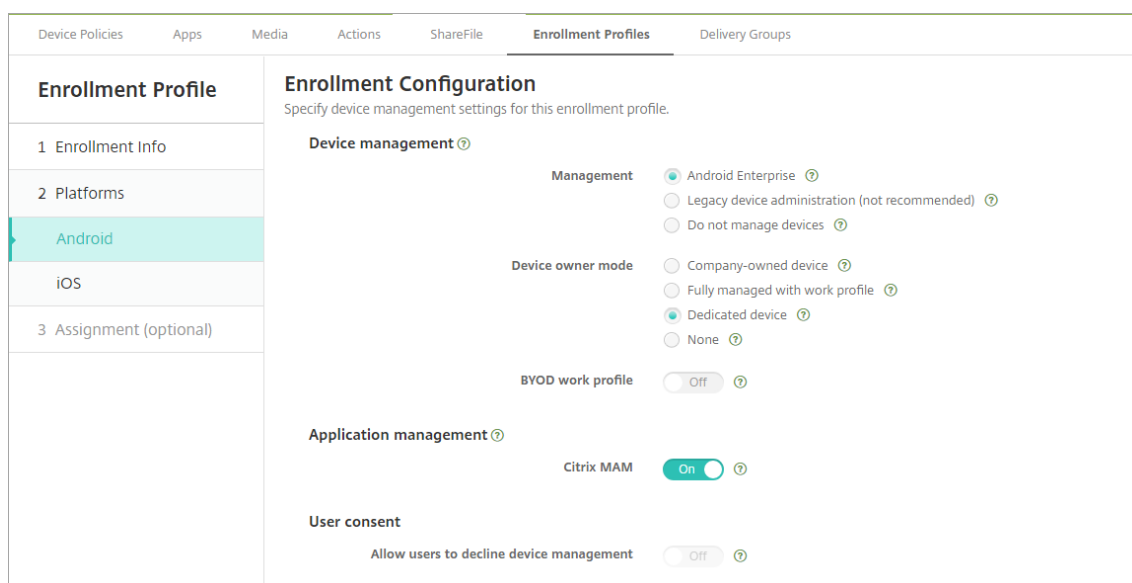
A página de Perfil de registro é exibida com o perfil que você adicionou.

<input type="checkbox"/>	Enrollment profile name	Created on	Updated on	Device limit
<input type="checkbox"/>	Fully managed devices	11/19/19 2:19:16 pm	11/19/19 2:19:16 pm	unlimited
<input type="checkbox"/>	Global	3/7/18 4:08:24 pm	3/7/18 4:08:24 pm	unlimited

Adicionar um perfil de registro de dispositivo dedicado

Quando a sua implantação do XenMobile inclui dispositivos dedicados, um único administrador XenMobile ou um pequeno grupo de administradores registra vários dispositivos dedicados. Para garantir que esses administradores possam registrar todos os dispositivos necessários, crie um perfil de registro para eles com dispositivos ilimitados permitidos por usuário.

1. No console XenMobile, vá para **Configurar > Perfis de registro**.
2. Para adicionar um perfil de registro, clique em **Adicionar**. Na página de Informações de registro, digite um nome para o perfil de registro. Certifique-se de que o número de dispositivos que os membros com este perfil podem registrar esteja definido como ilimitado.
3. Selecione **Android** em **Plataformas** ou clique em **Avançar**. A página de configuração de registro é exibida.
4. Defina **Gerenciamento** para **Android Enterprise**.
5. Defina **Modo de proprietário do dispositivo** como **Dispositivo dedicado**.



6. **Perfil de trabalho BYOD** permite configurar o perfil de registro para registrar dispositivos BYOD como dispositivos de perfil de trabalho. Dispositivos novos e com redefinição de fábrica são registrados como dispositivos dedicados. Defina **Perfil de trabalho BYOD** como **Ativado** para permitir o registro de dispositivos BYOD como dispositivos de perfil de trabalho. Defina **Perfil de trabalho BYOD** como **Desativado** para restringir o registro a dispositivos de propriedade da empresa. O padrão é **Ativado**.

7. Escolha se deseja registrar dispositivos no Citrix MAM.

8. Se você definir **Perfil de trabalho BYOD** como **Ativado**, configure o consentimento do usuário. Para permitir que os usuários de dispositivos de perfil de trabalho BYOD recusem o gerenciamento do dispositivo ao registrar seus dispositivos, defina **Permitir que os usuários recusem o gerenciamento de dispositivos** como **On**.

Se o **Perfil de trabalho BYOD** estiver definido como **On**, o valor padrão de **Permitir que os usuários recusem o gerenciamento de dispositivos** será **On**. Se o **Perfil de trabalho BYOD** estiver definido como **Off**, **Permitir que os usuários recusem o gerenciamento de dispositivos** será desabilitado.

9. Selecione **Atribuição (opções)**. A tela Atribuição de grupo de entrega é exibida.

10. Escolha um grupo de entrega ou grupos de entrega contendo os administradores que registram dispositivos dedicados. Em seguida, clique em **Save**.

A página de Perfil de registro é exibida com o perfil que você adicionou.

Enrollment profile name	Created on	Updated on	Device limit
Dedicated devices	11/1/19 3:30:36 pm	11/1/19 3:30:36 pm	unlimited
Global	10/28/19 5:30:39 am	10/28/19 5:30:39 am	unlimited

Adicionar um perfil de registro para dispositivos totalmente gerenciados com um perfil de trabalho

1. No console XenMobile, vá para **Configurar > Perfis de registro**.
2. Para adicionar um perfil de registro, clique em **Adicionar**. Na página de Informações de registro, digite um nome para o perfil de registro.
3. Defina o número de dispositivos que os membros com este perfil podem registrar.
4. Selecione **Android** em **Plataformas** ou clique em **Avançar**. A página de configuração de registro é exibida.
5. Defina **Gerenciamento** para **Android Enterprise**. Defina **Modo proprietário do dispositivo** como **Totalmente gerenciado com perfil de trabalho**.

6. **Perfil de trabalho BYOD** permite configurar o perfil de registro para registrar dispositivos BYOD como dispositivos de perfil de trabalho. Dispositivos novos e com redefinição de fábrica são reg-

istrados como dispositivos totalmente gerenciados com um perfil de trabalho. Defina **Perfil de trabalho BYOD** como **Ativado** para permitir o registro de dispositivos BYOD como dispositivos de perfil de trabalho. Defina **Perfil de trabalho BYOD** como **Desativado** para restringir o registro a dispositivos dedicados. O padrão é **Desativado**.

7. Escolha se deseja registrar dispositivos no Citrix MAM.
8. Se você definir **Perfil de trabalho BYOD** como **Ativado**, configure o consentimento do usuário. Para permitir que os usuários de dispositivos de perfil de trabalho BYOD recusem o gerenciamento do dispositivo ao registrar seus dispositivos, defina **Permitir que os usuários recusem o gerenciamento de dispositivos** como **On**.

Se o **Perfil de trabalho BYOD** estiver definido como **On**, o valor padrão de **Permitir que os usuários recusem o gerenciamento de dispositivos** será **On**. Se o **Perfil de trabalho BYOD** estiver definido como **Off**, **Permitir que os usuários recusem o gerenciamento de dispositivos** será desabilitado.

9. Selecione **Atribuição (opções)**. A tela Atribuição de grupo de entrega é exibida.
10. Escolha um grupo de entrega ou grupos de entrega contendo os administradores que registram dispositivos totalmente gerenciados com um perfil de trabalho. Em seguida, clique em **Save**.

A página de Perfil de registro é exibida com o perfil que você adicionou.

<input type="checkbox"/>	Enrollment profile name	Created on	Updated on	Device limit
<input type="checkbox"/>	COPE devices	11/1/19 1:01:51 pm	11/1/19 1:01:51 pm	unlimited
<input type="checkbox"/>	Global	10/28/19 5:30:39 am	10/28/19 5:30:39 am	unlimited

Adicionar um perfil de registro para dispositivos legados

Google preteriu o modo de administrador do dispositivo de gerenciamento de dispositivos. O Google incentiva os clientes a gerenciar todos os dispositivos Android no modo de proprietário do dispositivo ou no modo de proprietário do perfil. (Consulte [Device admin deprecation](#) nos guias do desenvolvedor do Google Android Enterprise.)

Para dar suporte a essa alteração:

- A Citrix torna o Android Enterprise a opção de registro padrão para dispositivos Android.

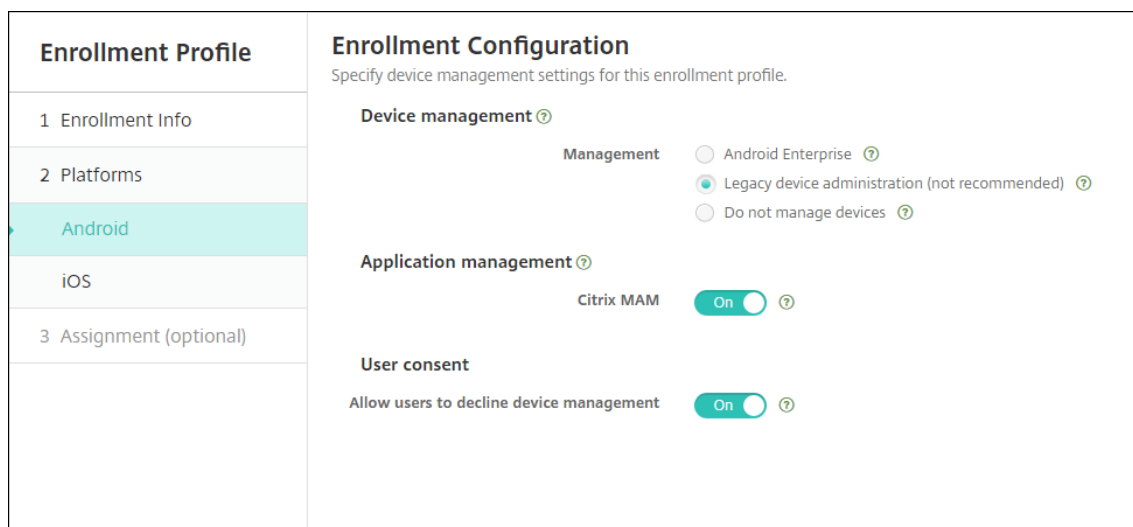
- Se o Android Enterprise estiver habilitado para sua implantação do XenMobile, todos os dispositivos Android recém-registrados ou registrados novamente serão registrados como dispositivos Android Enterprise.

Sua organização pode não estar pronta para começar a gerenciar dispositivos Android legados usando o Android Enterprise. Nesse caso, você pode continuar gerenciando-os no modo de administrador do dispositivo. Para dispositivos já registrados no modo de administrador de dispositivos, o XenMobile continua a gerenciá-los no modo de administrador de dispositivos.

Crie um perfil de registro para dispositivos legados para permitir que novos registros de dispositivos Android usem o modo de administrador de dispositivos.

Para criar um perfil de registro para dispositivos legados:

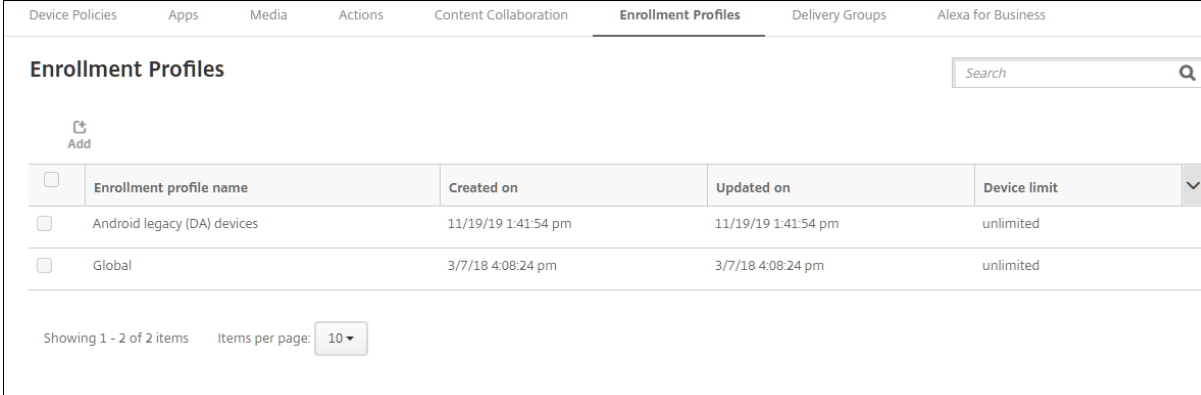
1. No console XenMobile, vá para **Configurar > Perfis de registro**.
2. Para adicionar um perfil de registro, clique em **Adicionar**. Na página de Informações de registro, digite um nome para o perfil de registro.
3. Defina o número de dispositivos que os membros com este perfil podem registrar.
4. Selecione **Android** em **Plataformas** ou clique em **Avançar**. A página de configuração de registro é exibida.
5. Defina **Gerenciamento** para **Administração de dispositivos herdados (não recomendado)**. Clique em **Next**.



6. Escolha se deseja registrar dispositivos no Citrix MAM.
7. Para permitir que os usuários recusem o gerenciamento do dispositivo ao registrar seus dispositivos, defina **Permitir que os usuários recusem o gerenciamento de dispositivos** como **Ativado**. O padrão é **Ativado**.
8. Selecione **Atribuição (opções)**. A tela Atribuição de grupo de entrega é exibida.

- Escolha um grupo de entrega ou grupos de entrega contendo os administradores que registram dispositivos dedicados. Em seguida, clique em **Save**.

A página de Perfil de registro é exibida com o perfil que você adicionou.



<input type="checkbox"/>	Enrollment profile name	Created on	Updated on	Device limit
<input type="checkbox"/>	Android legacy (DA) devices	11/19/19 1:41:54 pm	11/19/19 1:41:54 pm	unlimited
<input type="checkbox"/>	Global	3/7/18 4:08:24 pm	3/7/18 4:08:24 pm	unlimited

Para continuar a gerenciar um dispositivo legado no modo de administrador de dispositivos, registre-o ou registre-o novamente utilizando este perfil. Você registra dispositivos de administrador de dispositivos de modo similar aos dispositivos de perfil de trabalho, fazendo com que os usuários baixem o Secure Hub e fornecendo um URL do servidor de registro.

Provisionar dispositivos de perfil de trabalho Android Enterprise

Os dispositivos de perfil de trabalho Android Enterprise são registrados no modo de proprietário do perfil. Esses dispositivos não precisam ser novos ou com redefinição de fábrica. Os dispositivos BYOD são registrados como dispositivos de perfil de trabalho. A experiência de registro é semelhante ao registro do Android no XenMobile. Os usuários fazem o download do Secure Hub a partir do Google Play e registram seus dispositivos.

Por padrão, as configurações de **Depuração de USB e Fontes desconhecidas** são desativadas em um dispositivo quando ele é registrado no Android Enterprise como um dispositivo de perfil de trabalho.

Quando for registrar dispositivos no Android Enterprise como dispositivos de perfil de trabalho, sempre vá para o Google Play. A partir dali, habilite o Secure Hub para aparecer no perfil pessoal do usuário.

Provisionamento de dispositivos Android Enterprise totalmente gerenciados

Você pode registrar dispositivos totalmente gerenciados na implantação configurada nas seções anteriores. Dispositivos totalmente gerenciados são dispositivos de propriedade da empresa e estão registrados no modo proprietário do dispositivo. Somente dispositivos novos ou redefinidos de fábrica podem ser registrados no modo proprietário do dispositivo.

Você pode registrar dispositivos no modo proprietário do dispositivo usando qualquer um destes métodos de registro:

- **Token identificador DPC:** com esse método de registro, os usuários inserem os caracteres `afw##xenmobile` ao configurar o dispositivo. `afw##xenmobile` é o token identificador Citrix DPC. Esse token identifica o dispositivo como gerenciado pelo XenMobile e baixa o Secure Hub da loja Google Play. Consulte Registrar dispositivos usando o token identificador Citrix DPC.
- **Near field communication (NFC) bump:** o método de registro de colisão NFC transfere dados entre dois dispositivos usando comunicação a curta distância. Bluetooth, Wi-Fi e outros meios de comunicação estão desativados em um dispositivo que sofreu uma redefinição de fábrica ou novo. O NFC é o único protocolo de comunicação que o dispositivo pode usar nesse estado. Consulte Registrar dispositivos com NFC bump.
- **Código QR:** o registro de código QR pode ser usado para registrar uma frota distribuída de dispositivos que não suportam NFC, como tablets. O método de registro de código QR instala e configura o modo de perfil de dispositivo digitalizando um código QR no Assistente de instalação. Consulte Registrar dispositivos usando um código QR.
- **Sem toque:** o registro sem toque permite que você configure dispositivos para se registrarem automaticamente quando eles são ligados pela primeira vez. O registro sem toque é suportado em alguns dispositivos Android que executam o Android 8.0 ou posterior. Consulte Registro sem toque.
- **Contas do Google:** os usuários inserem suas credenciais da Conta do Google para iniciar o processo de provisionamento. Essa opção é para empresas que usam o Google Workspace.

Registrar dispositivos usando o token identificador Citrix DPC

Os usuários inserem `afw##xenmobile` quando solicitados a inserir uma conta do Google depois de ligarem dispositivos novos ou redefinidos de fábrica para instalação inicial. Essa ação baixa e instala o Secure Hub. Os usuários seguem os prompts de configuração do Secure Hub para concluir o registro.

Esse método de registro é recomendado para a maioria dos clientes, porque a versão mais recente do Secure Hub é baixada da loja Google Play. Ao contrário de outros métodos de registro, você não fornece o Secure Hub para download no servidor XenMobile Server.

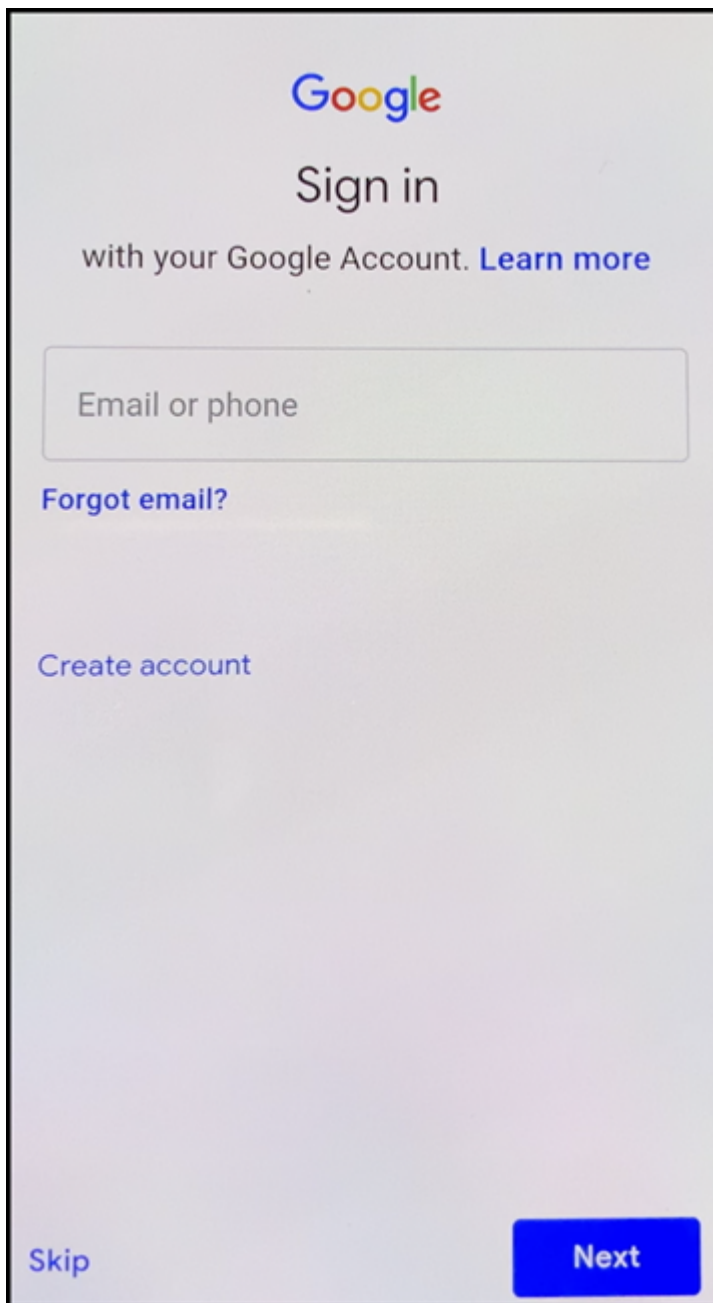
Requisitos do sistema

- Suportado em todos os dispositivos Android que executam o sistema operacional Android.

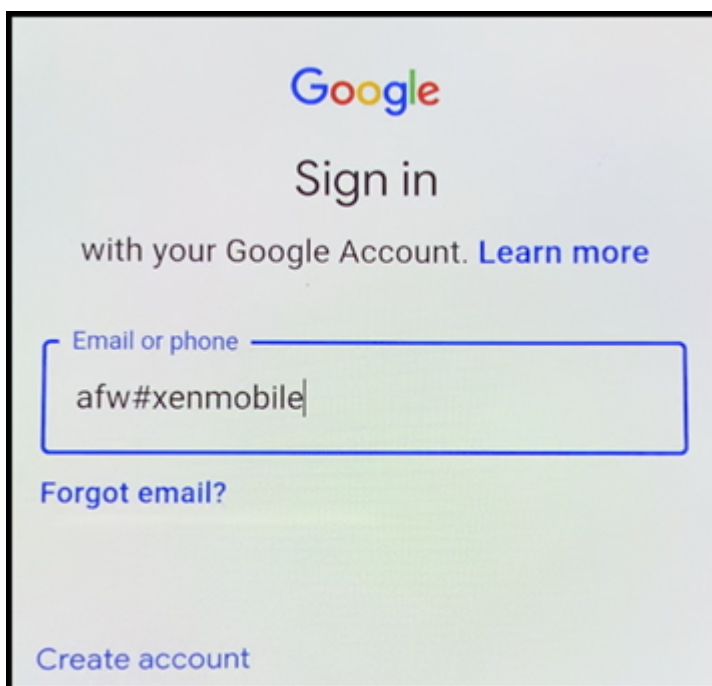
Para registrar o dispositivo

1. Ligue um dispositivo novo ou redefinido de fábrica.

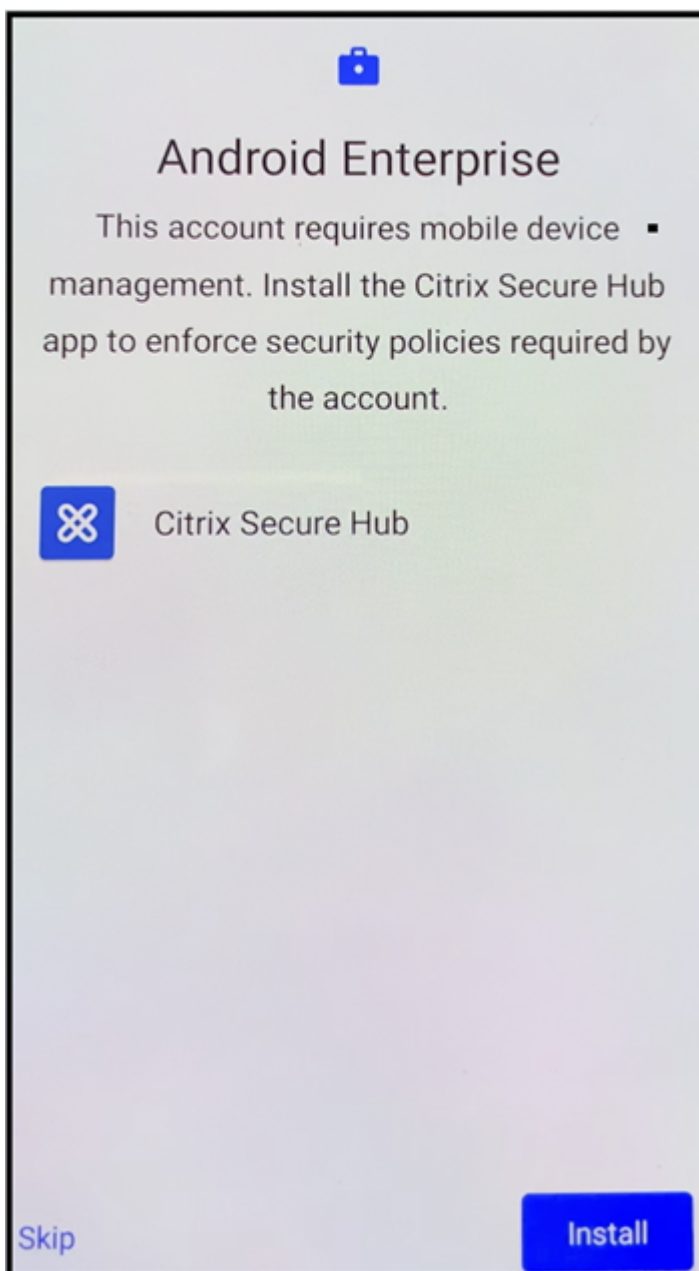
2. A instalação inicial do dispositivo é carregada e solicita uma conta do Google. Se o dispositivo carregar a tela inicial do dispositivo, verifique se há na barra de notificação uma notificação **Concluir instalação**.



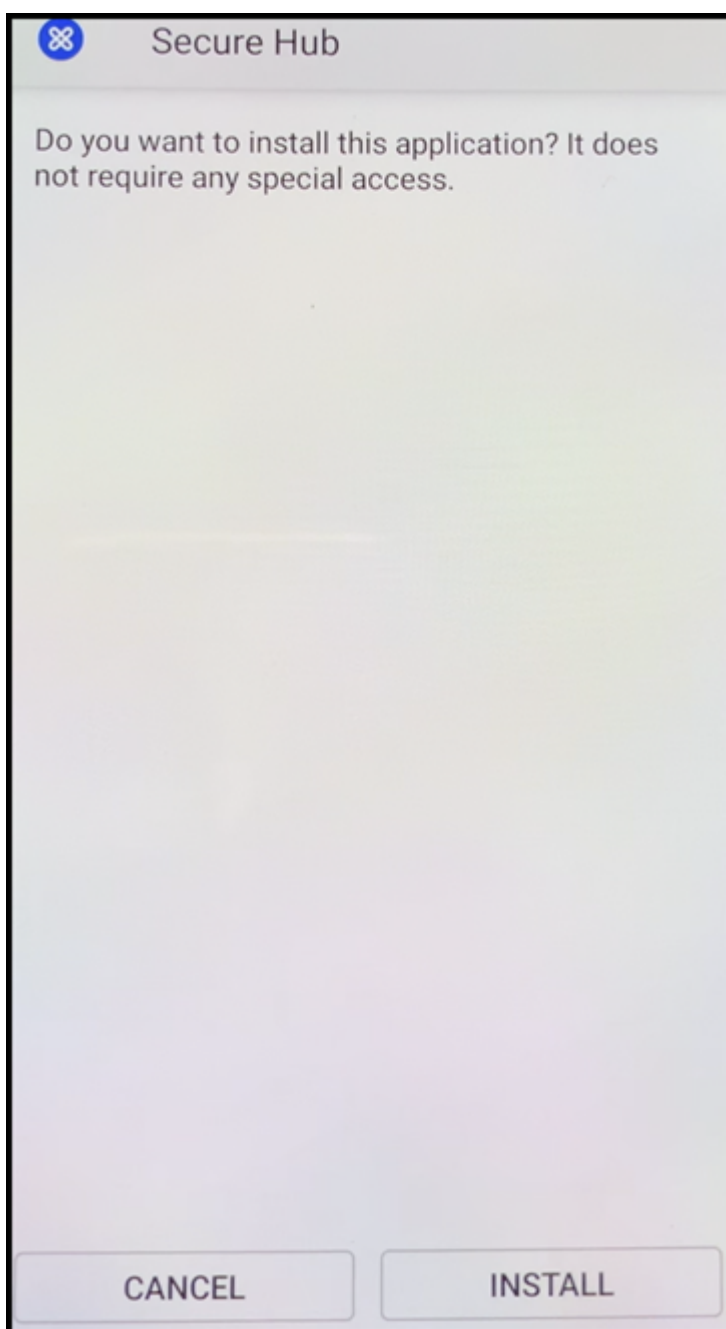
3. Digite `afw##xenmobile` no campo **E-mail ou telefone**.



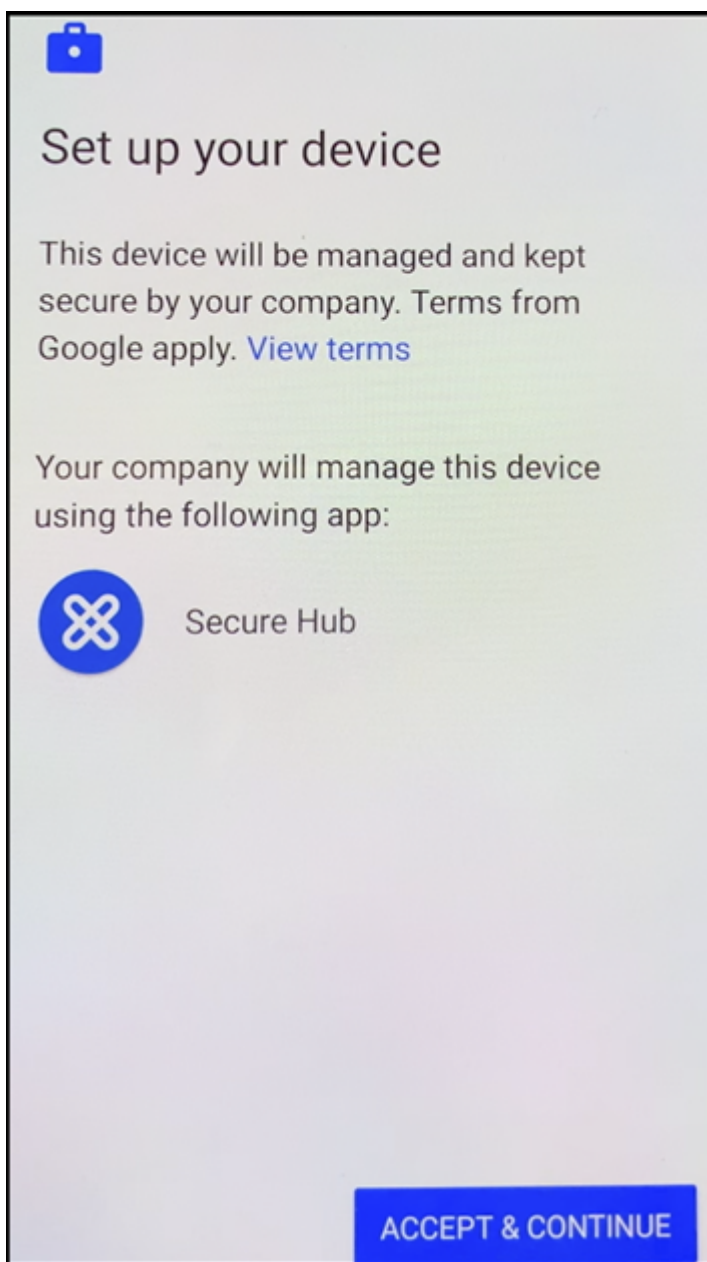
4. Toque em **Instalar** na tela do Android Enterprise solicitando a instalação do Secure Hub.



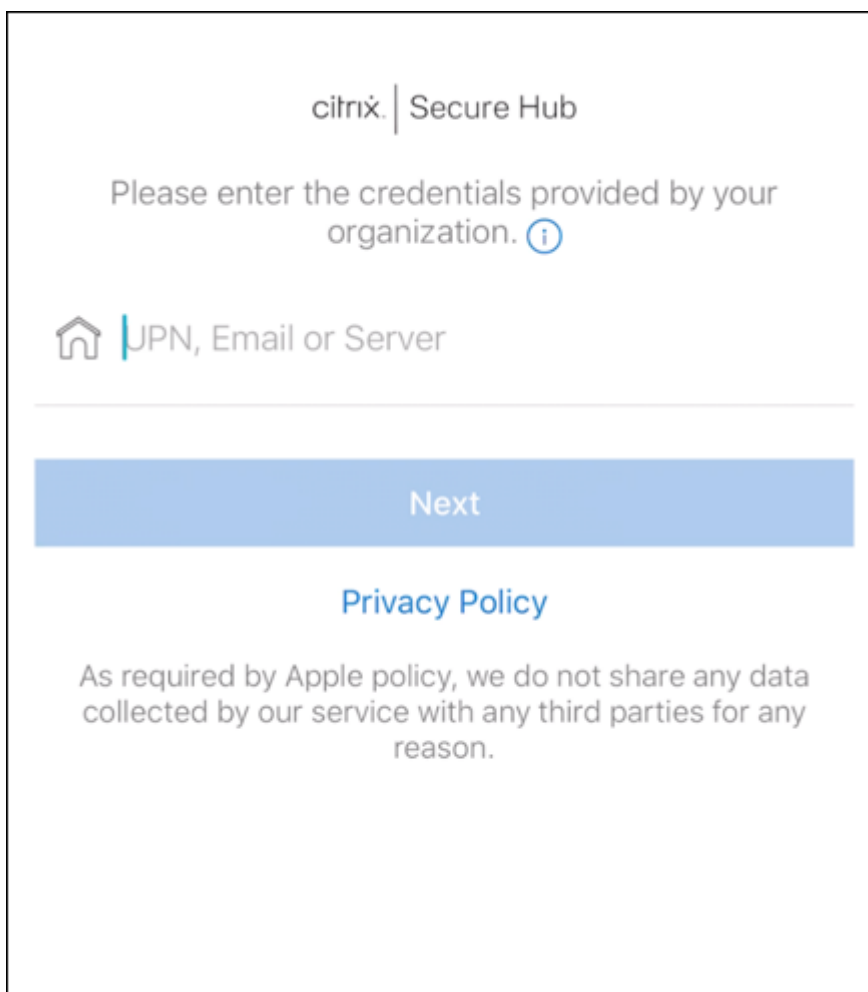
5. Toque em **Instalar** na tela do instalador do Secure Hub.



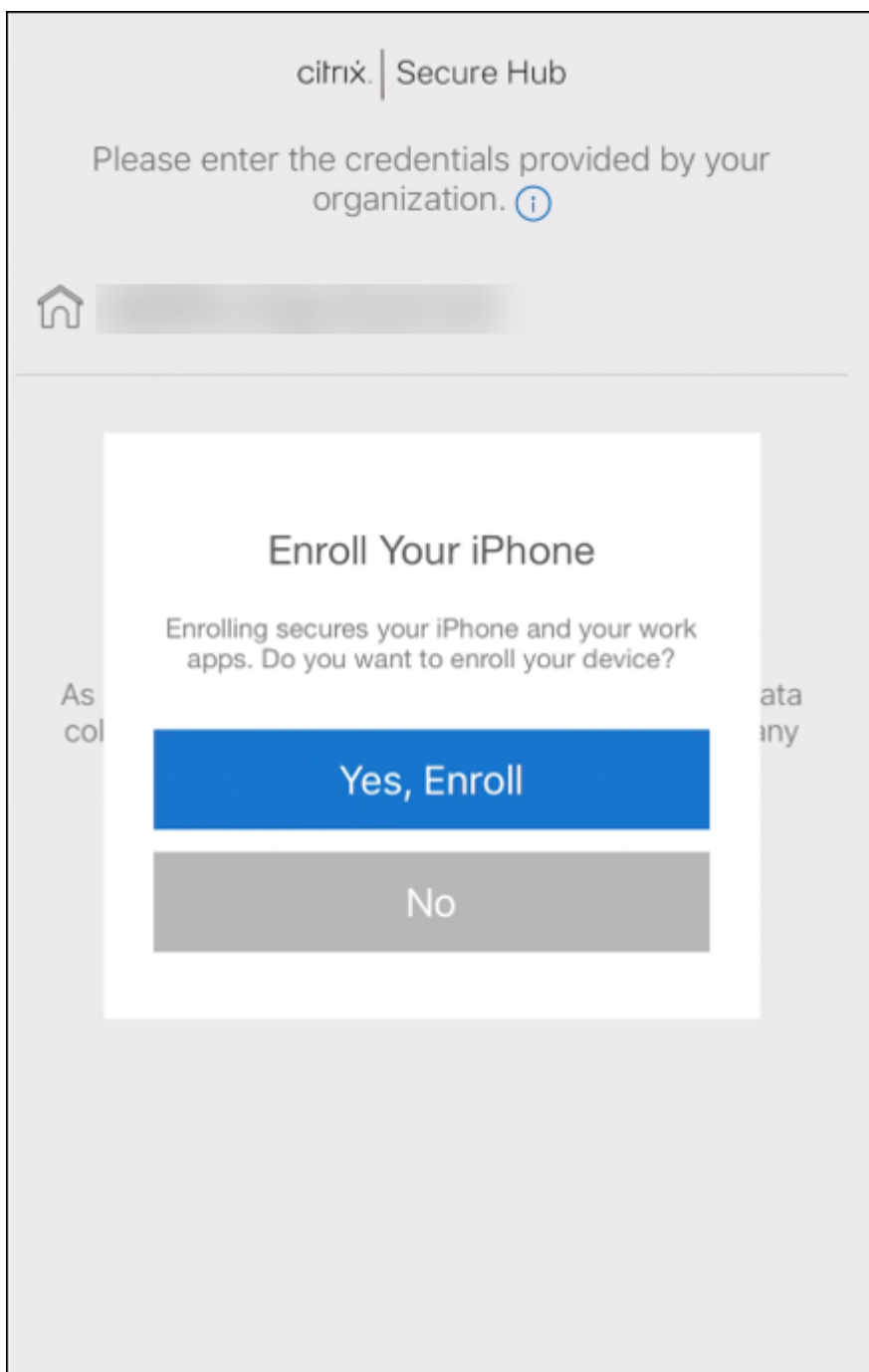
6. Toque em **Permitir** para todas as solicitações de permissão do aplicativo.
7. Toque em **Aceitar e continuar** para instalar o Secure Hub e permitir que ele gerencie o dispositivo.



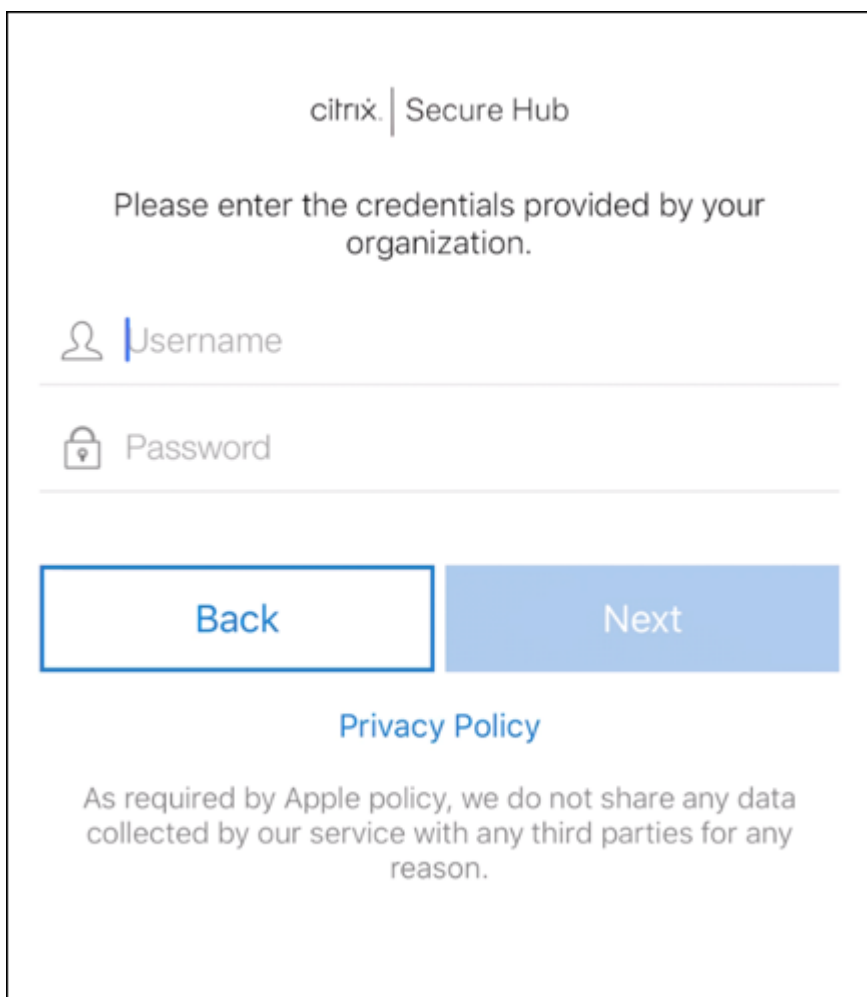
8. O Secure Hub agora está instalado e na tela de registro padrão. Neste exemplo, AutoDiscovery não está configurado. Se estivesse, o usuário poderá inserir seu nome de usuário/e-mail e um servidor será encontrado para ele. Em vez disso, insira a URL de registro do ambiente e toque em **Avançar**.



9. A configuração padrão do XenMobile permite que os usuários escolham se usarão MAM ou MDM+MAM. Se solicitado dessa forma, toque em **Sim, registrar** para escolher MDM+MAM.



10. Insira o nome de usuário e a senha e, em seguida, toque em **Avançar**.



citrix | Secure Hub

Please enter the credentials provided by your organization.

Username

Password

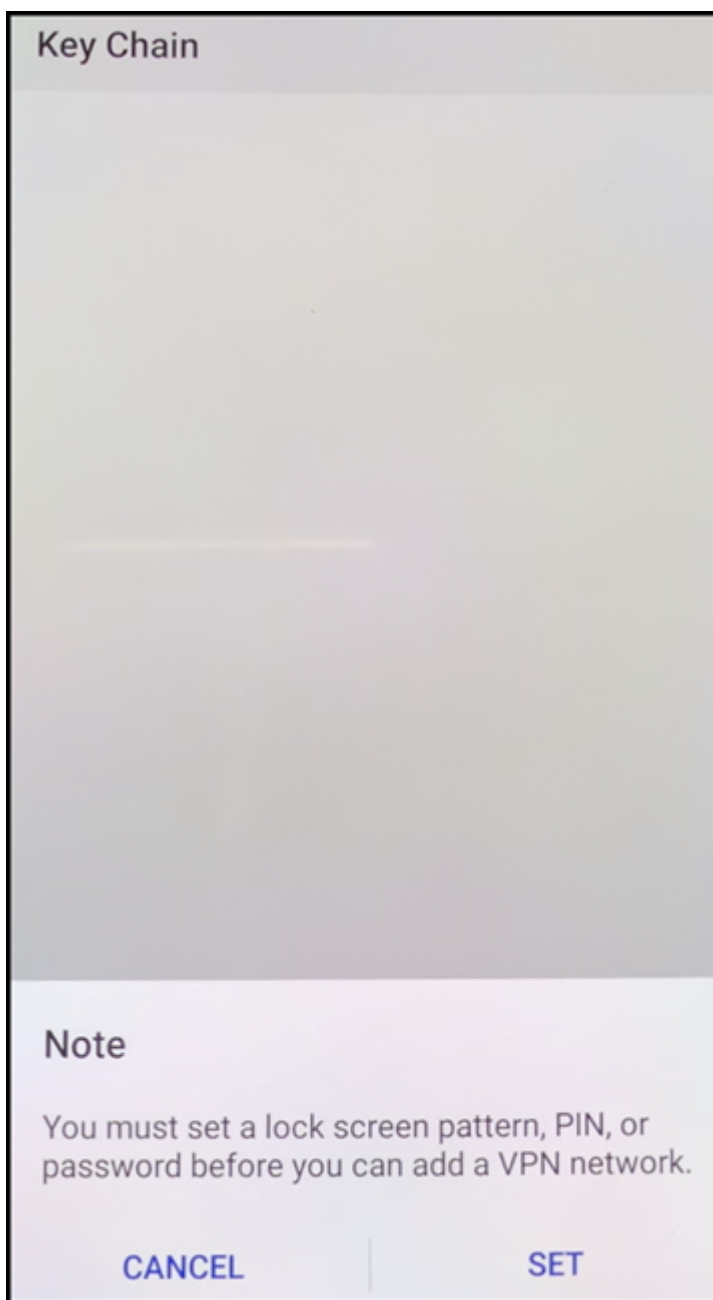
Back

Next

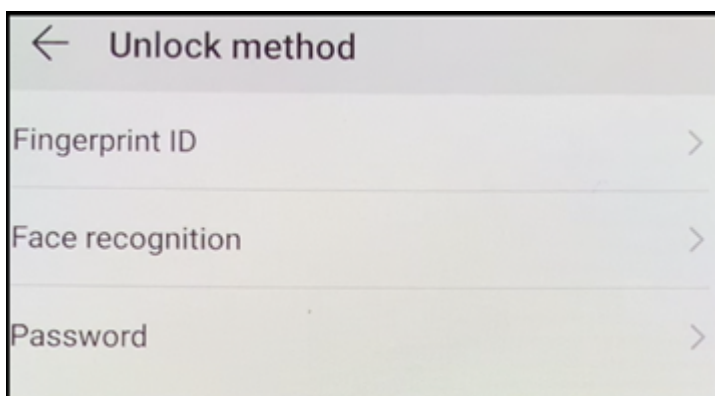
[Privacy Policy](#)

As required by Apple policy, we do not share any data collected by our service with any third parties for any reason.

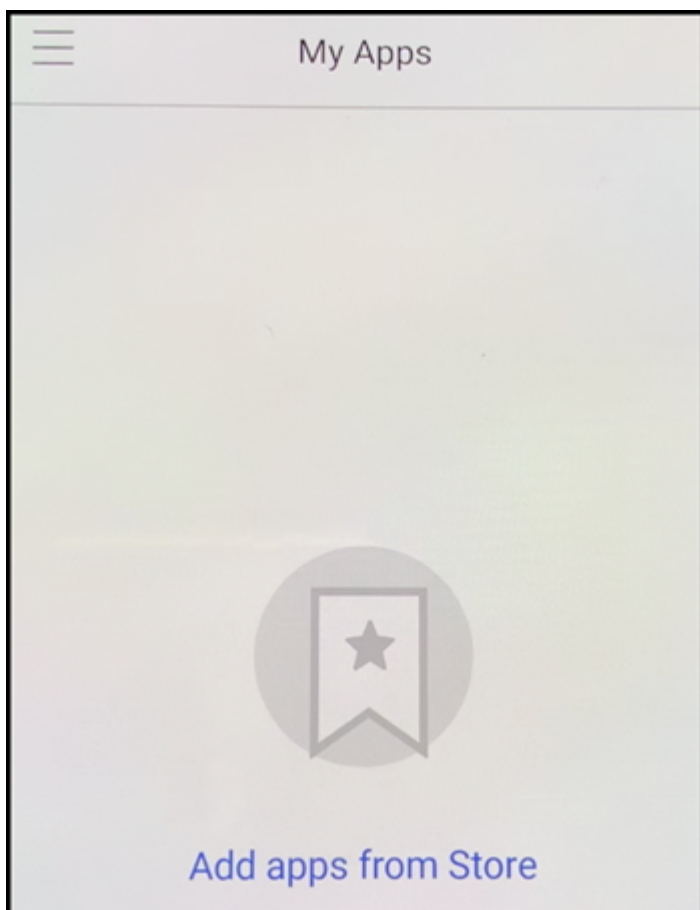
11. O usuário é solicitado a configurar o código secreto do dispositivo. Toque em **Definir** e insira um código secreto.



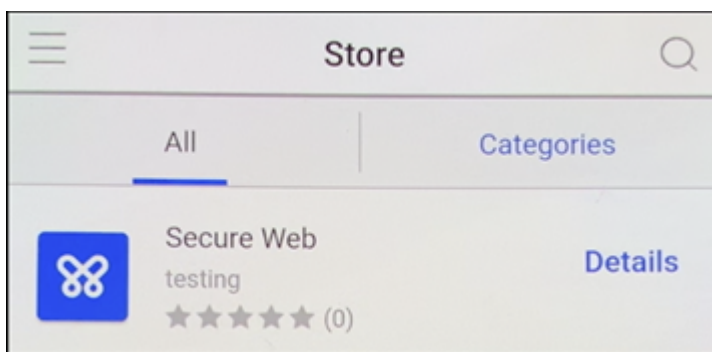
12. O usuário é solicitado a configurar um método de desbloqueio do perfil de trabalho. Para este exemplo, toque em **Senha**, toque em **PIN** e digite um PIN.



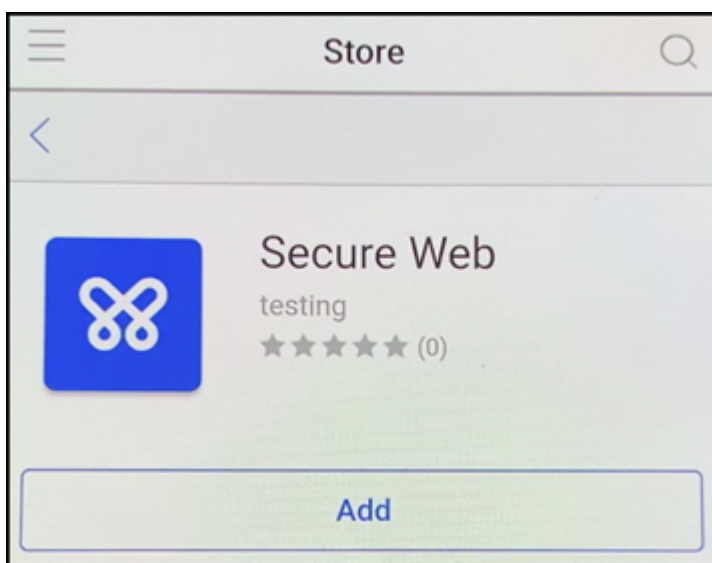
13. O dispositivo está agora na tela inicial **Meus aplicativos** do Secure Hub. Toque em **Adicionar aplicações da loja**.



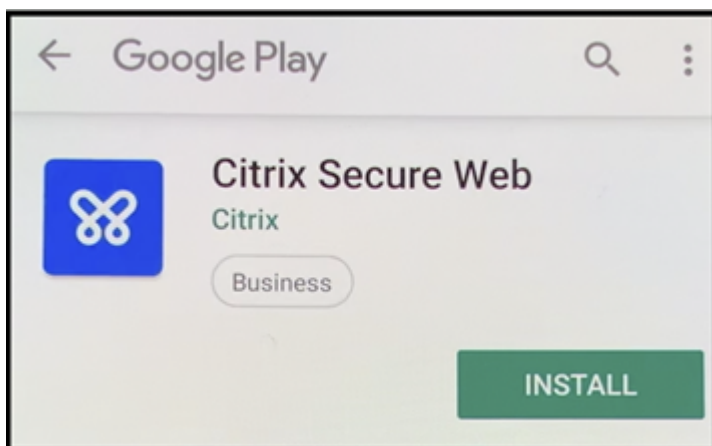
14. Para adicionar o Secure Web, toque em **Secure Web**.



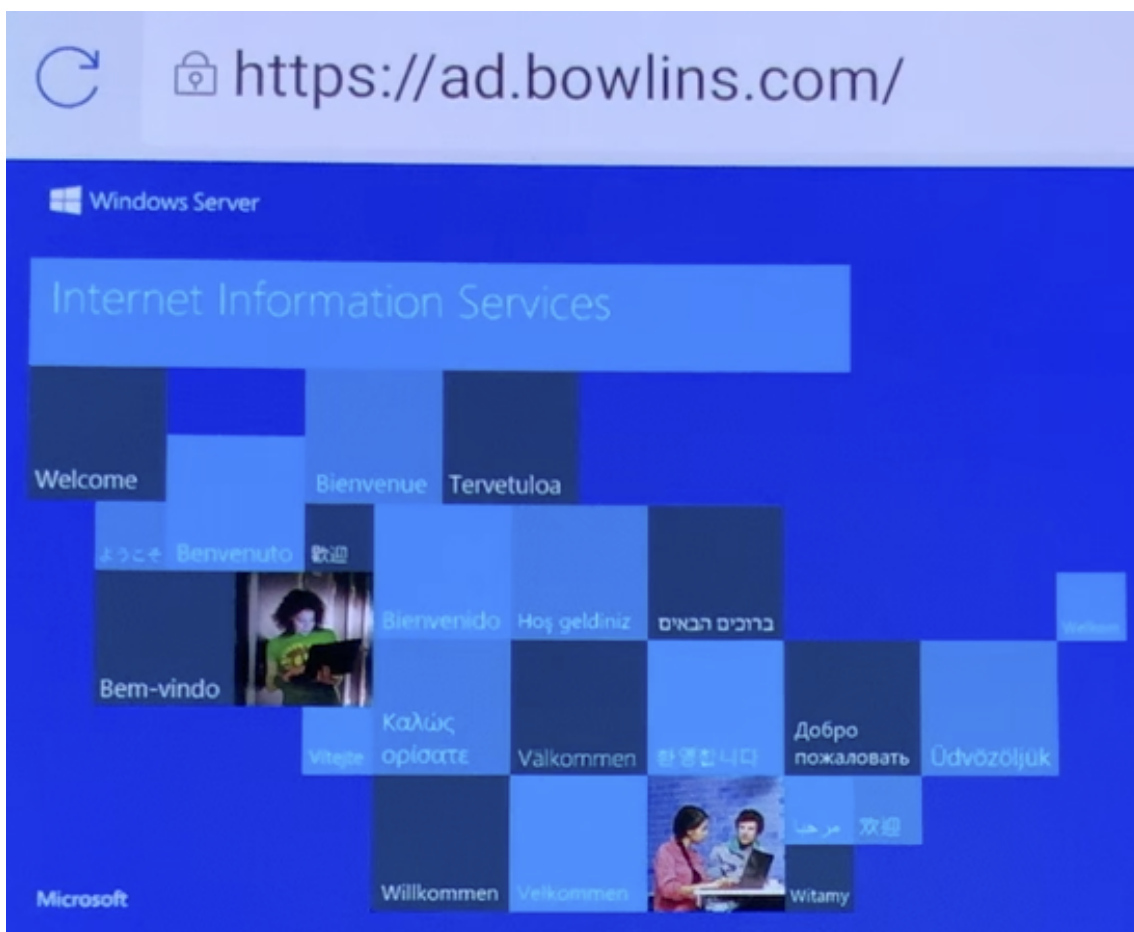
15. Toque em **Adicionar**.



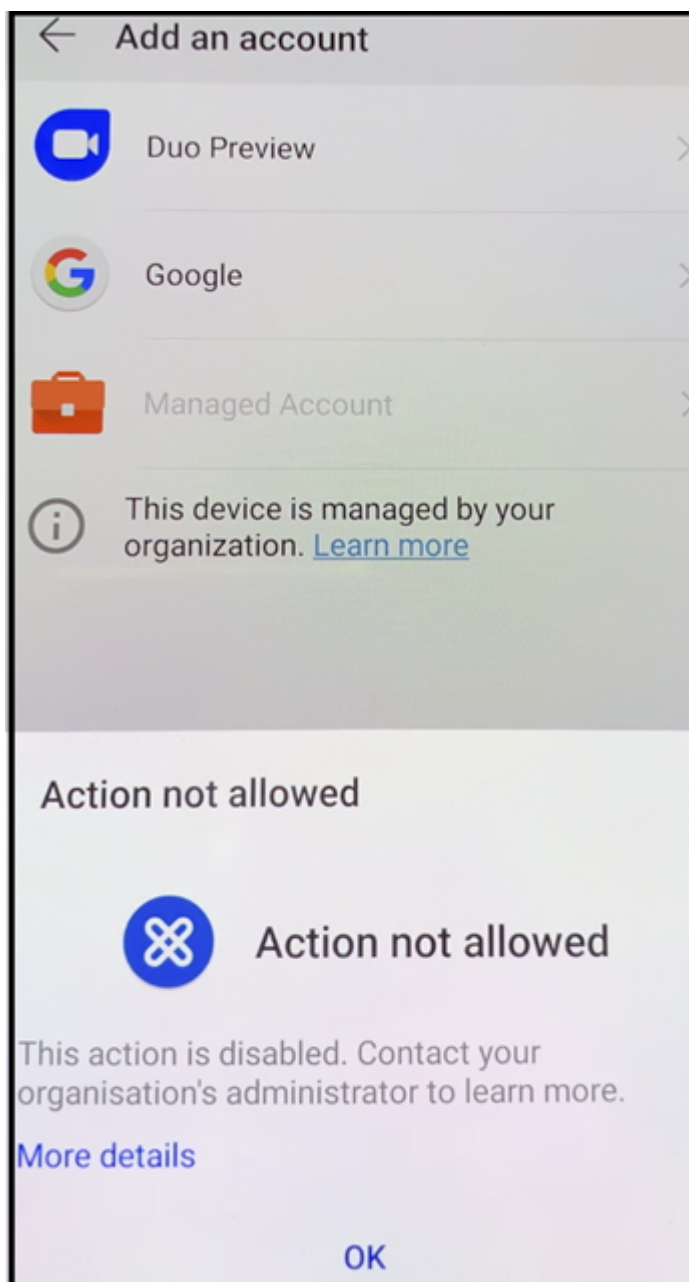
16. O Secure Hub direciona o usuário para o Google Play Store para instalar o Secure Web. Toque em **Instalar**.



17. Depois que o Secure Web for instalado, toque em **Abrir**. Insira a URL de um site interno na barra de endereços e verifique se a página é carregada.



18. Vá para **Configurações > Contas** no dispositivo. Observe que a **conta gerenciada** não pode ser modificada. As opções do desenvolvedor para compartilhamento de tela ou depuração remota também são bloqueadas.



Registrar dispositivos com NFC bump

Registrar um dispositivo como um dispositivo totalmente gerenciado usando compartilhamentos por NFC requer dois dispositivos: um cujas configurações de fábrica sejam redefinidas e um que esteja executando a XenMobile Provisioning Tool.

Requisitos do sistema e pré-requisito

- Dispositivos Android com suporte.

- Um dispositivo novo ou com redefinição de fábrica, provisionado para o Android Enterprise como um dispositivo totalmente gerenciado. Você pode encontrar as etapas para concluir esse pré-requisito neste artigo.
- Outro dispositivo com recursos NFC executando a Provisioning Tool configurada. A Provisioning Tool está disponível no Secure Hub ou na [página de downloads da Citrix](#).

Cada dispositivo pode ter apenas um perfil Android Enterprise gerenciado do Secure Hub. Somente um perfil é permitido em cada dispositivo. A tentativa de adicionar um segundo aplicativo DPC remove o Secure Hub instalado.

Dados transferidos através do aumento de NFC

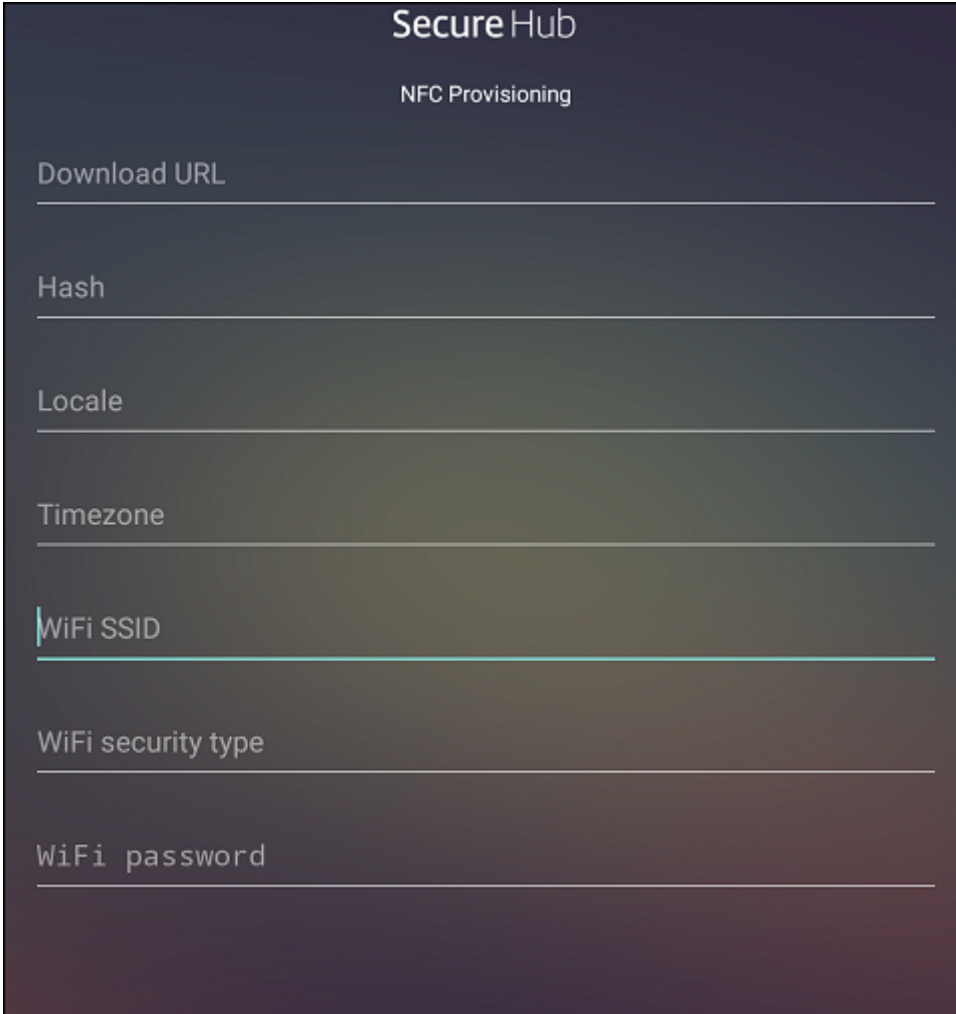
Provisionar um dispositivo com redefinição de fábrica requer que você envie os seguintes dados por meio de um NFC bump para inicializar o Android Enterprise:

- O nome do pacote do aplicativo DPC que atua como o proprietário do dispositivo (neste caso, o Secure Hub).
- A localização de Intranet/Internet da qual o dispositivo pode baixar o aplicativo DPC.
- O hash SHA1 do aplicativo DPC para verificar se o download é bem-sucedido.
- Os detalhes da conexão WiFi para que um dispositivo com redefinição de fábrica possa se conectar e baixar o aplicativo DPC. Nota: no momento, o Android não é compatível com WiFi 802.1x para esta etapa.
- O fuso horário do dispositivo (opcional).
- A localização geográfica do dispositivo (opcional).

Quando os dois dispositivos são aumentados, os dados da Provisioning Tool são enviados para o dispositivo com redefinição de fábrica. Esses dados são usados para baixar o Secure Hub com as configurações do administrador. Se você não inserir os valores de localização e fuso horário, o Android os configura automaticamente no novo dispositivo.

Configuração da XenMobile Provisioning Tool

Antes de realizar um aumento de NFC, você deve configurar a Provisioning Tool. Em seguida, essa configuração é transferida para o dispositivo com redefinição de fábrica durante o aumento de NFC.



Secure Hub

NFC Provisioning

Download URL

Hash

Locale

Timezone

WiFi SSID

WiFi security type

WiFi password

Você pode digitar dados nos campos obrigatórios ou preenchê-los usando um arquivo de texto. As etapas no procedimento a seguir descrevem como configurar o arquivo de texto e contém descrições para cada campo. O aplicativo não salva as informações depois que as digitar, portanto, convém criar um arquivo de texto para manter as informações para uso futuro.

Para configurar a Provisioning Tool usando um arquivo de texto

Dê ao arquivo o nome `ncfprovisioning.txt` e coloque-o na pasta `/sdcard/` no cartão SD do dispositivo. Em seguida, o aplicativo poderá ler o arquivo de texto e preencher os valores.

O arquivo de texto deve conter os seguintes dados:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<
download_location>
```

Essa linha é o local da intranet/internet do aplicativo do provedor EMM. Depois que o dispositivo com redefinição de fábrica se conectar a Wi-Fi em seguida ao aumento de NFC, o dispositivo deve ter

acesso a esse local para fazer o download. A URL é uma URL regular, sem necessidade de formatação especial.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA1 hash>
```

Essa linha é a soma de verificação do aplicativo do provedor EMM. Essa soma de verificação é usada para verificar se o download foi bem-sucedido. As etapas para obter a soma de verificação são discutidas neste artigo.

```
android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>
```

Esse é o SSID de Wi-Fi conectado do dispositivo no qual a Provisioning Tool está em execução.

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>
```

Os valores suportados são WEP e WPA2. Se o Wi-Fi for desprotegido, esse campo deverá estar vazio.

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>
```

Se o Wi-Fi for desprotegido, esse campo deverá estar vazio.

```
android.app.extra.PROVISIONING_LOCALE=<locale>
```

Insira os códigos de idioma e país. Os códigos de idioma são códigos de idioma ISO com duas letras minúsculas (por exemplo, en), conforme definido pela [ISO 639-1](#). Os códigos de país são códigos de país ISO com duas letras maiúsculas (por exemplo, US), conforme definido pela [ISO 3166-1](#). Por exemplo, digite en_US para o inglês falado nos Estados Unidos. Se você não digitar nenhum código, o país e o idioma serão preenchidos automaticamente.

```
android.app.extra.PROVISIONING_TIME_ZONE=<timezone>
```

O fuso horário no qual o dispositivo está em execução. Insira um [nome Olson da área/localização do formulário](#). Por exemplo, America/Los_Angeles para o horário do Pacífico. Se você não inserir nenhum nome, o fuso horário será preenchido automaticamente.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>
```

Isso não é necessário, pois o valor é inserido em código fixo no aplicativo, como o Secure Hub. Ele é mencionado aqui somente por uma questão de conclusão.

Se houver um Wi-Fi protegido por WPA2, um arquivo nfcprovisioning.txt preenchido terá a seguinte aparência:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk
```

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFk4Crh\nu003d
```

```
android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name
```

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2
```

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere
```

```
android.app.extra.PROVISIONING_LOCALE=en_US
```

```
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Se houver uma Wi-Fi desprotegida, um arquivo `nfcprovisioning.txt` preenchido terá a seguinte aparência:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk
```

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crh\u003d
```

```
android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name
```

```
android.app.extra.PROVISIONING_LOCALE=en_US
```

```
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Para obter a soma de verificação do Citrix Secure Hub

A soma de verificação do Secure Hub é um valor constante: `qn7oZUtheu3JBAinzZRrjCQv6L006Ll10jcxT3-yKM`. Para baixar um arquivo APK para o Secure Hub, use o seguinte link da loja do Google Play: <https://play.google.com/managed/downloadManagingApp?identifier=xenmobile>.

Para obter uma soma de verificação de aplicativo

Pré-requisitos:

- A ferramenta **apksigner** do Android SDK Build Tools
- Linha de comando OpenSSL

Para obter a soma de verificação de qualquer aplicativo, siga estas etapas:

1. Baixe o arquivo APK do aplicativo na loja do Google Play.
2. Na linha de comando OpenSSL, navegue até a ferramenta **apksigner**: `android-sdk/build-tools/<version>/apksigner` e digite o seguinte:

```
1 apksigner verify -print-certs <apk_path> | perl -nle 'print $$ if
   m{
2   (?<=SHA-256 digest:) .* }
3   ' | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/=' '-_'
4 <!--NeedCopy-->
```

O comando retorna uma soma de verificação válida.

3. Para gerar o código QR, insira a soma de verificação no campo `PROVISIONING_DEVICE_ADMIN_SIGNATURE`. Por exemplo:

```
1 {
2
3   "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.
4     zenprise/com.zenprise.configuration.AdminFunction",
5   "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "
6     qn7oZUtheu3JBAinzZRrjCQv6L006Ll10jcxT3-yKM",
7   "android.app.extra.
8     PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://
9     play.google.com/managed/downloadManagingApp?identifier=xenmobile",
10  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
11
12    "serverURL": "https://supportability.xm.cloud.com"
13  }
14 }
15 <!--NeedCopy-->
```

Bibliotecas usadas

A Provisioning Tool usa as seguintes bibliotecas no seu código-fonte:

- biblioteca v7 `appcompat`, Design Support Library e biblioteca v7 Palette do Google sob a licença Apache 2.0
- Para obter informações, consulte o [Guia de Recursos da Biblioteca de Suporte](#).
- `Butter Knife` de Jake Wharton sob a licença Apache 2.0

Registrar dispositivos usando um código QR

Para registrar um dispositivo totalmente gerenciado usando um código QR, você pode gerar um código QR criando um JSON e convertendo o JSON em um código QR. A câmera do dispositivo escaneia o código QR para registrar o dispositivo.

Requisitos do sistema

- Suportado em todos os dispositivos Android com Android 8.0 e superior.

Criar um código QR de um JSON

Crie um JSON com os seguintes campos.

Estes campos são obrigatórios:

Chave: `android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME`

Valor: `com.zenprise/com.zenprise.configuration.AdminFunction`

Chave: `android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM`

Valor: `qn7oZUtheu3JBAinzZRrjCQv6LOO6LL1OjcxT3-yKM`

Chave: `android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION`

Valor: <https://play.google.com/managed/downloadManagingApp?identifier=xenmobile>

Estes campos são opcionais:

- **android.app.extra.PROVISIONING_LOCALE:** insira os códigos de idioma e país.
Os códigos de idioma são códigos de idioma ISO com duas letras minúsculas (por exemplo, en), conforme definido pela [ISO 639-1](#). Os códigos de país são códigos de país ISO com duas letras maiúsculas (por exemplo, US), conforme definido pela [ISO 3166-1](#). Por exemplo, insira `en_US` para o inglês falado nos Estados Unidos.
- **android.app.extra.PROVISIONING_TIME_ZONE:** o fuso horário em que o dispositivo é executado.
Insira um [nome Olson da área/localização do formulário](#). Por exemplo, `America/Los_Angeles` para o horário do Pacífico. Se você não inserir um, o fuso horário será preenchido automaticamente.
- **android.app.extra.PROVISIONING_LOCAL_TIME:** tempo em milissegundos desde a época (Epoch).
A época do Unix (ou hora do Unix, hora do POSIX ou carimbo de data/hora do Unix) é o número de segundos decorridos desde 1º de janeiro de 1970 (meia-noite UTC/GMT). O tempo não inclui segundos bissextos (in ISO 8601: 1970-01-01T00:00:00Z).
- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** definido como **true** para ignorar a criptografia durante a criação do perfil. Defina como **false** para forçar a criptografia durante a criação do perfil.

Um JSON típico tem esta aparência:

Requisitos do sistema

- Suporte a registro sem toque começa com o Android 8.0.

Dispositivos e informações da conta fornecidas pelo seu revendedor

- Os dispositivos elegíveis para registro sem toque são comprados de um revendedor corporativo ou parceiro Google. Para obter uma lista de parceiros do Android Enterprise zero-touch, consulte o [site do Android](#).
- Uma conta do portal de registro sem toque do Android Enterprise, criada pelo seu revendedor.
- Informações de login da conta do portal de registro sem toque do Android Enterprise, fornecidas pelo seu revendedor.

Criar uma configuração sem toque

Quando você criar uma configuração toque zero, inclua um JSON personalizado para especificar detalhes da configuração.

Use este JSON para configurar o dispositivo para se registrar no XenMobile Server especificado. Substitua a URL do seu servidor por 'URL' neste exemplo.

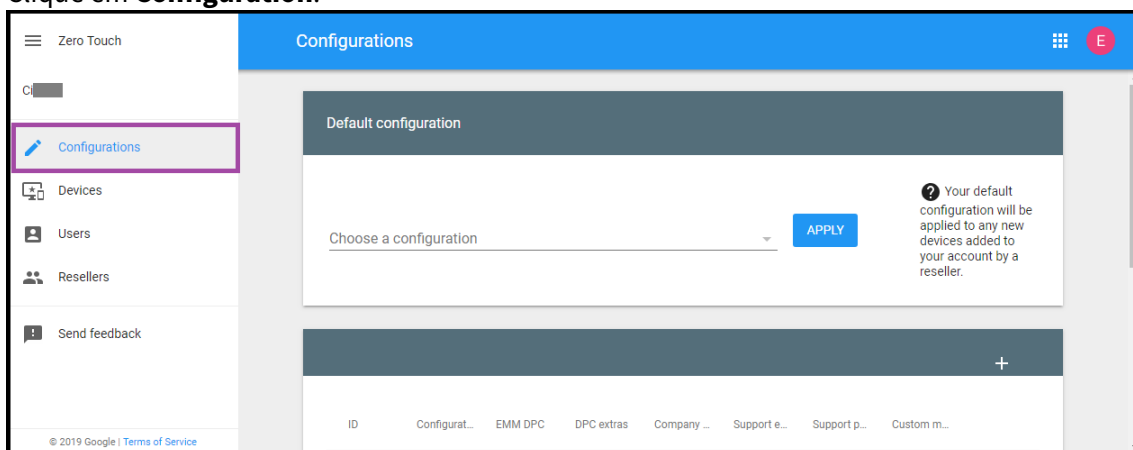
```
1      {
2
3          "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4      {
5
6          "serverURL": "URL",
7      }
8
9      }
10
11 <!--NeedCopy-->
```

Você pode usar um JSON opcional com mais parâmetros para personalizar ainda mais a sua configuração. Este exemplo especifica o XenMobile Server e o nome de usuário e senha que os dispositivos que usam essa configuração usam para fazer logon no servidor.

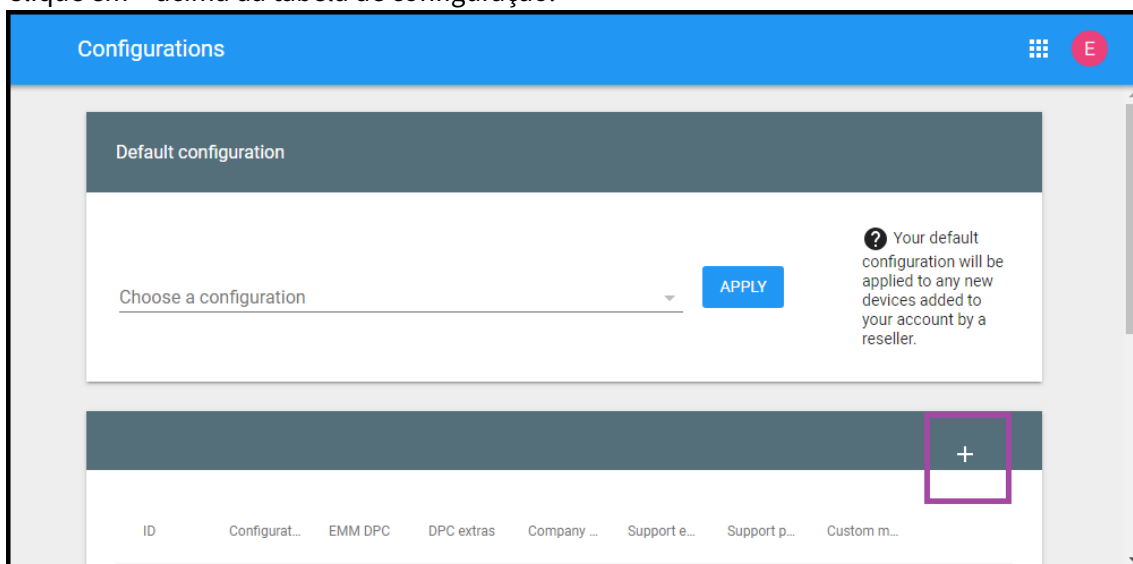
```
1      {
2
3          "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4      {
5
6          "serverURL": "URL",
7          "xm_username": "username",
```

```
8         "xm_password": "password"
9     }
10
11     }
12
13     <!--NeedCopy-->
```

1. Acesse o portal do Android zero-touch em <https://partner.android.com/zerotouch>. Inicie uma sessão com as informações da conta fornecidas pelo seu revendedor de dispositivos sem toque.
2. Clique em **Configuration**.



3. Clique em **+** acima da tabela de configuração.



4. Insira suas informações de configuração na janela de configuração que aparece.

The screenshot shows a mobile-style dialog box titled "Add a new configuration". It features a list of input fields for configuration details. The fields are: "Configuration name", "EMM DPC" (a dropdown menu with "Select" as the current selection), "DPC extras", "Company name", "Support email address", and "Support phone number". At the bottom right, there are two buttons: "CANCEL" and "ADD". A vertical scrollbar is visible on the right side of the dialog, with the number "132" partially visible at the bottom.

- **Configuration name:** digite o nome escolhido para esta configuração.
- **EMM DPC:** Escolha **Citrix Secure Hub**.
- **DPC extras:** Cole seu texto JSON personalizado neste campo.
- **Company name:** digite o nome que deseja que apareça nos dispositivos Android Enterprise sem toque durante o provisionamento do dispositivo.
- **Support email address:** digite um endereço de e-mail para que seus usuários possam

entrar em contato para obter ajuda. Esse endereço aparece nos seus dispositivos Android Enterprise sem toque antes do provisionamento do dispositivo.

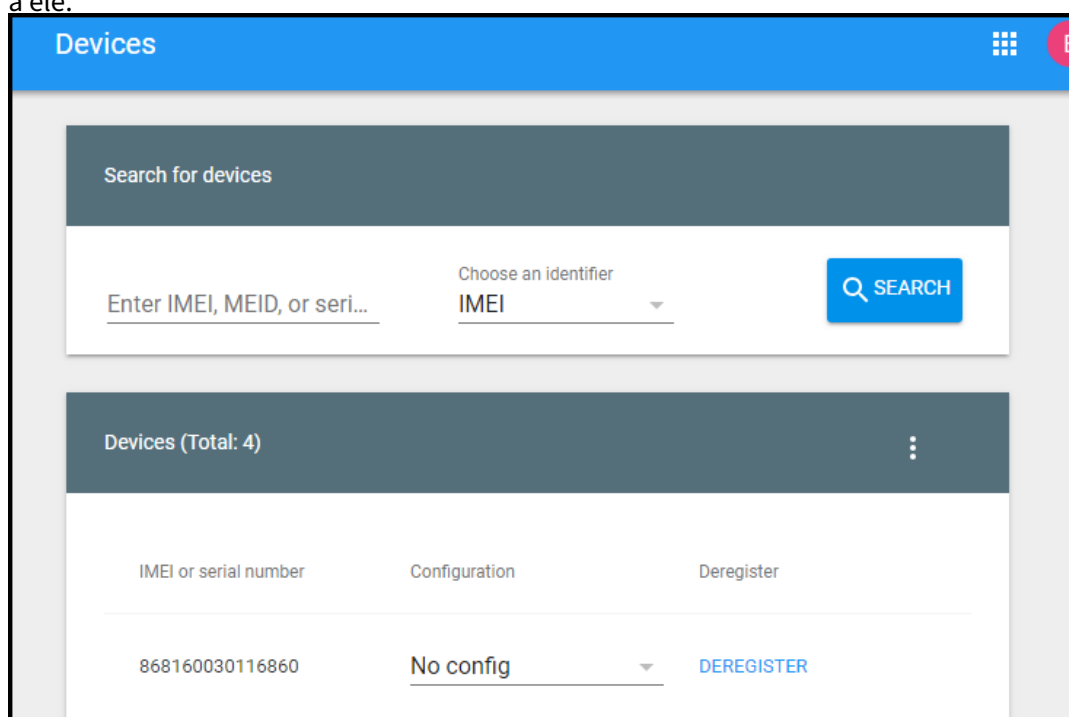
- **Support phone number:** digite um número de telefone para que seus usuários possam entrar em contato para obter ajuda. Esse número de telefone aparece nos seus dispositivos Android Enterprise sem toque antes do provisionamento do dispositivo.
- **Custom Message:** opcionalmente, adicione uma ou duas frases para ajudar os usuários a entrar em contato com você ou fornecer mais detalhes sobre o que está acontecendo com o dispositivo deles. Essa mensagem personalizada aparece nos seus dispositivos Android Enterprise sem toque antes do provisionamento do dispositivo.

5. Clique em **Add**.

6. Para criar mais configurações, repita as etapas 2 a 4.

7. Para aplicar uma configuração a um dispositivo:

- a) No portal de registro sem toque do Android, clique em **Devices**.
- b) Localize o dispositivo na lista de dispositivos e escolha a configuração que deseja atribuir a ele.



c) Clique em **Update**.

Você pode aplicar uma configuração a vários dispositivos usando um arquivo CSV.

Para obter informações sobre como aplicar uma configuração a vários dispositivos, consulte o tópico de ajuda do Android Enterprise [Zero-touch enrollment for IT admins](#). Esse tópico de ajuda do Android Enterprise contém mais informações sobre como gerenciar configurações e aplicá-las a dispositivos.

Provisionamento de dispositivos Android Enterprise dedicados

Os dispositivos Android Enterprise dedicados são dispositivos totalmente gerenciados e dedicados a atender a um único caso de uso. Dispositivos dedicados também são conhecidos como dispositivos corporativos para uso único (COSU). Você restringe esses dispositivos a um aplicativo ou a um pequeno conjunto de aplicativos necessários para executar as tarefas necessárias para o caso de uso. Você também impede que os usuários habilitem outros aplicativos ou executem outras ações no dispositivo.

Registrar dispositivos dedicados usando qualquer um dos métodos de registro usados para outros dispositivos totalmente gerenciados, conforme descrito em Provisionamento de dispositivos Android Enterprise totalmente gerenciados. O provisionamento de dispositivos dedicados requer mais configuração antes do registro.

Para provisionar dispositivos dedicados:

- Adicione um perfil de registro para administradores do XenMobile os quais você permite que registrem dispositivos dedicados na sua implantação do XenMobile. Consulte Criar perfis de registro.
- Acrescente à lista de permissão os aplicativos que você deseja que o dispositivo dedicado acesse.
- Opcionalmente, coloque o aplicativo na lista de permissão para permitir o modo de bloqueio de tarefa. Quando um aplicativo está no modo de bloqueio de tarefa, ele é fixado na tela do dispositivo quando o usuário o abre. O botão Início não aparece e o botão Voltar fica desativado. O usuário sai do aplicativo usando uma ação programada no aplicativo, como logoff.
- Registre cada dispositivo no perfil de registro que você adicionou.

Requisitos do sistema

- Suporte para registrar dispositivos dedicados começa com o Android 6.0.

Acrescentar aplicativos à lista de permissão e definir o modo de bloqueio de tarefa

A política de dispositivo de quiosque permite que você acrescente aplicativos à lista de permissão e defina o modo de bloqueio de tarefa. Por padrão, os serviços Secure Hub e Google Play são permitidos.

Para adicionar a política de quiosque:

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.
2. Clique em **Add**. É exibida a caixa de diálogo **Adicionar uma nova política**.
3. Expanda **Mais** e, em Segurança, clique em **Quiosque**. A página **Política de quiosque** é exibida.
4. Em Plataformas, selecione **Android Enterprise**. Limpe as outras plataformas.

5. No painel de Informações da Política, digite o **Nome da Política** e uma **Descrição** opcional.
6. Clique em **Avançar** e, em seguida, clique em **Adicionar**.
7. Para acrescentar um aplicativo à lista de permissão e permitir ou negar o modo de bloqueio de tarefa do aplicativo:

Selecione o aplicativo que você deseja permitir na lista.

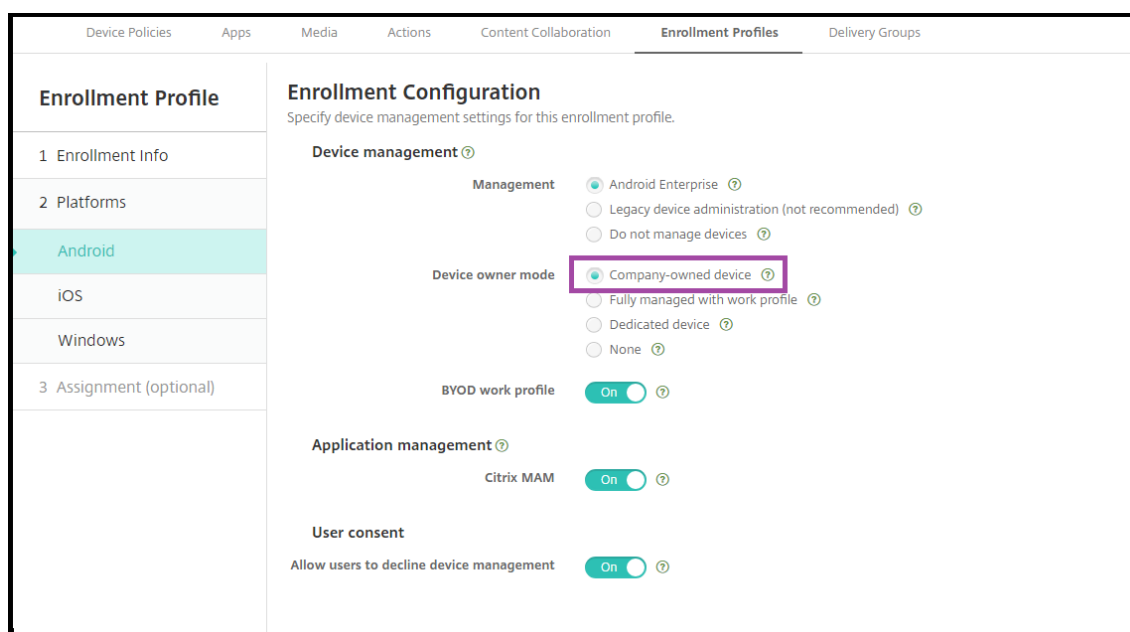
Escolha **Permitir** para que o aplicativo seja fixado na tela do dispositivo quando o usuário iniciar o aplicativo. Escolha **Negar** para que o aplicativo não seja fixado. O padrão é **Permitir**.

Apps to whitelist *	Lock task status	
Cosu App	<input checked="" type="radio"/> Allow <input type="radio"/> Deny	Save Cancel

8. Clique em **Save**.
9. Para acrescentar outro aplicativo à lista de permissão e permitir ou negar o modo de bloqueio de tarefa do aplicativo, clique em **Adicionar**.
10. Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte a [Política de dispositivo de VPN](#).

Para registrar o dispositivo

1. Clique em **Avançar** ou selecione **Android** em **Plataformas**. A página de configuração de registro é exibida.
2. Defina **Gerenciamento** para **Android Enterprise**.
3. Defina **Modo proprietário do dispositivo** como **Dispositivo de propriedade da empresa**.



4. Selecione **Atribuição (opções)**. A tela Atribuição de grupo de entrega é exibida.
5. Escolha um grupo de entrega ou grupos de entrega contendo os administradores que registram dispositivos dedicados. Em seguida, clique em **Save**.

Se você habilitou o **Perfil de trabalho BYOD** no perfil de registro, os dispositivos que não são novos ou redefinidos de fábrica serão registrados como dispositivos de perfil de trabalho. Consulte [Provisionar dispositivos de perfil de trabalho Android Enterprise](#).

Provisionar dispositivos Android Enterprise totalmente gerenciados com um perfil de trabalho (dispositivos COPE)

Dispositivos totalmente gerenciados com um perfil de trabalho, anteriormente chamados de dispositivos COPE, são dispositivos de propriedade da empresa que são usados para fins pessoais e profissionais. Sua organização gerencia os dispositivos por completo. Você pode aplicar um conjunto de políticas ao dispositivo e um conjunto separado de políticas ao perfil de trabalho.

No console XenMobile, os dispositivos totalmente gerenciados com um perfil de trabalho aparecem com estes termos:

- A propriedade do dispositivo é “Corporativo”.
- O tipo de instalação do dispositivo Android Enterprise é “Propriedade da empresa, habilitado pessoalmente”.

Requisitos do sistema

- O suporte para registrar dispositivos totalmente gerenciados com perfis de trabalho começa com o Android 8.0.

Adicionar um perfil de registro para dispositivos totalmente gerenciados com perfis de trabalho

Crie um perfil de registro para registrar dispositivos totalmente gerenciados com perfis de trabalho. Os administradores nos grupos de entrega atribuídos a esse perfil de registro podem registrar dispositivos totalmente gerenciados com perfis de trabalho. Para garantir que esses administradores possam registrar todos os dispositivos necessários, crie um perfil de registro para eles com dispositivos ilimitados permitidos por usuário. Atribua esse perfil a um grupo de entrega contendo os administradores que registram os dispositivos totalmente gerenciados com perfis de trabalho.

1. No console XenMobile, vá para **Configurar > Perfis de registro**.
2. Para adicionar um perfil de registro, clique em **Adicionar**. Na página de Informações de registro, digite um nome para o perfil de registro. Certifique-se de que o número de dispositivos que os membros com este perfil podem registrar esteja definido como ilimitado.
3. Clique em **Avançar** ou selecione **Android Enterprise** em **Plataformas**. A página de configuração de registro é exibida.
4. Defina o **Tipo de inscrição/registo** como um dos seguintes:
 - **Totalmente gerenciado/Perfil de trabalho:** novos dispositivos ou dispositivos com reconfiguração de fábrica se registram totalmente gerenciados. Os dispositivos BYOD se registram com apenas um perfil de trabalho gerenciado por você.
 - **COPE/Perfil de trabalho:** novos dispositivos ou dispositivos com reconfiguração de fábrica se registram totalmente gerenciados com um perfil de trabalho. Os dispositivos BYOD se registram com apenas um perfil de trabalho gerenciado por você.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	<p>Device management ?</p> <p>Management</p> <p><input checked="" type="radio"/> Android Enterprise ?</p> <p><input type="radio"/> Legacy device administration (not recommended) ?</p> <p><input type="radio"/> Do not manage devices ?</p> <p>Device owner mode</p> <p><input checked="" type="radio"/> Company-owned device ?</p> <p><input type="radio"/> Fully managed with work profile ?</p> <p><input type="radio"/> Dedicated device ?</p> <p><input type="radio"/> None ?</p> <p>BYOD work profile <input checked="" type="checkbox"/> ?</p> <p>Application management ?</p> <p>Citrix MAM <input checked="" type="checkbox"/> ?</p> <p>User consent</p> <p>Allow users to decline device management <input checked="" type="checkbox"/> ?</p>
Android	
iOS	
3 Assignment (optional)	

5. Selecione **Atribuição (opcional)** ou clique em **Avançar**. A tela Atribuição de grupo de entrega é exibida.
6. Escolha um grupo de entrega ou grupos de entrega contendo os administradores que registram dispositivos dedicados. Em seguida, clique em **Save**.

A página de Perfil de registro é exibida com o perfil que você adicionou.

Device Policies	Apps	Media	Actions	Content Collaboration	Enrollment Profiles	Delivery Groups															
<p>Enrollment Profiles</p> <p>Search <input type="text"/></p> <p> Add</p> <table border="1"> <thead> <tr> <th><input type="checkbox"/></th> <th>Enrollment profile name</th> <th>Created on</th> <th>Updated on</th> <th>Device limit</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>COPE devices</td> <td>11/1/19 1:01:51 pm</td> <td>11/1/19 1:01:51 pm</td> <td>unlimited</td> </tr> <tr> <td><input type="checkbox"/></td> <td>Global</td> <td>10/28/19 5:30:39 am</td> <td>10/28/19 5:30:39 am</td> <td>unlimited</td> </tr> </tbody> </table> <p>Showing 1 - 2 of 2 items Items per page: <input type="text" value="10"/></p>						<input type="checkbox"/>	Enrollment profile name	Created on	Updated on	Device limit	<input type="checkbox"/>	COPE devices	11/1/19 1:01:51 pm	11/1/19 1:01:51 pm	unlimited	<input type="checkbox"/>	Global	10/28/19 5:30:39 am	10/28/19 5:30:39 am	unlimited	
<input type="checkbox"/>	Enrollment profile name	Created on	Updated on	Device limit																	
<input type="checkbox"/>	COPE devices	11/1/19 1:01:51 pm	11/1/19 1:01:51 pm	unlimited																	
<input type="checkbox"/>	Global	10/28/19 5:30:39 am	10/28/19 5:30:39 am	unlimited																	

Se um usuário pertencer a vários grupos de entrega que têm perfis de registro diferentes, o nome do grupo de entrega determinará o perfil de registro usado. O XenMobile seleciona o grupo de entrega que aparece por último em uma lista alfabética de grupos de entrega,

Para registrar o dispositivo

Dispositivos novos e com reconfiguração de fábrica se registram como dispositivos totalmente gerenciados com um perfil de trabalho usando o token do identificador DPC, o compartilhamento de comu-

nicação a curta distância (NFC) ou métodos de código QR. Consulte Registrar dispositivos usando o token identificador Citrix DPC, Registrar dispositivos com NFC bump ou Registrar dispositivos usando um código QR.

Dispositivos que não são novos nem com reconfiguração de fábrica se registram como dispositivos de perfil de trabalho conforme descrito em [Provisionar dispositivos de perfil de trabalho Android Enterprise](#).

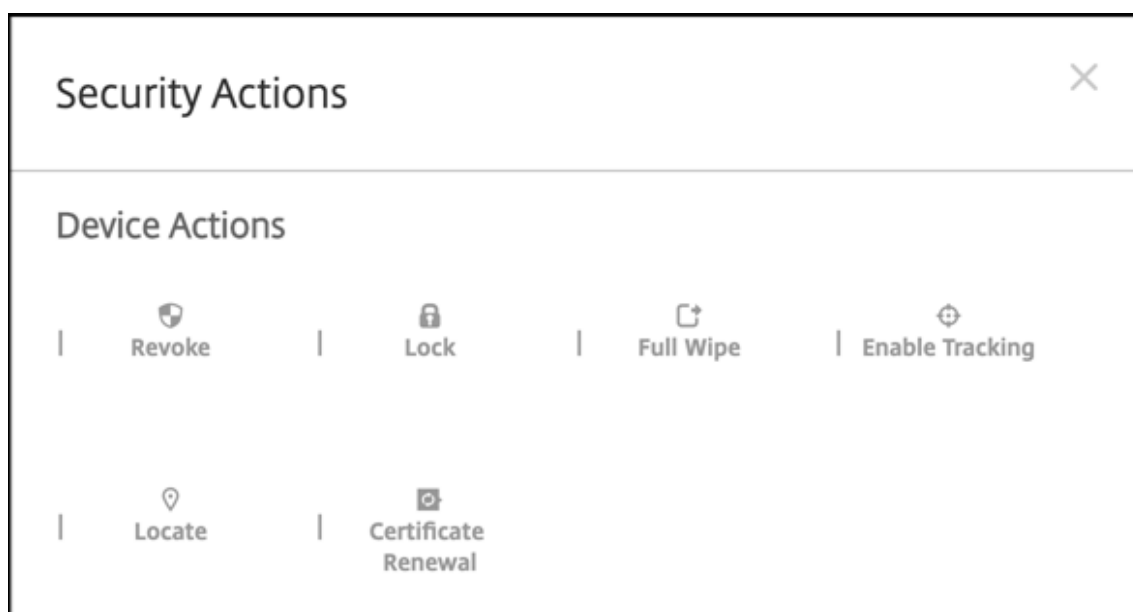
Exibir dispositivos Android Enterprise no console XenMobile

1. No console XenMobile, vá para **Gerenciar > Dispositivos**.
2. Adicione a coluna **Dispositivo Android Enterprise ativado?** clicando no menu à direita da tabela na página.

The screenshot shows the 'Enrolled Devices' page in the XenMobile console. At the top, there are tabs for 'Enrolled Devices' and 'Device Whitelist', and a search bar. Below the tabs, there are icons for 'Add', 'Import', 'Export', and 'Refresh'. The main area contains a table with the following columns: Status, Mode, User name, Device platform, Operating system version, Device model, Last access, Inactivity days, and Android Enterprise Enabled Device?. The table lists two devices: one with user 'mbbowlin' on an iOS device and another with user 'testing2' on an Android Pixel XL device. A dropdown menu is open on the right side of the table, showing a list of columns to be added, with 'Android Enterprise Enabled Device?' highlighted at the bottom.

Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days	Android Enterprise Enabled Device?
<input type="checkbox"/>	MDM	mbbowlin "mbbowlin"	iOS			5/7/19 1:01:50 pm	33 days	<input checked="" type="checkbox"/>
<input type="checkbox"/>	MDM MAM	testing2 "testing2"	Android	9	Pixel XL	6/10/19 8:06:51 am	0 day	<input checked="" type="checkbox"/>

3. Para exibir as ações de segurança disponíveis, selecione um dispositivo totalmente gerenciado e clique em **Segurança**. Quando o dispositivo é totalmente gerenciado, a ação **Apagamento completo** fica disponível, mas **Apagamento seletivo** não. Essa diferença se dá porque o dispositivo só permite aplicativos da loja Google Play gerenciada. Não há nenhuma opção para o usuário instalar aplicativos da loja pública. Sua organização gerenciou todo o conteúdo no dispositivo.



Configurar políticas de aplicativo e de dispositivo Android Enterprise

Para obter uma visão geral das políticas controladas nos níveis de dispositivo e aplicativo, consulte as [políticas de dispositivo suportadas](#) e [políticas MDX para Android Enterprise](#).

O que saber sobre políticas:

- **Proteção contra perda de dados:** a tecnologia de contêiner MAM XenMobile protege aplicativos com criptografia e outras tecnologias móveis de prevenção contra perda de dados (DLP). Use o Citrix MAM SDK, MDX Service ou MDX Toolkit para aplicativos habilitados para MDX.
- **Restrições do dispositivo:** dezenas de restrições de dispositivo permitem controlar recursos como:
 - Uso da câmera do dispositivo
 - Uso de copiar e colar entre perfis profissionais e pessoais
- **VPN por aplicativo:** use a política de dispositivo de Configurações gerenciadas para configurar perfis VPN para Android Enterprise.
- **Política de e-mail:** recomendamos usar a política de dispositivo de Configurações gerenciadas para configurar aplicativos.

Esta tabela lista todas as políticas de dispositivo disponíveis para dispositivos Android Enterprise.

Importante:

para dispositivos que se registram no Android Enterprise e usam aplicativos MDX: você pode con-

Controlar algumas configurações por meio do MDX e do Android Enterprise. Use as configurações de política menos restritivas para MDX e controle a política por meio do Android Enterprise.

Permissões do aplicativo Enterprise Android	Configurações gerenciadas do Android Enterprise	Inventário de aplicativos
Desinstalação de aplicativo	Atualizar automaticamente aplicativos gerenciados	Controlar atualização de SO
Credenciais	XML personalizado	Exchange
Arquivos	Gerenciamento de proteção do teclado	Quiosque
Localização	Código secreto	Restrições
Chave de licença MDM Samsung	Programação	Wi-Fi
Opções do XenMobile		

Políticas de dispositivo para dispositivos totalmente gerenciados com perfil de trabalho (dispositivos COPE)

Para dispositivos totalmente gerenciados com perfis de trabalho (dispositivos COPE), algumas políticas de dispositivo podem ser usadas para aplicar configurações separadas a todo o dispositivo e ao perfil de trabalho. Você pode usar outras políticas de dispositivo para aplicar configurações apenas para o dispositivo todo ou apenas para o perfil de trabalho de dispositivos totalmente gerenciados com perfis de trabalho.

Política	Aplica-se a
Permissões do aplicativo Enterprise Android	Perfil de trabalho
Configurações gerenciadas do Android Enterprise	Perfil de trabalho
Inventário de aplicativos	Perfil de trabalho
Desinstalação de aplicativo	Perfil de trabalho
Atualizar automaticamente aplicativos gerenciados	Perfil de trabalho
Controlar atualização de SO	N/A

Política	Aplica-se a
Credenciais	Perfil de trabalho
XML personalizado	N/A
Exchange	N/A
Arquivos	Perfil de trabalho
Gerenciamento de proteção do teclado	Dispositivo e perfil de trabalho
Quiosque	N/A
Localização	Dispositivo (somente modo de localização)
Código secreto	Dispositivo e perfil de trabalho
Restrições	Dispositivo e perfil de trabalho (crie políticas separadas para o dispositivo e o perfil de trabalho)
Chave de licença MDM Samsung	N/A
Programação	Perfil de trabalho
Wi-Fi	Dispositivo
Opções do XenMobile	Perfil de trabalho

Consulte também as [políticas MDX](#) e [políticas de dispositivo com suporte para Android Enterprise](#) e [Visão geral do MAM SDK](#).

Ações de segurança

O Android Enterprise suporta as seguintes ações de segurança. Para obter uma descrição de cada ação de segurança, consulte [Ações de segurança](#).

Ação de segurança	Perfil de trabalho	Totalmente gerenciado
Renovação de certificado	Sim	Sim
Apagamento completo	Não	Sim
Localizar	Sim	Sim
Bloquear	Sim	Sim
Bloquear e redefinir senha	Não	Sim
Notificar (Tocar)	Sim	Sim

Ação de segurança	Perfil de trabalho	Totalmente gerenciado
Revogar	Sim	Sim
Apagamento seletivo	Sim	Não

Observações sobre a Ação de segurança

- A ação de segurança Localizar falha a menos que a política de dispositivo de Localizar defina o modo de localização do dispositivo como **Alta precisão** ou **Economia de bateria**. Consulte [Política de dispositivo de localização](#).
- Em dispositivos de perfil de trabalho que executam versões do Android anteriores ao Android 8.0:
 - A ação de bloqueio e redefinição de senha não é suportada.
- Em dispositivos de perfil de trabalho com Android 8.0 ou superior:
 - O código secreto enviado bloqueia o perfil de trabalho. O dispositivo em si não é bloqueado.
 - Se nenhum código secreto estiver definido no perfil de trabalho:
 - * Se não for enviado um código secreto, ou se o código secreto enviado não atender aos requisitos de código secreto, o dispositivo será bloqueado.
 - Se um código secreto estiver definido no perfil de trabalho:
 - * Se não for enviado um código secreto, ou se o código secreto enviado não atender aos requisitos de código secreto: o perfil de trabalho será bloqueado, mas o dispositivo em si não será bloqueado.
- Em dispositivos totalmente gerenciados com perfis de trabalho (dispositivos COPE):
 - Você pode aplicar a ação de segurança Bloquear separadamente ao dispositivo ou ao perfil de trabalho

Cancelar o registro de um enterprise do Android Enterprise

Se você não quiser mais usar o seu enterprise do Android Enterprise, poderá cancelar o registro do enterprise.

Aviso:

Depois de cancelar o registro de um enterprise, os aplicativos Android Enterprise nos dispositivos já registrados por meio dele são redefinidos para os estados padrão. O Google não gerencia mais os dispositivos. Se você se registrar em um novo enterprise do Android Enterprise, deverá

aprovar aplicativos para a nova organização a partir do Google Play gerenciado. Depois, você pode atualizar os aplicativos a partir do console XenMobile.

Depois que o registro do enterprise do Android Enterprise for cancelado:

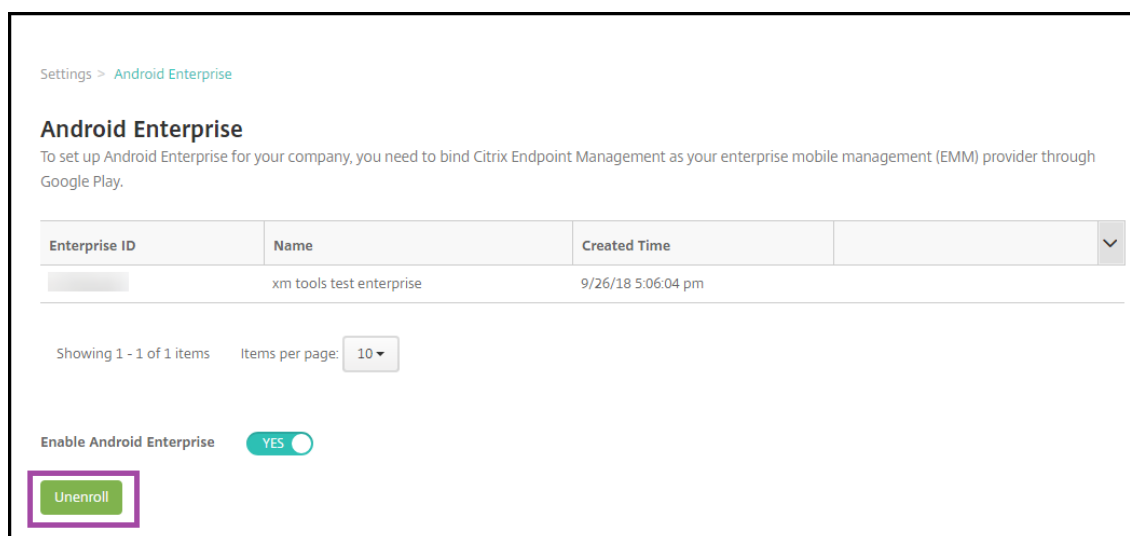
- Dispositivos e usuários registrados pelo Enterprise têm os aplicativos do Android Enterprise redefinidos para o estado padrão. As políticas de Configurações Gerenciadas do Android Enterprise aplicadas anteriormente não afetam mais as operações.
- O XenMobile gerencia dispositivos registrados por meio do enterprise. Do ponto de vista do Google, esses dispositivos não são gerenciados. Você não pode adicionar novos aplicativos Android Enterprise. Não é possível aplicar políticas de Configurações Gerenciadas do Android Enterprise. Você pode aplicar outras políticas, como Agendamento, Senha e Restrições a esses dispositivos.
- Se você tentar registrar dispositivos no Android Enterprise, eles serão registrados como dispositivos Android, não como dispositivos Android Enterprise.

Cancele o registro de um enterprise do Android Enterprise usando o console do XenMobile Server e o XenMobile Tools.

Quando você executa essa tarefa, o XenMobile abre uma janela pop-up para o XenMobile Tools. Antes de começar, verifique se o XenMobile tem permissão para abrir janelas pop-up no navegador que você está usando. Alguns navegadores, como o Google Chrome, exigem que você desabilite o bloqueio de pop-ups e acrescente o endereço do site do XenMobile à lista de permissão de bloqueio de pop-up.

Para cancelar o registro de um enterprise do Android Enterprise:

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página Settings é exibida.
2. Na página Settings, clique em **Android Enterprise**.
3. Clique em **Cancelar registro**.



```
amp; if m{(?<=SHA-256 digest:) .*}' | xxd -r -p | openssl base64 | tr -d '=' | tr -- '+/' '-_'  
<!--NeedCopy-->
```

O comando retorna uma soma de verificação válida.

Para gerar o código QR, insira a soma de verificação no campo `PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM`. Por exemplo:

```
1 {  
2  
3   "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.  
4     zenprise/com.zenprise.configuration.AdminFunction",  
5   "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "  
6     qn7oZUtheu3JBainzZRrjCQv6L006Ll10jcxT3-yKM",  
7   "android.app.extra.  
8     PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://  
9     play.google.com/managed/downloadManagingApp?identifier=xenmobile",  
10  "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {  
11    "serverURL": "https://supportability.xm.cloud.com"  
12  }  
13 }  
14 <!--NeedCopy-->
```

Bibliotecas usadas

A Provisioning Tool usa as seguintes bibliotecas no seu código-fonte:

- biblioteca v7 [appcompat](#), Design Support Library e biblioteca v7 Palette do Google sob a licença Apache 2.0
Para obter informações, consulte o [Guia de Recursos da Biblioteca de Suporte](#).
- [Butter Knife](#) de Jake Wharton sob a licença Apache 2.0

Registrar dispositivos usando um código QR

Para registrar um dispositivo totalmente gerenciado usando um código QR, você pode gerar um código QR criando um JSON e convertendo o JSON em um código QR. A câmera do dispositivo escaneia o código QR para registrar o dispositivo.

Requisitos do sistema

- Suportado em todos os dispositivos Android com Android 8.0 e superior.

Criar um código QR de um JSON

Crie um JSON com os seguintes campos.

Estes campos são obrigatórios:

Chave: `android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME`

Valor: `com.zenprise/com.zenprise.configuration.AdminFunction`

Chave: `android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM`

Valor: `qn7oZUtheu3JBAinzZRrjCQv6LOO6LL1OjcxT3-yKM`

Chave: `android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION`

Valor: <https://play.google.com/managed/downloadManagingApp?identifier=xenmobile>

Estes campos são opcionais:

- **android.app.extra.PROVISIONING_LOCALE:** insira os códigos de idioma e país.
Os códigos de idioma são códigos de idioma ISO com duas letras minúsculas (por exemplo, en), conforme definido pela [ISO 639-1](#). Os códigos de país são códigos de país ISO com duas letras maiúsculas (por exemplo, US), conforme definido pela [ISO 3166-1](#). Por exemplo, insira `en_US` para o inglês falado nos Estados Unidos.
- **android.app.extra.PROVISIONING_TIME_ZONE:** o fuso horário em que o dispositivo é executado.
Insira um [nome Olson da área/localização do formulário](#). Por exemplo, `America/Los_Angeles` para o horário do Pacífico. Se você não inserir um, o fuso horário será preenchido automaticamente.
- **android.app.extra.PROVISIONING_LOCAL_TIME:** tempo em milissegundos desde a época (Epoch).
A época do Unix (ou hora do Unix, hora do POSIX ou carimbo de data/hora do Unix) é o número de segundos decorridos desde 1º de janeiro de 1970 (meia-noite UTC/GMT). O tempo não inclui segundos bissextos (in ISO 8601: 1970-01-01T00:00:00Z).
- **android.app.extra.PROVISIONING_SKIP_ENCRYPTION:** definido como **true** para ignorar a criptografia durante a criação do perfil. Defina como **false** para forçar a criptografia durante a criação do perfil.

Um JSON típico tem esta aparência:

Requisitos do sistema

- Suporte a registro sem toque começa com o Android 8.0.

Dispositivos e informações da conta fornecidas pelo seu revendedor

- Os dispositivos elegíveis para registro sem toque são comprados de um revendedor corporativo ou parceiro Google. Para obter uma lista de parceiros do Android Enterprise zero-touch, consulte o [site do Android](#).
- Uma conta do portal de registro sem toque do Android Enterprise, criada pelo seu revendedor.
- Informações de login da conta do portal de registro sem toque do Android Enterprise, fornecidas pelo seu revendedor.

Criar uma configuração sem toque

Quando você criar uma configuração toque zero, inclua um JSON personalizado para especificar detalhes da configuração.

Use este JSON para configurar o dispositivo para se registrar no XenMobile Server especificado. Substitua a URL do seu servidor por 'URL' neste exemplo.

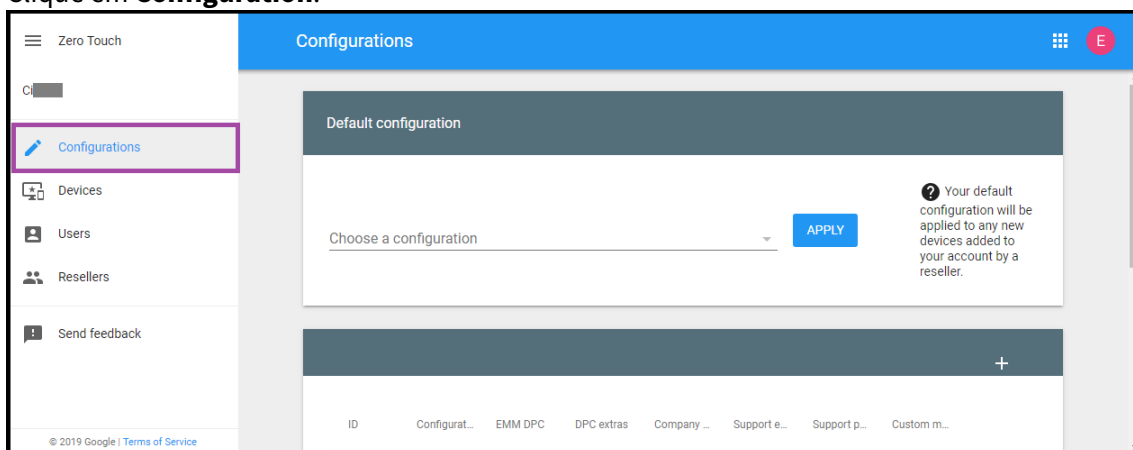
```
1      {
2
3          "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4      {
5
6          "serverURL": "URL",
7      }
8
9      }
10
11 <!--NeedCopy-->
```

Você pode usar um JSON opcional com mais parâmetros para personalizar ainda mais a sua configuração. Este exemplo especifica o XenMobile Server e o nome de usuário e senha que os dispositivos que usam essa configuração usam para fazer login no servidor.

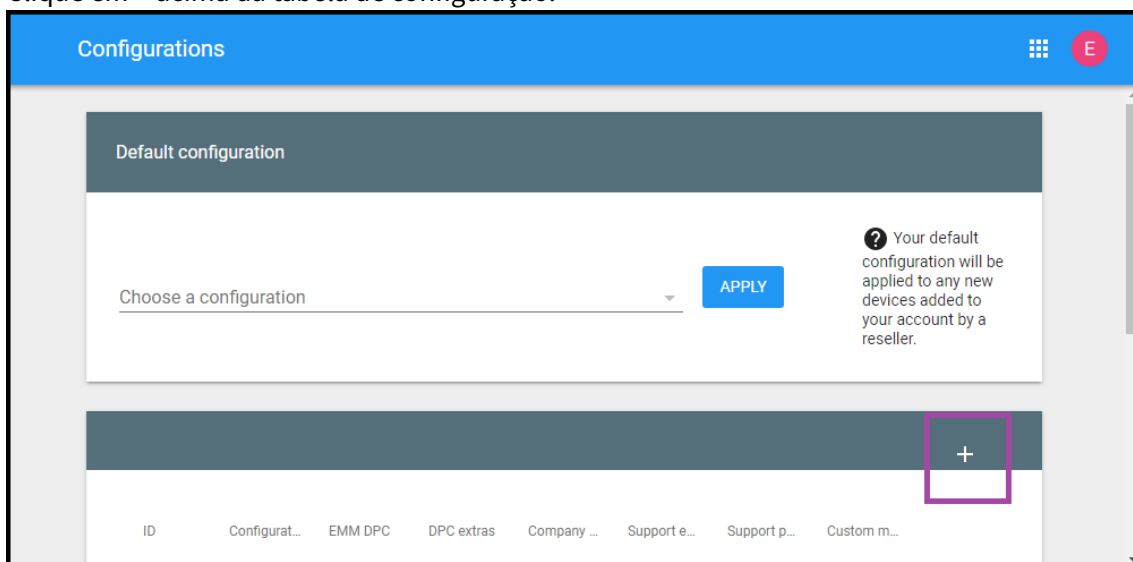
```
1      {
2
3          "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4      {
5
6          "serverURL": "URL",
7          "xm_username": "username",
```

```
8         "xm_password": "password"
9     }
10
11     }
12
13 <!--NeedCopy-->
```

1. Acesse o portal do Android zero-touch em <https://partner.android.com/zerotouch>. Inicie uma sessão com as informações da conta fornecidas pelo seu revendedor de dispositivos sem toque.
2. Clique em **Configuration**.



3. Clique em **+** acima da tabela de configuração.



4. Insira suas informações de configuração na janela de configuração que aparece.

The screenshot shows a mobile-style dialog box titled "Add a new configuration". It features a list of input fields for configuration details. The fields are: "Configuration name", "EMM DPC" (a dropdown menu with "Select" as the current selection), "DPC extras", "Company name", "Support email address", and "Support phone number". At the bottom right, there are two buttons: "CANCEL" and "ADD". A vertical scrollbar is visible on the right side of the dialog, and the number "132" is partially visible at the bottom right corner of the dialog area.

- **Configuration name:** digite o nome escolhido para esta configuração.
- **EMM DPC:** Escolha **Citrix Secure Hub**.
- **DPC extras:** Cole seu texto JSON personalizado neste campo.
- **Company name:** digite o nome que deseja que apareça nos dispositivos Android Enterprise sem toque durante o provisionamento do dispositivo.
- **Support email address:** digite um endereço de e-mail para que seus usuários possam

entrar em contato para obter ajuda. Esse endereço aparece nos seus dispositivos Android Enterprise sem toque antes do provisionamento do dispositivo.

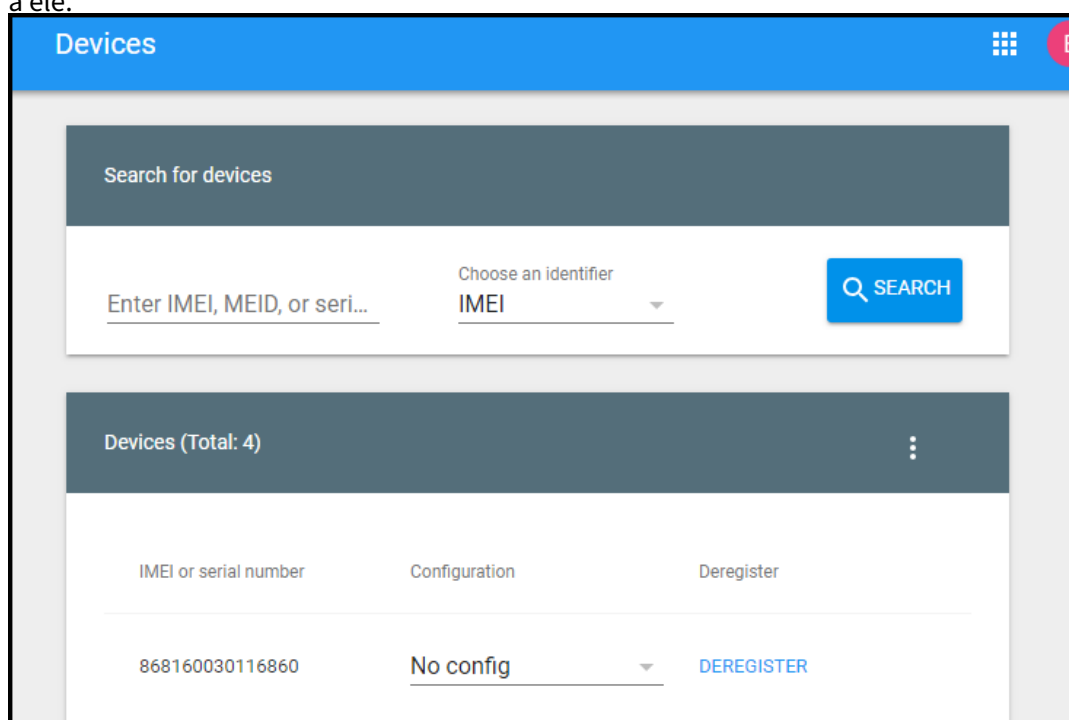
- **Support phone number:** digite um número de telefone para que seus usuários possam entrar em contato para obter ajuda. Esse número de telefone aparece nos seus dispositivos Android Enterprise sem toque antes do provisionamento do dispositivo.
- **Custom Message:** opcionalmente, adicione uma ou duas frases para ajudar os usuários a entrar em contato com você ou fornecer mais detalhes sobre o que está acontecendo com o dispositivo deles. Essa mensagem personalizada aparece nos seus dispositivos Android Enterprise sem toque antes do provisionamento do dispositivo.

5. Clique em **Add**.

6. Para criar mais configurações, repita as etapas 2 a 4.

7. Para aplicar uma configuração a um dispositivo:

- a) No portal de registro sem toque do Android, clique em **Devices**.
- b) Localize o dispositivo na lista de dispositivos e escolha a configuração que deseja atribuir a ele.



c) Clique em **Update**.

Você pode aplicar uma configuração a vários dispositivos usando um arquivo CSV.

Para obter informações sobre como aplicar uma configuração a vários dispositivos, consulte o tópico de ajuda do Android Enterprise [Zero-touch enrollment for IT admins](#). Esse tópico de ajuda do Android Enterprise contém mais informações sobre como gerenciar configurações e aplicá-las a dispositivos.

Provisionamento de dispositivos Android Enterprise dedicados

Os dispositivos Android Enterprise dedicados são dispositivos totalmente gerenciados e dedicados a atender a um único caso de uso. Dispositivos dedicados também são conhecidos como dispositivos corporativos para uso único (COSU). Você restringe esses dispositivos a um aplicativo ou a um pequeno conjunto de aplicativos necessários para executar as tarefas necessárias para o caso de uso. Você também impede que os usuários habilitem outros aplicativos ou executem outras ações no dispositivo.

Registrar dispositivos dedicados usando qualquer um dos métodos de registro usados para outros dispositivos totalmente gerenciados, conforme descrito em Provisionamento de dispositivos Android Enterprise totalmente gerenciados. O provisionamento de dispositivos dedicados requer mais configuração antes do registro.

Para provisionar dispositivos dedicados:

- Adicione um perfil de registro para administradores do XenMobile os quais você permite que registrem dispositivos dedicados na sua implantação do XenMobile. Consulte Criar perfis de registro.
- Acrescente à lista de permissão os aplicativos que você deseja que o dispositivo dedicado acesse.
- Opcionalmente, coloque o aplicativo na lista de permissão para permitir o modo de bloqueio de tarefa. Quando um aplicativo está no modo de bloqueio de tarefa, ele é fixado na tela do dispositivo quando o usuário o abre. O botão Início não aparece e o botão Voltar fica desativado. O usuário sai do aplicativo usando uma ação programada no aplicativo, como logoff.
- Registre cada dispositivo no perfil de registro que você adicionou.

Requisitos do sistema

- Suporte para registrar dispositivos dedicados começa com o Android 6.0.

Acrescentar aplicativos à lista de permissão e definir o modo de bloqueio de tarefa

A política de dispositivo de quiosque permite que você acrescente aplicativos à lista de permissão e defina o modo de bloqueio de tarefa. Por padrão, os serviços Secure Hub e Google Play são permitidos.

Para adicionar a política de quiosque:

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.
2. Clique em **Add**. É exibida a caixa de diálogo **Adicionar uma nova política**.
3. Expanda **Mais** e, em Segurança, clique em **Quiosque**. A página **Política de quiosque** é exibida.
4. Em Plataformas, selecione **Android Enterprise**. Limpe as outras plataformas.

5. No painel de Informações da Política, digite o **Nome da Política** e uma **Descrição** opcional.
6. Clique em **Avançar** e, em seguida, clique em **Adicionar**.
7. Para acrescentar um aplicativo à lista de permissão e permitir ou negar o modo de bloqueio de tarefa do aplicativo:

Selecione o aplicativo que você deseja permitir na lista.

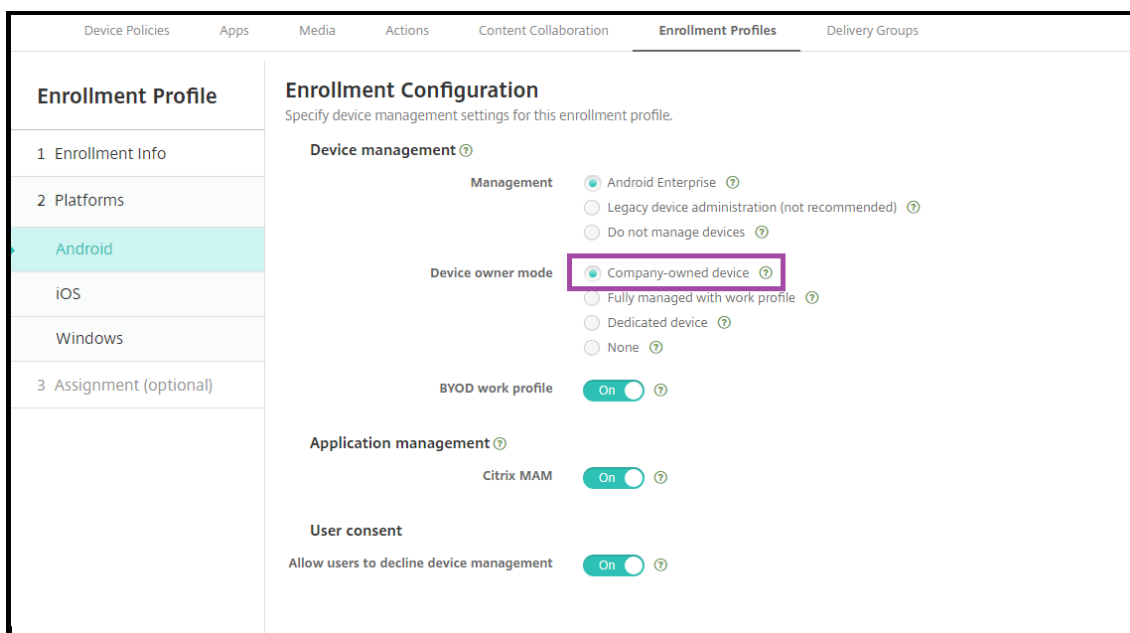
Escolha **Permitir** para que o aplicativo seja fixado na tela do dispositivo quando o usuário iniciar o aplicativo. Escolha **Negar** para que o aplicativo não seja fixado. O padrão é **Permitir**.

Apps to whitelist *	Lock task status
Cosu App	<input checked="" type="radio"/> Allow <input type="radio"/> Deny

8. Clique em **Save**.
9. Para acrescentar outro aplicativo à lista de permissão e permitir ou negar o modo de bloqueio de tarefa do aplicativo, clique em **Adicionar**.
10. Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte a [Política de dispositivo de VPN](#).

Para registrar o dispositivo

1. Clique em **Avançar** ou selecione **Android** em **Plataformas**. A página de configuração de registro é exibida.
2. Defina **Gerenciamento** para **Android Enterprise**.
3. Defina **Modo proprietário do dispositivo** como **Dispositivo de propriedade da empresa**.



4. Selecione **Atribuição (opções)**. A tela Atribuição de grupo de entrega é exibida.
5. Escolha um grupo de entrega ou grupos de entrega contendo os administradores que registram dispositivos dedicados. Em seguida, clique em **Save**.

Se você habilitou o **Perfil de trabalho BYOD** no perfil de registro, os dispositivos que não são novos ou redefinidos de fábrica serão registrados como dispositivos de perfil de trabalho. Consulte [Provisionar dispositivos de perfil de trabalho Android Enterprise](#).

Provisionar dispositivos Android Enterprise totalmente gerenciados com um perfil de trabalho (dispositivos COPE)

Dispositivos totalmente gerenciados com um perfil de trabalho, anteriormente chamados de dispositivos COPE, são dispositivos de propriedade da empresa que são usados para fins pessoais e profissionais. Sua organização gerencia os dispositivos por completo. Você pode aplicar um conjunto de políticas ao dispositivo e um conjunto separado de políticas ao perfil de trabalho.

No console XenMobile, os dispositivos totalmente gerenciados com um perfil de trabalho aparecem com estes termos:

- A propriedade do dispositivo é “Corporativo”.
- O tipo de instalação do dispositivo Android Enterprise é “Propriedade da empresa, habilitado pessoalmente”.

Requisitos do sistema

- O suporte para registrar dispositivos totalmente gerenciados com perfis de trabalho começa com o Android 8.0.

Adicionar um perfil de registro para dispositivos totalmente gerenciados com perfis de trabalho

Crie um perfil de registro para registrar dispositivos totalmente gerenciados com perfis de trabalho. Os administradores nos grupos de entrega atribuídos a esse perfil de registro podem registrar dispositivos totalmente gerenciados com perfis de trabalho. Para garantir que esses administradores possam registrar todos os dispositivos necessários, crie um perfil de registro para eles com dispositivos ilimitados permitidos por usuário. Atribua esse perfil a um grupo de entrega contendo os administradores que registram os dispositivos totalmente gerenciados com perfis de trabalho.

1. No console XenMobile, vá para **Configurar > Perfis de registro**.
2. Para adicionar um perfil de registro, clique em **Adicionar**. Na página de Informações de registro, digite um nome para o perfil de registro. Certifique-se de que o número de dispositivos que os membros com este perfil podem registrar esteja definido como ilimitado.
3. Clique em **Avançar** ou selecione **Android Enterprise** em **Plataformas**. A página de configuração de registro é exibida.
4. Defina o **Tipo de inscrição/registo** como um dos seguintes:
 - **Totalmente gerenciado/Perfil de trabalho:** novos dispositivos ou dispositivos com reconfiguração de fábrica se registram totalmente gerenciados. Os dispositivos BYOD se registram com apenas um perfil de trabalho gerenciado por você.
 - **COPE/Perfil de trabalho:** novos dispositivos ou dispositivos com reconfiguração de fábrica se registram totalmente gerenciados com um perfil de trabalho. Os dispositivos BYOD se registram com apenas um perfil de trabalho gerenciado por você.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	Device management ⓘ <ul style="list-style-type: none"> Management <ul style="list-style-type: none"> <input checked="" type="radio"/> Android Enterprise ⓘ <input type="radio"/> Legacy device administration (not recommended) ⓘ <input type="radio"/> Do not manage devices ⓘ Device owner mode <ul style="list-style-type: none"> <input checked="" type="radio"/> Company-owned device ⓘ <input type="radio"/> Fully managed with work profile ⓘ <input type="radio"/> Dedicated device ⓘ <input type="radio"/> None ⓘ BYOD work profile <input checked="" type="checkbox"/> ⓘ
Android	Application management ⓘ <ul style="list-style-type: none"> Citrix MAM <input checked="" type="checkbox"/> ⓘ
iOS	User consent <ul style="list-style-type: none"> Allow users to decline device management <input checked="" type="checkbox"/> ⓘ
3 Assignment (optional)	

5. Selecione **Atribuição (opcional)** ou clique em **Avançar**. A tela Atribuição de grupo de entrega é exibida.
6. Escolha um grupo de entrega ou grupos de entrega contendo os administradores que registram dispositivos dedicados. Em seguida, clique em **Save**.

A página de Perfil de registro é exibida com o perfil que você adicionou.

Enrollment Profiles				
Enrollment profile name	Created on	Updated on	Device limit	
COPE devices	11/1/19 1:01:51 pm	11/1/19 1:01:51 pm	unlimited	
Global	10/28/19 5:30:39 am	10/28/19 5:30:39 am	unlimited	

Showing 1 - 2 of 2 items Items per page: 10

Se um usuário pertencer a vários grupos de entrega que têm perfis de registro diferentes, o nome do grupo de entrega determinará o perfil de registro usado. O XenMobile seleciona o grupo de entrega que aparece por último em uma lista alfabética de grupos de entrega,

Para registrar o dispositivo

Dispositivos novos e com reconfiguração de fábrica se registram como dispositivos totalmente gerenciados com um perfil de trabalho usando o token do identificador DPC, o compartilhamento de comu-

nicação a curta distância (NFC) ou métodos de código QR. Consulte Registrar dispositivos usando o token identificador Citrix DPC, Registrar dispositivos com NFC bump ou Registrar dispositivos usando um código QR.

Dispositivos que não são novos nem com reconfiguração de fábrica se registram como dispositivos de perfil de trabalho conforme descrito em [Provisionar dispositivos de perfil de trabalho Android Enterprise](#).

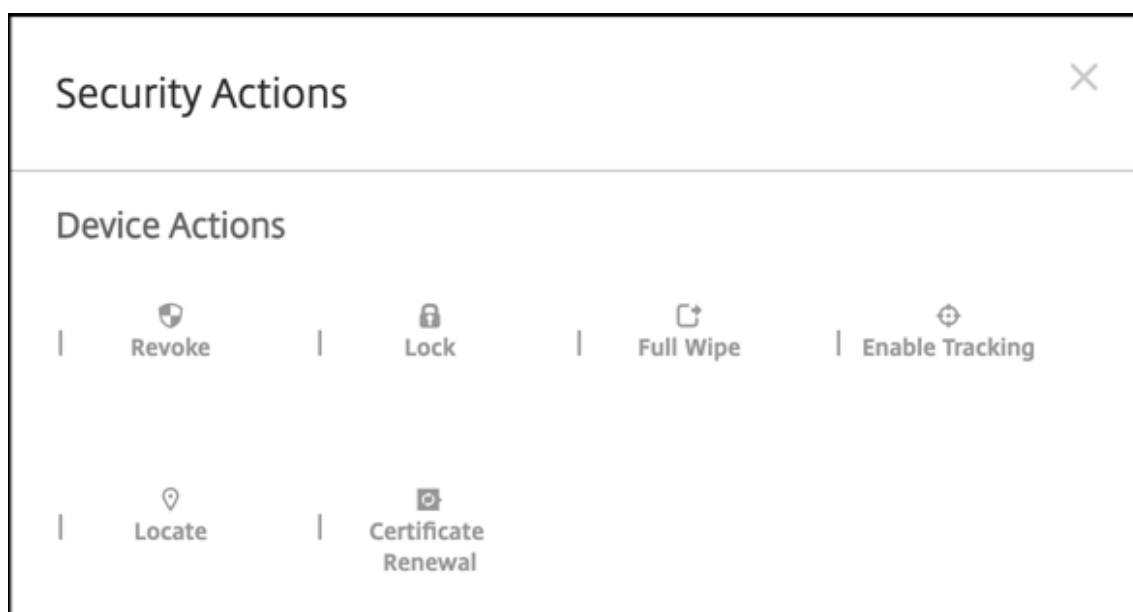
Exibir dispositivos Android Enterprise no console XenMobile

1. No console XenMobile, vá para **Gerenciar > Dispositivos**.
2. Adicione a coluna **Dispositivo Android Enterprise ativado?** clicando no menu à direita da tabela na página.

The screenshot shows the 'Enrolled Devices' page in the XenMobile console. At the top, there are tabs for 'Enrolled Devices' and 'Device Whitelist', and a search bar. Below the tabs, there are icons for 'Add', 'Import', 'Export', and 'Refresh'. The main area contains a table with the following columns: Status, Mode, User name, Device platform, Operating system version, Device model, Last access, Inactivity days, and Android Enterprise Enabled Device?. The table lists two devices: one with user 'mbbowlin' on an iOS device and another with user 'testing2' on an Android Pixel XL device. A dropdown menu is open on the right side of the table, showing a list of columns to be added, with 'Android Enterprise Enabled Device?' selected and highlighted in red.

Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days	Android Enterprise Enabled Device?
<input type="checkbox"/>	MDM	mbbowlin "mbbowlin"	iOS			5/7/19 1:01:50 pm	33 days	<input checked="" type="checkbox"/>
<input type="checkbox"/>	MDM MAM	testing2 "testing2"	Android	9	Pixel XL	6/10/19 8:06:51 am	0 day	<input checked="" type="checkbox"/>

3. Para exibir as ações de segurança disponíveis, selecione um dispositivo totalmente gerenciado e clique em **Segurança**. Quando o dispositivo é totalmente gerenciado, a ação **Apagamento completo** fica disponível, mas **Apagamento seletivo** não. Essa diferença se dá porque o dispositivo só permite aplicativos da loja Google Play gerenciada. Não há nenhuma opção para o usuário instalar aplicativos da loja pública. Sua organização gerenciou todo o conteúdo no dispositivo.



Configurar políticas de aplicativo e de dispositivo Android Enterprise

Para obter uma visão geral das políticas controladas nos níveis de dispositivo e aplicativo, consulte as [políticas de dispositivo suportadas](#) e [políticas MDX para Android Enterprise](#).

O que saber sobre políticas:

- **Proteção contra perda de dados:** a tecnologia de contêiner MAM XenMobile protege aplicativos com criptografia e outras tecnologias móveis de prevenção contra perda de dados (DLP). Use o Citrix MAM SDK, MDX Service ou MDX Toolkit para aplicativos habilitados para MDX.
- **Restrições do dispositivo:** dezenas de restrições de dispositivo permitem controlar recursos como:
 - Uso da câmera do dispositivo
 - Uso de copiar e colar entre perfis profissionais e pessoais
- **VPN por aplicativo:** use a política de dispositivo de Configurações gerenciadas para configurar perfis VPN para Android Enterprise.
- **Política de e-mail:** recomendamos usar a política de dispositivo de Configurações gerenciadas para configurar aplicativos.

Esta tabela lista todas as políticas de dispositivo disponíveis para dispositivos Android Enterprise.

Importante:

para dispositivos que se registram no Android Enterprise e usam aplicativos MDX: você pode con-

Controlar algumas configurações por meio do MDX e do Android Enterprise. Use as configurações de política menos restritivas para MDX e controle a política por meio do Android Enterprise.

Permissões do aplicativo Enterprise Android	Configurações gerenciadas do Android Enterprise	Inventário de aplicativos
Desinstalação de aplicativo	Atualizar automaticamente aplicativos gerenciados	Controlar atualização de SO
Credenciais	XML personalizado	Exchange
Arquivos	Gerenciamento de proteção do teclado	Quiosque
Localização	Código secreto	Restrições
Chave de licença MDM Samsung	Programação	Wi-Fi
Opções do XenMobile		

Políticas de dispositivo para dispositivos totalmente gerenciados com perfil de trabalho (dispositivos COPE)

Para dispositivos totalmente gerenciados com perfis de trabalho (dispositivos COPE), algumas políticas de dispositivo podem ser usadas para aplicar configurações separadas a todo o dispositivo e ao perfil de trabalho. Você pode usar outras políticas de dispositivo para aplicar configurações apenas para o dispositivo todo ou apenas para o perfil de trabalho de dispositivos totalmente gerenciados com perfis de trabalho.

Política	Aplica-se a
Permissões do aplicativo Enterprise Android	Perfil de trabalho
Configurações gerenciadas do Android Enterprise	Perfil de trabalho
Inventário de aplicativos	Perfil de trabalho
Desinstalação de aplicativo	Perfil de trabalho
Atualizar automaticamente aplicativos gerenciados	Perfil de trabalho
Controlar atualização de SO	N/A

Política	Aplica-se a
Credenciais	Perfil de trabalho
XML personalizado	N/A
Exchange	N/A
Arquivos	Perfil de trabalho
Gerenciamento de proteção do teclado	Dispositivo e perfil de trabalho
Quiosque	N/A
Localização	Dispositivo (somente modo de localização)
Código secreto	Dispositivo e perfil de trabalho
Restrições	Dispositivo e perfil de trabalho (crie políticas separadas para o dispositivo e o perfil de trabalho)
Chave de licença MDM Samsung	N/A
Programação	Perfil de trabalho
Wi-Fi	Dispositivo
Opções do XenMobile	Perfil de trabalho

Consulte também as [políticas MDX](#) e [políticas de dispositivo com suporte para Android Enterprise](#) e [Visão geral do MAM SDK](#).

Ações de segurança

O Android Enterprise suporta as seguintes ações de segurança. Para obter uma descrição de cada ação de segurança, consulte [Ações de segurança](#).

Ação de segurança	Perfil de trabalho	Totalmente gerenciado
Renovação de certificado	Sim	Sim
Apagamento completo	Não	Sim
Localizar	Sim	Sim
Bloquear	Sim	Sim
Bloquear e redefinir senha	Não	Sim
Notificar (Tocar)	Sim	Sim

Ação de segurança	Perfil de trabalho	Totalmente gerenciado
Revogar	Sim	Sim
Apagamento seletivo	Sim	Não

Observações sobre a Ação de segurança

- A ação de segurança Localizar falha a menos que a política de dispositivo de Localizar defina o modo de localização do dispositivo como **Alta precisão** ou **Economia de bateria**. Consulte [Política de dispositivo de localização](#).
- Em dispositivos de perfil de trabalho que executam versões do Android anteriores ao Android 8.0:
 - A ação de bloqueio e redefinição de senha não é suportada.
- Em dispositivos de perfil de trabalho com Android 8.0 ou superior:
 - O código secreto enviado bloqueia o perfil de trabalho. O dispositivo em si não é bloqueado.
 - Se nenhum código secreto estiver definido no perfil de trabalho:
 - * Se não for enviado um código secreto, ou se o código secreto enviado não atender aos requisitos de código secreto, o dispositivo será bloqueado.
 - Se um código secreto estiver definido no perfil de trabalho:
 - * Se não for enviado um código secreto, ou se o código secreto enviado não atender aos requisitos de código secreto: o perfil de trabalho será bloqueado, mas o dispositivo em si não será bloqueado.
- Em dispositivos totalmente gerenciados com perfis de trabalho (dispositivos COPE):
 - Você pode aplicar a ação de segurança Bloquear separadamente ao dispositivo ou ao perfil de trabalho

Cancelar o registro de um enterprise do Android Enterprise

Se você não quiser mais usar o seu enterprise do Android Enterprise, poderá cancelar o registro do enterprise.

Aviso:

Depois de cancelar o registro de um enterprise, os aplicativos Android Enterprise nos dispositivos já registrados por meio dele são redefinidos para os estados padrão. O Google não gerencia mais os dispositivos. Se você se registrar em um novo enterprise do Android Enterprise, deverá

aprovar aplicativos para a nova organização a partir do Google Play gerenciado. Depois, você pode atualizar os aplicativos a partir do console XenMobile.

Depois que o registro do enterprise do Android Enterprise for cancelado:

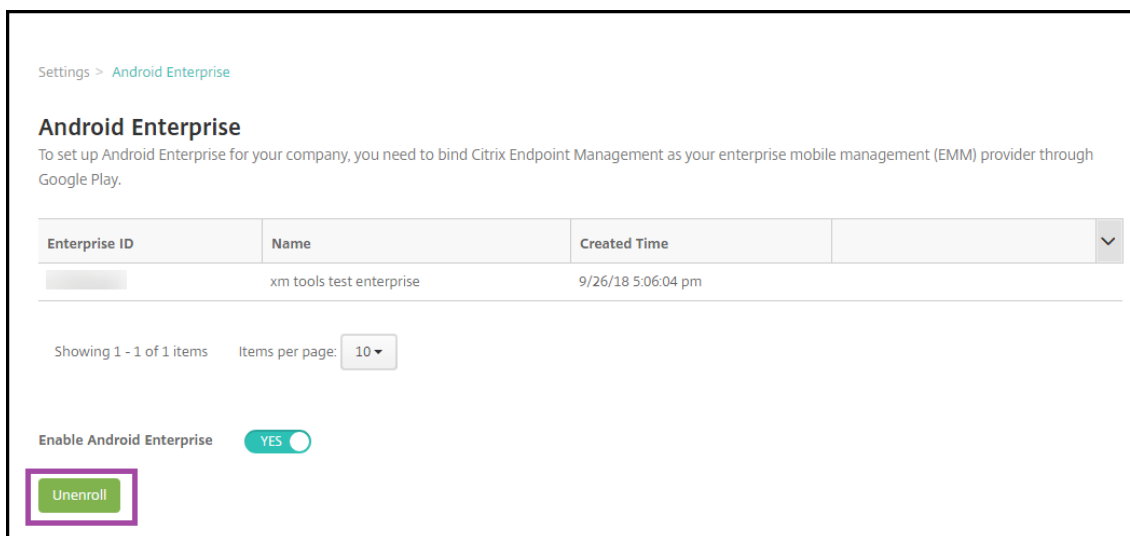
- Dispositivos e usuários registrados pelo Enterprise têm os aplicativos do Android Enterprise redefinidos para o estado padrão. As políticas de Configurações Gerenciadas do Android Enterprise aplicadas anteriormente não afetam mais as operações.
- O XenMobile gerencia dispositivos registrados por meio do enterprise. Do ponto de vista do Google, esses dispositivos não são gerenciados. Você não pode adicionar novos aplicativos Android Enterprise. Não é possível aplicar políticas de Configurações Gerenciadas do Android Enterprise. Você pode aplicar outras políticas, como Agendamento, Senha e Restrições a esses dispositivos.
- Se você tentar registrar dispositivos no Android Enterprise, eles serão registrados como dispositivos Android, não como dispositivos Android Enterprise.

Cancele o registro de um enterprise do Android Enterprise usando o console do XenMobile Server e o XenMobile Tools.

Quando você executa essa tarefa, o XenMobile abre uma janela pop-up para o XenMobile Tools. Antes de começar, verifique se o XenMobile tem permissão para abrir janelas pop-up no navegador que você está usando. Alguns navegadores, como o Google Chrome, exigem que você desabilite o bloqueio de pop-ups e acrescente o endereço do site do XenMobile à lista de permissão de bloqueio de pop-up.

Para cancelar o registro de um enterprise do Android Enterprise:

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página Settings é exibida.
2. Na página Settings, clique em **Android Enterprise**.
3. Clique em **Cancelar registro**.



Distribuir aplicativos Android Enterprise

April 8, 2021

O XenMobile gerencia aplicativos implantados em dispositivos. Você pode organizar e implantar os seguintes tipos de aplicativos do Android Enterprise.

- **Aplicativos da loja de aplicativos gerenciada:** esses aplicativos incluem aplicativos gratuitos ou pagos disponíveis no Google Play Store gerenciado. Por exemplo, o GoToMeeting.
- **MDX:** aplicativos preparados com o MAM SDK ou preparados com o MDX Toolkit. Esses aplicativos incluem políticas MDX. Você obtém aplicativos MDX de fontes internas e lojas públicas. Implante os aplicativos móveis de produtividade Citrix como aplicativos MDX.
- **Empresarial:** aplicativos privados que você desenvolve ou obtém de outra fonte. Você fornece esses aplicativos para seus usuários por meio do Google Play Store gerenciado. O Google Play Store gerenciado é a loja de aplicativos empresariais do Google.
- **Aplicativos privados habilitados para MDX:** aplicativos empresariais preparados com o MAM SDK ou preparados com o MDX Toolkit.

Você pode adicionar aplicativos empresariais e aplicativos privados habilitados para MDX de duas maneiras diferentes.

- Adicione os aplicativos ao console XenMobile como aplicativos empresariais, conforme descrito nas seções Aplicativos empresariais e Aplicativos privados habilitados para MDX neste artigo.
- Publique os aplicativos diretamente no Google Play Store gerenciado usando sua conta de desenvolvedor do Google. Em seguida, adicione os aplicativos ao console XenMobile como aplicativos gerenciados da loja de aplicativos. Consulte Aplicativos da loja de aplicativos gerenciada.

Se você publicar aplicativos usando sua conta de desenvolvedor do Google e depois mudar para usar o console XenMobile, a propriedade dos aplicativos será diferente. Gerencie seus aplicativos em ambos os locais, nesse caso. A Citrix recomenda adicionar seus aplicativos usando um método ou outro.

Se você precisar remover aplicativos autogerenciados do Google Play Store gerenciado, abra um tíquete no Google. Os desenvolvedores podem desativar, mas não excluir, aplicativos do Google Play Store gerenciado.

As seções a seguir fornecem informações mais detalhadas sobre a configuração do aplicativo Android Enterprise. Para obter informações sobre como distribuir aplicativos, consulte [Adicionar aplicativos](#). Esse artigo inclui:

- Os fluxos de trabalho gerais para adicionar aplicativos Web e SaaS ou links da Web
- O fluxo de trabalho do aplicativo necessário para aplicativos empresariais e de lojas públicas
- Como entregar aplicativos empresariais da Citrix Content Delivery Network (CDN) para Aplicativos Empresariais

Aplicativos da loja de aplicativos gerenciada

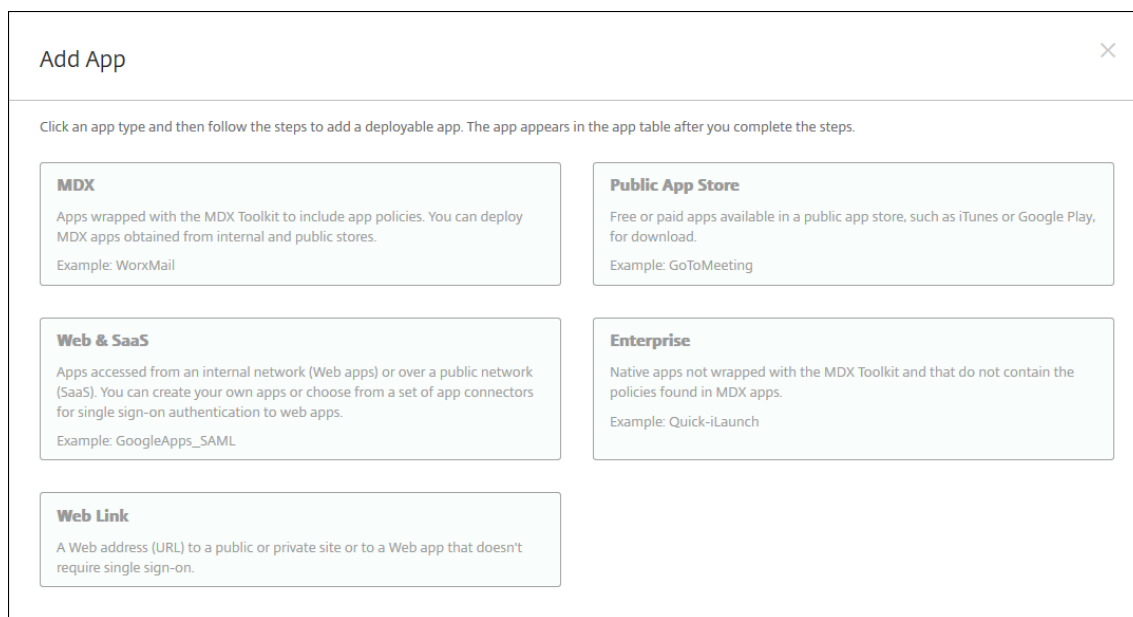
Você pode adicionar aplicativos gratuitos e pagos disponíveis no Google Play Store gerenciado ao XenMobile.

Nota:

Para tornar todos os aplicativos na loja Google Play acessíveis a partir do Google Play gerenciado, use a propriedade do servidor **Acessar todos os aplicativos na loja Google Play gerenciada**. Consulte [Propriedades do servidor](#). Definir esta propriedade como **true** permite que todos os usuários do Android Enterprise tenham acesso à loja pública do Google Play. Você pode usar a [Política de dispositivo de restrições](#) para controlar o acesso a esses aplicativos.

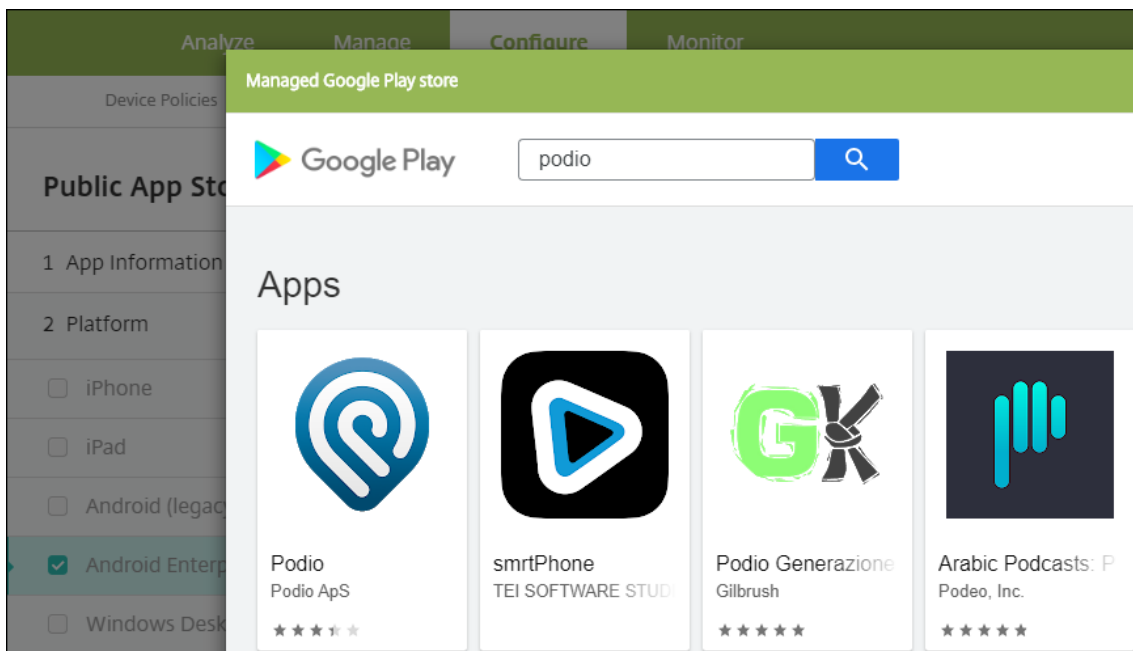
Etapa 1: adicionar e configurar aplicativos

1. No console XenMobile, navegue até **Configurar > Aplicativos**. Clique em **Adicionar**.
2. Clique em **Loja de aplicativos pública**.

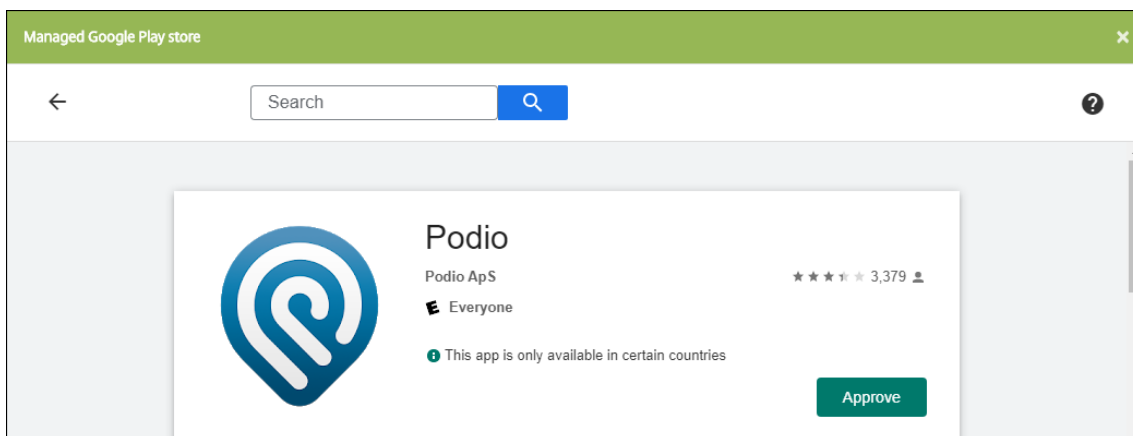


3. No painel **Informações do aplicativo**, digite as seguintes informações:
 - **Nome:** digite um nome descritivo para o aplicativo. O nome aparecerá em **Nome do aplicativo** na tabela **Aplicativos**.
 - **Descrição:** digite uma descrição opcional para o aplicativo.
 - **Categoria do aplicativo:** opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte [Sobre categorias de aplicativos](#).
4. Selecione **Android Enterprise** como a plataforma.

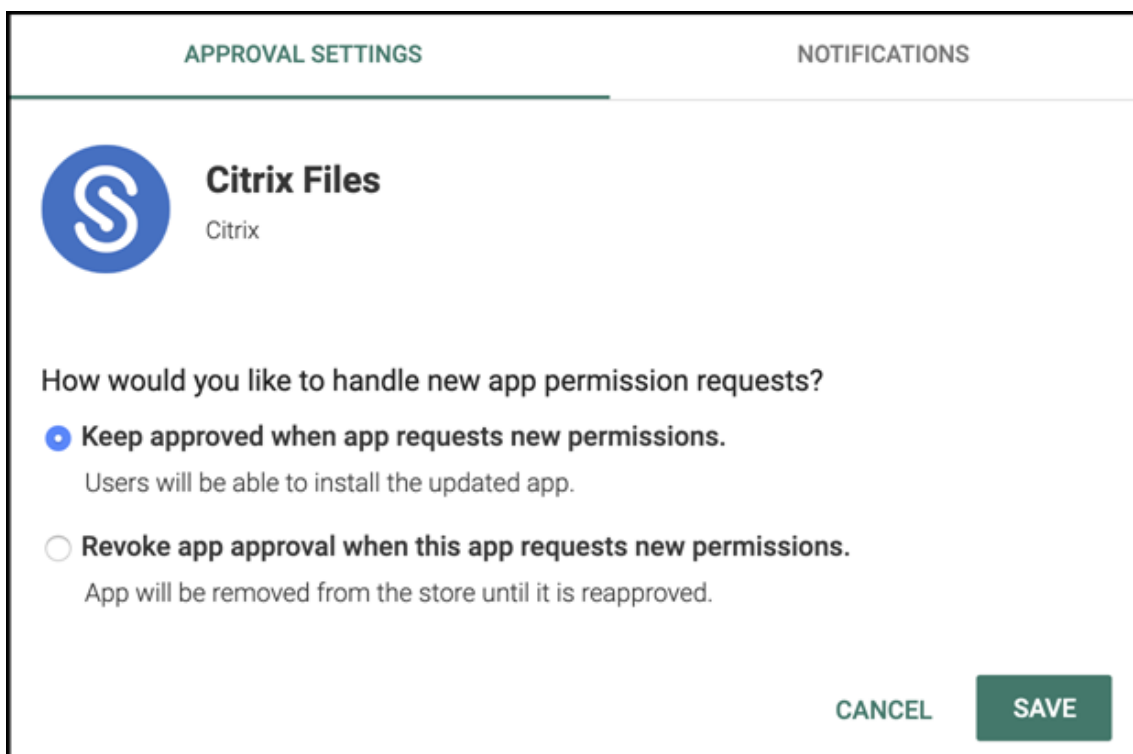
5. Digite o nome do aplicativo ou o ID do pacote na caixa de pesquisa e clique em **Pesquisar**. Você pode localizar o ID do pacote na loja do Google Play. O ID pode está no URL do aplicativo. Por exemplo, `com.Slack` é o ID do pacote em `https://play.google.com/store/apps/details?id=com.Slack&hl=en_US`.



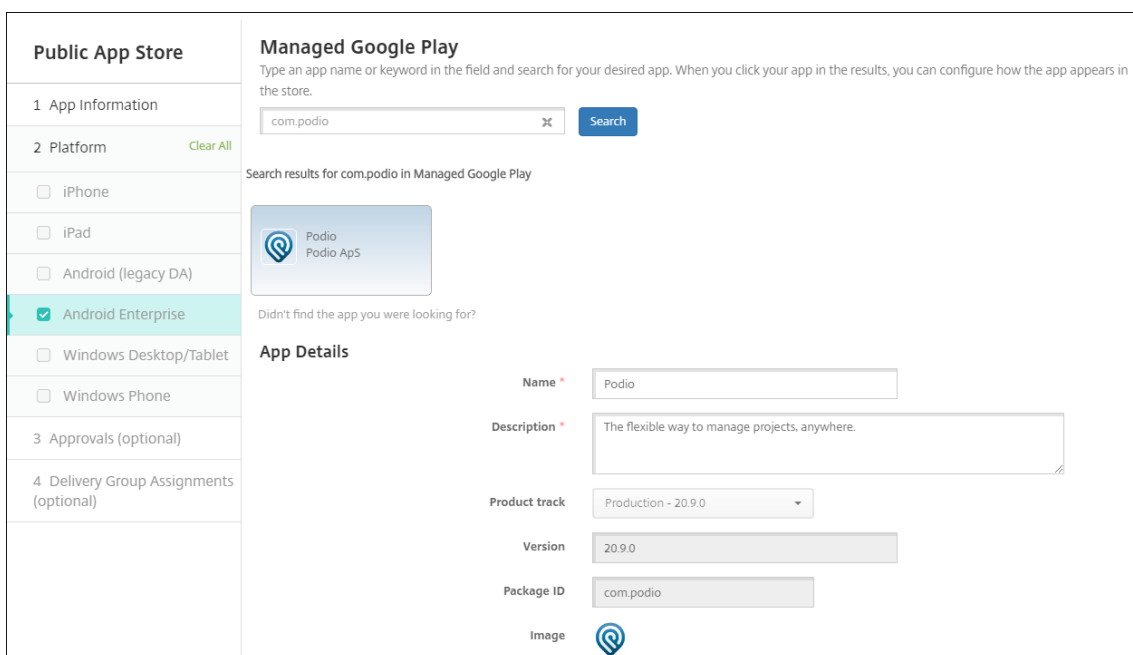
6. Os aplicativos que correspondem aos critérios de pesquisa são exibidos. Clique no aplicativo desejado e clique em **Aprovar**.



7. Clique em **Aprovar** novamente.
8. Selecione **Manter aprovado quando o aplicativo solicitar novas permissões**. Clique em **Salvar**.



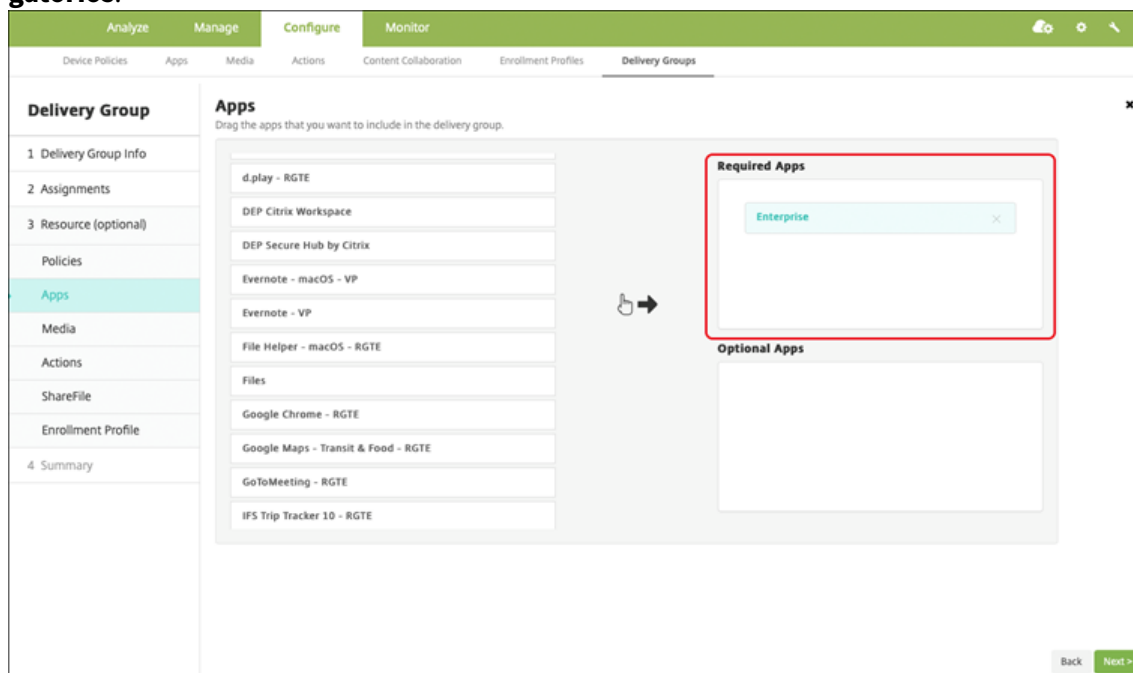
9. Clique no ícone do aplicativo e configure o **Nome** e a **Descrição** do aplicativo.



10. Atribua grupos de entrega ao aplicativo e clique em **Salvar**. Para obter informações, consulte [Implantar recursos](#).

Etapa 2: configurar implantação do aplicativo

1. Navegue até **Configurar > Grupos de Entrega** e selecione o grupo de entrega que você configurou. Clique em **Editar**.
2. Na seção **Aplicativos**, arraste os aplicativos desejados para a caixa de **Aplicativos obrigatórios**.



3. Na página **Resumo**, clique em **Salvar**.
4. Na página **Grupos de Entrega**, selecione o grupo de entrega e clique em **Implantar**.

Aplicativos MDX

Adicione arquivos MDX ao XenMobile e configure os detalhes do aplicativo e as configurações de política. Para configurar os aplicativos móveis de produtividade Citrix para Android Enterprise, adicione-os como aplicativos MDX. Para obter informações sobre as políticas de aplicativo que estão disponíveis para cada tipo de plataforma de dispositivo, consulte:

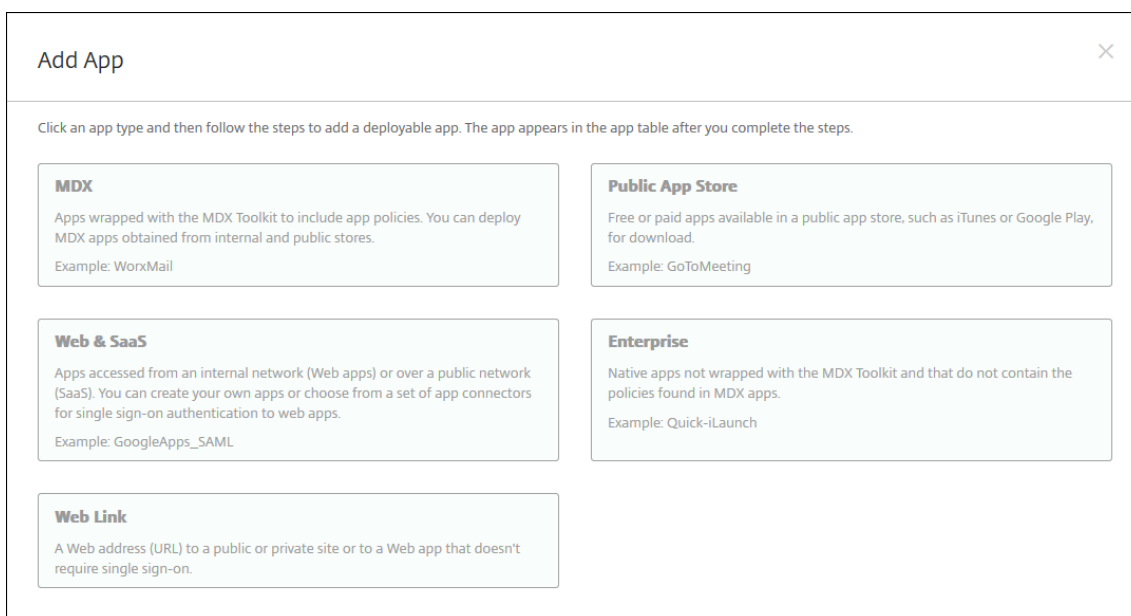
- [Visão geral do SDK MAM](#)
- [Resumo das políticas do MDX](#)

Etapa 1: adicionar e configurar aplicativos

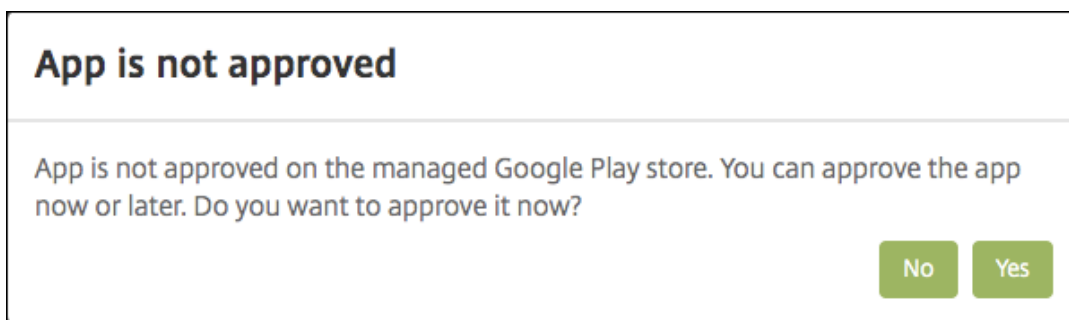
1. Para aplicativos móveis de produtividade Citrix, faça o download dos arquivos MDX da loja pública: vá para <https://www.citrix.com/downloads>. Navegue para **Citrix Endpoint Management (XenMobile) > Citrix Endpoint Management Productivity Apps**.

Para outros tipos de aplicativos MDX, obtenha o arquivo MDX.

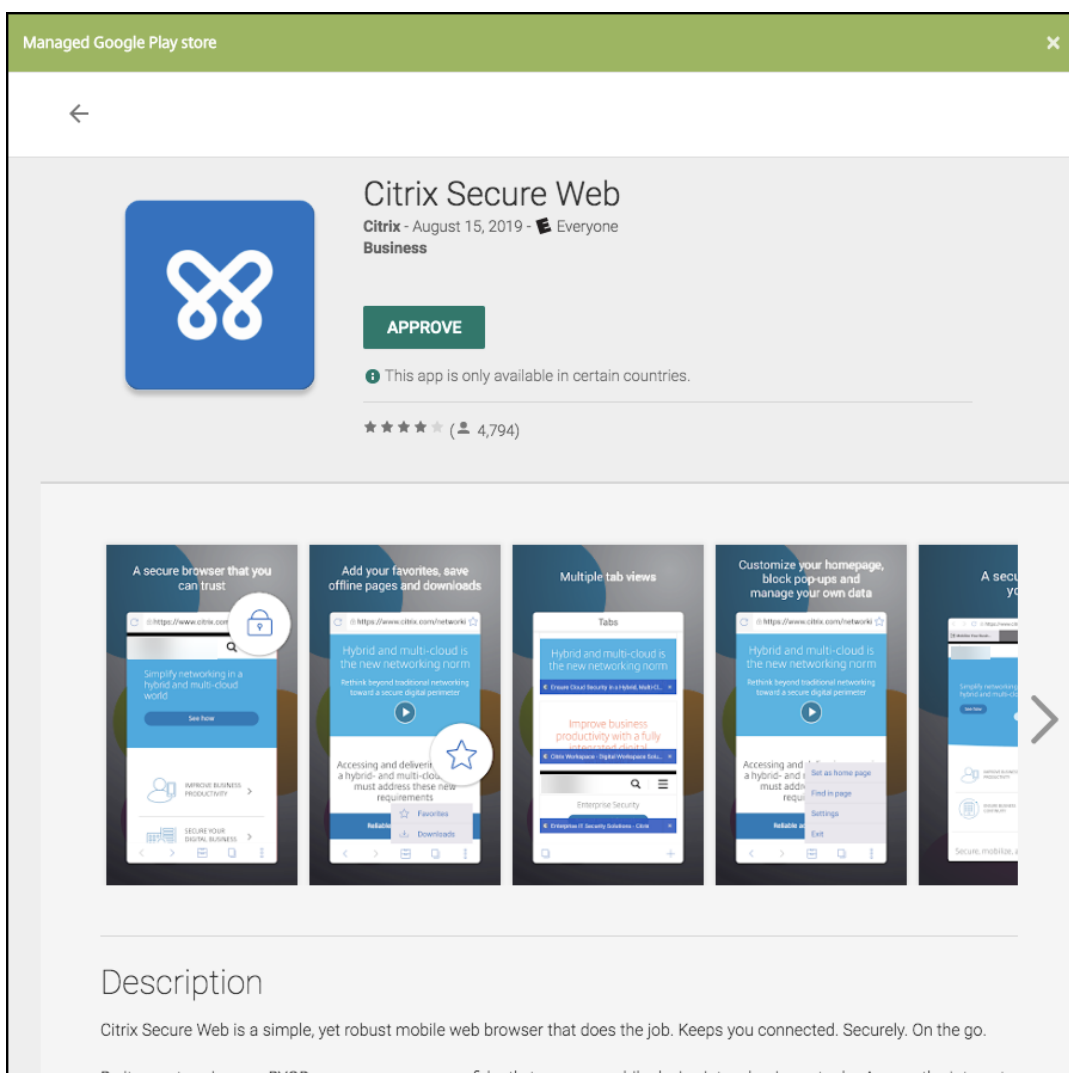
2. No console XenMobile, clique em **Configurar > Aplicativos**. Clique em **Adicionar**. A caixa de diálogo **Adicionar Aplicativo** é exibida.



3. Clique em **MDX**. A página **Informações do aplicativo MDX** é exibida. No painel **Informações do aplicativo**, digite as seguintes informações:
 - **Nome:** digite um nome descritivo para o aplicativo. O nome aparecerá em **Nome do aplicativo** na tabela **Aplicativos**.
 - **Descrição:** digite uma descrição opcional para o aplicativo.
 - **Categoria do aplicativo:** opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte [Sobre categorias de aplicativos](#).
4. Selecione **Android Enterprise** como a plataforma.
5. Clique em **Carregar** e navegue até o arquivo MDX. O Android Enterprise só oferece suporte a aplicativos preparados com o MAM SDK ou MDX Toolkit. Não prepare aplicativos usando o MDX Service.
 - A interface do usuário notificará você se o aplicativo anexado exigir aprovação do Google Play Store gerenciado. Para aprovar o aplicativo sem sair do console XenMobile, clique em **Sim**.



Depois que o Google Play Store gerenciado abrir, siga as instruções para aprovar e salvar o aplicativo.



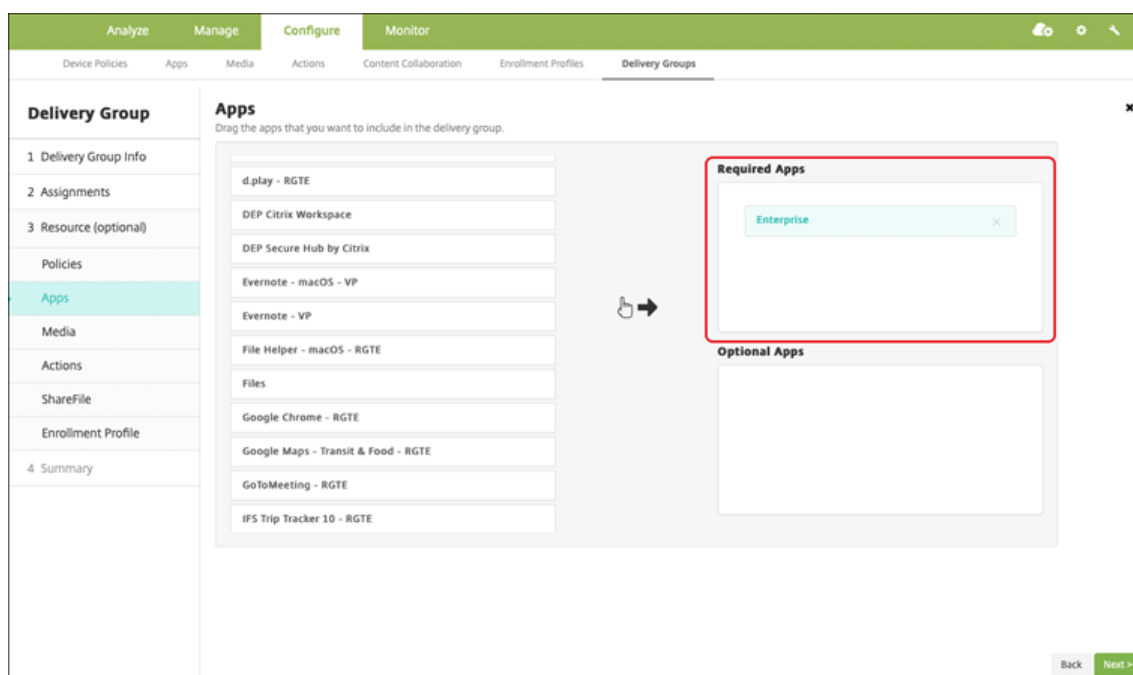
Quando você adicionar o aplicativo com êxito, a página **Detalhes do aplicativo** será exibida.

6. Defina estas configurações:

- **Nome do arquivo:** digite o nome de arquivo associado ao aplicativo.
 - **Descrição do aplicativo:** digite uma descrição para o aplicativo.
 - **Versão do aplicativo:** opcionalmente, digite o número da versão do aplicativo.
 - **ID de pacote:** digite o ID do pacote para o aplicativo, obtido no Google Play Store gerenciado.
 - **Versão do SO mínima:** opcionalmente, digite a versão mais antiga do sistema operacional que o dispositivo pode executar para usar o aplicativo.
 - **Versão do SO máxima:** opcionalmente, digite a versão mais recente do sistema operacional que o dispositivo deve executar para usar o aplicativo.
 - **Dispositivos excluídos:** opcionalmente, digite o fabricante ou os modelos de dispositivos que não podem executar o aplicativo.
7. Configure as **Políticas de MDX**. As políticas de MDX variam por plataforma e incluem opções para áreas de política como autenticação, segurança do dispositivo e restrições de aplicativo. No console, cada uma das políticas tem uma dica de ferramenta que descreve a política. Para obter informações sobre as políticas de aplicativo que estão disponíveis para cada tipo de plataforma de dispositivo, consulte:
- [Visão geral do SDK MAM](#)
 - [Resumo das políticas do MDX](#)
8. Configure as regras de implantação e a configuração de armazenamento.
9. Atribua grupos de entrega ao aplicativo e clique em **Salvar**. Para obter informações, consulte [Implantar recursos](#).

Etapa 2: configurar implantação do aplicativo

1. Navegue até **Configurar > Grupos de Entrega** e selecione o grupo de entrega que você configurou. Clique em **Editar**.
2. Na seção **Aplicativos**, arraste os aplicativos desejados para a caixa de **Aplicativos obrigatórios**.



3. Na página **Resumo**, clique em **Salvar**.
4. Na página **Grupos de Entrega**, selecione o grupo de entrega e clique em **Implantar**.

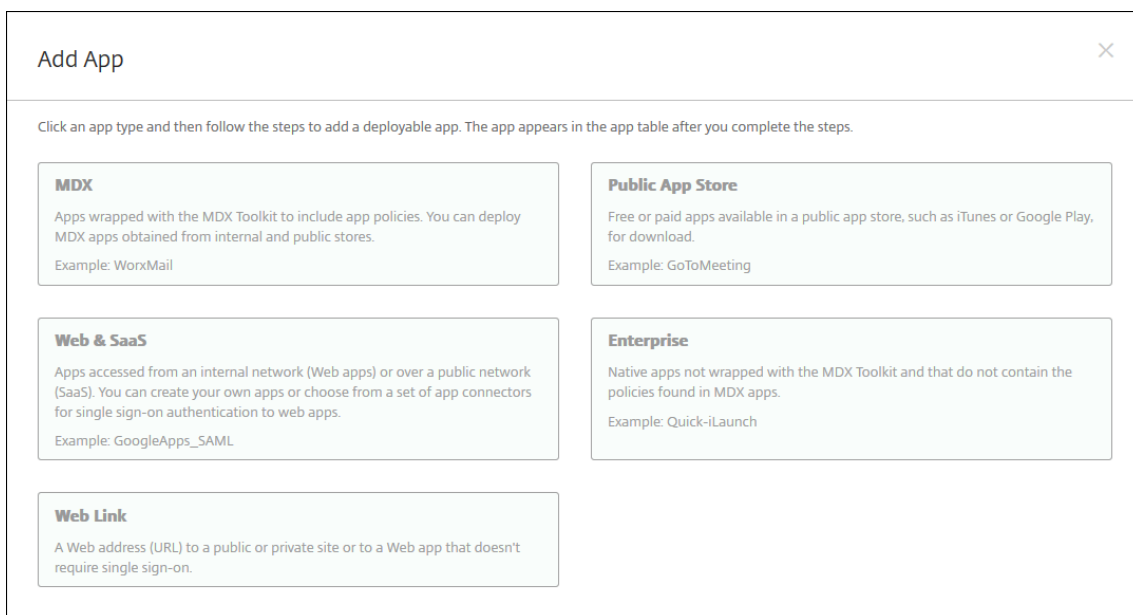
Aplicativos empresariais

Os aplicativos empresariais representam aplicativos privados que não são preparados com o MAM SDK ou MDX Toolkit. Você mesmo desenvolve esses aplicativos ou os obtém diretamente de outras fontes. Para adicionar um aplicativo empresarial, você precisa do arquivo APK associado ao aplicativo. Certifique-se de seguir as [Práticas recomendadas para apps particulares](#) do Google.

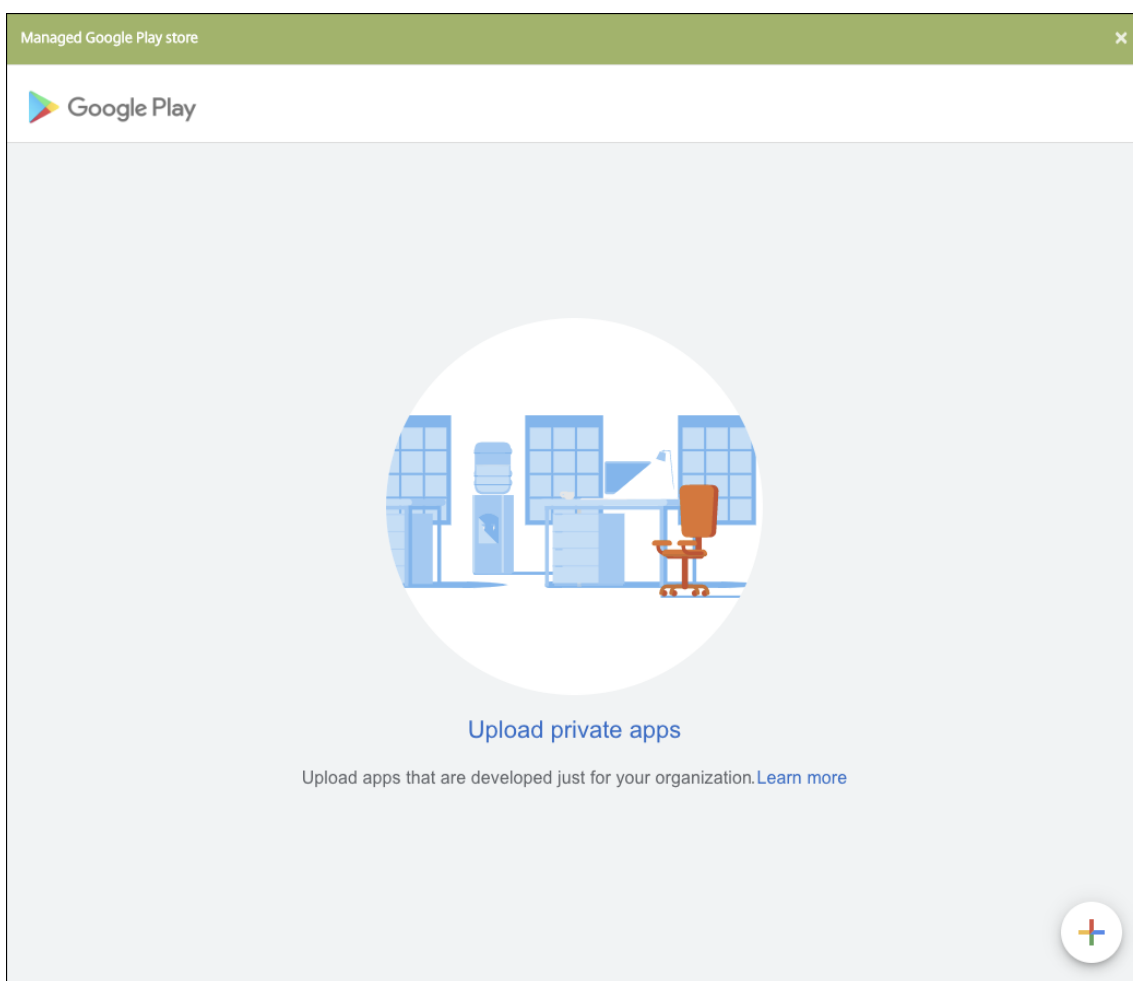
Etapa 1: adicionar e configurar aplicativos

Adicione o aplicativo de uma das duas maneiras:

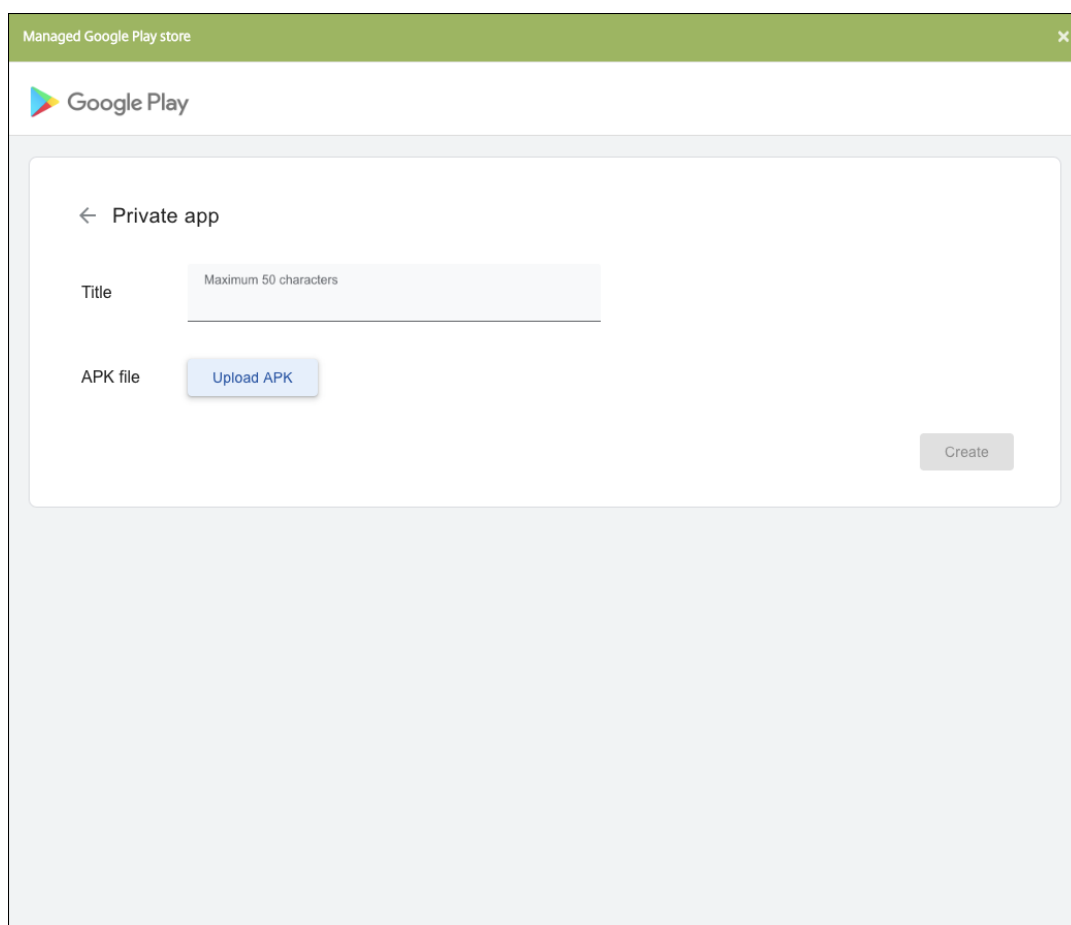
- Publique o aplicativo diretamente no Google Play Store gerenciado e adicione-o ao console XenMobile como um aplicativo gerenciado do Play Store. Veja a documentação do Google sobre como [Publicar apps particulares](#) e siga as etapas na seção Aplicativos da loja de aplicativos gerenciada.
- Adicione o aplicativo ao console XenMobile como um aplicativo empresarial. Execute as seguintes etapas:
 1. No console XenMobile, clique em **Configurar > Aplicativos**. Clique em **Adicionar**. A caixa de diálogo **Adicionar Aplicativo** é exibida.



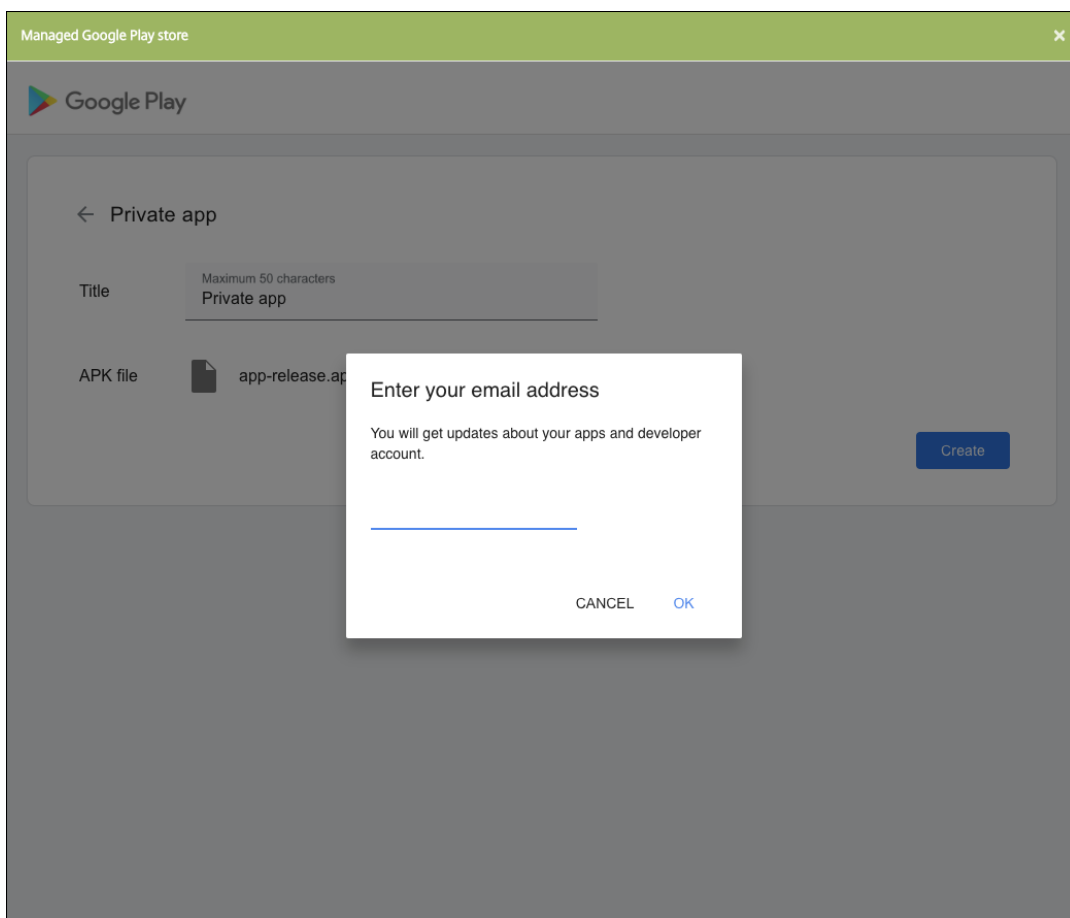
2. Clique em **Empresarial**. No painel **Informações do aplicativo**, digite as seguintes informações:
 - **Nome:** digite um nome descritivo para o aplicativo. Esse nome fica listado em Nome do aplicativo, na tabela Aplicativos.
 - **Descrição:** digite uma descrição opcional para o aplicativo.
 - **Categoria do aplicativo:** opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte [Sobre categorias de aplicativos](#).
3. Selecione **Android Enterprise** como a plataforma.
4. O botão **Carregar** abre o Google Play Store gerenciado. Você não precisa se registrar em uma conta de desenvolvedor para publicar um aplicativo privado. Clique no ícone de **adição** no canto inferior direito para continuar.



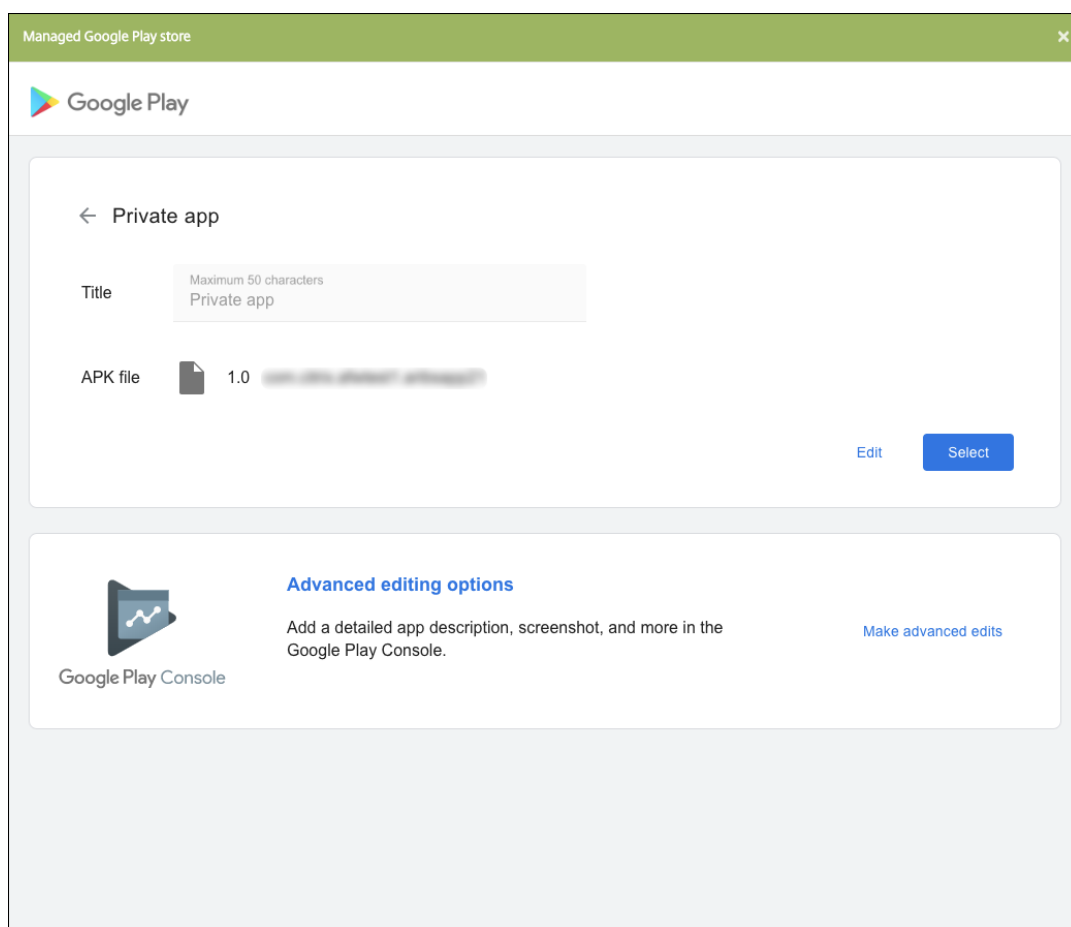
- a) Digite o nome do seu aplicativo e carregue o arquivo .apk. Quando terminar, clique em **Criar**. Pode levar até 10 minutos para que seu aplicativo privado seja publicado.



b) Insira um endereço de e-mail para receber atualizações sobre seus aplicativos.



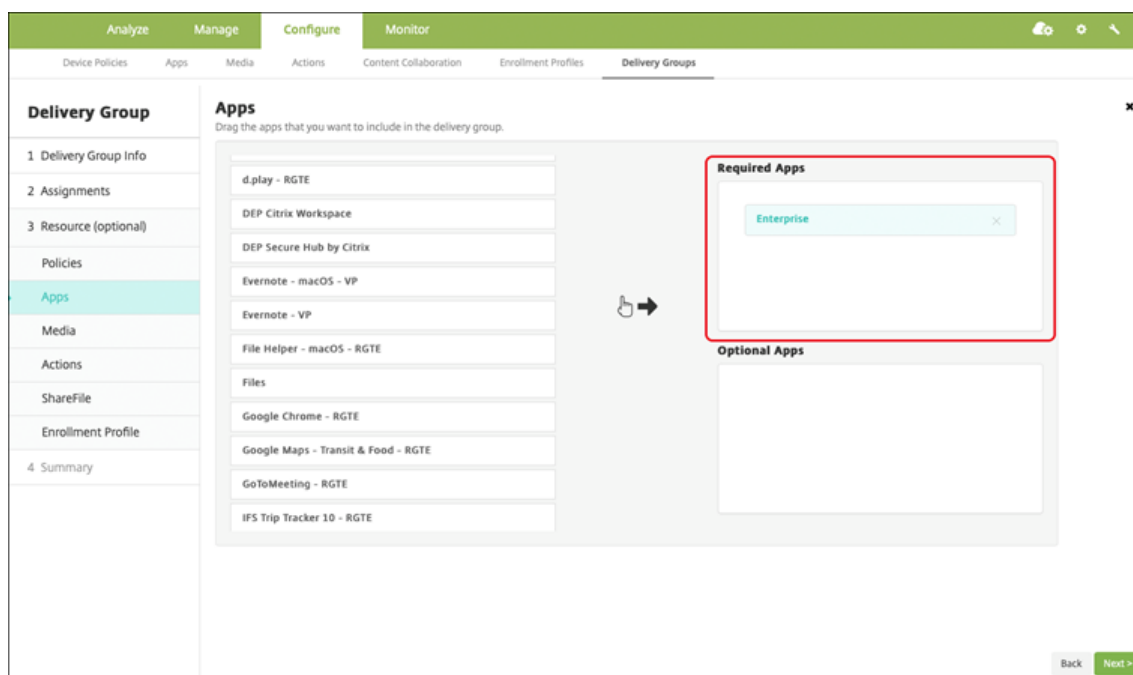
- c) Depois que o seu aplicativo for publicado, clique no ícone do aplicativo privado. Se você quiser adicionar uma descrição do aplicativo, alterar o ícone do aplicativo e outras ações, clique para **Fazer edições avançadas**. Caso contrário, clique em **Selecionar** para abrir a página de informações do aplicativo.



5. Clique em **Avançar**. A página de informações do aplicativo da plataforma é exibida.
6. Defina as configurações do tipo de plataforma, como:
 - **Nome do arquivo:** opcionalmente, digite um novo nome para o aplicativo.
 - **Descrição do aplicativo:** opcionalmente, digite uma nova descrição para o aplicativo.
 - **Versão do aplicativo:** você não pode alterar esse campo.
 - **ID de pacote:** Identificador exclusivo do seu aplicativo.
 - **Versão do SO mínima:** opcionalmente, digite a versão mais antiga do sistema operacional que o dispositivo pode executar para usar o aplicativo.
 - **Versão do SO máxima:** opcionalmente, digite a versão mais recente do sistema operacional que o dispositivo deve executar para usar o aplicativo.
 - **Dispositivos excluídos:** opcionalmente, digite o fabricante ou os modelos de dispositivos que não podem executar o aplicativo.
7. Configure as regras de implantação e a configuração de armazenamento.
8. Atribua grupos de entrega ao aplicativo e clique em **Salvar**. Para obter informações, consulte [Implantar recursos](#).

Etapa 2: configurar implantação do aplicativo

1. Navegue até **Configurar > Grupos de Entrega** e selecione o grupo de entrega que você configurou. Clique em **Editar**.
2. Na seção **Aplicativos**, arraste os aplicativos desejados para a caixa de **Aplicativos obrigatórios**.



3. Na página **Resumo**, clique em **Salvar**.
4. Na página **Grupos de Entrega**, selecione o grupo de entrega e clique em **Implantar**.

Aplicativos privados habilitados para MDX

Para adicionar aplicativos Android Enterprise como aplicativos empresariais habilitados para MDX:

1. Crie um aplicativo privado do Android Enterprise e habilite o aplicativo para MDX.
2. Adicione o aplicativo ao console XenMobile.
 - Hospede e publique o aplicativo no Google Play Store gerenciado.
 - Adicione o aplicativo ao console XenMobile como um aplicativo empresarial.
3. Adicione o arquivo MDX ao XenMobile.

Se você decidir hospedar e publicar aplicativos por meio do Google Play Store, não opte pela assinatura por certificado Google. Assine o aplicativo com o mesmo certificado usado para habilitar o aplicativo para MDX. Para obter mais informações sobre como publicar aplicativos, consulte a documentação do Google em [Publicar seu app](#) e [Assinar seu app](#). O MAM SDK não prepara aplicativos, portanto, ele não requer um certificado diferente daquele usado para desenvolver o aplicativo.

Para obter mais informações sobre como publicar aplicativos privados por meio do Google Play Console, consulte a documentação do Google sobre como fazer para [Publicar apps particulares no Play Console](#).

Para publicar um aplicativo por meio do XenMobile, consulte as seções a seguir.

Preparar um aplicativo privado Android Enterprise

Ao criar um aplicativo privado do Android Enterprise, certifique-se de seguir as [Práticas recomendadas para apps particulares](#) do Google.

Depois de criar um aplicativo privado do Android Enterprise, integre o MAM SDK ao aplicativo ou prepare o aplicativo usando o MDX Toolkit. O Android Enterprise não oferece suporte a aplicativos preparados usando o MDX Service. Em seguida, adicione os arquivos resultantes ao XenMobile.

Você pode atualizar o aplicativo carregando um arquivo .apk atualizado. As etapas a seguir cobrem a preparação do aplicativo com o MDX Toolkit.

1. Crie seu aplicativo privado Android Enterprise e gere um arquivo .apk assinado.
2. O arquivo de exemplo a seguir contém todas as políticas conhecidas, algumas das quais podem não ser aplicáveis ao seu ambiente. Todas as configurações não utilizáveis são ignoradas. Crie um arquivo XML com os seguintes parâmetros:

```
1 <?xml version="1.0" encoding="UTF-8"?>
2 <MobileAppPolicies>
3   <PolicySchemaVersion>
4     1.0
5   </PolicySchemaVersion>
6   <Policies>
7     <DevicePasscode>false</DevicePasscode>
8     <AppPasscode>false</AppPasscode>
9     <MaxOfflinePeriod>72</MaxOfflinePeriod>
10    <StepupAuthAddress/>
11    <RequireUserEntropy>false</RequireUserEntropy>
12    <BlockRootedDevices>true</BlockRootedDevices>
13    <BlockDebuggerAccess>false</BlockDebuggerAccess>
14    <RequireDeviceLock>false</RequireDeviceLock>
15    <NonCompliantDeviceBehavior>AllowAppAfterWarning</
      NonCompliantDeviceBehavior>
16    <WifiOnly>false</WifiOnly>
17    <RequireInternalNetwork>false</RequireInternalNetwork>
18    <InternalWifiNetworks/>
19    <AllowedWifiNetworks/>
20    <UpgradeGracePeriod>168</UpgradeGracePeriod>
21    <WipeDataOnAppLock>false</WipeDataOnAppLock>
```

```
22     <ActivePollPeriod>60</ActivePollPeriod>
23     <PublicFileAccessLimitsList/>
24     <CutAndCopy>Unrestricted</CutAndCopy>
25     <Paste>Unrestricted</Paste>
26     <DocumentExchange>Unrestricted</DocumentExchange>
27     <OpenInExclusionList/>
28     <InboundDocumentExchange>Unrestricted</
29         InboundDocumentExchange>
30     <InboundDocumentExchangeWhitelist/>
31     <connectionSecurityLevel>TLS</connectionSecurityLevel>
32     <DisableCamera>false</DisableCamera>
33     <DisableGallery>false</DisableGallery>
34     <DisableMicrophone>false</DisableMicrophone>
35     <DisableLocation>false</DisableLocation>
36     <DisableSms>false</DisableSms>
37     <DisableScreenCapture>false</DisableScreenCapture>
38     <DisableSensor>false</DisableSensor>
39     <DisableNFC>false</DisableNFC>
40     <BlockLogs>false</BlockLogs>
41     <DisablePrinting>false</DisablePrinting>
42     <MvpnNetworkAccess>MvpnNetworkAccessUnrestricted</
43         MvpnNetworkAccess>
44     <MvpnSessionRequired>False</MvpnSessionRequired>
45     <NetworkAccess>NetworkAccessUnrestricted</NetworkAccess>
46     <DisableLocalhostConnections>false</
47         DisableLocalhostConnections>
48     <CertificateLabel/>
49     <DefaultLoggerOutput>file,console</DefaultLoggerOutput>
50     <DefaultLoggerLevel>15</DefaultLoggerLevel>
51     <MaxLogFiles>2</MaxLogFiles>
52     <MaxLogFileSize>2</MaxLogFileSize>
53     <RedirectSystemLogs>false</RedirectSystemLogs>
54     <EncryptLogs>false</EncryptLogs>
55     <GeofenceLongitude>0</GeofenceLongitude>
56     <GeofenceLatitude>0</GeofenceLatitude>
57     <GeofenceRadius>0</GeofenceRadius>
58     <EnableGoogleAnalytics>false</EnableGoogleAnalytics>
59     <Authentication>OfflineAccessOnly</Authentication>
60     <ReauthenticationPeriod>480</ReauthenticationPeriod>
61     <AuthFailuresBeforeLock>5</AuthFailuresBeforeLock>
62 </Policies>
63 </MobileAppPolicies>
64 <!--NeedCopy-->
```

3. Prepare o aplicativo usando o MDX Toolkit. Para obter informações sobre como usar o MDX

Toolkit, consulte [Preparação de aplicativos móveis Android](#).

Defina o parâmetro **apptype** como **Premium**. Use o arquivo XML da etapa anterior no comando descrito a seguir.

Se você souber o URL da loja para o aplicativo, defina o parâmetro **storeURL** como o URL da loja. Os usuários baixam o aplicativo do URL da loja depois que você publicar o aplicativo.

Aqui está um exemplo de um comando MDX Toolkit usado para preparar um aplicativo chamado SampleAEapp:

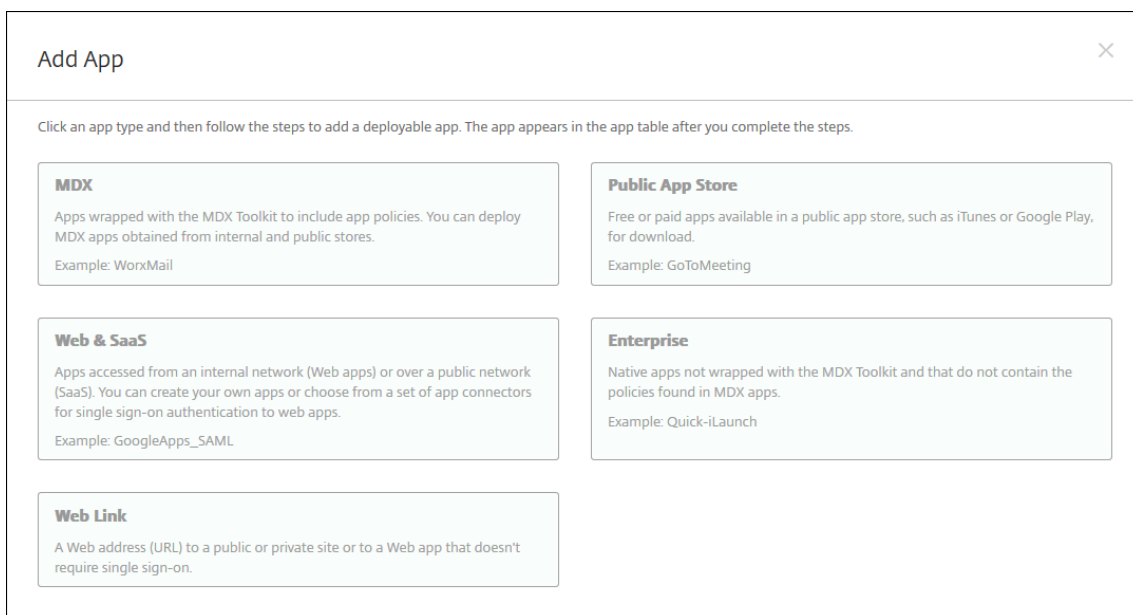
```
1  ```
2  java -Dfile.encoding=UTF-8 -Duser.country=US -Duser.language=en -
      Duser.variant
3  -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar wrap
4  -in ~/Desktop/AEAppFiles/SampleAEApp-input.apk
5  -out ~/Desktop/AEAppFiles/SampleAEApp.mdx
6  -MinPlatform 5.0
7  -keystore /MyKeystore
8  -storepass mystorepwd123
9  -keyalias key0
10 -keypass mykeypwd123
11 -storeURL "https://play.google.com/store/apps/details?id=
      SampleAEAppPackage"
12 -appType Premium
13 -premiumMdxPolicies <Path to Premium policy XML>
14 <!--NeedCopy--> ```
```

Preparar o aplicativo gera um arquivo .apk preparado e um arquivo .mdx.

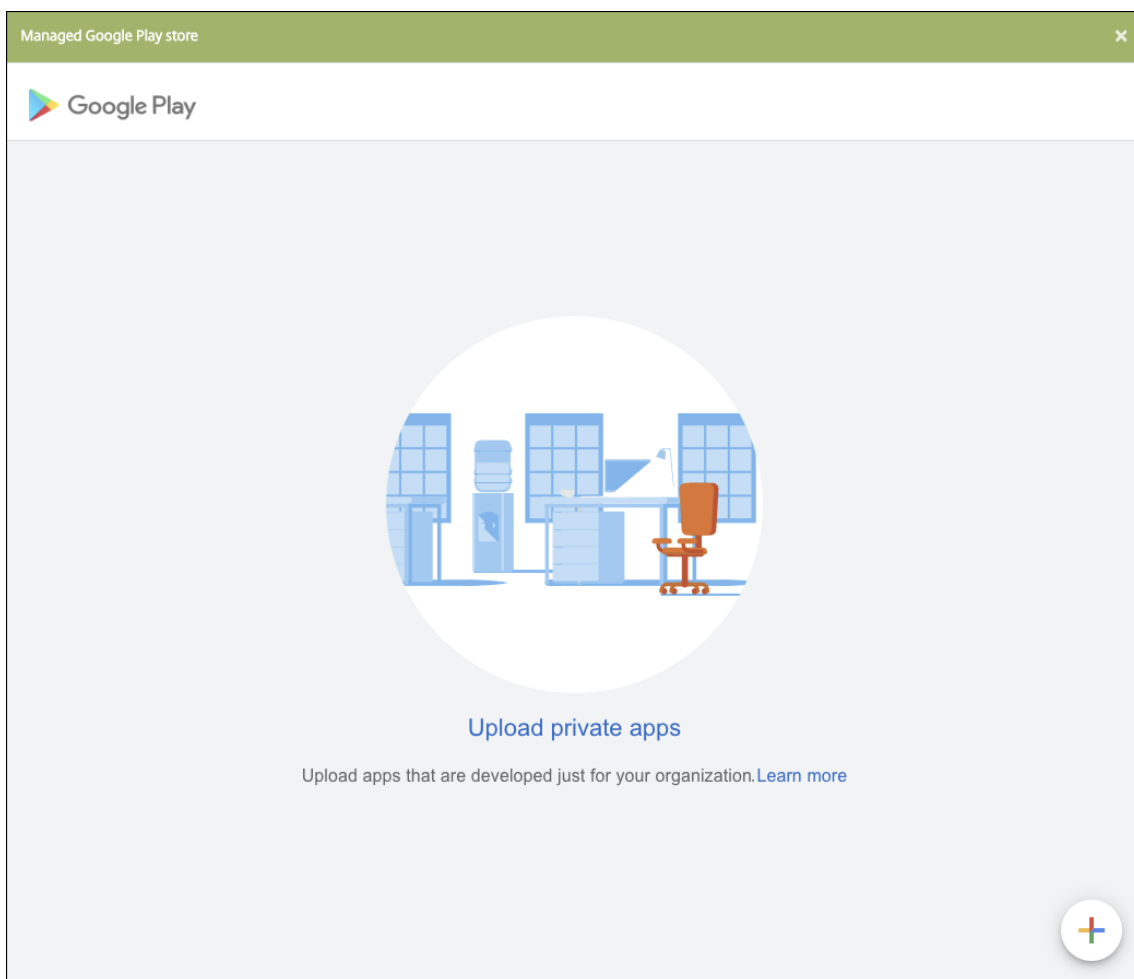
Adicionar o arquivo .apk preparado

Adicione o aplicativo de uma das duas maneiras:

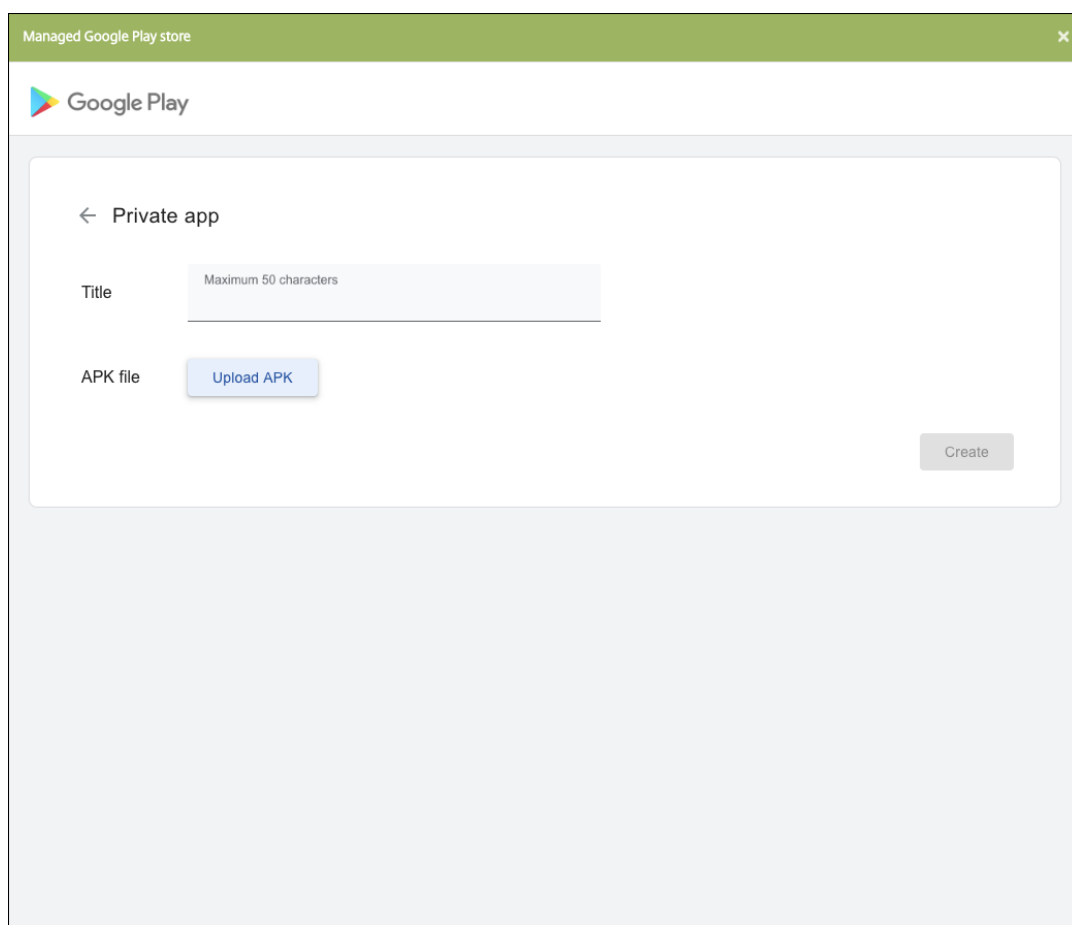
- Publique o aplicativo diretamente no Google Play Store gerenciado e adicione-o ao console XenMobile como um aplicativo gerenciado do Play Store. Veja a documentação do Google sobre como [Publicar apps particulares](#) e siga as etapas na seção Aplicativos da loja de aplicativos gerenciada.
- Adicione o aplicativo ao console XenMobile como um aplicativo empresarial. Execute as seguintes etapas:
 1. No console XenMobile, clique em **Configurar > Aplicativos**. A página **Aplicativos** é aberta.
 2. Clique em **Adicionar**. A caixa de diálogo **Adicionar Aplicativo** é exibida.



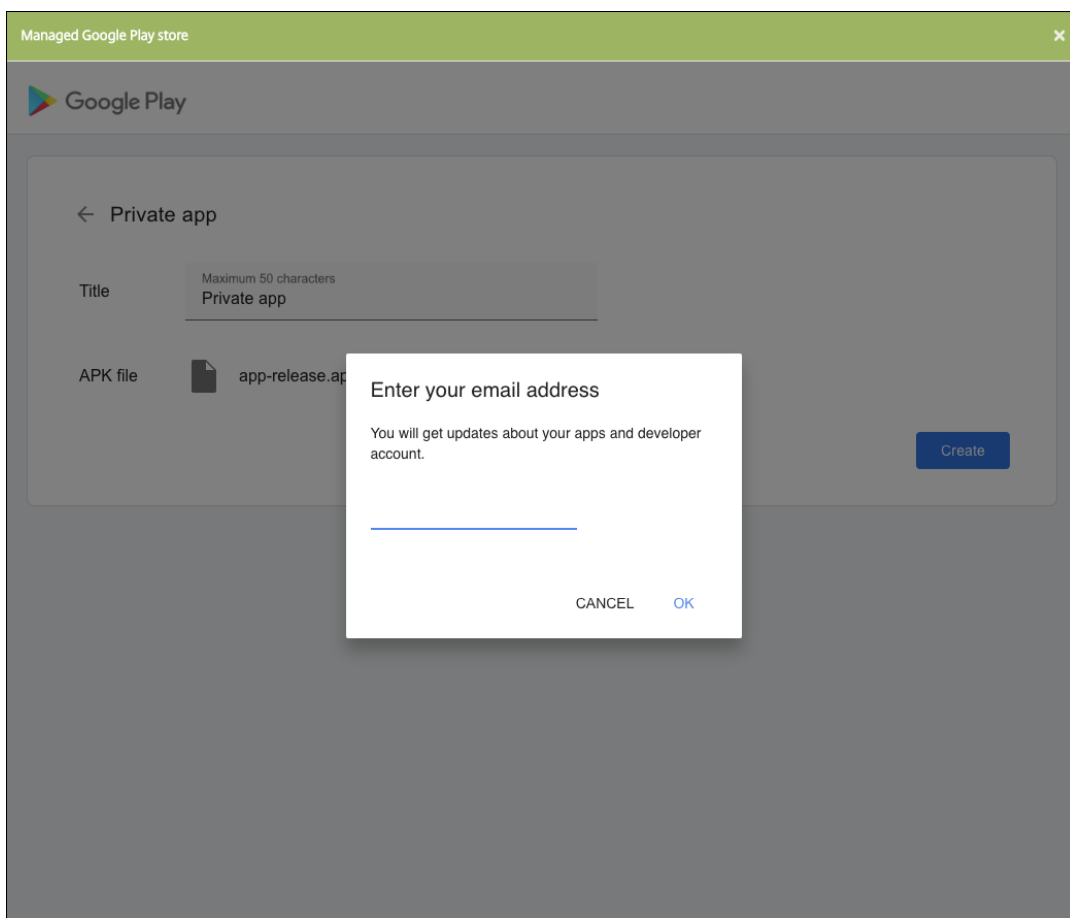
3. Clique em **Empresarial**. No painel **Informações do aplicativo**, digite as seguintes informações:
 - **Nome**: digite um nome descritivo para o aplicativo. Esse nome fica listado em Nome do aplicativo, na tabela Aplicativos.
 - **Descrição**: digite uma descrição opcional para o aplicativo.
 - **Categoria do aplicativo**: opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte [Sobre categorias de aplicativos](#).
4. Selecione **Android Enterprise** como a plataforma.
5. O botão **Carregar** abre o Google Play Store gerenciado. Você não precisa se registrar em uma conta de desenvolvedor para publicar um aplicativo privado. Clique no ícone de **adição** no canto inferior direito para continuar.



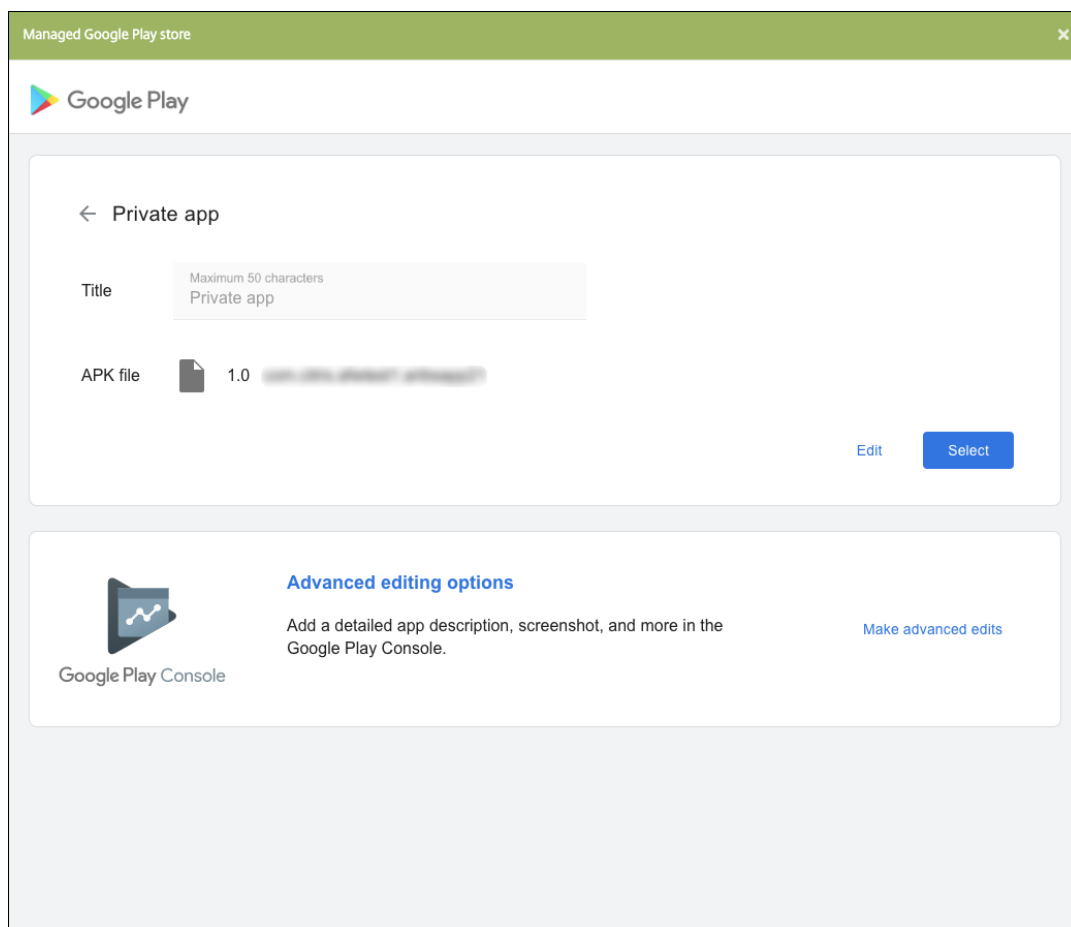
- a) Digite o nome do seu aplicativo e carregue o arquivo .apk. Quando terminar, clique em **Criar**. Pode levar até 10 minutos para que seu aplicativo privado seja publicado.



b) Insira um endereço de e-mail para receber atualizações sobre seus aplicativos.



- c) Após a publicação do aplicativo, clique no ícone de um aplicativo privado e clique em **Selecionar** para abrir a página de informações do aplicativo.



6. Clique em **Avançar**. A página de informações do aplicativo da plataforma é exibida.

7. Defina as configurações do tipo de plataforma, como:

- **Nome do arquivo:** opcionalmente, digite um novo nome para o aplicativo.
- **Descrição do aplicativo:** opcionalmente, digite uma nova descrição para o aplicativo.
- **Versão do aplicativo:** você não pode alterar esse campo.
- **ID de pacote:** Identificador exclusivo do seu aplicativo.
- **Versão do SO mínima:** opcionalmente, digite a versão mais antiga do sistema operacional que o dispositivo pode executar para usar o aplicativo.
- **Versão do SO máxima:** opcionalmente, digite a versão mais recente do sistema operacional que o dispositivo deve executar para usar o aplicativo.
- **Dispositivos excluídos:** opcionalmente, digite o fabricante ou os modelos de dispositivos que não podem executar o aplicativo.

8. Configure as regras de implantação e a configuração de armazenamento.

9. Na página **Android Enterprise Enterprise App**, clique em **Avançar**. A página **Aprovações** é exibida.

Para usar fluxos de trabalho para exigir aprovação antes de permitir que os usuários acessem o

aplicativo, consulte [Aplicar fluxos de trabalho](#). Se você não precisar de um fluxo de trabalho de aprovação, pule para a Etapa 13.

10. Clique em **Avançar**.
11. A página **Atribuição de grupo de entrega** é exibida. Nenhuma ação é necessária nesta página. Você configura os grupos de entrega e o cronograma de implantação para esse aplicativo ao adicionar o arquivo .mdx. Clique em **Salvar**.

Opcional: adicionar ou alterar o URL da loja

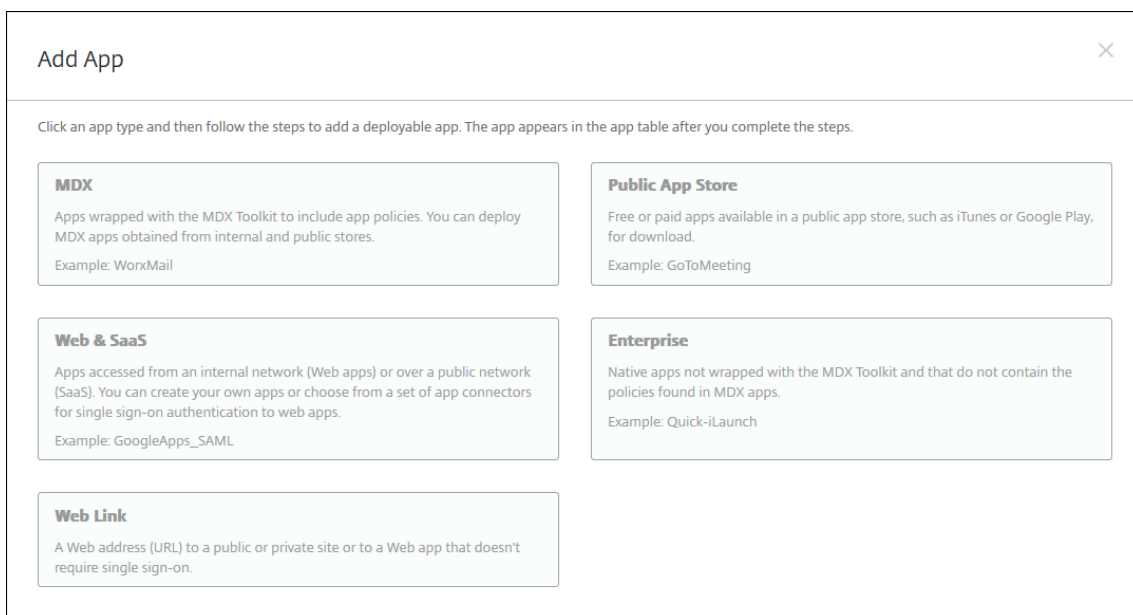
Se você não sabia o URL da loja quando preparou o aplicativo, adicione o URL da loja agora.

1. Visualize o aplicativo no Google Play Store gerenciado. Quando você seleciona o aplicativo, o URL da loja aparece na barra de endereços do navegador. Copie o nome do pacote do aplicativo do formulário do URL. Por exemplo: <https://play.google.com/store/apps/details?id=SampleAEappPackage>. O URL que você copia pode começar com <https://play.google.com/work/>. Certifique-se de mudar *work* para *store*.
2. Use o MDX Toolkit para adicionar o URL da loja ao arquivo .mdx:

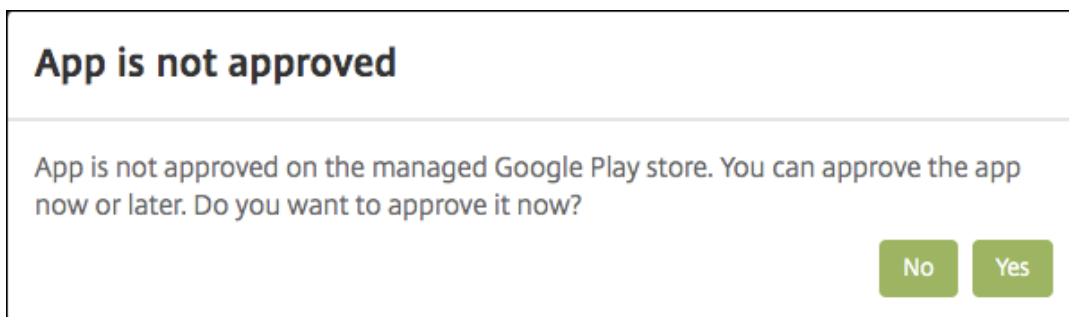
```
1 java -jar /Applications/Citrix/MDXToolkit/ManagedAppUtility.jar \  
2 setinfo \  
3 -in ~/Desktop/SampleApps/Sample.mdx \  
4 -out ~/Desktop/SampleApps/wrapped/Sample.mdx \  
5 -storeURL "https://play.google.com/store/apps/details?id=  
   SampleAEappPackage"  
6 <!--NeedCopy-->
```

Adicionar o arquivo .mdx

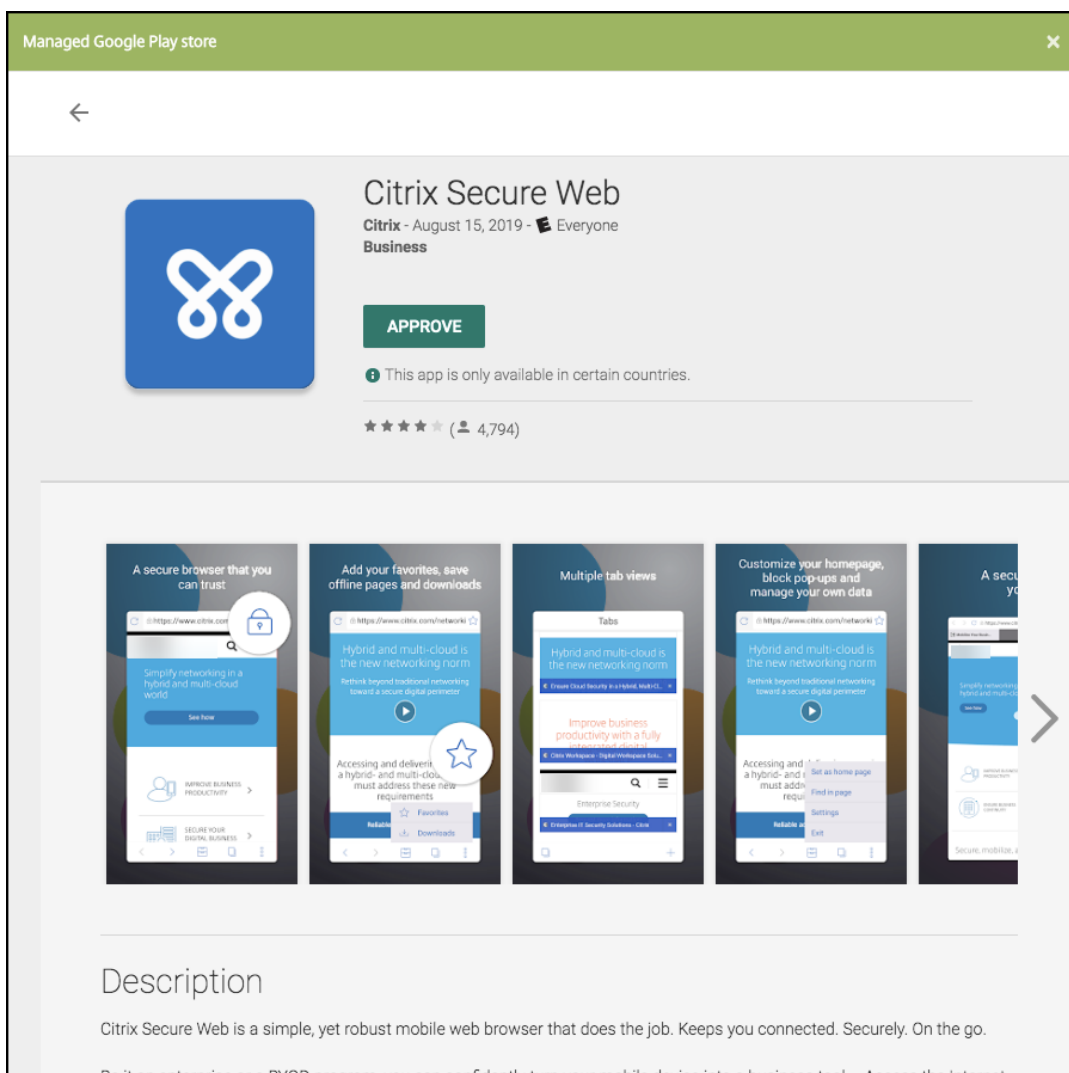
1. No console XenMobile, clique em **Configurar > Aplicativos**. Clique em **Adicionar**. A caixa de diálogo **Adicionar Aplicativo** é exibida.



2. Clique em **MDX**. A página **Informações do aplicativo MDX** é exibida. No painel **Informações do aplicativo**, digite as seguintes informações:
 - **Nome**: digite um nome descritivo para o aplicativo. O nome aparecerá em **Nome do aplicativo** na tabela **Aplicativos**.
 - **Descrição**: digite uma descrição opcional para o aplicativo.
 - **Categoria do aplicativo**: opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte [Sobre categorias de aplicativos](#).
3. Selecione **Android Enterprise** como a plataforma.
4. Clique em **Carregar** e navegue até o arquivo MDX. O Android Enterprise só suporta aplicativos preparados com o MDX Toolkit. Não prepare aplicativos usando o MDX Service.
 - A interface do usuário notificará você se o aplicativo anexado exigir aprovação do Google Play Store gerenciado. Para aprovar o aplicativo sem sair do console XenMobile, clique em **Sim**.



Depois que o Google Play Store gerenciado abrir, siga as instruções para aprovar e salvar o aplicativo.



Quando você adicionar o aplicativo com êxito, a página **Detalhes do aplicativo** será exibida.

5. Defina estas configurações:

- **Nome do arquivo:** digite o nome de arquivo associado ao aplicativo.
- **Descrição do aplicativo:** digite uma descrição para o aplicativo.
- **Versão do aplicativo:** opcionalmente, digite o número da versão do aplicativo.
- **ID de pacote:** digite o ID do pacote para o aplicativo, obtido no Google Play Store gerenciado.
- **Versão do SO mínima:** opcionalmente, digite a versão mais antiga do sistema operacional que o dispositivo pode executar para usar o aplicativo.
- **Versão do SO máxima:** opcionalmente, digite a versão mais recente do sistema operacional que o dispositivo deve executar para usar o aplicativo.
- **Dispositivos excluídos:** opcionalmente, digite o fabricante ou os modelos de dispositivos que não podem executar o aplicativo.

6. Configure as **Políticas de MDX**. As políticas de MDX variam por plataforma e incluem opções para áreas de política, incluindo Autenticação, Segurança do dispositivo e Restrições de aplicativo. No console, cada uma das políticas tem uma dica de ferramenta que descreve a política. Para obter informações sobre as políticas de aplicativo que estão disponíveis para cada tipo de plataforma de dispositivo, consulte:

- [Visão geral do SDK MAM](#)
- [Resumo das políticas de aplicativos MDX de terceiros](#)

7. Configure as regras de implantação e a configuração de armazenamento.

Implantar para conexões permanentes é aplicável quando você tiver configurado a chave de implantação em segundo plano do cronograma em **Configurações > Propriedades do servidor**.

A opção sempre ativa:

- Não estão disponíveis para clientes Android Enterprise que começaram a usar o Endpoint Management com a versão 10.18.19 ou posterior
- Não é recomendado para clientes Android Enterprise que começaram a usar o Endpoint Management antes da versão 10.18.19

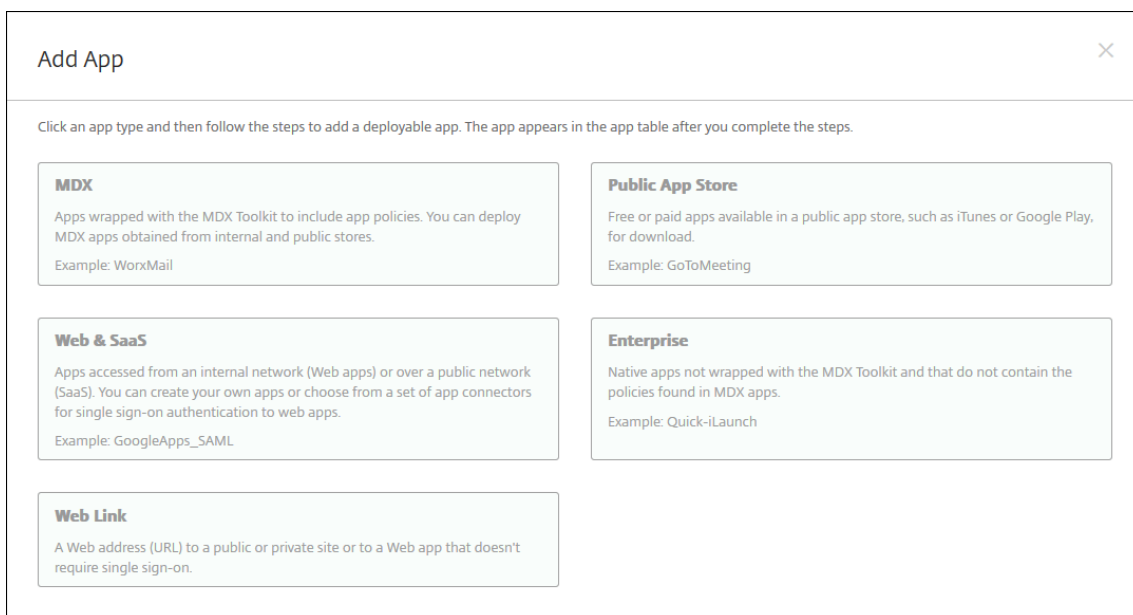
O cronograma de implantação que você configura é o mesmo para todas as plataformas. Todas as alterações feitas se aplicam a todas as plataformas, exceto **Implantar para conexões permanentes**.

8. Atribua grupos de entrega ao aplicativo e clique em **Salvar**. Para obter informações, consulte [Implantar recursos](#).

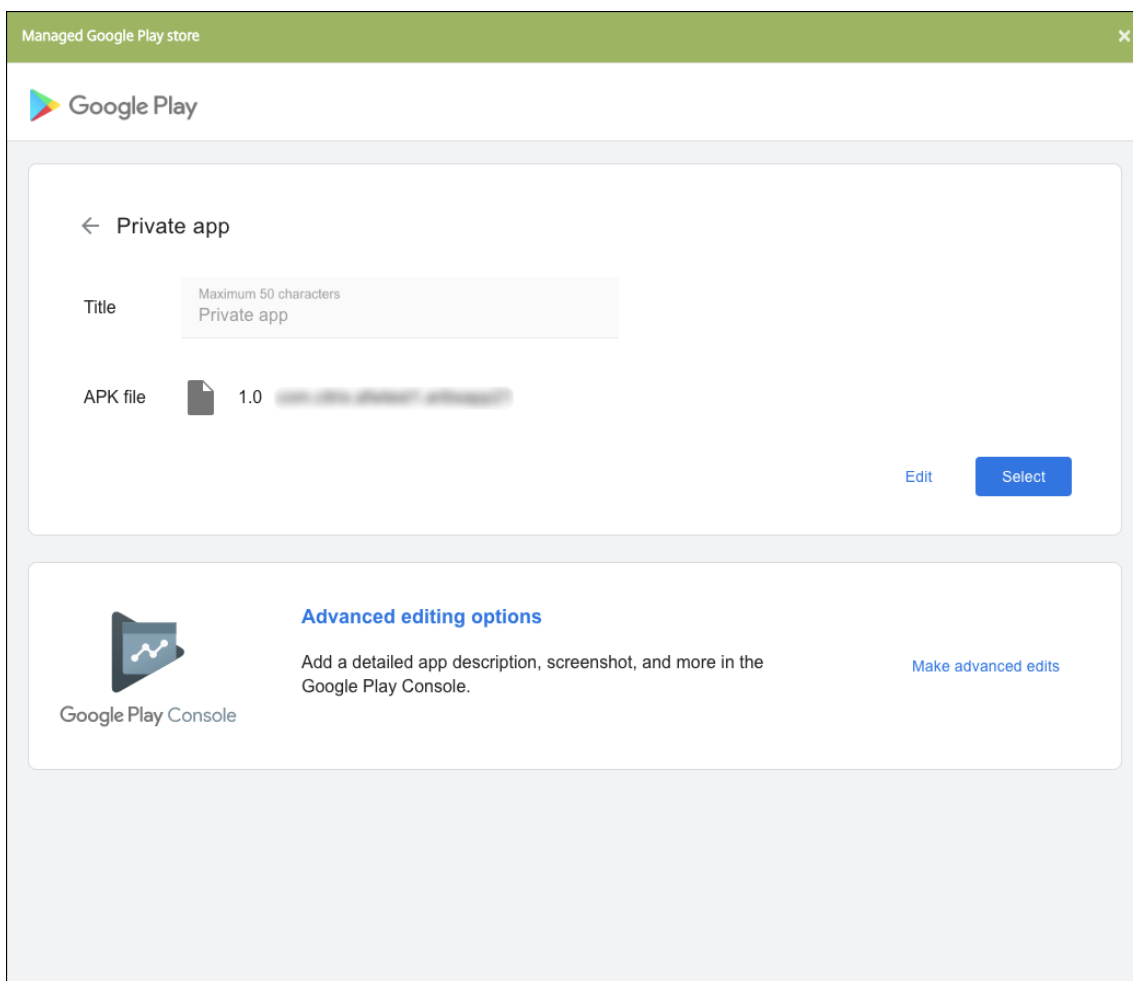
Atualizar o aplicativo

Para atualizar o aplicativo Android Enterprise, prepare e carregue um arquivo .apk atualizado:

1. Prepare o arquivo .apk do aplicativo atualizado usando o MAM SDK ou MDX Toolkit.
2. No console XenMobile, clique em **Configurar > Aplicativos**. A página **Aplicativos** é aberta.



3. Clique em **Adicionar**. A caixa de diálogo **Adicionar Aplicativo** é exibida.
4. Clique em **Empresarial**. No painel **Informações do aplicativo**, digite as seguintes informações:
 - **Nome**: digite um nome descritivo para o aplicativo. Esse nome fica listado em Nome do aplicativo, na tabela Aplicativos.
 - **Descrição**: digite uma descrição opcional para o aplicativo.
 - **Categoria do aplicativo**: opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte [Sobre categorias de aplicativos](#).
5. Selecione **Android Enterprise** como a plataforma.
6. Clique em **Avançar**. A página **Aplicativo enterprise do Android Enterprise** é exibida.
7. Clique em **Carregar**.
8. Na página do Google Play Store gerenciado, selecione o aplicativo que deseja atualizar.
9. Na página de informações do aplicativo, clique em **Editar** ao lado do nome do arquivo .apk.



10. Navegue até o novo arquivo .apk e carregue-o.
11. Na página do Google Play Store gerenciado, clique em **Salvar**.

Clientes do Android Enterprise herdado para Google Workspace (anteriormente G Suite)

August 20, 2021

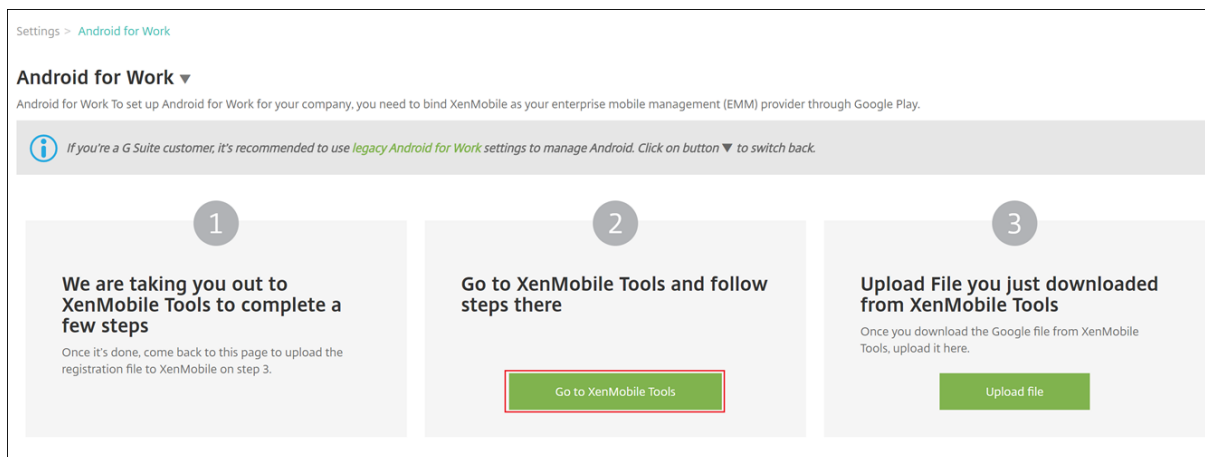
Os clientes do Google Workspace (anteriormente G Suite) devem usar as configurações do Android Enterprise legado para configurar o Android Enterprise legado.

Requisitos para o Android Enterprise herdado:

- Um domínio publicamente acessível
- Uma conta de administrador do Google
- Os dispositivos que têm gerenciadas perfis e que executam o Android 5.0 + lollipop compatíveis

- Uma conta do Google que tenha o Google Play instalado
- Um perfil de trabalho configurado no dispositivo

Para iniciar a configuração do Android Enterprise herdado, clique em **Android Enterprise herdado** na página **Android Enterprise** nas configurações do XenMobile.



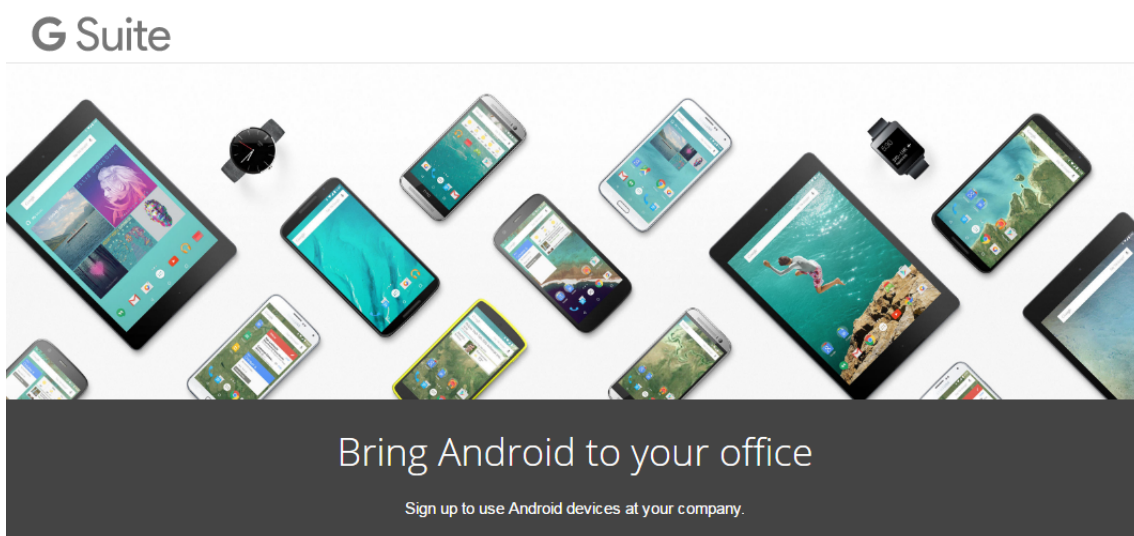
Criar uma conta do Android Enterprise

Antes de poder configurar uma conta do Android Enterprise, você deve confirmar seu nome de domínio com o Google.

Se você já tiver verificado o nome do domínio junto ao Google, poderá seguir para esta etapa: Configurar uma conta de serviço do Android Enterprise e baixar um certificado do Android Enterprise.

1. Navegue até https://www.google.com/a/signup/?enterprise_product=ANDROID_WORK.

A seguinte página é exibida, na qual você pode digitar suas informações de administrador e da empresa.



① About you

Name

First Name Last Name

Current work email Doesn't have to be an official business email.

Phone

2. Insira as informações de usuário administrador.

① About you

Name

Justa User

Current work email Doesn't have to be an official business email.

justa.user@gmail.com

Phone

+15551234567

3. Digite as informações da sua empresa, além de informações da sua conta de administrador.

② About your business

Business name
EXAMPLE CORP ✓

Business domain address You'll need to verify that you own this domain.
example.com ✓

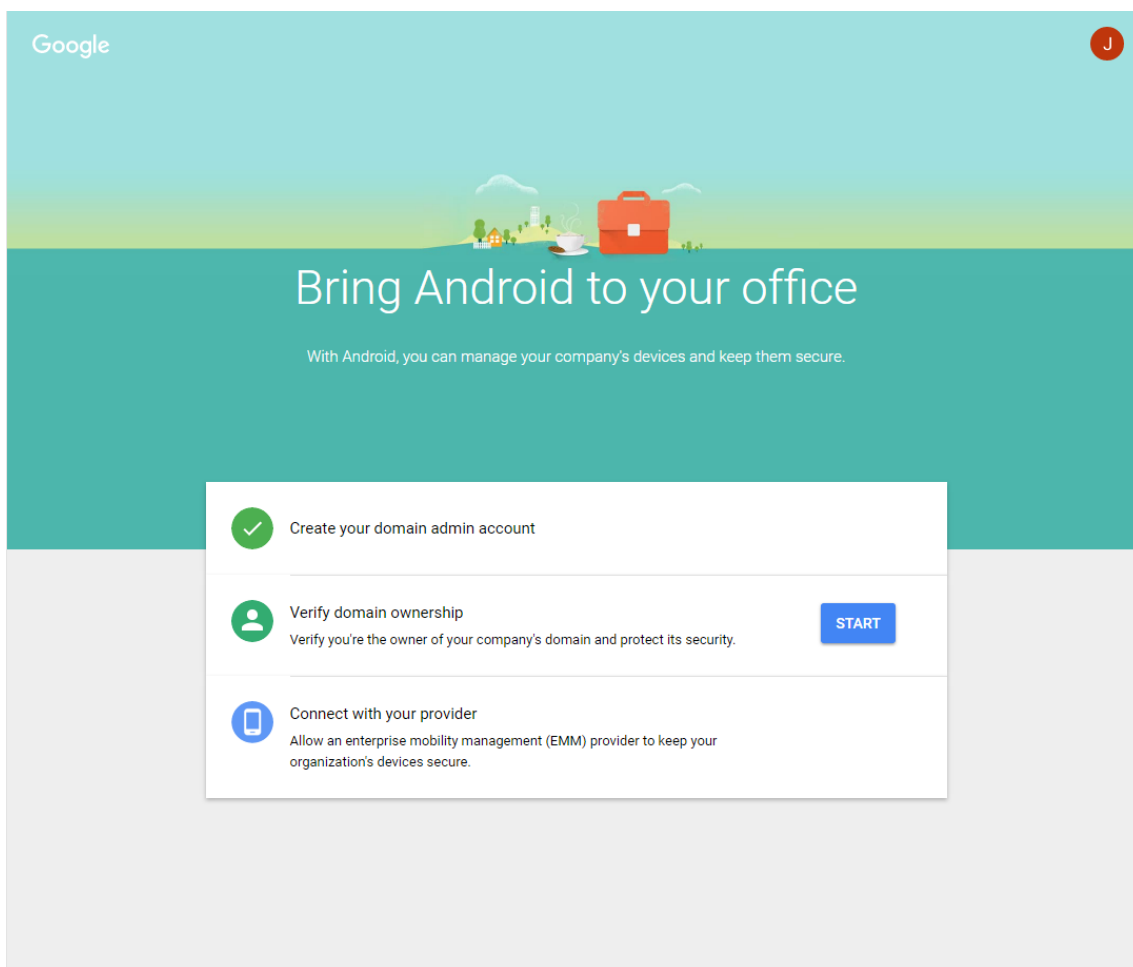
Number of employees Country/Region
1 employee United States

③ Your Google admin account Why do I need this?

Username Create an account to manage Android for Work
justa.user ✓ @ example.com

Create a password 8-character minimum; case sensitive
..... ✓
..... ✓

A primeira etapa no processo foi concluída e você vê a página a seguir.



Verificar a propriedade do domínio


Permitir que o Google Verifique o seu domínio de uma das seguintes maneiras:

- Adicione um registro TXT ou CNAME no site do host seu domínio.
- Carrega um arquivo HTML para o servidor web do seu domínio.
- Adicione uma marca `<meta>` para a sua página inicial. O Google recomenda o primeiro método. Este artigo não aborda as etapas para verificar a propriedade do seu domínio, mas você pode encontrar as informações de que precisa aqui: <https://support.google.com/a/answer/6248925/>.

1. Clique em **Start** para iniciar a verificação do seu domínio.

A página **Verify domain ownership** é exibida. Siga as instruções nessa página para verificar o seu domínio.

2. Clique em **Verify**.



Verify domain ownership


Before you can use Google Apps with domain **example.com**, we need to contact your domain host to verify that you own it. Doing this helps ensure that no one can pose as you on Google Apps and send email from your domain. [Learn more](#)


After your domain is verified, we will set up Google Apps email for your users on **example.com**. This will automatically re-route your emails to Google Apps. [Learn more](#)

We have detected that **example.com** is hosted at **GoDaddy.com**. If you're having trouble, try to [verify your domain here](#).

Note: Before you route email to Google Apps, make sure that you create a user on Google Apps for each person receiving mail at **example.com**.

[VERIFY](#)

 Need help? Search the [Help Center](#) or call **844-390-7627** and provide your unique PIN **12345678**



Verify domain ownership

Verification checklist

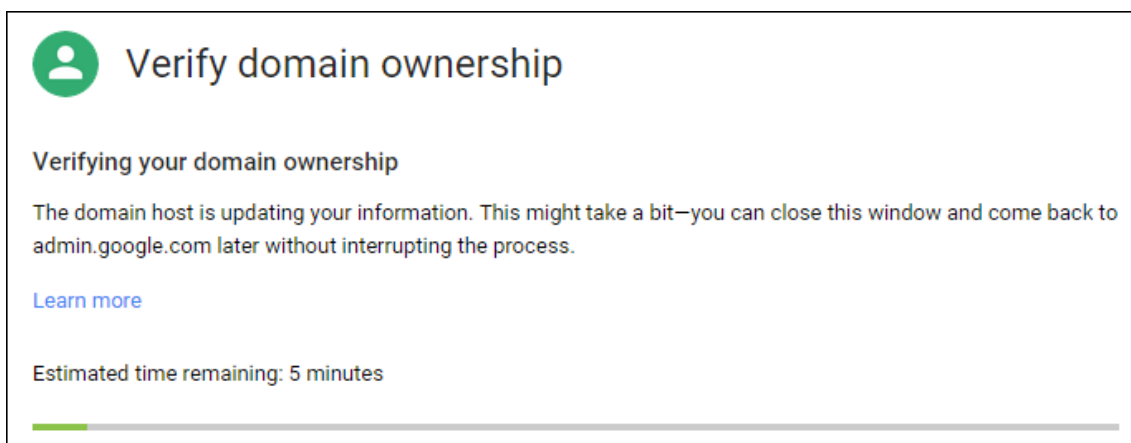
Follow these steps to help Google verify that you own the domain **example.com**.

[Learn more](#)

- I have successfully logged in.
- I have opened the control panel for my domain.
- I have created the CNAME record.
- I have saved the CNAME record.

[VERIFY](#)

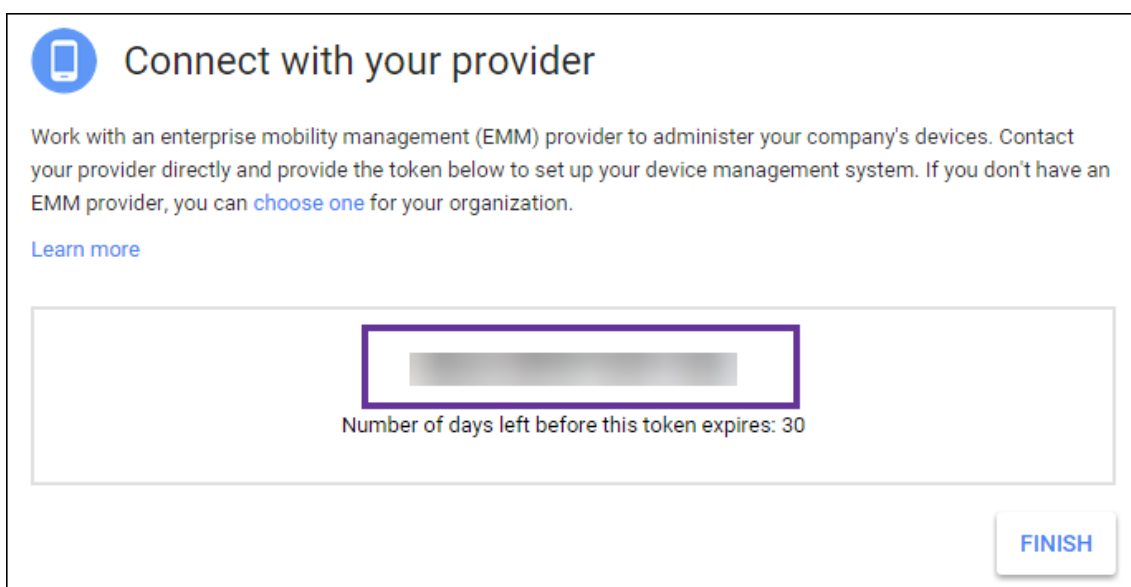
3. O Google verifica a propriedade do domínio.



4. Após uma verificação bem-sucedida, a página a seguir é exibida. Clique em **Continue**.



5. O Google cria um token de associação de EMM que você fornece para a Citrix e usa ao definir as configurações do Android Enterprise. Copie e salve o token; você precisará dele mais tarde no processo de instalação.



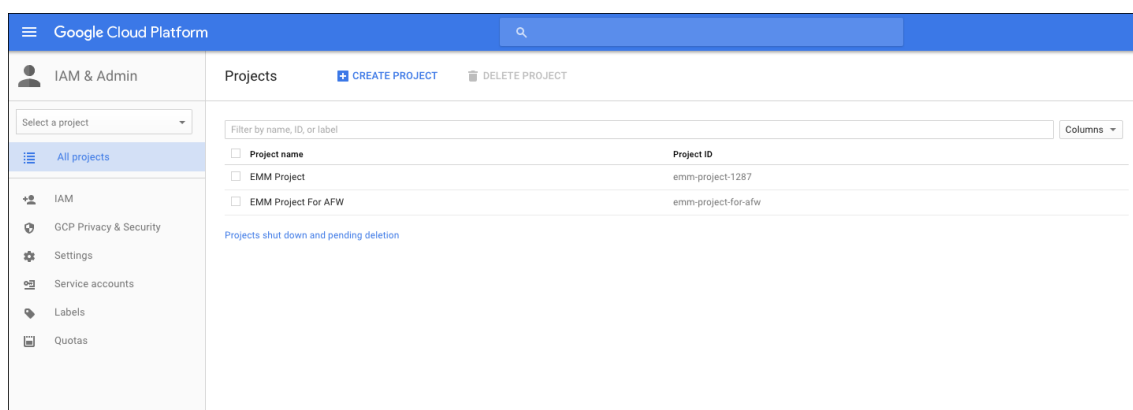
6. Clique em **Finish** para concluir a instalação do Android Enterprise. Uma página será exibida, indicando que com êxito verificar seu domínio.

Depois de criar uma conta de serviço do Android Enterprise, você poderá fazer login no console do Google Admin para gerenciar as configurações de gerenciamento de mobilidade.

Configurar uma conta de serviço do Android Enterprise e baixar um certificado do Android Enterprise

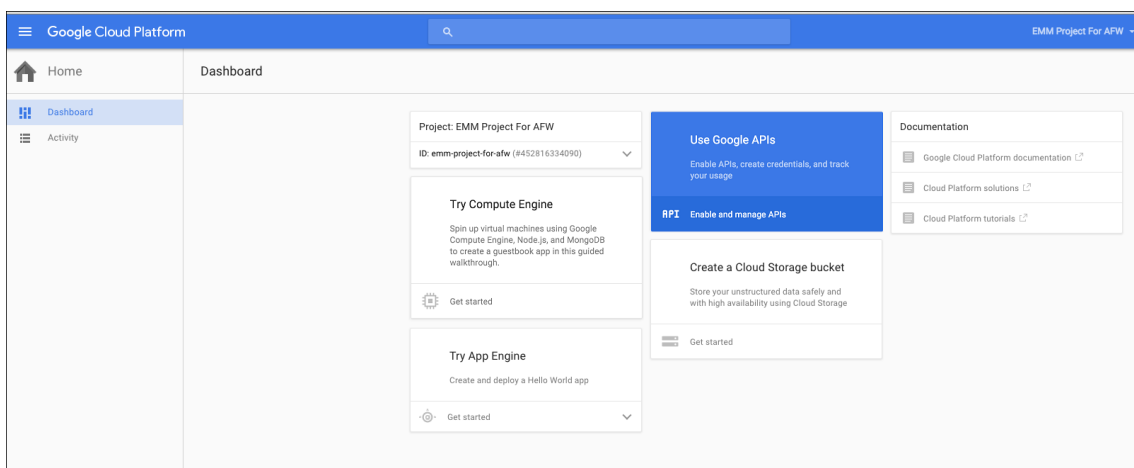
Para permitir que o XenMobile contate os serviços do Google Play e do Directory, você deverá criar uma conta de serviço usando o portal Google Project para desenvolvedores. Essa conta de serviço é usada para a comunicação servidor-a-servidor entre o XenMobile e os serviços do Google para o Android at Work. Para obter mais informações sobre o protocolo de autenticação usado, vá para <https://developers.google.com/identity/protocols/OAuth2ServiceAccount>.

1. Em um navegador da web, acesse <https://console.cloud.google.com/project> e faça login com suas credenciais de administrador do Google
2. Na lista **Projects**, clique em **Create Project**.

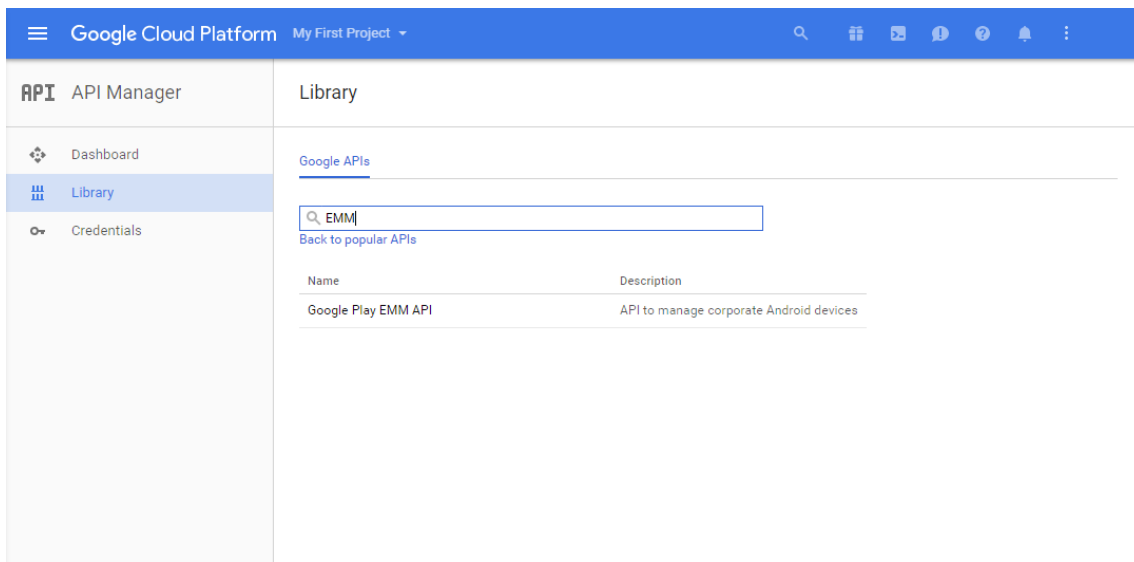


3. Em **Project name**, digite um nome para o projeto.

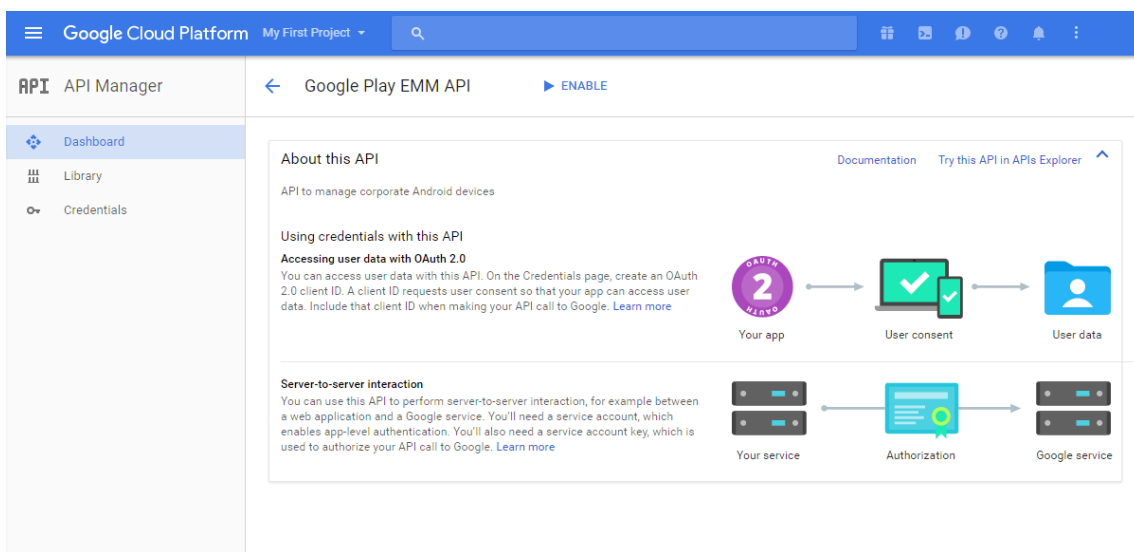
4. Em Dashboard, clique em **Use Google APIs**.



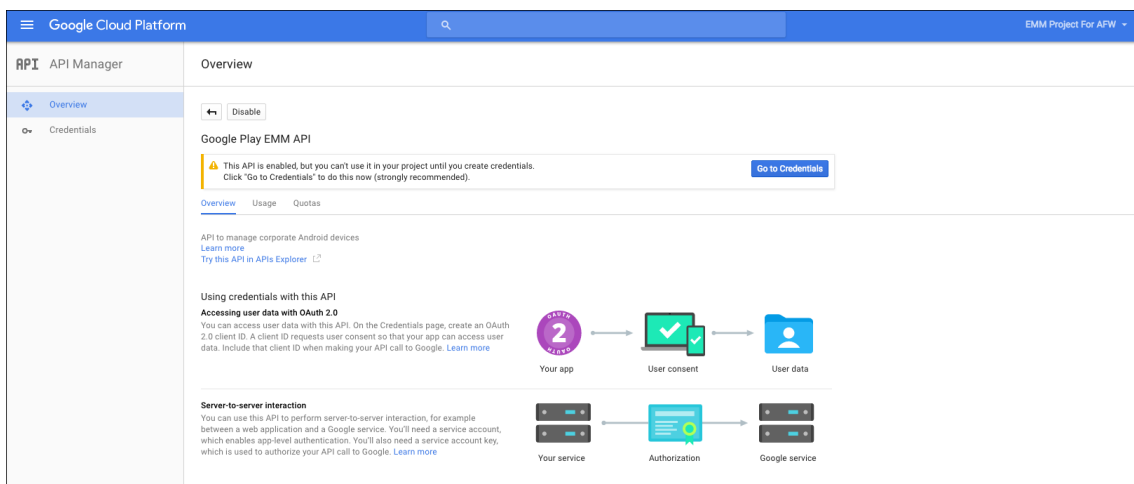
5. Clique em **Library**, em **Search**, tipo **EMM** e, em seguida, clique no resultado da pesquisa.



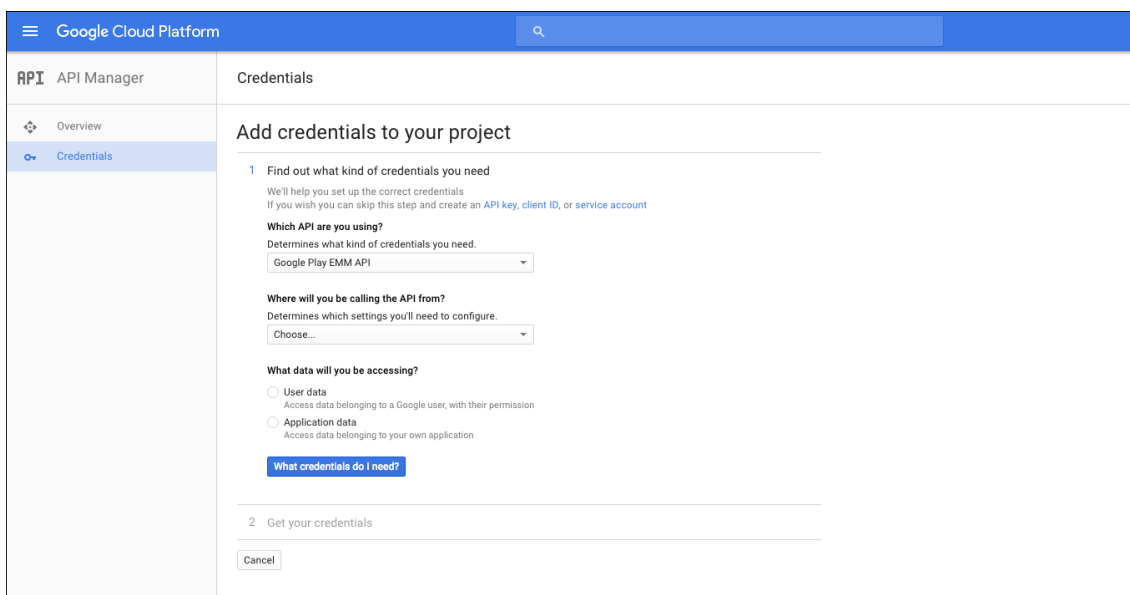
6. Na página **Overview**, clique em **Enable**.



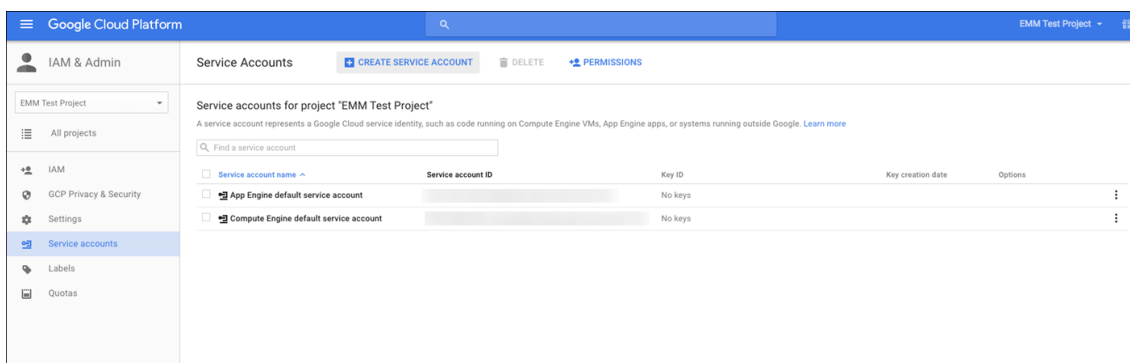
7. Ao lado de **Google Play EMM API**, clique em **Go to Credentials**.



8. Na lista **Add credentials to our project**, na etapa 1, clique em **service account**.



9. Na página **Service Accounts**, clique em **Create Service Account**.



10. Em **Create service account**, dê um nome à conta e marque a caixa de seleção **Furnish a new private key**. Clique em **P12**, marque a caixa de seleção **Enable Google Apps Domain-wide Delegation** e, em seguida, clique em **Create**.

Create service account

Service account name [?]
testemmsvcacct

Service account ID
testemmsvcacct @

Furnish a new private key
Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

Key type

JSON
Recommended

P12
For backward compatibility with code using the P12 format

Enable Google Apps Domain-wide Delegation
Grants a client access to all users' data on a Google Apps domain without manual authorization on their part. [Learn more](#)

To change settings for Google Apps domain, product name for the OAuth consent screen must be configured. Assign the product name below or configure the OAuth consent screen.

Product name for the consent screen
anynamewilldo

Create **Configure consent screen** **Cancel**

O certificado (arquivo P12) é baixado para o seu computador. Não se esqueça de salvar o certificado em uma localização segura.

11. Na tela de confirmação **Service account created**, clique em **Close**.

Service account created

The service account "testemmsvcacct" was given editor permission for the project.

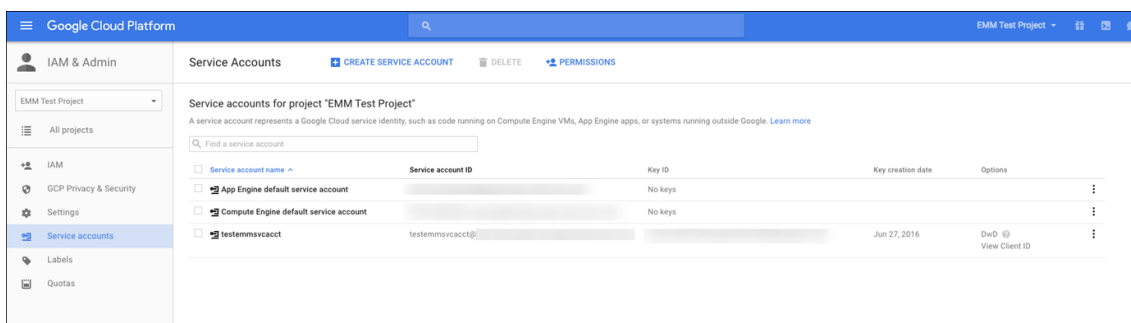
The account's private key **EMM Test Project-37cb73ad0169.p12** has been saved on your computer. This is the only copy of the key, so store it securely.

This is the private key's password. It will not be shown again. You must present this password to use the private key. [Learn more](#)

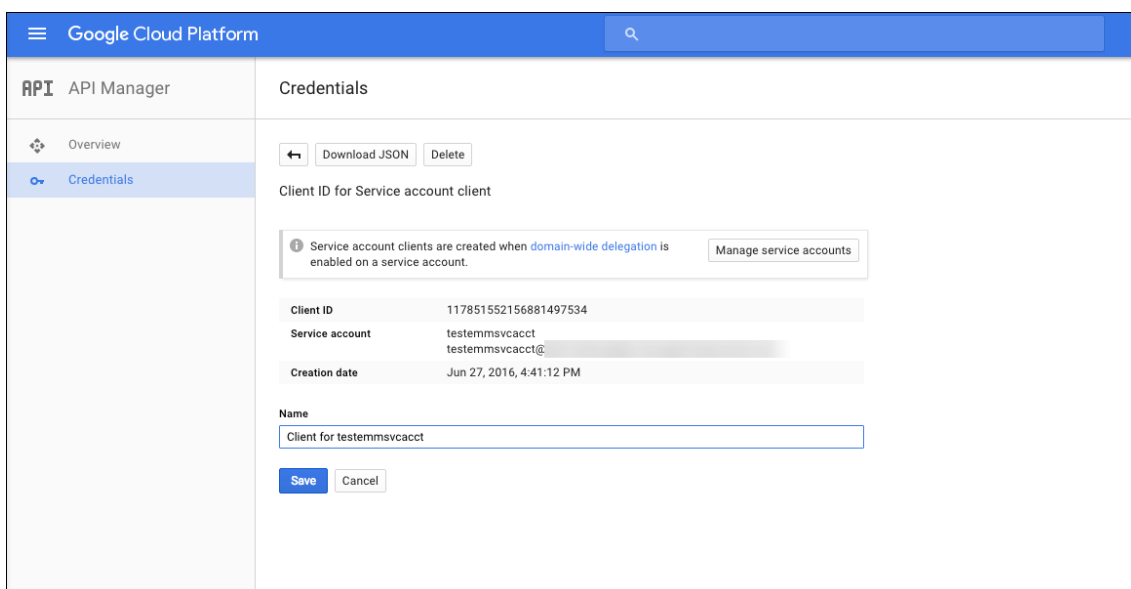
notasecret

Close

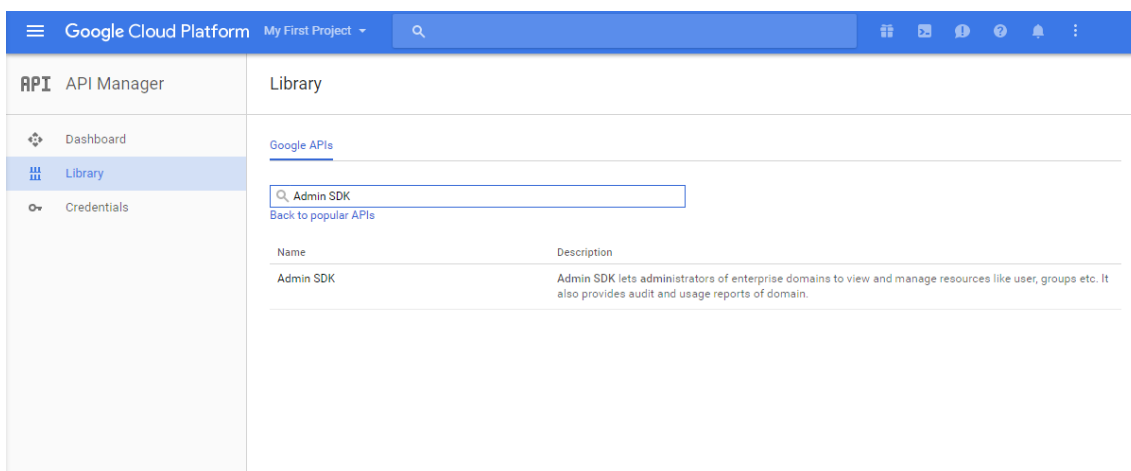
12. Em **Permissions**, clique em **Service accounts** e depois sob **Options** da sua conta de serviço, clique em **View Client ID**.



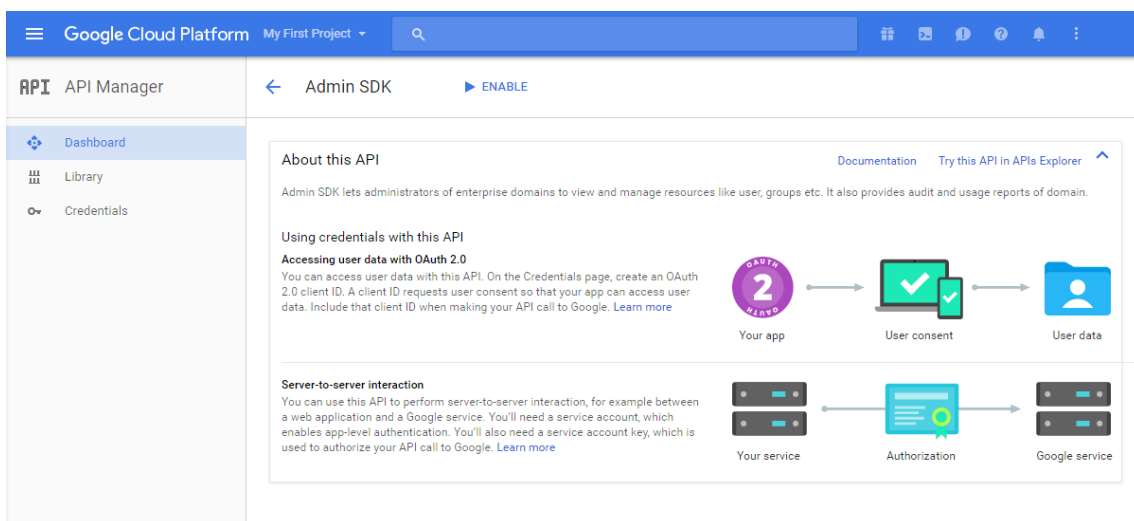
- Os detalhes necessários para a autorização da conta no console de administração do Google são exibidos. Copie o **Cliente ID** e o **Service account ID** para um local onde você possa recuperar as informações posteriormente. Você precisa dessas informações, juntamente com o nome de domínio, para enviar para o suporte da Citrix para inclusão na lista de permissão.



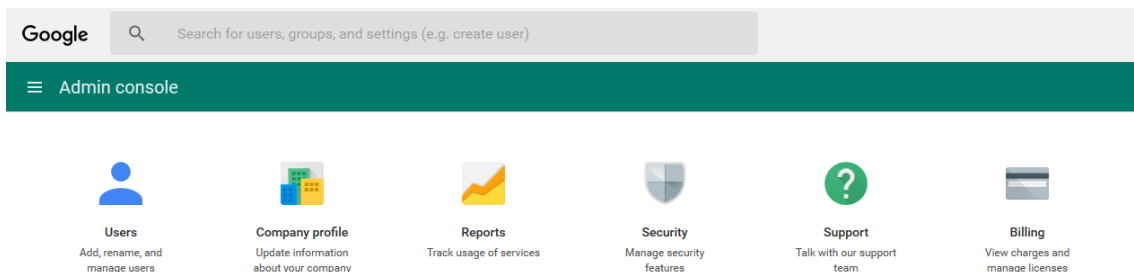
- Na página **Library**, procure **Admin SDK** e, em seguida, clique no resultado da pesquisa.



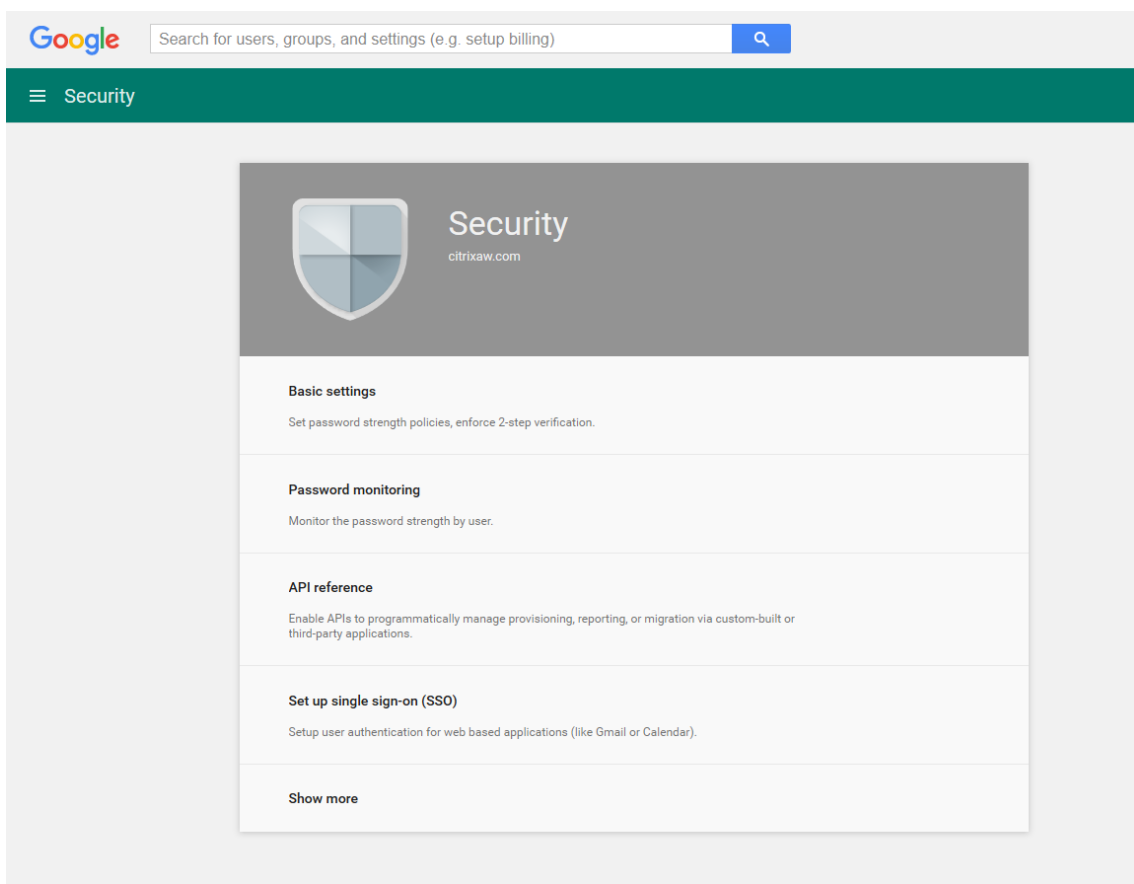
- Na página **Overview**, clique em **Enable**.

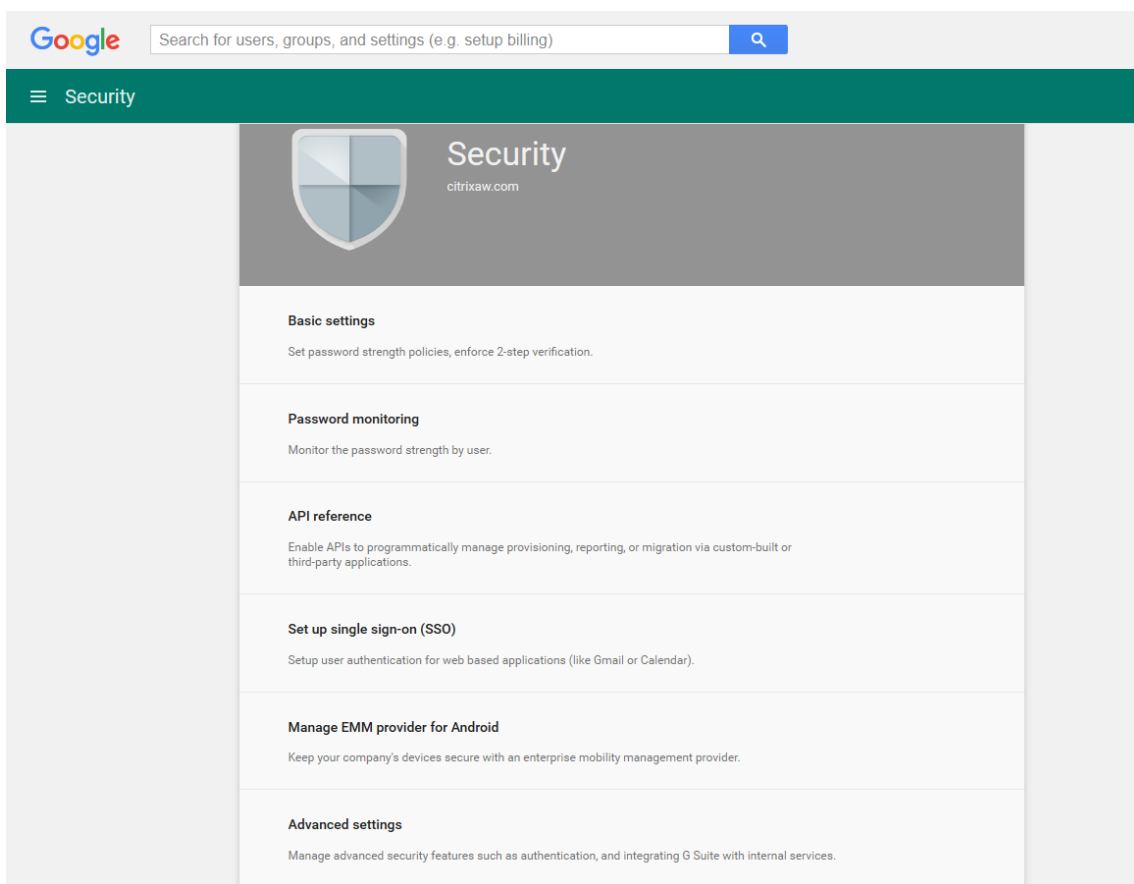


16. Abra o console de administração do Google do seu domínio e clique em **Security**.

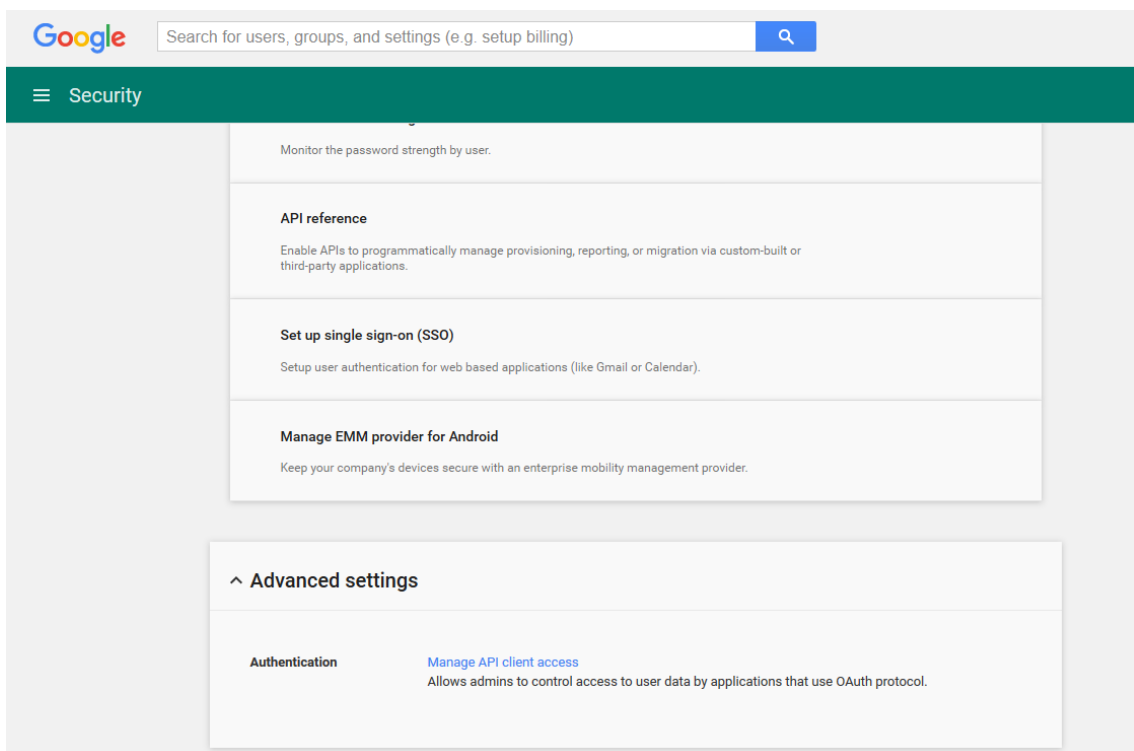


17. Na página **Settings**, clique em **Show more** e, em seguida, clique em **Advanced settings**.

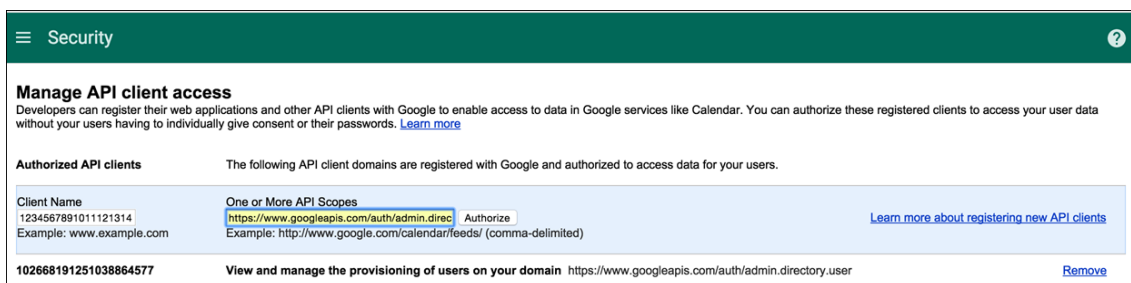




18. Clique em **Manage API client access**.



- Em **Client Name**, insira o ID de cliente que você salvou anteriormente, em **One or More API Scopes**, insira `https://www.googleapis.com/auth/admin.directory.user` e clique em **Authorize**.



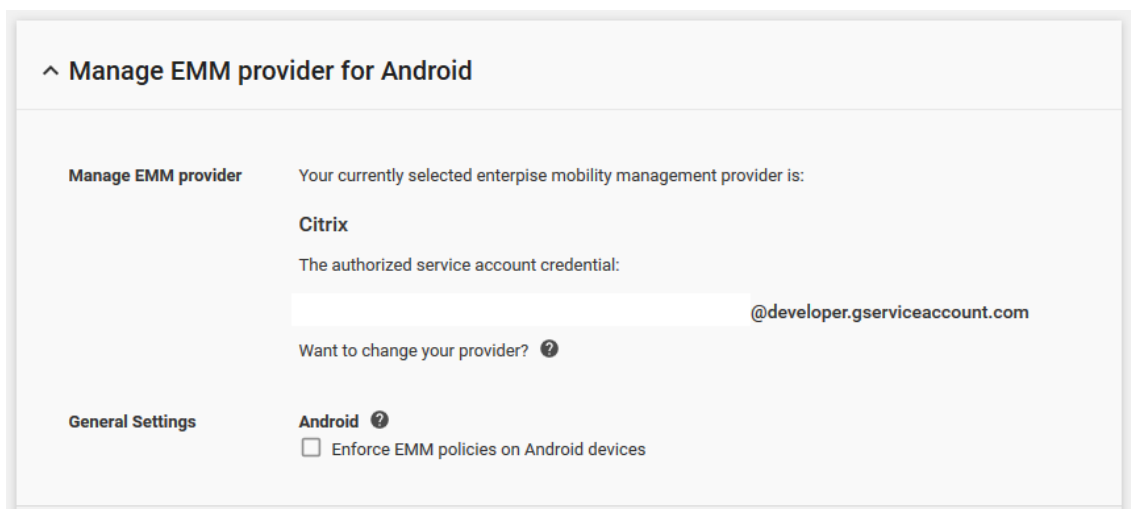
Vinculando ao EMM

Antes de usar o XenMobile para gerenciar os seus dispositivos do Android, você deve contatar o Suporte Técnico da Citrix e fornecer o seu nome de domínio, conta de serviço e token de associação. A Citrix associa o token ao XenMobile como o seu provedor de gerenciamento de mobilidade empresarial (EMM). Para informações de contato para suporte técnico da Citrix, consulte o [Suporte Técnico da Citrix](#).

- Para confirmar a associação, faça login no portal do Google Admin e clique em **Security**.
- Clique em **Manage EMM provider for Android**.

Você verá que a conta do Google Android Enterprise está associada à Citrix como seu provedor de EMM.

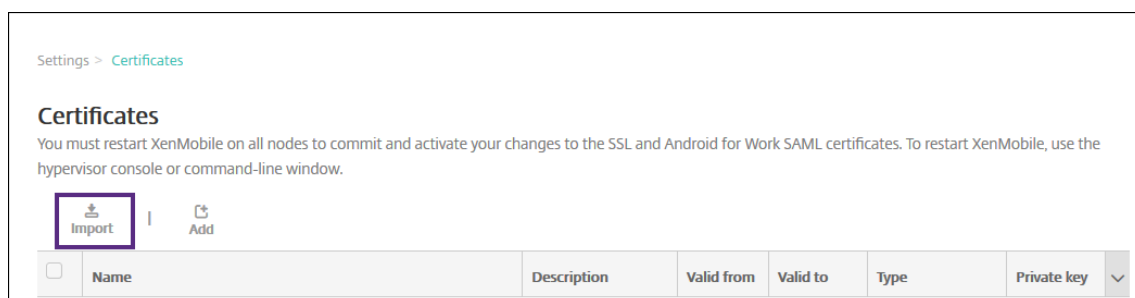
Depois de confirmar o token de associação, você poderá começar a usar o XenMobile para gerenciar dispositivos Android. Importe o certificado P12 gerado na etapa 14. Defina as configurações do servidor do Android Enterprise, ative o logon único (SSO) baseado em SAML e defina pelo menos uma política de dispositivo do Android Enterprise.



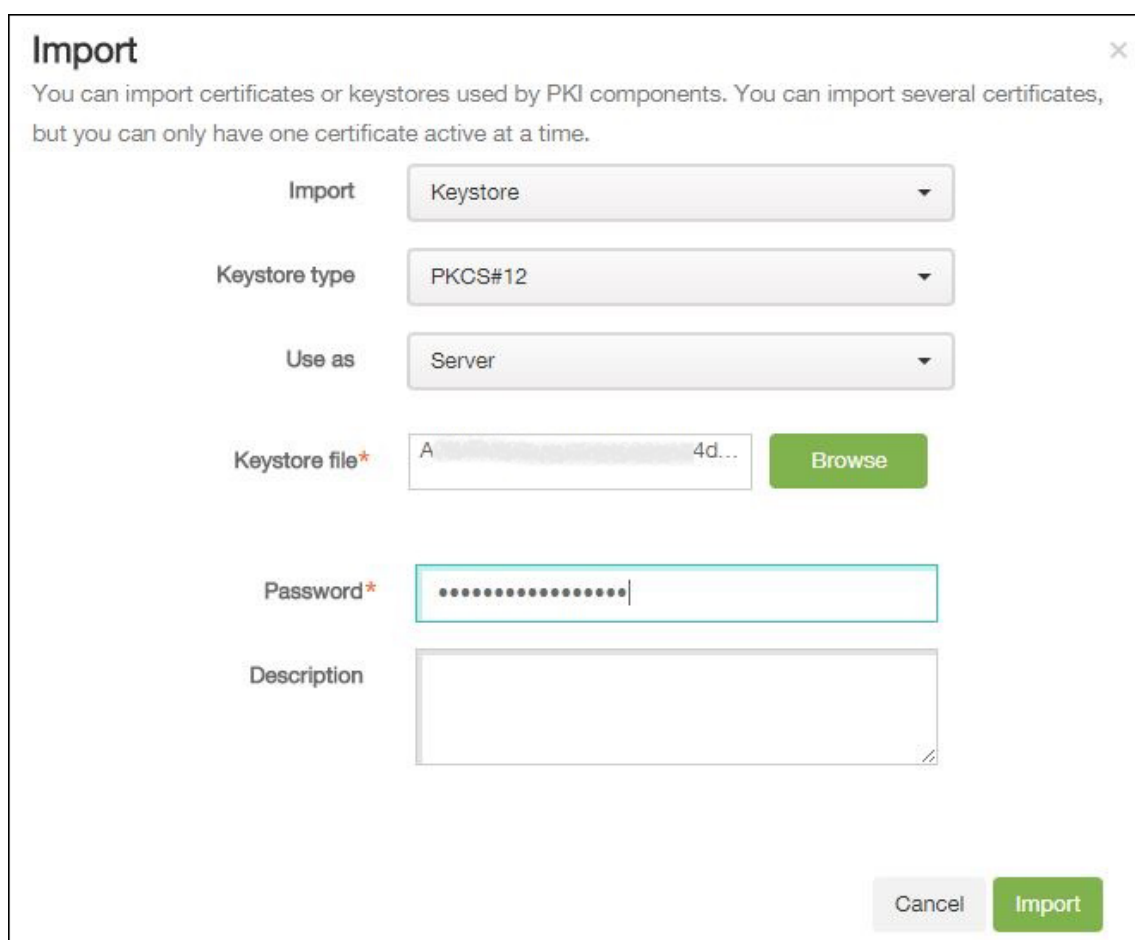
Importe o certificado P12

Siga estas etapas para importar o certificado P12 do Android Enterprise:

1. Faça login no console XenMobile.
2. Clique no ícone de engrenagem no canto superior direito do console para abrir a página **Configurações** e clique em **Certificados**. A página **Certificados** é exibida.



3. Clique em **Importar**. A caixa de diálogo **Importar** é exibida.



Faça as seguintes configurações:

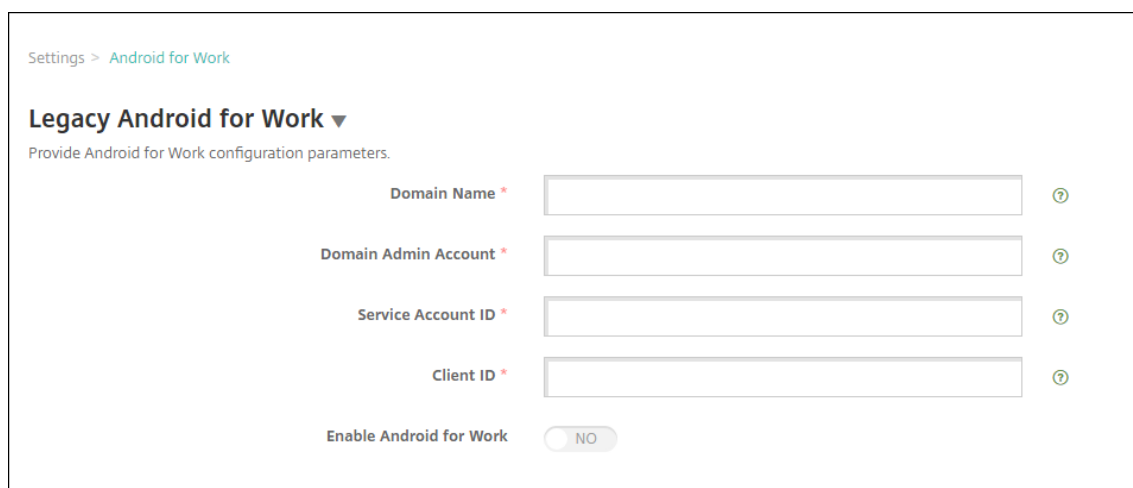
- **Importar:** na lista, clique em **Keystore**.

- **Tipo de keystore:** na lista, clique em **PKCS#12**.
- **Usar como:** na lista, clique em **Servidor**.
- **Arquivo de keystore:** clique em **Procurar** e navegue até o certificado P12.
- **Senha:** digite a senha do keystore.
- **Descrição:** opcionalmente, digite uma descrição do certificado.

4. Clique em **Importar**.

Definir as configurações de servidor do Android Enterprise

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Settings** é exibida.
2. Em **Servidor**, clique em **Android Enterprise**. A página **Android Enterprise** é exibida.



Settings > Android for Work

Legacy Android for Work ▼

Provide Android for Work configuration parameters.

Domain Name * ⓘ

Domain Admin Account * ⓘ

Service Account ID * ⓘ

Client ID * ⓘ

Enable Android for Work NO

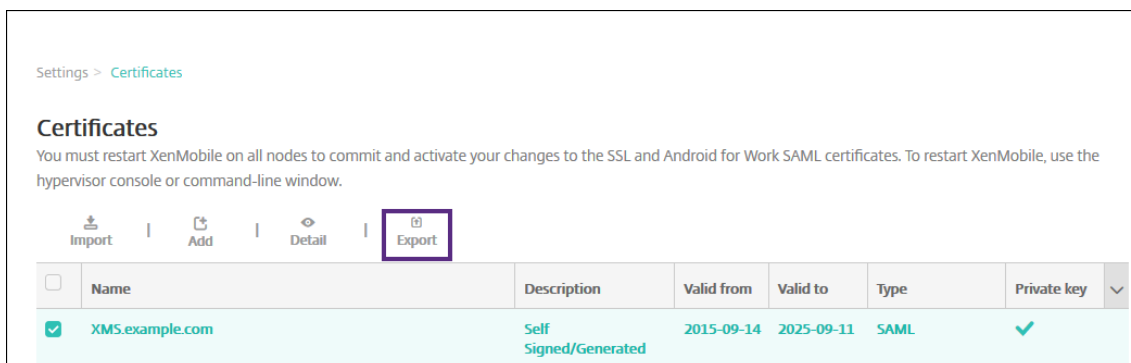
Defina as configurações a seguir e clique em **Salvar**.

- **Nome de domínio:** digite o nome de domínio do Android Enterprise, por exemplo, domínio.com.
- **Conta de administrador de domínio:** digite o nome de usuário do administrador de domínio, por exemplo, a conta de email utilizada no Google Developer Portal.
- **ID da conta de serviço:** digite o ID da sua conta de serviço, por exemplo, o e-mail associado à Conta de serviço do Google (serviceaccountemail@xxxxxxxxx.iam.gserviceaccount.com).
- **ID do cliente:** digite o ID numérico do cliente da sua conta de serviço do Google.
- **Ativar o Android Enterprise:** selecione para ativar ou desativar o Android Enterprise.

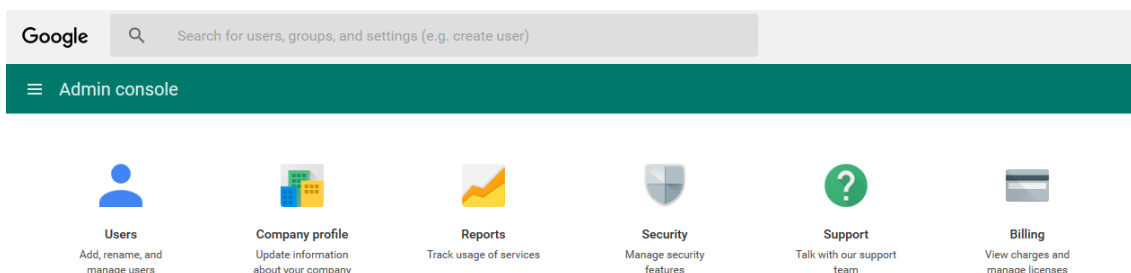
Ativar o logon único baseado em SAML

1. Faça login no console XenMobile.

2. Clique no ícone de engrenagem no canto superior direito do console. A página **Settings** é exibida.
3. Clique em **Certificados**. A página **Certificados** é exibida.



4. Na lista de certificados, clique no certificado SAML.
5. Clique em **Exportar** e salve o certificado no seu computador.
6. Faça login no portal do Google Admin usando as credenciais de administrador do Android Enterprise. Para acessar o portal, consulte [Portal do Google Admin](#).
7. Clique em **Security**.



8. Em **Security**, clique em **Set up single sign-on (SSO)** e faça as seguintes configurações.

^ Set up single sign-on (SSO)

SAML-based Single Sign-On allows you to authenticate accounts for web based applications (like Gmail or Calendar). With SSO, users sign in for one web application, and are automatically signed in for all other Google web apps. For desktop applications (or POP access to Gmail), users must sign in directly with the username and password set up via the Admin console. ?

Setup SSO with third party identity provider

To setup third party as your identity provider, please provide the information below. ?

Sign-in page URL	<input type="text" value="https://example.com/aw/saml/signin"/> <p style="font-size: small; margin-top: 5px;">URL for signing in to your system and Google Apps</p>
Sign-out page URL	<input type="text" value="https://example.com/aw/saml/signout"/> <p style="font-size: small; margin-top: 5px;">URL for redirecting users to when they sign out</p>
Change password URL	<input type="text" value="https://example.com/aw/saml/changepassword"/> <p style="font-size: small; margin-top: 5px;">URL to let users change their password in your system; when defined here, this is shown even when Single Sign-on is not enabled</p>
Verification certificate	<div style="display: flex; gap: 10px;"> <input type="button" value="CHOOSE FILE"/> <input type="button" value="UPLOAD"/> </div> <p style="font-size: small; margin-top: 5px;">The certificate file must contain the public key for Google to verify sign-in requests. ?</p>

Use a domain specific issuer ?

Network masks

Network masks determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network. Use a semicolon to separate the masks. Example: (64.233.187.99/8; 72.14.0.0/16). For ranges, use a dash. Example: (64.233.167-204.99/32). All network masks must end with a CIDR. ?

- **Sign-in page URL:** digite a URL para os usuários que estão fazendo login no seu sistema e no Google Apps. Por exemplo: `https://<Xenmobile-FQDN>/aw/saml/signin`.
- **Sign out page URL:** digite a URL para a qual os usuários são redirecionados quando fazem logoff. Por exemplo: `https://<Xenmobile-FQDN>/aw/saml/signout`.
- **Change password URL:** digite a URL para permitir que os usuários alterem as respectivas senhas no seu sistema. Por exemplo: `https://<Xenmobile-FQDN>/aw/saml/changepassword`. Se este campo é definido, os usuários veem esse prompt, mesmo quando o SSO não está disponível.
- **Verification certificate:** clique em **CHOOSE FILE** e navegue até o certificado SAML exportado do XenMobile.

9. Clique em **SAVE CHANGES**.

Configurar uma política de dispositivo do Android Enterprise

Configure uma política de código secreto para que os usuários tenham que estabelecer um código secreto em seus dispositivos quando se registrarem pela primeira vez.

As etapas básicas para configurar qualquer política de dispositivo são as seguintes.

1. Faça login no console XenMobile.
2. Clique **Configurar** e, em seguida, clique em **Políticas de dispositivo**.
3. Clique em **Adicionar** e, em seguida, na caixa de diálogo **Adicionar uma nova política**, selecione a política que você deseja adicionar. Nesse exemplo, você clica em **Código secreto**.
4. Preencha a página **Informações sobre a política**.
5. Clique em **Android Enterprise** e defina as configurações da política.
6. Atribua a política a um Grupo de Entrega.

Defina as configurações da conta do Android Enterprise

Antes de começar a gerenciar aplicativos Android e políticas em dispositivos, você deverá configurar as informações de domínio e conta do Android Enterprise no XenMobile. Primeiro, conclua as tarefas de instalação do Android Enterprise no Google para configurar um administrador de domínio e obter um ID de conta de serviço e um token de associação.

1. No console da Web XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Em **Servidor**, clique em **Android Enterprise**. A página de configuração do **Android Enterprise** é exibida.

Settings > Android for Work

Legacy Android for Work ▼

Provide Android for Work configuration parameters.

Domain Name * ⓘ

Domain Admin Account * ⓘ

Service Account ID * ⓘ

Client ID * ⓘ

Enable Android for Work NO

1. Na página **Android Enterprise**, faça as seguintes configurações:
 - **Nome de domínio:** digite seu nome de domínio.
 - **Conta de administrador de domínio:** digite o nome do usuário do seu administrador de domínio.
 - **ID de conta de serviço:** digite o seu ID de Conta de Serviço do Google.
 - **ID do cliente:** digite o ID do cliente da sua conta de serviço do Google.
 - **Ativar o Android Enterprise:** selecione se deseja ativar ou não o Android Enterprise.
2. Clique em **Save**.

Configurar o acesso de parceiro do Google Workspace para o XenMobile

Alguns recursos de gerenciamento de ponto de extremidade do Chrome usam APIs de parceiros do Google para se comunicar entre o XenMobile e seu domínio do Google Workspace. Por exemplo, o XenMobile exige as APIs para políticas de dispositivos que gerenciam recursos do Chrome, como o modo de navegação Anônima e o modo Visitante.

Para ativar as APIs de parceiros, você configura seu domínio do Google Workspace no console XenMobile e configura sua conta do Google Workspace.

Configurar seu domínio do Google Workspace (anteriormente G Suite) no XenMobile

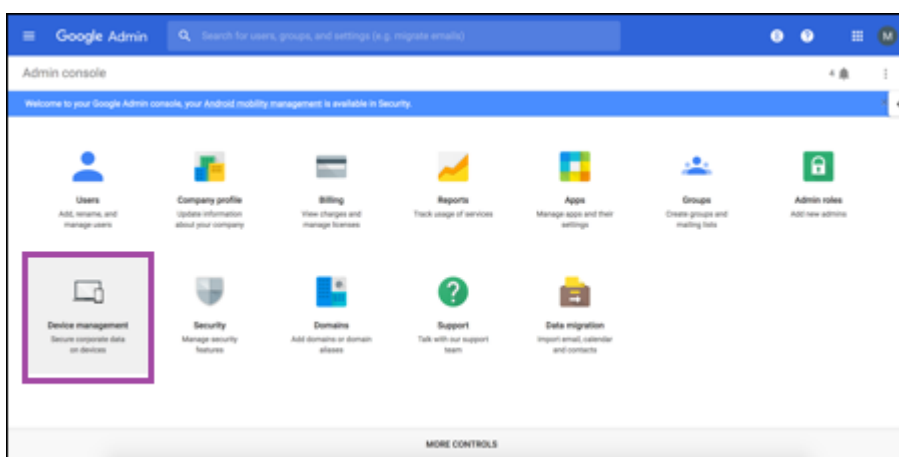
Para permitir que o XenMobile se comunique com as APIs no seu domínio do Google Workspace, acesse **Configurações > Configuração do Google Chrome** e defina as configurações.

- **Domínio do G Suite:** o domínio do Google Workspace que hospeda as APIs necessárias ao XenMobile.
- **Conta de administrador do G Suite:** a conta de administrador do seu domínio do G Suite.

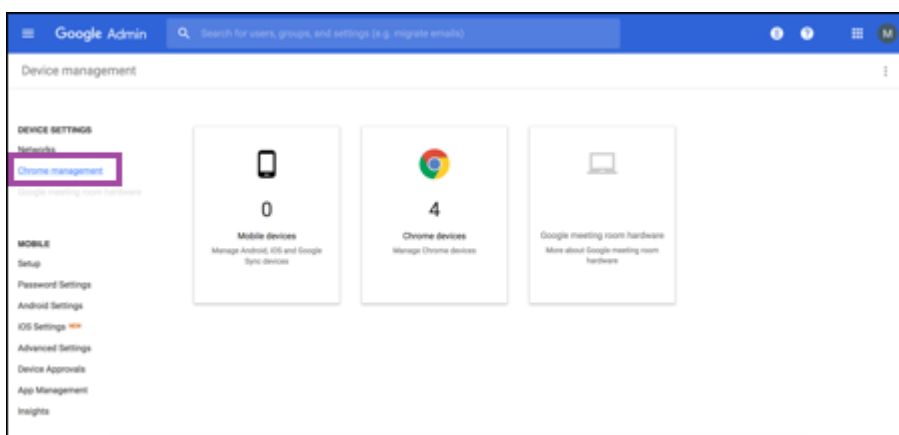
- **ID de cliente do G Suite:** o ID de cliente para a Citrix. Use esse valor para configurar o acesso de parceiros para seu domínio do Google Workspace.
- **ID empresarial do G Suite:** o ID empresarial da sua conta, preenchido a partir da sua conta corporativa do Google.

Ativar o acesso de parceiros para dispositivos e usuários no seu domínio do Google Workspace

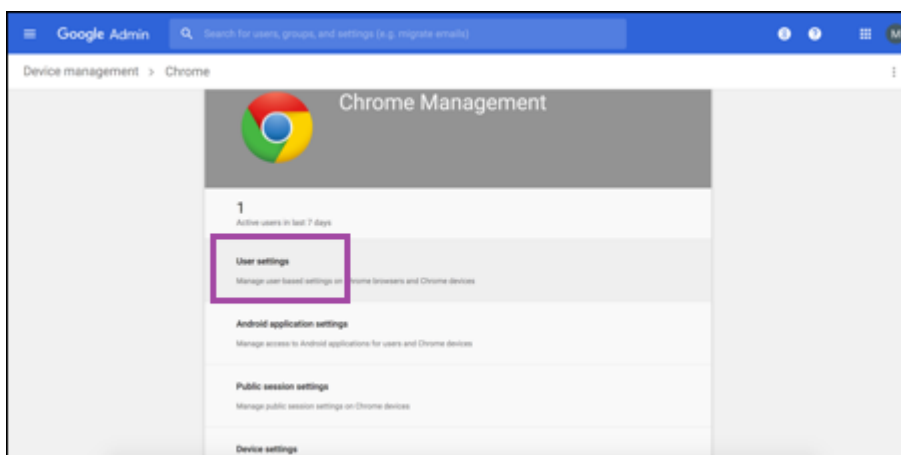
1. Faça login no Admin Console do Google: <https://admin.google.com>
2. Clique em **Gerenciamento de dispositivos**.



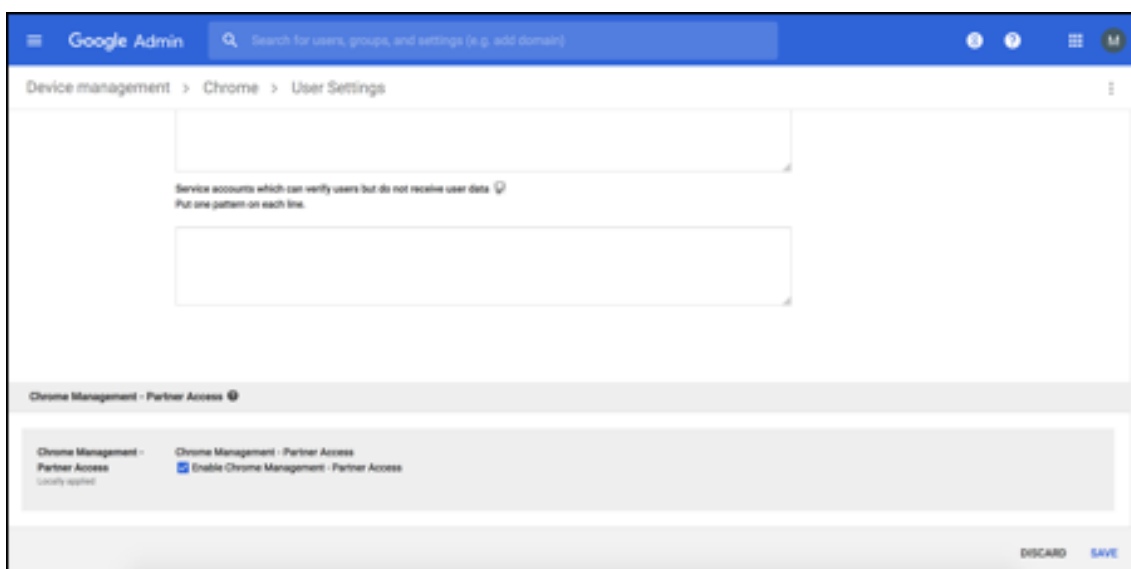
3. Clique em **Gerenciamento do Chrome**.



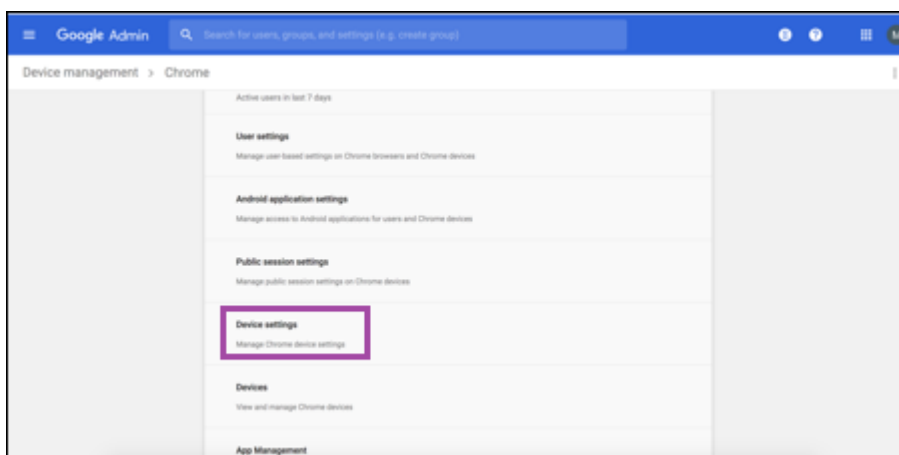
4. Clique em **Configurações do usuário**.



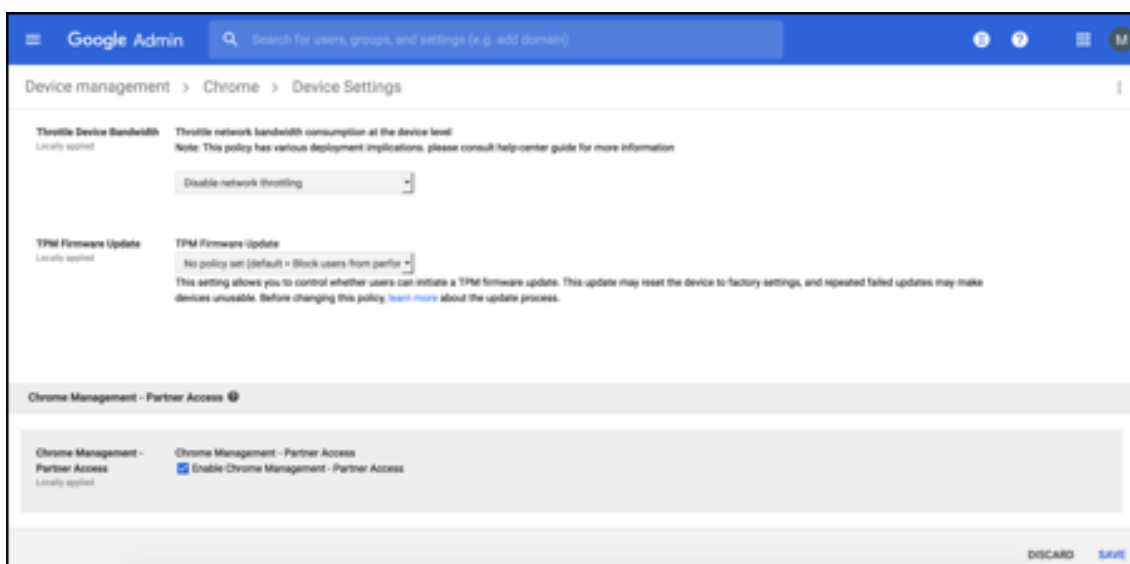
5. Pesquise pelo **Gerenciamento do Chrome - Acesso para parceiros**.



6. Marque a caixa de seleção **Ativar o gerenciamento do Chrome - Acesso para parceiros**.
7. Aceite que você entende e deseja ativar o acesso para parceiros. Clique em **Save**.
8. Na página de gerenciamento do Chrome, clique em **Configurações do dispositivo**.



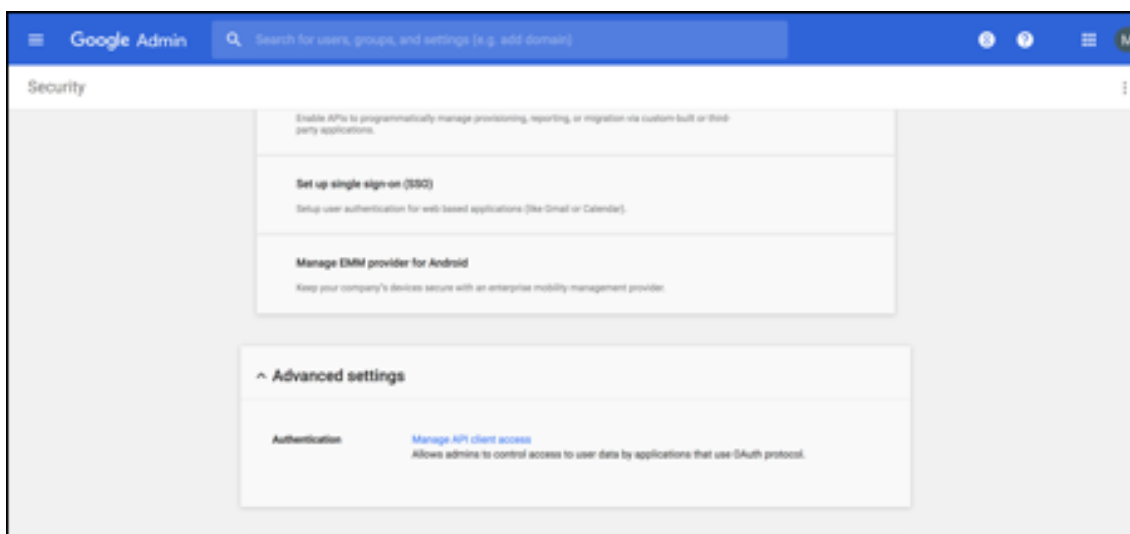
9. Pesquise pelo **Gerenciamento do Chrome - Acesso para parceiros**.



10. Marque a caixa de seleção **Ativar o gerenciamento do Chrome - Acesso para parceiros**.

11. Aceite que você entende e deseja ativar o acesso para parceiros. Clique em **Save**.

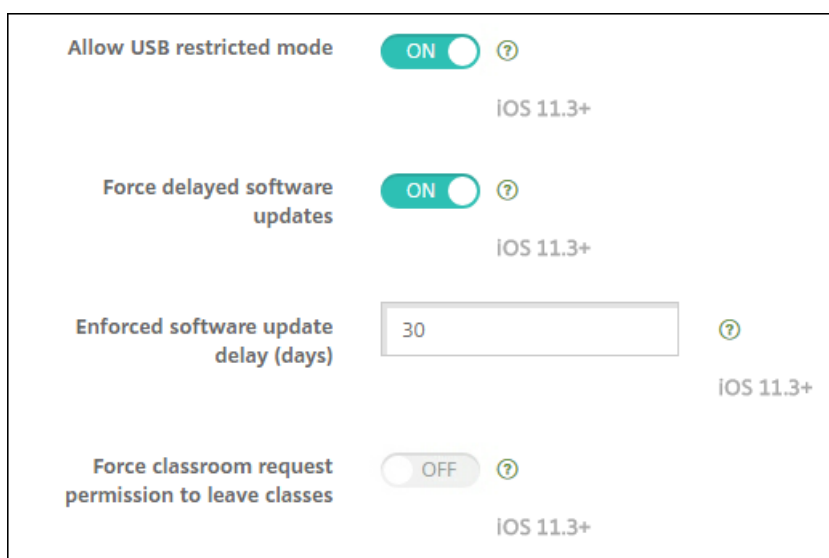
12. Vá para a página **Segurança** e clique em **Configurações avançadas**.



13. Clique em **Gerenciar acesso de cliente de API**.
14. No console XenMobile, acesse **Configurações > Configuração do Google Chrome** e copie o valor do ID do cliente do Google Workspace. Em seguida, retorne à página **Gerenciar acesso de cliente de API** e cole o valor copiado no campo **Nome do cliente**.
15. Em **Um ou mais escopos de API**, adicione a URL: <https://www.googleapis.com/auth/chromedevicemanagementapi>



16. Clique em **Autorizar**.
A mensagem “Suas configurações foram salva” é exibida.



Registrar dispositivos Android Enterprise

Se o processo de inscrição de seu dispositivo exigir que os usuários digitem um nome de usuário ou ID do usuário, o formato aceito depende da forma como o servidor XenMobile está configurado para procurar usuários pelo nome UPN ou pelo nome da conta SAM.

Se o XenMobile Server estiver configurado para procurar usuários por UPN, os usuários devem inserir um UPN no formato:

- *nome de usuário@domínio*

Se o XenMobile Server estiver configurado para procurar usuários por SAM, os usuários devem inserir um SAM em um destes formatos:

- *nome de usuário@domínio*
- *domínio\nome de usuário*

Para determinar para qual tipo de nome de usuário o XenMobile Server está configurado:

1. No console XenMobile Server, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida.
2. Clique em **LDAP** para visualizar a configuração da conexão LDAP.
3. Perto da parte inferior da página, verifique o campo **Pesquisa de usuário por**:
 - Se estiver definido como **userPrincipalName**, o servidor XenMobile estará definido para UPN.
 - Se estiver definido como **sAMAccountName**, o servidor XenMobile estará definido para SAM.

Cancelar o registro de um enterprise do Android Enterprise

O XenMobile agora permite cancelar o registro de um enterprise do Android Enterprise usando o console XenMobile Server e o XenMobile Tools.

Quando você executa essa tarefa, o XenMobile Server abre uma janela pop-up para o XenMobile Tools. Antes de começar, verifique se o XenMobile Server tem permissão para abrir janelas pop-up no navegador que você está usando. Alguns navegadores, como o Google Chrome, exigem que você desabilite o bloqueio de pop-ups e acrescente o endereço do site do XenMobile à lista de permissão de bloqueio de pop-up.

Aviso:

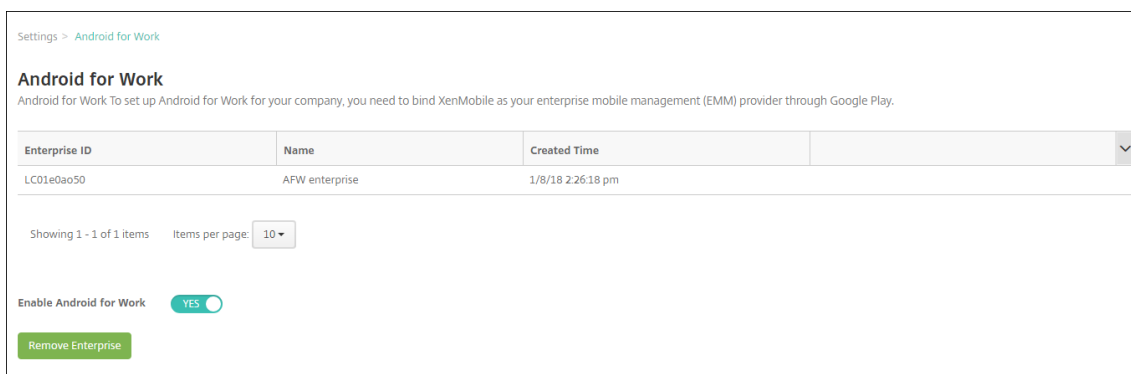
Depois de o registro de um enterprise ser cancelado, os aplicativos Android Enterprise nos dispositivos já registrados por meio dele são redefinidos para os estados padrão. Os dispositivos não serão mais gerenciados pelo Google. Registrá-los novamente em um enterprise do Android Enterprise pode não restaurar a funcionalidade anterior sem configuração adicional.

Depois que o registro do enterprise do Android Enterprise for cancelado:

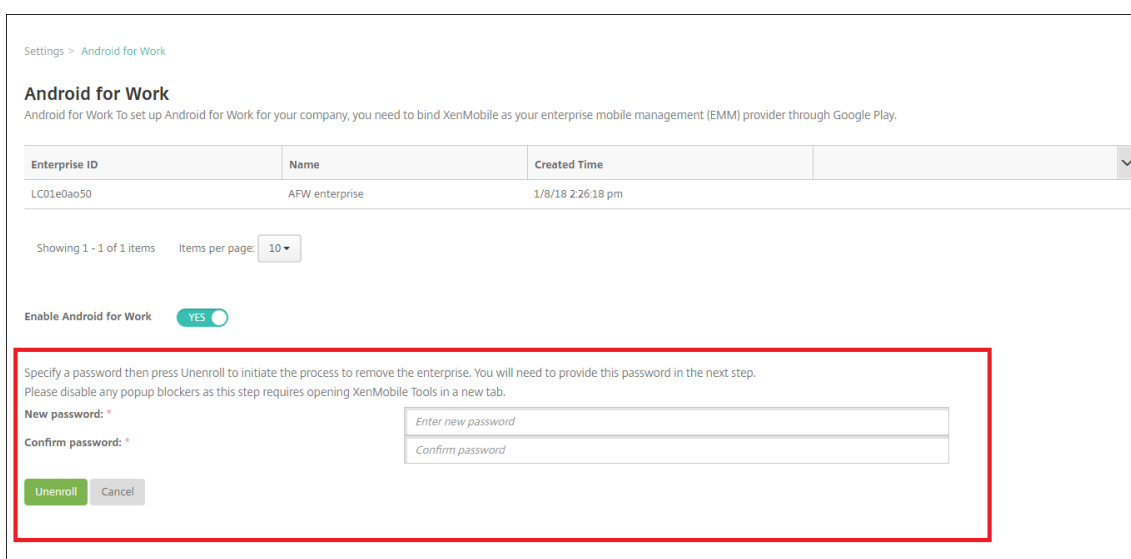
- Dispositivos e usuários registrados pelo Enterprise têm os aplicativos do Android Enterprise redefinidos para o estado padrão. As políticas de Permissões do aplicativo Android Enterprise e de Restrições de aplicativo Android Enterprise aplicadas anteriormente não afetam mais.
- Os dispositivos registrados por meio do Enterprise são gerenciados pelo XenMobile, mas não são gerenciados pela perspectiva do Google. Não é possível adicionar novos aplicativos do Android Enterprise. Não se aplica nenhuma política de Permissões do aplicativo Android Enterprise ou de Restrições de aplicativo Android Enterprise. Outras políticas, como Agendamento, Senha e Restrições, ainda podem ser aplicadas a esses dispositivos.
- Se você tentar registrar dispositivos no Android Enterprise, eles serão registrados como dispositivos Android, não como dispositivos Android Enterprise.

Para cancelar o registro de um enterprise do Android Enterprise:

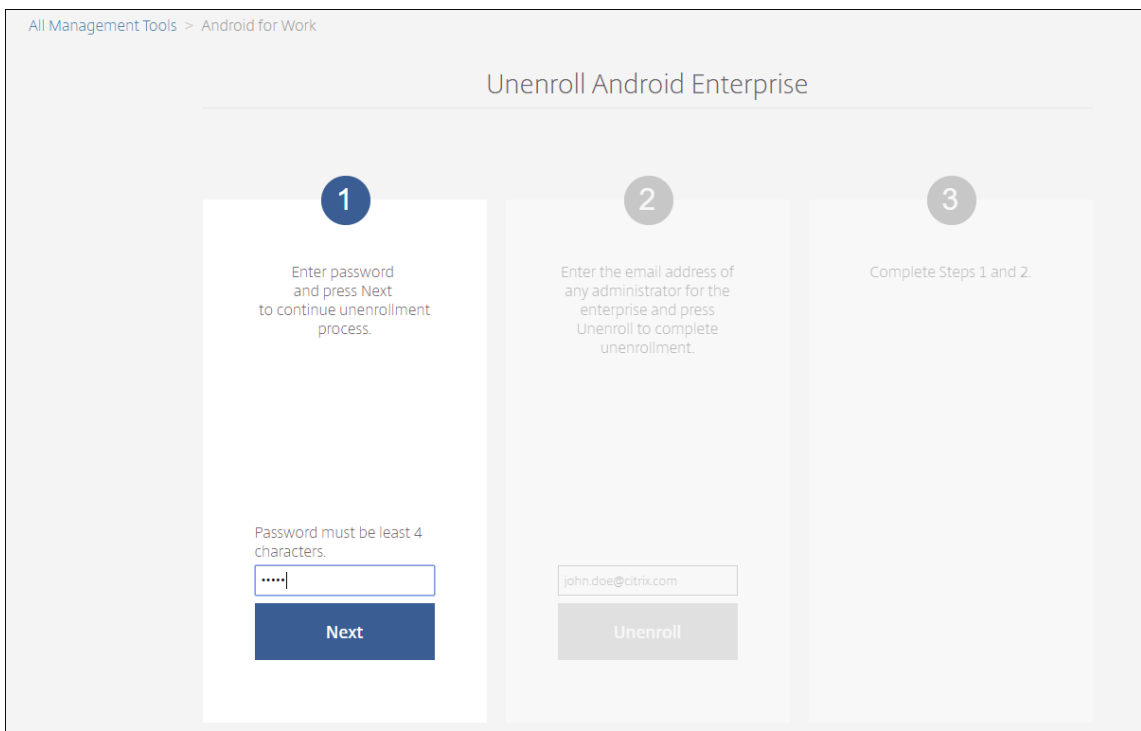
1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página Settings é exibida.
2. Na página Settings, clique em **Android Enterprise**.
3. Clique em **Remover Enterprise**.



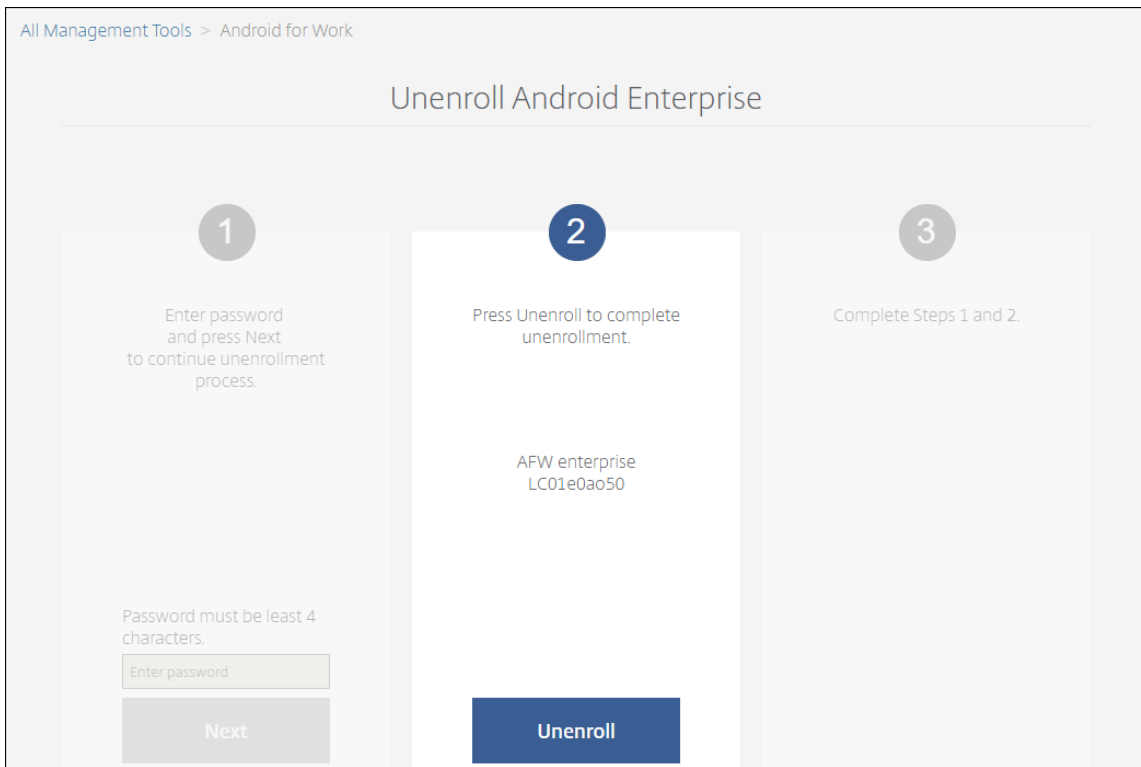
4. Especifique uma senha. Você precisará dela na próxima etapa para concluir o cancelamento do registro. Em seguida, clique em **Cancelar registro**.



5. Quando a página do XenMobile Tools for aberta, insira a senha que você criou na etapa anterior.



6. Clique em **Cancelar registro**.



Provisionamento de dispositivos totalmente gerenciados no Android Enterprise

Somente os dispositivos da empresa podem ser totalmente gerenciados para Android Enterprise. Em dispositivos totalmente gerenciados, todo o dispositivo, não apenas o perfil de trabalho, é controlado pela empresa ou organização. Dispositivos totalmente gerenciados também são conhecidos como dispositivos de trabalho gerenciados.

O XenMobile é compatível com estes métodos de registro para dispositivos totalmente gerenciados:

- **afw#xenmobile:** com esse método de registro, o usuário insere os caracteres “afw#xenmobile” ao configurar o dispositivo. Esse token identifica o dispositivo como gerenciado pelo XenMobile e baixa o Secure Hub.
- **Código QR:** o provisionamento de código QR é uma maneira fácil de provisionar uma frota distribuída de dispositivos que não são compatíveis com NFC, como tablets. O método de registro de código QR pode ser usado em dispositivos de frota que tenham sido redefinidos às suas configurações de fábrica. O método de registro de código QR instala e configura dispositivos totalmente gerenciados digitalizando um código QR no Assistente de instalação.
- **Aumento da comunicação a curta distância (NFC):** o método de registro de aumento de NFC pode ser usado em dispositivos de frota que tenham sido redefinidos às suas configurações de fábrica. Um aumento de NFC transfere dados entre dois dispositivos usando comunicação a curta distância. Bluetooth, Wi-Fi e outros meios de comunicação estão desativados em um dispositivo que sofreu uma redefinição de fábrica. O NFC é o único protocolo de comunicação que o dispositivo pode usar nesse estado.

afw#xenmobile

O método de registro é usado após ligar um novo dispositivo ou dispositivos com a configuração inicial de fábrica redefinida. Os usuários digitam “afw#xenmobile” quando solicitados a inserir uma conta do Google. Essa ação baixa e instala o Secure Hub. Os usuários seguem os prompts de configuração do Secure Hub para concluir o registro.

Esse método de registro é recomendado para a maioria dos clientes, porque a versão mais recente do Secure Hub é baixada da loja Google Play. Ao contrário de outros métodos de registro, você não fornece o Secure Hub para download no servidor XenMobile.

Pré-requisitos:

- Suportado em todos os dispositivos Android com Android 5.0 e superior.

Código QR

Para registrar um dispositivo no modo de dispositivo usando um código QR, você pode gerar um código QR criando um JSON e convertendo o JSON em um código QR. A câmera do dispositivo escaneia o código QR para registrar o dispositivo.

Pré-requisitos:

- Suportado em todos os dispositivos Android com Android 7.0 e superior.

Criar um código QR de um JSON

Crie um JSON com os seguintes campos.

Estes campos são obrigatórios:

Chave: `android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME`

Valor: `com.zenprise/com.zenprise.configuration.AdminFunction`

Chave: `android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM`

Valor: `qn7oZUtheu3JBAinzZRrjCQv6LOO6LL1OjcxT3-yKM`

Chave: `android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION`

Valor: `https://path/to/securehub.apk`

Nota:

Se o Secure Hub for carregado para o Citrix XenMobile Server como um aplicativo empresarial, ele pode ser baixado de `https://<fqdn>:4443/*instanceName*/worxhome.apk`. O caminho para o Secure Hub APK deve ser acessível através da conexão Wi-Fi em que o dispositivo se conecta durante o provisionamento.

Estes campos são opcionais:

- **android.app.extra.PROVISIONING_LOCALE:** insira os códigos de idioma e país.
Os códigos de idioma são códigos de idioma ISO com duas letras minúsculas (por exemplo, en), conforme definido pela [ISO 639-1](#). Os códigos de país são códigos de país ISO com duas letras maiúsculas (por exemplo, US), conforme definido pela [ISO 3166-1](#). Por exemplo, insira `_US` para o inglês falado nos Estados Unidos.
- **android.app.extra.PROVISIONING_TIME_ZONE:** o fuso horário em que o dispositivo é executado.
Insira um [nome Olson da área/localização do formulário](#). Por exemplo, `America/Los_Angeles` para o horário do Pacífico. Se você não inserir um, o fuso horário será preenchido automaticamente.
- **android.app.extra.PROVISIONING_LOCAL_TIME:** tempo em milissegundos desde a época (Epoch).
A época do Unix (ou hora do Unix, hora do POSIX ou carimbo de data/hora do Unix) é o número de segundos decorridos desde 1º de janeiro de 1970 (meia-noite UTC/GMT). O tempo não inclui segundos bissextos (in ISO 8601: 1970-01-01T00:00:00Z).

- Suportado em todos os dispositivos Android com Android 5.0, Android 5.1, Android 6.0 e superior.
- Um XenMobile Server versão 10.4 que está ativado para o Android Enterprise.
- Um dispositivo novo ou com redefinição de fábrica, provisionado para o Android Enterprise como um dispositivo totalmente gerenciado. Você pode encontrar as etapas para concluir esse pré-requisito neste artigo.
- Outro dispositivo com recursos NFC executando a Provisioning Tool configurada. A Provisioning Tool está disponível no Secure Hub 10.4 ou na [página de downloads da Citrix](#).

Cada dispositivo pode ter somente um perfil do Android Enterprise, gerenciado por um aplicativo de gerenciamento de mobilidade empresarial (EMM). No XenMobile, o Secure Hub é o aplicativo EMM. Somente um perfil é permitido em cada dispositivo. A tentativa de adicionar um segundo aplicativo EMM remove o primeiro aplicativo EMM.

Dados transferidos através do aumento de NFC

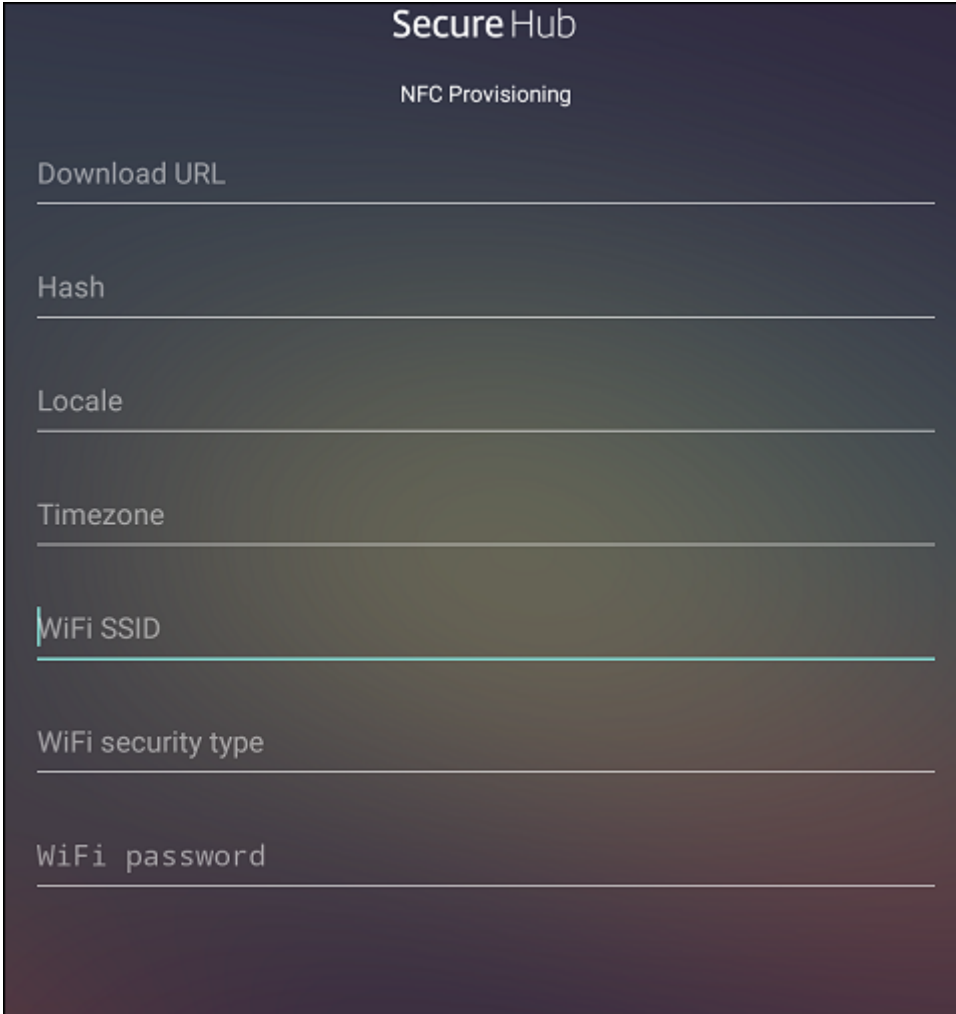
Provisionar um dispositivo com redefinição de fábrica requer que você envie os seguintes dados por meio de um NFC bump para inicializar o Android Enterprise:

- O nome do pacote do aplicativo do provedor EMM que atua como o proprietário do dispositivo (neste caso, o Secure Hub).
- A localização de Intranet/Internet do qual o dispositivo pode baixar o aplicativo do provedor EMM.
- O hash SHA1 do aplicativo do provedor EMM para verificar se o download é bem-sucedido.
- Os detalhes da conexão WiFi para que um dispositivo com redefinição de fábrica possa se conectar e baixar o aplicativo do provedor EMM. Nota: No momento, o Android não é compatível com WiFi 802.1x para esta etapa.
- O fuso horário do dispositivo (opcional).
- A localização geográfica do dispositivo (opcional).

Quando os dois dispositivos são aumentados, os dados da Provisioning Tool são enviados para o dispositivo com redefinição de fábrica. Esses dados são usados para baixar o Secure Hub com as configurações do administrador. Se você não inserir os valores de localização e fuso horário, o Android os configura automaticamente no novo dispositivo.

Configuração da XenMobile Provisioning Tool

Antes de realizar um aumento de NFC, você deve configurar a Provisioning Tool. Em seguida, essa configuração é transferida para o dispositivo com redefinição de fábrica durante o aumento de NFC.



Secure Hub

NFC Provisioning

Download URL

Hash

Locale

Timezone

WiFi SSID

WiFi security type

WiFi password

Você pode digitar dados nos campos obrigatórios ou preenchê-los usando um arquivo de texto. As etapas no procedimento a seguir descrevem como configurar o arquivo de texto e contém descrições para cada campo. O aplicativo não salva as informações depois que as digitar, portanto, convém criar um arquivo de texto para manter as informações para uso futuro.

Para configurar a Provisioning Tool usando um arquivo de texto

Dê ao arquivo o nome `nfcp provisioning.txt` e coloque-o na pasta `/sdcard/` no cartão SD do dispositivo. Em seguida, o aplicativo poderá ler o arquivo de texto e preencher os valores.

O arquivo de texto deve conter os seguintes dados:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=<
download_location>
```

Essa linha é o local da intranet/internet do aplicativo do provedor EMM. Depois que o dispositivo com redefinição de fábrica se conectar a Wi-Fi em seguida ao aumento de NFC, o dispositivo deve ter

acesso a esse local para fazer o download. A URL é uma URL regular, sem necessidade de formatação especial.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=<SHA1 hash>
```

Essa linha é a soma de verificação do aplicativo do provedor EMM. Essa soma de verificação é usada para verificar se o download foi bem-sucedido. As etapas para obter a soma de verificação são discutidas neste artigo.

```
android.app.extra.PROVISIONING_WIFI_SSID=<wifi ssid>
```

Esse é o SSID de Wi-Fi conectado do dispositivo no qual a Provisioning Tool está em execução.

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=<wifi security type>
```

Os valores suportados são WEP e WPA2. Se o Wi-Fi for desprotegido, esse campo deverá estar vazio.

```
android.app.extra.PROVISIONING_WIFI_PASSWORD=<wifi password>
```

Se o Wi-Fi for desprotegido, esse campo deverá estar vazio.

```
android.app.extra.PROVISIONING_LOCALE=<locale>
```

Insira os códigos de idioma e país. Os códigos de idioma são códigos de idioma ISO com duas letras minúsculas (por exemplo, en), conforme definido pela [ISO 639-1](#). Os códigos de país são códigos de país ISO com duas letras maiúsculas (por exemplo, US), conforme definido pela [ISO 3166-1](#). Por exemplo, digite en_US para o inglês falado nos Estados Unidos. Se você não digitar nenhum código, o país e o idioma serão preenchidos automaticamente.

```
android.app.extra.PROVISIONING_TIME_ZONE=<timezone>
```

O fuso horário no qual o dispositivo está em execução. Insira um [nome Olson da área/localização do formulário](#). Por exemplo, America/Los_Angeles para o horário do Pacífico. Se você não inserir nenhum nome, o fuso horário será preenchido automaticamente.

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_NAME=<package name>
```

Isso não é necessário, pois o valor é inserido em código fixo no aplicativo, como o Secure Hub. Ele é mencionado aqui somente por uma questão de conclusão.

Se houver um Wi-Fi protegido por WPA2, um arquivo nfcprovisioning.txt preenchido terá a seguinte aparência:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk
```

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFk4Crh\nu003d
```

```
android.app.extra.PROVISIONING_WIFI_SSID=Protected_WiFi_Name
```

```
android.app.extra.PROVISIONING_WIFI_SECURITY_TYPE=WPA2
```



```
android.app.extra.PROVISIONING_WIFI_PASSWORD=wifiPasswordHere
```

```
android.app.extra.PROVISIONING_LOCALE=en_US
```

```
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Se houver uma Wi-Fi desprotegida, um arquivo nfcprovisioning.txt preenchido terá a seguinte aparência:

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION=https://www.somepublicurlhere.com/path/to/securehub.apk
```

```
android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_CHECKSUM=ga50TwdCmfdJ72LGRFkke4Crh\n\u003d
```

```
android.app.extra.PROVISIONING_WIFI_SSID=Unprotected_WiFi_Name
```

```
android.app.extra.PROVISIONING_LOCALE=en_US
```

```
android.app.extra.PROVISIONING_TIME_ZONE=America/Los_Angeles
```

Para obter a soma de verificação do Secure Hub

Para obter a soma de verificação de qualquer aplicativo, adicione o aplicativo como um aplicativo empresarial.

1. No console XenMobile, clique em **Configurar > Aplicativos** e em **Adicionar**.

A janela **Adicionar aplicativos** é exibida.

2. Clique em **Empresarial**.

A página **Informações do Aplicativo** é exibida.

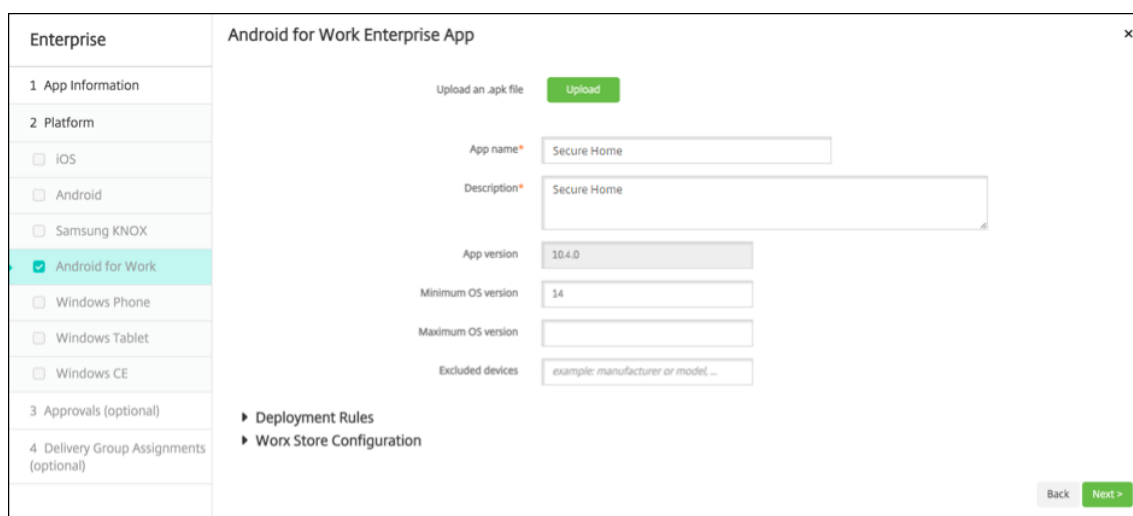
3. Selecione a configuração a seguir e clique em **Avançar**.

A página **Aplicativo enterprise do Android Enterprise** é exibida.

The screenshot shows the 'App Information' configuration page in the XenMobile console. The sidebar on the left indicates the current step is '1. App Information'. Under the 'Platform' section, the 'Android for Work' option is selected, highlighted with a red box. The main form area contains the following fields: 'Name*' with the value 'Secure Home' (also highlighted with a red box), 'Description' (empty), and 'App category' set to 'All Selected'. A red arrow points to the 'Next >' button at the bottom right of the form.

4. Forneça o caminho até o arquivo .apk e clique em **Avançar** para carregá-lo.

Depois que a instalação for concluída, serão exibidos os detalhes do pacote carregado.



5. Clique em **Avançar** para abrir uma página para baixar o arquivo JSON, que você usará para carregar no Google Play. Para o Secure Hub, não é necessário carregar para Google Play, mas você precisa do arquivo JSON para ler o valor SHA1 dele.

Um arquivo JSON típico tem esta aparência:

6. Copie o **valor file_sha1_base64** e use-o no campo **Hash** na Provisioning Tool.

Nota:

O hash deve ser seguro para URLs.

- Converta os símbolos + para -
- Converta os símbolos / para _
- Substitua o trailing \u003d por =

Se você armazenar o hash no arquivo nfcprovisioning.txt no cartão SD do dispositivo, o aplicativo faz a conversão de segurança. No entanto, se você optar por digitar o hash manualmente, será sua responsabilidade garantir a segurança da URL.

Bibliotecas usadas

A Provisioning Tool usa as seguintes bibliotecas no seu código-fonte:

- Biblioteca v7 appcompat, Biblioteca de suporte ao design e biblioteca de paletas v7 do Google sob licença Apache 2.0

Para obter informações, consulte o [Guia de Recursos da Biblioteca de Suporte](#).

- [Butter Knife](#) de Jake Wharton sob a licença Apache 2.0

Provisionar dispositivo de perfil de trabalho no Android Enterprise

Em dispositivos de perfil de trabalho no Android Enterprise, você separa com segurança as áreas corporativa e pessoal em um dispositivo. Por exemplo, dispositivos BYOD podem ser dispositivos de perfil de trabalho. A experiência de registro de dispositivos de perfil de trabalho é semelhante ao registro do Android no XenMobile. Os usuários fazem o download do Secure Hub a partir do Google Play e registram seus dispositivos.

Por padrão, as configurações de Depuração de USB e Fontes desconhecidas são desativadas em um dispositivo quando ele é registrado no Android Enterprise como um dispositivo de perfil de trabalho.

Dica:

Quando for registrar dispositivos no Android Enterprise como dispositivos de perfil de trabalho, sempre vá para o Google Play. A partir dali, habilite o Secure Hub para aparecer no perfil pessoal do usuário.

iOS

April 26, 2021

Para gerenciar dispositivos iOS no XenMobile Server, configure um certificado de serviço de Notificação por Push (APNs) da Apple. Para obter informações, consulte [Certificados APNs](#).

Os perfis de registro determinam se os dispositivos iOS se registram ou não no MDM+MAM, com uma opção para que os usuários optem por não receber MDM. O XenMobile Server suporta os seguintes tipos de autenticação para dispositivos iOS no MDM+MAM. Para obter informações, consulte os artigos em [Certificados e autenticação](#).

- Domínio
- Domínio mais token de segurança
- Certificado de cliente
- Certificado de cliente mais domínio

Requisitos para certificados confiáveis no iOS 13:

A Apple tem novos requisitos para certificados de servidor TLS. Verifique se todos os certificados seguem os novos requisitos da Apple. Consulte a publicação da Apple, <https://support.apple.com/en-us/HT210176>. Para obter ajuda com o gerenciamento de certificados, consulte [Carregando certificados no XenMobile Server](#).

Para obter os sistemas operacionais compatíveis, consulte [Sistemas operacionais compatíveis de dispositivos](#).

Compatibilidade com iOS 14

O XenMobile Server e os aplicativos móveis Citrix são compatíveis com o iOS 14, mas atualmente não são compatíveis com os novos recursos do iOS 14.

Para dispositivos iOS supervisionados, você pode adiar atualizações de software por até 90 dias. Na política de dispositivo Restrições para iOS, use estas configurações:

- **Forçar atualizações de software atrasadas**
- **Atraso forçado de atualização de software**

Consulte [Configurações de iOS](#). Essas configurações não estão disponíveis para dispositivos no modo de registro de usuário ou no modo não supervisionado (MDM completo).

Nomes de host da Apple que devem permanecer abertos

Alguns nomes de host da Apple devem permanecer abertos para garantir o funcionamento correto do iOS, macOS e Apple App Store. Bloquear esses nomes de host pode afetar a instalação, atualização e operação adequada do iOS, aplicativos iOS, operação de MDM e registro de dispositivos e aplicativos. Para obter mais informações, consulte <https://support.apple.com/en-us/HT201999>.

Métodos de registro suportados

Você especifica como gerenciar dispositivos iOS em perfis de registro. Você pode escolher o registro do dispositivo ou o registro não MDM.

Para definir as configurações de registro para dispositivos iOS, vá para **Configurar > Perfis de registro > iOS**.

Enrollment Profile	Enrollment Configuration
1 Enrollment Info	Specify device management settings for this enrollment profile.
2 Platforms	Device management ⓘ
Android	Management <input checked="" type="radio"/> Device enrollment ⓘ <input type="radio"/> Do not manage devices ⓘ
iOS	Application management ⓘ
3 Assignment (optional)	Citrix MAM <input checked="" type="checkbox"/> ⓘ
	User consent
	Allow users to decline device management <input checked="" type="checkbox"/> ⓘ

A tabela a seguir lista os métodos de registro que o XenMobile Server suporta para dispositivos iOS:

Método	Compatível
Programa de implantação da Apple	Sim
Apple School Manager	Sim
Apple Configurator	Sim
Registro manual	Sim
Convites para registro	Sim

A Apple possui programas de registro de dispositivos para contas de negócios e educação. Para contas de negócios, você se inscreve no Programa de Implantação da Apple para usar o Programa de Implantação da Apple para cadastro e gerenciamento de dispositivos no XenMobile Server. Esse programa é para dispositivos iOS e macOS. Consulte [Implantar dispositivos através do Programa de implantação da Apple](#).

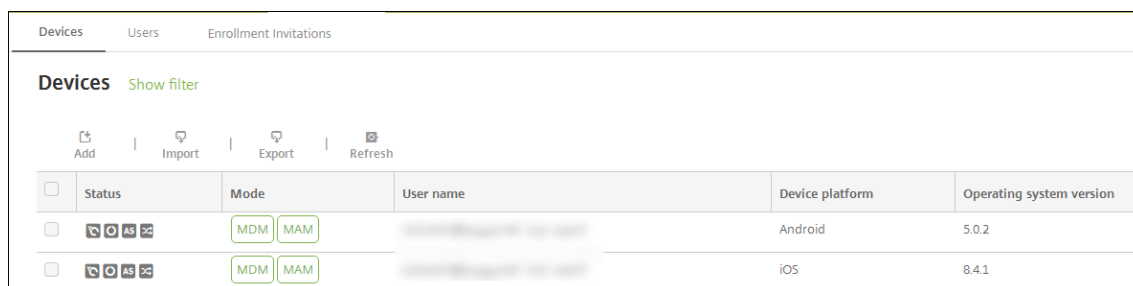
Para contas de educação, você cria uma conta do Apple School Manager. O Apple School Manager unifica o Programa de Implantação e a compra por volume. O Apple School Manager é um tipo de Programa de Implantação do Apple Educação. Consulte [Integração com os recursos do Apple Educação](#).

Você pode usar o Programa de Implantação da Apple para registrar em massa dispositivos iOS e macOS. Você pode comprar esses dispositivos diretamente da Apple, de um Revendedor Autorizado Apple participante ou de uma operadora. Independentemente de comprar dispositivos iOS diretamente da Apple, você pode usar o Apple Configurator para registrar os dispositivos. Consulte [Registro em massa de dispositivos Apple](#).

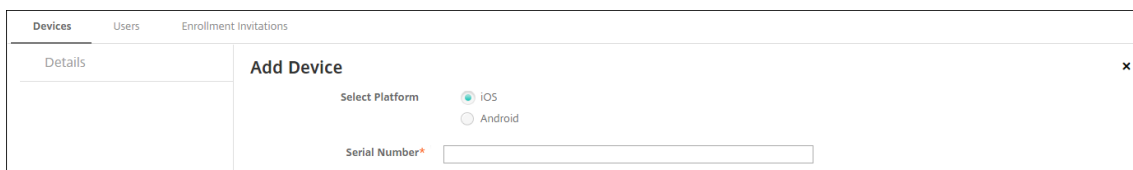
Adicionar um dispositivo iOS manualmente

Se pretender adicionar um dispositivo iOS manualmente, para fins de teste, por exemplo, siga estes passos.

1. No console XenMobile Server, clique em **Gerenciar > Dispositivos**. A página **Dispositivos** é exibida.



2. Clique em **Adicionar**. A página **Adicionar dispositivo** é exibida.



The screenshot shows a web interface with a navigation bar at the top containing 'Devices', 'Users', and 'Enrollment Invitations'. Below the navigation bar, there is a 'Details' section on the left and a main content area titled 'Add Device'. In the 'Add Device' section, there is a 'Select Platform' label followed by two radio buttons: 'iOS' (which is selected) and 'Android'. Below the radio buttons is a text input field labeled 'Serial Number' with a red asterisk to its left, indicating it is a required field.

3. Defina estas configurações:

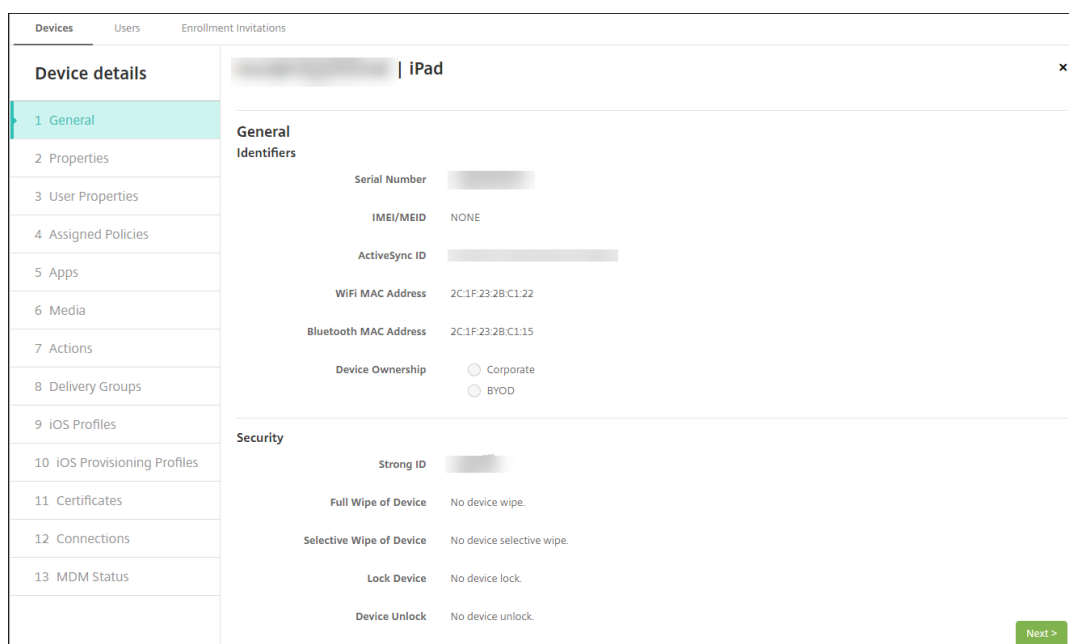
- **Selecionar plataforma:** clique em **iOS**.
- **Número de série:** digite o número de série do dispositivo.

4. Clique em **Adicionar**. A tabela **Dispositivos** é exibida com o dispositivo adicionado à parte inferior da lista. Para exibir e confirmar os detalhes do dispositivo, escolha o dispositivo que você adicionou e, no menu exibido, clique em **Editar**.

Nota:

quando você marca a caixa de seleção ao lado de um dispositivo, o menu de opções é exibido acima da lista de dispositivos. Quando você clica em qualquer outro lugar da lista, o menu de opções é exibido no lado direito da listagem.

- LDAP configurado
- Se estiver usando grupos locais e usuários locais:
 - Um ou mais grupos locais.
 - Usuários locais atribuídos a grupos locais.
 - Grupos de entrega são associados a grupos locais.
- Se estiver usando o Active Directory:
 - Grupos de entrega são associados a grupos do Active Directory.



5. A página **Geral** lista **identificadores** de dispositivo, como o número de série e outras informações para o tipo de plataforma. Para **Propriedade do dispositivo**, selecione **Corporativo** ou **BYOD**.

A página **Geral** também lista propriedades de **segurança**, como ID forte, Bloquear dispositivo, Ignorar bloqueio de ativação e outras informações, para o tipo de plataforma. O campo de **apagamento completo do dispositivo** inclui o código PIN do usuário. O usuário deve digitar o código depois que o dispositivo for apagado. Se o usuário esquecer o código, você pode procurá-lo aqui.

6. A página **Propriedades** lista as propriedades de dispositivo que o XenMobile Server provisionará. Esta lista mostra as propriedades de dispositivo incluídas no arquivo de provisionamento usado para adicionar o dispositivo. Para adicionar uma propriedade, clique em **Adicionar** e, em seguida, selecione uma propriedade na lista. Para obter os valores válidos para cada propriedade, consulte o PDF [Nomes de propriedade do dispositivo e os valores](#).

Quando você adicionar uma propriedade, ela inicialmente aparece na categoria em que você adicionou. Depois de clicar em **Avançar** e voltar para a página **Propriedades**, a propriedade aparece na lista apropriada.

Para excluir uma propriedade, passe o mouse sobre a listagem e clique no **X** à direita. O XenMobile Server exclui o item imediatamente.

7. As seções restantes de **Detalhes do dispositivo** contêm informações resumidas do dispositivo.
 - **Propriedades do usuário:** exibe funções RBAC, associações de grupo, contas de compra por volume e propriedades do usuário. Você pode desativar uma conta de compra por volume nesta página.

- **Políticas atribuídas:** exibe o número de políticas atribuídas, incluindo o número de políticas implantadas, pendentes e com falha. Fornece o nome da política, tipo e últimas informações de implantação de cada política.
- **Aplicativos:** exibe, para o último inventário, o número de implementações de aplicativo instaladas, pendentes e com falha. Fornece o nome do aplicativo, identificador, tipo e outras informações. Para obter uma descrição das chaves de inventário do iOS e do macOS, como **HasUpdateAvailable**, consulte [Protocolo MDM \(Gerenciamento de dispositivo móvel\)](#).
- **Mídia:** exibe, para o último inventário, o número de implementações de mídia implantadas, pendentes e com falha.
- **Ações:** exibe o número de ações implantadas, pendentes e com falha. Fornece o nome da ação e a hora da última implantação.
- **Grupos de entrega:** exibe o número de grupos de entrega bem-sucedidos, pendentes e com falha. Para cada implantação fornece o tempo nome e a implantação do grupo de entrega. Selecione um grupo de entrega para exibir informações mais detalhadas, incluindo status, ação e canal ou usuário.
- **Perfis de iOS:** exibe o último inventário de perfil de iOS, incluindo nome, tipo, organização e descrição.
- **Perfis de provisionamento do iOS:** exibe informações de perfil de provisionamento de distribuição empresarial, como o UUID, a data de expiração e o status gerenciado.
- **Certificados:** exibe, para certificados válidos, expirados ou revogados, informações como o tipo, provedor, emissor, número de série e o número de dias restantes antes da expiração.
- **Conexões:** exibe o status da primeira conexão e o status da última conexão. Fornece para cada conexão, o nome do usuário, penúltimo (próxima ao último) tempo de autenticação e última vez de autenticação.
- **Status de MDM:** exibe informações como o status do MDM, o último envio por push e a hora da última resposta do dispositivo.

Configurar políticas de dispositivo iOS

Use estas políticas para configurar como o XenMobile Server interage com dispositivos que executam o iOS. Esta tabela lista todas as políticas de dispositivo disponíveis para dispositivos iOS.

Espelhamento de AirPlay	AirPrint	APN
Acesso aos aplicativos	Atributos de aplicativo	Configuração do aplicativo
Inventário de aplicativos	Bloqueio de aplicativo	Uso de rede de aplicativos

Desinstalação de aplicativo	Notificações de aplicativos	Calendário (CalDAV)
Celular	Contatos (CardDAV)	Controlar atualização de SO
Credenciais	Nome do dispositivo	Configuração de educação
Exchange	Fonte	Layout da tela inicial
Importar perfil de iOS e macOS	LDAP	Localização
Email	Domínios gerenciados	Opções de MDM
Informações sobre a organização	Código secreto	Ponto de acesso pessoal
Remoção de perfil	Perfil de provisionamento	Remoção de perfil de provisionamento
Proxy	Restrições	Roaming
SCEP	iPad compartilhado - Máximo de usuários residentes	iPad compartilhado - Período de tolerância de bloqueio de código secreto
Conta SSO	Store	Calendários inscritos
Termos e Condições	VPN	Papel de parede
Filtro de conteúdo Web	Clip web	WiFi

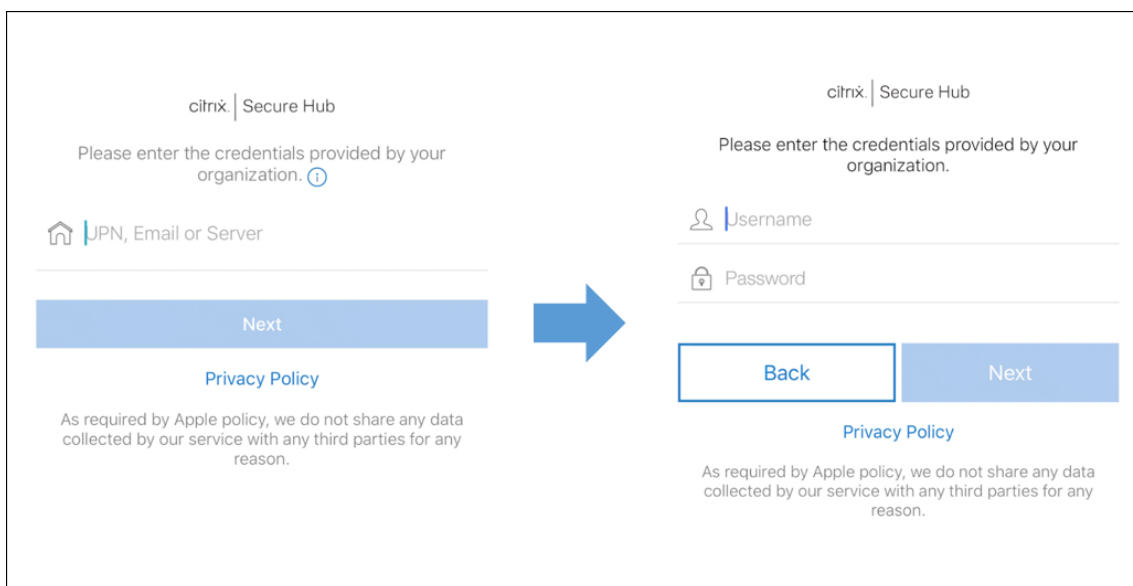
Registrar dispositivos iOS

Esta seção mostra como os usuários registram dispositivos iOS (12.2 ou posterior) no XenMobile Server. Para obter mais informações sobre o registro no iOS, abra o seguinte vídeo:

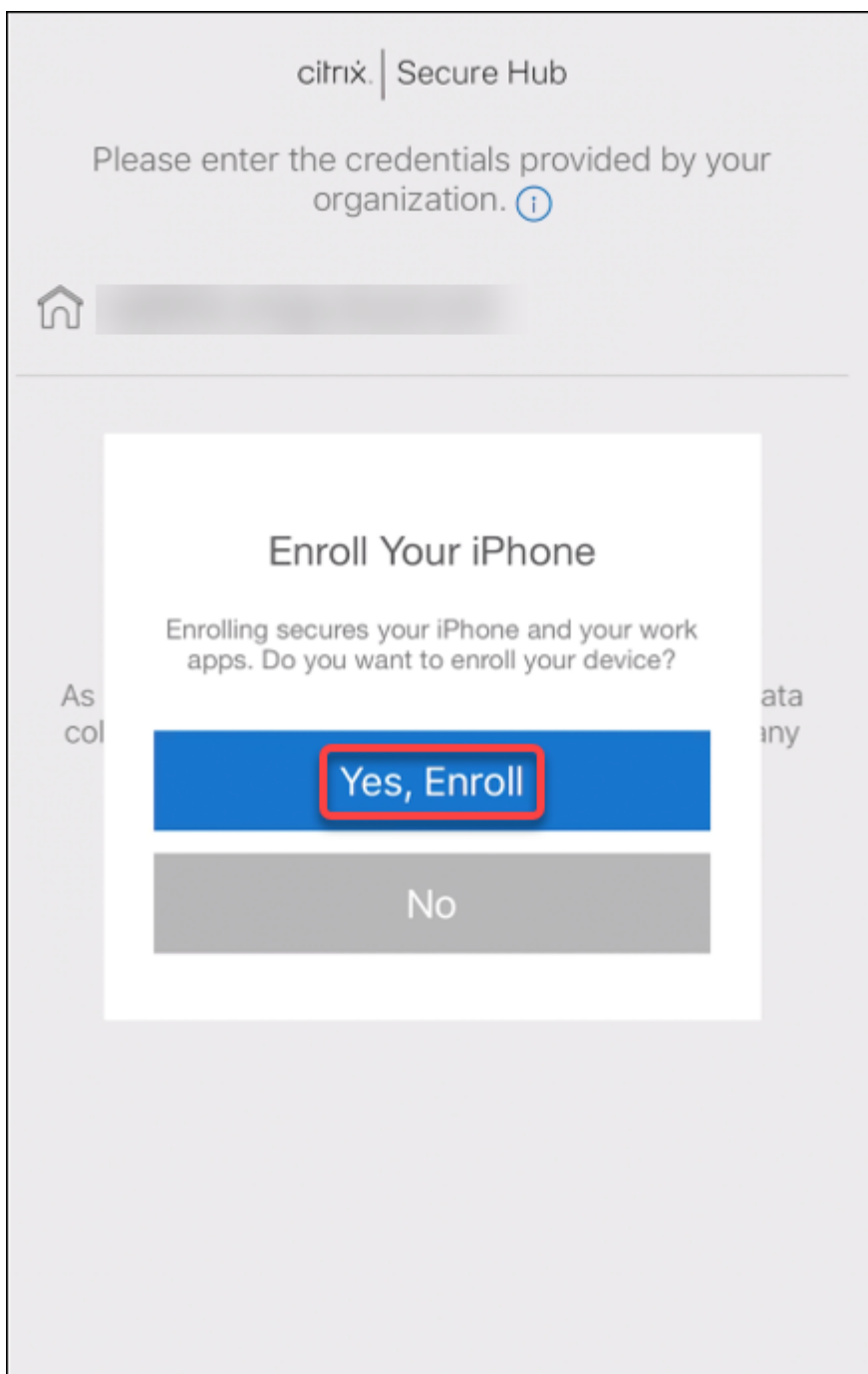
Enroll using Secure Hub



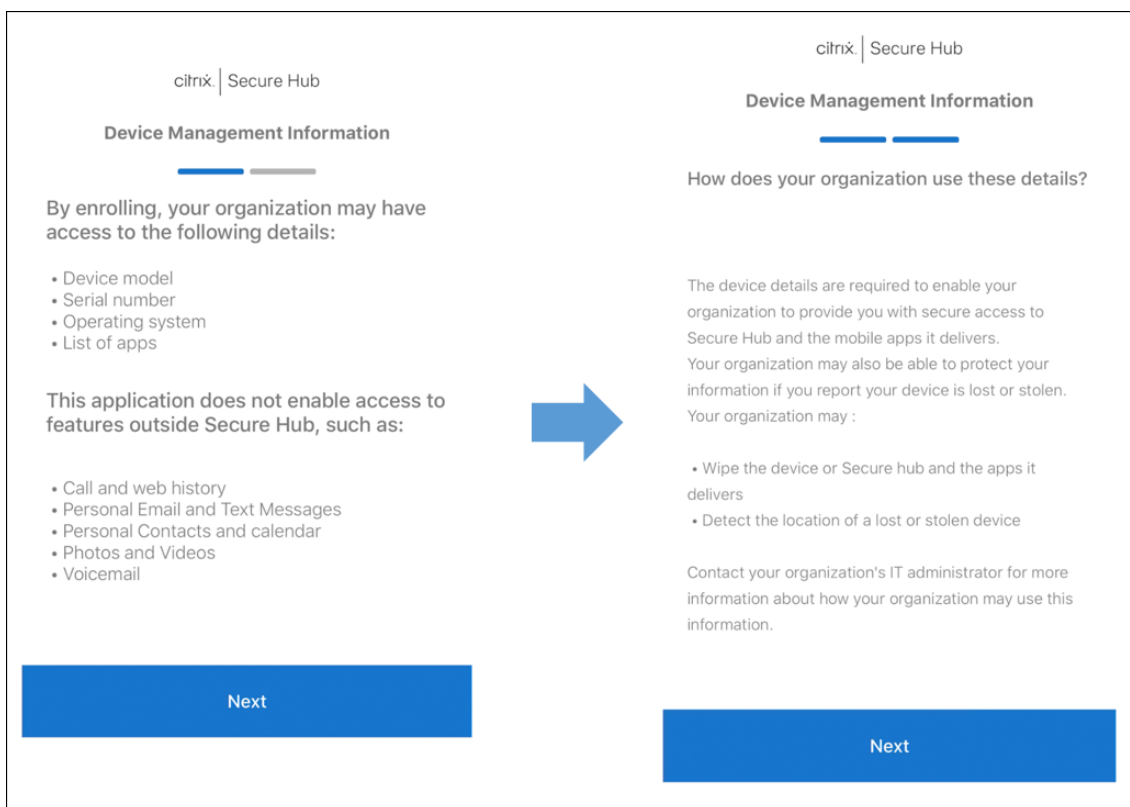
1. Acesse a Apple Store no seu dispositivo iOS, baixe o aplicativo Citrix Secure Hub e toque no aplicativo.
2. Quando solicitado a instalar o aplicativo, toque em **Avançar** e, em seguida, toque em **Instalar**.
3. Depois que o Secure Hub for instalado, toque em **Abrir**.
4. Insira suas credenciais corporativas, como o nome de servidor do XenMobile Server, o nome UPN ou o endereço de email. Em seguida, clique em **Avançar**.



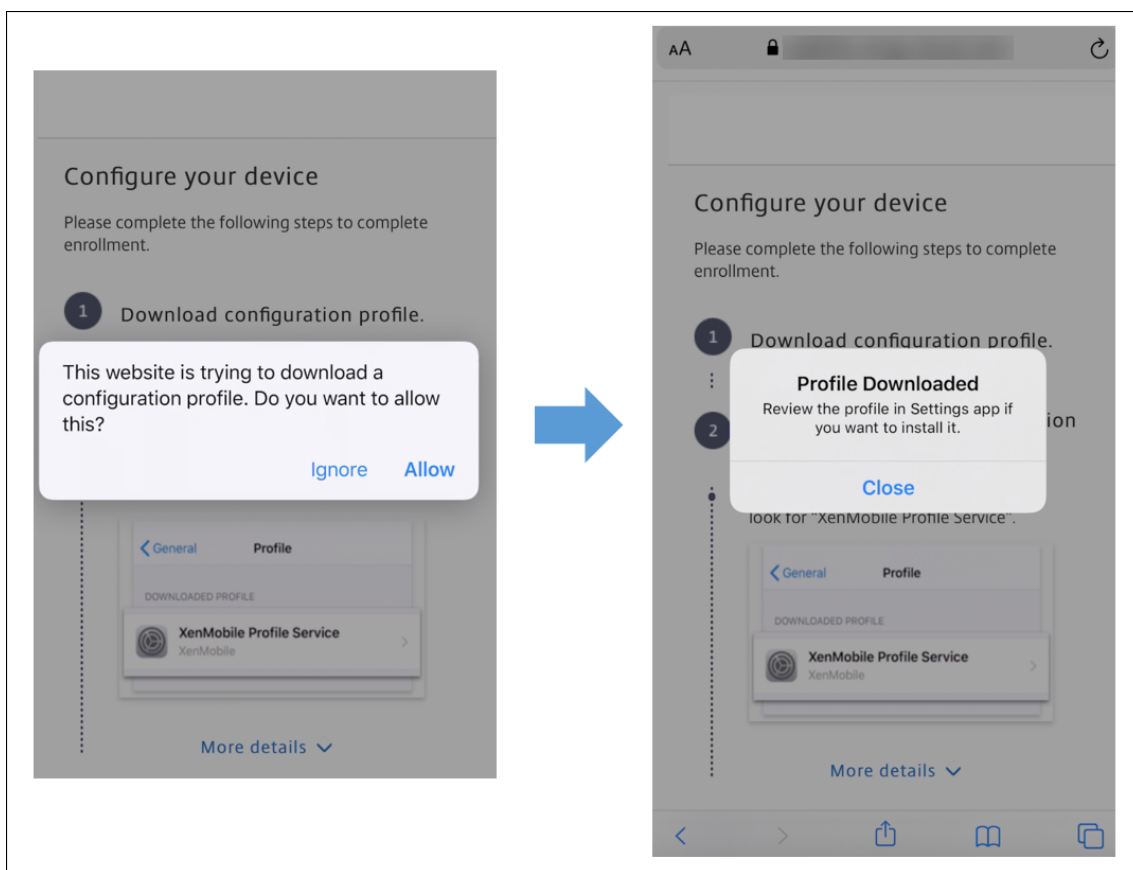
5. Toque em **Sim, registrar** para registrar seu dispositivo iOS.



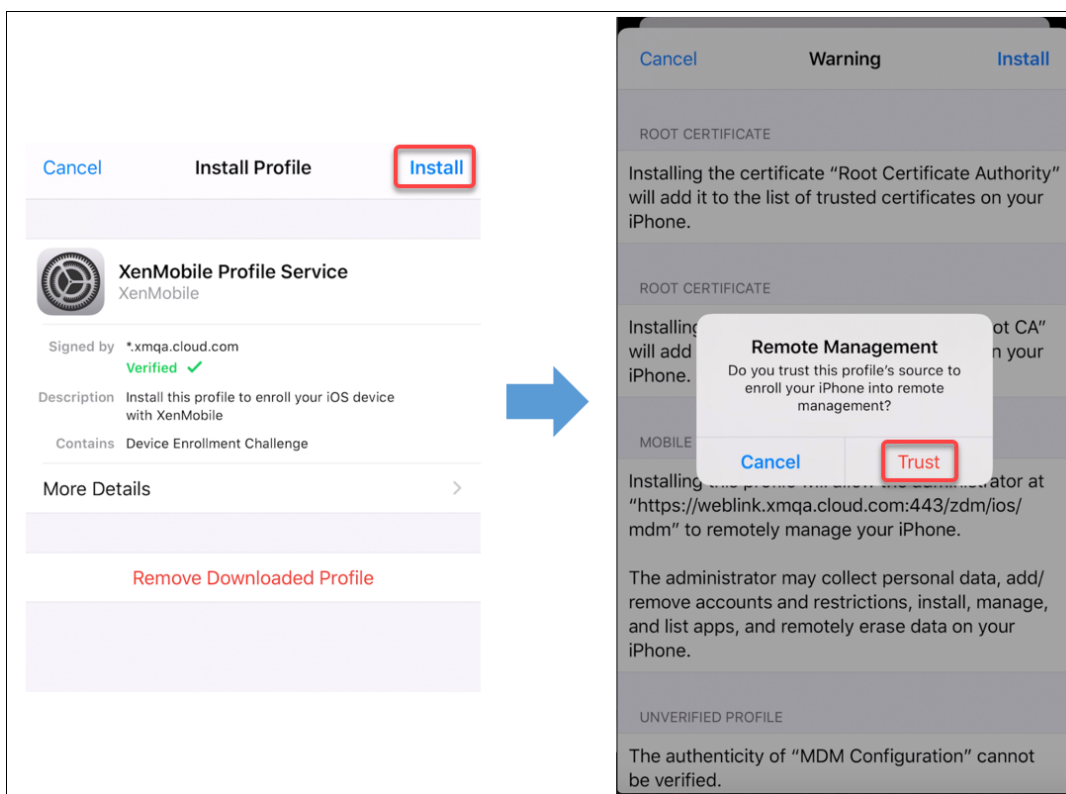
6. A lista dos dados que o XenMobile Server coleta é exibida. Clique em **Avançar**. A explicação de como uma organização usa esses dados aparece. Clique em **Avançar**.



7. Depois de digitar suas credenciais, toque em **Permitir**, quando solicitado, para baixar o perfil de configuração. Depois de baixar o perfil de configuração, toque em **Fechar**.



8. Nas configurações do dispositivo, instale o certificado iOS e adicione o dispositivo à lista confiável.
- Vá para **Configurações > Geral > Perfil > XenMobile Profile Service** e toque em **Instalar** para adicionar o perfil.
 - Na janela de notificação, toque em **Confiar** para registrar seu dispositivo no gerenciamento remoto.



9. Quando o registro for bem-sucedido, abra o Secure Hub. Se você estiver se registrando no MDM+MAM, depois que suas credenciais forem validadas, crie e confirme seu PIN Citrix quando solicitado.
10. Após a conclusão do fluxo de trabalho, o dispositivo é registrado. Você pode acessar a loja de aplicativos para exibir os aplicativos que pode instalar no seu dispositivo iOS.

Ações de segurança

O iOS suporta as seguintes ações de segurança. Para obter uma descrição de cada ação de segurança, consulte [Ações de segurança](#).

Ignorar bloqueio de ativação	Bloqueio de aplicativo	Apagamento de aplicativos
Bloqueio de ativação ASM	Renovação de certificado	Limpar restrições
Ativar/Desativar o Modo Perdido	Ativar/Desativar rastreamento	Apagamento completo
Localizar	Bloquear	Anel
Solicitar/Parar espelhamento de AirPlay	Reiniciar/Desligar	Revogar/Autorizar

Apagamento seletivo

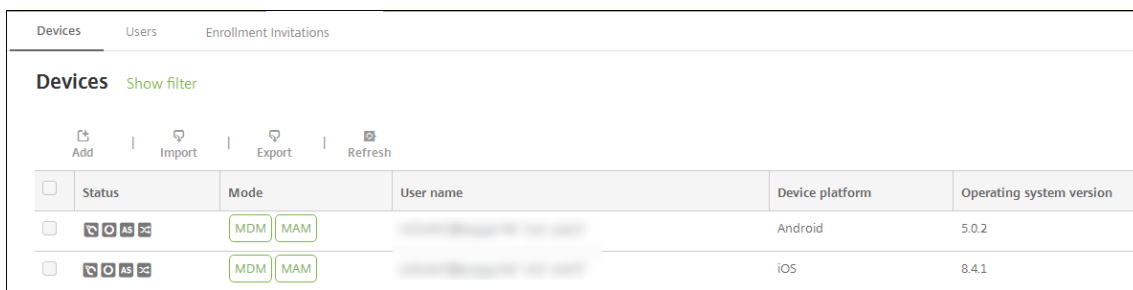
Desbloquear

Bloquear dispositivos iOS

Você pode bloquear um dispositivo iOS perdido com uma exibição de acompanhamento de uma mensagem e um número de telefone que aparecem na tela de bloqueio do dispositivo.

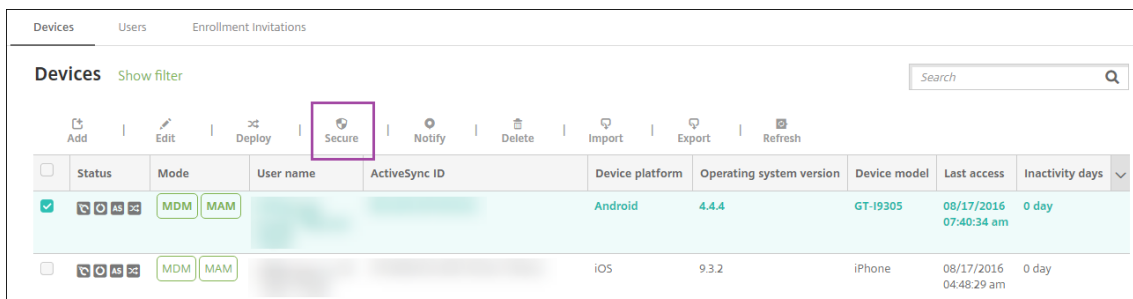
Para exibir uma mensagem e o número de telefone em um dispositivo bloqueado, defina a política de [Código secreto](#) como **true** no console XenMobile Server. Como alternativa, os usuários podem ativar o código secreto no dispositivo manualmente.

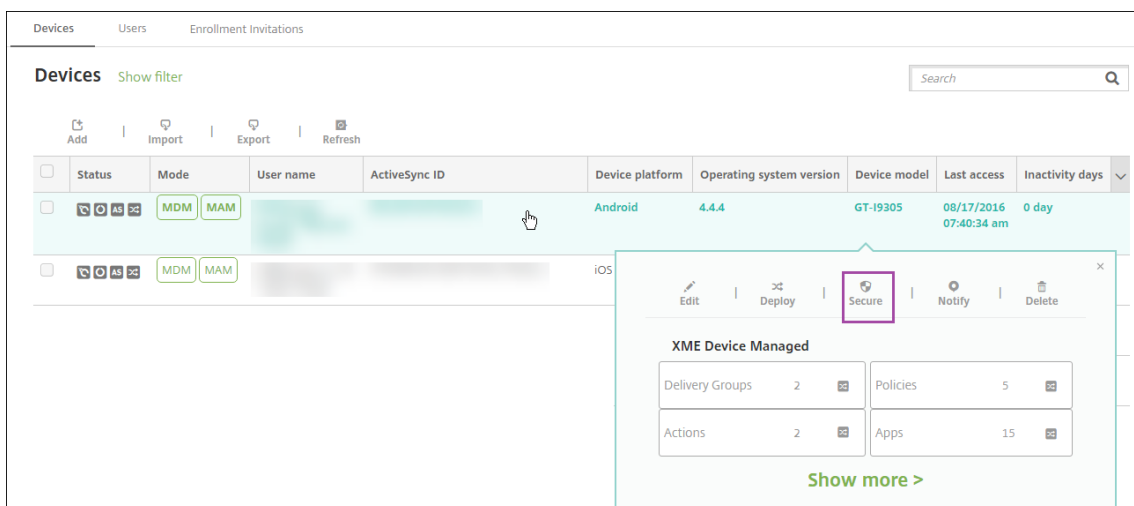
1. Clique em **Gerenciar > Dispositivos**. A página **Dispositivos** é exibida.



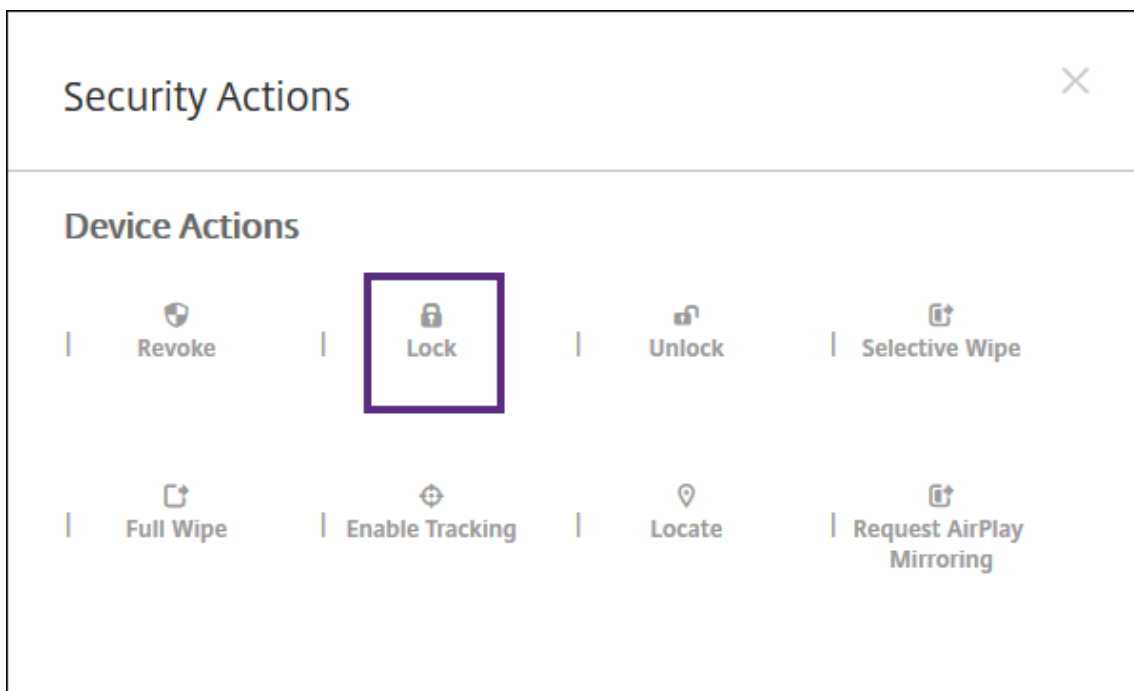
2. Selecione o dispositivo iOS que você deseja bloquear.

Marque a caixa de seleção ao lado de um dispositivo para exibir o menu de opções acima da lista de dispositivos. Clique em qualquer outro lugar na lista para exibir o menu de opções no lado direito da listagem.

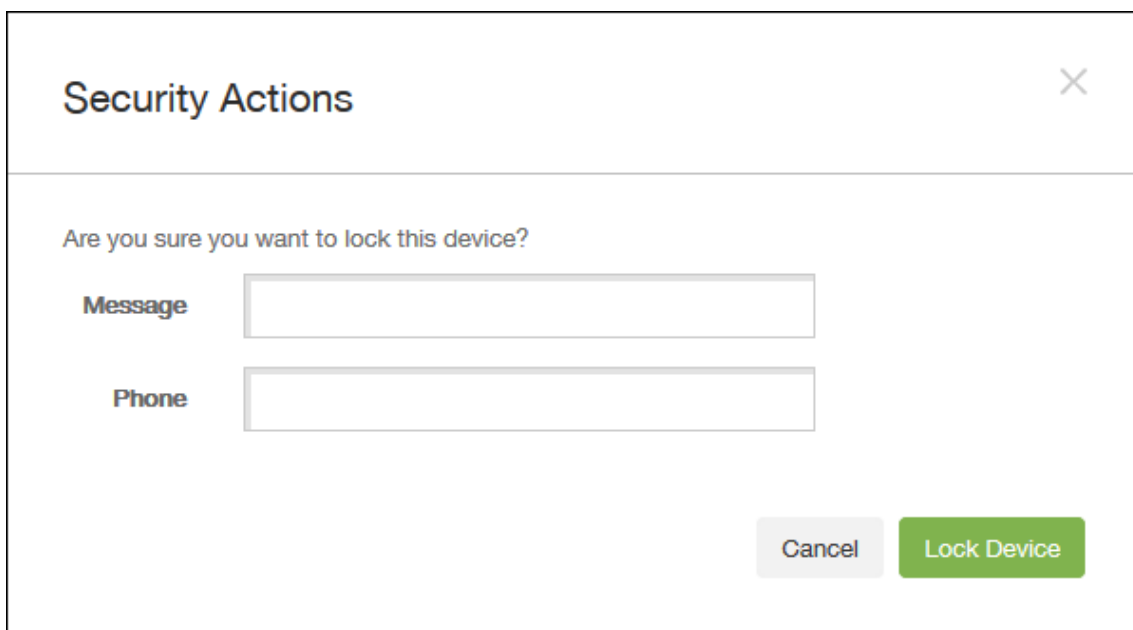




3. No menu de opções, clique em **Segurança**. A caixa de diálogo **Ações de Segurança** é exibida.



4. Clique em **Bloquear**. A caixa de diálogo de confirmação **Ações de segurança** é exibida.



Security Actions

Are you sure you want to lock this device?

Message

Phone

Cancel Lock Device

5. Opcionalmente, digite uma mensagem e um número de telefone que aparecerão na tela de bloqueio do dispositivo.

O iOS acrescenta as palavras “iPad perdido” ao conteúdo digitado no campo **Mensagem**.

Se você deixar o campo **Mensagem** vazio e fornecer um número de telefone, a Apple exibirá a mensagem “Ligar para o proprietário” na tela de bloqueio do dispositivo.

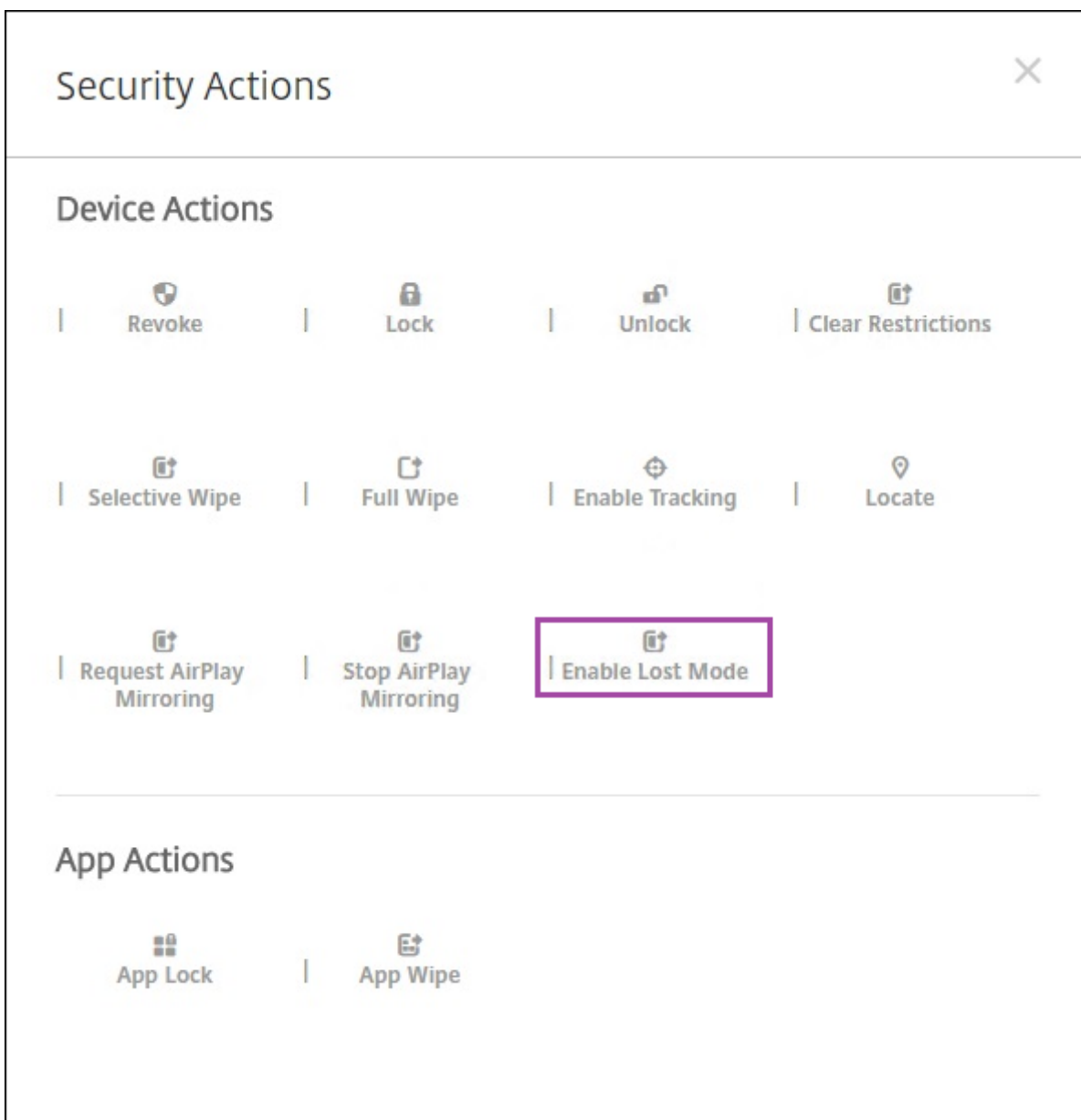
6. Clique em **Bloquear Dispositivo**.

Colocar dispositivos iOS no Modo Perdido

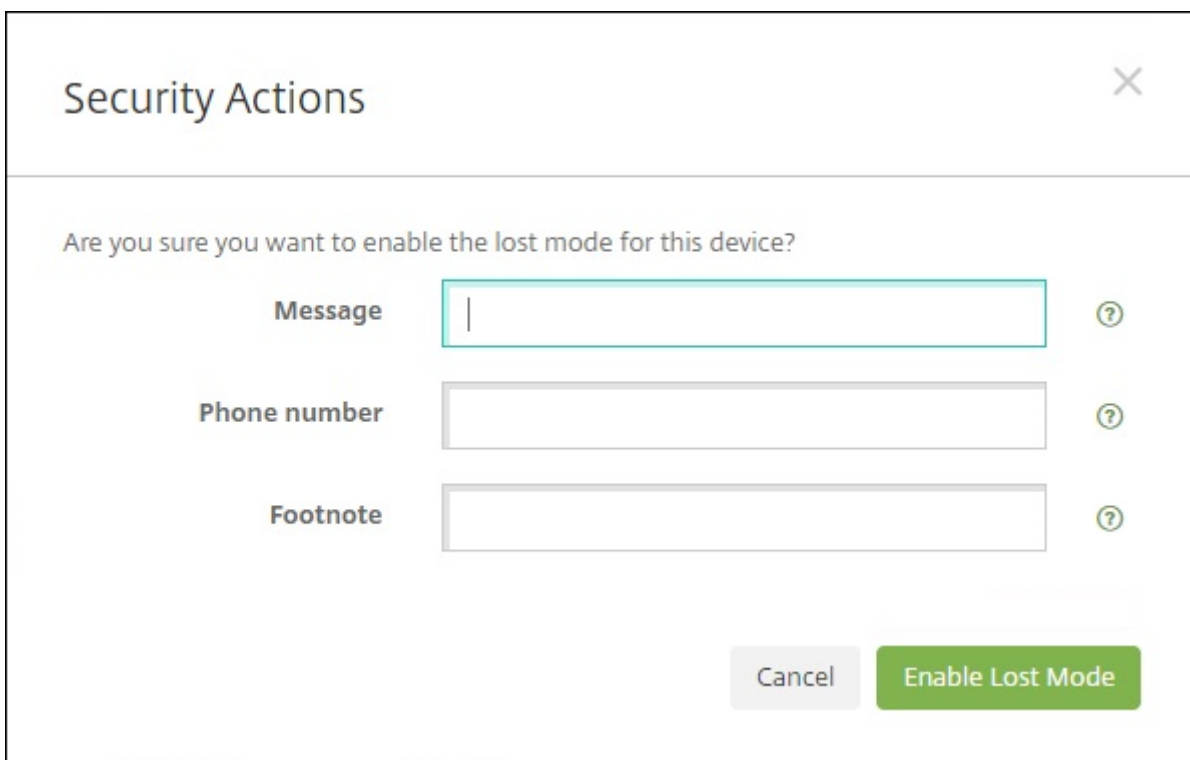
A propriedade de dispositivo Modo Perdido do XenMobile Server coloca um dispositivo iOS no Modo Perdido. Ao contrário do Modo perdido gerenciado da Apple, o Modo perdido do XenMobile Server não requer que um usuário realize nenhuma das seguintes ações para ativar a localização de seu dispositivo: definir a configuração **Buscar iPhone/iPad** ou ativar os Serviços de localização para o Citrix Secure Hub.

No Modo perdido do XenMobile Server, somente o XenMobile Server pode desbloquear o dispositivo. (Em contraste, se você usar o recurso de bloqueio de dispositivo do XenMobile Server, os usuários podem desbloquear o dispositivo diretamente usando um código PIN fornecido por você.)

Para ativar ou desativar o Modo perdido: vá para **Gerenciar > Dispositivos**, escolha um dispositivo iOS supervisionado e clique em **Segurança**. Em seguida, clique em **Ativar modo perdido** ou **Desativar modo perdido**.

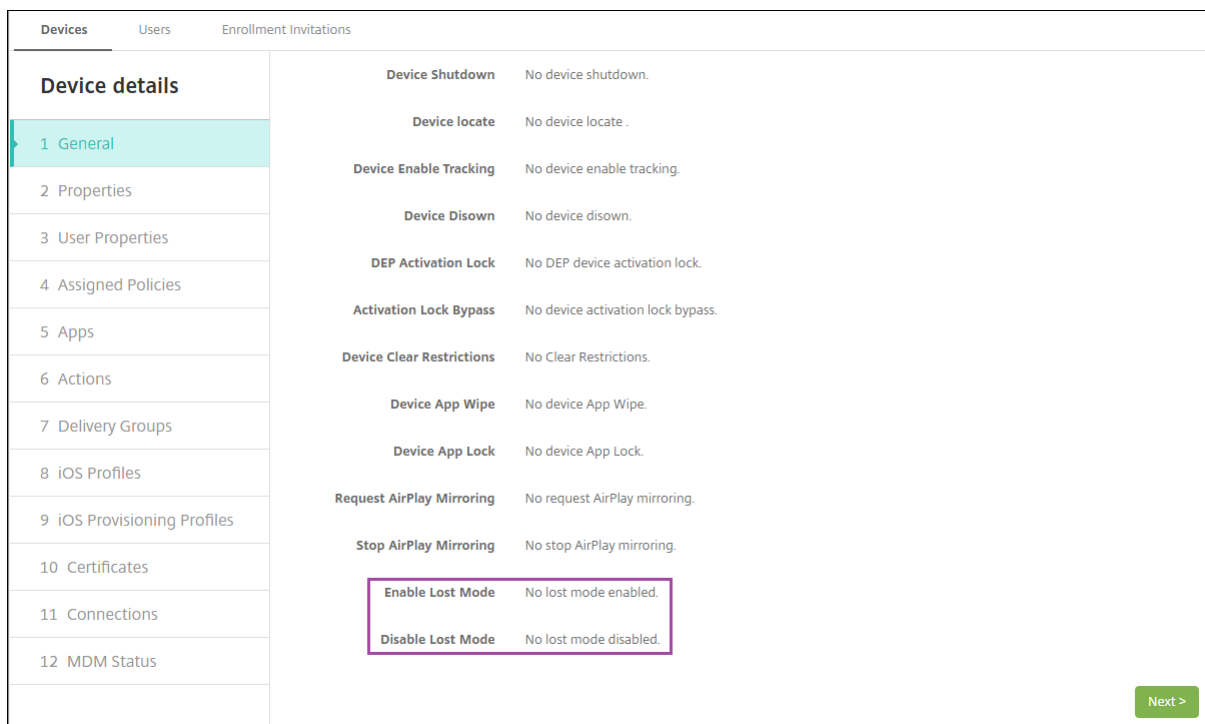


Se você clicar em **Ativar Modo Perdido**, digite informações para aparecer no dispositivo quando estiver no modo perdido.



Use qualquer um dos seguintes métodos para verificar o status do Modo perdido:

- Na janela **Ações de segurança**, verifique se o botão é **Desativar modo perdido**.
- Em **Gerenciar > Dispositivos**, na guia **Geral**, em **Segurança**, veja a última ação Ativar modo perdido ou Desativar modo perdido.



Device details	Setting	Status
1 General	Device Shutdown	No device shutdown.
2 Properties	Device locate	No device locate.
3 User Properties	Device Enable Tracking	No device enable tracking.
4 Assigned Policies	Device Disown	No device disown.
5 Apps	DEP Activation Lock	No DEP device activation lock.
6 Actions	Activation Lock Bypass	No device activation lock bypass.
7 Delivery Groups	Device Clear Restrictions	No Clear Restrictions.
8 iOS Profiles	Device App Wipe	No device App Wipe.
9 iOS Provisioning Profiles	Device App Lock	No device App Lock.
10 Certificates	Request AirPlay Mirroring	No request AirPlay mirroring.
11 Connections	Stop AirPlay Mirroring	No stop AirPlay mirroring.
12 MDM Status	Enable Lost Mode	No lost mode enabled.
	Disable Lost Mode	No lost mode disabled.

- Em **Gerenciar > Dispositivos**, na guia **Propriedades**, confirme que o valor da configuração de **Modo perdido de MDM ativado** esteja correta.

Devices	Users	Enrollment Invitations
Device details		
1 General	Activation lock enabled	No
2 Properties	Hardware encryption capabilities	Block and file levels encryption
3 User Properties	Internal storage encrypted	No
4 Assigned Policies	Jailbroken/Rooted	No
5 Apps	MDM lost mode enabled	No
6 Actions	Passcode compliant	Yes
7 Delivery Groups	Passcode compliant with configuration	Yes
8 iOS Profiles	Passcode present	No
9 iOS Provisioning Profiles	Supervised	No
10 Certificates	- Storage space Add	
11 Connections	Available storage space	10.92 GB
12 MDM Status	Total storage space	12.28 GB ×
	- System information Add	
	Active iTunes account	Yes
	Cloud backup enabled	No
		Back Next >

Se você ativar o Modo perdido do XenMobile Server em um dispositivo iOS, o console XenMobile Server também mudará, da seguinte maneira:

- Em **Configurar > Ações**, a lista **Ações** não inclui estas ações automatizadas: **Revogar o dispositivo**, **Apagar seletivamente o dispositivo** e **Apagar completamente o dispositivo**.
- Em **Gerenciar > Dispositivos**, a lista **Ações de segurança** não inclui mais as ações de dispositivo **Revogar** e **Apagamento seletivo**. Você ainda pode usar uma ação de segurança para executar uma ação de **Apagamento completo**, conforme necessário.

O iOS acrescenta as palavras “iPad perdido” ao conteúdo digitado na caixa **Mensagem** na tela **Ações de segurança**.

Se você deixar a **Mensagem** vazia e fornecer um número de telefone, a Apple exibirá a mensagem “Ligar para o proprietário” na tela de bloqueio do dispositivo.

Ignorar bloqueio de ativação do iOS

Bloqueio de ativação é um recurso do Buscar iPhone/iPad que impede a reativação de um dispositivo supervisionado perdido ou roubado. O Bloqueio de Ativação requer o ID Apple e a senha do usuário antes que qualquer pessoa possa executar estas ações: desligar o Buscar iPhone/iPad, apagar o dispositivo ou reativar o dispositivo. Para os dispositivos de propriedade da organização, ignorar um bloqueio de ativação é necessário, por exemplo, para redefinir ou realocar dispositivos.

Para ativar o Bloqueio de Ativação, você configura e implanta a política do dispositivo de Opções de MDM do XenMobile Server. Você pode gerenciar um dispositivo a partir do console XenMobile Server sem as credenciais Apple do usuário. Para desviar do requisito de credenciais Apple de um bloqueio de ativação, execute a ação de segurança Ignorar Bloqueio de Ativação a partir do console XenMobile Server.

Por exemplo, se o usuário retorna um telefone perdido ou para configurar o dispositivo antes ou após um apagamento completo: quando o telefone pede as credenciais da conta da Apple App Store, você pode ignorar essa etapa emitindo a ação de segurança Ignorar Bloqueio de Ativação no console XenMobile Server.

Requisitos do dispositivo para o desvio de bloqueio de ativação

- Supervisionado por meio do Apple Configurator ou do Programa de Implantação da Apple
- Configurado com uma conta do iCloud
- Buscar iPhone/iPad ativado
- Registrado no XenMobile Server
- A política de dispositivo de Opções do MDM, com o bloqueio de ativação habilitado, é implantada nos dispositivos

Para ignorar um bloqueio de ativação antes de emitir um apagamento completo de um dispositivo:

1. Acesse **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Segurança** e em **Ignorar bloqueio de ativação**.
2. Apagar o dispositivo. A tela de bloqueio de ativação não aparece durante a configuração do dispositivo.

Para ignorar um bloqueio de ativação depois de emitir um apagamento completo de um dispositivo:

1. Redefinir ou apagar o dispositivo. A tela de bloqueio de ativação aparece durante a configuração do dispositivo.
2. Acesse **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Segurança** e em **Ignorar bloqueio de ativação**.
3. Toque no botão Voltar no dispositivo. É exibida a tela de início.

Tenha em mente o seguinte:

- Aconselhe seus usuários a não desligar o Buscar iPhone/iPad. Não execute um apagamento completo a partir do dispositivo. Em ambos os casos, o usuário é solicitado a digitar a senha da conta do iCloud. Após a validação da conta, o usuário não verá uma tela Ativar iPhone/iPad depois de apagar todo o conteúdo e configurações.
- Para um dispositivo com um código de desvio do bloqueio de ativação gerado e com o bloqueio de ativação ativado: se você não pode ignorar a página Ativar iPhone/iPad após um apagamento completo, não é necessário excluir o dispositivo do XenMobile Server. Você ou o usuário pode entrar em contato com o suporte da Apple para desbloquear o dispositivo diretamente.

- Durante um inventário de hardware, o XenMobile Server consulta um dispositivo para obter um código de desvio de bloqueio de Ativação. Se um código de desvio estiver disponível, o dispositivo o envia para o XenMobile Server. Em seguida, para remover o código de desvio do dispositivo, envie a ação de segurança Ignorar Bloqueio de Ativação a partir do console XenMobile Server. Nesse ponto, o XenMobile Server e a Apple têm o código de desvio necessário para desbloquear o dispositivo.
- A ação de segurança Ignorar Bloqueio de Ativação utiliza a disponibilidade de um serviço Apple. Se a ação não funcionar, você pode desbloquear um dispositivo da seguinte maneira. No dispositivo, insira manualmente as credenciais da conta do iCloud. Ou deixe o campo do nome do usuário vazio e digite o código de desvio no campo da senha. Para ver o código de desvio, vá para **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Editar** e clique em **Propriedades**. O **código de desvio do bloqueio de ativação** está em **Informações de segurança**.

macOS

April 26, 2021

Para gerenciar dispositivos macOS no XenMobile, configure um certificado de serviço de Notificação por Push (APNs) da Apple. Para obter informações, consulte [Certificados APNs](#).

O XenMobile registra dispositivos macOS no MDM. O XenMobile oferece suporte aos seguintes tipos de autenticação de registro para dispositivos macOS em MDM.

- Domínio
- Domínio e senha única
- URL de convite e senha única

Requisitos para certificados confiáveis no macOS 15:

A Apple tem novos requisitos para certificados de servidor TLS. Verifique se todos os certificados seguem os novos requisitos da Apple. Consulte a publicação da Apple, <https://support.apple.com/en-us/HT210176>. Para obter ajuda com o gerenciamento de certificados, consulte [Carregando certificados no XenMobile](#).

Um fluxo de trabalho geral para iniciar o gerenciamento de dispositivos macOS é o seguinte:

1. Configurar políticas de dispositivos macOS.
2. Registrar dispositivos macOS.
3. Configurar ações de segurança de dispositivos e aplicativos. Consulte [Ações de segurança](#).

Para obter os sistemas operacionais compatíveis, consulte [Sistemas operacionais compatíveis de dispositivos](#).

Nomes de host da Apple que devem permanecer abertos

Alguns nomes de host da Apple devem permanecer abertos para garantir o funcionamento correto do iOS, macOS e Apple App Store. Bloquear esses nomes de host pode afetar a instalação, atualização e operação adequada do iOS, aplicativos iOS, operação de MDM e registro de dispositivos e aplicativos. Para obter mais informações, consulte <https://support.apple.com/en-us/HT201999>.

Métodos de registro suportados

A tabela a seguir lista os métodos de registro compatíveis com o XenMobile para dispositivos macOS:

Método	Compatível
Programa de implantação da Apple	Sim
Apple School Manager	Sim
Apple Configurator	Não
Registro manual	Sim
Convites para registro	Sim

A Apple possui programas de registro de dispositivos para contas de negócios e educação. Para contas de negócios, você se registra no Programa de Implantação da Apple para usar o Programa de Implantação da Apple para registro e gerenciamento de dispositivos no XenMobile. Esse programa é para dispositivos iOS e macOS. Consulte [Implantar dispositivos através do Programa de implantação da Apple](#).

Para contas de educação, você cria uma conta do Apple School Manager. O Apple School Manager unifica o Programa de Implantação e a compra por volume. O Apple School Manager é um tipo de Programa de Implantação do Apple Educação. Consulte [Integração com os recursos do Apple Educação](#).

Você pode usar o Programa de Implantação da Apple para registrar em massa dispositivos iOS e macOS. Você pode comprar esses dispositivos diretamente da Apple, de um Revendedor Autorizado Apple participante ou de uma operadora.

Configurar políticas de dispositivos macOS

Use estas políticas para configurar como o XenMobile interage com dispositivos que executam o macOS. Esta tabela lista todas as políticas de dispositivo disponíveis para dispositivos macOS.

Espelhamento de AirPlay	Inventário de aplicativos	Calendário (CalDAV)
Contatos (CardDAV)	Controlar atualização de SO	Credenciais
Nome do dispositivo	Exchange	FileVault
Firewall	Fonte	Importar perfil de iOS e macOS
LDAP	Email	Código secreto
Remoção de perfil	Restrições	SCEP
VPN	Clipes web	Wi-Fi

Registrar dispositivos macOS

O XenMobile fornece dois métodos para registrar dispositivos que executam o macOS. Os dois modos permite que os usuários de macOS façam o registro diretamente dos seus dispositivos pela rede celular.

- **Send users an enrollment invitation:** este método de registro permite definir qualquer um dos seguintes modos de segurança de registro para dispositivos macOS:
 - Nome de usuário + senha
 - Nome de usuário + PIN
 - Autenticação de dois fatores

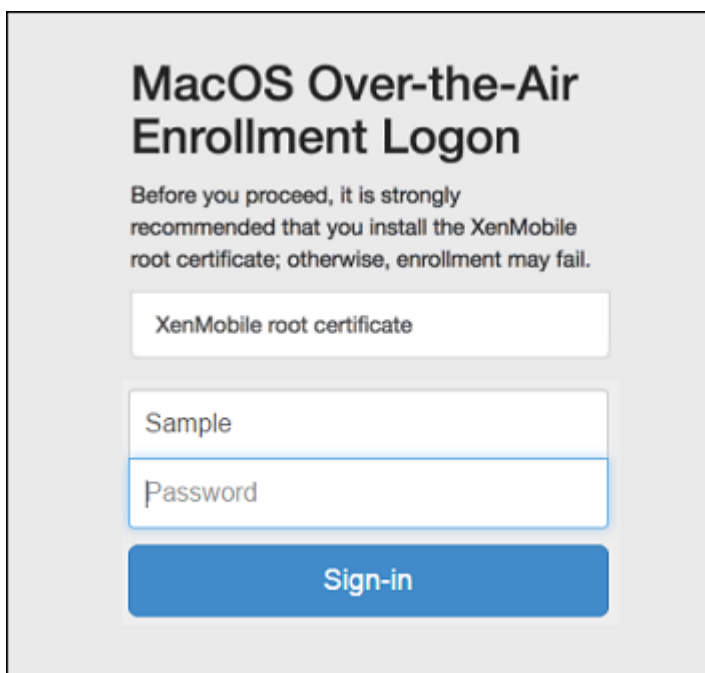
Quando o usuário segue as instruções no convite de registro, é exibida uma tela de logon com o nome de usuário preenchido.

- **Send users an enrollment link:** este método de registro para dispositivos macOS envia aos usuários um link de registro que eles podem abrir nos navegadores Safari ou Chrome. Um usuário se registra fornecendo seu nome de usuário e senha.

Para impedir o uso de um link de registro para dispositivos macOS, defina a propriedade do servidor **Enable macOS OTAE** como **false**. Como resultado, os usuários do macOS apenas podem se registrar usando um convite para registro.

Enviar aos usuários macOS um convite para registro

1. Adicione um convite para registro de usuário do macOS. Consulte [Criar um convite para registro](#).
2. Depois que os usuários recebem o convite e clicam no link, é exibida a seguinte tela no navegador Safari. O XenMobile preenche o nome do usuário. Se você escolher **Dois fatores** para o modo de segurança de registro, outro campo será exibido.



3. Os usuários instalam os certificados conforme necessário. A exibição do prompt para os usuários instalarem certificados depende se você configurou o seguinte para o macOS: um certificado SSL publicamente confiável e um certificado de assinatura digital publicamente confiável. Para obter informações sobre certificados, consulte [Certificados e autenticação](#).
4. Os usuários fornecem as credenciais solicitadas.

As políticas de dispositivo Mac são instaladas. Agora você pode começar a gerenciar dispositivos macOS com o XenMobile, da mesma forma como gerencia os dispositivos móveis.

Enviar um link de instalação para os usuários macOS

1. Envie o link de registro <https://serverFQDN:8443/instanceName/macOS/otae>, que os usuários podem abrir nos navegadores Safari ou Chrome.
 - **serverFQDN** é o nome de domínio totalmente qualificado (FQDN) do servidor que executa o XenMobile.
 - A Porta **8443** é a porta segura padrão. Se você tiver configurado uma porta diferente, use essa porta em vez da 8443.
 - O **instanceName**, geralmente mostrado como **zdm**, é o nome especificado durante a instalação do servidor.

Para obter mais informações sobre o envio de links de instalação, consulte [Envie um convite para registro](#).

2. Os usuários instalam os certificados conforme necessário. Se você configurou um certificado SSL publicamente confiável e um certificado de assinatura digital para iOS e macOS, os usuários

verão o prompt para instalar certificados. Para obter informações sobre certificados, consulte [Certificados e autenticação](#).

3. Os usuários fazem login nos Macs.

As políticas de dispositivo Mac são instaladas. Agora você pode começar a gerenciar dispositivos macOS com o XenMobile, da mesma forma como gerencia os dispositivos móveis.

Ações de segurança

O macOS suporta as seguintes ações de segurança. Para obter uma descrição de cada ação de segurança, consulte [Ações de segurança](#).

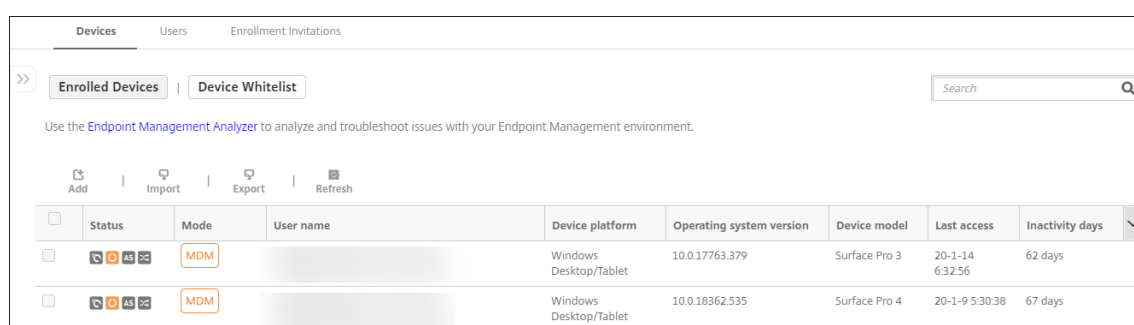
Revogar	Bloquear	Apagamento seletivo
Apagamento completo	Renovação de certificado	

Bloquear dispositivos macOS

Você pode bloquear remotamente um dispositivo macOS perdido. O XenMobile bloqueia o dispositivo. Ele gera um código PIN e o configura no dispositivo. Para acessar o dispositivo, o usuário digita o código PIN. Use **Cancelar bloqueio** para remover o bloqueio do console XenMobile

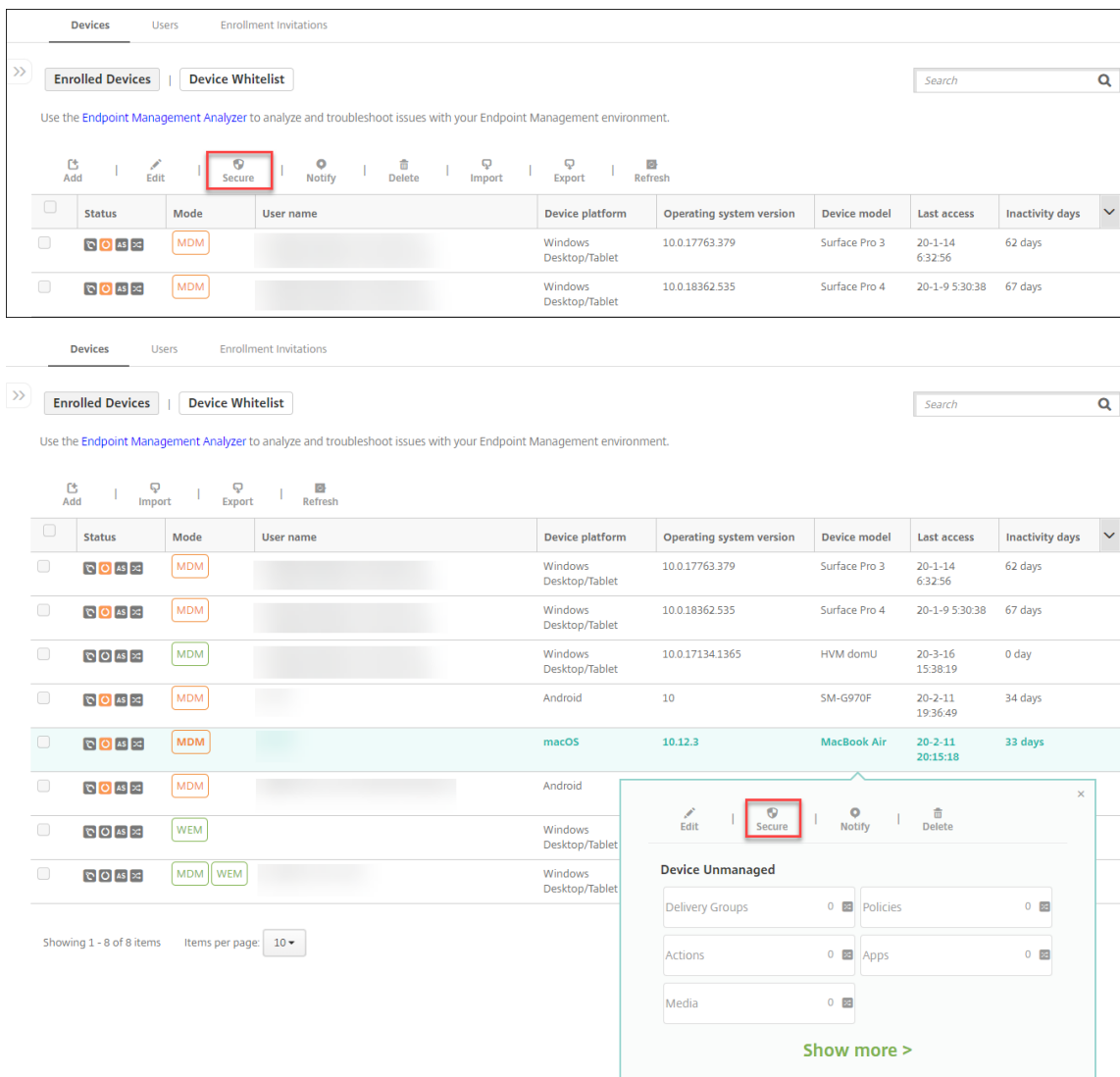
Você pode usar a política de dispositivo de [Código secreto](#) para definir mais configurações associadas ao código PIN. Para obter mais informações, consulte [Configurações do macOS](#).

1. Clique em **Gerenciar > Dispositivos**. A página **Dispositivos** é exibida.

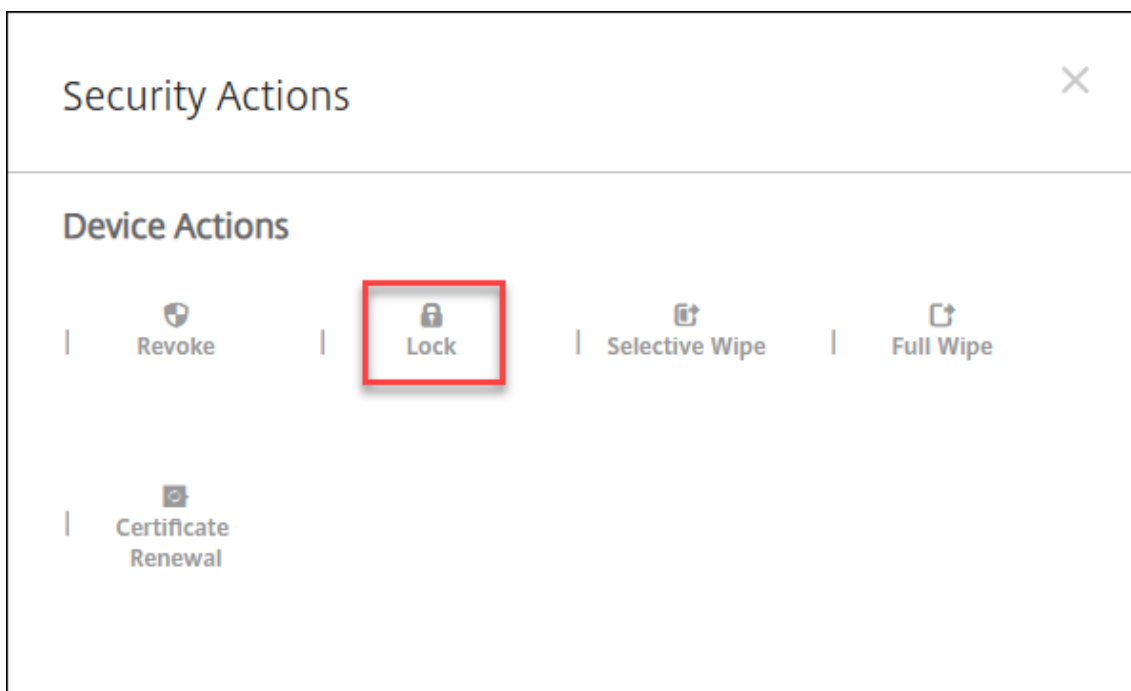


2. Selecione o dispositivo macOS que você deseja bloquear.

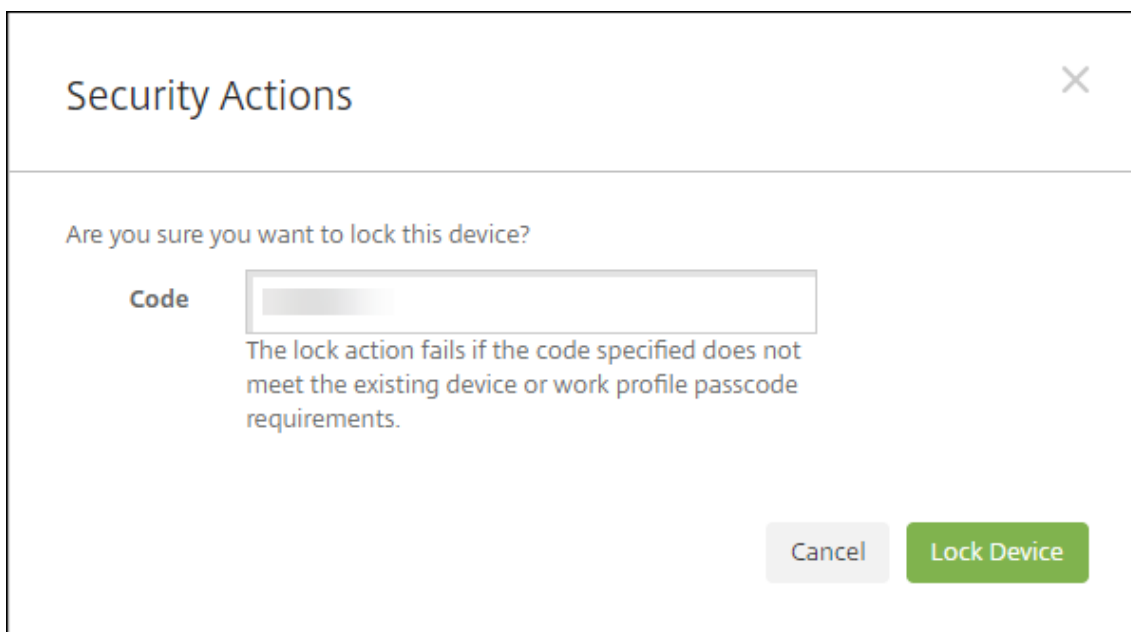
Marque a caixa de seleção ao lado de um dispositivo para exibir o menu de opções acima da lista de dispositivos. Você também pode clicar em qualquer outro lugar em um item listado para exibir o menu de opções no lado direito da lista.



3. No menu de opções, clique em **Segurança**. A caixa de diálogo **Ações de Segurança** é exibida.



4. Clique em **Bloquear**. A caixa de diálogo de confirmação **Ações de segurança** é exibida.



5. Clique em **Bloquear Dispositivo**.

Importante:

Você também pode especificar um código secreto em vez de usar o código gerado pelo XenMobile. A ação de bloqueio falhará se o código especificado não atender aos requisitos de código do dispositivo ou perfil de trabalho existente.

Registro em massa de dispositivos Apple

May 6, 2021

Você pode registrar um grande número de dispositivos iOS, iPadOS e macOS no XenMobile de duas maneiras.

- Use o Programa de Implantação da Apple para registrar os dispositivos iOS, iPadOS e macOS comprados diretamente da Apple, de um revendedor participante autorizado pela Apple ou de uma operadora. Esse suporte inclui iPads compartilhados. O XenMobile oferece suporte ao Programa de Implantação da Apple para Apple Business Manager (ABM) e Apple School Manager (ASM) para Educação. Este artigo descreve como integrar vários dispositivos com a sua conta ABM. Para obter informações sobre como se registrar no ABM e conectar sua conta ABM ao XenMobile, consulte [Implantar dispositivos através do Programa de implantação da Apple](#). Para obter informações sobre as contas do Apple School Manager, consulte [Integração com os recursos do Apple Educação](#).

Para o registro de dispositivos macOS, o XenMobile requer que os dispositivos executem o macOS 10.10 ou versões posteriores.

- Você também pode usar o Apple Configurator 2 para registrar dispositivos iOS, quer eles tenham sido comprados diretamente da Apple ou não.

Com ABM:

- Você não precisa tocar ou preparar os dispositivos. Em vez disso, você envia os números de série ou os números de pedido de compra dos dispositivos por meio do ABM para configurá-los e registrá-los.
- Depois que o XenMobile registrar os dispositivos, você poderá oferecê-los aos usuários, que poderão começar a usá-los imediatamente. Quando você configura dispositivos usando o ABM, pode eliminar algumas etapas do Assistente de Instalação que os usuários poderiam precisar concluir quando iniciassem os dispositivos deles pela primeira vez.
- Para obter mais informações sobre como configurar o ABM, consulte a documentação disponível no [Apple Business Manager](#).

Com o Apple Configurator 2:

- Conecte os dispositivos iOS a um computador Apple que executa o macOS 10.7.2 ou versões posteriores e o aplicativo Apple Configurator 2. Prepare os dispositivos iOS e configure políticas usando o Apple Configurator 2.
- Depois de provisionar os dispositivos com as políticas necessárias, na primeira vez que os dispositivos se conectarem ao XenMobile, eles receberão políticas do XenMobile. Em seguida, será possível começar a gerenciá-los.

- Para obter mais informações sobre como usar o Apple Configurator 2, consulte a [Ajuda do Apple Configurator](#).

Pré-requisitos

Abra as portas necessárias para a conectividade entre o XenMobile e a Apple. Para obter mais informações, consulte [Requisitos de porta](#).

Integrar sua conta do Apple Business Manager com o XenMobile

Se você não tiver uma conta ABM configurada com o XenMobile, conclua as etapas a seguir em [Implantar dispositivos através do Programa de implantação da Apple](#).

- Registre-se no Apple Business Manager.
- Conecte sua conta do Apple Business Manager ao XenMobile.
- Adquira dispositivos ativados para o Programa de Implantação
- Gerencie os dispositivos ativados para o Programa de Implantação

Definir um servidor padrão para registro em massa

Para atribuir grandes volumes de pedidos de dispositivos iOS, iPadOS e macOS a um servidor MDM, você pode definir o XenMobile como o servidor padrão.

1. Faça logon no [Apple Business Manager](#) usando uma conta de administrador ou gerente de registro de dispositivo.
2. Na barra lateral, clique em **Settings > Device Management Settings**.
3. Escolha um servidor MDM existente. Em **Default Device Assignment**, clique em **Change**. Selecione o servidor XenMobile padrão para cada tipo de dispositivo. Clique em **Concluído**.

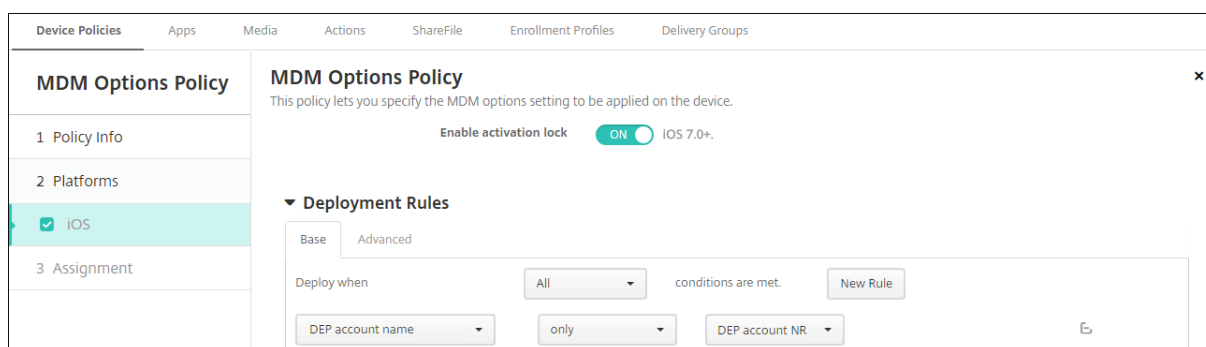
Configurar regras de implantação de políticas de dispositivo e aplicativos para contas ABM

Você pode associar contas ABM a políticas de dispositivo e aplicativos diferentes usando a seção **Regras de implantação** em **Configurar > Políticas de dispositivo** e **Configurar > Aplicativos**. É possível especificar que uma política ou um aplicativo:

- Seja implantado somente para uma determinada conta ABM.
- Seja implantado para todas as contas ABM, exceto a selecionada.

A lista de contas ABM inclui apenas as contas com o status Ativada ou Desativada. Se a conta ABM estiver desativada, o dispositivo ABM não pertencerá a essa conta. Portanto, o XenMobile não implantará o aplicativo ou a política nesse dispositivo.

No exemplo a seguir, uma política de dispositivo é implantada somente para dispositivos com a conta ABM de nome “ABM Account NR”.



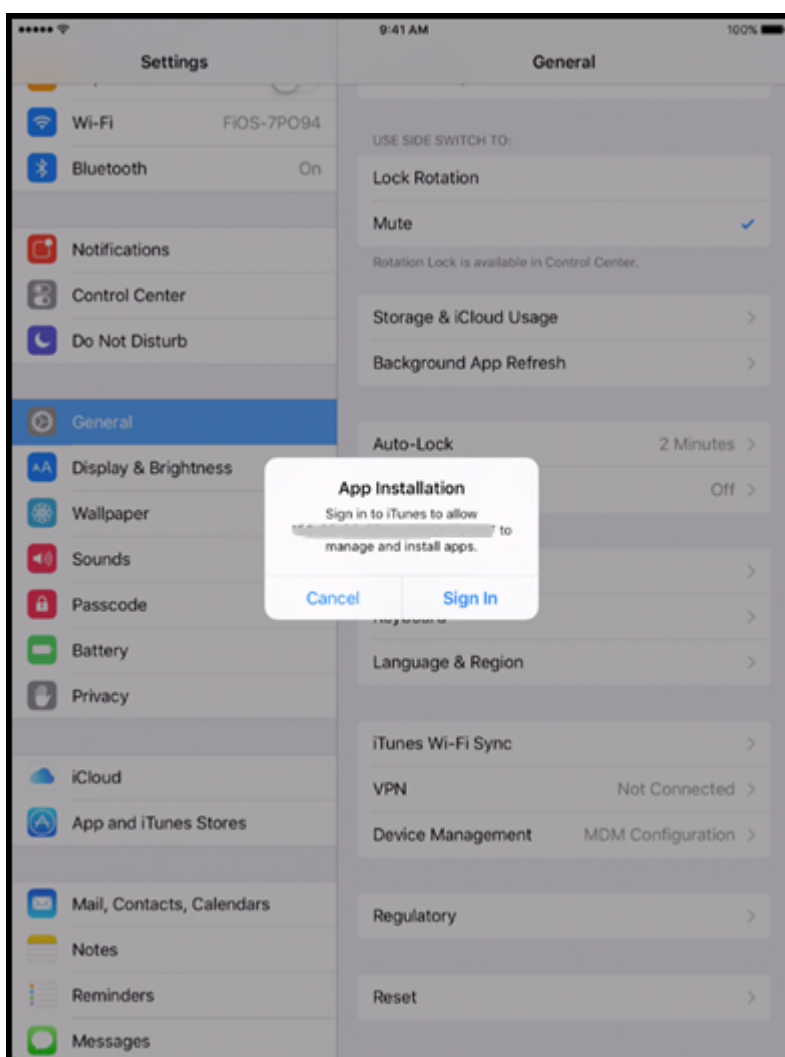
Experiência do usuário ao registrar um dispositivo ativado para o Programa de implantação da Apple

Quando os usuários registram um dispositivo ativado para o Programa de implantação da Apple, a experiência deles é a seguinte.

1. Os usuários iniciam o dispositivo ativado para o Programa de implantação da Apple.
2. O XenMobile fornece a configuração do Programa de implantação da Apple que você definiu no console XenMobile para o dispositivo ativado para o Programa de implantação da Apple.
3. Os usuários definem as configurações iniciais em seus dispositivos.
4. O dispositivo inicia automaticamente o processo de registro de dispositivo do XenMobile.
5. Os usuários continuam a definir as outras configurações iniciais em seus dispositivos.
6. Na tela inicial, os usuários podem ser solicitados a fazer logon no Apple App Store para baixar o Citrix Secure Hub.

Nota:

Essa etapa será opcional se você configurou o XenMobile para implantar o aplicativo Secure Hub usando a atribuição de aplicativos de compra por volume com base em dispositivo. Nesse caso, você não precisa criar uma conta do Apple App Store ou usar uma conta existente.



7. Os usuários abrem o Secure Hub e digitam as respectivas credenciais. Se for exigido pela política, os usuários poderão ser solicitados a criar e verificar um PIN da Citrix.

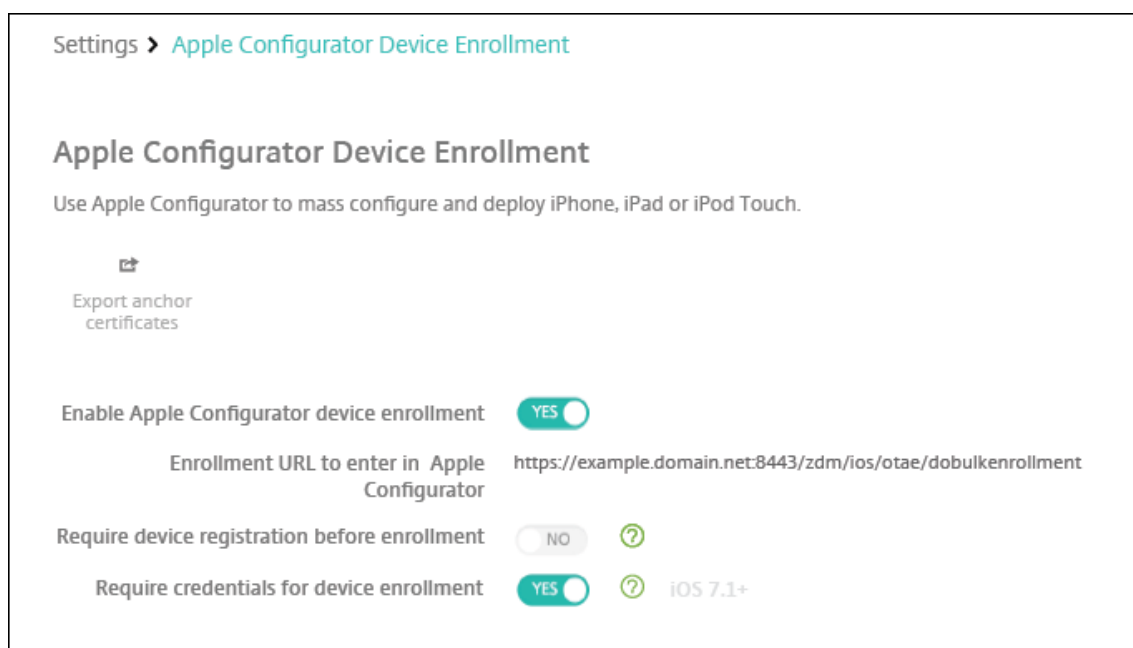
O XenMobile implanta os aplicativos necessários restantes no dispositivo.

Para definir as configurações do Apple Configurator

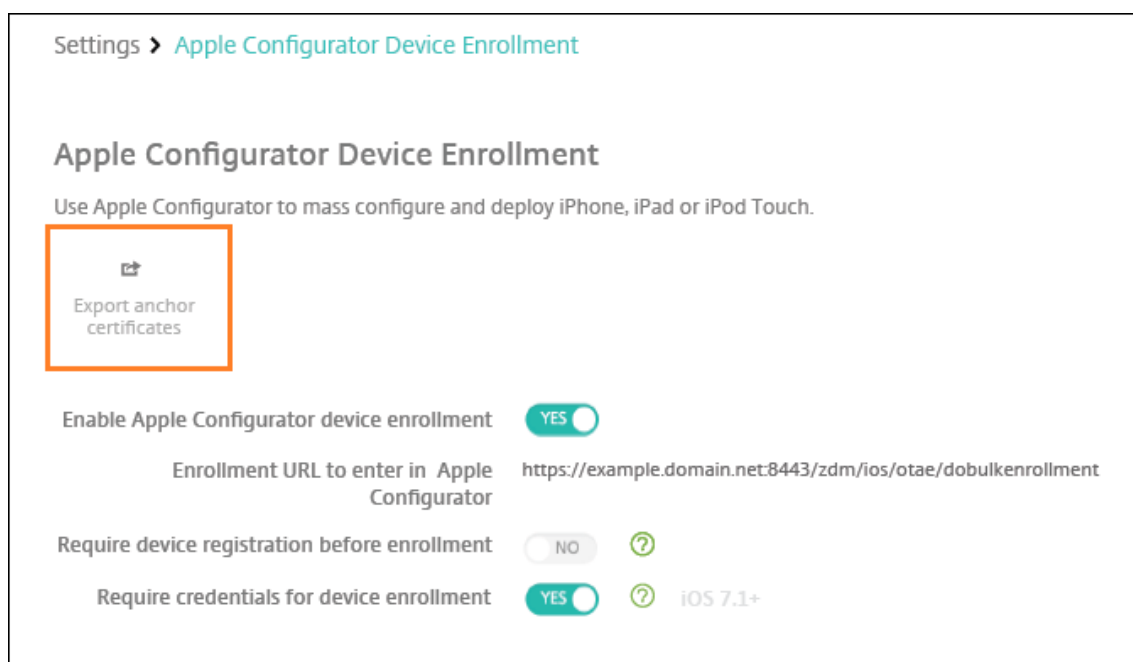
Você pode configurar e implantar dispositivos iPhone e iPad em massa usando o Apple Configurator 2 em vez do Apple Business Manager.

Etapa 1: Definir configurações no XenMobile

1. No console XenMobile, vá para **Configurações > Registro no Apple Configurator Device Enrollment**.



2. Defina **Ativar registro de dispositivo no Apple Configurator** como **Sim**.
3. O campo **URL de registro para entrar no Apple Configurator** é somente leitura. Essa configuração fornece a URL para o XenMobile Server que se comunica com a Apple. Copie e cole a URL quando definir as configurações no Apple Configurator 2. A URL de registro é o nome de domínio totalmente qualificado (FQDN) do XenMobile Server, como `mdm.server.url.com`, ou o endereço IP.
4. Para impedir que dispositivos desconhecidos se registrem, defina **Exigir cadastro do dispositivos antes do registro** como **Sim**. Nota: se essa configuração for **Sim**, você deverá adicionar os dispositivos configurados a **Gerenciar > Dispositivos** no XenMobile manualmente ou usando um arquivo CSV antes do registro.
5. Para exigir que os usuários de dispositivos iOS insiram suas credenciais ao se registrarem, defina **Exigir credenciais para registro de dispositivo** como **Sim**. O padrão é não exigir credenciais para o registro.
6. Nota: se o XenMobile Server estiver usando um certificado SSL confiável, ignore essa etapa. Clique em **Exportar certificados de âncora** e salve o arquivo `certchain.pem` nas chaves do macOS (login ou System).



Etapa 2: Definir configurações no Apple Configurator 2

1. Instale o Apple Configurator 2 a partir da App Store.
2. Use um Cabo Dock Connector para USB para conectar os dispositivos ao Mac que executa o Apple Configurator 2. Você pode configurar até 30 dispositivos conectados simultaneamente. Se você não tiver um Dock Connector, use um ou mais hubs de alta velocidade USB 2.0 alimentados para conectar os dispositivos.
3. Inicie o Apple Configurator 2. O configurador mostra todos os dispositivos que você pode preparar para supervisão.
4. Para preparar um dispositivo para supervisão:
 - Selecione **Supervise devices** se você pretende manter o controle do dispositivo reaplicando uma configuração regularmente. Clique em **Avançar**.

Importante:

Colocar um dispositivo no modo supervisionado instala a versão selecionada do iOS no dispositivo, apagando completamente os dados ou os aplicativos do usuário armazenados anteriormente.

- No iOS, clique em **Latest** para obter a versão mais recente do iOS que você deseja instalar.
5. Em **Enroll in MDM Server**, escolha um servidor MDM. Para adicionar um novo servidor, clique em **Next**

6. Em **Define an MDM server**, forneça um nome para o servidor e cole a URL do servidor MDM no console XenMobile.
7. Em **Assign to organization**, escolha uma organização para supervisionar o dispositivo.
Para obter mais informações sobre como preparar os dispositivos com o Apple Configurator 2, consulte a página de ajuda do Apple Configurator, [Prepare devices](#).
8. À medida que cada dispositivo for preparado, ligue-o para iniciar o Assistente de Instalação do iOS, que prepara o dispositivo para ser usado pela primeira vez.

Para atribuir dispositivos do Apple Configurator 2 ao Apple Business Manager

Você pode associar dispositivos iPhone e iPad do Apple Configurator 2 à sua conta do Apple Business Manager. Quando você adiciona dispositivos, eles aparecem na seção **Devices**. Esses dispositivos já não incluem mais configurações de registro atribuídas através do Apple Configurator 2. Para obter mais informações, consulte [Atribuir dispositivos adicionados do Apple Configurator 2 ao Apple Business Manager](#).

Renovar ou atualizar certificados ao usar o Programa de Implantação da Apple

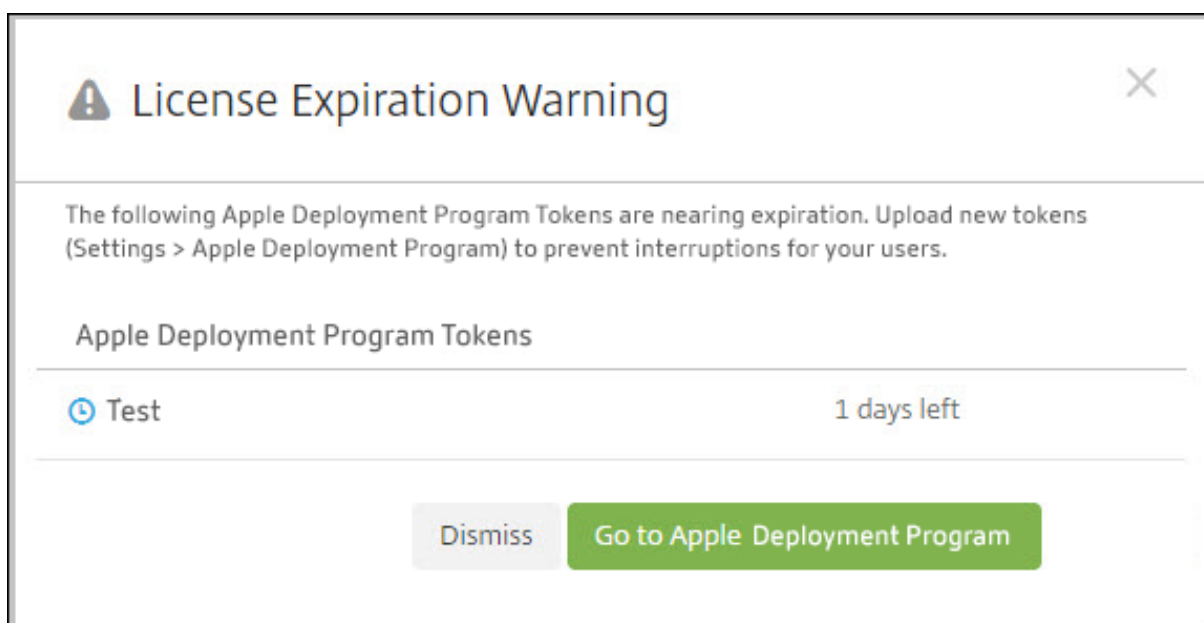
Quando o certificado Secure Sockets Layer (SSL) do XenMobile é renovado, você carrega um novo certificado no console XenMobile em **Configurações > Certificados**. Na caixa de diálogo **Importar**, em **Usar como**, clique em **Ouvinte SSL** para que o certificado seja usado para SSL. Depois que você reiniciar o servidor, o XenMobile usará o novo certificado SSL. Para obter mais informações sobre certificados no XenMobile, consulte [Carregando certificados para o XenMobile](#).

Não é necessário restabelecer a relação de confiança entre o Programa de implantação da Apple e o XenMobile quando você renova ou atualiza o certificado SSL. Você pode, no entanto, redefinir as configurações do seu **Programa de Implantação da Apple** a qualquer momento seguindo as etapas anteriores neste artigo.

Para obter mais informações sobre o Programa de implantação da Apple, consulte a [Documentação da Apple](#).

Renovar sua conexão entre o Programa de implantação da Apple e o XenMobile

O XenMobile exibe um aviso de expiração de licença quando o token do servidor de registro automatizado de dispositivo expira.



Substitua o token do Apple School Manager/Apple Business Manager.

Etapa 1: baixe uma chave pública do XenMobile Server

1. No console XenMobile, vá para **Configurações > Programa de implantação da Apple** para baixar uma nova chave pública.

Etapa 2: crie e baixe um arquivo de token de servidor da sua conta da Apple

1. Faça logon no Apple Business Manager para baixar o token.
2. Abra **Settings** e selecione o servidor do qual você precisa de um token. Clique em **Edit**.
3. Em **MDM Server Settings**, carregue a nova chave pública que você baixou do XenMobile e salve as alterações.
4. Clique em **Download Token** para baixar o novo token.

Etapa 3: carregue um arquivo de token de servidor para o XenMobile

1. No Citrix XenMobile, vá para **Configurações > Programa de Implantação da Apple**.
2. Selecione a conta do Programa de Implantação, clique em **Editar** e carregue o arquivo de token do servidor.
3. Clique em **Avançar** e salve as alterações.

Propriedades do cliente

April 26, 2021

As propriedades do cliente contêm informações que são fornecidas diretamente para o Secure Hub em dispositivos de usuários. Você pode usar essas propriedades para definir configurações avançadas, como PIN da Citrix. Obtenha as propriedades do cliente junto ao suporte da Citrix.

As propriedades do cliente estão sujeitas a alterações a cada versão do Secure Hub e, ocasionalmente, em aplicativos clientes. Para obter detalhes sobre as propriedades do cliente mais comumente configuradas, consulte Referência da propriedade de cliente, posteriormente neste artigo.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida.
2. Em **Cliente**, clique em **Propriedades do cliente**. A página **Propriedades do cliente** é exibida. Você pode adicionar, editar e excluir propriedades do cliente nessa página.

Settings > Client Properties

Client Properties
To change a property, select the property and then click Edit.

Add

<input type="checkbox"/>	Name	Key	Value	Description
<input type="checkbox"/>	Enable Citrix PIN Authentication	ENABLE_PASSCODE_AUTH	false	Enable Citrix PIN Authentication
<input type="checkbox"/>	Enable User Password Caching	ENABLE_PASSWORD_CACHING	false	Enable User Password Caching
<input type="checkbox"/>	Encrypt secrets using Passcode	ENCRYPT_SECRETS_USING_PASSCODE	false	Encrypt secrets using Pin or AD password
<input type="checkbox"/>	PIN Strength Requirement	PASSCODE_TYPE	Numeric	PIN Strength Requirement
<input type="checkbox"/>	PIN Type	PASSCODE_STRENGTH	Medium	PIN Type
<input type="checkbox"/>	PIN Length Requirement	PASSCODE_MIN_LENGTH	6	PIN Length Requirement
<input type="checkbox"/>	PIN Change Requirement	PASSCODE_EXPIRY	90	PIN Change Requirement
<input type="checkbox"/>	PIN History	PASSCODE_HISTORY	5	PIN History
<input type="checkbox"/>	Inactivity Timer	INACTIVITY_TIMER	15	Inactivity Timer
<input type="checkbox"/>	Enable FIPS Mode	ENABLE_FIPS_MODE	false	Enable FIPS Mode

Para adicionar uma propriedade do cliente

1. Clique em **Adicionar**. A página **Adicionar nova propriedade de cliente** é exibida.

Settings > Client Properties > Add New Client Property

Add New Client Property

Key ?

Value*

Name*

Description*

2. Defina estas configurações:

- **Chave:** na lista, clique na chave de propriedade que você deseja adicionar. Importante: entre em contato com o suporte Citrix antes de atualizar as configurações. Você pode solicitar uma chave especial.
- **Valor:** o valor da propriedade selecionada.
- **Nome:** um nome para a propriedade.
- **Descrição:** uma descrição da propriedade.

3. Clique em **Salvar**.

Para editar uma propriedade do cliente

1. Na tabela **Propriedades do cliente**, selecione a propriedade do cliente que você deseja editar.

Quando você marca a caixa de seleção ao lado de uma propriedade de cliente, o menu de opções é exibido acima da lista de propriedades do cliente. Quando você clica em qualquer outro lugar da lista, o menu de opções é exibido no lado direito da listagem.

2. Clique em **Editar**. A página **Editar propriedade do cliente** é exibida.

Settings > Client Properties > Edit Client Property

Edit Client Property

Key: ENABLE_PASSCODE_AUTH

Value*: true

Name*: Enable Citrix PIN Authentication

Description*: Enable Citrix PIN Authentication

3. Altere as seguintes informações conforme apropriado:
 - **Chave:** você não pode alterar esse campo.
 - **Valor:** o valor da propriedade.
 - **Nome:** o nome da propriedade.
 - **Descrição:** a descrição da propriedade.
4. Clique em **Salvar** para salvar suas alterações ou em **Cancelar** para deixar a propriedade inalterada.

Para excluir uma propriedade do cliente

1. Na tabela **Propriedades do cliente**, selecione a propriedade do cliente que você deseja excluir. Você pode selecionar mais de uma propriedade para excluir marcando a caixa de seleção ao lado de cada propriedade.
2. Clique em **Excluir**. Uma caixa de diálogo de confirmação é exibida. Clique em **Excluir** novamente.

Referência da propriedade de cliente

As propriedades de cliente predefinidas do XenMobile e suas configurações padrão estão descritas abaixo.

- **CONTAINER_SELF_DESTRUCT_PERIOD**
 - Nome de exibição: Período de autodestruição do contêiner de MDX
 - A autodestruição impede o acesso ao Secure Hub e aos aplicativos gerenciados, após um determinado número de dias de inatividade. Depois do limite de tempo, os aplicativos deixam de ser utilizáveis. Apagar os dados inclui limpar os dados de cada aplicativo instalado, incluindo o cache do aplicativo e os dados do usuário.

O tempo de inatividade é quando o servidor não recebe uma solicitação de autenticação para validar o usuário em um determinado período de tempo. Por exemplo, se essa

política for de 30 dias e o usuário não usar os aplicativos por mais de 30 dias, a política entrará em vigor.

Essa política de segurança global é aplicável às plataformas iOS e Android e é um aprimoramento das políticas existentes de bloqueio e apagamento de aplicativos.

- Para configurar essa política global, vá até **Configurações > Propriedades do cliente** e adicione a chave personalizada **CONTAINER_SELF_DESTRUCT_PERIOD**.
- Valor: número de dias

- **DEVICE_LOGS_TO_IT_HELP_DESK**

- Nome de exibição: Enviar logs do dispositivo para o suporte técnico de TI
- Essa propriedade ativa ou desativa a capacidade de enviar os logs para o suporte técnico de TI.
- Valores possíveis: **true** ou **false**
- Valor padrão: **false**

- **DISABLE_LOGGING**

- Nome de exibição: Desativar log
- Use esta propriedade para impedir que os usuários colem e enviem logs de seus dispositivos. Esta propriedade desativa o registro em log no Secure Hub e para todos os aplicativos MDX instalados. Os usuários não podem enviar logs para nenhum aplicativo na página de Suporte. Embora a caixa de diálogo de composição de email seja exibida, os logs não são anexados. Uma mensagem indica que o registro em log está desativado. Esta configuração também evita que você atualize as configurações de log no console XenMobile para aplicativos do Secure Hub e MDX.

Quando esta propriedade está definida como **true**, o Secure Hub define **Bloquear logs de aplicativo** como **true**. Como resultado, os aplicativos MDX param o registro em log quando a nova política é aplicada.

- Valores possíveis: **true** ou **false**
- Valor padrão: **false** (a geração de log não é desativada)

- **ENABLE_CRASH_REPORTING**

- Nome de exibição: Ativar relatórios de falhas
- Se for **true**, a Citrix coletará relatórios e diagnósticos de falhas para ajudar a solucionar problemas com o Secure Hub para iOS e Android. Se for **false**, não haverá coleta de dados.
- Valores possíveis: **true** ou **false**
- Valor padrão: **true**

- **ENABLE_CREDENTIAL_STORE**

- Nome de exibição: ativar armazenamento de credenciais
- Com a ativação do armazenamento de credenciais, os usuários de Android ou iOS informam a senha uma única vez ao acessarem os aplicativos móveis de produtividade. Você pode usar o armazenamento de credenciais independentemente da ativação ou não do PIN da Citrix. Se você não ativar o PIN da Citrix, os usuários devem digitar a senha do Active Directory. O XenMobile dá suporte ao uso de senhas do Active Directory com o armazenamento de credenciais somente para o Secure Hub e os aplicativos de loja pública. Se você usa senhas do Active Directory com o armazenamento de credenciais, o XenMobile não dá suporte à autenticação de PKI.
- O registro automático no Secure Mail requer que você defina esta propriedade como **true**.
- Para configurar essa política de cliente personalizada, vá para **Configurações > Propriedades do cliente**, adicione a chave personalizada **ENABLE_CREDENTIAL_STORE** e defina o **Valor** como **true**.

- **ENABLE_FIPS_MODE**

- Nome de exibição: ativar o modo FIPS
- Essa propriedade ativa ou desativa o modo FIPS em dispositivos móveis. Depois de alterar o valor, o Secure Hub passa o novo valor para o dispositivo quando o Secure Hub não a autenticação online Avançar.
- Valores possíveis: **true** ou **false**
- Valor padrão: **false**

- **ENABLE_PASSCODE_AUTH**

- Nome de exibição: ativar Autenticação do Citrix PIN
- Essa propriedade permite que você ative a funcionalidade do PIN da Citrix. Com o PIN ou código secreto da Citrix, os usuários são solicitados a definir um PIN a ser usado em vez da senha do Active Directory. Essa configuração é ativada automaticamente quando a **ENABLE_PASSWORD_CACHING** está ativada, ou quando o XenMobile está usando a autenticação de certificado.

Para a autenticação offline, o PIN da Citrix será validado localmente e os usuários terão permissão para acessar o aplicativo ou o conteúdo que eles solicitaram. Para a autenticação online, o PIN ou código secreto da Citrix desbloqueará a senha ou o certificado do Active Directory, que é enviado para realizar a autenticação no XenMobile.

Se **ENABLE_PASSCODE_AUTH** for **true** e **ENABLE_PASSWORD_CACHING** for **false**, a autenticação online sempre solicitará a senha porque o Secure Hub não a salva.

- Valores possíveis: **true** ou **false**
- Valor padrão: **false**

- **ENABLE_PASSWORD_CACHING**

- Nome de exibição: ativar Armazenamento em Cache de Senha do Usuário
- Esta propriedade permite as senhas do Active Directory sejam armazenadas em cache localmente no dispositivo móvel. Quando você define essa propriedade como **true**, também deve definir a propriedade **ENABLE_PASSCODE_AUTH** como **true**. Com o cache de senha de usuário ativado, o XenMobile avisa aos usuários para configurar um PIN ou código secreto da Citrix.
- Valores possíveis: **true** ou **false**
- Valor padrão: **false**

- **ENABLE_TOUCH_ID_AUTH**

- Nome de exibição: Ativar Autenticação de Touch ID
- Em dispositivos que dão suporte à autenticação Touch ID, essa propriedade ativa ou desativa a autenticação Touch ID no dispositivo. Requisitos:

Os dispositivos de usuário devem ter o PIN ou LDAP da Citrix ativado. Se a autenticação LDAP estiver desativada (por exemplo, porque somente a autenticação baseada em certificados é usada), os usuários deverão definir um PIN da Citrix. Nesse caso, o XenMobile exige o PIN da Citrix mesmo que a propriedade do cliente **ENABLE_PASSCODE_AUTH** seja **false**.

Defina **ENABLE_PASSCODE_AUTH** como **false** para que, quando os usuários iniciarem um aplicativo, eles devam responder a uma solicitação para usar o Touch ID.

- Valores possíveis: **true** ou **false**
- Valor padrão: **false**

- **ENABLE_WORXHOME_CEIP**

- Nome de exibição: Ativar CEIP do Worx Home
- Essa propriedade ativa o Programa de Melhoria de Experiência do Cliente. Esse recurso envia dados de configuração e de uso anônimos para a Citrix periodicamente. Os dados ajudam a Citrix a melhorar a qualidade, a confiabilidade e o desempenho do XenMobile.
- Valor: **true** ou **false**
- Valor padrão: **false**

- **ENABLE_WORXHOME_GA**

- Nome de exibição: Ativar o Google Analytics no Worx Home
- Essa propriedade ativa ou desativa a capacidade de coletar dados usando o Google Analytics no Secure Hub. Quando você alterar essa configuração, o novo valor será definido somente quando o usuário fizer login novamente no Secure Hub (chamado anteriormente Worx Home).
- Valores possíveis: **true** ou **false**
- Valor padrão: **true**

- **ENCRYPT_SECRETS_USING_PASSCODE**

- Nome de exibição: Criptografar segredos usando o Código Secreto
- Essa propriedade armazena dados confidenciais no dispositivo em um cofre secreto em vez de em um armazenamento nativo baseada na plataforma, como as chaves do iOS. Esta propriedade permite uma forte criptografia de artefatos-chave e adiciona entropia de usuário. A entropia de usuário é um código PIN aleatório gerado pelo usuário que apenas o usuário conhece.

A Citrix recomenda que você ative essa propriedade para ajudar a proporcionar maior segurança nos dispositivos de usuário. Como resultado, os usuários recebem mais pedidos de autenticação para o PIN da Citrix.

- Valores possíveis: **true** ou **false**
- Valor padrão: **false**

- **INACTIVITY_TIMER**

- Nome de exibição: Timer de Inatividade
- Essa propriedade define por quanto tempo os usuários podem deixar seus dispositivos inativos e acessar um aplicativo sem que lhes seja solicitado um PIN ou código secreto da Citrix. Para ativar essa configuração em um aplicativo MDX, defina a política Código Secreto do Aplicativo como Ativado. Se a configuração de código secreto de aplicativo estiver definida como Desativado, os usuários serão redirecionados para o Secure Hub para efetuar uma autenticação completa. Quando você altera essa configuração, o valor entra em vigor na próxima vez em que houver solicitação para que os usuários se autentiquem.

No iOS, o Timer de Inatividade também rege o acesso ao Secure Hub para aplicativos MDX e não MDX.

- Valores possíveis: qualquer número inteiro positivo
- Valor padrão: **15** (minutos)

- **ON_FAILURE_USE_EMAIL**

- Nome de exibição: Em caso de falha use email para enviar logs do dispositivo para o suporte técnico de TI
- Essa chave ativa ou desativa a capacidade de usar emails para enviar os logs do dispositivo para a TI.
- Valores possíveis: **true** ou **false**
- Valor padrão: **true**

- **PASSCODE_EXPIRY**

- Nome de exibição: Requisito de troca do PIN

- Essa propriedade define por quanto tempo o PIN ou código secreto da Citrix é válido, após o qual o usuário é forçado a alterar seu PIN ou código secreto da Citrix. Quando você alterar essa configuração, o novo valor será definido somente quando o PIN ou código secreto da Citrix atual expirar.
 - Valores possíveis: **1** até **99** recomendados. Para eliminar redefinições de PINs, defina o valor como um número muito alto (por exemplo, 100.000.000.000). Se você definiu originalmente o período de expiração entre 1 e 99 dias e depois mudou para o número grande durante esse período, os PINs ainda expirarão no final do período inicial, mas nunca mais expirarão novamente.
 - Valor padrão: **90** (dias)
- **PASSCODE_HISTORY**
 - Nome de exibição: Histórico de PIN
 - Essa propriedade define o número de PINs ou códigos secretos da Citrix usados anteriormente que os usuários não podem reutilizar quando mudam o PIN ou código secreto da Citrix. Quando você alterar essa configuração, o novo valor será definido somente na próxima vez em que os usuários reiniciarem o PIN ou código secreto da Citrix.
 - Valores possíveis: **1** até **99**
 - Valor padrão: **5**
- **PASSCODE_MAX_ATTEMPTS**
 - Nome de exibição: Tentativas de PIN
 - Essa propriedade define quantas tentativas erradas de PIN ou código secreto da Citrix os usuários podem fazer antes que a autenticação completa seja solicitada. Depois que os usuários executam com êxito uma autenticação completa, eles são solicitados a criar um PIN ou código secreto da Citrix.
 - Valores possíveis: qualquer número inteiro positivo
 - Valor padrão: **15**
- **PASSCODE_MIN_LENGTH**
 - Nome de exibição: Requisito de comprimento do PIN
 - Essa propriedade define o comprimento mínimo de PINs da Citrix.
 - Valores possíveis: **4** a **10**
 - Valor padrão: **6**
- **PASSCODE_STRENGTH**
 - Nome de exibição: requisito de Força do PIN
 - Essa propriedade define a força do PIN ou código secreto da Citrix. Quando você alterar essa configuração, os usuários serão solicitados a criar um PIN ou código secreto da Citrix na próxima vez em que eles forem solicitados a autenticar.
 - Valores possíveis: **Baixa**, **Média**, **Alta** ou **Forte**

- Valor padrão: **Média**
- As regras de senha para cada configuração de força baseada na configuração PASS-CODE_TYPE são as seguintes:

Regras para códigos secretos numéricos:

Força do código secreto	Regras para o tipo de senha numérica	Permitido	Não permitido
Baixo	Todos os números, qualquer sequência permitida	444444, 123456, 654321	
Média (configuração padrão)	Os números não podem ser todos consecutivos nem os mesmos.	444333, 124567, 136790, 555556, 788888	444444, 123456, 654321
Alta	Números adjacentes não podem ser iguais.	123512, 134134, 132312, 131313, 987456	080080, 112233, 135579, 987745, 919199
Forte	Não use o mesmo número mais de duas vezes. Não use três ou mais números consecutivos seguidos. Não use três ou mais números consecutivos na ordem inversa.	102983, 085085, 824673, 132312	132132, 131313, 902030

Regras para códigos secretos alfanuméricos:

Força do código secreto	Regras para tipos de códigos secretos alfanuméricos	Permitido	Não permitido
Baixo	Deve conter pelo menos um número e uma letra	aa11b1, Abcd1#, Ab123~, aaaa11, aa11aa	AAAaaa, aaaaaa, abcdef

Força do código secreto	Regras para tipos de códigos secretos alfanuméricos		
	Permitido	Não permitido	
Média (configuração padrão)	Além das regras para a força de código secreto baixa, as letras e todos os números não podem ser os mesmos. As letras e os números não podem ser consecutivos.	aa11b1, aaa11b, aaa1b2, abc145, xyz135, sdf123, ab12c3, a1b2c3, Abcd1#, Ab123~	aaaa11, aa11aa ou aaa111; abcd12, bcd123, 123abc, xy1234, xyz345 ou cba123
Alta	Incluir pelo menos uma letra maiúscula e uma letra minúscula.	Abcd12, jkrtA2, 23Bc#, AbCd	abcd12, DFGH2
Forte	Incluir pelo menos um número, um símbolo especial, uma letra maiúscula e uma letra minúscula.	Abcd1#, Ab123~, xY12#3, Car12#, AAbc1#	abcd12, Abcd12, dfgh12, jkrtA2

• PASSCODE_TYPE

- Nome de exibição: Tipo de PIN
- Essa propriedade define se os usuários são capazes de definir um PIN numérico ou um código secreto alfanumérico da Citrix. Quando você seleciona **Numérico**, os usuários podem usar apenas números (PIN da Citrix). Quando você seleciona **Alfanumérico**, os usuários podem usar uma combinação de letras e números para o código secreto.

Se você alterar essa configuração, os usuários deverão definir um novo PIN ou código secreto da Citrix na próxima vez em que eles forem solicitados a autenticar.

- Valores possíveis: **Numérico** ou **Alfanumérico**
- Valor padrão: **Numérico**

• REFRESHINTERVAL

- Nome de exibição: REFRESHINTERVAL
- Por padrão, o XenMobile ping Auto Discovery servidor (ADS) para os certificados fixados cada 3 dias. Para alterar o intervalo de atualização, vá para **Configurações > Propriedades do cliente**, adicione a chave personalizada **REFRESHINTERVAL** e defina o

Valor como o número de horas.

- Valor padrão: **72** horas (3 dias)

- **SEND_LDAP_ATTRIBUTES**

- Para implantações de somente MAM de dispositivos Android, iOS ou macOS: você pode configurar o XenMobile para que os usuários que se registrarem no Secure Hub com credenciais de email sejam automaticamente registrados no Secure Mail. Como resultado, os usuários não fornecem informações adicionais ou tomam medidas extras para se registrar no Secure Mail.

- Para configurar essa política global de cliente, vá para **Configurações > Propriedades do cliente**, adicione a chave personalizada **SEND_LDAP_ATTRIBUTES** e defina o **Valor** da seguinte maneira.

- Valor: `userPrincipalName=${ user.userprincipalname } ,sAMAccountName=${ user.samaccountname } , displayName=${ user.displayName } ,mail=${ user.mail }`

- Os valores de atributo estão especificados como macros, semelhante a políticas MDM.

- Aqui está um exemplo de resposta de serviço de conta de exemplo para esta propriedade:

```
<property value="userPrincipalName=user@site.com,sAMAccountName=eng1,displayName=user\,test1,email=user@site.com\,user@site.com" name="SEND_LDAP_ATTRIBUTES"/>
```

- Para esta propriedade, XenMobile trata caracteres de vírgula como terminadores de sequências de caracteres. Portanto, se um valor de atributo incluir uma vírgula, preceda-a com uma barra invertida. A barra invertida impede que o cliente interprete a vírgula inserida como o fim do valor do atributo. Represente caracteres de barra invertida com `"\"`.

- **HIDE_THREE_FINGER_TAP_MENU**

- Quando essa propriedade não estiver configurada ou estiver definida como **false**, os usuários podem acessar o menu de recursos ocultos executando um toque de três dedos em seus dispositivos. O menu de recursos ocultos permitia aos usuários redefinir os dados do aplicativo. Definir esta propriedade como **true** desabilita o acesso dos usuários ao menu de recursos ocultos.

- Para configurar essa política global de cliente, vá para **Configurações > Propriedades do cliente**, adicione a chave personalizada **HIDE_THREE_FINGER_TAP_MENU** e defina o **Valor**.

- **TUNNEL_EXCLUDE_DOMAINS**

- Nome de exibição: Tunnel Exclude Domains

- Por padrão, o MDX exclui do encapsulamento de micro VPN alguns pontos de extremidade de serviço que XenMobile SDKs e aplicativos usam para vários recursos. Por exemplo, os pontos de extremidade incluem serviços que não exigem roteamento por meio de redes corporativas, como o Google Analytics, serviços do Citrix Cloud e serviços do Active Directory. Use essa propriedade de cliente para substituir a lista padrão de domínios excluídos.
- Para configurar essa política global de cliente, vá para **Configurações > Propriedades do cliente**, adicione a chave personalizada **TUNNEL_EXCLUDE_DOMAINS** e defina o **Valor**.
- Valor: para substituir a lista padrão pelos domínios que deseja excluir do encapsulamento, digite uma lista de sufixos de domínio separados por vírgulas. Para incluir todos os domínios em encapsulamento, digite **none**. O padrão é:

```
app.launchdarkly.com,cis.citrix.com,cis-staging.citrix.com,cis-test.citrix.com,clientstream,launchdarkly.com,crashlytics.com,events.launchdarkly.com,fabric.io,firehose.launchdarkly.com, hockeyapp.net ,mobile.launchdarkly.com,pushreg.xml.citrix.com,rttf.citrix.com,rttf-staging.citrix.com,rttf-test.citrix.com,ssl.google-analytics.com,stream.launchdarkly.com
```

Implantar dispositivos através do Programa de Implantação da Apple

April 26, 2021

A Apple possui programas de registro de dispositivos para contas de negócios e educação. Para contas de negócios, você se registra no Programa de Implantação da Apple. para usar o Apple Business Manager (ABM) ou o Apple School Manager (ASM) para registro e gerenciamento de dispositivos no XenMobile. Esse programa é para dispositivos iOS, iPadOS e macOS.

O Programa de Implantação da Apple está disponível para organizações e não pessoas. Você deve fornecer uma quantidade considerável de detalhes e informações corporativas para criar uma conta do Programa de Implantação da Apple. Portanto, o processo de solicitação e recebimento de aprovação para contas pode ser demorado.

Para contas de educação, você cria uma conta do Apple School Manager. O ASM unifica o Programa de Implantação da Apple e a compra por volume da Apple. Para criar uma conta do Apple School Manager, acesse o [site da Apple School](#).

Cadastrar-se no Programa de Implantação da Apple

Para se registrar no Apple Business Manager, acesse business.apple.com. Clique em **Enroll now** para solicitar uma nova conta. A prática recomendada é usar um endereço de e-mail relacionado à organi-

zação, como implantação@empresa.com. O processo de registro pode levar alguns dias. Depois de receber as credenciais de login, siga as etapas fornecidas no Apple Business Manager para criar uma conta.

Nota:

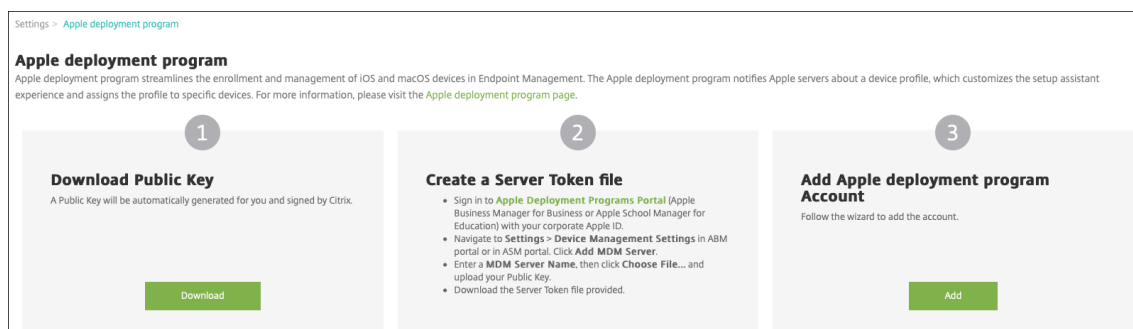
Para contas de educação, consulte [Integração com os recursos do Apple Educação](#).

Conectar sua conta do Apple Business Manager ao XenMobile

Para conectar sua conta do Apple Business Manager à implantação do XenMobile, insira as informações no console XenMobile e no Apple Business Manager. Siga esses passos:

Etapa 1: baixe uma chave pública do XenMobile Server

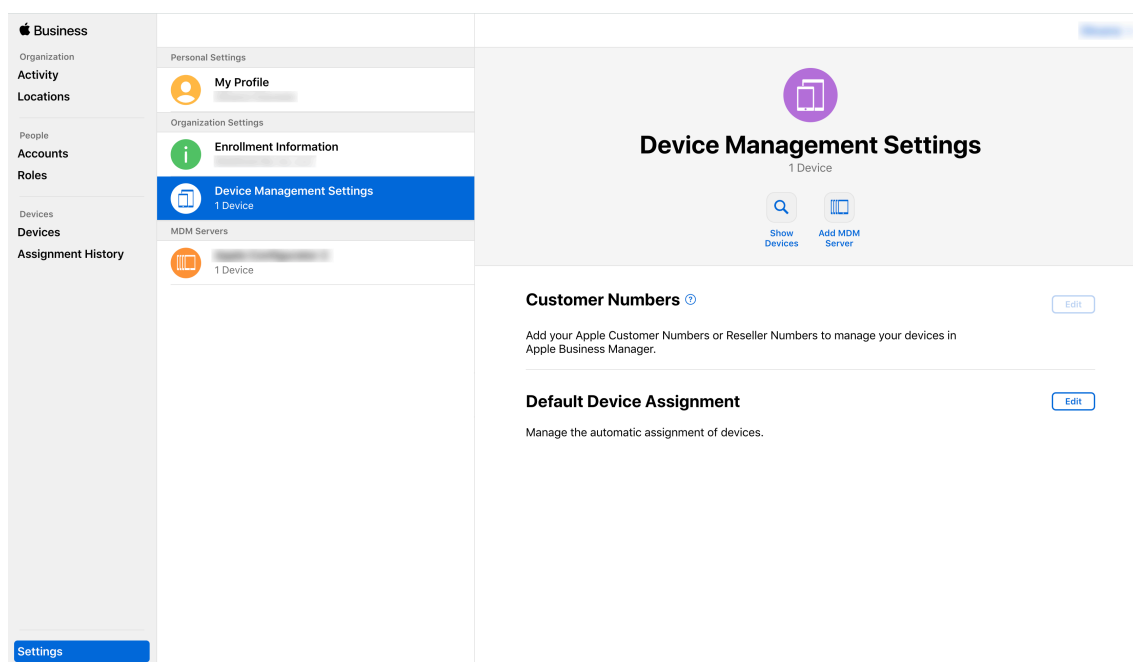
1. No console XenMobile, vá para **Configurações > Programa de implantação da Apple**.



2. Em **Baixar chave pública**, clique em **Baixar**.

Etapa 2: crie e baixe um arquivo de token de servidor da sua conta da Apple

1. Faça login no [Apple Business Manager](#) usando uma conta de administrador ou gerente de registro de dispositivo.
2. Na parte inferior da barra lateral, clique em **Configurações** e, em seguida, clique em **Configurações de gerenciamento de dispositivos > Adicionar servidor MDM**.



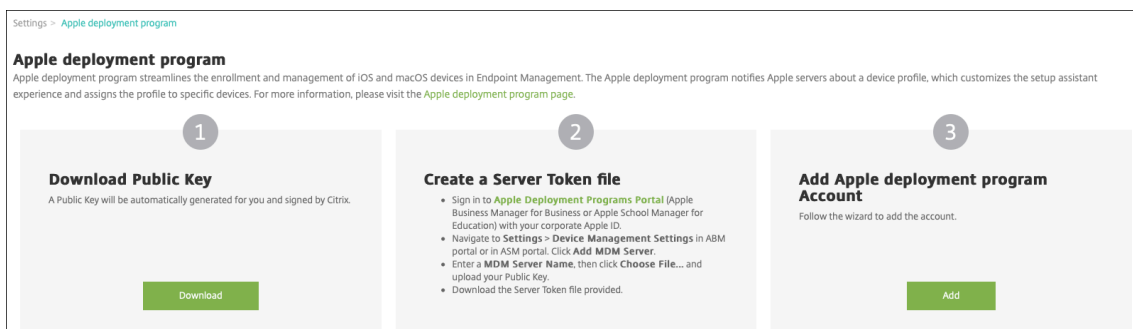
3. Na configuração de **Nome do servidor MDM**, digite um nome para o servidor XenMobile. O nome do servidor que você digita é para sua referência. Não é a URL ou nome do servidor.
4. Em **Upload Public Key**, clique em **Choose File**. Carregue a chave pública que você baixou do XenMobile e salve as alterações.
5. Clique em **Download Token** para baixar o arquivo de token do servidor para o seu computador. Você deve carregar o arquivo de token de servidor ao adicionar a conta ABM ao XenMobile. As informações de token do ABM são exibidas no console XenMobile depois que você importa o arquivo de token.
6. Em **Default Device Assignment**, clique em **Change**. Escolha como deseja atribuir dispositivos e, em seguida, forneça as informações solicitadas. Para obter informações, consulte o [Guia do usuário do ABM](#).

Etapa 3: adicione uma conta ABM ao XenMobile

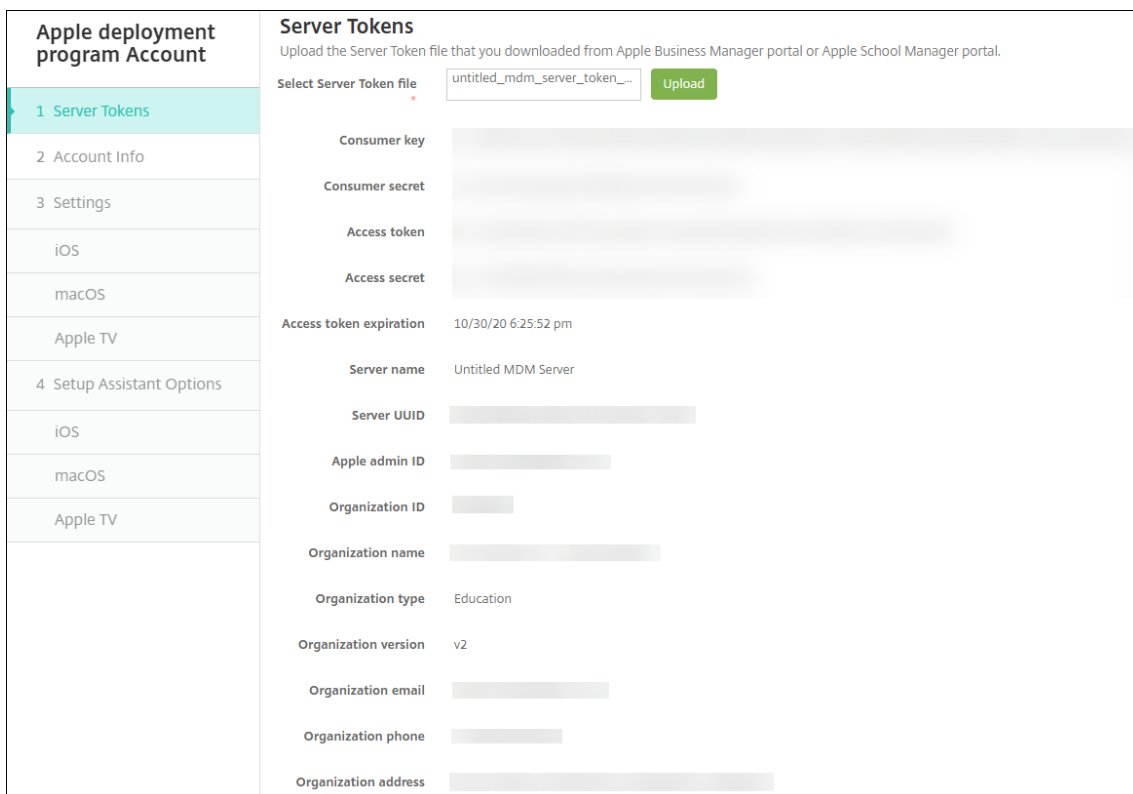
Você pode adicionar várias contas ABM ao XenMobile. Este recurso permite usar diversas configurações de registro e opções de assistente de configuração por país, departamento e assim por diante. Em seguida, você associa contas ABM a diferentes políticas de dispositivo.

Por exemplo, você pode centralizar a todas as suas contas ABM de diferentes países no mesmo servidor XenMobile, para importar e supervisionar todos os dispositivos ABM. Ao personalizar as configurações de registro e as opções do assistente de instalação por departamento, hierarquia organizacional ou outra estrutura, as políticas oferecem funcionalidades apropriadas para toda a organização e os usuários recebem a assistência apropriada.

1. No console XenMobile, vá para **Configurações > Programa de implantação da Apple** e, em **Adicionar conta do programa de implantação da Apple**, clique em **Adicionar**.



2. Na página **Tokens de servidor**, especifique o arquivo de token de servidor e clique em **Carregar**.



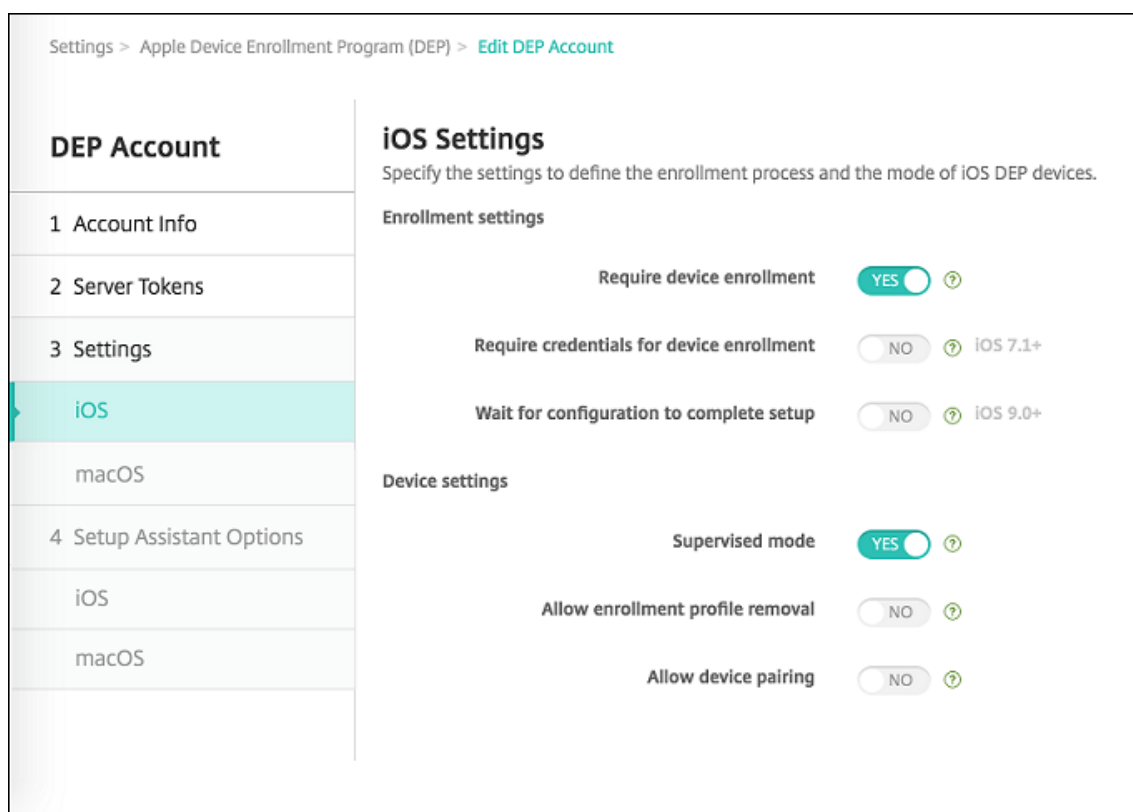
Suas informações de token de servidor são exibidas.

3. Na página **Informações sobre a conta**, especifique estas configurações:

Apple deployment program Account	Account Info
1 Server Tokens	Specify your Apple deployment program account information.
2 Account Info	<p>Apple deployment program account name * <input type="text" value="ASM Deployment"/></p> <p>Business/Education unit * <input type="text" value="Central High School"/></p> <p>Unique service ID <input type="text" value="2359487"/></p> <p>Support phone number * <input type="text" value="555555555"/></p> <p>Support email address <input type="text"/></p> <p>Education suffix * <input type="text" value="suffix"/></p>
3 Settings	
iOS	
macOS	
Apple TV	
4 Setup Assistant Options	
iOS	
macOS	
Apple TV	

- **Nome da conta do Programa de Implantação da Apple:** um nome exclusivo para esta conta do Programa de Implantação da Apple. Use nomes que reflitam como você organiza contas do Programa de implantação da Apple, como por país ou hierarquia organizacional.
- **Unidade de negócios/educação:** a unidade de negócios ou o departamento ao qual o dispositivo é atribuído. Este campo é obrigatório.
- **ID de serviço exclusiva:** um ID exclusivo opcional para ajudar você a identificar ainda mais a conta.
- **Número de telefone de suporte:** um número de telefone de suporte para o qual os usuários ligam para pedir ajuda durante a instalação. Este campo é obrigatório.
- **Endereço de email de suporte:** um endereço de email de suporte opcional, disponível para os usuários finais.

4. Em **Configurações do iOS**, especifique estas configurações:



Configurações de registro:

- **Exigir registro de dispositivo:** selecione se os usuários devem ser obrigados a registrar seus dispositivos. O padrão é **Sim**.
- **Exigir credenciais para registro de dispositivo:** selecione se os usuários são obrigados a inserir as respectivas credenciais durante a configuração do ABM. A Citrix recomenda que você solicite a todos os usuários que insiram suas credenciais durante o registro do dispositivo, permitindo assim que apenas usuários autorizados registrem dispositivos. O padrão é **Sim**.

Quando você ativa o ABM antes da primeira configuração sem selecionar essa opção, o XenMobile cria os componentes do ABM. Essa criação inclui componentes como usuário ABM, Secure Hub, inventário de software e grupo de implantação ABM. Se você selecionar essa opção, o XenMobile não criará os componentes. Como resultado, se você desmarcar essa opção posteriormente, os usuários que não inseriram suas credenciais não poderão se registrar no ABM porque esses componentes do ABM não existirão. Nesse caso, para adicionar componentes do ABM desative e ative a conta ABM.

- **Aguardar que a configuração conclua a instalação:** selecione se os dispositivos dos usuários devem ser obrigados a permanecer no modo do Assistente de instalação até que todos os recursos do MDM sejam implantados no dispositivo. Essa configuração está disponível para dispositivos no modo supervisionado. O padrão é **Não**.

- A documentação da Apple declara que os seguintes comandos poderão não funcionar enquanto o dispositivo estiver no modo Assistente de Instalação:
 - InviteToProgram
 - InstallApplication
 - ApplyRedemptionCode
 - InstallMedia
 - RequestMirroring
 - DeviceLock

Configurações do dispositivo:

- **Modo supervisionado:** deverá ser definido como **Sim** se você estiver usando o Apple Configurator para gerenciar dispositivos registrados no ABM ou quando a opção **Aguardar que a configuração conclua a instalação** estiver ativada. O padrão é **Sim**. Para obter detalhes sobre como colocar um dispositivo iOS no modo supervisionado, consulte [Para colocar um dispositivo iOS no modo Supervisionado usando o Apple Configurator](#).
- **Permitir remoção do perfil de registro:** selecione se os dispositivos devem ter permissão para usar um perfil que você pode remover remotamente. O padrão é **Não**.
- **Permitir pareamento de dispositivo:** para dispositivos registrados por meio do ABM, selecione se você pode gerenciá-los usando a Apple Music e o Apple Configurator. O padrão é **Não**.

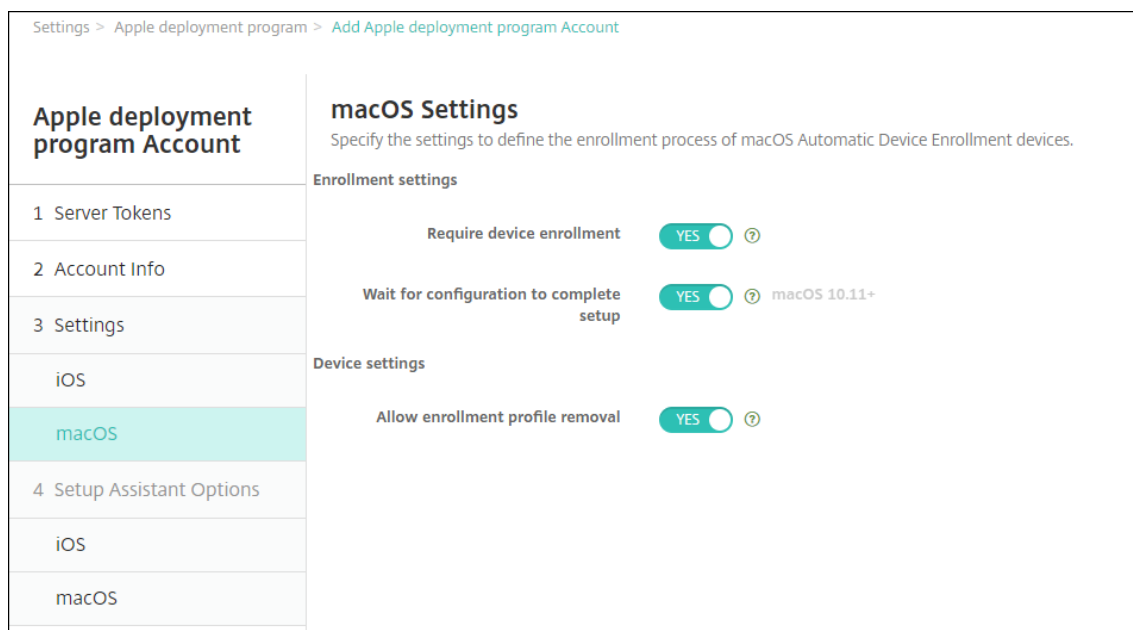
Identities de supervisão

Se você usar a ferramenta GroundControl, poderá adicionar um certificado para fazer o seguinte:

- Substituir restrições de emparelhamento para evitar o prompt “Confiar neste host”.
- Escalonar as ações do dispositivo gerenciado por USB para executar atividades como a instalação do perfil sem interação do usuário. Isso permite que o GroundControl habilite o modo de aplicativo único e o bloqueio do dispositivo na saída.
- Restaurar um backup para dispositivos ABM.

Para obter mais informações sobre o GroundControl, consulte [O site do GroundControl](#).

5. Em **Configurações do iOS**, especifique estas configurações:

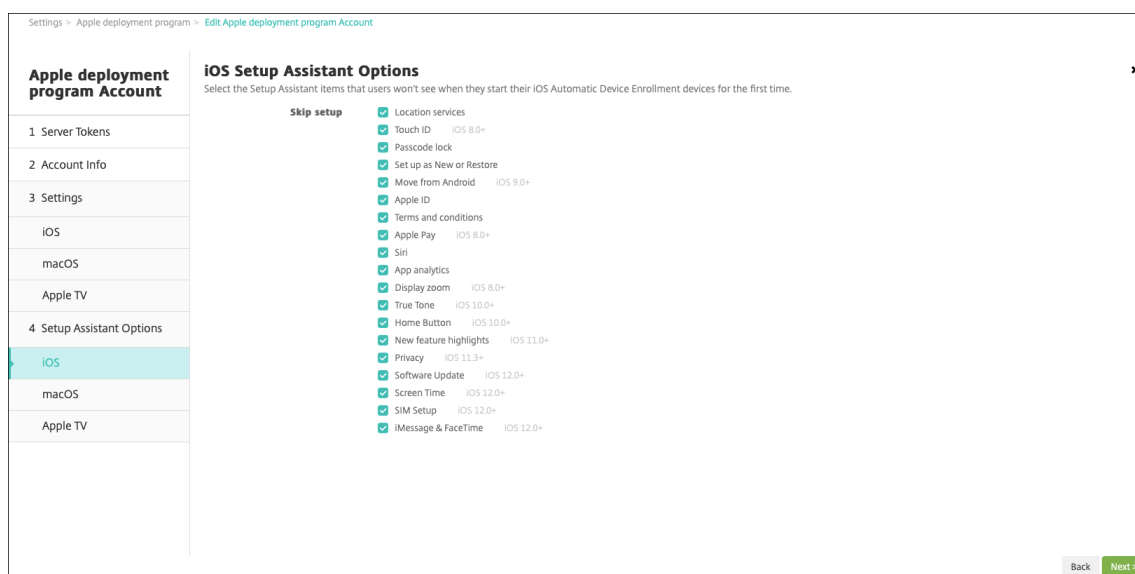


Configurações de registro:

- **Exigir registro de dispositivo:** selecione se os usuários devem ser obrigados a registrar seus dispositivos. O padrão é **Sim**.
- **Aguardar que a configuração conclua a instalação:** se a opção for **Sim**, o dispositivo macOS não continuará o assistente de instalação até que o código secreto de recursos do MDM seja implantado no dispositivo. Essa implantação ocorre antes de a criação da conta local. Essa configuração está disponível para dispositivos macOS 10.11 e versões posteriores. O padrão é **Não**.

Configurações do dispositivo:

- **Permitir remoção do perfil de registro:** selecione se os dispositivos devem ter permissão para usar um perfil que você pode remover remotamente. O padrão é **Não**.
6. Em **Opções do assistente de instalação do iOS**, selecione as etapas do Assistente de instalação do iOS que os usuários irão ignorar quando iniciarem seus dispositivos pela primeira vez. O padrão é desmarcar essa opção para todos os itens.

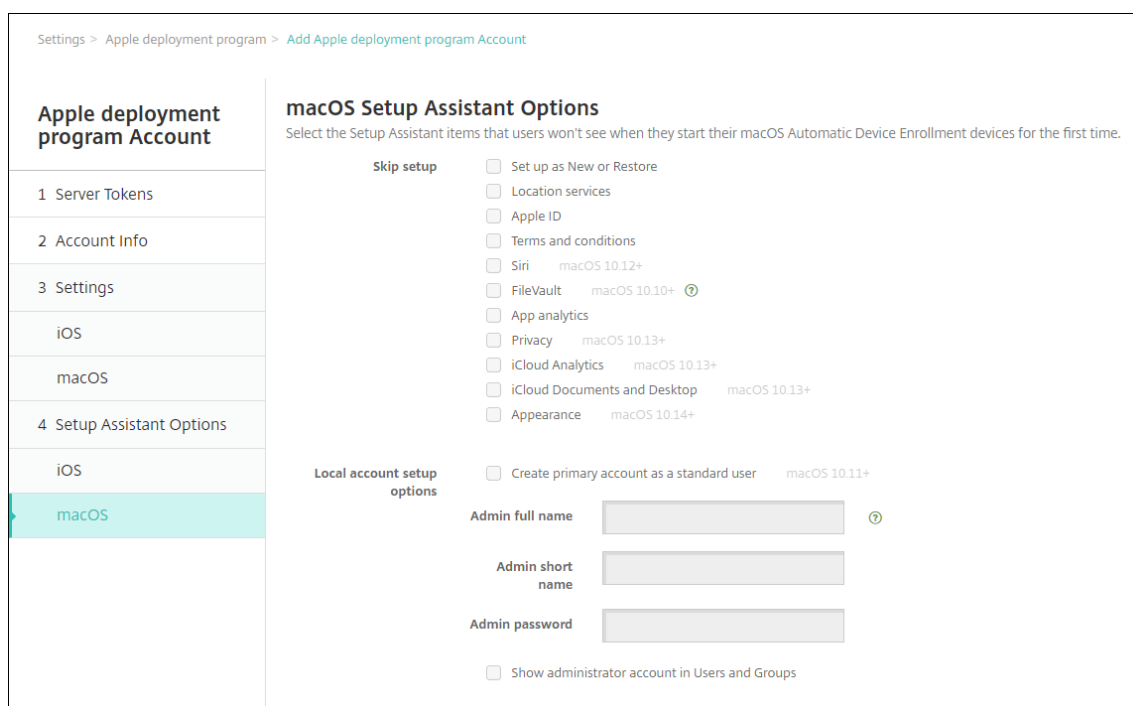


- **Serviços de localização:** configurar o serviço de localização no dispositivo.
- **Touch ID:** configurar o Touch ID nos dispositivos iOS.
- **Bloqueio de código secreto:** criar uma senha para o dispositivo.
- **Configurar como novo ou restaurar:** configurar o dispositivo como novo ou de um backup do iCloud ou da Apple App Store.
- **Mover do Android:** permitir a transferência de dados de um dispositivo Android para um dispositivo iOS. Essa opção está disponível somente quando **Configurar como novo ou restaurar** está selecionada (ou seja, a etapa é ignorada).
- **ID Apple:** configurar uma conta de ID Apple gerenciada para o dispositivo.
- **Termos e condições:** exigir que os usuários aceitem os termos e as condições de uso do dispositivo.
- **Apple Pay:** configurar o Apple Pay em dispositivos iOS.
- **Siri:** usar ou não a Siri no dispositivo.
- **Análise de aplicativo:** configurar se os dados de falha e as estatísticas de uso devem ser compartilhados com a Apple.
- **Zoom de exibição:** configurar a resolução da tela (padrão ou ampliada) nos dispositivos iOS.
- **True Tone:** configurar o True Tone Display nos dispositivos iOS.
- **Botão Home:** configurar a sensibilidade da tela do Botão **Home** em dispositivos iOS.
- **Destaques do novo recurso:** configurar as telas informativas de integração, acessar o Dock em qualquer lugar e alternar entre aplicativos recentes em dispositivos iOS 11.0 (versão mínima).
- **Privacidade:** impedir que os usuários vejam os dados e o painel de privacidade durante a configuração dos dispositivos ABM. Para iOS 11.3 e posterior.
- **SoftwareUpdate:** impedir que o usuário veja a tela obrigatória de atualização de software ao configurar dispositivos ABM. Para iOS 12.0 e posterior.

- **ScreenTime:** impedir que o usuário veja a tela Tempo de Tela durante a configuração dos dispositivos ABM. Para iOS 12.0 e posterior.
- **Configuração do SIM:** impedir que o usuário veja a tela Add Cellular Plan durante a configuração de dispositivos ABM. Para iOS 12.0 e posterior.
- **iMessage & FaceTime:** impedir que o usuário veja a tela do iMessage e do FaceTime durante a configuração dos dispositivos ABM. Para iOS 12.0 e posterior.
- **Aparência:** impede que o usuário veja a tela **Escolher sua aparência**. Para iOS 13.0 e posterior.
- **Welcome:** impede que o usuário veja a tela **Introdução**. Para iOS 13.0 e posterior.

A conta ABM aparece em **Configurações > Programa de implantação da Apple**.

7. Em **Opções do assistente de instalação do macOS**, selecione as etapas do Assistente de instalação do macOS que os usuários ignoram quando iniciam seus dispositivos pela primeira vez. O padrão é desmarcar essa opção para todos os itens.



- **Configurar como novo ou restaurar:** configurar o dispositivo como novo ou de um backup do iCloud ou da Apple App Store.
- **Serviços de localização:** configurar o serviço de localização no dispositivo.
- **ID Apple:** configurar uma conta de ID Apple gerenciada para o dispositivo.
- **Termos e condições:** exigir que os usuários aceitem os termos e as condições de uso do dispositivo.
- **Siri:** usar ou não a Siri no dispositivo.

- **FileVault:** usar o FileVault para criptografar o disco de inicialização. O XenMobile somente aplicará a configuração do FileVault se o sistema tiver uma conta de usuário local e essa conta estiver conectada ao iCloud.

Você pode usar o recurso de Criptografia de disco do FileVault do macOS para proteger o volume do sistema, criptografando seu conteúdo (<https://support.apple.com/en-us/HT204837>). Se o Assistente de instalação for executado em um Mac portátil mais atual sem o FileVault ativado, talvez você seja solicitado a ativar esse recurso. O aviso aparecerá em sistemas novos e em sistemas atualizados para o OS X 10.10 ou 10.11, mas somente se esse sistema tiver uma única conta de administrador local e essa conta estiver conectada ao iCloud.

- **Análise de aplicativo:** configurar se os dados de falha e as estatísticas de uso devem ser compartilhados com a Apple.
- **Privacidade:** impedir que os usuários vejam os dados e o painel de privacidade durante a configuração dos dispositivos ABM. Para macOS 10.13 e versões posteriores.
- **iCloud Analytics:** impedir que os usuários vejam a tela de análise do iCloud durante a configuração dos dispositivos ABM. Para macOS 10.13 e versões posteriores.
- **Área de trabalho e documentos do iCloud:** impedir que os usuários vejam os documentos do iCloud e a tela da área de trabalho durante a configuração dos dispositivos ABM. Para macOS 10.13 e versões posteriores.
- **Aparência:** impedir que o usuário veja a tela Escolher sua aparência durante a configuração dos dispositivos ABM. Para macOS 10.14 e versões posteriores.
- **Opções de configuração de conta local:** especificar as configurações para criar uma conta de administrador no dispositivo. Os usuários fazem login no dispositivo macOS com essas informações. O XenMobile cria a conta usando as informações especificadas.
 - **Criar conta primária como um usuário padrão:** em vez de conceder privilégios de administrador a esse usuário no dispositivo, o XenMobile cria o usuário com permissões padrão. Como o macOS requer uma conta de administrador, o XenMobile cria uma conta de administrador primeiro, depois cria uma nova conta padrão e a define como primária.
 - **Nome completo do administrador:** digite o nome que o sistema exibe para a conta de administrador.
 - **Nome abreviado do administrador:** digite o nome que o dispositivo exibe para a pasta base e no shell.
 - **Senha do administrador:** digite uma senha segura para a conta de administrador.
 - **Exibir a conta do administrador em Usuários e grupos:** se desmarcada, a conta de administrador não aparece em **Usuários e Grupos** nas configurações do macOS.

Se você criar a conta primária como um usuário padrão, ative essa configuração para ocultar a conta de administrador que o XenMobile cria primeiro.

Pedido de dispositivos ativados para o programa de implantação

Você pode solicitar dispositivos ativados para o Programa de Implantação diretamente da Apple ou com revendedores ou operadoras autorizadas do Programa de Implantação. Para encomendar com a Apple, forneça o ID de cliente Apple no Portal do Programa de Implantação da Apple. Seu ID de cliente permite que a Apple associe à sua conta do Programa de Implantação da Apple os dispositivos que você adquiriu.

Para encomendar com o seu revendedor ou operadora, entre em contato com o revendedor da Apple ou a operadora para verificar se eles participam do Programa de Implantação da Apple. Peça o ID do Programa de Implantação da Apple do revendedor ao adquirir dispositivos. A Apple exige essas informações quando você adiciona seu revendedor do Programa de Implantação da Apple à sua conta do Programa de Implantação da Apple. Depois de adicionar o ID do Programa de Implantação da Apple do revendedor, você receberá um ID de cliente do Programa de Implantação. Forneça o ID de cliente do Programa de Implantação ao revendedor, que o usará para enviar informações sobre suas compras de dispositivos para a Apple. Para obter mais informações, consulte este [site de registro de dispositivo de uso da Apple](#).

Gerenciar dispositivos ativados para o Programa de Implantação

Depois que o seu pedido for enviado, você pode associar dispositivos iOS, iPadOS e macOS ao seu servidor XenMobile.

1. Faça logon no [Apple Business Manager](#) usando uma conta de administrador ou gerente de registro de dispositivo.
2. Na barra lateral, clique em **Devices**. Os dispositivos que você adquiriu diretamente da Apple são exibidos automaticamente. Para atribuir dispositivos do Apple Configurator 2 ao Apple Business Manager, consulte [Guia de usuário do Apple Business Manager](#).
3. Na lista, selecione um dispositivo ou o número total de dispositivos e clique em **Edit Device Management**. Você tem duas opções:
 - Para atribuir um dispositivo a um servidor MDM, em **Assign to Server**, escolha o nome do seu servidor XenMobile. Clique em **Continue**.
Para atribuir novos dispositivos ao Apple Business Manager em massa, defina um servidor XenMobile padrão para implantação. Para obter mais informações, consulte [Definir um servidor padrão para registro em massa](#).
 - Para cancelar a atribuição de um dispositivo a partir do servidor XenMobile, escolha **Unassign**.

Os dispositivos do Programa de Implantação da Apple estão associados ao servidor XenMobile selecionado.

Se você enviar um dispositivo iOS, iPadOS ou macOS para manutenção, será necessário remover o dispositivo do Apple Business Manager. Quando você receber o dispositivo de volta da manutenção, deverá reatribuir o dispositivo ao servidor XenMobile. Quando substituir o dispositivo, você pode atribuir um novo dispositivo ao servidor XenMobile usando um número de pedido.

Para revisar o histórico de dispositivos atribuídos:

1. Faça login no [Apple Business Manager](#) usando uma conta de administrador ou gerente de registro de dispositivo.
2. Na barra lateral, clique em **Assignment History**. Em seguida, escolha uma atribuição para exibir mais informações.
3. Clique em **Download** para baixar um arquivo CSV com os números de série de todos os dispositivos atribuídos e não atribuídos.

Você pode remover dispositivos iOS, iPadOS e macOS do Apple Business Manager se o dispositivo tiver sido vendido, roubado ou não puder ser reparado.

1. Faça login no [Apple Business Manager](#) usando uma conta de administrador ou gerente de registro de dispositivo.
2. Na barra lateral, clique em **Devices** e procure um dispositivo.
3. Selecione um dispositivo e clique em **Release Device**. Na caixa de diálogo, confirme suas alterações para remover o dispositivo do programa. Para adicionar dispositivos iOS e iPadOS de volta, use o Apple Configurator 2. Não é possível adicionar dispositivos macOS de volta com o Apple Configurator 2.

Registrar dispositivos

April 8, 2021

Para gerenciar dispositivos de usuários remotamente e com segurança, registre-os no XenMobile. O software cliente do XenMobile é instalado no dispositivo do usuário e a identidade do usuário é autenticada. Em seguida, o XenMobile e o perfil do usuário são instalados. Em seguida, no console XenMobile, você pode realizar tarefas de gerenciamento de dispositivo. Você pode aplicar políticas, implantar aplicativos, enviar dados por push para o dispositivo, além de bloquear, apagar e localizar dispositivos perdidos ou roubados.

O registro do Active Directory do Azure é compatível com dispositivos iOS, Android e Windows 10. Para obter mais informações sobre como configurar o Azure como seu provedor de identidade (IDP), consulte [Integração do XenMobile com o Azure Active Directory como IDP](#).

Nota:

Antes que você possa registrar usuários de dispositivos iOS, é necessário solicitar um certificado de APNs. Para obter detalhes, consulte [Certificados e autenticação](#).

Para atualizar as opções de configuração para os usuários e dispositivos, use a página **Gerenciar > Convites para registro**. Para obter detalhes, consulte [Envie um convite para registro](#) neste artigo.

Dispositivos Android

Nota:

Para obter informações sobre como registrar os dispositivos do Android Enterprise, consulte [Android Enterprise](#).

1. Acesse a Google Play Store no seu dispositivo Android, baixe o aplicativo Citrix Secure Hub e toque no aplicativo.
2. Quando solicitado a instalar o aplicativo, clique em **Avançar** e, em seguida, clique em **Instalar**.
3. Depois que o Secure Hub for instalado, toque em **Abrir**.
4. Insira suas credenciais corporativas, como o nome do XenMobile Server, o nome UPN ou o endereço de email. Em seguida, clique em **Avançar**.
5. Na tela **Ativar o administrador do dispositivo**, toque em **Ativar**.
6. Digite sua senha corporativa e toque em **Conectar**.
7. Dependendo da forma como XenMobile está configurado, você pode ser solicitado a criar um PIN da Citrix. Esse PIN pode ser usado para fazer login no Secure Hub e em outros aplicativos habilitados para o XenMobile, como o Secure Mail e o Citrix Files. Insira o PIN da Citrix duas vezes. Na tela **Criar PIN da Citrix**, insira um PIN.
8. Insira novamente o PIN. O Secure Hub é aberto. Você pode acessar a XenMobile Store para exibir os aplicativos que pode instalar no seu dispositivo Android.
9. Se você tiver configurado o XenMobile para enviar aplicativos automaticamente por push aos dispositivos após o registro, os usuários serão solicitados a instalar esses aplicativos. Além disso, as políticas que você define no XenMobile são implantadas no dispositivo. Toque em **Instalar** para instalar os aplicativos.

Para cancelar o registro e registrar novamente um dispositivo Android

Os usuários podem cancelar o registro no Secure Hub. Quando os usuários cancelam o registro usando o procedimento a seguir, o dispositivo ainda é exibido no inventário de dispositivos do console XenMobile. No entanto, você não pode executar nenhuma ação no dispositivo. Você não pode rastrear o dispositivo e não pode monitorar a conformidade do dispositivo.

1. Toque para abrir o aplicativo Secure Hub.
2. Dependendo de você ter um telefone ou um tablet, faça o seguinte:

Em um telefone:

- Deslize a partir do lado esquerdo da tela para abrir um painel de configurações.
- Toque em **Preferências**, toque em **Contas** e, em seguida, toque em **Excluir conta**.

Em um tablet:

- Toque na seta ao lado do seu endereço de email no canto superior direito.
- Toque em **Preferências**, toque em **Contas** e, em seguida, toque em **Excluir conta**.

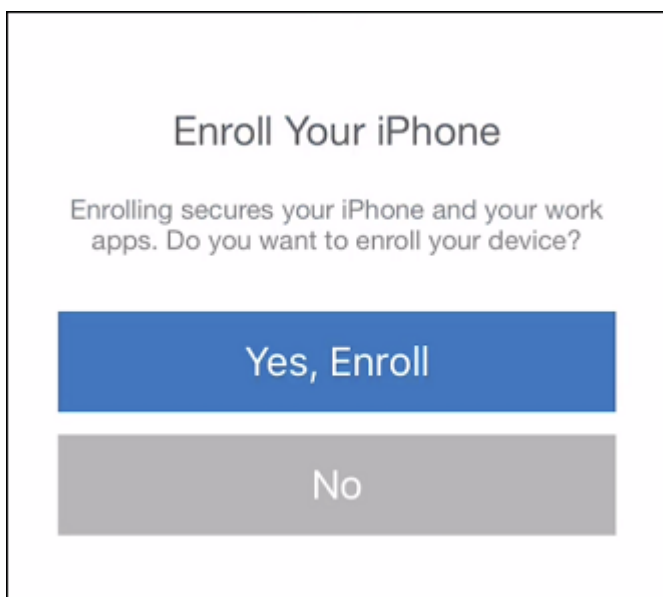
3. Toque em **Registrar novamente**. Uma mensagem é exibida para confirmar que você deseja registrar novamente o dispositivo.
4. Toque em **OK**.
O registro do dispositivo é cancelado.
5. Siga-as instruções na tela para registrar novamente o dispositivo.

Registrar dispositivos iOS

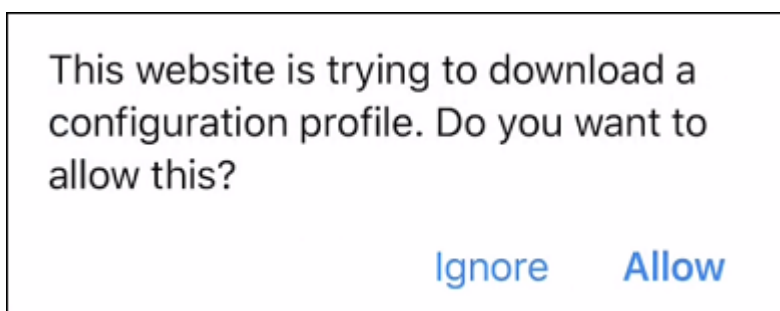
Esta seção mostra como os usuários registram dispositivos iOS (12.2 ou posterior) no XenMobile Server. Para obter mais informações sobre o registro no iOS, abra o seguinte vídeo:



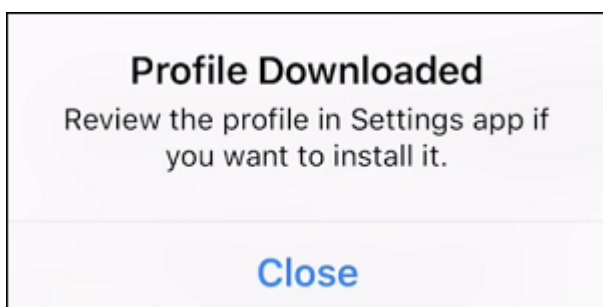
1. Acesse a Apple Store no seu dispositivo iOS, baixe o aplicativo Citrix Secure Hub e toque no aplicativo.
2. Quando solicitado a instalar o aplicativo, toque em **Avançar** e, em seguida, toque em **Instalar**.
3. Depois que o Secure Hub for instalado, toque em **Abrir**.
4. Insira suas credenciais corporativas, como o nome do XenMobile Server, o nome UPN ou o endereço de email. Em seguida, clique em **Avançar**.
5. Toque em **Sim, registrar** para registrar seu dispositivo iOS.



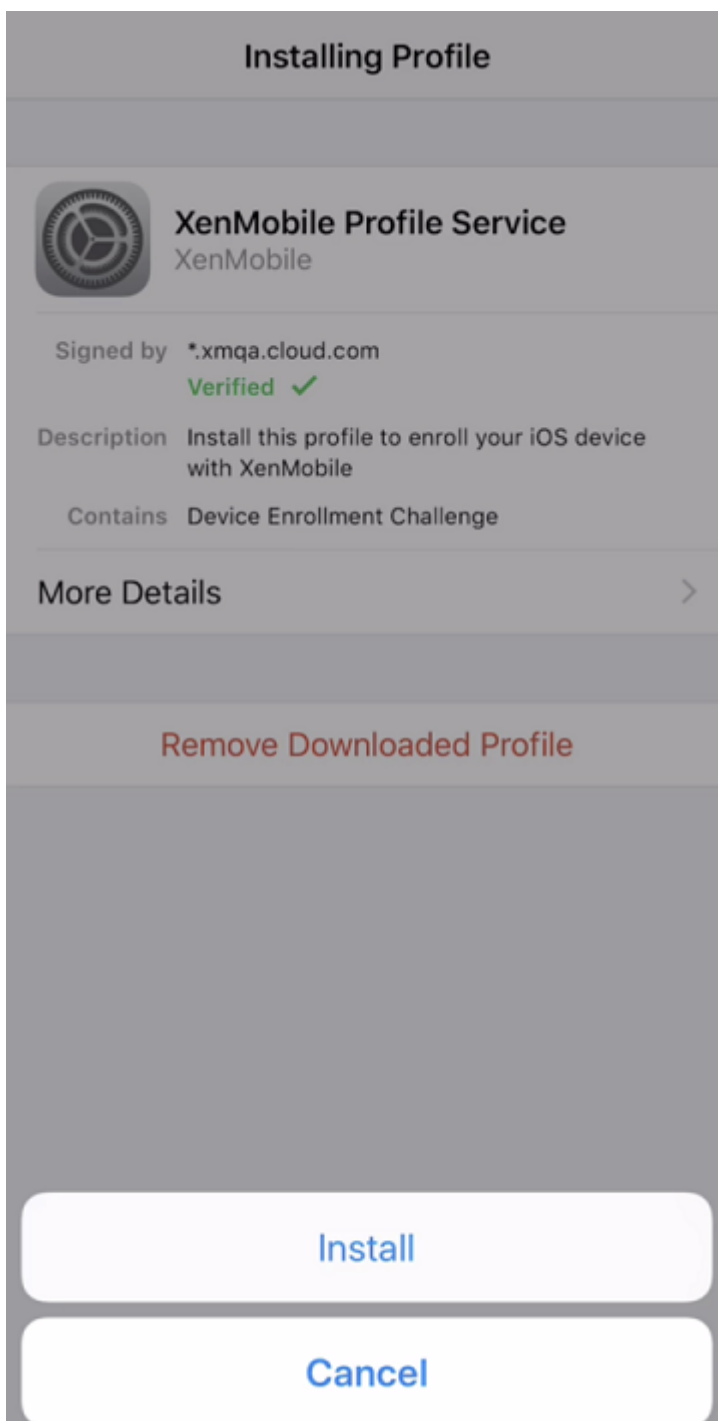
6. Depois de digitar suas credenciais, toque em **Permitir**, quando solicitado, para baixar o perfil de configuração.



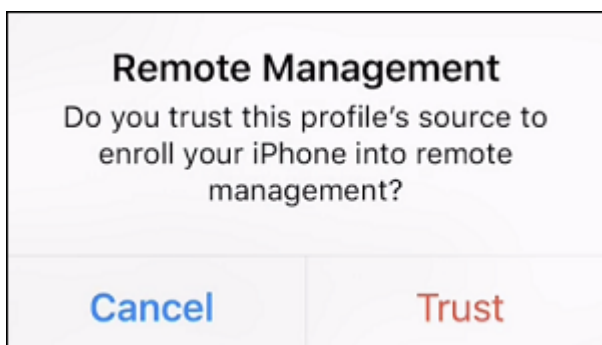
7. Depois de baixar o perfil de configuração, toque em **Fechar**.



8. Nas configurações do dispositivo, instale o certificado iOS e adicione o dispositivo à lista confiável.
- Vá para **Configurações > Geral > Perfil > XenMobile Profile Service** e toque em **Instalar** para adicionar o perfil.



- Na janela de notificação, toque em **Confiar** para registrar seu dispositivo no gerenciamento remoto.



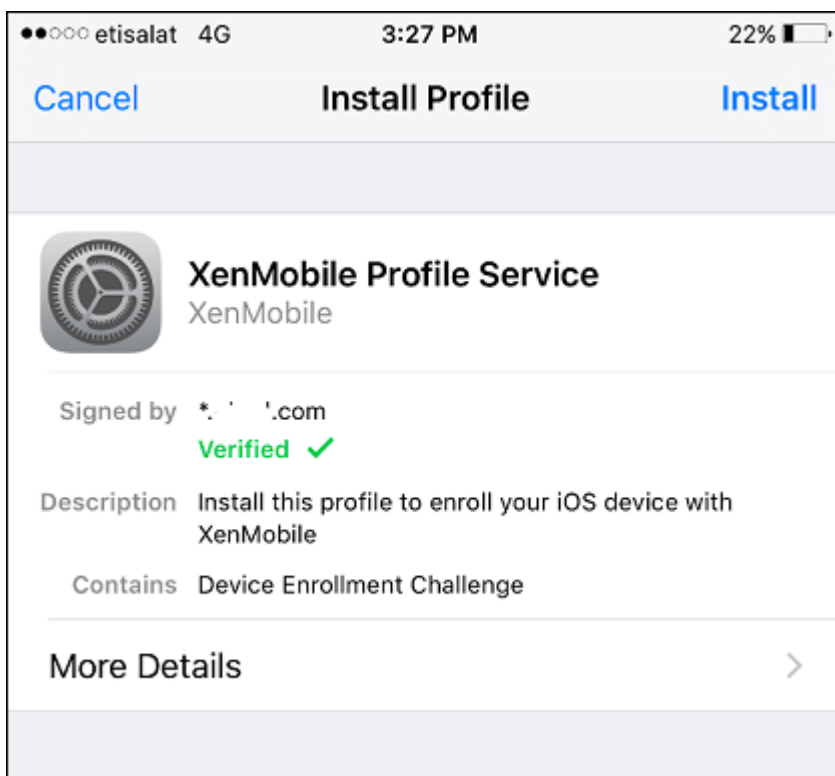
9. Faça login no Secure Hub. Se você estiver se registrando no MDM+MAM, depois que suas credenciais forem validadas, crie e confirme seu PIN Citrix quando solicitado.
10. Após a conclusão do fluxo de trabalho, o dispositivo é registrado. Você pode acessar a loja de aplicativos para exibir os aplicativos que pode instalar no seu dispositivo iOS.

Dispositivos iOS

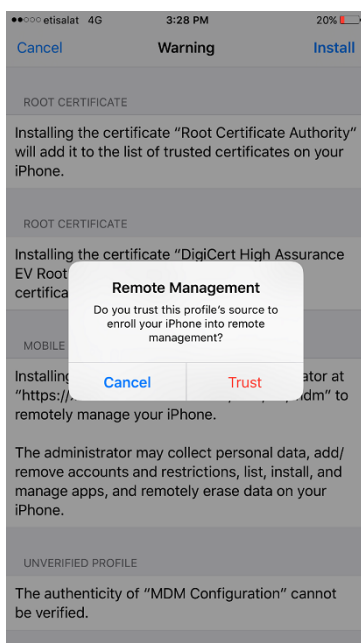
1. Baixe o aplicativo Secure Hub da App Store do Apple iTunes no dispositivo e instale-o no dispositivo.
2. Na tela inicial do dispositivo iOS, toque no aplicativo Secure Hub.
3. Quando o aplicativo Secure Hub é aberto, insira o endereço de servidor fornecido pela sua central de ajuda.

A tela apresentada pode ser diferente destes exemplos, dependendo de como o XenMobile está configurado.

4. Quando solicitado, digite o nome de usuário e senha ou PIN. Clique em **Avançar**.
5. Quando solicitado a se registrar, clique em **Sim, registrar** e insira suas credenciais quando solicitado.
6. Toque em **Instalar** para instalar o Citrix Profile Services.



7. Toque em **Confiar**.



8. Toque em **Abrir** e insira suas credenciais.

Dispositivos macOS

O XenMobile fornece dois métodos para registrar dispositivos que executam o macOS. Os dois modos permitem que os usuários de macOS façam o registro diretamente dos seus dispositivos pela rede celular.

- **Send users an enrollment invitation:** este método de registro permite definir qualquer um dos seguintes modos de segurança de registro para dispositivos macOS:
 - Nome de usuário + senha
 - Nome de usuário + PIN
 - Dois Fatores

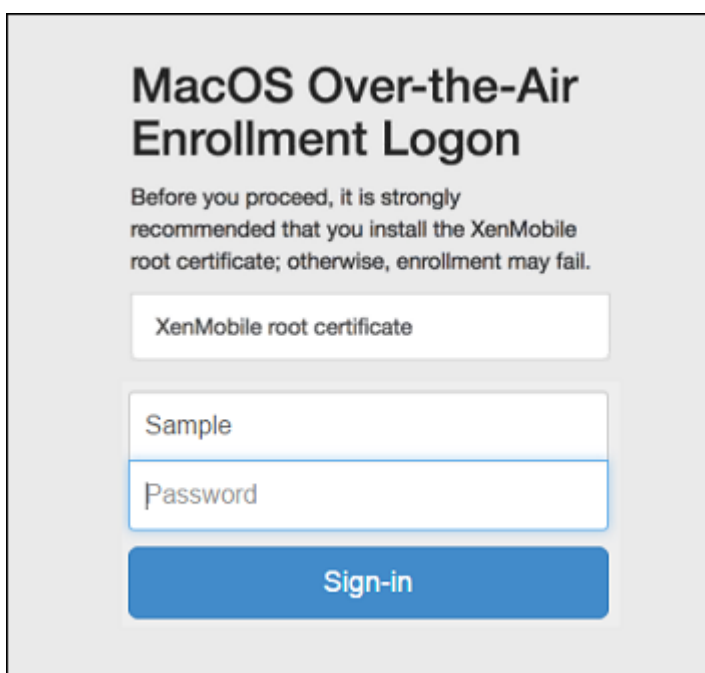
Quando o usuário segue as instruções no convite de registro, é exibida uma tela de login com o nome de usuário preenchido.

- **Enviar um link de instalação para os usuários:** esse método de registro para dispositivos macOS envia aos usuários um link de registro que eles podem abrir nos navegadores Safari ou Chrome. Um usuário se registra fornecendo seu nome de usuário e senha.

Para impedir o uso de um link de registro para dispositivos macOS, defina a propriedade do servidor **Enable macOS OTAE** como **false**. Como resultado, os usuários do macOS apenas podem se registrar usando um convite para registro.

Enviar aos usuários um convite para registro

1. Opcionalmente, configure as políticas de dispositivo macOS no console XenMobile. Para obter mais informações sobre políticas de dispositivo, consulte [Políticas de dispositivo](#).
2. Adicione um convite para registro de usuário do macOS. Para obter mais informações, consulte [Envie um convite para registro](#) neste artigo.
3. Depois que os usuários recebem o convite e clicam no link, é exibida a seguinte tela no navegador Safari. O XenMobile preenche o nome do usuário. Se você escolher **Dois fatores** para o modo de segurança de registro, outro campo será exibido.



4. Os usuários instalam os certificados conforme necessário. A exibição do prompt para os usuários instalarem certificados depende se você configurou o seguinte para o macOS: um certificado SSL publicamente confiável e um certificado de assinatura digital publicamente confiável. Para obter mais informações sobre certificados, consulte [Certificados e autenticação](#).
5. Os usuários fornecem as credenciais solicitadas.

As políticas de dispositivo Mac são instaladas. Agora você pode começar a gerenciar Macs com o XenMobile, da mesma forma como gerencia os dispositivos móveis.

Enviar um link de instalação para os usuários

1. Opcionalmente, configure as políticas de dispositivo macOS no console XenMobile. Para obter mais informações sobre políticas de dispositivo, consulte [Políticas de dispositivo](#).
2. Envie o link de registro `https://serverFQDN:8443/instanceName/macOS/otae`, que os usuários podem abrir nos navegadores Safari ou Chrome.
 - **serverFQDN** é o nome de domínio totalmente qualificado (FQDN) do servidor que executa o XenMobile.
 - A Porta **8443** é a porta segura padrão. Se você tiver configurado uma porta diferente, use essa porta em vez da 8443.
 - O **instanceName**, geralmente mostrado como zdm, é o nome especificado durante a instalação do servidor.

Para obter mais informações sobre o envio de links de instalação, consulte [Para enviar um link de instalação](#).

3. Os usuários instalam os certificados conforme necessário. Se você configurou um certificado SSL publicamente confiável e um certificado de assinatura digital para iOS e macOS, os usuários verão o prompt para instalar certificados. Para obter mais informações sobre certificados, consulte [Certificados e autenticação](#).
4. Os usuários fazem login nos Macs.

As políticas de dispositivo Mac são instaladas. Agora você pode começar a gerenciar Macs com o XenMobile, da mesma forma como gerencia os dispositivos móveis.

Dispositivos Windows

Nota:

Esta seção inclui referências aos dispositivos Windows Phone 8.1, que a Microsoft moveu para Fim de Suporte em 11 de julho de 2017. O XenMobile oferece suporte aos dispositivos Windows Phone 8.1 para o registro de MDM apenas.

Os dispositivos que executam o Windows 10 são registrados no Azure como um meio federado de autenticação do Active Directory. Você pode ingressar os dispositivos Windows 10 no AD do Microsoft Azure de qualquer uma das seguintes maneiras:

- Registre-se no MDM como parte do Ingresso no AD do Azure imediato na primeira vez que o dispositivo for ligado.
- Registre-se no MDM como parte do Ingresso no AD do Azure da página Configurações do Windows, depois que o dispositivo for configurado.

Você pode registrar dispositivos no XenMobile que executam os seguintes sistemas operacionais Windows:

- Windows 10 Phone e Tablet
- Windows Phone 8.1

Os usuários podem se registrar diretamente por meio de seus dispositivos.

Nota:

Para telefones e tablets Windows 10 RS2, durante o novo registro, um usuário não é solicitado a especificar a URL do servidor. Para resolver esse problema, reinicie o dispositivo. Ou, na tela de endereço de email, toque no X em **Conectando-se a um serviço** para ir até a página da URL do servidor. Esse é um problema de terceiros.

Você deve configurar a detecção automática e o serviço de detecção do Windows para o registro de usuário para ativar o gerenciamento de dispositivos Windows com suporte.

Antes que os usuários de dispositivos do Windows possam se registrar usando o Azure, você deve configurar as configurações do servidor Microsoft Azure no XenMobile. Para obter detalhes, consulte [Configurações do servidor do Active Directory do Microsoft Azure](#).

Para registrar dispositivos Windows com a detecção automática

Para ativar o gerenciamento de dispositivos Windows, a Citrix recomenda que você configure o Serviço de Descoberta Automática e o serviço de Descoberta do Windows. Para obter detalhes, consulte [XenMobile AutoDiscovery Service](#).

1. No dispositivo, verifique e instale todas as atualizações disponíveis do Windows.
2. Em Windows 10: no menu de botões, toque em **Configurações** e em **Contas > Acessar o trabalho ou a escola > Conectar ao trabalho ou à escola**. Em telefones Windows 8.1: toque em **Configurações do PC > Rede > Local de Trabalho**.
3. Insira o seu endereço de email corporativo e toque em **Continuar** no Windows 10 ou em **Ativar o gerenciamento de dispositivo** no Windows 8.1. Para se registrar como um usuário local, insira um endereço de email inexistente com o nome de domínio correto (por exemplo, foo@mydomain.com). Isso permite que você ignore uma limitação conhecida da Microsoft na qual o registro é realizado pelo Gerenciamento de Dispositivo interno no Windows; na caixa de diálogo **Conectando a um serviço**, digite o nome do usuário e a senha associados ao usuário local. O dispositivo detecta automaticamente um XenMobile Server e inicia o processo de registro.
4. Digite sua senha. Use a senha associada a uma conta que faz parte de um grupo de usuários no XenMobile.
5. Em Windows 10: na caixa de diálogo **Termos de uso**, indique que você concorda com o gerenciamento do seu dispositivo e, em seguida, toque em **Aceitar**. Em Windows 8.1: na caixa de diálogo **Permitir aplicativos e serviços do administrador de TI**, indique que você concorda com o gerenciamento do seu dispositivo e, em seguida, toque em **Ligar**.

Para registrar dispositivos Windows sem a detecção automática

É possível registrar dispositivos Windows sem a detecção automática. A Citrix, no entanto, recomenda que você configure a detecção automática. O registro sem detecção automática resulta em uma chamada para a porta 80 antes da conexão com a URL desejada, portanto, não é considerado uma prática recomendada para implantações de produção. A Citrix recomenda que você use esse processo somente em ambientes de teste e implantações de prova de conceito.

1. No dispositivo, verifique e instale todas as atualizações disponíveis do Windows.

2. Em Windows 10: no menu de botões, toque em **Configurações** e em **Contas > Acessar o trabalho ou a escola > Conectar ao trabalho ou à escola**. Em Windows 8.1: toque em **Configurações do PC > Rede > Local de Trabalho**.
3. Insira o seu endereço de email da empresa.
4. Em Windows 10: se a detecção automática não estiver configurada, uma opção será exibida na qual você pode inserir os detalhes do servidor, conforme descrito na etapa 5. No Windows 8.1: se a opção **Detectar automaticamente o endereço do servidor** estiver definida como **ativada**, **desative** a opção.
5. Em Windows 10, no campo **Inserir endereço do servidor**, digite o endereço: `https://serverfqdn:8443/serverInstance/wpe`.

Se uma porta diferente de 8443 for usada para as conexões SSL não autenticadas, use esse número de porta em vez de 8443 nesse endereço.

No Windows 8.1: digite o endereço do servidor no seguinte formato: `https://serverfqdn:8443/serverInstance/Discovery.svc`.

Se uma porta diferente de 8443 for usada para as conexões SSL não autenticadas, use esse número de porta em vez de 8443 nesse endereço.
6. Digite sua senha.
7. Em Windows 10: na caixa de diálogo **Termos de uso**, indique que você concorda com o gerenciamento do seu dispositivo e, em seguida, toque em **Aceitar**. Em Windows 8.1: na caixa de diálogo **Permitir aplicativos e serviços do administrador de TI**, indique que você concorda com o gerenciamento do seu dispositivo e, em seguida, toque em **Ligar**.

Para registrar dispositivos Windows Phone

Para registrar dispositivos Windows Phone no XenMobile, os usuários precisam dos respectivos endereços de email e senha do Active Directory ou da rede interna. Se a detecção automática não estiver configurada, os usuários precisarão também do endereço da Web do XenMobile Server. Em seguida, eles seguem este procedimento nos dispositivos deles para se registrarem.

Nota:

Se você planeja implantar aplicativos usando a loja da empresa do Windows Phone, antes que os usuários se registrem, verifique se uma política do [Hub empresarial](#) foi configurada (com um aplicativo assinado Secure Hub e Windows Phone para cada plataforma à qual você deseja oferecer compatibilidade).

1. Na tela principal do Windows Phone, toque no ícone **Configurações**.

- Em Windows 10: dependendo da versão, toque em **Contas > Acessar trabalho ou escola > Conectar ao trabalho ou à escola** ou toque em **Contas > Acesso corporativo > Registrar-se no gerenciamento de dispositivo**.
 - Em Windows 8.1: toque em **Configurações do PC > Rede > Local de trabalho** e depois toque em **Adicionar conta**.
2. Na tela seguinte, insira um endereço de email e uma senha e, em seguida, toque em **entrar**.

Se a detecção automática estiver configurada para o seu domínio, as informações solicitadas nas próximas etapas serão preenchidas automaticamente. Prossiga para a Etapa 8.

Se a detecção automática não estiver configurada para o seu domínio, continue até a próxima etapa. Para se registrar como um usuário local, insira um endereço de email inexistente com o nome de domínio correto (por exemplo, `foo@mydomain.com`). Isso permite que você ignore uma limitação conhecida da Microsoft: na caixa de diálogo **Conectando a um serviço**, digite o nome do usuário e a senha associados ao usuário local.
 3. Na tela seguinte, digite o endereço da Web do XenMobile Server, como: `https://<xenmobile_server>:<portnumber>/<instancename>/wpe`. Por exemplo, `https://mycompany.mdm.com:8443/zdm/wpe`.
- Nota:**
- O número da porta deve ser adaptado para a sua implementação. Ela deve ser a mesma porta que você usou para uma inscrição do iOS.
4. Insira o nome do usuário e o domínio se a autenticação for validada por meio de um nome do usuário e um domínio e, em seguida, toque em **entrar**.
 5. No Windows Phone 8.1, quando a conta é adicionada, você tem a opção de selecionar **Instalar aplicativo da empresa**. Se o administrador tiver configurado uma loja de aplicativos da empresa, selecione essa opção e toque em **concluído**. Se você desmarcar essa opção, precisará registrar novamente o seu dispositivo para receber a Loja de aplicativos da empresa.
 6. No Windows Phone 8.1, na tela **Conta adicionada**, toque em **concluído**.
 7. Para forçar uma conexão com o servidor, toque no ícone de atualização. Se o dispositivo não se conectar manualmente ao servidor, o XenMobile tentará se reconectar. O XenMobile se conecta ao dispositivo a cada três minutos por cinco vezes sucessivas, e depois a cada duas horas. Você pode alterar essa taxa de conexão na opção **Windows WNS Heartbeat Interval** localizada em **Propriedades do servidor**. Depois que o registro for concluído, o Secure Hub se registrará em segundo plano. Nenhum indicador é exibido quando a instalação é concluída. Toque em Secure Hub na tela **Todos os Aplicativos**.

Envie um convite para registro

No console XenMobile, você pode enviar um convite para registro aos usuários com dispositivos iOS, macOS e Android. Você também pode enviar um link de instalação aos usuários com dispositivos iOS ou Android.

Convites para registro são enviados da seguinte maneira:

- Se o convite para registro for para um local ou um usuário do Active Directory: o usuário receberá o convite via SMS com o nome de número e a operadora de telefone especificada.
- Se o convite para registro é para um grupo: os usuários recebem convites via SMS. Se os usuários do Active Directory tiverem um endereço de email e número do telefone celular no Active Directory, eles receberão o convite. Usuários locais recebem o convite no email e número de telefone especificados nas propriedades do usuário.

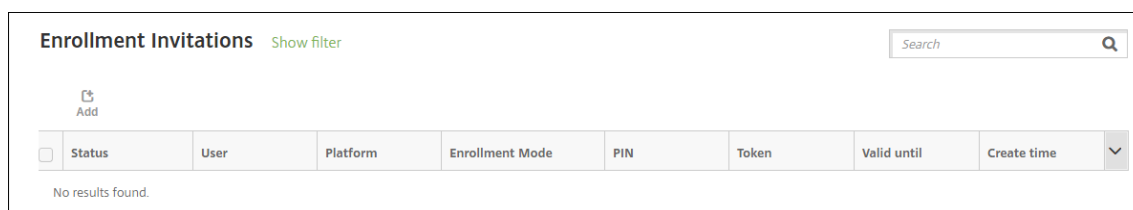
Após o registro dos usuários, seus dispositivos aparecem como gerenciados em **Gerenciar > Dispositivos**. O status da URL de convite é mostrado como **Resgatado**.

Pré-requisitos

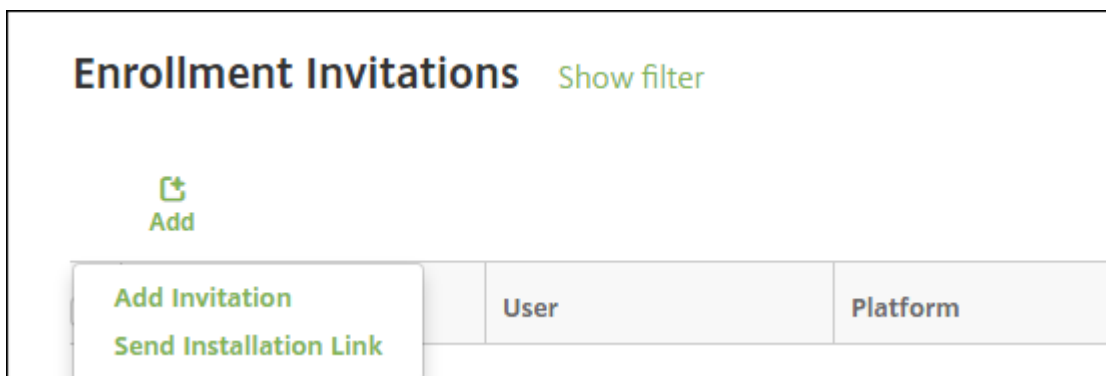
- XenMobile Server configurado no modo Empresarial (XME) ou MDM
- LDAP configurado
- Se estiver usando grupos locais e usuários locais:
 - Um ou mais grupos locais.
 - Usuários locais atribuídos a grupos locais.
 - Grupos de entrega são associados a grupos locais.
- Se estiver usando o Active Directory:
 - Grupos de entrega são associados a grupos do Active Directory.

Criar um convite para registro

1. No console XenMobile, clique em **Gerenciar > Convites para registro**. A página **Convites para registro** é exibida.



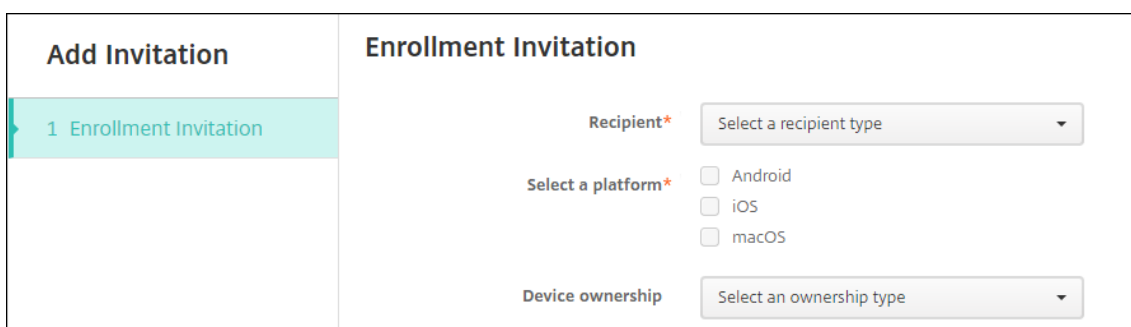
2. Clique em **Adicionar**. É exibido um menu de opções de registro.



- Para enviar um convite para registro para um usuário ou grupo, clique em **Adicionar convite**.
- Para enviar um link de instalação de registro para uma lista de destinatários via SMTP ou SMS, clique em **Enviar link de instalação**.

O processo de enviar convites para registro e links de instalação é descrito após estas etapas.

3. Clique em **Adicionar convite**. A tela **Convite para registro** é exibida.



4. Defina estas configurações:

- **Destinatário:** escolha **Grupo** ou **Usuário**.
- **Selecionar uma plataforma:** se **Destinatário** for **Grupo**, todas as plataformas estarão selecionadas. É possível alterar a seleção da plataforma. Se **Destinatário** for **Usuário**, nenhuma plataforma estará selecionada. Selecione uma plataforma.
- **Propriedade do dispositivo:** selecione **Corporativo** ou **BYOD**.

Configurações para usuários ou grupos são exibidas, conforme descrito nas seções a seguir.

Para enviar um convite para registro a um usuário

Add Invitation	Enrollment Invitation
<p>1 Enrollment Invitation</p>	<p>Recipient* <input type="text" value="User"/></p> <p>Select a platform* <input type="checkbox"/> Android <input type="checkbox"/> iOS <input type="checkbox"/> macOS</p> <p>Device ownership <input type="text" value="Select an ownership type"/></p> <p>User name* <input type="text"/> ?</p> <p>Enrollment mode* <input type="text" value="User name + Password"/></p> <p>Template for agent download <input type="text" value="Select a template"/></p> <p>Template for enrollment URL <input type="text" value="Select a template"/></p> <p>Template for enrollment confirmation <input type="text" value="Select a template"/></p> <p>Expire after <input type="text" value="Never"/></p> <p>Maximum Attempts <input type="text" value="0"/></p> <p>Send invitation <input type="button" value="OFF"/></p>

1. Defina estas configurações de **Usuário**:

- **Nome de usuário:** digite um nome de usuário. O usuário deve existir no XenMobile Server como um usuário local ou como um usuário no Active Directory. Se o usuário for local, verifique se a propriedade de email desse usuário esteja definida, para que você possa enviar notificações ao usuário. Se o usuário estiver no Active Directory, verifique se o LDAP está configurado.
- **Informações do dispositivo:** essa configuração não aparecerá se você selecionar várias plataformas ou se selecionar somente o macOS. Escolha **Número de série**, **UDID** ou **IMEI**. Depois de escolher uma opção, é exibido um campo no qual você pode digitar o valor correspondente do dispositivo.
- **Número de telefone:** essa configuração não aparecerá se você selecionar várias plataformas ou se selecionar somente o macOS. Opcionalmente, digite o número de telefone do usuário.
- **Operadora:** essa configuração não aparecerá se você selecionar várias plataformas ou se selecionar somente o macOS. Escolha uma operadora a ser associada ao número de telefone do usuário.
- **Modo de registro:** escolha o modo de segurança de registro para usuários. O padrão é **Nome de usuário + Senha**. Algumas das opções a seguir não estão disponíveis para todas as plataformas:

- Nome de usuário + Senha
- Alta Segurança
- URL de Convite
- URL de Convite + PIN
- URL de Convite + Senha
- Dois Fatores
- Nome de usuário + PIN

Um PIN para o registro também é chamado de PIN ocasional. Esses PINs são válidos somente quando o usuário se registra.

Nota:

Quando você seleciona qualquer modo de segurança de registro que inclui um PIN, o campo **Modelo de PIN de registro** é exibido, onde você clica em **PIN de registro**.

- **Modelo para download do agente:** escolha o modelo do link de download denominado **Link para download**. Esse modelo é para todas as plataformas com suporte.
- **Modelo para URL de registro:** escolha **Convite para registro**.
- **Modelo para confirmação de registro:** escolha **Confirmação de registro**.
- **Expira após:** esse campo é definido quando você configura o modo de registro e indica quando o registro expira. Para obter mais informações sobre como configurar os modos de segurança de registro, consulte [Para configurar modos de segurança de registro](#).
- **Máximo de tentativas:** esse campo é definido quando você configura o **Modo de registro** e indica o número máximo de vezes que o processo de registro ocorre. Para obter mais informações sobre como configurar os modos de segurança de registro, consulte [Para configurar modos de segurança de registro](#).
- **Enviar convite:** selecione **I** para enviar o convite imediatamente. Selecione **O** para adicionar o convite à tabela na página **Convites para registro**, mas não enviá-lo.

2. Clique em **Salvar e enviar** se tiver ativado a opção **Enviar convite**. Caso contrário, clique em **Salvar**. O convite é exibido na tabela na página **Convites para registro**.

<input type="checkbox"/>	Status	User	Platform	Enrollment Mode	PIN	Token	Valid until	Create time
<input type="checkbox"/>	PENDING	[Redacted]	Android	User name + Password	[Redacted]	[Redacted]	[Redacted]	05/03/2017 10:32:24 am
<input type="checkbox"/>	PENDING	[Redacted]	macOS	User name + Password	[Redacted]	[Redacted]	[Redacted]	05/01/2017 07:33:38 pm
<input type="checkbox"/>	PENDING	[Redacted]	iOS	User name + Password	[Redacted]	[Redacted]	[Redacted]	05/01/2017 07:29:02 pm

Para enviar um convite para registro a um grupo

A figura a seguir mostra as definições para configurar um convite de registro para um grupo.

The screenshot shows the 'Add Invitation' configuration page. On the left, there is a sidebar with '1 Enrollment Invitation' selected. The main area is titled 'Enrollment Invitation' and contains the following settings:

- Recipient***: Group (dropdown)
- Select a platform***: Android, iOS, macOS
- Device ownership**: Select an ownership type (dropdown)
- Domain***: Select a domain (dropdown)
- Group***: Select a group (dropdown)
- Enrollment mode***: User name + Password (dropdown)
- Template for agent download**: Select a template (dropdown)
- Template for enrollment URL**: Select a template (dropdown)
- Template for enrollment confirmation**: Select a template (dropdown)
- Expire after**: Never
- Maximum Attempts**: 0
- Send invitation**: OFF (toggle)

1. Defina estas configurações:

- **Domínio:** selecione o domínio do grupo para receber o convite.
- **Grupo:** escolha o grupo que receberá o convite.
- **Modo de registro:** escolha como você deseja que os usuários do grupo se registrem. O padrão é **Nome de usuário + Senha**. Algumas das opções a seguir não estão disponíveis para todas as plataformas:
 - Nome de usuário + Senha
 - Alta Segurança
 - URL de Convite
 - URL de Convite + PIN
 - URL de Convite + Senha
 - Dois Fatores
 - Nome de usuário + PIN

Somente os modos de segurança de registro válidos para cada uma das plataformas sele-

cionadas são exibidos.

Nota:

Quando você seleciona qualquer modo de segurança de registro que inclui um PIN, o campo **Modelo de PIN de registro** é exibido, onde você clica em **PIN de registro**.

- **Modelo para download do agente:** escolha o modelo do link de download denominado **Link para download**. Esse modelo é para todas as plataformas com suporte.
- **Modelo para URL de registro:** escolha **Convite para registro**.
- **Modelo para confirmação de registro:** escolha **Confirmação de registro**.
- **Expira após:** esse campo é definido quando você configura o modo de registro e indica quando o registro expira. Para obter mais informações sobre como configurar os modos de segurança de registro, consulte [Para configurar modos de segurança de registro](#).
- **Máximo de tentativas:** esse campo é definido quando você configura o Modo de registro e indica o número máximo de vezes que o processo de registro ocorre. Para obter mais informações sobre como configurar os modos de segurança de registro, consulte [Para configurar modos de segurança de registro](#).
- **Enviar convite:** selecione **I** para enviar o convite imediatamente. Selecione **O** para adicionar o convite à tabela na página **Convites para registro**, mas não enviá-lo.

2. Clique em **Salvar e enviar** se tiver ativado a opção **Enviar convite**. Caso contrário, clique em **Salvar**. O convite é exibido na tabela na página **Convite para registro**.

Status	Mode	User name	Serial number	Device platform	Operating system version	Device model	Last access	Inactivity days	DEP account name
	MDM MAM	[Redacted]	[Redacted]	iOS	10.1.1	iPad	01/20/2017 02:00:09 pm	2 days	Default DEP Account
	MDM MAM	[Redacted]	[Redacted]	iOS	10.1.1	iPhone	12/15/2016 05:14:24 pm	38 days	
	MDM MAM	[Redacted]	[Redacted]	iOS	10.1.1	iPhone	01/20/2017 02:51:41 pm	2 days	

Para enviar um link de instalação

Para enviar um link de instalação de registro, antes é preciso configurar canais (SMTP ou SMS) no servidor de notificação na página **Configurações**. Para obter detalhes, consulte [\[Notificações\]\(/pt-br/xenmobile/server/users/notifications.html\)](#)

Send Link	Send Installation Link			
1 Details	<p>Recipients*</p> <table border="1"> <tr> <td>Email*</td> <td>Phone number*</td> <td>+ Add</td> </tr> </table> <p>Channels ⓘ</p> <p><input checked="" type="checkbox"/> SMTP ⚠ Channel cannot be activated until you define the SMTP server in the Notification Server section in Settings.</p> <p>Sender: <input type="text"/> ⓘ</p> <p>Subject: <input type="text" value="Enroll Your Device"/> ⓘ</p> <p>Message: <input type="text" value="Enroll your device to gain access to company email and intranet. For instructions visit: \${zdmserver.hostPath}/enroll"/> ⓘ</p> <p><input type="checkbox"/> SMS ⚠ Channel cannot be activated until you define the SMS server in the Notification Server section in Settings.</p> <p>Message: <input type="text" value="Download XenMobile Agent: \${zdmserver.hostPath}/enroll"/> ⓘ</p>	Email*	Phone number*	+ Add
Email*	Phone number*	+ Add		

1. Defina essas configurações e clique em **Salvar**.

- **Destinatário:** para cada destinatário que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
 - **Email:** digite o endereço de email do destinatário. Este campo é obrigatório.
 - **Número de telefone:** digite o número de telefone do destinatário. Este campo é obrigatório.

Nota:

Para excluir um destinatário existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de lixeira à direita. Uma caixa de diálogo de confirmação é exibida. Clique em **Excluir** para excluir a listagem ou em **Cancelar** para mantê-la.

Para editar um destinatário existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Atualize a listagem e clique em **Salvar** para salvar a alteração ou em **Cancelar** para deixá-la inalterada.

- **Canais:** selecione um canal a ser usado para enviar o link de instalação de registro. Você pode enviar notificações por **SMTP** ou **SMS**. Esses canais não podem ser ativados até que você defina as configurações de servidor na página **Configurações** em **Servidor de notificação**. Para obter detalhes, consulte [Notificações](#).
- **SMTP:** defina estas configurações opcionais. Se você não digitar nada nesses campos, os valores padrão especificados no modelo de notificação configurado para a plataforma que você selecionou serão usados:
 - **Remetente:** insira um remetente opcional.
 - **Assunto:** digite um assunto opcional para a mensagem. Por exemplo, “Registre o seu dispositivo”.
 - **Mensagem:** digite uma mensagem opcional a ser enviada para o destinatário. Por

exemplo, “Registre o seu dispositivo para obter acesso aos aplicativos e ao email organizacionais”.

- **SMS:** defina essa configuração. Se você não digitar nada nesse campo, o valor padrão especificado no modelo de notificação configurado para a plataforma que você selecionou será usado:
 - **Mensagem:** digite uma mensagem opcional a ser enviada para os destinatários. Esse campo é obrigatório para notificações baseadas em SMS.

Nota: na América do Norte, as mensagens SMS que excedem 160 caracteres são entregues em várias mensagens.

2. Clique em **Send**.

Nota:

Se seu ambiente usar sAMAccountName, depois que os usuários receberem o convite e clicarem no link, eles deverão editar o nome do usuário para concluir a autenticação. O nome do usuário é exibido no formato sAMAccountName@domainname.com. Os usuários devem remover a parte @domainname.com.

Firebase Cloud Messaging

August 20, 2021

Nota:

Firebase Cloud Messaging (FCM) era anteriormente conhecido como Google Cloud Messaging (GCM). Alguns rótulos e mensagens do console XenMobile usam a terminologia do GCM.

A Citrix recomenda que você use o Firebase Cloud Messaging (FCM) para controlar como e quando dispositivos Android se conectam ao XenMobile. O XenMobile, quando configurado para FCM, envia notificações de conexão para dispositivos Android habilitados para FCM. Qualquer ação de segurança ou comando de implantação dispara uma notificação por push para solicitar ao usuário que se reconecte ao servidor XenMobile.

Depois de concluir as etapas de configuração deste artigo e um dispositivo fazer check-in, o dispositivo se registra no serviço FCM no XenMobile Server. Essa conexão permite a comunicação quase em tempo real do seu serviço XenMobile com o seu dispositivo usando o FCM. O registro do FCM funciona para registros de novos dispositivos e dispositivos registrados anteriormente.

Quando o XenMobile precisa iniciar uma conexão com o dispositivo, ele se conecta ao serviço FCM. Em seguida, o serviço FCM notifica o dispositivo para se conectar. Esse tipo de conexão é semelhante ao que a Apple usa para seu Serviço de Notificação por Push.

Pré-requisitos

- Secure Hub cliente mais recente
- Credenciais de conta de desenvolvedor do Google
- Serviços do Google Play instalados em dispositivos Android habilitados para FCM

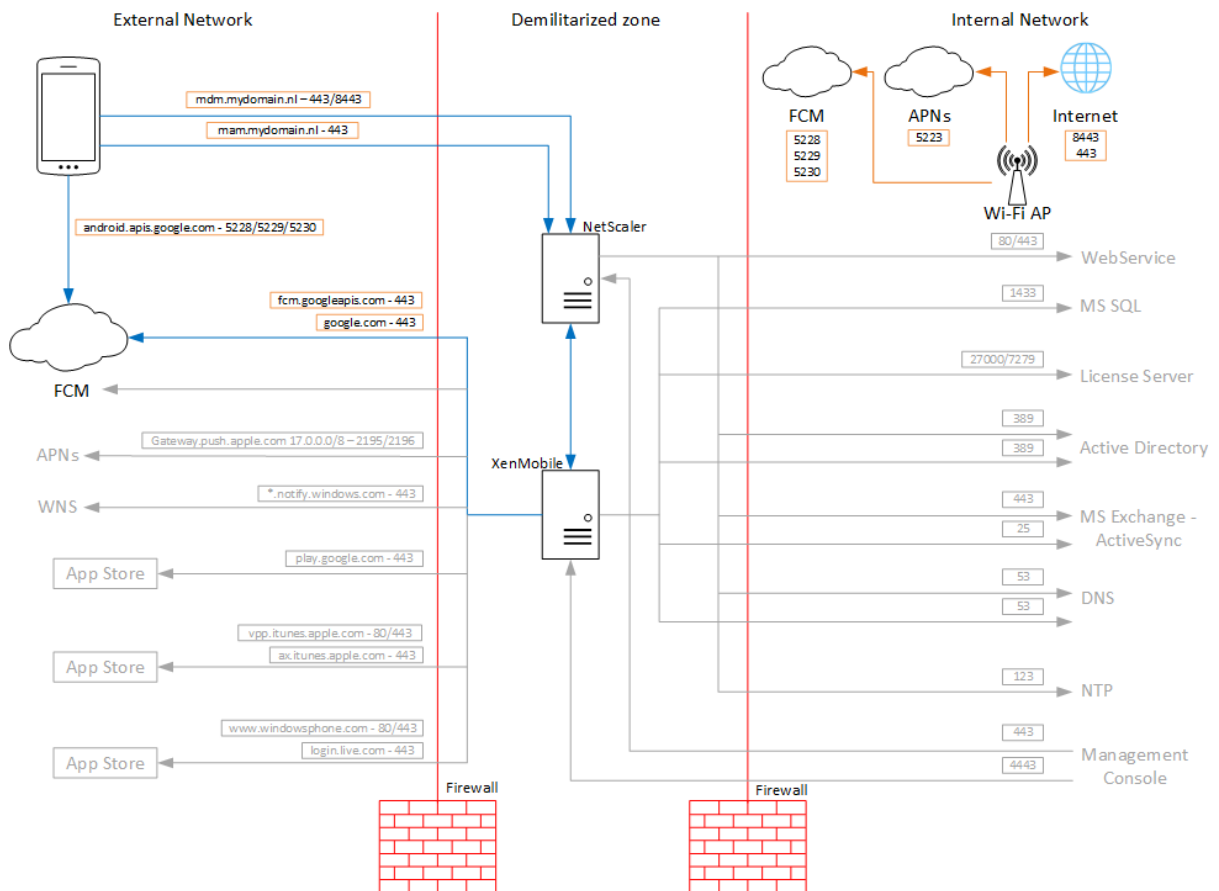
Portas de firewall

- Abra a porta 443 no XenMobile para `fcm.googleapis.com` e `Google.com`.
- Abrir comunicação com a Internet de saída para dispositivo Wi-Fi nas portas 5228, 5229 e 5230.
- Para permitir conexões de saída, o FCM recomenda a inclusão das portas de 5228 a 5230 na lista de permissão sem restrições de IP. No entanto, se você precisar de restrições de IP, o FCM recomenda colocar na lista de permissão todos os endereços IP nos blocos IPv4 e IPv6. Esses blocos estão listados no Google [ASN de 15169](#). Atualize essa lista mensalmente.

Para obter mais informações, consulte [Requisitos de porta](#).

Arquitetura

Esse diagrama mostra o fluxo de comunicação do FCM nas redes externa e interna.

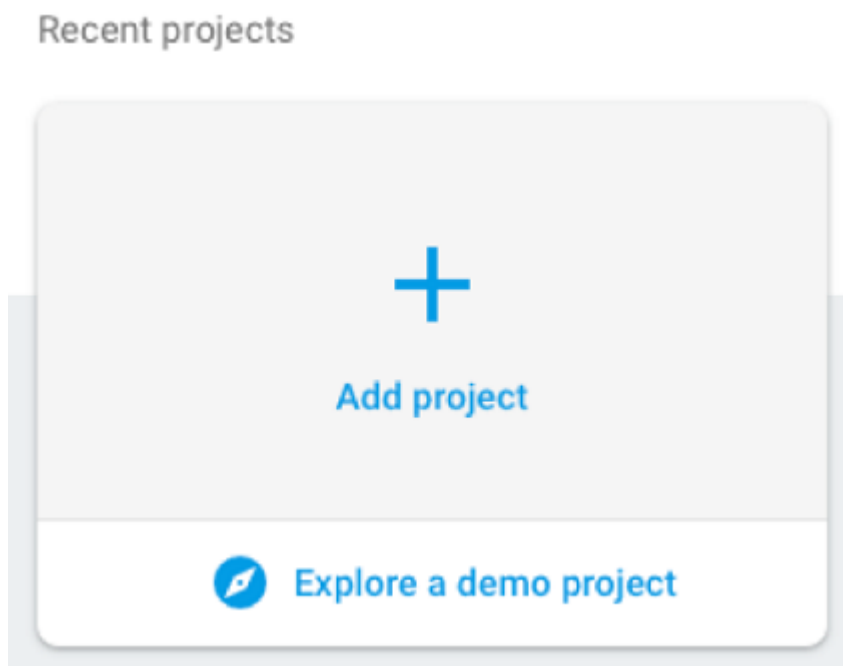


Para configurar sua conta do Google para FCM

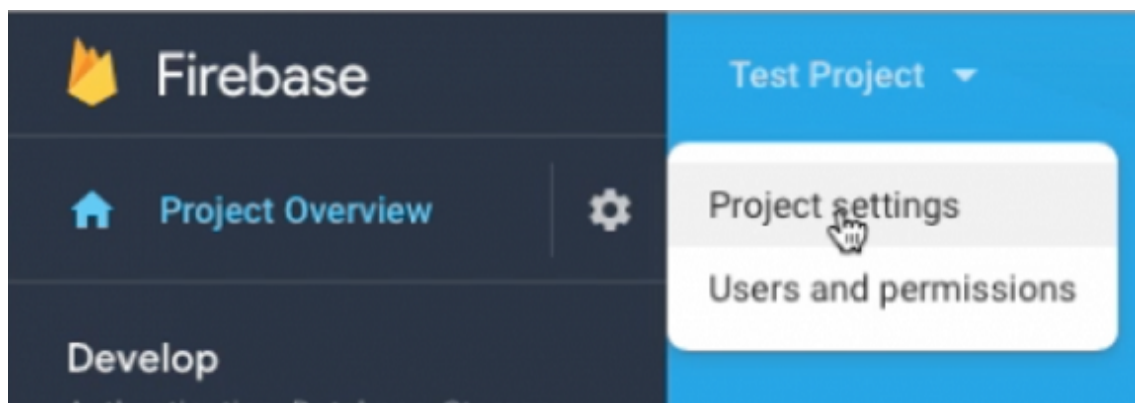
1. Faça login na seguinte URL usando suas credenciais de conta de desenvolvedor do Google:

<https://console.firebase.google.com/>

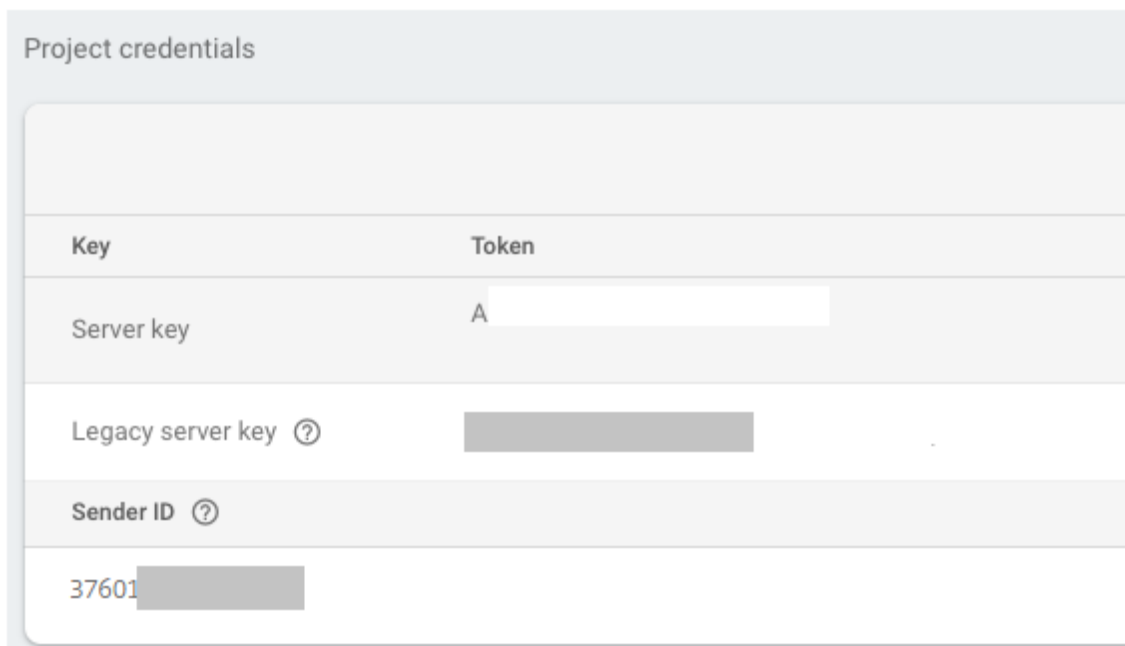
2. Clique em **Add project**.



3. Depois de criar o projeto, clique em **Project settings**.



4. Clique na guia **Cloud Messaging**. Copie os valores de **Server key** e **Sender ID**. No próximo procedimento, você cola esses valores no console XenMobile. A partir de outubro de 2016, você deve criar chaves de servidor no console do Firebase.

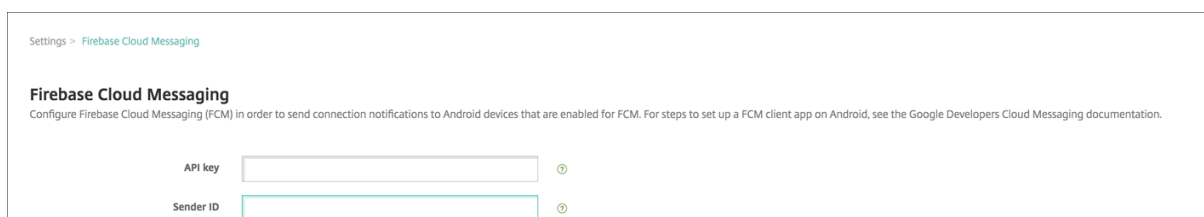


Para obter as etapas para configurar um aplicativo cliente FCM no Android, consulte este artigo do Google Developers Cloud Messaging: <https://firebase.google.com/docs/cloud-messaging/android/client>.

Para configurar o XenMobile para FCM

No console XenMobile, acesse **Configurações > Firebase Cloud Messaging**.

- Edite a **chave de API** e digite a **chave do servidor** do Firebase Cloud Messaging que você copiou na última etapa da configuração do Firebase Cloud Messaging.
- Edite o **ID do remetente** e digite o valor de **ID do remetente** copiado no procedimento anterior.

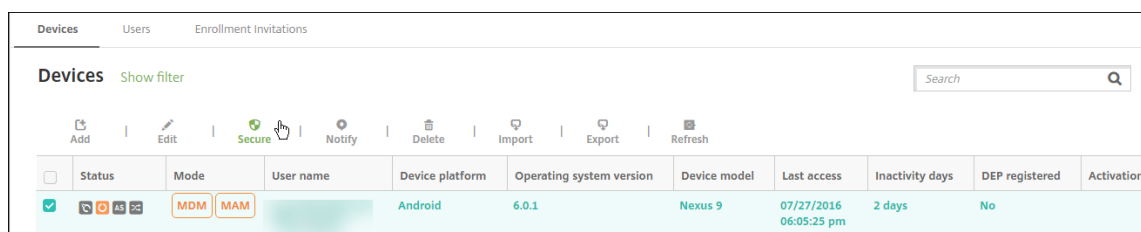


Depois de concluir a configuração, você pode remover a política de dispositivo Agendamento ou alterar essa política para se conectar com menos frequência.

Para testar sua configuração

1. Registre um dispositivo Android.
2. Deixe o dispositivo ocioso por algum tempo, para que ele seja desconectado do XenMobile.

3. Faça login no console XenMobile, clique em **Gerenciar**, selecione o dispositivo Android e clique em **Segurança**.



4. Em **Ações do dispositivo**, clique em **Apagamento seletivo**.



Em uma configuração bem-sucedida, o apagamento seletivo ocorre no dispositivo.

Integração com os recursos do Apple Educação

May 24, 2021

Você pode usar o XenMobile como sua solução de gerenciamento de dispositivos móveis (MDM) em um ambiente que usa o Apple Educação. O suporte ao XenMobile inclui o Apple School Manager (ASM) e o aplicativo Sala de Aula para iPad. A política de dispositivo de Configuração de Educação do XenMobile configura os dispositivos de instrutor e estudante para uso com o Apple Educação.

Você fornece iPads pré-configurados e supervisionados para instrutores e alunos. Essa configuração inclui o registro do ASM no XenMobile, uma conta do ID Apple gerenciado configurada com uma nova senha e os aplicativos e iBooks de compra por volume necessários.

Aqui estão os destaques do suporte do XenMobile para os recursos do Apple Educação.

Apple School Manager

ASM é um serviço que permite configurar, implantar e gerenciar dispositivos iOS (iPadOS) e laptops macOS utilizados em instituições educacionais. O ASM inclui um portal baseado na web que permite aos administradores de TI:

- Atribuir dispositivos do Programa de Implantação da Apple a diferentes servidores MDM.
- Comprar licenças de compra por volume para aplicativos e iBooks
- Crie **IDs Apple gerenciados** em massa. Esses IDs Apple personalizados fornecem acesso aos serviços da Apple, como armazenar documentos no iCloud Drive e registrar-se em cursos no Apple App Store.

Você pode adicionar várias contas ASM ao XenMobile. Por exemplo, este recurso permite usar diversas configurações de registro e opções de Assistente de Configuração por departamento ou unidade Educação. Em seguida, você associa contas ASM a diferentes políticas de dispositivo.

Depois de adicionar uma conta ASM ao console XenMobile, o XenMobile recupera as informações da aula e da lista. Durante a configuração do dispositivo, o XenMobile:

- Registra os dispositivos.
- Instala os recursos que você configurou para a implantação, como as políticas de dispositivo (Configuração de Educação, layout da tela inicial e assim por diante).
- Também instala aplicativos e iBooks adquiridos por meio da compra por volume.

Você fornece dispositivos pré-configurados e supervisionados para instrutores e alunos. Se um dispositivo for perdido ou roubado, você pode usar o recurso de modo Perdido do MDM para bloquear e localizar dispositivos.

Aplicativo Sala de Aula para iPad

O aplicativo Sala de Aula para iPad permite que os instrutores se conectem e gerenciem os dispositivos dos alunos. Você pode visualizar telas de dispositivos, abrir aplicativos em iPads e compartilhar e abrir links da Web.

O Sala de Aula é gratuito na App Store. Você carrega os arquivos para o console XenMobile. Em seguida, você usa a política do dispositivo Configuração de Educação para configurar o aplicativo Sala de Aula, que você implementa nos dispositivos dos instrutores.

Para obter mais informações sobre os recursos do Apple Educação, consulte o site Apple [Education](#) e o Guia de implementação para Educação da Apple que você encontra no site.

Pré-requisitos

- Citrix Gateway

- Perfil de registro configurado para MDM+MAM.
- Apple iPad 3ª geração (versão mínima) ou iPad Mini, com iOS 9.3 (versão mínima)

Nota:

O XenMobile não valida contas de usuário ASM em relação ao LDAP ou ao Active Directory. No entanto, você pode conectar o XenMobile ao LDAP ou ao Active Directory para gerenciamento de usuários e dispositivos não relacionados aos instrutores ou alunos do ASM. Por exemplo, você pode usar o Active Directory para fornecer o Secure Mail e Secure Web para outros membros do ASM, como administradores de TI e gerentes.

Como os instrutores e estudantes do ASM são usuários locais, não é necessário implantar o Citrix Secure Hub em seus dispositivos.

A inscrição da MAM que inclui a autenticação do Citrix Gateway não é compatível com usuários locais (apenas usuários do Active Directory). Portanto, o XenMobile implanta apenas aplicativos e iBooks de compra por volume necessários para os dispositivos dos instrutores e dos estudantes.

Pré-requisitos para iPads compartilhados

- Qualquer iPad Pro, iPad de 5ª geração, iPad Air 2, ou posterior, e iPad mini 4, ou posterior
- Pelo menos 32 GB de armazenamento
- Supervisionado

Configurar Apple School Manager e XenMobile

Depois de comprar iPads da Apple ou de Revendedores ou operadoras autorizadas da Apple: siga o fluxo de trabalho nesta seção para configurar sua conta ASM e seus dispositivos. Este fluxo de trabalho inclui etapas que você executa no portal ASM e no console XenMobile.

Siga estas instruções para configurar a integração para todos os iPads que você usa nos moldes um-para-um (um iPad por aluno) ou para iPads do instrutor (não compartilhado). Para configurar iPads compartilhados, consulte [Configurar iPads compartilhados](#).

Etapa 1: Crie sua conta do Apple School Manager e siga o Assistente de Configuração

Se você planeja atualizar o Programa de Implantação da Apple, consulte o artigo de suporte da Apple [Faça o upgrade da sua instituição para ASM](#). Para criar sua conta ASM, acesse <https://school.apple.com/> e siga as instruções para se registrar. Na primeira vez que você fizer logon no ASM, o Assistente de Configuração é aberto.

- Para obter informações sobre os pré-requisitos do ASM, o Assistente de Configuração e as tarefas de gerenciamento, consulte o [Guia do usuário do Apple School Manager](#).

- Ao configurar um ASM, use um nome de domínio diferente do nome de domínio do Active Directory. Por exemplo, prefixe o nome de domínio do ASM com algo como `appleid`.
- Quando você conecta o ASM aos dados na sua lista, o ASM cria IDs Apple gerenciados para instrutores e alunos. Os seus dados de listagem incluem instrutores, alunos e aulas. Para obter informações sobre como adicionar dados de lista ao ASM, consulte o Guia do Usuário do ASM, mencionado anteriormente.
- Você pode personalizar o formato do ID Apple gerenciado para sua instituição, conforme descrito no Guia do Usuário do ASM, mencionado anteriormente.

Importante:

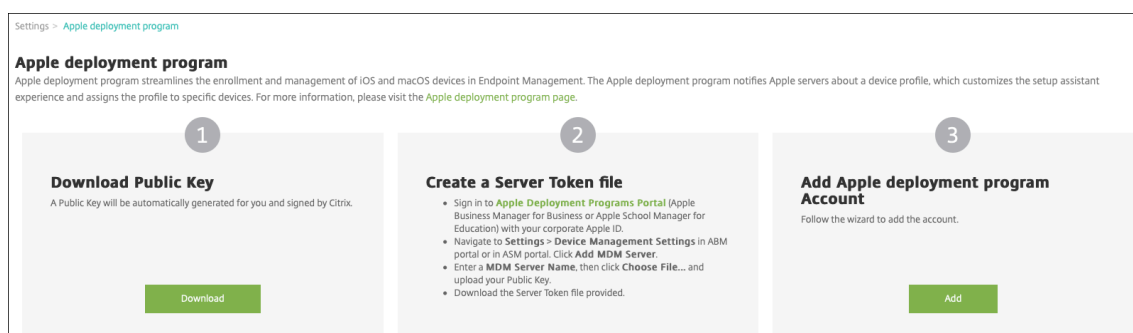
Não altere IDs Apple gerenciados depois de importar as informações do ASM para o XenMobile.

- Se você comprou dispositivos através de revendedores ou operadoras, faça a ligação desses dispositivos ao ASM Para obter informações, consulte o Guia do Usuário do ASM, mencionado anteriormente.

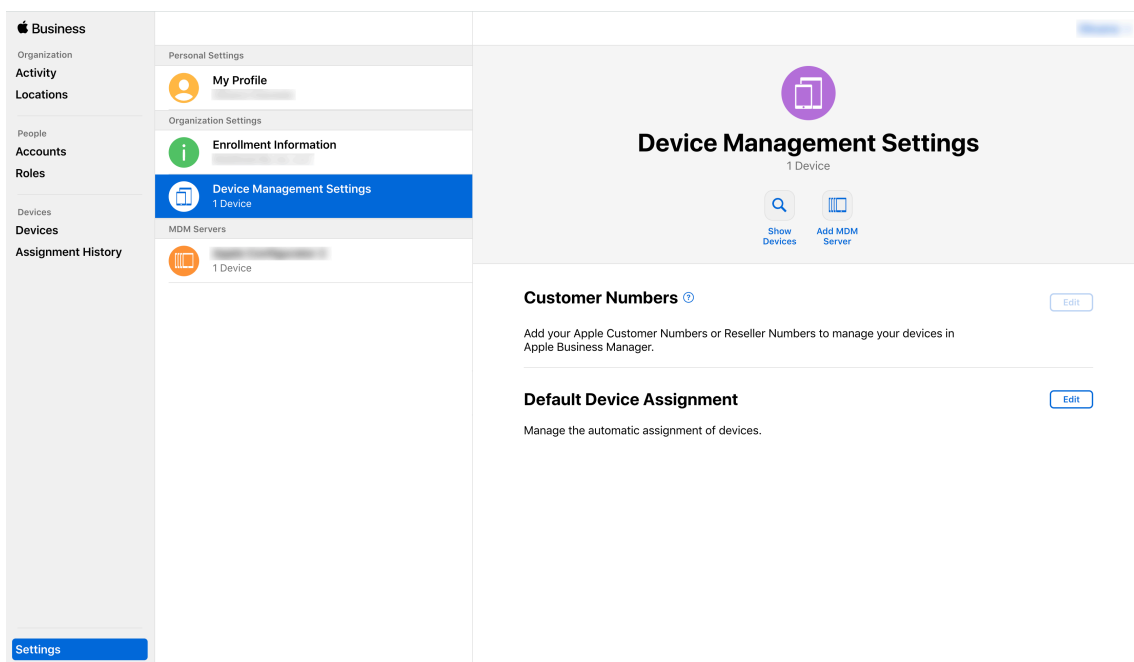
Etapa 2: Configure o XenMobile como o servidor MDM para o Apple School Manager e configure as atribuições do dispositivo

O portal ASM inclui uma guia de **Servidores MDM**. Você precisa do arquivo de chave pública do XenMobile para concluir a configuração.

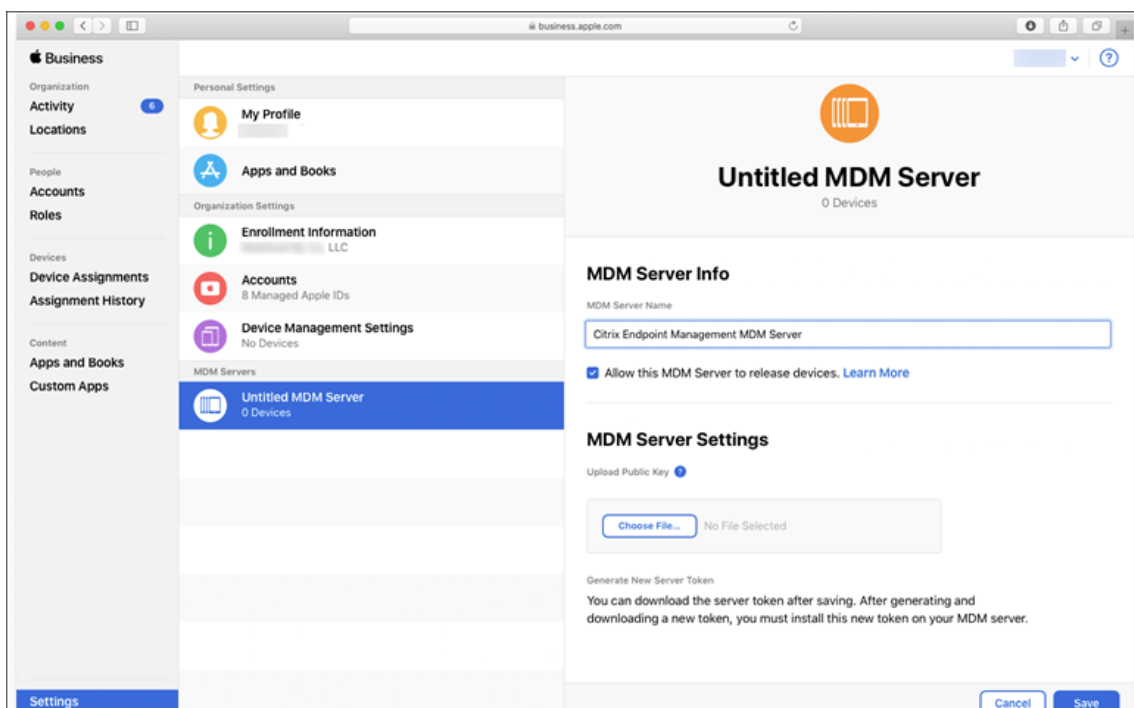
1. Baixe sua chave pública do XenMobile para o computador local: no console XenMobile, acesse **Configurações > Programa de implantação da Apple**.



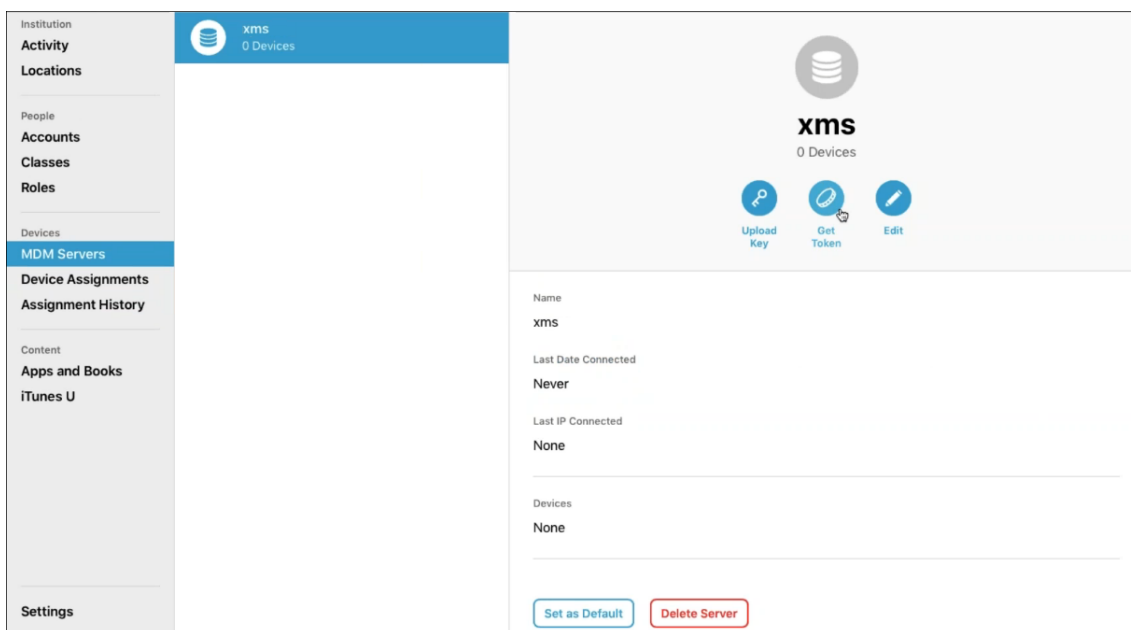
2. Em **Baixar a chave pública**, clique em **Download** e salve o arquivo PEM.
3. No portal do **Apple School Manager**, clique em **Settings** e em **Device Management Settings**. Clique em **Add MDM Server**.



4. Digite um nome para o XenMobile. O nome do servidor que você digita é para sua referência e não é a URL ou o nome do servidor. Em **Upload Public Key**, clique em **Choose File**.



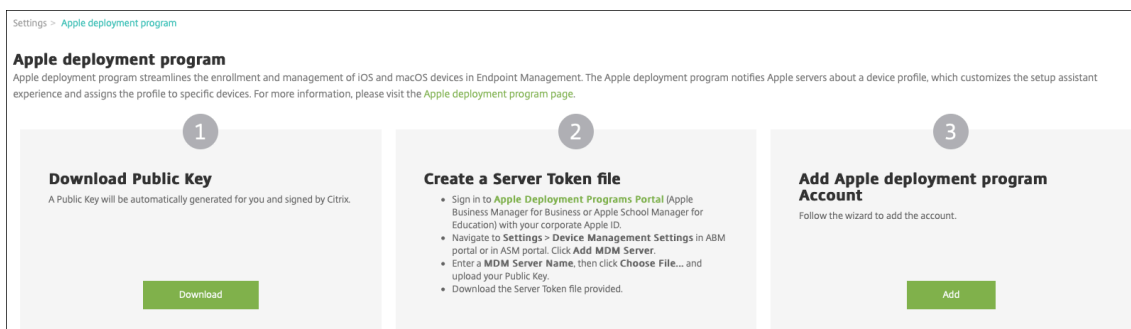
5. Carregue a chave pública que você baixou do XenMobile e clique em **Save**.
6. Gere um token de servidor: clique em **Download Token** e baixe o arquivo de token do servidor para o seu computador.



7. Em **Default Device Assignment**, clique em **Change**. Escolha como deseja atribuir dispositivos e, em seguida, forneça as informações solicitadas. Para obter informações, consulte o [Guia do Usuário do ASM](#).

Etapa 3: Adicione a conta do Apple School Manager ao XenMobile

1. No console XenMobile, acesse **Configurações > Programa de implantação da Apple** e, em **Adicionar conta do programa de implantação da Apple**, clique em **Adicionar**.



2. Na página **Tokens de servidor**, clique em **Carregar** e escolha o arquivo de token do servidor (um arquivo P7M) que você baixou do portal ASM. As informações do token são exibidas.

Apple deployment program Account	Server Tokens
1 Server Tokens	Upload the Server Token file that you downloaded from Apple Business Manager portal or Apple School Manager portal.
2 Account Info	Select Server Token file <input type="text" value="untitled_mdm_server_token_..."/> <input type="button" value="Upload"/>
3 Settings	Consumer key [Redacted]
iOS	Consumer secret [Redacted]
macOS	Access token [Redacted]
Apple TV	Access secret [Redacted]
4 Setup Assistant Options	Access token expiration 10/30/20 6:25:52 pm
iOS	Server name Untitled MDM Server
macOS	Server UUID [Redacted]
Apple TV	Apple admin ID [Redacted]
	Organization ID [Redacted]
	Organization name [Redacted]
	Organization type Education
	Organization version v2
	Organization email [Redacted]
	Organization phone [Redacted]
	Organization address [Redacted]

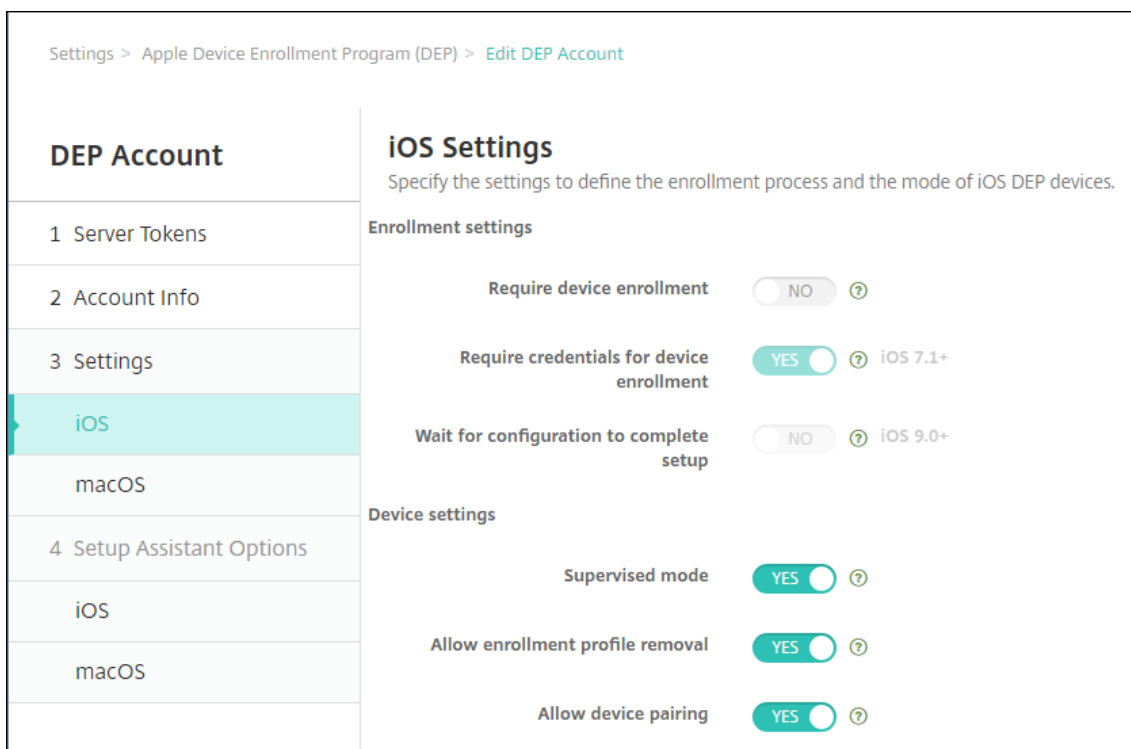
Notas:

- **ID da organização** é o seu ID de cliente do Programa de Implantação da Apple.
 - As contas ASM possuem **Tipo da organização** de **Educação** e **Versão da organização** de **v2**.
3. Na página **Informações sobre a conta**, especifique as seguintes configurações.

Apple deployment program Account	Account Info
1 Server Tokens	Specify your Apple deployment program account information.
2 Account Info	<p>Apple deployment program account name * <input type="text" value="ASM Deployment"/></p> <p>Business/Education unit * <input type="text" value="Central High School"/></p> <p>Unique service ID <input type="text" value="2359487"/></p> <p>Support phone number * <input type="text" value="555555555"/></p> <p>Support email address <input type="text"/></p> <p>Education suffix * <input type="text" value="suffix"/></p>
3 Settings	
iOS	
macOS	
Apple TV	
4 Setup Assistant Options	
iOS	
macOS	
Apple TV	

- **Nome da conta do Programa de Implantação da Apple:** um nome exclusivo para esta conta do Programa de Implantação da Apple. Use nomes que reflitam como você organiza contas do Programa de implantação da Apple, como por país ou hierarquia organizacional.
- **Unidade de negócios/educação:** a unidade ou departamento de Educação para a atribuição de dispositivos. Este campo é obrigatório.
- **ID de serviço exclusiva:** um ID exclusivo opcional para ajudar você a identificar ainda mais a conta.
- **Número de telefone de suporte:** um número de telefone de suporte para o qual os usuários podem ligar para pedir ajuda durante a instalação. Este campo é obrigatório.
- **Endereço de email de suporte:** um endereço de email de suporte opcional, disponível para os usuários finais.
- **Sufixo de educação:** sinaliza as classes de uma determinada conta do Programa de implantação do ASM. (O sufixo de compra por volume sinaliza aplicativos e iBooks para uma determinada conta de compra por volume.) A recomendação é usar o mesmo sufixo para ambas as contas, do Programa de Implantação do ASM e de compra por volume do ASM.

4. Clique em **Avançar**. Em **Configurações do iOS**, especifique as seguintes configurações.



• Configurações de registro

- **Exigir registro de dispositivo:** solicite que os usuários registrem seus dispositivos. Altere essa configuração para **Não**.
- **Exigir credenciais para registro de dispositivo:** requer que os usuários insiram suas credenciais durante a configuração do Programa de implantação da Apple. Para a integração do ASM com o XenMobile, essa configuração é **Sim** por padrão e não pode ser alterada. O Programa de Implementação da Apple requer credenciais para o registro do dispositivo.
- **Aguardar que a configuração conclua a instalação:** selecione se os dispositivos do usuário devem ser obrigados a permanecer no modo do Assistente de instalação até que todos os recursos do MDM sejam implantados no dispositivo. Para a integração do ASM com o XenMobile, essa configuração é **Não** por padrão. De acordo com a documentação da Apple, os seguintes comandos poderão não funcionar enquanto o dispositivo estiver no modo Assistente de Instalação:
 - * InviteToProgram
 - * InstallApplication
 - * InstallMedia
 - * ApplyRedemptionCode

• Configurações do dispositivo

- **Modo supervisionado:** colocar os dispositivos iOS no modo supervisionado. Não al-

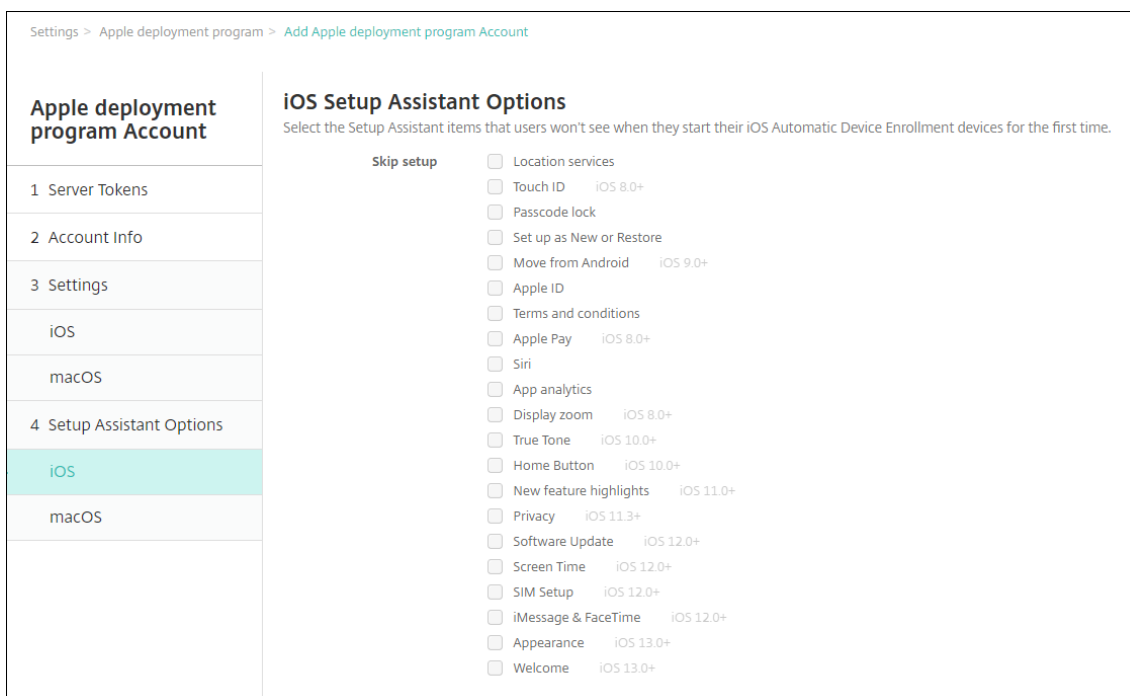
tere o padrão, **Sim**. Para obter detalhes sobre como colocar um dispositivo iOS no modo supervisionado, consulte [Para colocar um dispositivo iOS no modo Supervisionado usando o Apple Configurator](#).

- **Modo compartilhado:** habilitar o modo compartilhado em iPads. Dispositivos que não atendam aos requisitos mínimos não podem compartilhar.
- **Permitir remoção do perfil de registro:** na integração do ASM, permita que o usuário remova o perfil de registro do dispositivo. Altere essa configuração para **Sim**.
- **Permitir o emparelhamento de dispositivos:** na integração do ASM, permita o emparelhamento de dispositivos para que você possa gerenciá-los através da Apple App Store e do Apple Configurator. Altere essa configuração para **Sim**.

5. Em **Opções do assistente de instalação do iOS**, selecione as etapas do Assistente de instalação do iOS que serão ignoradas quando os usuários iniciarem seus dispositivos pela primeira vez. Por padrão, o Assistente de instalação inclui todas as etapas. Considere que remover etapas do Assistente de Configuração simplifica a experiência do usuário.

Importante:

A Citrix recomenda que você inclua as etapas de **ID Apple e Termos e Condições**. Essas etapas permitem que os instrutores e os alunos forneçam suas novas senhas do ID Apple Gerenciado e aceitem os termos e condições exigidos.



- **Serviços de localização:** configurar o serviço de localização no dispositivo.
- **Touch ID:** configurar o Touch ID nos dispositivos iOS.

- **Bloqueio de código secreto:** criar uma senha para o dispositivo.
 - **Configurar como novo ou restaurar:** configurar o dispositivo como novo ou de um backup do iCloud ou da Apple App Store.
 - **Mover do Android:** permitir a transferência de dados de um dispositivo Android para um dispositivo iOS. Essa opção está disponível somente quando **Configurar como novo ou restaurar** está selecionada (ou seja, a etapa é ignorada).
 - **ID Apple:** configurar uma conta do ID Apple para o dispositivo. A Citrix recomenda que você marque a caixa de seleção para incluir esta etapa.
 - **Termos e condições:** exigir que os usuários aceitem os termos e as condições de uso do dispositivo. A Citrix recomenda que você marque a caixa de seleção para incluir esta etapa.
 - **Apple Pay:** configurar o Apple Pay em dispositivos iOS.
 - **Siri:** usar ou não a Siri no dispositivo.
 - **Análise de aplicativo:** configurar se os dados de falha e as estatísticas de uso devem ser compartilhados com a Apple.
 - **Zoom de exibição:** configurar a resolução da tela (padrão ou ampliada) nos dispositivos iOS.
 - **True Tone:** configurar o True Tone Display nos dispositivos iOS.
 - **Botão Home:** configurar a sensibilidade da tela do botão Home.
 - **Destaques do novo recurso:** configurar as telas informativas de integração, acessar o Dock em qualquer lugar e alternar entre aplicativos recentes em dispositivos iOS 11.0 (versão mínima).
 - **Privacidade:** impedir que os usuários vejam os dados e o painel de privacidade durante a configuração dos dispositivos do Programa de implantação da Apple. Para iOS 11.3 e posterior.
 - **SoftwareUpdate:** impedir que o usuário veja a tela de atualização de software obrigatória durante a configuração dos dispositivos do Programa de implantação da Apple. Para iOS 12.0 e posterior.
 - **ScreenTime:** impedir que o usuário veja a tela Tempo de Tela durante a configuração dos dispositivos do Programa de implantação da Apple. Para iOS 12.0 e posterior.
 - **Configuração do SIM:** impedir que o usuário veja a tela Add Cellular Plan durante a configuração de dispositivos do Programa de implantação da Apple. Para iOS 12.0 e posterior.
 - **iMessage & FaceTime:** impedir que o usuário veja a tela do iMessage e do FaceTime durante a configuração dos dispositivos do Programa de implantação da Apple. Para iOS 12.0 e posterior.
6. A conta aparece em **Configurações > Programa de implantação da Apple**. Para testar a conectividade entre o XenMobile e a sua conta ASM, selecione a conta e clique em **Testar conectividade**.

Settings > Apple Deployment Program

Apple Deployment Program

Apple deployment program streamlines the enrollment and management of iOS and macOS devices in Endpoint Management. The Apple deployment program notifies Apple servers about a device profile, which customizes the setup assistant experience and assigns the profile to specific devices. For more information, please visit the [Apple deployment program page](#).

1

Download Public Key

A Public Key will be automatically generated for you and signed by Citrix.

Download

2

Create a Server Token file

- Sign in to [Apple deployment programs portal](#) (Apple Business Manager for Business or Apple School Manager for Education) with your corporate Apple ID.
- Navigate to Settings > Device Management Settings in ABM portal or in ASM portal. Click Add MDM Server.
- Enter a MDM Server Name, then click Choose File... and upload your Public Key.
- Download the Server Token file provided.

3

Add Apple Deployment Program Account

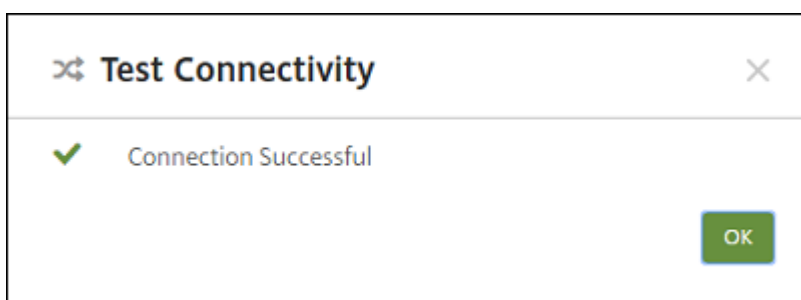
Follow the wizard to add the account.

Add

<input type="checkbox"/>	Apple deployment program account name	Business/Education unit	Status	Organization type	Organization email	Created on	Server token expires on
--------------------------	---------------------------------------	-------------------------	--------	-------------------	--------------------	------------	-------------------------

No results found.

É exibida uma mensagem de status.



Após alguns minutos, as contas de usuário ASM aparecem na página **Gerenciar > Usuários**. O XenMobile cria contas de usuário locais com base no ID Apple gerenciado importado para cada usuário. No exemplo a seguir, o prefixo de nome de domínio de IDs Apple personalizados para contas de usuário é `appleid`.

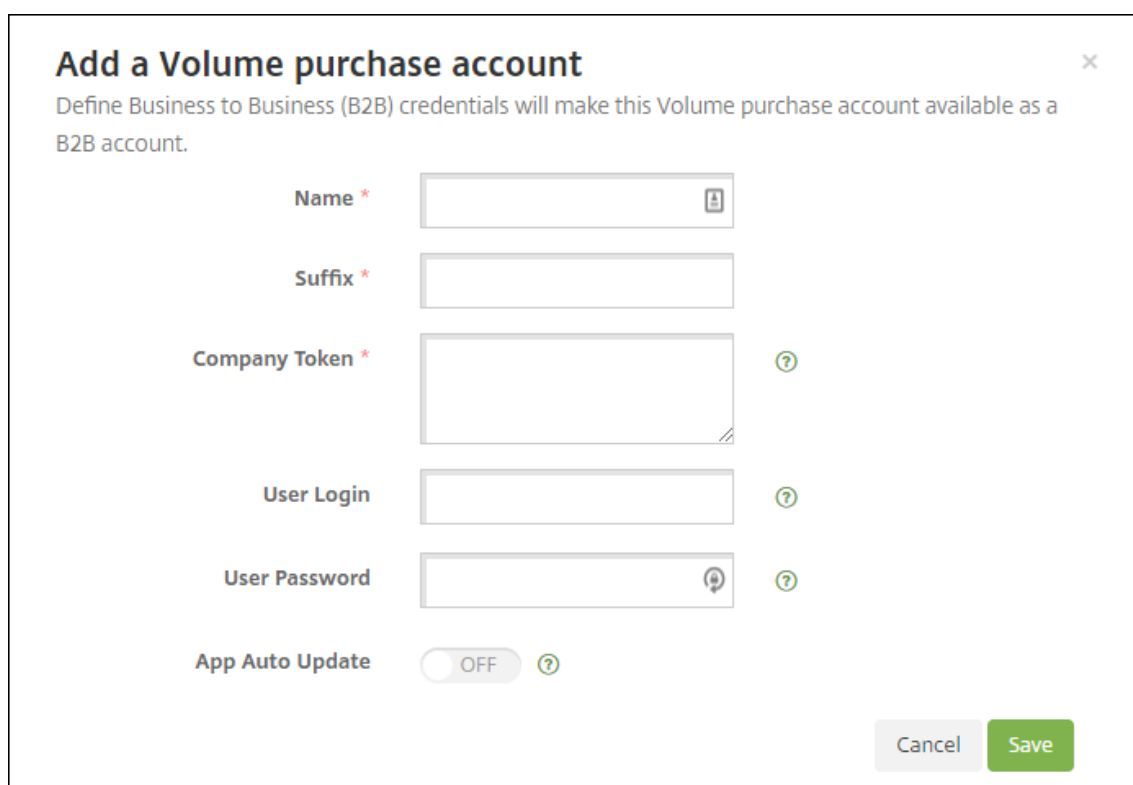
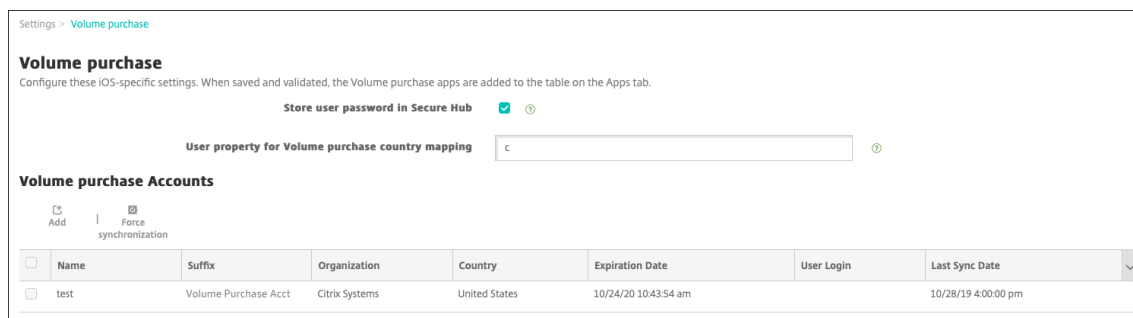
<input type="checkbox"/>	User name	First name	Last name	User type	Roles	Groups	Domain	Created	Last authenticated	ASM account name
<input type="checkbox"/>		Brooklyn	Baily	ASM	USER	SAMPLE-CLASS-1010.SAMPLE-CLASS-1014	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM account
<input type="checkbox"/>		Lucas	Leong	ASM	USER	SAMPLE-CLASS-1013.SAMPLE-CLASS-1014	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM account
<input type="checkbox"/>		Alex	Mieull	ASM	USER	SAMPLE-CLASS-0001	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM account
<input type="checkbox"/>		Savannah	Cashman	ASM	USER	SAMPLE-CLASS-1010.SAMPLE-CLASS-1011	local	6/6/17 3:21 PM	6/13/17 6:46 PM	US ASM account
<input type="checkbox"/>		Aiden	Westover	ASM	USER	SAMPLE-CLASS-0001	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM account
<input type="checkbox"/>		Ava	Meinerth	ASM	USER	SAMPLE-CLASS-0001	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM account
<input type="checkbox"/>		Liam	Wilson	ASM	USER	SAMPLE-CLASS-1013.SAMPLE-CLASS-1014	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM account
<input type="checkbox"/>		Brayden	Anderson	ASM	USER	SAMPLE-CLASS-0001	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM account
<input type="checkbox"/>		Gabriel	Zeifman	ASM	USER	SAMPLE-CLASS-1012.SAMPLE-CLASS-1014	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM account
<input type="checkbox"/>		Gavin	Tien	ASM	USER	SAMPLE-CLASS-1012.SAMPLE-CLASS-1014	local	6/6/17 3:21 PM	6/12/17 5:04 PM	US ASM account

Para encontrar todos os usuários de uma determinada conta ASM, digite o nome da conta no filtro de pesquisa do usuário.

Etapa 4: Configure uma conta de compra por volume de Educação para o Apple School Manager

Nesta seção, aponte o XenMobile para a conta de compra por volume usada para adquirir licenças de compra por volume para aplicativos e eBooks.

1. Para configurar uma conta de compra por volume de Educação para o ASM, siga as instruções em [Compra por volume da Apple](#). A tela Adicionar uma conta de compra por volume requer que você forneça um token da empresa. Baixe seu token diretamente da sua conta de compra por volume de Educação e cole-o na tela **Adicionar uma conta de compra por volume**.



2. Aguarde alguns minutos para que as licenças de compra por volume sejam importadas para o XenMobile.

Etapa 5: Adicione senhas para usuários do Apple School Manager

Depois de adicionar uma conta ASM, o XenMobile importa classes e usuários do ASM. O XenMobile trata classes como grupos locais e usa o termo “grupo” no console. Se uma classe tiver um nome de grupo no ASM, o XenMobile atribui o nome do grupo à classe. Caso contrário, o XenMobile usa o ID do sistema de origem para o nome do grupo. O XenMobile não usa o nome do curso para o nome da classe porque os nomes dos cursos no ASM não são exclusivos.

O XenMobile usa os IDs Apple gerenciados para criar usuários locais com o tipo de usuário **ASM**. Os usuários são locais porque o ASM cria as credenciais independentemente de todas as fontes de dados externas. Como resultado, o XenMobile não usa um servidor de diretório para autenticar esses novos usuários.

O ASM não envia senhas de usuário temporárias para o XenMobile. Você pode importá-las de um arquivo CSV ou adicioná-las manualmente. Para importar senhas temporárias de usuários:

1. Obtenha o arquivo CSV gerado pelo ASM ao criar as senhas temporárias do ID Apple gerenciado.
2. Edite o arquivo CSV, substituindo as senhas temporárias por novas senhas que os usuários fornecem para se inscrever no XenMobile. Não há restrições no tipo de senha para este propósito.

O formato de uma entrada no arquivo CSV é o seguinte: `user@appleid.citrix.com,Firstname,Middle,Lastname>Password123!`

Onde:

Usuário: `user@appleid.citrix.com`

Nome: `Firstname`

Segundo nome: `Middle`

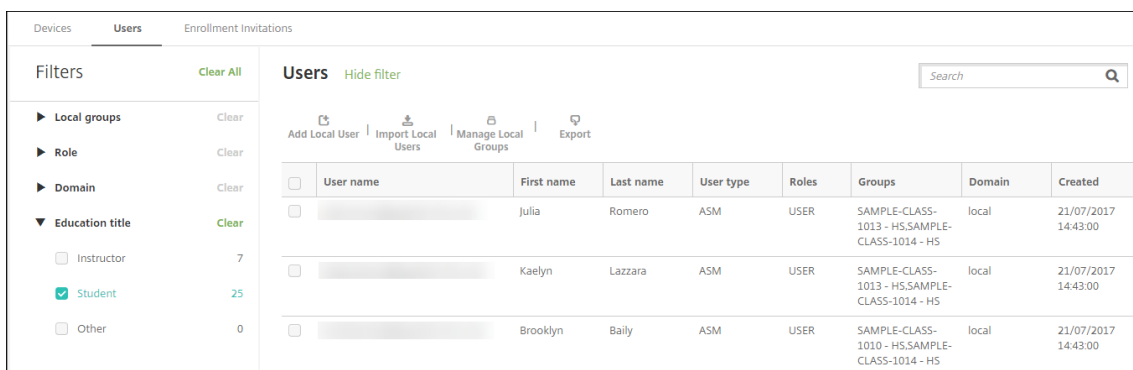
Sobrenome: `Lastname`

Senha: `Password123!`

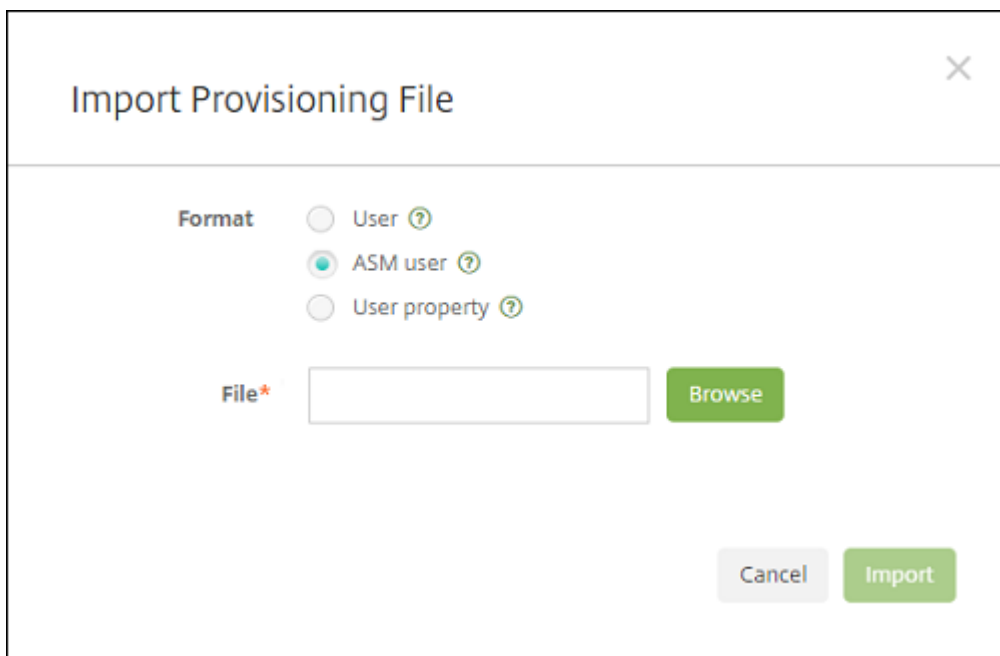
3. No console XenMobile, clique em **Gerenciar > Usuários**. A página **Usuários** é exibida.

O seguinte exemplo da tela **Gerenciar > Usuários** mostra uma lista de usuários importados do ASM. Na lista **Usuários**:

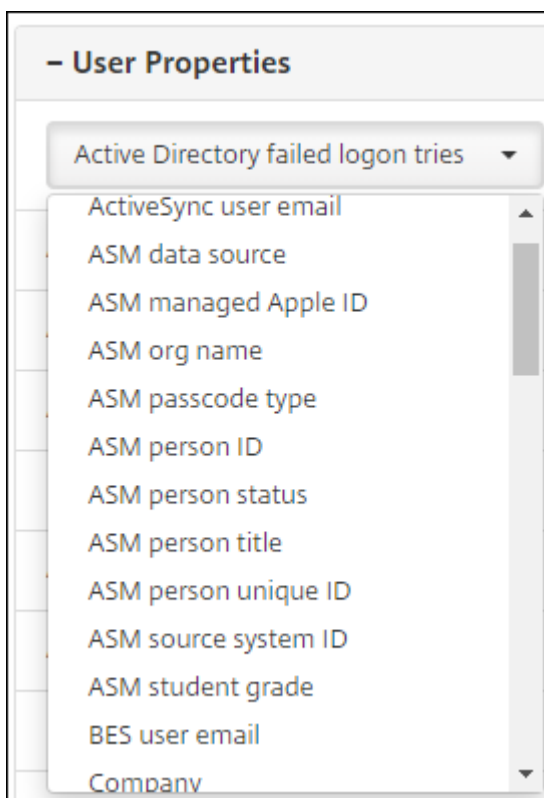
- **Nome do usuário** mostra o ID Apple gerenciado.
- O tipo de usuário é **ASM**, para indicar que a conta originou do ASM.
- **Grupos** mostram as classes.



4. Clique em **Importar usuários locais**. A caixa de diálogo **Importar Arquivo de Provisionamento** é exibida.
5. Para Formato, escolha **Usuário ASM**, navegue até o arquivo CSV que você preparou na etapa 2 e clique em **Importar**.



6. Para exibir as propriedades de um usuário local, selecione o usuário e, em seguida, clique em **Editar**.



Além das propriedades de nome, estas propriedades ASM estão disponíveis:

- **Origem de dados ASM:** a origem dos dados da classe, como **CSV** ou **SFTP**.
- **ID Apple gerenciado no ASM:** o ID Apple gerenciado pode incluir o nome da sua instituição e `appleid`. Por exemplo, o ID pode ser semelhante a `johnappleseed@appleid.myschool.edu`. O XenMobile requer um ID Apple Gerenciado para autenticação.
- **Nome da organização ASM:** o nome que você deu à conta no XenMobile.
- **Tipo de código secreto do ASM:** política de senha da pessoa: **complexa** (uma senha não estudantil de oito ou mais números e letras), **quatro** (dígitos) ou **seis** (dígitos).
- **ID exclusivo da pessoa no ASM:** identificador do usuário.
- **Status da pessoa no ASM:** especifica se o ID Apple gerenciado está **Ativo** ou **Inativo**. Esse status se torna ativo depois que o usuário fornece sua nova senha da conta do ID Apple gerenciado.
- **Título de pessoa no ASM:** o instrutor, aluno ou outro.
- **ID exclusivo da pessoa no ASM:** um identificador exclusivo para o usuário.
- **ID do sistema de origem ASM:** identificador da origem do sistema.
- **Nível do aluno no ASM:** informações do nível do aluno (não utilizadas pelos instrutores).

Etapa 6: Opcionalmente, adicione fotos de alunos

Você pode adicionar uma foto de cada aluno. Se os instrutores usam o aplicativo Apple Classroom, as fotos aparecem neste aplicativo.

Recomendado para fotos:

- Resolução: 256 x 256 pixels (512 x 512 pixels em um dispositivo 2x)
- Formato: JPEG, PNG ou TIFF

Para adicionar uma foto, vá para **Gerenciar > Usuários**, selecione um usuário, clique em **Editar** e, em seguida, clique em **Escolher imagem**.

The screenshot shows the 'Edit Local User' interface. It includes the following elements:

- Navigation tabs: Devices, Users, Enrollment Invitations.
- Form fields: User name, Password (placeholder: Enter new password), Role (dropdown: USER), Membership (checkboxes for local\SAMPLE-CLASS-1012 - ASM, local\SAMPLE-CLASS-1013 - ASM, local\SAMPLE-CLASS-1014 - ASM).
- Buttons: Manage Groups, Choose image.
- Text: ASM student image (256 x 256 or 512 x 512 pixels on a 2x device).
- Table: User Properties table with columns for property name and value.

- User Properties		Add
ASM account name	US ASM .	
ASM person title	Student	
ASM person unique ID		

Etapa 7: Planeje e adicione recursos e grupos de entrega ao XenMobile

Um grupo de entrega especifica os recursos para implantar em categorias de usuários. Por exemplo, você pode criar um grupo de entrega para instrutores e alunos. Alternativamente, você pode criar vários grupos de entrega para poder personalizar aplicativos, mídias e políticas enviadas para vários instrutores ou alunos. Você pode criar um ou mais grupos de entrega por aula. Você também pode criar um ou mais grupos de entrega para gerentes (outras equipes na sua instituição educacional).

Os recursos que você implementa nos dispositivos do usuário incluem políticas do dispositivo, aplicativos de compra por volume e iBooks.

- Políticas de dispositivo:

Se os instrutores usam o aplicativo de Sala de Aula, é necessária a política do dispositivo Configuração de Educação. Lembre-se de revisar outras políticas de dispositivo para determinar como você deseja configurar e restringir iPads e alunos e instrutores.

- Aplicativos de compra por volume:

O XenMobile requer que você implante aplicativos de compra por volume como aplicativos necessários para que os usuários de educação. O XenMobile não oferece suporte à implantação de aplicativos de compra por volume como opcionais.

Se você usa o aplicativo Apple Classroom, implemente-o apenas nos dispositivos de instrutores.

Implemente quaisquer outros aplicativos que você queira fornecer aos instrutores ou alunos. Esta solução não usa o aplicativo Citrix Secure Hub, portanto, não há necessidade de implementá-lo para instrutores ou alunos.

- iBooks de compra por volume:

Depois que o XenMobile se conecta à sua conta ASM, seus iBooks adquiridos aparecem no console XenMobile, em **Configurar > Mídia**. Os iBooks listados nessa página estão disponíveis para adicionar a grupos de entrega. O XenMobile suporta a adição de iBooks apenas como mídia obrigatória.

Depois de planejar os recursos e os grupos de entrega para instrutores e alunos, você pode criar esses itens no console XenMobile.

1. Crie as políticas de dispositivo que você deseja implantar nos dispositivos do instrutor ou aluno. Para obter informações sobre a política do dispositivo de Configuração de Educação, consulte a [Política de dispositivo Configuração de Educação](#).

Education Configuration Policy

This policy defines the Apple Classroom app settings for instructor devices and the certificates used to perform client authentication between instructor and student devices. When you choose a class in this policy, XenMobile fills in the instructors and students from your Apple School Manager configuration.

Display Name*	Description	Instructors*	Students*	⊞ Add
SAMPLE-CLASS-0001 - HS		@appleid.citrix.com, @appleid.citrix.com	@appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com	
SAMPLE-CLASS-1010 - HS		@appleid.citrix.com	@appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com	
SAMPLE-CLASS-1011 - HS		@appleid.citrix.com	@appleid.citrix.com	
SAMPLE-CLASS-1012 - HS		@appleid.citrix.com	@appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com	

Allow students to change screen observation permission ON ⓘ
iOS 10.3+

Policy Settings

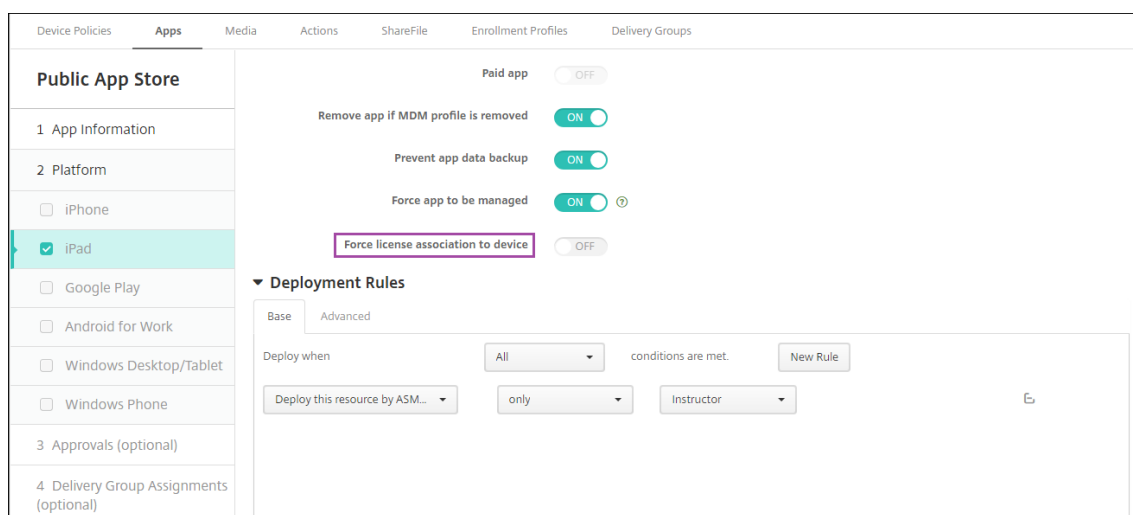
Remove policy Select date
 Duration until removal (in hours)

Consulte [Políticas de dispositivo](#) e os artigos individuais para obter informações sobre as políticas de dispositivo.

2. Configure aplicativos (**Configurar > Aplicativos**) e iBooks (**Configurar > Mídia**):

- Por padrão, o XenMobile atribui aplicativos e iBooks no nível do usuário. Durante a implantação pela primeira vez, instrutores e alunos recebem uma mensagem para se registrar no ASM. Após aceitar o convite, os usuários recebem seus aplicativos e iBooks do ASM na próxima implantação (dentro seis horas). A Citrix recomenda que você force a implantação de aplicativos e iBooks para novos usuários ASM. Para fazer isso, selecione o grupo de entrega e clique em **Implantar**.

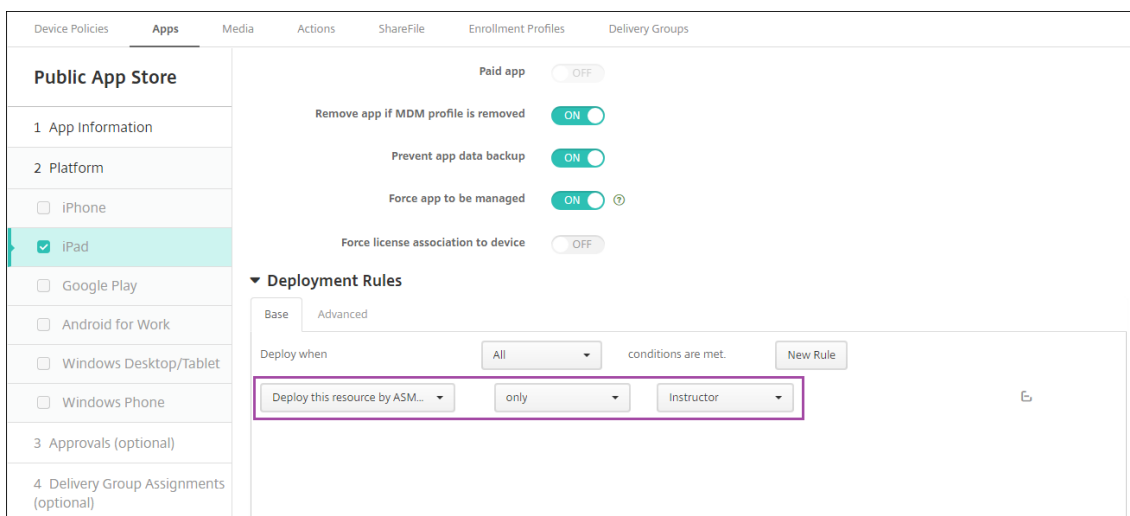
Você pode optar por atribuir aplicativos (mas não iBooks) no nível do dispositivo. Para fazer isso, mude a configuração **Forçar a associação da licença ao dispositivo** para **Ativado**. Quando você atribui aplicativos no nível de dispositivo, os usuários não recebem um convite para participar da compra por volume da Apple.



- Para implantar um aplicativo somente para instrutores, selecione um grupo de entrega que inclua apenas instrutores ou use a seguinte regra de implantação:

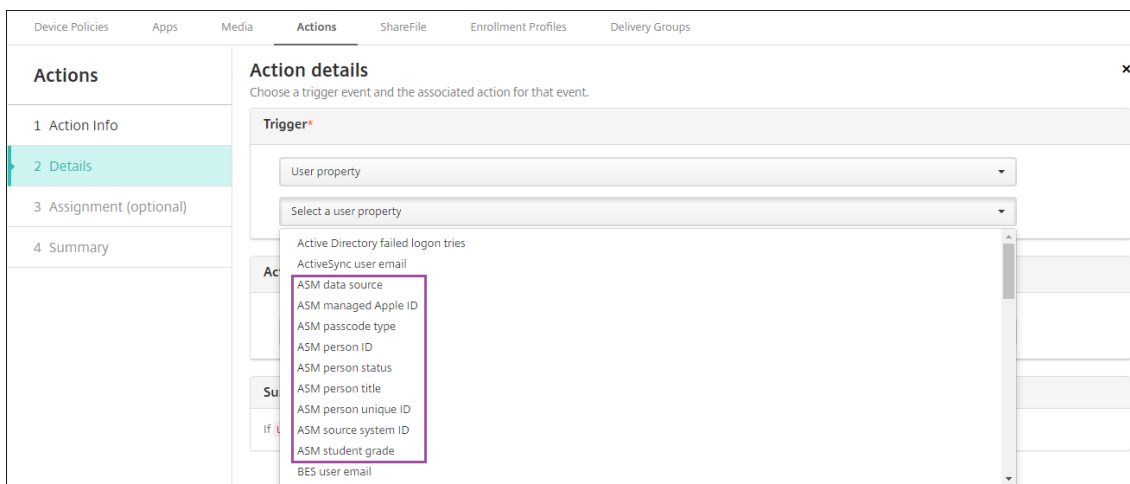
```

1 Deploy this resource by ASM device type
2 only
3 Instructor
4 <!--NeedCopy-->
    
```

- Para obter ajuda com a adição de aplicativos de compra por volume, consulte [Acrescentar um aplicativo da loja de aplicativos pública](#).

3. Opcional. Crie ações com base nas propriedades do usuário ASM. Por exemplo, você pode criar uma ação para enviar uma notificação para os dispositivos do aluno quando um novo aplicativo for instalado. Alternativamente, você pode criar uma ação que uma propriedade do usuário dispara, como mostrado no exemplo a seguir.



Para criar uma ação, vá para **Configurar > Ações**. Para obter informações sobre as ações, consulte [Ações automatizadas](#).

4. Em **Configurar > Grupos de entrega**, crie os grupos de entrega para instrutores e alunos. Escolha as classes que foram importadas do ASM. Além disso, crie uma regra de implantação para instrutores e alunos.

Por exemplo, as seguintes atribuições do usuário são para instrutores. A regra de implantação é:

1 Limit by user property

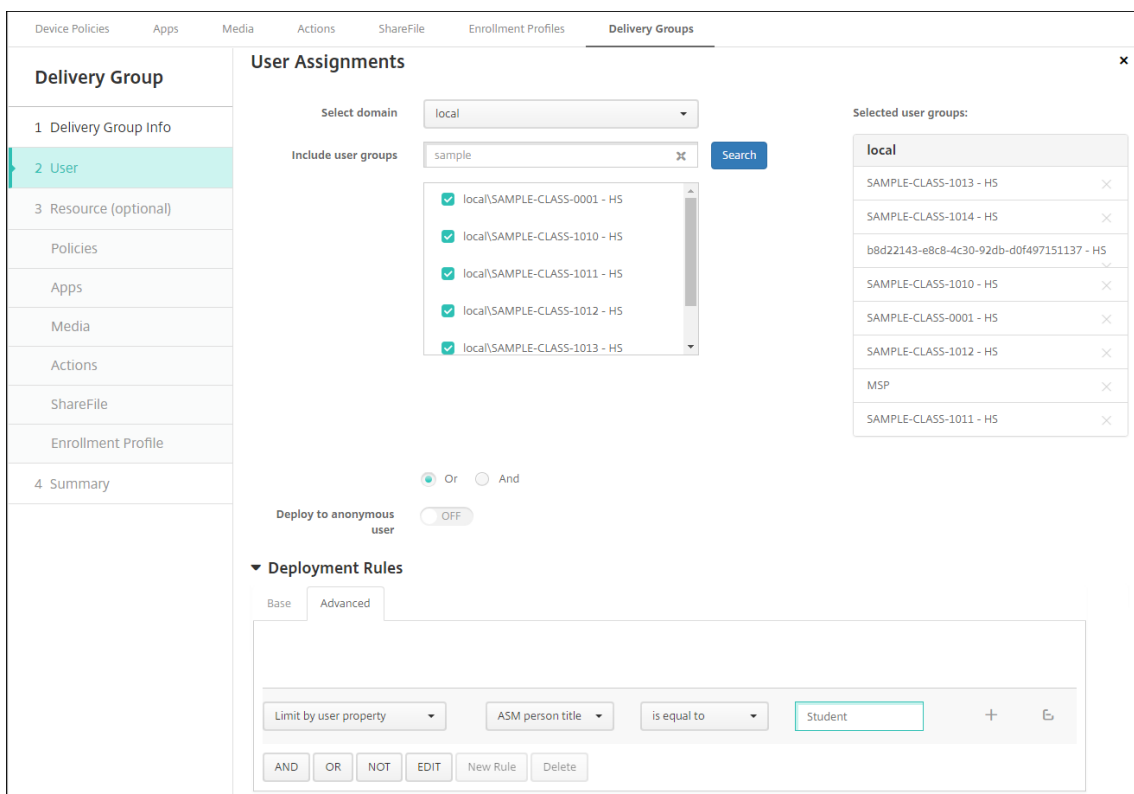
```

2  ASM person title
3  is equal to
4  Instructor
5  <!--NeedCopy-->
    
```

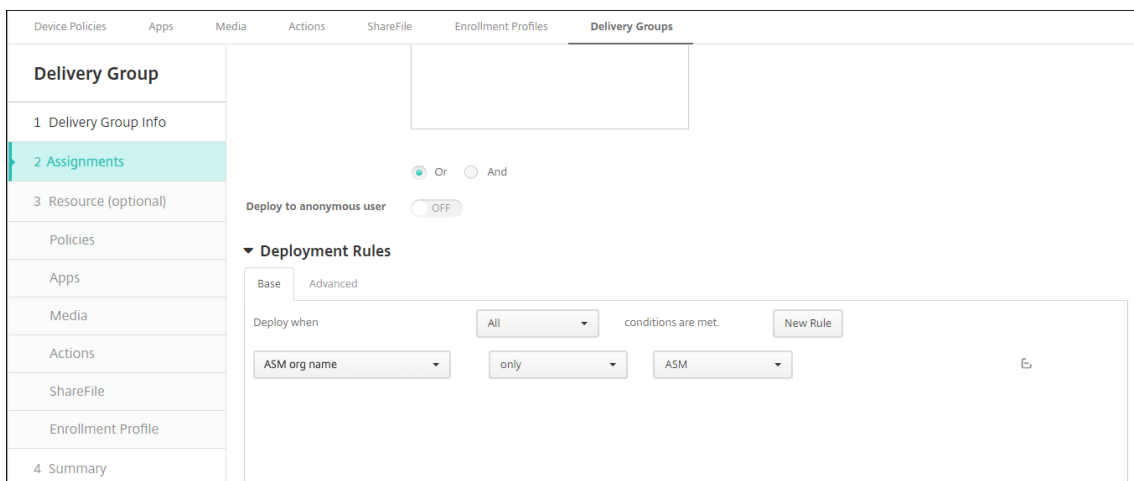
As seguintes atribuições do usuário são para alunos. A regra de implantação é:

```

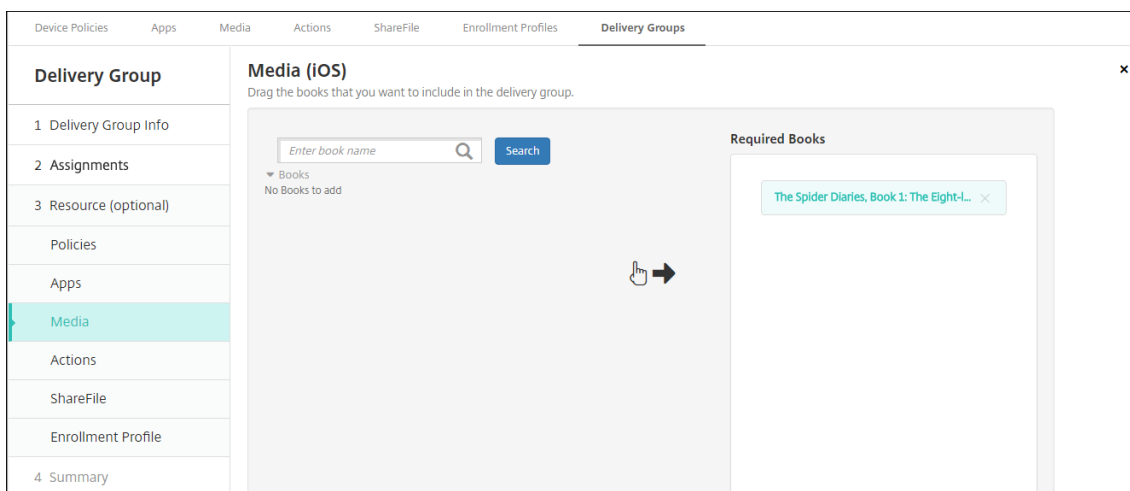
1  Limit by user property
2  ASM person title
3  is equal to
4  Student
5  <!--NeedCopy-->
    
```



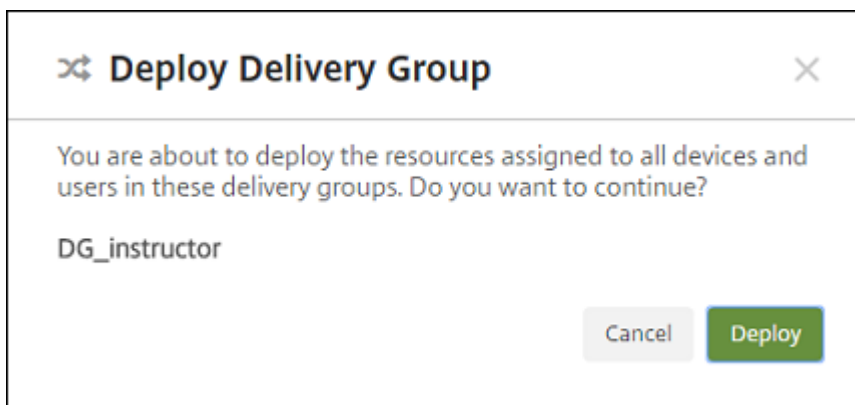
Você também pode filtrar um grupo de entrega usando uma regra de implantação baseada no nome da organização ASM.



5. Atribua os recursos a grupos de entrega. O exemplo a seguir mostra um iBook contido em um grupo de entrega.



O exemplo a seguir mostra a caixa de diálogo de confirmação que é exibida quando você seleciona um grupo de entrega e clica em **Implantar**.



Para obter mais informações, consulte “Para editar um grupo de entrega” e “Para implantar em grupos de entrega” em [Implantar recursos](#).

Etapa 8: Teste o registro do dispositivo do instrutor e aluno

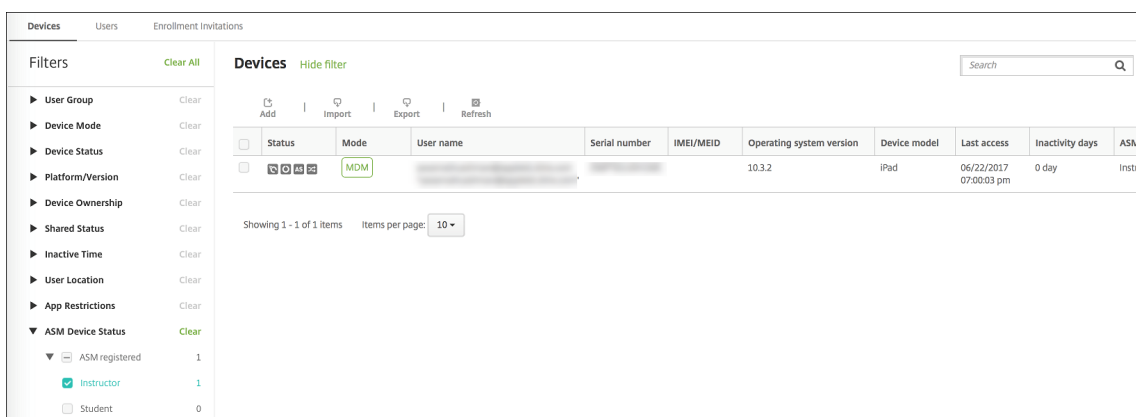
Você pode registrar dispositivos por meio de um dos seguintes métodos:

- O administrador da escola pode registrar dispositivos de instrutores e alunos usando a senha de usuário que você pode configurar no console XenMobile. Como resultado, você pode fornecer aos usuários dispositivos que já estejam configurados com aplicativos e mídia.
- Quando os usuários recebem os dispositivos, eles se registram usando a senha de usuário que você fornece a eles. Depois que o registro for concluído, o XenMobile envia as políticas de dispositivo, aplicativos e mídia para os dispositivos.

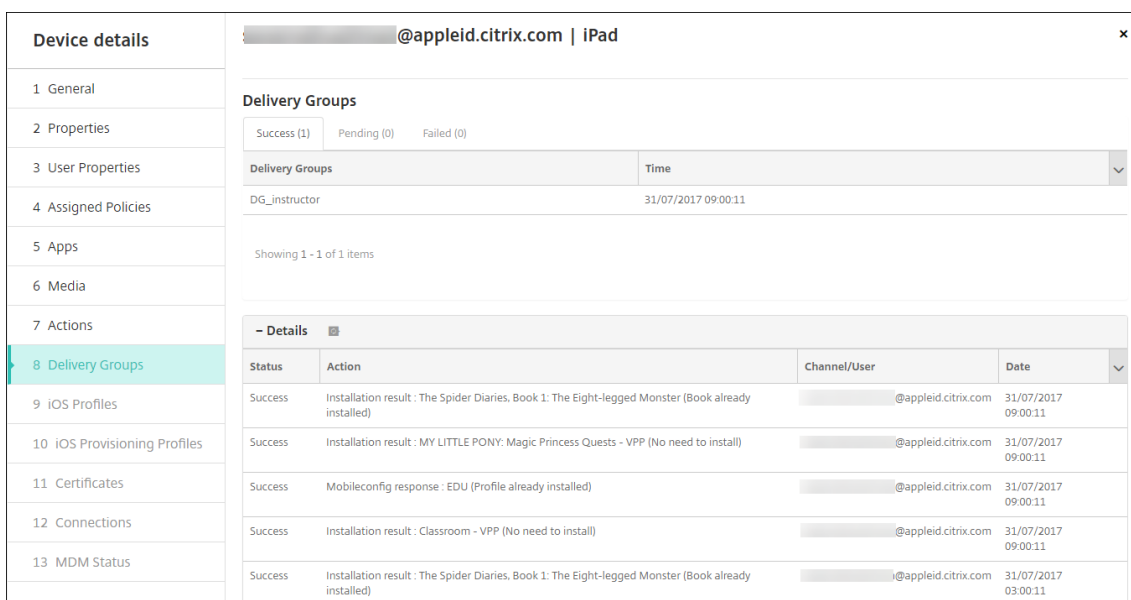
Para testar o registro, use os dispositivos do Programa de Implantação da Apple vinculados ao ASM.

1. Se os dispositivos não estiverem vinculados ao ASM, apague o conteúdo e as configurações do dispositivo executando uma reinicialização.
2. Registre um dispositivo ASM com um instrutor. Em seguida, registre um dispositivo ASM com um aluno.
3. Na página **Gerenciar > Dispositivos**, verifique se ambos os dispositivos ASM estão registrados somente no MDM.

Você pode filtrar a página **Dispositivos** pelo status do dispositivo ASM: **ASM registrado**, **ASM compartilhado**, **Instrutor** e **Estudante**.



4. Para verificar se os recursos do MDM foram implantados corretamente para cada dispositivo: selecione o dispositivo, clique em **Editar** e verifique as várias páginas.



Etapa 9: Distribua os dispositivos

A Apple recomenda que você promova um evento para que possa distribuir dispositivos para instrutores e alunos.

Se você não distribuir dispositivos pré-inscritos, forneça o seguinte a esses usuários:

- Senhas do XenMobile para registro
- Senhas temporárias do ASM para IDs Apple gerenciados.

A primeira experiência de uso do usuário é a seguinte.

1. A primeira vez que um usuário inicia o seu dispositivo após uma reinicialização, o XenMobile solicita, na tela de registro, que o usuário registre o dispositivo.
2. O usuário fornece o ID Apple gerenciado e a senha do XenMobile usados para se autenticar no XenMobile.
3. Na etapa de configuração do ID Apple, o dispositivo solicita ao usuário que forneça seu ID Apple gerenciado e a senha temporária do ASM. Esses itens autenticam o usuário nos serviços Apple.
4. O dispositivo solicita ao usuário que crie uma senha para o ID Apple gerenciado usado para proteger seus dados no iCloud.
5. No final do Assistente de Configuração, o XenMobile inicia a instalação das políticas, aplicativos e mídia no dispositivo. Para aplicativos e iBooks atribuídos no nível de usuário, o assistente solicita a instrutores e alunos o registro na compra por volume. Após aceitar o convite, os usuários recebem seus aplicativos e iBooks de compra por volume na próxima implantação (dentro seis horas).

Configurar iPads compartilhados

Vários alunos em uma sala de aula podem compartilhar um iPad para diferentes disciplinas lecionadas por um ou vários instrutores.

Você ou os instrutores registram iPads compartilhados e implantam políticas de dispositivos, aplicativos e mídias nos dispositivos. Depois, os alunos fornecem suas credenciais gerenciadas do ID Apple para se conectar a um iPad compartilhado. Se você implantou anteriormente uma política de Configuração de Educação para estudantes, eles não mais se conectam como “Outro usuário” para compartilhar dispositivos.

O XenMobile usa dois canais de comunicação para iPads compartilhados: o canal do sistema para o proprietário do dispositivo (instrutor) e o canal do usuário para o usuário residente atual (estudante). O XenMobile usa esses canais para enviar os comandos MDM apropriados para os recursos suportados pela Apple.

Os recursos implantados no canal do sistema são:

- Políticas de dispositivo, como Configuração de educação, Mensagem de bloqueio de tela, Máximo de usuários residentes e Período de tolerância de bloqueio de código secreto
- Aplicativos de compra por volume com base em dispositivo

A Apple não oferece suporte a aplicativos empresariais ou aplicativos de compra por volume com base no usuário em iPads compartilhados. Os aplicativos instalados em um iPad compartilhado são globais para o dispositivo e não por usuário.

- iBooks de compra por volume com base no usuário:

A Apple suporta a atribuição de iBooks de compra por volume com base no usuário em iPads compartilhados.

Os recursos implantados no canal do usuário são:

- Políticas do dispositivo: Notificações de aplicativos, Layout da tela inicial e Restrições

O XenMobile oferece suporte somente a essas políticas de dispositivo pelo canal do usuário.

Ao configurar políticas de dispositivo, você especifica o canal de implantação no parâmetro da política **Escopo do perfil**.

Policy Settings

Remove policy Select date
 Duration until removal (in hours)

Allow user to remove policy Always

Profile scope User

iOS 9.3+

Para remover as políticas de dispositivo implantadas pelo canal do usuário, escolha um **Alcance de implantação** de **Usuário** para a política de Remoção de perfil.

Fluxo de trabalho geral

Normalmente, você fornece iPads compartilhados pré-configurados e supervisionados a instrutores. Em seguida, os instrutores distribuem os dispositivos para os alunos. Se você não distribuir iPads compartilhados pré-registrados para instrutores: certifique-se de fornecer aos instrutores as senhas do XenMobile Server para que possam registrar seus dispositivos.

O fluxo de trabalho geral para configurar e registrar iPads compartilhados é o seguinte.

1. Use o console do servidor XenMobile para adicionar contas ASM (**Configurações > Programa de implantação da Apple**) com o **Modo compartilhado** ativado. Para obter mais informações, consulte “Gerenciar contas ASM para iPads compartilhados” a seguir.

2. Conforme descrito nesta seção, adicione as políticas de dispositivo, aplicativos e mídias necessárias ao XenMobile. Atribua esses recursos a grupos de entrega.
3. Peça aos instrutores que executem uma redefinição com os padrões de fábrica nos iPads compartilhados. A tela Gerenciamento Remoto é exibida para o registro.
4. Os instrutores registram os iPads compartilhados.

O XenMobile implanta recursos configurados em cada iPad compartilhado registrado. Após o reinício automático, os instrutores podem compartilhar os dispositivos com os alunos. Uma página de login é exibida no iPad.
5. O aluno escolhe a classe e, em seguida, insere o ID Apple gerenciado e a senha temporária do ASM.

O iPad compartilhado autentica no ASM e solicita ao aluno que crie uma senha ASM. No próximo login no iPad compartilhado, o aluno fornece a nova senha ASM.
6. Outro aluno que esteja compartilhando o iPad pode se conectar repetindo a etapa anterior.

Gerenciar contas ASM para iPads compartilhados

Se você já usa o XenMobile com o Apple Educação: você tem uma conta ASM configurada no XenMobile para dispositivos que não são compartilhados, como os dispositivos usados pelos instrutores. Você pode usar o mesmo ASM e o mesmo servidor XenMobile para os dispositivos compartilhados e não compartilhados.

O XenMobile oferece suporte a esses cenários de implantação:

- Um grupo de iPads compartilhados por classe

Nesse cenário, você atribui os iPads compartilhados a uma classe de alunos. Os iPads ficam na sala de aula. Os instrutores que ensinam diferentes disciplinas nessa classe usam o mesmo grupo de iPads.

- Um grupo de iPads compartilhados por instrutor

Nesse cenário, você atribui os iPads compartilhados a um instrutor, que usa esses iPads para as várias classes que lecionam.

Organizar iPads compartilhados em grupos de dispositivos

O ASM permite organizar dispositivos em grupos criando vários servidores MDM. Ao atribuir os iPads compartilhados a um servidor MDM, crie um grupo de dispositivos para cada grupo de iPads compartilhados, por classe ou por instrutor:

- Grupo 1 de iPads compartilhados > Servidor MDM do grupo de dispositivos 1
- Grupo 2 de iPads compartilhados > Servidor MDM do grupo de dispositivos 2
- Grupo N de iPads compartilhados > Servidor MDM do grupo de dispositivos N

Adicionar contas ASM para cada grupo de dispositivos

Ao criar várias contas ASM a partir do console do servidor XenMobile, você importa automaticamente grupos de iPads compartilhados (um para cada classe ou instrutor):

- Servidor MDM do grupo de dispositivos 1 > Conta do grupo de dispositivos 1
- Servidor MDM do grupo de dispositivos 2 > Conta do grupo de dispositivos 2
- Servidor MDM do grupo de dispositivos N > Conta do grupo de dispositivos N

Os requisitos específicos para iPads compartilhados são os seguintes:

- Uma conta ASM para cada grupo de dispositivos com estas configurações ativadas:
 - **Exigir registro de dispositivo**
 - **Modo supervisionado**
 - **Modo compartilhado**
- Para uma determinada organização educacional, certifique-se de usar o mesmo **sufixo de educação** em todas as contas ASM.

Para adicionar uma conta, acesse **Configurações > Programa de implantação da Apple**.

Settings > Apple deployment program > Edit Apple deployment program Account

Apple deployment program Account

iOS Settings

Specify the settings to define the enrollment process and the mode of iOS Automatic Device Enrollment devices.

Enrollment settings

- Require device enrollment: YES
- Require credentials for device enrollment: YES (iOS 7.1+)
- Wait for configuration to complete setup: NO (iOS 9.0+)

Device settings

- Supervised mode: YES
- Shared mode: NO
- Allow enrollment profile removal: NO
- Allow device pairing: NO

Supervision Identities

+ Add

<input type="checkbox"/>	Name	Description	Valid from	Valid to
No results found.				

Back Next >

Aplicativos para iPads compartilhados

iPads compartilhados suportam a atribuição de aplicativos de compra por volume com base em dispositivo. Antes de implantar um aplicativo em um iPad compartilhado, o XenMobile envia uma solicitação ao servidor de compras por volume da Apple para atribuir licenças de compra por volume aos dispositivos. Para verificar as atribuições de compra por volume, vá para **Configurar > Aplicativos > iPad** e expanda **Compra por volume**.

Mídia para iPads compartilhados

iPads compartilhados suportam a atribuição de iBooks de compra por volume com base no usuário. Antes de implantar iBooks em um iPad compartilhado, o XenMobile envia uma solicitação ao servidor de compras por volume da Apple para atribuir licenças de compra por volume aos estudantes. Para verificar as atribuições de compra por volume, vá para **Configurar > Mídia > iPad** e expanda **Compra por volume**.

The screenshot shows the XenMobile console configuration for iBook deployment on iPads. The interface is divided into a sidebar and a main content area.

Sidebar:

- Device Policies
- Apps
- Media** (selected)
- Actions
- ShareFile
- Enrollment Profiles
- Delivery Groups

iBook Configuration:

- 1 Book Information
- 2 Platform
 - iPhone
 - iPad** (selected)
- 3 Delivery Group Assignments (optional)

Deployment Rules:

- Base: Advanced
- Deploy when: All conditions are met. (New Rule)
- Deploy this resource by device model: only iPad
- Device operating system version: is greater than or equal to 9.3
- Supervised: True
- Apple Deployment Program account name: only ASM Automated Device Enrollment

Volume Purchase:

- Volume purchase License: Use Volume purchase company token
- Volume purchase Account: test

Volume purchase ID Assignment:

License ID	Usage Status	Associated User
7545903139	Used	[Redacted]
7545903138	Used	[Redacted]

License Usage: 2 of 5

Buttons: Back, Next >

Regras de implantação para iPads compartilhados

Para implantação do iPad compartilhado, as regras no nível do grupo de entrega não se aplicam porque elas se relacionam às propriedades do usuário. Para filtrar as políticas, aplicativos e mídias para cada grupo de dispositivos: adicione uma regra de implantação para os recursos com base no nome da conta. Por exemplo:

- Para a conta do grupo de dispositivos 1, defina esta regra de implantação:

```

1 Apple Deployment Program account name
2 Only
3 Device Group 1 account
4
5 <!--NeedCopy-->
    
```

- Para a conta do grupo de dispositivos 2, defina esta regra de implantação:

```

1 Apple Deployment Program account name
2 Only
    
```

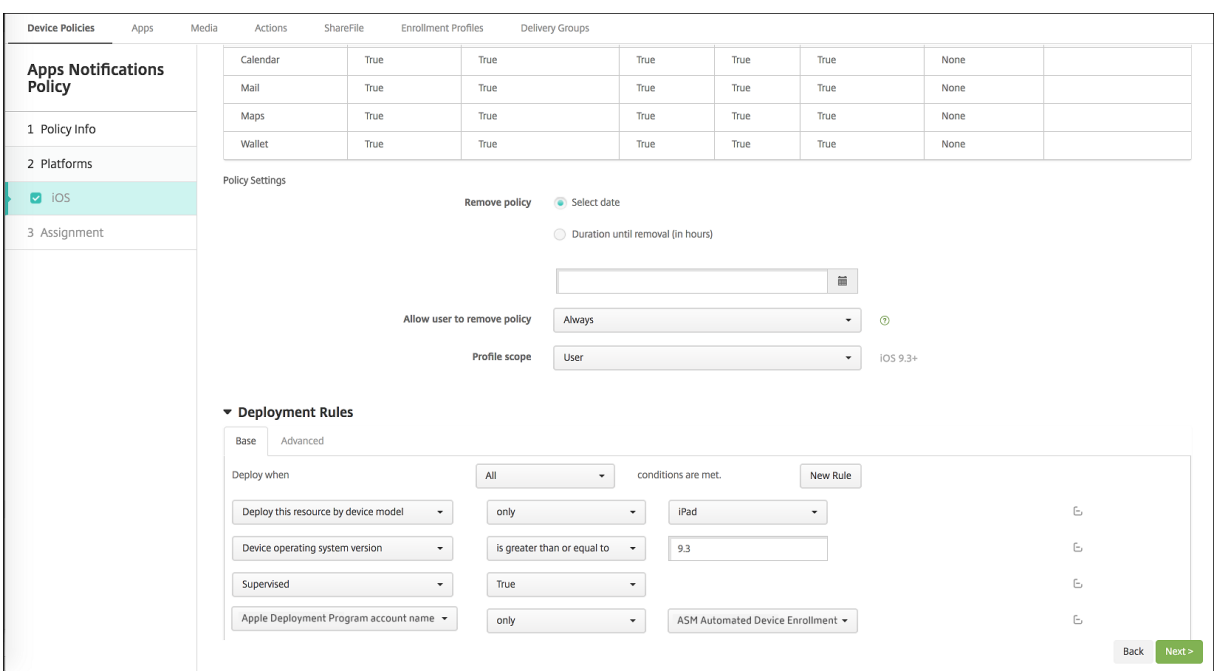
```

3 Device Group 2 account
4
5 <!--NeedCopy-->
    
```

- Para a conta do grupo de dispositivos N, defina esta regra de implantação:

```

1 Apple Deployment Program account name
2 Only
3 Device Group N account
4
5 <!--NeedCopy-->
    
```



Para implantar o aplicativo Apple Classroom somente para instrutores (usando iPads não compartilhados), filtre os recursos pelo status compartilhado ASM com estas regras de implantação:

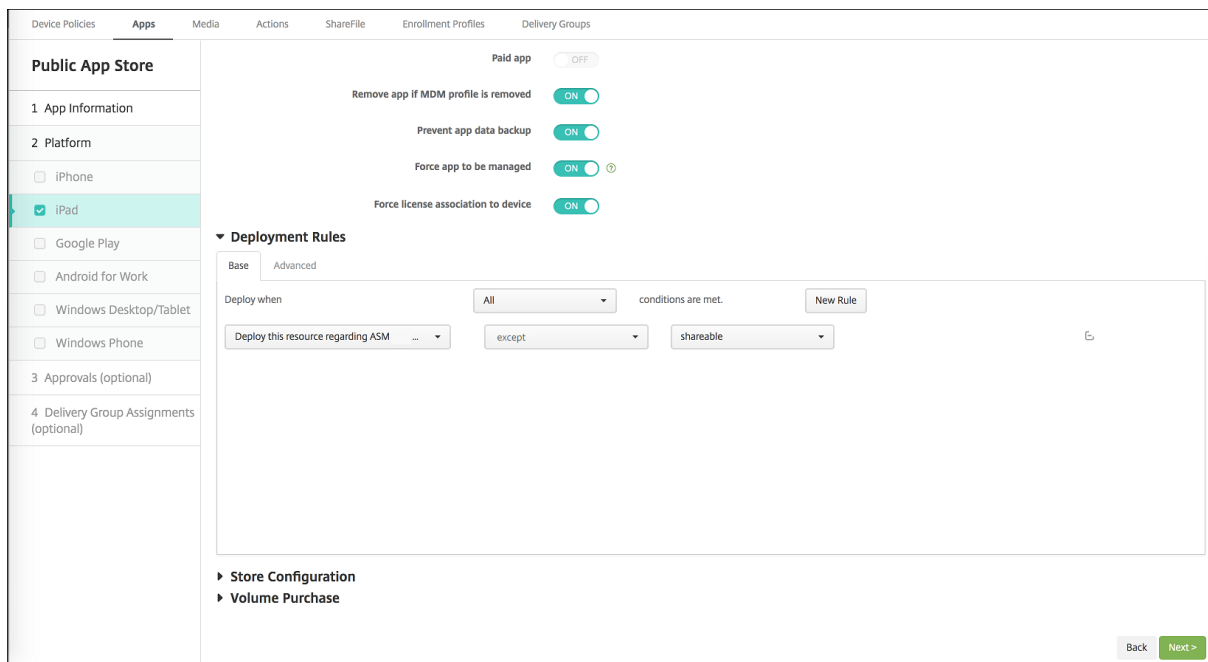
```

1 Deploy this resource regarding ASM shared mode
2 only
3 unshared
4
5 <!--NeedCopy-->
    
```

Ou:

```

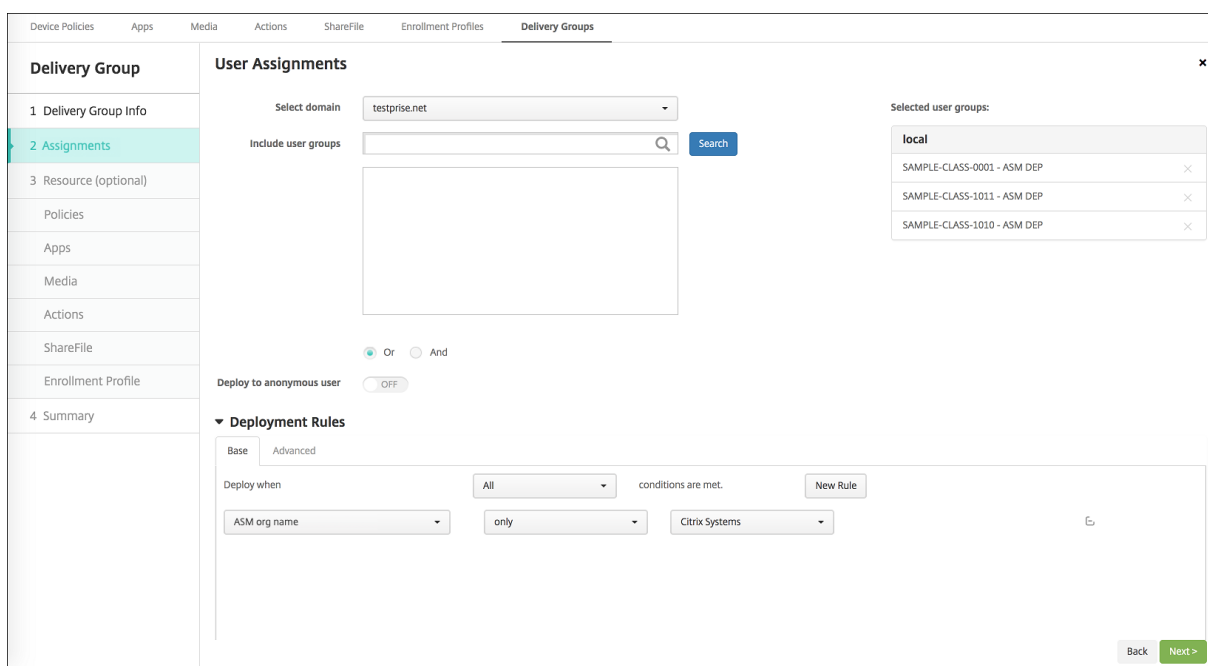
1 Deploy this resource regarding ASM shared mode
2 except
3 shareable
4
    
```



Grupos de entrega para iPads compartilhados

No grupo de dispositivos de cada instrutor:

- Configure um grupo de entrega. Para o instrutor, atribua todas as classes que a política de Configuração de Educação define.



- O grupo de entrega deve incluir estes recursos MDM:
 - Políticas de dispositivo:
 - * Configuração de educação
 - * Mensagem de bloqueio de tela
 - * Notificações de aplicativos
 - * Layout da tela inicial
 - * Restrições
 - * Máximo de usuários residentes
 - * Período de tolerância de bloqueio de código secreto
 - Aplicativos de compra por volume necessários
 - iBooks de compra por volume necessários

The screenshot displays the configuration for a Delivery Group named "iOS Education DG". The interface is divided into several sections:

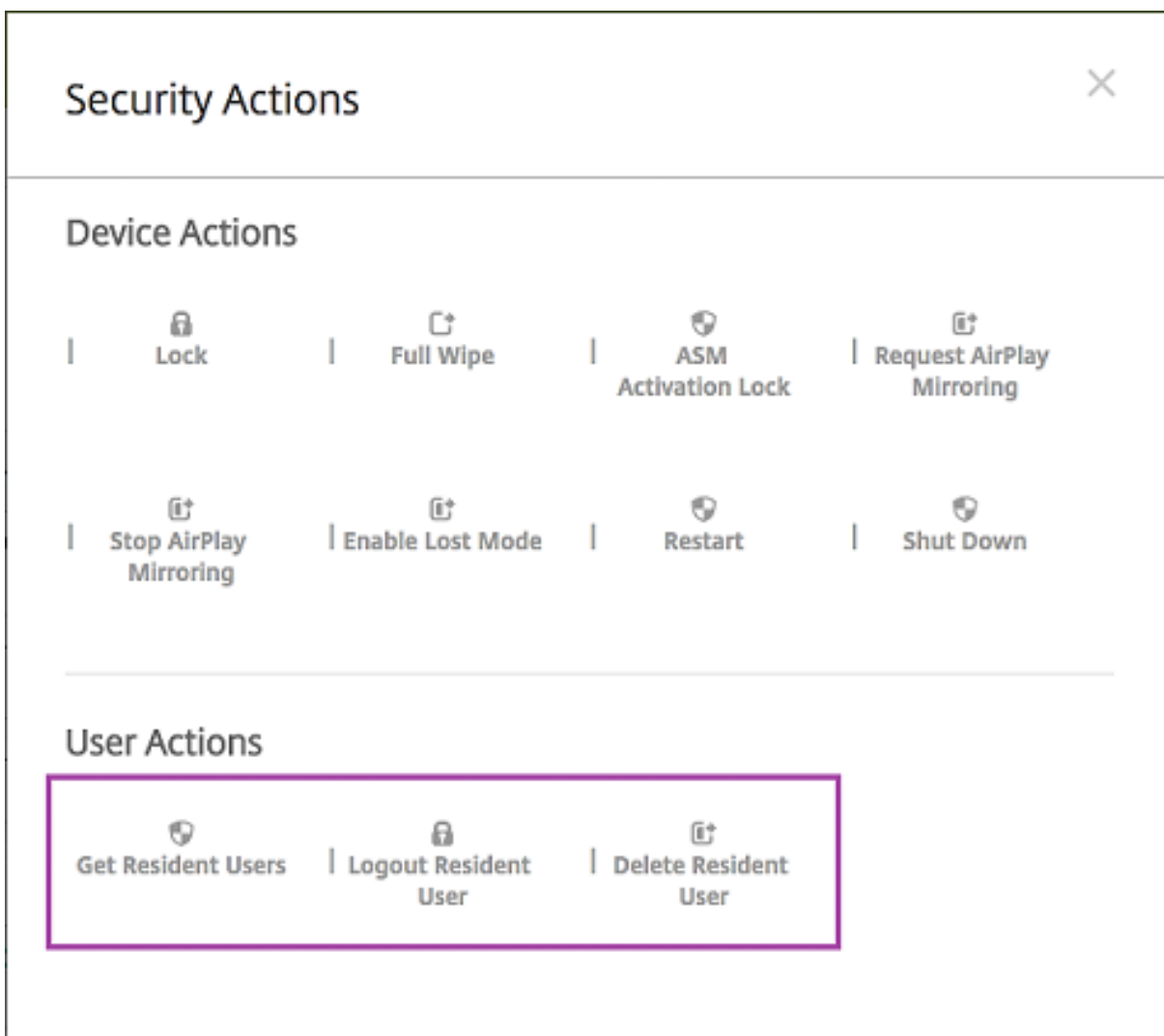
- General:** Name: iOS Education DG; Description: (empty).
- User:** Include local user groups: local\SAMPLE-CLASS-1011 - ASM, local\SAMPLE-CLASS-0001 - ASM, local\SAMPLE-CLASS-1010 - ASM.
- Resource:** Logic: OR. This section contains categorized lists of resources:
 - Policies (7):** DEP Software Inventory, Test 1 HSL, Test 1 Notifications, SAMPLE CLASS 0001 Restrictions, Test Maximum Resident Users, ASM DEP Edu Config, Test Passcode Lock Grace Period.
 - Apps (2):** MY LITTLE PONY: MAGIC PRINCESS - ASM, Classroom - ASM.
 - Media (2):** Rome - ASM, The Spider Diaries, Book 1: The Eight-leg... - ASM.
 - Actions (0):** (None listed)
 - ShareFile:** Disabled
 - Enrollment Profile:** Global

Buttons for "Back" and "Save" are located at the bottom right of the configuration area.

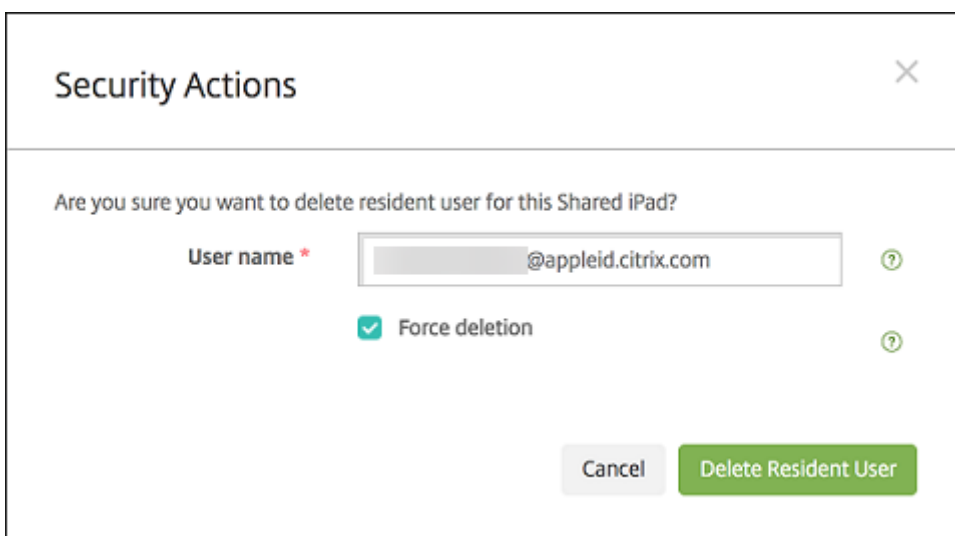
Ações de segurança para iPads compartilhados

Além das ações de segurança existentes, você pode usar estas ações de segurança para iPads compartilhados:

- **Obter usuários residentes:** lista os usuários que têm contas ativas no dispositivo atual. Essa ação força uma sincronização entre o dispositivo e o console XenMobile.
- **Fazer logout do usuário residente:** força o logout do usuário atual.
- **Excluir usuário residente:** exclui a sessão atual de um usuário específico. O usuário pode fazer logon novamente.



Depois de clicar em **Excluir usuário residente**, você pode especificar o nome de usuário.



Os resultados das ações de segurança aparecem nas páginas **Gerenciar > Dispositivos > Geral** e **Gerenciar > Dispositivos > Grupos de Entrega**.

Obter informações sobre iPads compartilhados

Encontre informações específicas sobre iPads compartilhados na página **Gerenciar > Dispositivos**:

- Veja:
 - Se o dispositivo é ou não é compartilhado (**ASM compartilhado**)
 - Quem está conectado ao dispositivo compartilhado (**Usuário de ASM conectado**)
 - Todos os usuários atribuídos ao dispositivo compartilhado (**Usuários de ASM residentes**)

Serial number	Device platform	Operating system version	Device model	ASM device type	ASM shared	ASM logged-in user	ASM resident users
feid.citrix.com feid.citrix.com*	iOS	11.2.2	iPad	Instructor	Yes		

- Filtre a lista de dispositivos pelo **Status de dispositivo ASM**:

platform	Operating system version	Device model	ASM device type	ASM shared	ASM logged-in user	ASM resident users
	11.2.2	iPad	Instructor	Yes		

- Exiba detalhes do usuário conectado a um iPad compartilhado na página **Gerenciar > Dispositivos > Propriedades do usuário conectado**.

Devices Users Enrollment Invitations

Device details | iPad

- General
- Properties
- User Properties
- Logged-in User Properties**
- Assigned Policies
- Apps
- Media
- Actions
- Delivery Groups
- iOS Profiles
- iOS Provisioning Profiles
- Certificates
- Connections
- MDM Status

User Properties

User name:

Password:

Role:

Membership:

- local\Android Default Group [Manage Groups](#)
- local\Android SD Enroller Group
- local\Android SD Group
- local\Apple Configurator Group
- local\CWC_GRP

VPP Accounts:

- ASM VPP [Retire](#)

[Back](#) [Next >](#)

Devices Users Enrollment Invitations

Device details

- General
- Properties
- User Properties
- Logged-in User Properties**
- Assigned Policies
- Apps
- Media
- Actions
- Delivery Groups
- iOS Profiles
- iOS Provisioning Profiles
- Certificates
- Connections
- MDM Status

- User Properties [Add](#)

ASM DEP org name	Citrix Systems
ASM person title	Student
ASM person unique ID	<input type="text"/>
Name	Brayden Anderson
ASM source system ID	S25-008
ASM person status	Active
First name	Brayden
ASM person ID	SAMPLE-STUDENT-0008
ASM managed Apple ID	<input type="text"/>
Surname	Anderson
ASM student grade	4
ASM passcode type	four
ASM data source	SFTP

[Back](#) [Next >](#)

- Consulte o canal usado para implantar recursos para instrutores e usuários em um grupo de entrega na página **Gerenciar > Dispositivos > Grupos de Entrega**. A coluna **Canal/Usuário** mostra o tipo (**Sistema** ou **Usuário**) e o destinatário (instrutor ou estudante).

The screenshot displays the 'Device details' page for an iPad. The left sidebar contains a navigation menu with 14 items, where '9 Delivery Groups' is selected. The main content area shows the 'Delivery Groups' section with a summary of 1 success, 0 pending, and 0 failed items. Below this, a table lists the details of the delivery group actions.

Status	Action	Channel/User	Date
Failure	NotNow response : SecurityInfo MDM command (PARK)		11/30/17 5:48:04 pm
Success	Mobileconfig response : Test 1 Notifications (Profile already installed)		11/30/17 5:48:04 pm
Success	Package deploy end : SAMPLE CLASS 0001 DG		11/30/17 5:48:04 pm
Success	Mobileconfig response : Test 1 HSL (Profile already installed)		11/30/17 5:48:04 pm
Success	Mobileconfig response : SAMPLE CLASS 0001 Restrictions (Profile already installed)		11/30/17 5:48:03 pm
Success	Installation result : The Spider Diaries, Book 1: The Eight-legged Monster (Installed)		11/30/17 4:51:22 pm
Success	Installation result : Rome (Installed)		11/30/17 4:51:22 pm
Done	Software inventory requested		11/30/17 4:50:49 pm
Success	Software inventory response		11/30/17 4:50:49 pm
Done	Installation result : The Spider Diaries, Book 1: The Eight-legged Monster - ASM (Installing)		11/30/17 4:50:49 pm

- Obter informações sobre usuários residentes:
 - **Tem dados para sincronizar:** se o usuário tem dados a serem sincronizados com a nuvem.
 - **Cotas de dados:** a cota de dados definida para o usuário em bytes. Uma cota pode não aparecer se as cotas do usuário estiverem temporariamente desativadas ou se não forem impostas para o usuário.
 - **Dados usados:** a quantidade de dados usada pelo usuário em bytes. Um valor pode não aparecer se ocorrer um erro enquanto o sistema coleta as informações.
 - **Está conectado:** se o usuário está conectado ao dispositivo.

Device details | iPad

Connections

First connection: 8/30/17 12:42:38 pm
 Status: Active
 Last connection: 11/30/17 5:48:04 pm

User name	Penultimate authentication	Last authentication	Has data to sync	Data quota	Data used	Is logged-in
ios	10/12/17 10:15:34 am	10/12/17 10:19:00 am				
	11/23/17 3:45:28 pm	11/23/17 3:45:29 pm				
	11/23/17 5:48:03 pm	11/23/17 5:48:03 pm				
	11/30/17 5:48:03 pm	11/30/17 5:48:04 pm				
	11/30/17 5:48:03 pm	11/30/17 5:48:04 pm	Yes			Yes
	11/29/17 7:02:32 pm	11/29/17 7:02:32 pm	No		120.82 MB	No

Showing 1 - 6 of 6 items

Back Next >

- Veja o status de push dos dois canais.

Device details | iPad

System channel

Push status: Active
 Last push initiation: 1/24/18 1:00:03 pm
 Last notification completion: 1/24/18 1:00:03 pm
 Last reply time: 1/24/18 1:00:03 pm

User channel

Push status: Active
 Last push initiation: 1/24/18 1:00:03 pm
 Last notification completion: 1/24/18 1:00:03 pm
 Last reply time: 1/24/18 1:00:03 pm

Refresh

Back Save

Gerenciar instrutor, aluno e dados da classe

Ao gerenciar o instrutor, aluno e dados da classe, observe o seguinte:

- Não altere IDs Apple gerenciados depois de importar as informações do ASM para o XenMobile. O XenMobile também usa identificadores de usuários ASM para identificar usuários.
- Se você adicionar ou alterar dados de classe no ASM depois de criar uma ou mais políticas de

dispositivo de Configuração de Educação: edite as políticas e, em seguida, reimplante-as.

- Se o instrutor de uma classe mudar depois de você implantar a política do dispositivo de Configuração de Educação: revise a política para garantir que ela seja atualizada no console XenMobile e depois reimplante a política.
- Se você atualizar as propriedades do usuário no portal ASM, o XenMobile também atualizará essas propriedades no console. No entanto, o XenMobile não recebe a propriedade do título da pessoa no ASM (Instrutor (Professor), Estudante ou Outros) da mesma forma que recebe outras propriedades. Assim, se você alterar o título de pessoa do ASM no ASM, conclua as seguintes etapas para refletir essa alteração no XenMobile.

Para gerenciar os dados:

1. No portal ASM, atualize a nota do aluno e limpe a nota do instrutor.
2. Se você tiver alterado uma conta de aluno para uma conta de instrutor, remova o usuário da lista de alunos na classe. Em seguida, adicione o usuário à lista de instrutores na mesma ou em outra classe.

Se você tiver alterado uma conta de instrutor para uma conta de aluno, remova o usuário da classe. Em seguida, adicione o usuário à lista de alunos na mesma ou em outra classe. Suas atualizações aparecem no console XenMobile durante a próxima sincronização (a cada cinco minutos por padrão) ou obtenção/busca (a cada 24 horas, por padrão).

3. Edite a política do dispositivo Configuração de Educação para aplicar a alteração e reimplante-a.
 - Se você excluir um usuário do portal ASM, o XenMobile também exclui esse usuário do console XenMobile após uma busca.

Você pode reduzir o intervalo entre duas linhas de base alterando este valor da propriedade de servidor: **bulk.enrollment.fetchRosterInfoDelay** (o padrão é **1440** minutos).
 - Depois de implantar recursos: se um aluno ingressar em uma classe, crie um grupo de entrega com apenas esse aluno e implemente os recursos para o aluno.
 - Se um aluno ou instrutor perder sua senha temporária, entre em contato com o administrador do ASM. O administrador pode fornecer a senha temporária ou gerar uma nova.

Gerenciar um dispositivo perdido ou roubado que esteja registrado no Programa de implantação da Apple do Apple School Manager

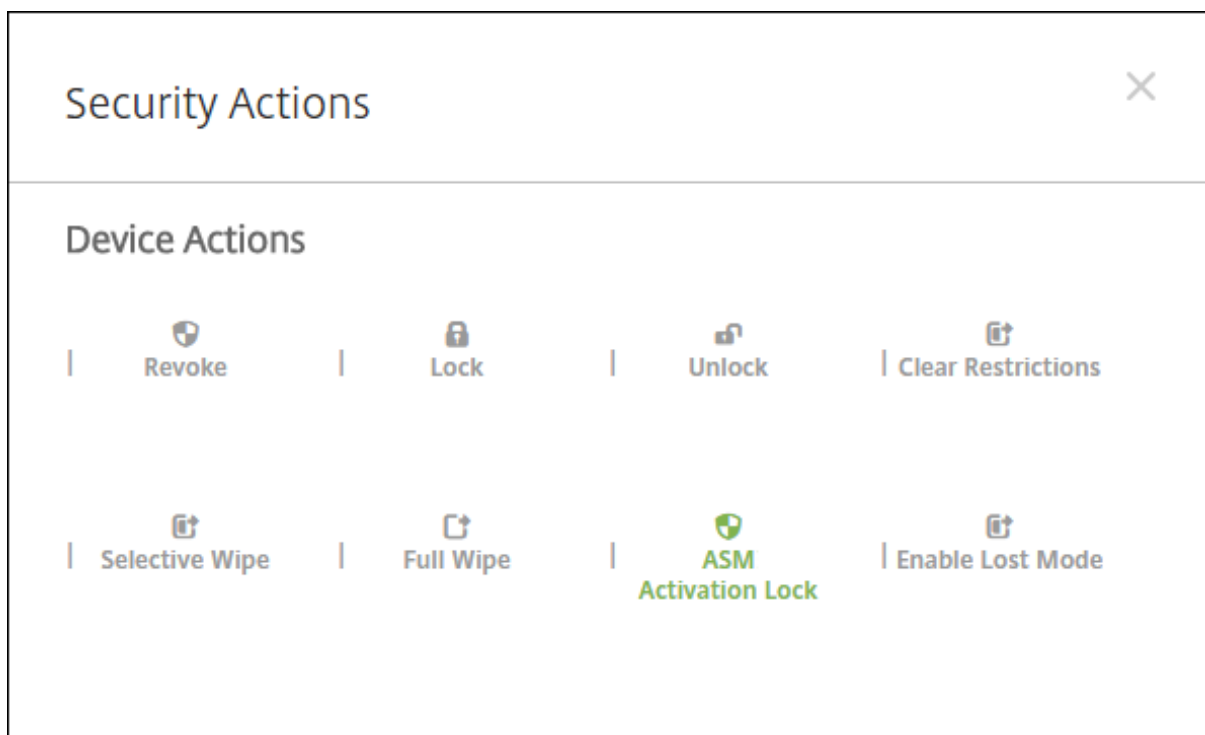
O serviço Apple Buscar do iPhone/iPad inclui um recurso de bloqueio de ativação. O Bloqueio de Ativação impede usuários não autorizados de usar ou revender um dispositivo perdido ou roubado que esteja registrado no Programa de implantação da Apple.

O XenMobile inclui uma ação de segurança **Bloqueio de Ativação do ASM** que permite enviar um código de bloqueio para um dispositivo registrado no Programa de Implantação da Apple do ASM.

Quando você usa a ação de segurança de **Bloqueio de ativação do ASM**, o XenMobile pode localizar dispositivos sem a necessidade de os usuários ativarem o serviço Buscar do iPhone/iPad. Quando um dispositivo ASM é reconfigurado ou totalmente apagado, o usuário fornece o ID Apple gerenciado e a senha para desbloquear o dispositivo.

Para liberar o bloqueio a partir do console, clique na ação de segurança **Ignorar bloqueio de ativação**. Para obter informações sobre como ignorar um bloqueio de ativação, consulte [Ignorar bloqueio de ativação do iOS](#). O usuário também pode deixar o logon em branco e digitar o **código de desvio do bloqueio de ativação do ASM** como a senha. Essa informação está disponível em **Detalhes do dispositivo**, na guia **Propriedades**.

Para configurar o bloqueio de ativação, vá para **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Segurança** e, em seguida, clique em **Bloqueio de ativação do ASM**.



As propriedades **Chave de caução ASM** e **código de desvio do bloqueio de ativação ASM** aparecem nos **Detalhes do dispositivo**.

Devices		Users	Enrollment Invitations
Device details			
- Security information Add			
1 General		ASM Automated Device Enrollment escrow key	
2 Properties		ASM Automated Device Enrollment activation lock bypass code	
3 User Properties		Activation lock bypass code	
4 Assigned Policies		Activation lock enabled No	
5 Apps		Hardware encryption capabilities Block and file levels encryption	
6 Media		Internal storage encrypted No	
7 Actions		jailbroken/Rooted No	
8 Delivery Groups		MDM lost mode enabled No	
9 iOS Profiles		Passcode compliant Yes	
10 iOS Provisioning Profiles		Passcode compliant with configuration Yes	
11 Certificates		Passcode present No	
12 Connections		Supervised Yes	
13 MDM Status		- Storage space Add	
		Available storage space 25.58 GB	
		Total storage space 27.05 GB	

A permissão RBAC para um bloqueio de ativação ASM é **Dispositivos > Ativar desvio do bloqueio de ativação ASM**.

Settings > Role-Based Access Control		
Role-Based Access Control		
Add		
+ ADMIN ✎		
+ DEVICE_PROVISIONING ✎		
+ SHARED_DEVICES_ENROLLER ✎ 🗑		
+ SUPPORT ✎		
- USER ✎		
Authorized access	Console features	Restrict group access
Self Help Portal access	<ul style="list-style-type: none"> Devices Full Wipe device Selective Wipe device View locations <ul style="list-style-type: none"> Locate device Track device Lock device Unlock device Lock container Unlock container Reset container password Enable ASM /Bypass activation lock Rings the device Reboot the device View software inventory Enable lost mode Disable lost mode Enrollment <ul style="list-style-type: none"> Add/Delete enrollment Notify user 	

Distribuir aplicativos da Apple

December 10, 2020

O XenMobile gerencia aplicativos implantados em dispositivos. Você pode organizar e implantar os

seguintes tipos de aplicativos iOS/iPadOS e macOS.

- **Loja de aplicativos pública (somente iOS/iPadOS):** estes aplicativos incluem os aplicativos gratuitos ou pagos em uma loja de aplicativos pública, como o Apple App Store ou o Google Play. Por exemplo, o GoToMeeting.
- **Enterprise (iOS/iPadOS/macOS):** aplicativos nativos que não são habilitados para MDX e não contêm as políticas associadas a aplicativos MDX.
- **MDX (somente iOS/iPadOS):** aplicativos preparados com o MAM SDK ou com o MDX Service ou MDX Toolkit. Esses aplicativos incluem políticas MDX. Você obtém aplicativos MDX de fontes internas e lojas públicas.
- **Compra por volume (iOS/iPadOS/macOS):** aplicativos com licenças gerenciadas por meio do programa de compra por volume da Apple.
- **Aplicativos personalizados para iOS (somente iOS/iPadOS):** aplicativos empresariais proprietários desenvolvidos internamente ou por terceiros.

Para obter mais informações sobre diferentes tipos de aplicativos, consulte [Adicionar aplicativos](#).

Algumas implantações exigem uma conta Apple Business Management (ABM) ou Apple School Management (ASM). Consulte as seções a seguir para obter mais informações.

Para cada tipo de aplicativo e método de distribuição, a Citrix recomenda um conjunto de práticas de configuração. Para obter informações sobre como distribuir aplicativos para outras plataformas, consulte [Adicionar aplicativos](#). As seções a seguir fornecem informações mais detalhadas sobre a configuração do aplicativo iOS.

Etapas gerais para distribuição de aplicativos

Cenário	Etapa 1: vincular contas	Etapa 2: adicionar e configurar aplicativos	Etapa 3: configurar grupos de entrega e implantar aplicativos
Aplicativos da loja de aplicativos pública, incluindo aplicativos de mobilidade Citrix	Não aplicável	No XenMobile: Configurar > Aplicativos , adicione aplicativos da Loja de aplicativos pública para iPhone ou iPad. Configure os aplicativos e atribua-os a grupos de entrega.	No XenMobile: configure e implante aplicativos usando grupos de entrega.

Cenário	Etapa 1: vincular contas	Etapa 2: adicionar e configurar aplicativos	Etapa 3: configurar grupos de entrega e implantar aplicativos
Aplicativos da loja de aplicativos pública entregues com a compra por volume da Apple, incluindo aplicativos de mobilidade Citrix	Cadastre-se em um programa de implantação da Apple. No XenMobile: acesse Configurações > Compra por volume para adicionar sua conta de compra por volume.	No ABM ou ASM: compre e adicione aplicativos de Apps e Livros. No XenMobile: vá para Configurar > Aplicativos , configure os aplicativos e atribua-os a grupos de entrega.	No XenMobile: configure e implante aplicativos usando grupos de entrega.
Aplicativos empresariais	Não aplicável	No XenMobile: vá para Configurar > Aplicativos . Clique em Adicionar e clique em Empresarial . Carregue o arquivo IPA. Configure os aplicativos e atribua-os a grupos de entrega.	No XenMobile: configure e implante aplicativos usando grupos de entrega.

Cenário	Etapa 1: vincular contas	Etapa 2: adicionar e configurar aplicativos	Etapa 3: configurar grupos de entrega e implantar aplicativos
Aplicativos MDX	Não aplicável	<p>No XenMobile: vá para Configurar > Aplicativos. Clique em Adicionar e clique em MDX. Certifique-se de selecionar iPad/iPhone para a plataforma. Carregue o arquivo MDX. Configure os aplicativos e atribua-os a grupos de entrega.</p>	<p>No XenMobile: configure e implante aplicativos usando grupos de entrega.</p>
Aplicativos MDX distribuídos através da compra por volume da Apple	<p>Cadastre-se em um programa de implantação da Apple. No XenMobile: acesse Configurações > Compra por volume para adicionar sua conta de compra por volume.</p>	<p>No ABM: compre e adicione aplicativos de Apps e Livros. Vincule o aplicativo à sua conta ABM. No XenMobile: vá para Configurar > Aplicativos, configure os aplicativos e atribua-os a grupos de entrega.</p>	<p>No XenMobile: configure e implante aplicativos usando grupos de entrega.</p>

Cenário	Etapa 1: vincular contas	Etapa 2: adicionar e configurar aplicativos	Etapa 3: configurar grupos de entrega e implantar aplicativos
Aplicativos personalizados	Cadastre-se em um programa de implantação da Apple. No XenMobile: acesse Configurações > Compra por volume para adicionar sua conta de compra por volume.	No ABM: adicione seu aplicativo à App Store como um aplicativo privado. Vincule o aplicativo à sua conta ABM. No XenMobile: vá para Configurar > Aplicativos , configure os aplicativos e atribua-os a grupos de entrega.	No XenMobile: configure e implante aplicativos usando grupos de entrega.
Aplicativos personalizados habilitados com MDX	Cadastre-se em um programa de implantação da Apple. No XenMobile: acesse Configurações > Compra por volume para adicionar sua conta de compra por volume.	No ABM: adicione seu aplicativo à loja como um aplicativo privado. Vincule o aplicativo à sua conta ABM. No XenMobile: vá para Configurar > Aplicativos e carregue o arquivo MDX. Configure os aplicativos e atribua-os a grupos de entrega.	No XenMobile: configure e implante aplicativos usando grupos de entrega.

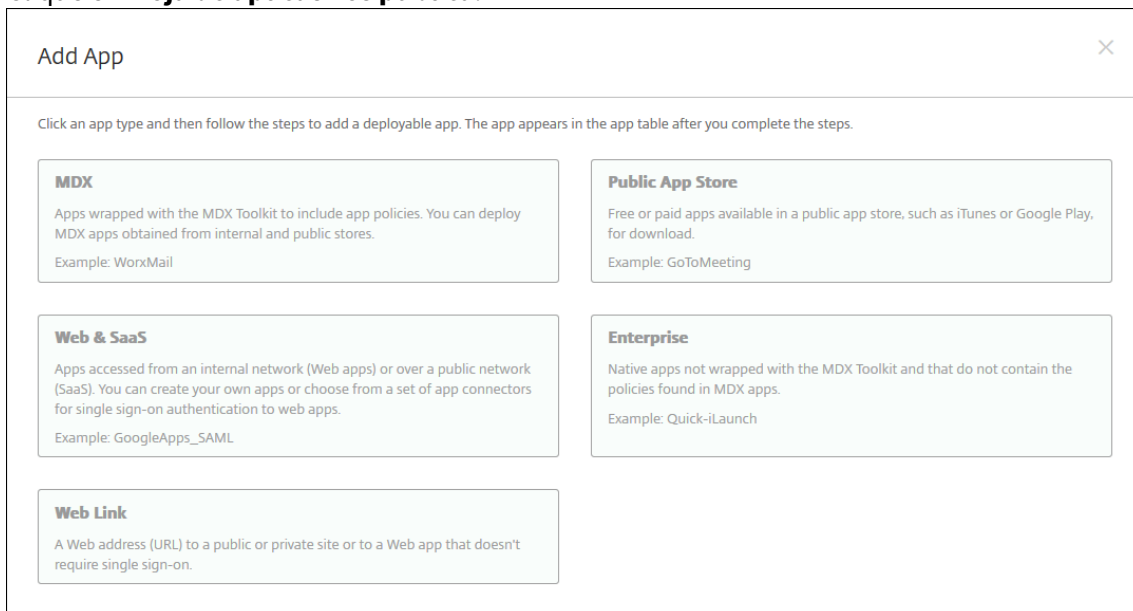
Aplicativos da loja de aplicativos pública

Você pode adicionar aplicativos gratuitos e pagos disponíveis na App Store ao XenMobile.

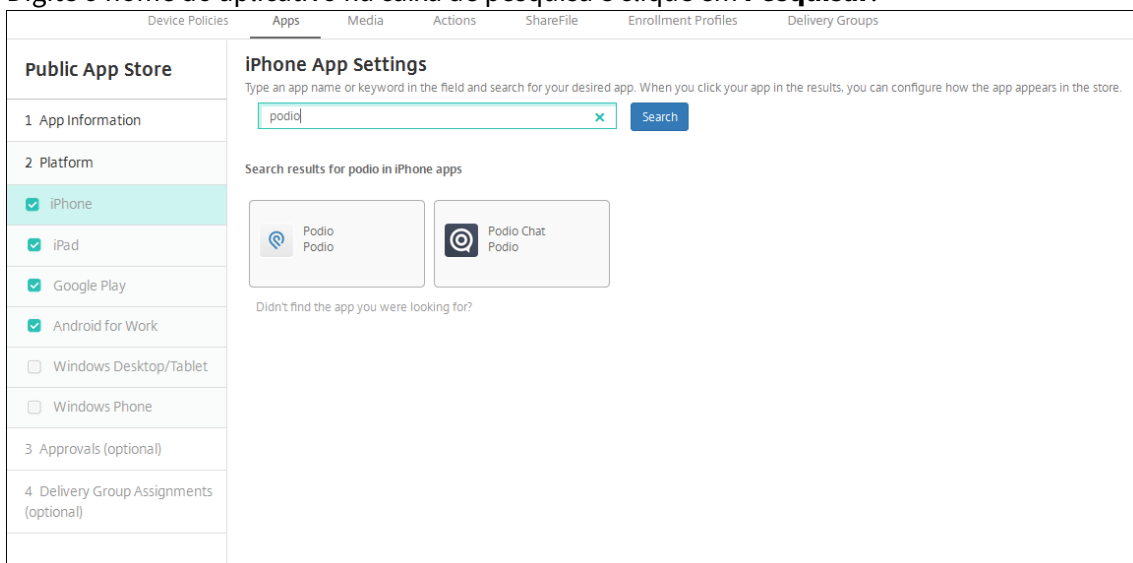
Disponibilidade de recursos	
Requer supervisão do dispositivo	Não
Disponível para o modo de registro do usuário	Não
Disponível em	iOS/iPadOS

Etapa 1: adicionar e configurar aplicativos

1. No console XenMobile, navegue até **Configurar > Aplicativos**. Clique em **Adicionar**.
2. Clique em **Loja de aplicativos pública**.



3. Selecione **iPhone** ou **iPad** para plataformas
4. Digite o nome do aplicativo na caixa de pesquisa e clique em **Pesquisar**.

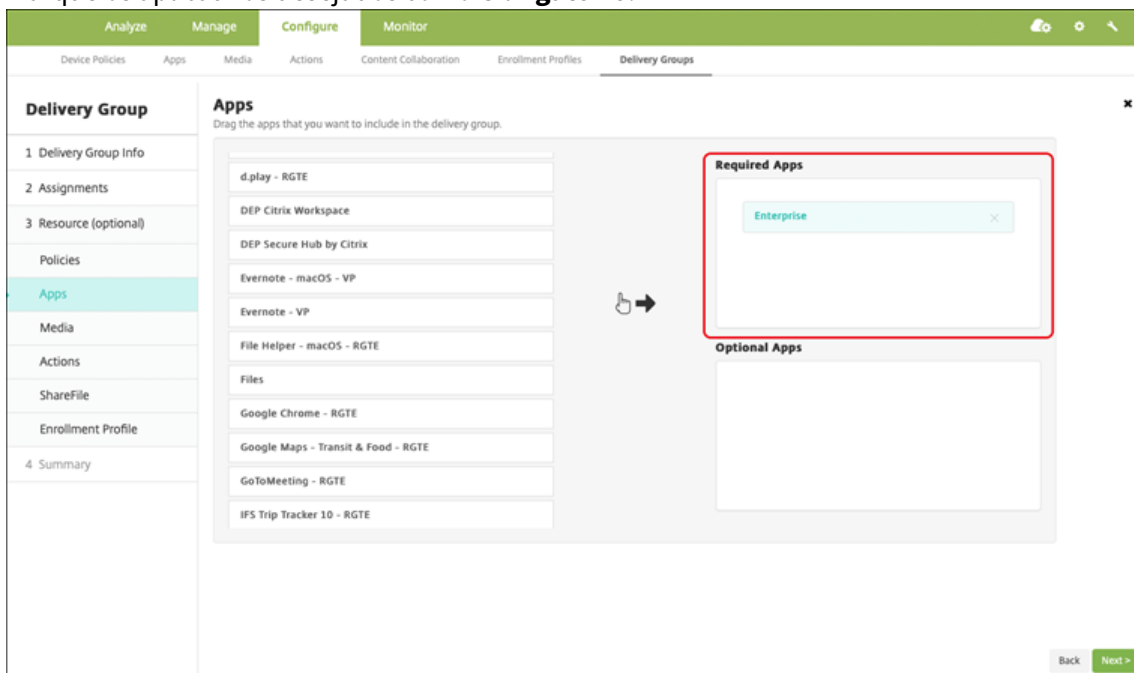


5. Os aplicativos que correspondem aos critérios de pesquisa são exibidos. Clique no aplicativo desejado.
6. Atribua um grupo de entrega ao aplicativo e clique em **Salvar**.

Etapa 2: configurar implantação do aplicativo

1. No console XenMobile, navegue até **Configurar > Aplicativos**.

2. Selecione o aplicativo que deseja configurar e clique em **Editar**.
3. A Citrix recomenda ativar o recurso **Forçar aplicativo a ser gerenciado**.
4. Atribua grupos de entrega e clique em **Salvar**.
5. Navegue até **Configurar > Grupos de entrega > Aplicativos**.
6. Marque os aplicativos desejados como **Obrigatório**.



7. Navegue até **Configurar > Grupos de entrega**.
8. Selecione o grupo de entrega e clique em **Implantar**.
9. Os usuários recebem uma solicitação para instalar o aplicativo e o aplicativo é instalado em segundo plano depois de aceitarem.



Aplicativos da loja de aplicativos pública entregues com a compra por volume da Apple

Você pode gerenciar licenças de aplicativos iOS/iPadOS por meio do programa de compra por volume da Apple. Siga estas etapas para adicionar aplicativos de compra por volume ao XenMobile.

Disponibilidade de recursos

Requer supervisão do dispositivo	Não
Disponível para o modo de registro do usuário	Sim
Disponível em	iOS/iPadOS/macOS

Etapa 1: vincular contas

1. Configure e cadastre-se no Apple Business Manager (ABM) ou no Apple School Manager (ASM). Para obter mais informações sobre esses programas, consulte a [Documentação da Apple](#).
2. Vincule sua conta ABM/ASM ao XenMobile. Para obter mais informações sobre como vincular contas de compra em volume, consulte [Compra por volume da Apple](#).
3. Ao adicionar sua conta de compra por volume, ative a **Atualização automática do aplicativo**. Essa configuração garante que os aplicativos nos dispositivos do usuário sejam atualizados au-

automaticamente quando uma atualização aparece na Apple Store.

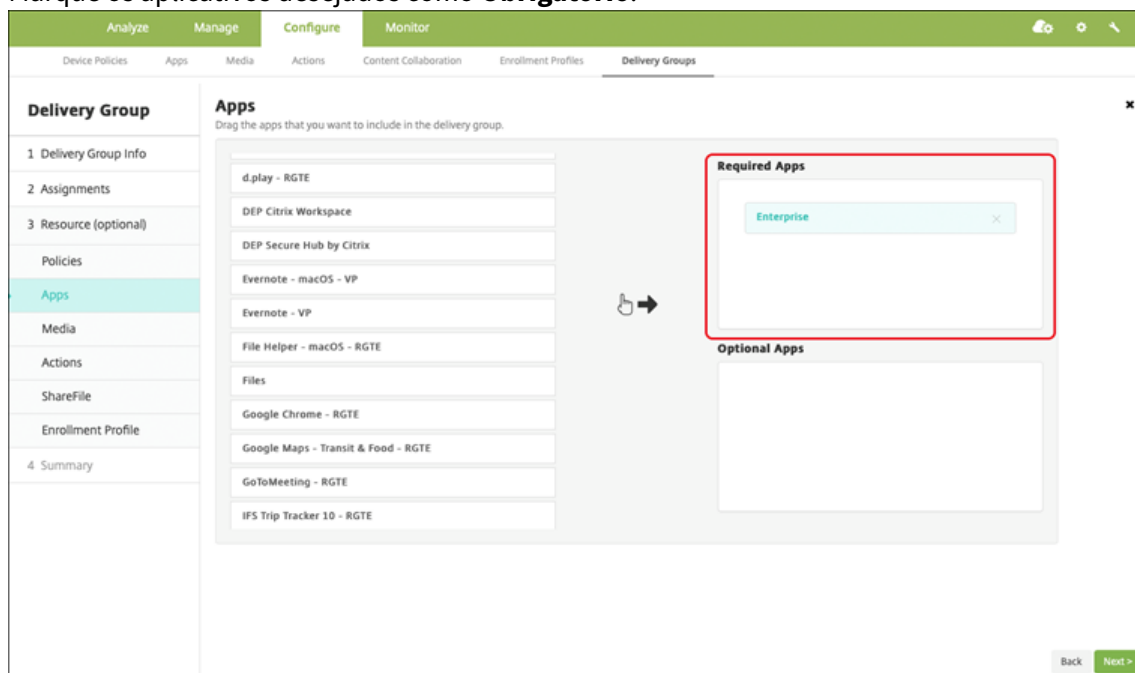
Etapa 2: obter aplicativos e licenças da Apple

Adicione aplicativos à sua conta ABM/ASM. Você pode adicionar compras da Apple App Store ou Apple Books (somente para iOS/iPadOS). Tenha em mente que você deve comprar todos os aplicativos, mesmo que eles sejam gratuitos.

Para obter informações sobre como disponibilizar aplicativos para sua empresa, consulte a [Documentação da Apple](#).

Etapa 3: configurar implantação do aplicativo

1. No console XenMobile, navegue até **Configurar > Aplicativos**.
2. Selecione o aplicativo de compra por volume que deseja configurar e clique em **Editar**.
3. Selecione as plataformas: **iPhone, iPad** ou **macOS**.
4. A Citrix recomenda ativar o recurso **Forçar aplicativo a ser gerenciado** (somente iOS/iPadOS).
5. Atribua grupos de entrega e clique em **Salvar**.
6. Navegue até **Configurar > Grupos de entrega > Aplicativos**.
7. Marque os aplicativos desejados como **Obrigatório**.



8. Navegue de volta para **Configurar > Grupos de entrega**.
9. Selecione o grupo de entrega e clique em **Implantar**.
10. Os usuários recebem uma solicitação para instalar o aplicativo e o aplicativo é instalado em segundo plano depois de aceitarem.



Aplicativos empresariais

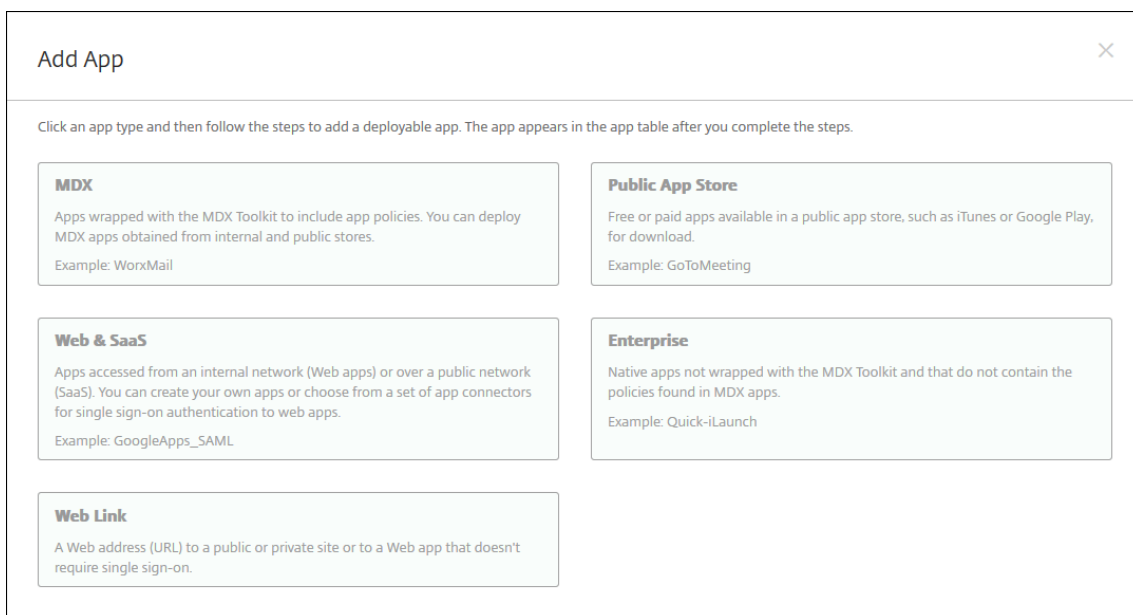
Você também pode adicionar aplicativos nativos que não têm políticas MDX associadas a eles. Siga estas etapas para adicionar aplicativos que não existem na App Store.

Disponibilidade de recursos

Requer supervisão do dispositivo	Não
Disponível para o modo de registro do usuário	Sim
SO	iOS/iPadOS/macOS

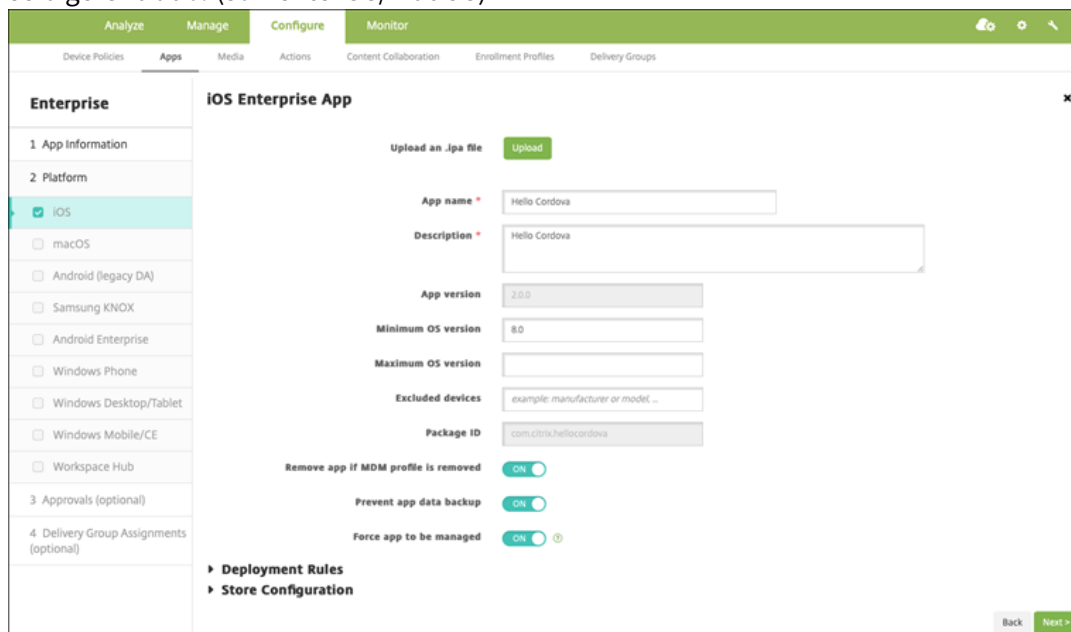
Etapa 1: adicionar e configurar aplicativos

1. No console XenMobile, navegue até **Configurar > Aplicativos**. Clique em **Adicionar**.
2. Clique em **Empresarial**.



3. Na página **Informações do aplicativo**, configure o seguinte:
 - **Nome:** digite um nome descritivo para o aplicativo. O nome aparecerá em Nome do aplicativo na tabela Aplicativos.
 - **Descrição:** digite uma descrição opcional para o aplicativo.
 - **Categoria do aplicativo:** opcionalmente, na lista, clique na categoria à qual deseja adicionar o aplicativo.
4. Clique em **Avançar**. A página **Plataformas do aplicativo** é exibida.
5. Selecione as plataformas: **iPhone**, **iPad** ou **macOS**.
6. Carregue o arquivo IPA (iOS/iPadOS) ou carregue o arquivo PKG (macOS)
7. Clique em **Avançar**. A página **Detalhes do Aplicativo** é exibida.
8. Defina estas configurações:
 - **Nome do arquivo:** opcionalmente, digite um novo nome para o aplicativo.
 - **Descrição do aplicativo:** opcionalmente, digite uma nova descrição para o aplicativo.
 - **Versão do aplicativo:** você não pode alterar esse campo.
 - **Versão do SO mínima:** opcionalmente, digite a versão mais antiga do sistema operacional que o dispositivo pode executar para usar o aplicativo.
 - **Versão do SO máxima:** opcionalmente, digite a versão mais recente do sistema operacional que o dispositivo deve executar para usar o aplicativo.
 - **Dispositivos excluídos:** opcionalmente, digite o fabricante ou os modelos de dispositivos que não podem executar o aplicativo.
 - **Remover aplicativo se o perfil MDM for removido:** selecione se o aplicativo deve ser removido de um dispositivo quando o perfil MDM é removido. O padrão é Ativado. (somente iOS/iPadOS)
 - **Evitar o backup de dados do aplicativo:** selecione se o aplicativo deve ser impedido de realizar o backup de dados. O padrão é Ativado. (somente iOS/iPadOS)

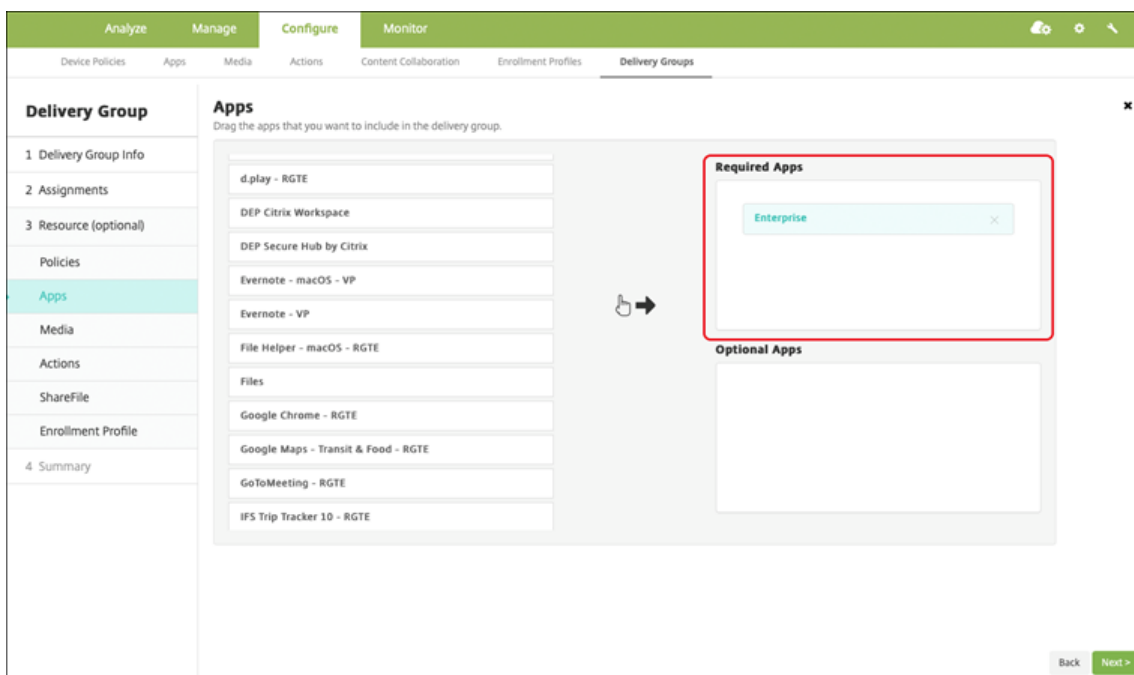
- **Forçar aplicativo a ser gerenciado:** se você instalar um aplicativo não gerenciado, selecione **I** se quiser que os usuários em dispositivos não supervisionados vejam uma solicitação para permitir o gerenciamento do aplicativo. Se aceitarem a solicitação, o aplicativo será gerenciado. (somente iOS/iPadOS)



9. Atribua um grupo de entrega ao aplicativo e clique em **Salvar**.

Etapa 2: configurar implantação do aplicativo

1. No console XenMobile, navegue até **Configurar > Grupos de entrega**. Selecione o grupo de entrega a ser configurado e clique na página **Aplicativos**.
2. Marque os aplicativos desejados como **Obrigatório**.



3. Navegue para **Configurar > Grupos de entrega**.
4. Selecione o grupo de entrega e clique em **Implantar**.
5. Os usuários recebem uma solicitação para instalar o aplicativo e o aplicativo é instalado em segundo plano depois de aceitarem.



Aplicativos MDX

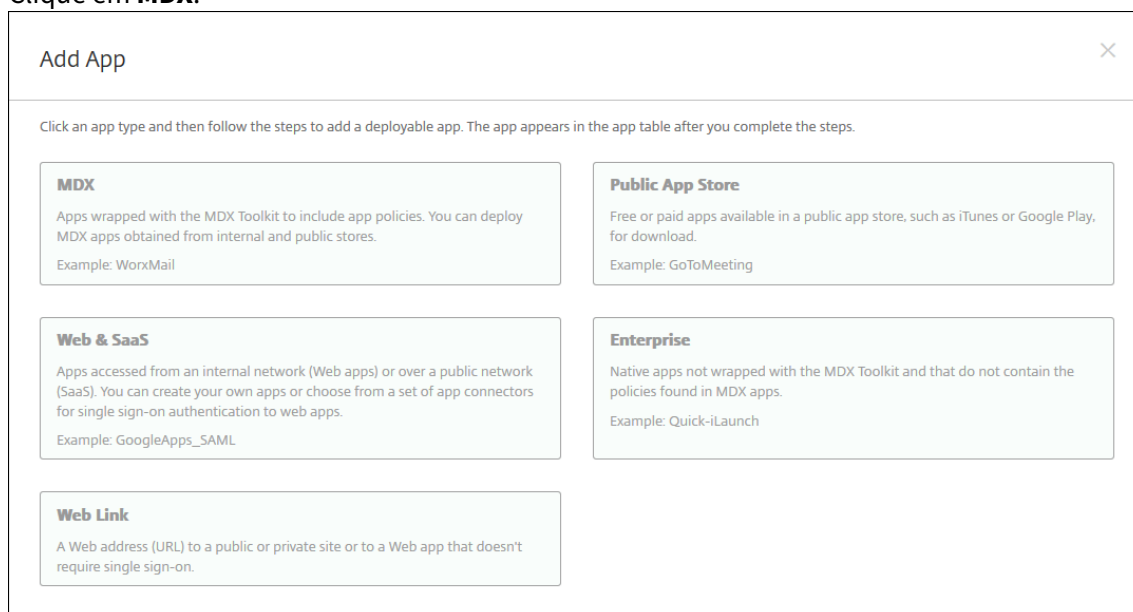
Para usar políticas de MDX e recursos de segurança, adicione aplicativos que estejam habilitados para MAM SDK ou preparados com MDX. Você pode implantar aplicativos MDX usando a compra por volume ou sem ela.

Disponibilidade de recursos

Requer supervisão do dispositivo	Não
Disponível para o modo de registro do usuário	Sim
Disponível em	iOS/iPadOS

Etapa 1: adicionar e configurar aplicativos

1. No console XenMobile, navegue até **Configurar > Aplicativos**. Clique em **Adicionar**.
2. Clique em **MDX**.



3. Selecione **iPhone** ou **iPad** para plataformas.
4. Carregue o arquivo MDX.
5. Configure os detalhes do aplicativo. Defina **Aplicativo implantado via compra por volume** como **Desativado**. A Citrix também recomenda ativar o recurso **Forçar aplicativo a ser gerenciado**.

Use the [MDX Service](#) on Citrix Cloud to wrap an app for delivery.

File name *	<input type="text" value="Secure Mail"/>
App Description *	<input type="text" value="Managed Enterprise Application"/>
App version	<input type="text" value="19.3.5"/>
Package ID	<input type="text" value="XGFUKY3NSP.com.citrix.mail.ios"/>
Minimum OS version	<input type="text" value="10.0"/>
Maximum OS version	<input type="text"/>
Excluded devices	<input type="text" value="example: manufacturer or model, ..."/>
Remove app if MDM profile is removed	<input checked="" type="checkbox"/>
Prevent app data backup	<input checked="" type="checkbox"/>
Force app to be managed	<input checked="" type="checkbox"/>
App deployed via Volume purchase	<input type="checkbox"/>
MDX Policies	
Authentication	
Device passcode	<input type="checkbox"/>

6. Configure as políticas de MDX. Defina **Desativar obrigatoriedade de atualização** como **Ativado**.

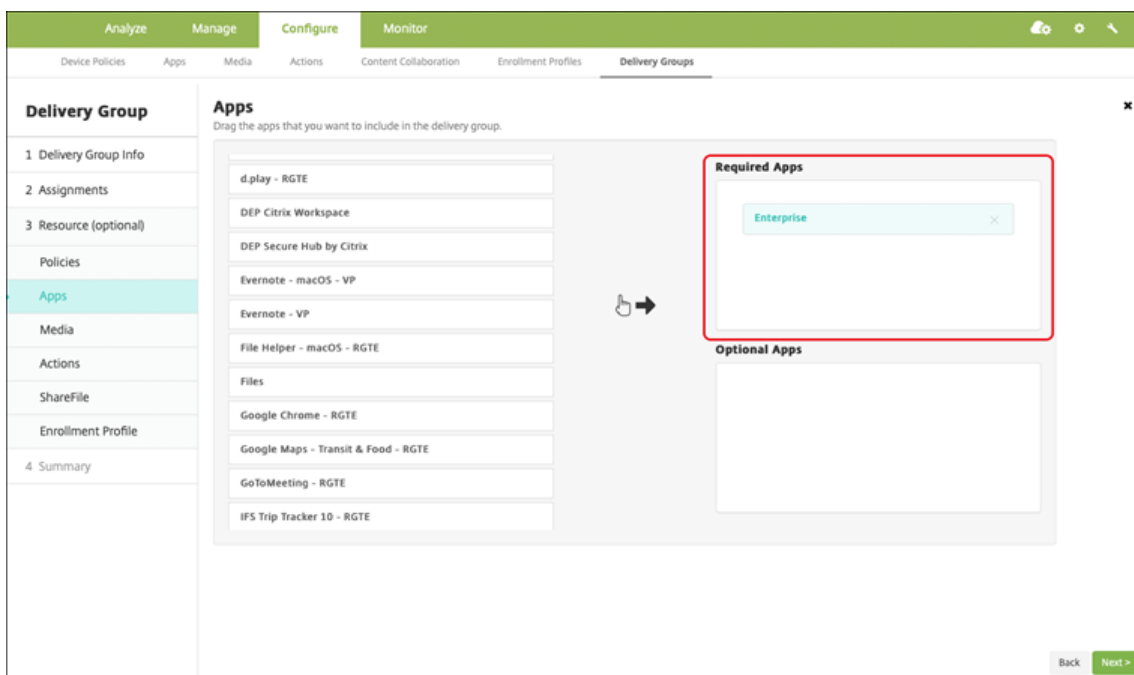
The screenshot displays the configuration interface for XenMobile, organized into three main sections:

- Miscellaneous Access:**
 - Disable required upgrade:** A toggle switch is turned ON.
 - App update grace period (hours):** A text input field contains the value 168.
 - Erase app data on lock:** A toggle switch is turned OFF.
 - Active poll period (minutes):** A text input field contains the value 60.
- Encryption:**
 - Enable encryption:** A dropdown menu is set to On.
 - Database encryption exclusions:** An empty text input field.
 - File encryption exclusions:** An empty text input field.
- App Interaction:**
 - Cut and copy:** A dropdown menu is set to Restricted.
 - Paste:** A dropdown menu is set to Unrestricted.

7. Atribua um grupo de entrega ao aplicativo e clique em **Salvar**.

Etapa 2: configurar implantação do aplicativo

1. No console XenMobile, navegue até **Configurar > Grupos de entrega > Aplicativos**.
2. Marque os aplicativos desejados como **Obrigatório**.



3. Navegue para **Configurar > Grupos de entrega**.
4. Selecione o grupo de entrega e clique em **Implantar**.
5. Os usuários recebem uma solicitação para instalar o aplicativo e o aplicativo é instalado em segundo plano depois de aceitarem.



Aplicativos MDX distribuídos através da compra por volume da Apple

Para usar políticas de MDX e recursos de segurança, adicione aplicativos que estejam habilitados para MAM SDK ou preparados com MDX. Para implantar aplicativos usando a compra por volume, os aplicativos devem existir na loja de aplicativos.

Disponibilidade de recursos

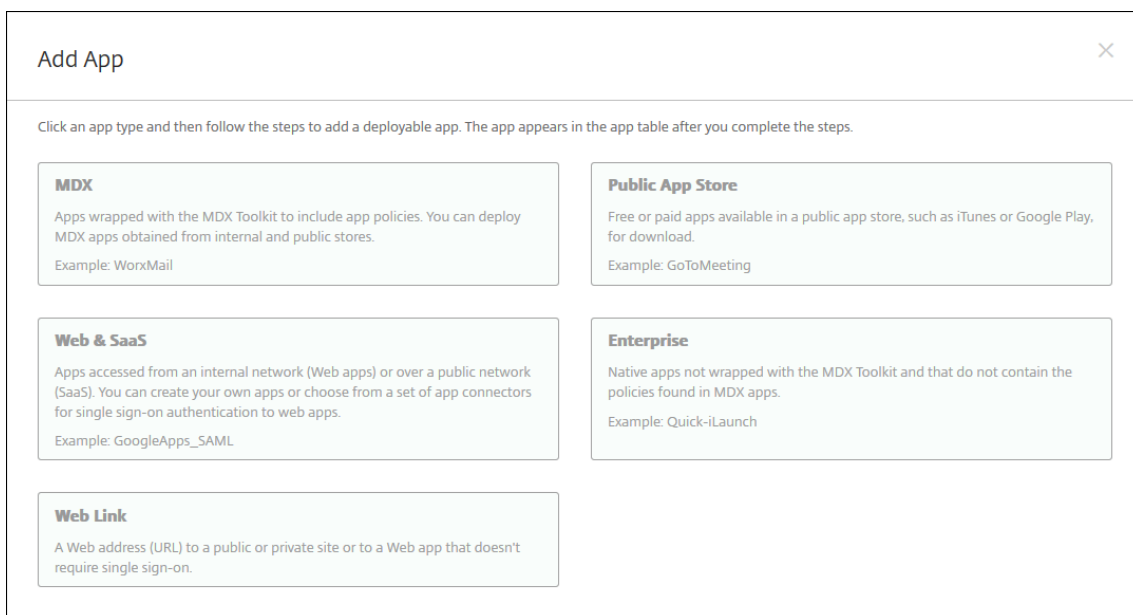
Requer supervisão do dispositivo	Não
Disponível para o modo de registro do usuário	Sim
Disponível em	iOS/iPadOS

Etapa 1: vincular contas

1. Configure e cadastre-se no Apple Business Manager (ABM) ou no Apple School Manager (ASM). Para obter mais informações sobre esses programas, consulte [Documentação da Apple](#).
2. Vincule sua conta ABM/ASM ao XenMobile. Para obter mais informações sobre como vincular contas de compra em volume, consulte [Compra por volume da Apple](#).
3. Ao adicionar sua conta de compra por volume, ative a **Atualização automática do aplicativo**. Essa configuração garante que os aplicativos nos dispositivos do usuário sejam atualizados automaticamente quando uma atualização aparece na Apple Store.

Etapa 2: adicionar e configurar aplicativos

1. No console XenMobile, navegue até **Configurar > Aplicativos**. Clique em **Adicionar**.
2. Clique em **MDX**.



3. Selecione **iPhone** ou **iPad** para plataformas.
4. Carregue o arquivo MDX.
5. Configure os detalhes do aplicativo. Defina **Aplicativo implantado via compra por volume** como **Ativado**. A Citrix também recomenda ativar o recurso **Forçar aplicativo a ser gerenciado**.

File name *	<input type="text" value="Secure Mail"/>
App Description *	<input type="text" value="Managed Enterprise Application"/>
App version	<input type="text" value="19.3.5"/>
Package ID	<input type="text" value="XGFUKY3NSP.com.citrix.mail.ios"/>
Minimum OS version	<input type="text" value="10.0"/>
Maximum OS version	<input type="text"/>
Excluded devices	<input type="text" value="example: manufacturer or model, ..."/>
Remove app if MDM profile is removed	<input checked="" type="checkbox"/>
Prevent app data backup	<input checked="" type="checkbox"/>
Force app to be managed	<input checked="" type="checkbox"/>
App deployed via Volume purchase	<input checked="" type="checkbox"/>
▼ MAM SDK Policies	
Authentication	
Device passcode	<input type="checkbox"/>

- Configure as políticas de MDX. Defina **Desativar obrigatoriedade de atualização** como **Ativado**.

The screenshot displays the configuration interface for an application, organized into three sections:

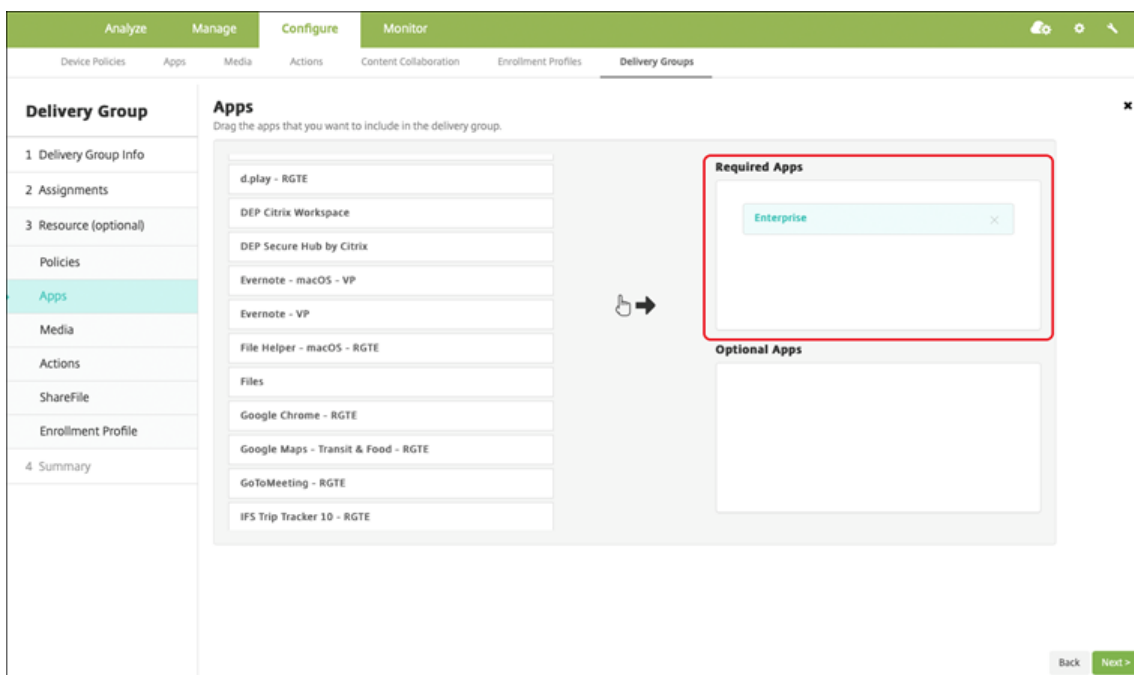
- Miscellaneous Access:**
 - Disable required upgrade:** A toggle switch is turned ON.
 - App update grace period (hours):** A text input field contains the value 168.
 - Erase app data on lock:** A toggle switch is turned OFF.
 - Active poll period (minutes):** A text input field contains the value 60.
- Encryption:**
 - Enable encryption:** A dropdown menu is set to On.
 - Database encryption exclusions:** An empty text input field.
 - File encryption exclusions:** An empty text input field.
- App Interaction:**
 - Cut and copy:** A dropdown menu is set to Restricted.
 - Paste:** A dropdown menu is set to Unrestricted.

7. Atribua um grupo de entrega ao aplicativo para cada plataforma e clique em **Salvar**.

Esta configuração resulta em duas entradas listadas para este aplicativo na lista de aplicativos. Quando você seleciona um aplicativo para configurar, selecione o aplicativo com **Tipo MDX**.

Etapa 3: configurar implantação do aplicativo

1. No console XenMobile, navegue até **Configurar > Grupos de entrega > Aplicativos**.
2. Marque os aplicativos de compra por volume desejados como **Obrigatório**.



3. Navegue para **Configurar > Grupos de entrega**.
4. Selecione o grupo de entrega e clique em **Implantar**.
5. Os usuários recebem uma solicitação para instalar o aplicativo e o aplicativo é instalado em segundo plano depois de aceitarem.



Aplicativos personalizados

Os aplicativos personalizados são aplicativos empresariais proprietários. Você pode usar o XenMobile e a compra por volume da Apple para distribuir aplicativos proprietários de forma privada e segura. Você pode distribuir os aplicativos para parceiros específicos, clientes, franqueados e funcionários internos.

Disponibilidade de recursos

Requer supervisão do dispositivo	Não
Disponível para o modo de registro do usuário	Sim
Disponível em	iOS/iPadOS

Requisitos para aplicativos personalizados

- Conta do Apple Business Manager ou Apple School Manager
- Conta de compra por volume da Apple (requer dispositivos com iOS 7 ou posterior)
- Registre os dispositivos no XenMobile usando um dos seguintes modos de registro da Apple:
 - Registro automatizado do dispositivo
 - Registro do dispositivo
 - Registro do usuário

Etapa 1: vincular contas

Para implantar aplicativos personalizados usando a compra por volume, vincule sua conta de compra por volume ao XenMobile.

1. Configure e cadastre-se no Apple Business Manager (ABM). Para obter mais informações sobre esses programas, consulte a [Documentação da Apple](#).
2. Vincule sua conta ABM ao XenMobile. Para obter mais informações sobre como vincular contas de compra em volume, consulte [Compra por volume da Apple](#).
3. Ao adicionar sua conta de compra por volume, ative a **Atualização automática do aplicativo**. Essa configuração garante que os aplicativos nos dispositivos do usuário sejam atualizados automaticamente quando uma atualização aparece na Apple Store.

Etapa 2: configurar aplicativos no ABM

Adicione aplicativos à sua conta ABM. Você pode carregar e distribuir seus próprios aplicativos personalizados ou comprar licenças para aplicativos personalizados de outras organizações. Para obter

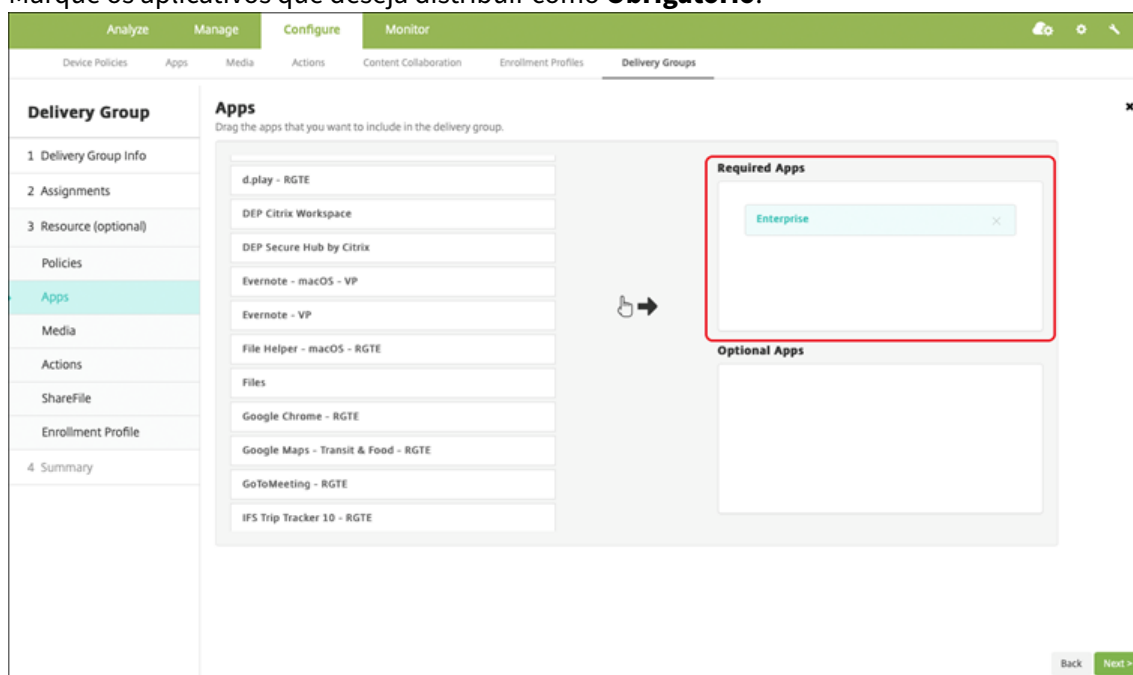
mais informações sobre como adicionar e ativar aplicativos personalizados no ABM, consulte a [Documentação da Apple](#).

Etapa 3: adicionar e configurar aplicativos no XenMobile

1. No console XenMobile, navegue até **Configurar > Aplicativos**. Os aplicativos de compra por volume são apresentados na lista de aplicativos.
2. Selecione o aplicativo que deseja configurar. Clique em **Edit**.
3. Selecione as plataformas: **iPhone, iPad** ou **macOS**.
4. Escolha os grupos de entrega aos quais deseja que o aplicativo seja distribuído. Clique em **Salvar**.

Etapa 4: configurar implantação do aplicativo

1. No console XenMobile, navegue até **Configurar > Grupos de entrega > Aplicativos**.
2. Marque os aplicativos que deseja distribuir como **Obrigatório**.



3. Navegue de volta para **Configurar > Grupos de entrega**.
4. Selecione o grupo de entrega que deseja implantar e clique em **Implantar**.
5. Os usuários recebem uma solicitação para implantar aplicativos. Os aplicativos são instalados em segundo plano depois que os usuários os aceitam.



Aplicativos personalizados habilitados com MDX

Para usar políticas de MDX e recursos de segurança, adicione aplicativos personalizados que estejam habilitados para MAM SDK ou preparados com MDX.

Disponibilidade de recursos

Requer supervisão do dispositivo	Não
Disponível para o modo de registro do usuário	Sim
Disponível em	iOS/iPadOS

Etapa 1: vincular contas

Para implantar aplicativos personalizados usando a compra por volume, vincule sua conta de compra por volume ao XenMobile.

1. Configure e cadastre-se no Apple Business Manager (ABM). Para obter mais informações sobre esses programas, consulte a [Documentação da Apple](#).
2. Vincule sua conta ABM ao XenMobile. Para obter mais informações sobre como vincular contas de compra em volume, consulte [Compra por volume da Apple](#).

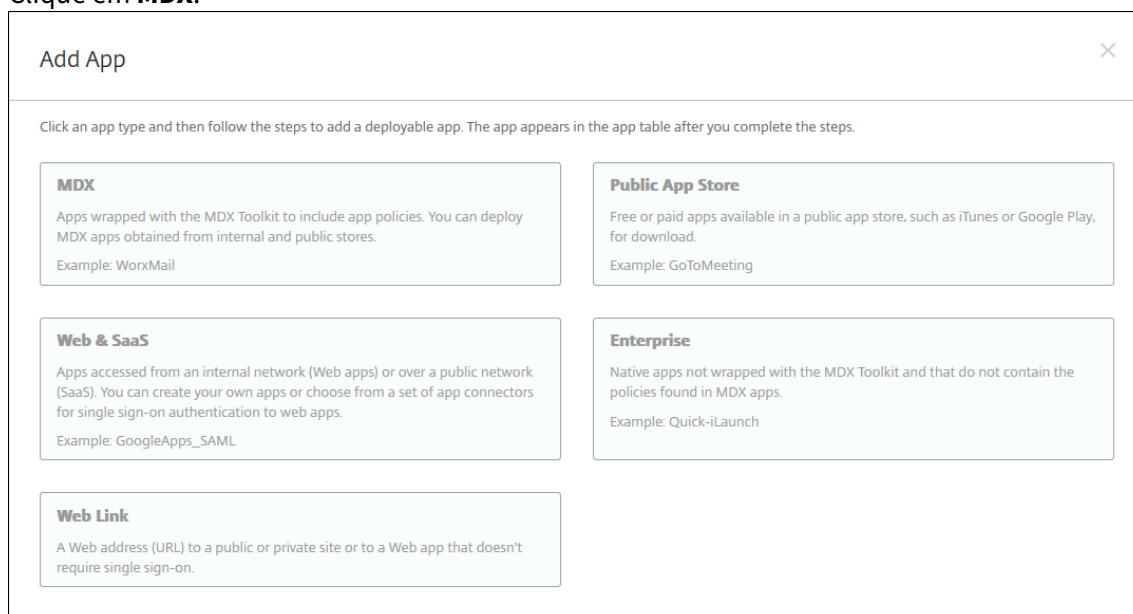
3. Ao adicionar sua conta de compra por volume, ative a **Atualização automática do aplicativo**. Essa configuração garante que os aplicativos nos dispositivos do usuário sejam atualizados automaticamente quando uma atualização aparece na Apple Store.

Etapa 2: configurar aplicativos no ABM

Adicione aplicativos à sua conta ABM. Você pode carregar e distribuir seus próprios aplicativos personalizados ou comprar licenças para aplicativos personalizados de outras organizações. Para obter mais informações sobre como adicionar e ativar aplicativos personalizados no ABM, consulte a [Documentação da Apple](#).

Etapa 3: adicionar e configurar aplicativos no XenMobile

1. No console XenMobile, navegue até **Configurar > Aplicativos**. Clique em **Adicionar**.
2. Clique em **MDX**.



3. Selecione as plataformas **iPhone** ou **iPad**.
4. Carregue o arquivo MDX para o aplicativo que você deseja adicionar.
5. Configure os detalhes do aplicativo. Defina **Aplicativo implantado via compra por volume** como **Ativado**. A Citrix também recomenda ativar o recurso **Forçar aplicativo a ser gerenciado**.

File name *	<input type="text" value="Secure Mail"/>
App Description *	<input type="text" value="Managed Enterprise Application"/>
App version	<input type="text" value="19.3.5"/>
Package ID	<input type="text" value="XGFUKY3NSP.com.citrix.mail.ios"/>
Minimum OS version	<input type="text" value="10.0"/>
Maximum OS version	<input type="text"/>
Excluded devices	<input type="text" value="example: manufacturer or model, ..."/>
Remove app if MDM profile is removed	<input checked="" type="checkbox"/>
Prevent app data backup	<input checked="" type="checkbox"/>
Force app to be managed	<input checked="" type="checkbox"/>
App deployed via Volume purchase	<input checked="" type="checkbox"/>
▼ MAM SDK Policies	
Authentication	
Device passcode	<input type="checkbox"/>

6. Configure as políticas de MDX. Defina **Desativar obrigatoriedade de atualização** como **Ativado**.

The screenshot displays the configuration interface for an application, organized into three sections:

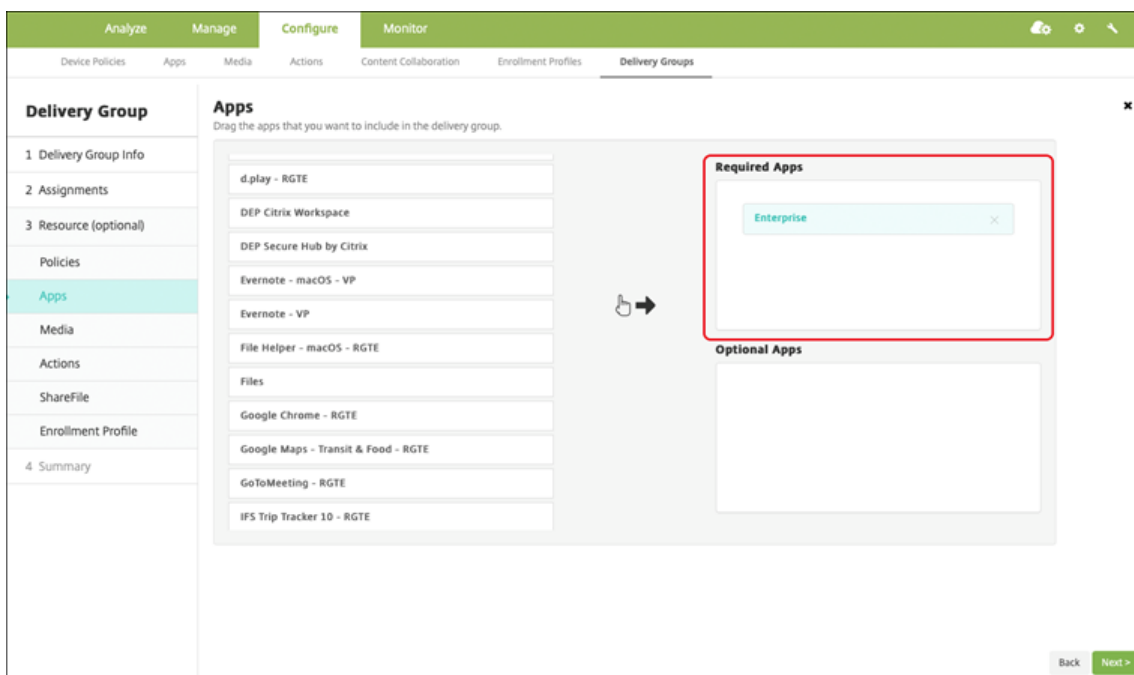
- Miscellaneous Access:**
 - Disable required upgrade:** A toggle switch is turned ON.
 - App update grace period (hours):** A text input field contains the value 168.
 - Erase app data on lock:** A toggle switch is turned OFF.
 - Active poll period (minutes):** A text input field contains the value 60.
- Encryption:**
 - Enable encryption:** A dropdown menu is set to On.
 - Database encryption exclusions:** An empty text input field.
 - File encryption exclusions:** An empty text input field.
- App Interaction:**
 - Cut and copy:** A dropdown menu is set to Restricted.
 - Paste:** A dropdown menu is set to Unrestricted.

7. Atribua um grupo de entrega ao aplicativo e clique em **Salvar**.

Esta configuração resulta em duas entradas listadas para este aplicativo na lista de aplicativos. Quando você seleciona um aplicativo para configurar, selecione o aplicativo com **Tipo MDX**.

Etapa 4: configurar implantação do aplicativo

1. No console XenMobile, navegue até **Configurar > Aplicativos**. Os aplicativos de compra por volume são apresentados na lista de aplicativos.
2. Selecione o aplicativo que deseja configurar. Clique em **Edit**.
3. Escolha os grupos de entrega aos quais deseja que o aplicativo seja distribuído em cada plataforma. Clique em **Salvar**.
4. Navegue de volta para **Configurar > Grupos de entrega > Aplicativos**.
5. Marque os aplicativos que deseja distribuir como **Obrigatório**.



6. Navegue de volta para **Configurar > Grupos de entrega**.
7. Selecione o grupo de entrega que deseja implantar e clique em **Implantar**.
8. Os usuários recebem uma solicitação para implantar aplicativos. Os aplicativos são instalados em segundo plano depois de aceitarem.

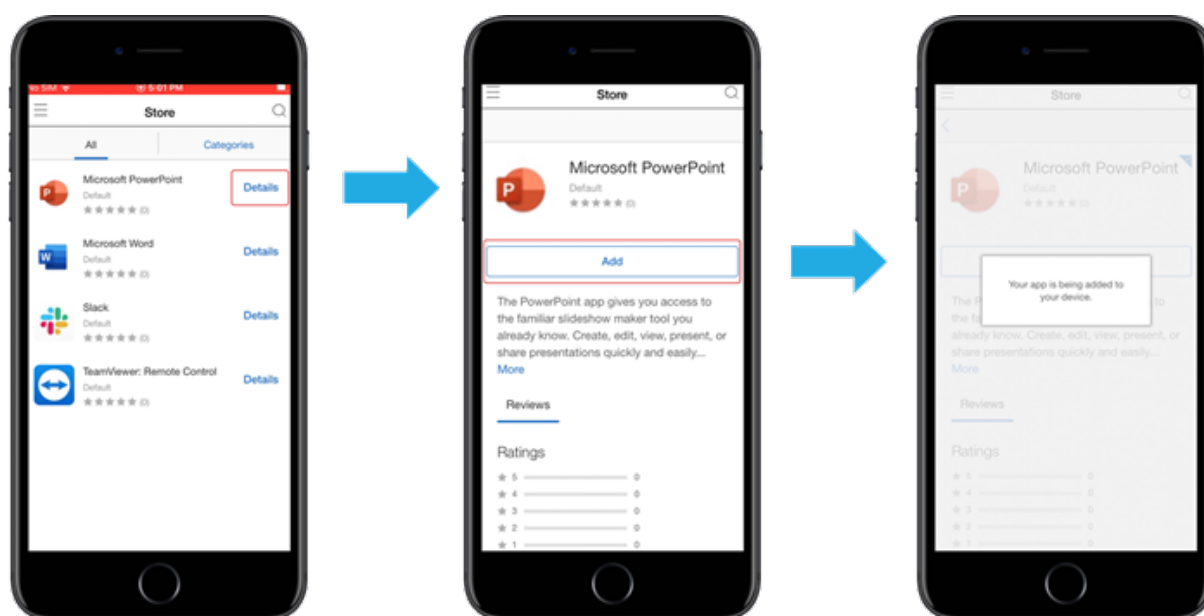


Aplicativos opcionais (somente iOS/iPadOS)

A Citrix recomenda a implantação de aplicativos conforme **Obrigatório**. Aplicativos obrigatórios são instalados silenciosamente nos dispositivos do usuário, minimizando a interação. Ter esse recurso habilitado também permite que os aplicativos sejam atualizados automaticamente.

Os aplicativos opcionais permitem que os usuários escolham quais aplicativos instalar, mas os usuários devem iniciar a instalação manualmente por meio do Secure Hub.

Para instalar aplicativos opcionais, os usuários devem iniciar o Secure Hub, acessar **Loja**, selecionar **Detalhes** do aplicativo desejado e clicar em **Adicionar**.



Controle de Acesso da Rede

May 6, 2021

Você pode usar sua solução de Controle de Acesso à Rede (NAC) para estender a avaliação de segurança do dispositivo Endpoint Management para dispositivos Android e Apple. A sua solução NAC usa a avaliação de segurança do XenMobile para facilitar e manipular decisões de autenticação. Depois de configurar o dispositivo NAC, as políticas de dispositivo e os filtros NAC configurados no XenMobile são impostas.

O uso do XenMobile com uma solução NAC adiciona QoS e um controle mais granular sobre dispositivos internos à sua rede. Para obter um resumo das vantagens de integrar NAC ao XenMobile, consulte [Controle de acesso](#).

A Citrix oferece suporte a estas soluções para integração com o XenMobile:

- Citrix Gateway
- Cisco Identity Services Engine (ISE)
- ForeScout

A Citrix não garante integração para outras soluções NAC.

Com um dispositivo NAC em sua rede:

- O XenMobile oferece suporte a NAC como um recurso de segurança de ponto de extremidade para dispositivos iOS, Android Enterprise e Android.
- Você pode habilitar filtros no XenMobile para definir dispositivos como compatíveis ou não compatíveis com NAC, com base em regras ou propriedades. Por exemplo:
 - Se um dispositivo gerenciado no XenMobile não atender aos critérios especificados, o XenMobile marcará o dispositivo como não compatível. Um dispositivo NAC bloqueia dispositivos não compatíveis na sua rede.
 - Se um dispositivo gerenciado no XenMobile tiver aplicativos não compatíveis instalados, um filtro NAC poderá bloquear a conexão VPN. Como resultado, um dispositivo de usuário não compatível não pode acessar aplicativos ou sites por meio da VPN.
 - Se você usa o Citrix Gateway para NAC, poderá habilitar o túnel dividido para impedir que o Citrix Gateway Plug-in envie tráfego de rede desnecessário para o Citrix Gateway. Para obter mais informações sobre túnel dividido, consulte [Configurar túnel dividido](#).

Filtros de conformidade com NAC suportados

O XenMobile Server é compatível com os seguintes filtros de conformidade com NAC:

Dispositivos Anônimos: verifica se um dispositivo está no modo anônimo. Essa verificação estará disponível se o XenMobile não conseguir autenticar novamente o usuário quando um dispositivo tentar se reconectar.

Erro de atestado de Samsung Knox: verifica se um dispositivo falhou em uma consulta do servidor de atestado do Samsung Knox.

Aplicativos proibidos: verifica se um dispositivo tem aplicativos proibidos, conforme definido em uma política de dispositivo de Acesso aos Aplicativos. Para obter informações sobre essa política, consulte [Políticas de dispositivo de acesso aos aplicativos](#).

Dispositivos inativos: verifica se um dispositivo está inativo conforme definido pela configuração **Limite de Dias de Inatividade do dispositivo** em **Propriedades do Servidor**. Para obter detalhes, consulte [Propriedades do servidor](#).

Aplicativos obrigatórios ausentes: verifica se um dispositivo não tem algum aplicativo obrigatório, conforme definido em uma política de Acesso aos aplicativos.

Aplicativos não sugeridos: verifica se um dispositivo tem aplicativos não sugeridos, conforme definido em uma Política de acesso aos aplicativos.

Senha não compatível: verifica se a senha de usuário está em conformidade. Nos dispositivos Android e iOS, o XenMobile pode determinar se a senha no dispositivo no momento está em conformidade com a política de código secreto enviada para o dispositivo. Por exemplo, no iOS, o usuário tem 60 minutos para definir uma senha se o XenMobile enviar uma política de código secreto para o dispositivo. Antes que o usuário defina a senha, o código secreto pode não estar em conformidade.

Dispositivos sem conformidade: verifica se um dispositivo está fora de conformidade, com base na propriedade de dispositivo Sem Conformidade. Normalmente, ações automatizadas ou terceiros que usam as APIs do XenMobile alteram essa propriedade do dispositivo.

Status revogado: verifica se o certificado do dispositivo está revogado. Um dispositivo revogado não pode se registrar novamente até que tenha autorização novamente.

Dispositivos Android com root e iOS com jailbreak: verifica se um dispositivo Android ou iOS tem root ou jailbreak.

Dispositivos não gerenciados: verifica se um dispositivo ainda está em um estado gerenciado, sob o controle do XenMobile. Por exemplo, um dispositivo registrado no MAM ou um dispositivo não registrado não é gerenciado.

Nota:

O filtro Conformidade/Não conformidade implícita define o valor padrão somente nos dispositivos que o XenMobile está gerenciando. Por exemplo, qualquer dispositivo que tenha um aplicativo na lista de bloqueio instalado ou que não esteja registrado é marcado como Não compatível. O dispositivo NAC bloqueia o dispositivo da sua rede.

Visão geral da configuração

Recomendamos que você configure os componentes NAC na ordem listada.

1. Configurar políticas de dispositivo para suportar NAC:

Para dispositivos iOS: consulte [Configurar a política de dispositivo de VPN para suportar NAC](#).

Para dispositivos Android Enterprise: consulte [Criar uma configuração gerenciada do Android Enterprise para o Citrix SSO](#).

Para dispositivos Android: consulte [Configurar o protocolo Citrix SSO para Android](#).

2. Ativar filtros NAC no XenMobile.

3. Configurar uma solução NAC:

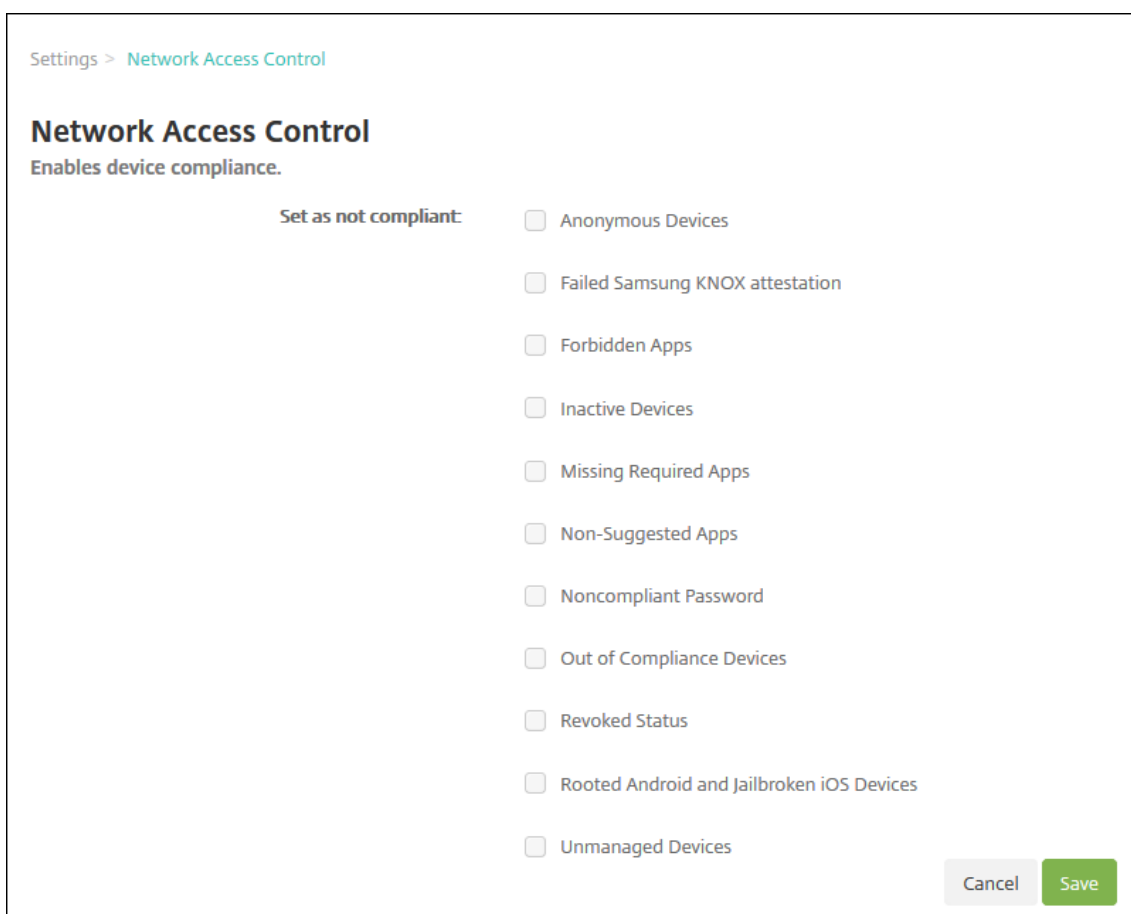
- Citrix Gateway, detalhado em [Atualizar políticas do Citrix Gateway para suportar NAC](#).

Requer que você a instale o Citrix SSO nos dispositivos. Consulte [Clientes Citrix Gateway](#).

- Cisco ISE: consulte a documentação da Cisco.
- ForeScout: consulte a documentação da ForeScout.

Ativar filtros NAC no XenMobile

1. No console XenMobile, vá para **Configurações > Controle de acesso da rede**.



2. Marque as caixas de seleção dos filtros **Definir como não compatível** que você deseja ativar.
3. Clique em **Salvar**.

Atualizar políticas do Citrix Gateway para suportar NAC

Você deve configurar políticas avançadas (não clássicas) de autenticação e sessões VPN em seu servidor virtual VPN.

Estas etapas atualizam um Citrix Gateway com uma destas características:

- Está integrado a um ambiente do XenMobile Server.
- Ou está configurado para VPN, não faz parte do ambiente do XenMobile Server e pode acessar o XenMobile.

No servidor VPN virtual, em uma janela do console, faça o seguinte. Os endereços IP nos comandos e exemplos são fictícios.

1. Se você estiver usando políticas clássicas em seu servidor virtual VPN, remova e desvincule todas as políticas clássicas. Para verificar, digite:

```
show vpn vserver <VPN_VServer>
```

Remova os resultados que contenham a palavra Classic. Por exemplo: `VPN Session Policy Name: PL_OS_10.10.1.1 Type: Classic Priority: 0`

Para remover a política, digite:

```
unbind vpn vserver <VPN_VServer> -policy <policy_name>
```

2. Crie a política de sessão avançada correspondente digitando o seguinte.

```
add vpn sessionPolicy <policy_name> <rule> <session action>
```

Por exemplo: `add vpn sessionPolicy vpn_nac true AC_OS_10.10.1.1_A_`

3. Vincule a política ao seu servidor virtual VPN digitando o seguinte.

```
bind vpn vserver _XM_XenMobileGateway -policy vpn_nac -priority 100
```

4. Crie um servidor virtual de autenticação digitando o seguinte.

```
add authentication vserver <authentication vserver name> <service type>  
<ip address>
```

Por exemplo: `add authentication vserver authvs SSL 0.0.0.0`

No exemplo, `0.0.0.0` significa que o servidor virtual de autenticação não é público.

5. Vincule um certificado SSL ao servidor virtual digitando o seguinte.

```
bind ssl vserver <authentication vserver name> -certkeyName <Webserver  
certificate>
```

Por exemplo: `bind ssl vserver authvs -certkeyName Star_mpg_citrix.pfx_CERT_KEY`

6. Associe um perfil de autenticação ao servidor virtual de autenticação a partir do servidor virtual VPN. Primeiro, crie o perfil de autenticação digitando o seguinte.

```
add authentication authnProfile <profile name> -authnVsName <authentication  
vserver name>
```

Por exemplo:

```
add authentication authnProfile xm_nac_prof -authnVsName authvs
```

7. Associe o perfil de autenticação ao servidor virtual VPN digitando o seguinte.

```
set vpn vserver <vpn vserver name> -authnProfile <authn profile name>
```

Por exemplo:

```
set vpn vserver _XM_XenMobileGateway -authnProfile xm_nac_prof
```

8. Verifique a conexão do Citrix Gateway com um dispositivo digitando o seguinte.

```
curl -v -k https://<XenMobile server>:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_<device_id>"
```

Por exemplo, esta consulta verifica a conectividade obtendo o status de conformidade do primeiro dispositivo (`deviceid_1`) registrado no ambiente:

```
curl -v -k https://10.10.1.1:4443/Citrix/Device/v1/Check --header "X-Citrix-VPN-Device-ID: deviceid_1"
```

Um resultado bem-sucedido é semelhante ao exemplo a seguir.

```
1 HTTP/1.1 200 OK
2 < Server: Apache-Coyote/1.1
3 < X-Citrix-Device-State: Non Compliant
4 < Set-Cookie: ACNODEID=181311111;Path=/; HttpOnly; Secure
5 <!--NeedCopy-->
```

9. Quando a etapa anterior for bem-sucedida, crie a ação de autenticação da Web para o XenMobile. Primeiro, crie uma expressão de política para extrair o ID do dispositivo do plug-in VPN no iOS. Digite o seguinte.

```
add policy expression xm_deviceid_expression "HTTP.REQ.BODY(10000).TYPECAST_NVLIST_T(\ '=' \', \ '& \').VALUE(\ "deviceidvalue \")"
```

10. Envie a solicitação para o XenMobile digitando o seguinte. Neste exemplo, o IP do XenMobile Server é 10.207.87.82 e o FQDN é `example.em.server.com:4443`.

```
add authentication webAuthAction xm_nac -serverIP 10.207.87.82 -serverPort 4443 -fullReqExpr q{ "GET /Citrix/Device/v1/Check HTTP/1.1\r\n" + "Host: example.em.server.com:4443\r\n" + "X-Citrix-VPN-Device-ID: " + xm_deviceid_expression + "\r\n\r\n"} -scheme https -successRule "HTTP.RES.STATUS.EQ(\ "200 \") && HTTP.RES.HEADER(\ "X-Citrix-Device-State \").EQ (\ "Compliant \")"
```

O resultado bem-sucedido para XenMobile NAC é HTTP status 200 OK. O cabeçalho `X-Citrix-Device-State` deve ter o valor de `Compliant`.

11. Crie uma política de autenticação com a qual associar a ação digitando o seguinte.

```
add authentication Policy <policy name> -rule <rule> -action <web authentication action>
```

Por exemplo: `add authentication Policy xm_nac_webauth_pol -rule "HTTP.REQ.HEADER(\ "User-Agent \").CONTAINS(\ "NAC \")" -action xm_nac`

12. Converta a política LDAP existente em uma política avançada digitando o seguinte.

```
add authentication Policy <policy_name> -rule <rule> -action <LDAP  
action name>
```

Por exemplo: `add authentication Policy ldap_xm_test_pol -rule true -action 10.10.1.1_LDAP`

13. Adicione um rótulo de política ao qual associar a política de LDAP digitando o seguinte.

```
add authentication policylabel <policy_label_name>
```

Por exemplo: `add authentication policylabel ldap_pol_label`

14. Associe a política de LDAP ao rótulo de política digitando o seguinte.

```
bind authentication policylabel ldap_pol_label -policyName ldap_xm_test_pol  
-priority 100 -gotoPriorityExpression NEXT
```

15. Conecte um dispositivo compatível para fazer um teste de NAC para confirmar a autenticação LDAP bem-sucedida. Digite o seguinte.

```
bind authentication vserver <authentication vserver> -policy <web  
authentication policy> -priority 100 -nextFactor <ldap policy label> -  
gotoPriorityExpression END
```

16. Adicione a IU para associar ao servidor virtual de autenticação. Digite o seguinte comando para recuperar o ID do dispositivo.

```
add authentication loginSchemaPolicy <schema policy>-rule <rule> -  
action lschema_single_factor_deviceid
```

17. Vincule o servidor virtual de autenticação digitando o seguinte.

```
bind authentication vserver authvs -policy lschema_xm_nac_pol -priority  
100 -gotoPriorityExpression END
```

18. Crie uma política de autenticação avançada de LDAP para habilitar a conexão do Secure Hub. Digite o seguinte.

```
add authentication Policy ldap_xm_test_pol -rule "HTTP.REQ.HEADER(\ "  
User-Agent\").CONTAINS(\ "NAC\").NOT"-action 10.200.80.60_LDAP
```

```
bind authentication vserver authvs -policy ldap_xm_test_pol -priority  
110 -gotoPriorityExpression NEXT
```

Samsung Knox

April 8, 2021

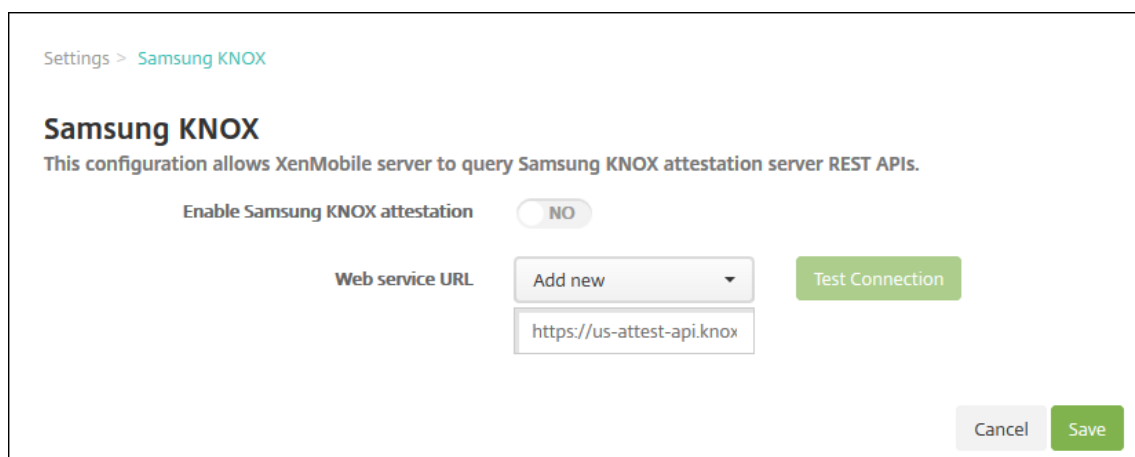
A Samsung oferece várias soluções compatíveis com o XenMobile Server.

- O XenMobile suporta e amplia as políticas do Samsung Knox em dispositivos Samsung compatíveis.
- O Knox Service Plug-in (KSP) é um aplicativo que suporta um subconjunto de recursos do Knox Platform for Enterprise (KPE). Para obter informações da Samsung sobre o KPE, consulte [Configure Knox Platform for Enterprise](#) e [Visão geral](#).

Você pode configurar o XenMobile para consultar as APIs REST do servidor de atestado do Samsung Knox.

O Samsung Knox usa os recursos de segurança de hardware que oferecem vários níveis de proteção para o sistema operacional e os aplicativos. Um nível dessa segurança reside na plataforma por meio do atestado. Um servidor de atestado fornece a verificação do software de sistema central do dispositivo móvel (por exemplo, os carregadores de inicialização e o kernel). A verificação ocorre em tempo de execução com base nos dados coletados durante a inicialização confiável.

1. No console da Web XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida.
2. Em **Plataformas**, clique em **Samsung KNOX**. A página **Samsung KNOX** é exibida.



3. Em **Ativar atestado do Samsung KNOX**, selecione se o atestado do Samsung Knox deve ser ativado. O padrão é **NÃO**.
4. Quando você define **Ativar atestado do Samsung KNOX** como **SIM**, a opção **URL de serviço da Web** é ativada. Em seguida, na lista, siga um dos seguintes procedimentos:
 - Clique no servidor de atestado apropriado.
 - Clique em **Adicionar novo** e, em seguida, digite a URL do serviço da Web.
5. Clique em **Testar conexão** para verificar a conexão. É exibida uma mensagem de êxito ou falha.
6. Clique em **Salvar**.

Nota:

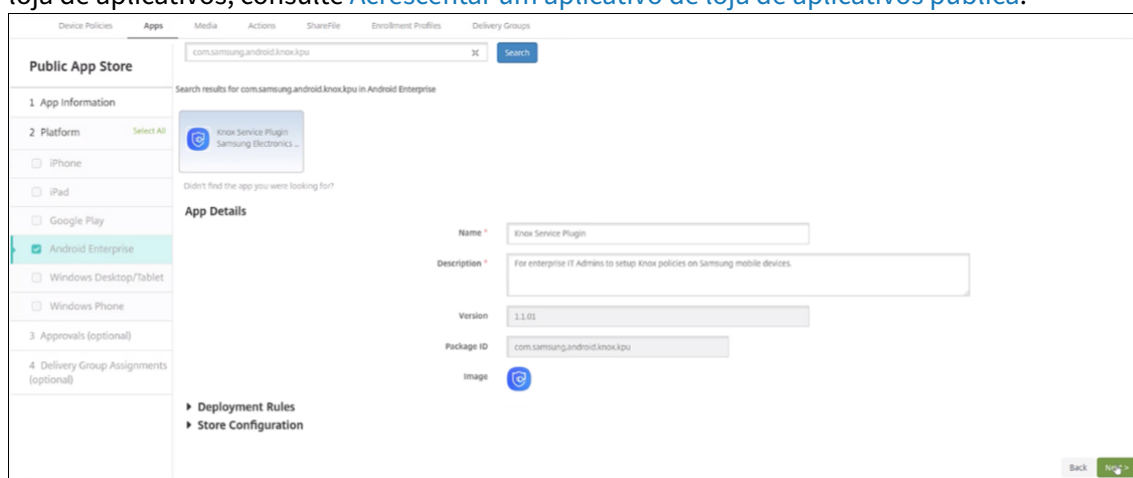
Você pode usar o Samsung Knox Mobile Enrollment para registrar vários dispositivos Samsung Knox no XenMobile (ou qualquer gerenciador de dispositivos móveis) sem configurar manualmente cada dispositivo. Para obter informações, consulte [Registro em massa do Samsung Knox](#).

Adicionar o aplicativo Knox Service Plug-in

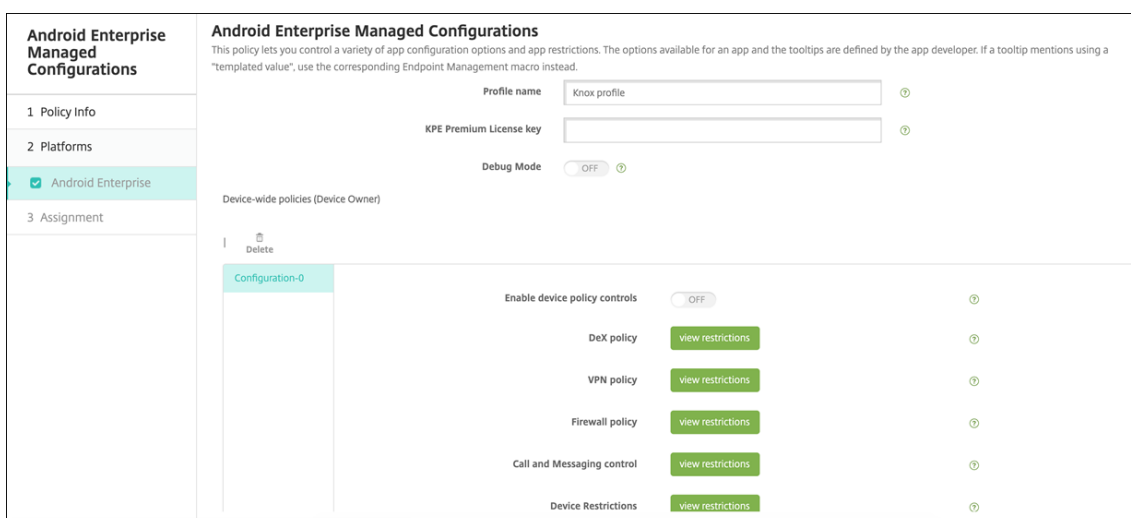
Se você planeja usar o Android Enterprise com o Knox, adicione o Knox Service Plug-in Knox (KSP) ao XenMobile. O aplicativo KSP usa o AndroidOEMConfig para dar suporte a recursos como políticas de segurança, configuração VPN flexível e controles de autenticação biométrica. O AndroidOEMConfig permite que OEMs e gerenciadores de mobilidade de pontos de extremidade (EMM) suportem APIs OEM personalizadas. Essas APIs cobrem casos de uso não suportados pelo Android Enterprise.

Para obter mais informações sobre o KSP, consulte o [Guia de administração do Knox Service Plug-in](#).

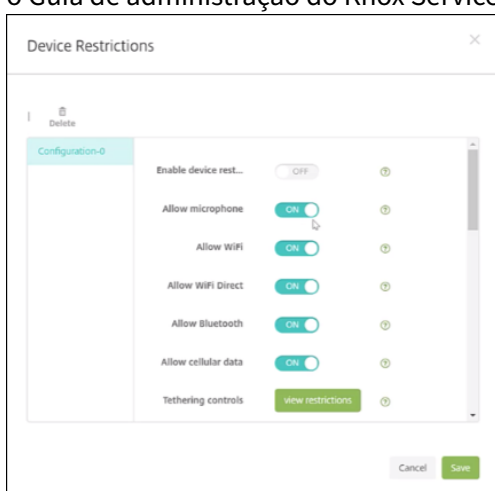
1. Entre na sua conta do Google e navegue até <https://play.google.com/work/apps/details?id=com.samsung.android.knox.kpu>. Aprove o aplicativo Knox Service Plug-in.
2. Entre no console XenMobile e adicione o Knox Service Plug-in como um aplicativo público da loja de aplicativos. Para obter mais informações sobre como adicionar aplicativos públicos da loja de aplicativos, consulte [Acrescentar um aplicativo de loja de aplicativos pública](#).



3. No console XenMobile, navegue até **Configurar > Políticas de dispositivo**. Clique em **Adicionar**.
4. Clique em **Configuração gerenciada do Android Enterprise**. Na caixa de diálogo que aparece, selecione **Knox Service Plugin** no menu. Para obter mais informações sobre a política de configuração gerenciada do Android Enterprise, consulte [Política de configurações gerenciadas do Android Enterprise](#).
5. Digite um nome para a política e continue para a página da plataforma.



6. Na página da plataforma, digite um **Nome de perfil** para o seu perfil Knox e insira o valor de **KPE Premium License key** da Samsung. As políticas que aparecem abaixo desses campos provêm da sua implantação do Knox. Para obter mais informações sobre as políticas do Knox, consulte o Guia de administração do Knox Service Plug-in mencionado anteriormente nesta seção.



7. Clique em **Avançar** e configure as regras de implantação para a política.
8. Clique em **Salvar**.

Registro em massa do Samsung Knox

April 1, 2021

Para registrar vários dispositivos Samsung Knox no XenMobile (ou qualquer gerenciador de dispositivos móveis) sem configurar manualmente cada dispositivo, use o Knox Mobile Enrollment. O registro ocorre após o primeiro uso ou após uma redefinição de fábrica. Os administradores também podem passar nomes de usuário e senhas diretamente para o dispositivo, para que os usuários não

precisem inserir informações no momento do registro.

Nota:

A configuração do Knox Mobile Enrollment não está relacionada ao contêiner XenMobile Knox. Para obter mais informações sobre o Knox Mobile Enrollment, consulte o [Guia de administração do Knox Mobile Enrollment](#).

Pré-requisitos de Knox Mobile Enrollment

- O XenMobile deve estar configurado (incluindo licenças e os certificados) e em execução.
- Arquivo APK do Secure Hub. Você carrega o arquivo ao configurar o Knox Mobile Enrollment.
- Para obter uma lista de requisitos do KME, consulte a [Introdução ao Knox Mobile Enrollment](#).
- Licença do Samsung Knox Platform for Enterprise (PKE), necessária para aplicar políticas de dispositivos. Forneça a chave de licença na política de dispositivo do XenMobile, Knox Platform for Enterprise.

Para baixar o arquivo APK do Secure Hub

Acesse a loja do Google Play para baixar o arquivo Citrix Secure Hub para Android.

Configurar exceções de firewall

Para acessar o Knox Mobile Enrollment, configure as seguintes exceções de firewall. Algumas dessas exceções de firewall são necessárias para todos os serviços e algumas são específicas para a região geográfica do dispositivo.

Região do dispositivo	URL	Porta	Destino
Todos	https://gs1b.secb2b.com	443	Balanceador de carga global para iniciação de Know Mobile Enrollment
Todos	https://gs1b.secb2b.com	80	Balanceador de carga global para iniciação de Know Mobile Enrollment em alguns dispositivos legados limitados

Região do dispositivo	URL	Porta	Destino
Todos	<code>umc-cdn.secb2b.com</code>	443	Servidores de atualização de agente Samsung
Todos	<code>bulkenrollment.s3.amazonaws.com</code>	80	EULAs de cliente de Knox Mobile Enrollment
Todos	<code>eula.secb2b.com</code>	443	EULAs de cliente de Knox Mobile Enrollment
Todos	<code>us-be-api-mssl.samsungknox.com</code>	443	Servidores Samsung para verificação de IMEI
Estados Unidos	<code>https://us-segd-api.secb2b.com</code>	443	Samsung Enterprise Gateway para a região dos EUA
Europa	<code>https://eu-segd-api.secb2b.com</code>	443	Samsung Enterprise Gateway para a região da Europa
China	<code>https://china-segd-api.secb2b.com</code>	443	Samsung Enterprise Gateway para a região da China

Nota:

Você pode encontrar uma lista completa de exceções de firewall no [Guia de administração do Knox Mobile Enrollment](#).

Obter acesso ao Knox Mobile Enrollment

Siga a documentação da Samsung para obter acesso ao Knox Mobile Enrollment em [Get started with KME](#).

Configuração do Knox Mobile Enrollment

Depois de obter acesso ao Knox Mobile Enrollment, faça logon no portal do Knox.

O processo de registro segue estas etapas gerais.

1. Crie um perfil MDM com o seu console do MDM, informações e configurações.
O perfil do MDM informa aos seus dispositivos como conectar ao seu MDM.
2. Adicione dispositivos ao seu perfil MDM.
Você pode carregar um arquivo CSV com informações do dispositivo ou instalar e usar o aplicativo de implantação Knox do Google Play.
3. A Samsung alerta você quando a propriedade do dispositivo é confirmada.
4. Forneça aos usuários as credenciais de MDM. Instrua-os para que se conectem à Internet usando Wi-Fi e aceitem o aviso para registrar o dispositivo.

Para criar um perfil de MDM

Siga os passos descritos na documentação da Samsung em [Profile Configuration](#).

Quando você encontrar os seguintes campos ou etapas, configure-os conforme descrito:

- **Pick your MDM:** selecione **Citrix** no menu. Somente para perfis de proprietário de dispositivo.
- **MDM Agent APK:** apenas para perfis de proprietário de dispositivo. Digite o URL de download do APK do Secure Hub: `https://play.google.com/managed/downloadManagingApp?identifier=xenmobile`.

O arquivo APK pode estar em um servidor que os dispositivos podem acessar durante o registro. Durante o registro, um dispositivo:

- Baixa o Secure Hub a partir da URL de download do APK
- Instala o Secure Hub
- Em seguida, abre o Secure Hub com os dados JSON personalizados descritos a seguir.

o uso de maiúsculas e minúsculas do nome do arquivo .apk deve corresponder à URL que você insere. Por exemplo, se o nome do arquivo é todo em minúsculas, ele também deve ser todo em minúsculas no URL.

- **MDM Server URI:** não especifique nenhuma URI de servidor MDM. O XenMobile não usa o protocolo Samsung MDM.
- **Custom JSON Data:** o Secure Hub precisa do endereço do servidor XenMobile além do nome de usuário e da senha para o registro. Você pode fornecer esses dados no JSON de modo que o Secure Hub não solicite aos usuários. O Secure Hub solicita aos usuários o endereço do servidor, o nome de usuário ou a senha somente se o campo for omitido do JSON.

O formato para dados JSON personalizados é:

```
{ "serverURL": "URL", "xm_username": "Username", "xm_password": "Password" }
```

Neste exemplo, típico do registro em massa, o Secure Hub não solicita aos usuários o endereço do servidor ou suas credenciais durante o registro:

```
{ "serverURL":"https://example.com/zdm", "xm_username":"userN", "xm_password":"password1234"}
{ "serverURL":"https://pmdm.mycorp-inc.net/zdm", "xm_username":"userN2", "xm_password":"password7890"}
```

Neste exemplo, típico para dispositivos baseados em quiosques, o Secure Hub solicita aos usuários suas credenciais:

```
{ "serverURL":"https://example.com/zdm"}
```

Você também pode inserir o JSON personalizado para o registro zero-touch do Android Enterprise.

```
1      {
2
3          "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
4          {
5
6              "serverURL":"URL", "xm_username":"username", "xm_password":"password"
7          }
8
9      }
10
11 <!--NeedCopy-->
```

Quando um dispositivo inicia o registro, ele baixa o Secure Hub do URL fornecido, instala o Secure Hub e abre o Secure Hub.

Configuração adicional

Consulte as seguintes páginas de documentação da Samsung para obter mais informações sobre a configuração:

- [Device configuration](#): Adicionar dispositivos em massa.
- [Samsung Knox Deployment App](#): registrar dispositivos através de registro Bluetooth, NFC ou Wi-Fi Direct.
- [Knox Mobile Enrollment](#): explorar a documentação da Samsung para obter mais informações sobre o Samsung Knox.

Para registrar dispositivos que executam uma versão anterior à Knox API 2.4

Em dispositivos que tenham a API Knox anterior à versão 2.4, o registro em massa não é iniciado durante a configuração inicial do dispositivo. Portanto, os usuários devem iniciar o registro. Para fazer isso, os usuários acessam um site da Samsung para baixar o novo cliente do Mobile Enrollment e iniciar o registro.

O registro de cliente baixado usa o mesmo perfil MDM e APKs configurados no portal Knox Bulk Enrollment para os dispositivos Knox 2.4/2.4.1.

Normalmente, os usuários devem seguir essas etapas:

1. Ative o dispositivo e conecte-se a uma rede Wi-Fi. Se o registro móvel não iniciar ou o Wi-Fi não está disponível, faça o seguinte:
 - a) Acesse [Samsung Knox Mobile Enrollment](#).
 - b) Toque no botão **Next** para registrar dispositivos nos dados móveis.
2. Quando for exibido o aviso **Enroll with Knox**, toque em **Continue**.
3. Leia as EULAs (se disponíveis). Toque em **Next**.
4. Se solicitado, digite **User ID** e **Password** fornecidos pelo administrador de TI.

Neste ponto, as credenciais do usuário são validadas e seu dispositivo é registrado no ambiente de TI empresarial da sua organização.

Ativar e desativar autenticação biométrica dos dispositivos Samsung

O XenMobile oferece suporte à autenticação por impressão digital e por varredura de íris, também conhecida como autenticação biométrica. Você pode ativar e desativar a autenticação biométrica para dispositivos Samsung sem exigir nenhuma ação dos usuários. Se você desabilitar a autenticação biométrica no XenMobile, os usuários e aplicativos de terceiros não poderão ativar o recurso.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.
2. Clique em **Adicionar**. É exibida a página **Adicionar uma nova política**.
3. Clique em **Código secreto**. É exibida a página de **Informações sobre a política de código secreto**.
4. No painel **Informações sobre a política**, insira as seguintes informações:
 - **Nome da política:** digite um nome descritivo para a política.
 - **Descrição:** opcionalmente, digite uma descrição para a política.
5. Clique em **Avançar**. A página **Plataformas** é exibida.
6. Em **Plataformas**, selecione **Android** ou **Samsung Knox**.

7. Defina **Configurar a autenticação biométrica** como **Ativada**.
8. Se você tiver selecionado **Android**, em **Samsung SAFE**, selecione **Permitir impressão digital**, **Permitir íris** ou ambas.

The screenshot shows the 'Passcode Policy' configuration page. On the left, a sidebar lists platforms: iOS, Mac OS X, Android (checked), Samsung KNOX, Android for Work, and Windows Phone. The main area is titled 'Passcode Policy' and includes a toggle for 'use same passcode across all users' (OFF). Below this are input fields for 'Changed characters', 'Number of times a character can occur', 'Alphabetic sequence length', and 'Numeric sequence length', all set to 0. There are two toggle switches: 'Allow users to make password visible' (ON) and 'Configure biometric authentication' (ON). Under the biometric toggle, there are checkboxes for 'Allow fingerprint' (unchecked) and 'Allow Iris' (checked). A 'Forbidden Strings' section is partially visible at the bottom.

Ações de segurança

May 6, 2021

Você pode executar ações de segurança em um dispositivo e aplicativo na página **Gerenciar > Dispositivos**. Ações do dispositivo incluem revogar, bloqueio, desbloqueio e apagar. Ações de segurança de aplicativo incluem o bloqueio de aplicativo e apagamento de aplicativos.

- **Ignorar bloqueio de ativação:** remove o bloqueio de ativação dos dispositivos iOS supervisionados antes da ativação do dispositivo. Esse comando não requer o ID Apple pessoal ou a senha de um usuário.
- **Bloqueio de aplicativo:** nega acesso a todos os aplicativos em um dispositivo. No Android, depois de um bloqueio de aplicativo, os usuários não podem fazer login no XenMobile. No iOS, os usuários podem fazer login, mas não podem acessar nenhum aplicativo.
- **Apagamento de aplicativos:** remove a conta de usuário do Secure Hub e cancela o registro do dispositivo. Os usuários não podem se registrar novamente até que você execute a ação **Cancelar apagamento de aplicativos**.
- **Bloqueio de ativação do programa de implantação ASM:** cria um código de desvio de bloqueio de ativação para dispositivos iOS registrados no DEP Apple School Manager.
- **Limpar restrições:** em dispositivos iOS supervisionados, este comando permite que o XenMobile limpe as restrições de configurações de senha e restrições configuradas pelo usuário.
- **Ativar/desativar o Modo Perdido:** coloca um dispositivo iOS supervisionado no Modo Perdido e envia ao dispositivo uma mensagem, número de telefone e nota de rodapé para exibir. A segunda vez que você envia esse comando tira o dispositivo do Modo Perdido.

- **Ativar rastreamento:** em dispositivos Android ou iOS, este comando permite que o XenMobile faça a sondagem de localização de dispositivos específicos em uma frequência definida por você. Para exibir as coordenadas do dispositivo e sua localização no mapa, vá para **Gerenciar > Dispositivos**, selecione um dispositivo e clique em **Editar**. As informações do dispositivo estão na guia **Geral** em **Segurança**. Use **Ativar rastreamento** para rastrear o dispositivo continuamente. O Secure Hub informa a localização periodicamente quando o dispositivo está em uso.
- **Apagamento completo:** apaga imediatamente todos os dados e aplicativos de um dispositivo, inclusive de qualquer cartão de memória.
 - Para dispositivos Android, esta solicitação também pode incluir a opção de apagar os cartões de memória.
 - Para dispositivos Android Enterprise totalmente gerenciados com um perfil de trabalho (dispositivos COPE), você pode executar um apagamento completo após uma apagamento seletivo para remover o perfil de trabalho.
 - Para dispositivos iOS e macOS, o apagamento ocorre imediatamente, mesmo que o dispositivo esteja bloqueado. Para dispositivos iOS 11 (versão mínima): quando você confirmar o apagamento completo, poderá optar por preservar o plano de dados celulares no dispositivo.
 - Para dispositivos Windows Phone, um apagamento completo remove todas as informações do XenMobile e todos os dados do usuário. Esses dados incluem conteúdo pessoal, como aplicativos, e-mails, contatos e mídia.
 - Para dispositivos Windows Mobile que estão executando o Windows Mobile 6 ou versões anteriores, após o apagamento, pode ser necessário enviar o dispositivo de volta para o fabricante para recarregar o sistema operacional, o software ou ambos.
 - Se o usuário do dispositivo desligar o dispositivo antes do conteúdo do cartão de memória ser excluído, o usuário ainda poderá ter acesso aos dados do dispositivo.
 - Você pode cancelar a solicitação de apagamento até que a solicitação seja enviada para o dispositivo.
- **Localizar:** localiza um dispositivo e relata a localização do dispositivo, incluindo um mapa, na página **Gerenciar > Dispositivos**, em **Detalhes do dispositivo > Geral**. Localizar é uma ação única. Use **Localizar** para exibir a localização do dispositivo atual no momento em que você executar a ação. Para rastrear continuamente o dispositivo durante um período, use **Ativar rastreamento**.
 - Ao aplicar essa ação a dispositivos Android (exceto Android Enterprise) ou a dispositivos Android Enterprise (propriedade da empresa ou BYOD), esteja ciente do seguinte comportamento:

- * **Localizar** requer que o usuário conceda permissão de localização durante o registro. O usuário pode decidir por não conceder permissão de localização. Se o usuário não conceder a permissão durante o registro, o XenMobile solicita permissão de localização novamente quando enviar o comando **Localizar**.
- Ao aplicar esse recurso a dispositivos iOS ou Android Enterprise, esteja ciente das seguintes limitações:
 - * Nos dispositivos Android Enterprise esta solicitação falha, a menos que [Política de dispositivo de localização](#) tenha definido o modo de localização do dispositivo como **Alta precisão** ou **Economia de bateria**.
 - * Para dispositivos iOS, este comando só terá êxito se os dispositivos estiverem no Modo MDM Perdido.
- **Bloquear:** bloqueia remotamente um dispositivo. Essa ação é útil quando você perde um dispositivo e não sabe se o dispositivo foi roubado. O XenMobile gera um código PIN e o configura no dispositivo. Para acessar o dispositivo, o usuário digita o código PIN. Use **Cancelar bloqueio** para remover o bloqueio do console XenMobile
- **Bloquear e redefinir senha:** bloqueia remotamente um dispositivo e redefine o código secreto.
 - Não há suporte para dispositivos registrados no Android Enterprise no modo de perfil de trabalho que executam versões do Android anteriores ao Android 8.0.
 - Em dispositivos registrados no Android Enterprise no modo de perfil de trabalho que estejam executando o Android 8.0 ou superior:
 - * O código secreto enviado bloqueia o perfil de trabalho. O dispositivo não é bloqueado.
 - * Se não for enviado um código secreto, ou se o código secreto enviado não atender aos requisitos de código secreto, e não houver um código secreto já definido no perfil de trabalho, o dispositivo será bloqueado.
 - * Se não for enviado um código secreto, ou se o código secreto enviado não atender aos requisitos de código secreto, mas houver um código secreto já definido no perfil de trabalho, o perfil de trabalho será bloqueado, mas o dispositivo não será bloqueado.
- **Notificar (toque):** emite um som em dispositivos Android.
- **Reinicializar:** reinicia os dispositivos Windows 10. Em Windows Tablet e PCs, a mensagem “Sistema reinicializará em breve” aparece e a reinicialização ocorre em cinco minutos. No Windows Phone, a reinicialização ocorre após alguns poucos minutos, sem mensagem de aviso para os usuários.
- **Solicitar/Parar espelhamento de AirPlay:** inicia e interrompe o espelhamento do AirPlay em dispositivos iOS supervisionados.
- **Reiniciar/Desligar:** reinicia imediatamente ou encerra os dispositivos iOS supervisionados.

- **Revogar:** proíbe um dispositivo de se conectar ao XenMobile Server.
- **Revogar/Autorizar (iOS, macOS):** executa as mesmas ações que um apagamento seletivo. Depois de revogação, você pode reautorizar um dispositivo para registrá-lo novamente.
- **Tocar:** se o dispositivo estiver no Modo Perdido, Tocar emite um som em um dispositivo iOS supervisionado. O som toca até que você retire o dispositivo do Modo Perdido ou o usuário desative o som.
- **Apagamento seletivo:** apaga todos os dados e aplicativos corporativos de um dispositivo, deixando dados pessoais e aplicativos no local. Depois de um apagamento seletivo, um usuário pode registrar novamente o dispositivo.
 - Apagar seletivamente um dispositivo Android não desconecta o dispositivo do Device Manager nem da rede corporativa. Para impedir que o dispositivo acesse o Device Manager, você também precisa revogar os certificados do dispositivo.
 - O apagamento seletivo de um dispositivo Android também revoga o dispositivo. Você pode registrar novamente o dispositivo somente depois de reautorizá-lo ou excluí-lo do console.
 - Para dispositivos Android Enterprise totalmente gerenciados com um perfil de trabalho (dispositivos COPE), você pode executar um apagamento completo após um apagamento seletivo para remover o perfil de trabalho. Ou, você pode registrar novamente o dispositivo com o mesmo nome de usuário. Registrar novamente o dispositivo recria o perfil de trabalho.
 - Se a API do Samsung Knox estiver habilitada, apagar seletivamente o dispositivo também remove o contêiner Samsung Knox.
 - Para dispositivos iOS e macOS, esse comando remove qualquer perfil instalado por meio do MDM.
 - Um apagamento seletivo em um dispositivo Windows também remove o conteúdo da pasta de perfil para qualquer usuário atualmente conectado. Um apagamento seletivo não remove os clipes web que você fornece para os usuários por meio de uma configuração. Para remover clipes web, os usuários manualmente cancelam o registro de seus dispositivos. Você não poderá registrar novamente um dispositivo seletivamente apagado.
 - Limpar seletivamente um dispositivo Windows Phone remove o token da empresa que permite que o XenMobile instale os aplicativos no dispositivo. Além disso, o apagamento remove todos os certificados do XenMobile e as configurações implantadas no dispositivo. Você não poderá registrar novamente um dispositivo Windows Phone seletivamente apagado.
- **Desbloquear:** libera o código secreto enviado para o dispositivo quando ele foi bloqueado. Este comando não desbloqueia o dispositivo.

Em **Gerenciar > Dispositivos**, a **página de detalhes** do dispositivo também lista as propriedades de segurança do dispositivo. Essas propriedades incluem ID forte, Bloquear dispositivo, Ignorar blo-

queio de ativação e outras informações para o tipo de plataforma. O campo de **apagamento completo do dispositivo** inclui o código PIN do usuário. O usuário deve digitar o código depois que o dispositivo for apagado. Se o usuário esquecer o código, você pode procurá-lo aqui.

Ações de segurança para dispositivos Android

Ação de segurança	Android (exceto para dispositivos Android Enterprise)	Android Enterprise (BYOD)	Android Enterprise (propriedade corporativa)
Bloqueio de aplicativo	Sim	Não	Não
Apagamento de aplicativos	Sim	Não	Não
Apagamento completo	Sim	Não	Sim
Localizar	Sim: para dispositivos com Android 6.0+, Locate requer que o usuário dê a permissão de localização durante o registro. O usuário pode optar por não conceder permissão de localização. Se o usuário não conceder a permissão durante o registro, o XenMobile solicita permissão de localização novamente quando enviar o comando Locate.	Sim: para dispositivos com Android 6.0+, Locate requer que o usuário dê a permissão de localização durante o registro. O usuário pode optar por não conceder permissão de localização. Se o usuário não conceder a permissão durante o registro, o XenMobile solicita permissão de localização novamente quando enviar o comando Locate.	Sim: para dispositivos com Android 6.0+, Locate requer que o usuário dê a permissão de localização durante o registro. O usuário pode optar por não conceder permissão de localização. Se o usuário não conceder a permissão durante o registro, o XenMobile solicita permissão de localização novamente quando enviar o comando Locate.
Bloquear	Sim	Sim	Sim
Bloquear e redefinir senha	Sim	Não	Sim

Ação de segurança	Android (exceto para dispositivos Android Enterprise)	Android Enterprise (BYOD)	Android Enterprise (propriedade corporativa)
Notificar (Tocar)	Sim	Sim	Sim
Revogar	Sim	Sim	Sim
Apagamento seletivo	Sim	Sim	Não

Ações de segurança para dispositivos iOS e macOS

Ação de segurança	iOS	macOS
Ignorar bloqueio de ativação	Sim	Não
Bloqueio de aplicativo	Sim	Não
Apagamento de aplicativos	Sim	Não
Bloqueio de ativação do programa de implantação ASM	Sim	Não
Limpar restrições	Sim	Não
Ativar/Desativar o Modo Perdido	Sim	Não
Ativar/Desativar rastreamento	Sim	Não
Apagamento completo	Sim	Sim
Localizar	Sim	Não
Bloquear	Sim	Sim
Anel	Sim	Sim
Solicitar/Parar espelhamento de AirPlay	Sim	Não
Reiniciar/Desligar	Sim	Não
Revogar/Autorizar	Sim	Sim
Apagamento seletivo	Sim	Sim
Desbloquear	Sim	Não

Ações de segurança para dispositivos Windows

Ação de segurança	Windows Phone 10	Windows Tablet 10	Windows Phone 8.1
Localizar	Sim	Sim	Não
Bloquear	Sim	Sim	Sim
Bloquear e redefinir senha	Sim	Não	Sim
Reinicializar	Sim	Sim	Não
Revogar	Sim	Sim	Sim
Anel	Sim	Não	Sim
Apagamento seletivo	Sim	Sim	Sim
Apagar	Sim	Sim	Sim

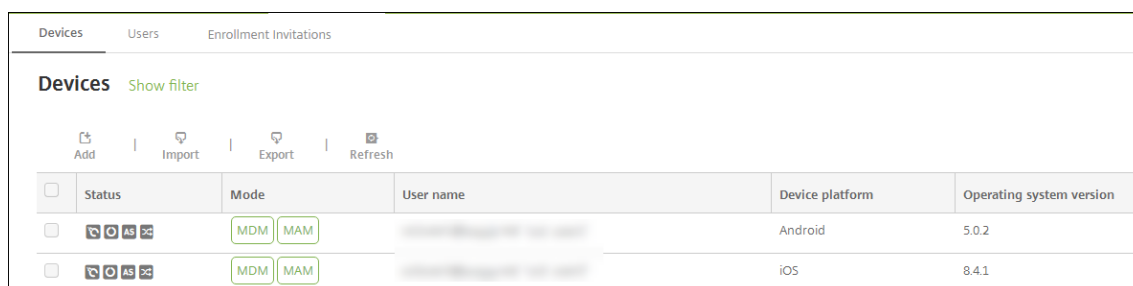
O restante deste artigo fornece as etapas para executar várias ações de segurança. Você também pode automatizar algumas ações. Para obter mais informações, consulte [Ações automatizadas](#).

Bloquear dispositivos iOS

Você pode bloquear um dispositivo iOS perdido com uma exibição de acompanhamento de uma mensagem e um número de telefone que aparecem na tela de bloqueio do dispositivo. Esse recurso tem suporte em dispositivos que executam o iOS 7 e versões posteriores.

Para exibir uma mensagem e o número de telefone em um dispositivo bloqueado, defina a política de [Código secreto](#) como **true** no console XenMobile. Como alternativa, os usuários podem ativar o código secreto no dispositivo manualmente.

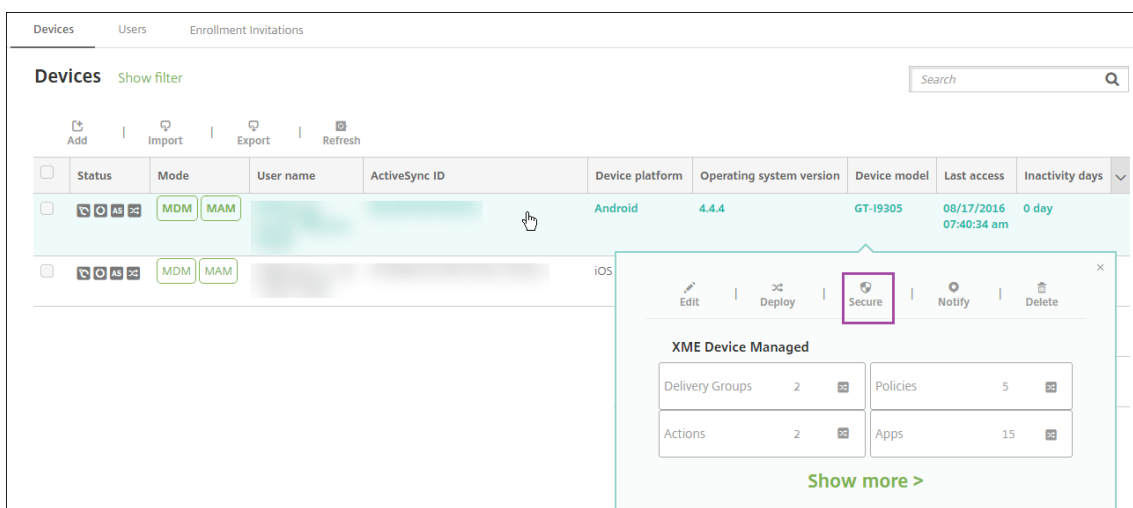
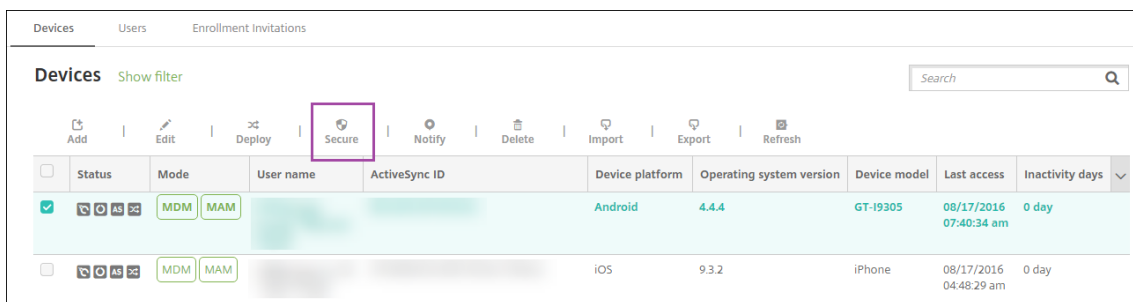
1. Clique em **Gerenciar > Dispositivos**. A página **Dispositivos** é exibida.



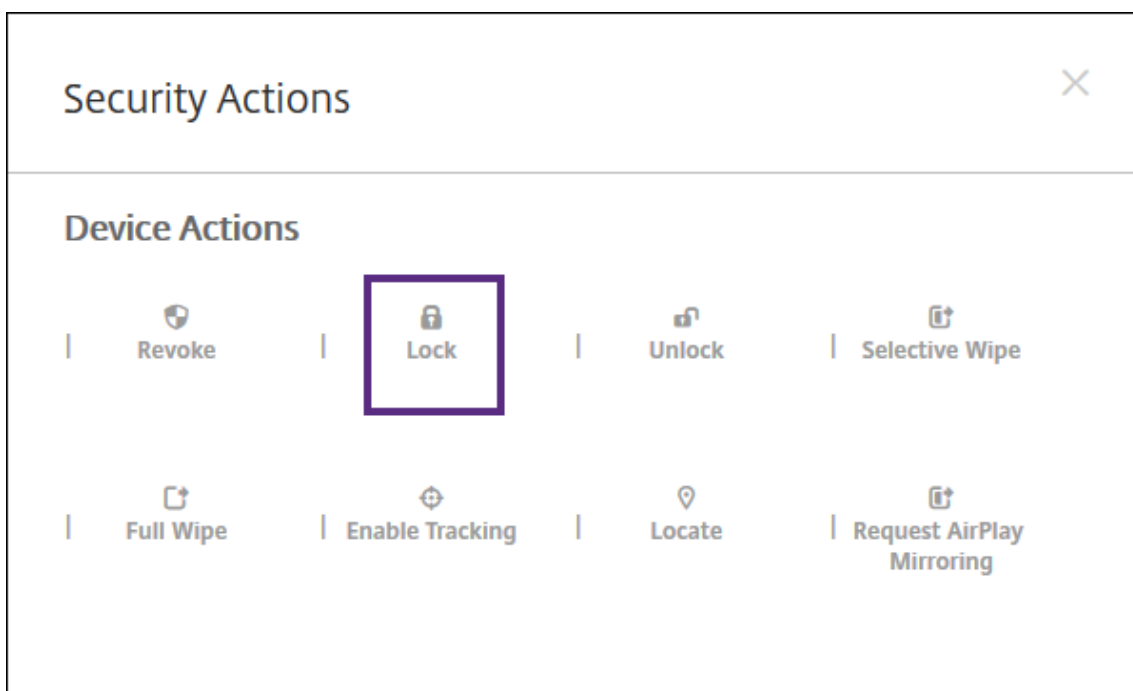
2. Selecione o dispositivo iOS que você deseja bloquear.

Quando você marca a caixa de seleção ao lado de um dispositivo, o menu de opções é exibido acima da lista de dispositivos. Quando você clica em qualquer outro lugar da lista, o menu de

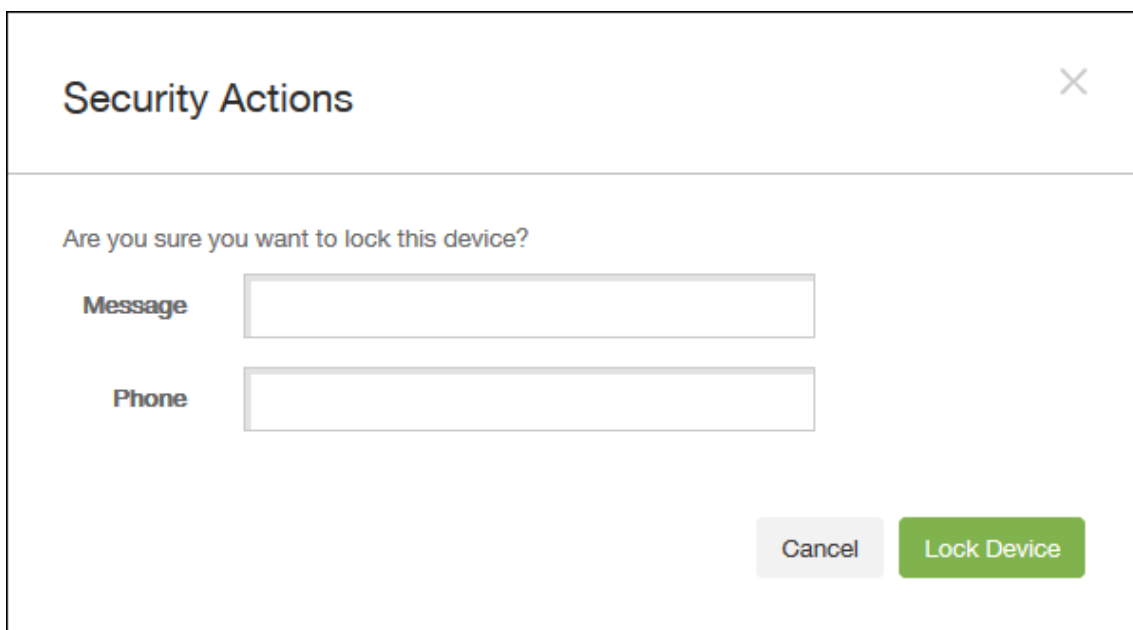
opções é exibido no lado direito da listagem.



3. No menu de opções, clique em **Segurança**. A caixa de diálogo **Ações de Segurança** é exibida.



4. Clique em **Bloquear**. A caixa de diálogo de confirmação **Ações de segurança** é exibida.



5. Opcionalmente, digite uma mensagem e um número de telefone que aparecerão na tela de bloqueio do dispositivo.

Para iPads com iOS 7 e versões posteriores: o iOS acrescenta as palavras “iPad perdido” ao conteúdo digitado na caixa **Mensagem**.

Para iPhones que executam o iOS 7 e versões posteriores: se você deixar o campo **Mensagem** vazio e fornecer um número de telefone, a Apple exibirá a mensagem “Ligar para o proprietário” na tela de bloqueio do dispositivo.



6. Clique em **Bloquear Dispositivo**.

Remover um dispositivo do console XenMobile

Importante:

Quando você remove um dispositivo do console XenMobile, aplicativos gerenciados e dados permanecem no dispositivo. Para remover os aplicativos gerenciados e os dados do dispositivo, consulte “Excluir um dispositivo” neste artigo.

Para remover um dispositivo do console XenMobile, vá até **Gerenciar > Dispositivos**, selecione o dispositivo gerenciado e, em seguida, clique em **Excluir**.

Status	Mode	User name	Serial number	Device platform	Operating system version	Device model	Inactivity days	Available storage space	Device name	XenMobile agent version
 	MDM MAM			Android	5.1.1	SM-T900	0 day	13.05 GB	Android(0)	10.6.0

Apagar dispositivo seletivamente


1. Acesse **Gerenciar > Dispositivos**, selecione um dispositivo gerenciado e clique em **Segurança**.
2. Em **Ações de segurança**, clique em **Apagamento seletivo**.
3. Somente para dispositivos Android, desconecte o dispositivo da rede corporativa: depois que o dispositivo for apagado, em **Ações de segurança**, clique em **Revogar**.

Para retirar uma solicitação de apagamento seletivo antes do apagamento ocorrer, em **Ações de segurança**, clique em **Cancelar apagamento seletivo**.

Excluir um dispositivo

Este procedimento remove aplicativos gerenciados e dados do dispositivo e exclui o dispositivo da lista Dispositivos no console XenMobile. Você pode usar a API REST Pública do Endpoint Management para excluir dispositivos em massa.

1. Acesse **Gerenciar > Dispositivos**, selecione um dispositivo gerenciado e clique em **Segurança**.
2. Clique em **Apagamento seletivo**. Quando solicitado, clique em **Executar apagamento seletivo**.
3. Para verificar se o comando de apagamento foi bem-sucedido, atualize **Gerenciar > Dispositivos**. Na coluna **Modo**, a cor âmbar para MDM e MAM indica que o comando de apagamento foi bem-sucedido.



Status	Mode	User name	Serial number	Device platform	Operating system version	Device model	Inactivity days	Available storage space	Device name	XenMobile agent version
	MDM MAM			Android	5.1.1	SM-T900	0 day	13.05 GB	Android(0)	10.6.0

4. Em **Gerenciar > Dispositivos**, selecione o dispositivo e, em seguida, clique em **Excluir**. Quando solicitado, clique em **Excluir** novamente.

Bloquear, desbloquear, apagar ou cancelar apagamento de aplicativos

1. Acesse **Gerenciar > Dispositivos**, selecione um dispositivo gerenciado e clique em **Segurança**.
2. Em **Ações de segurança**, clique na ação do aplicativo.

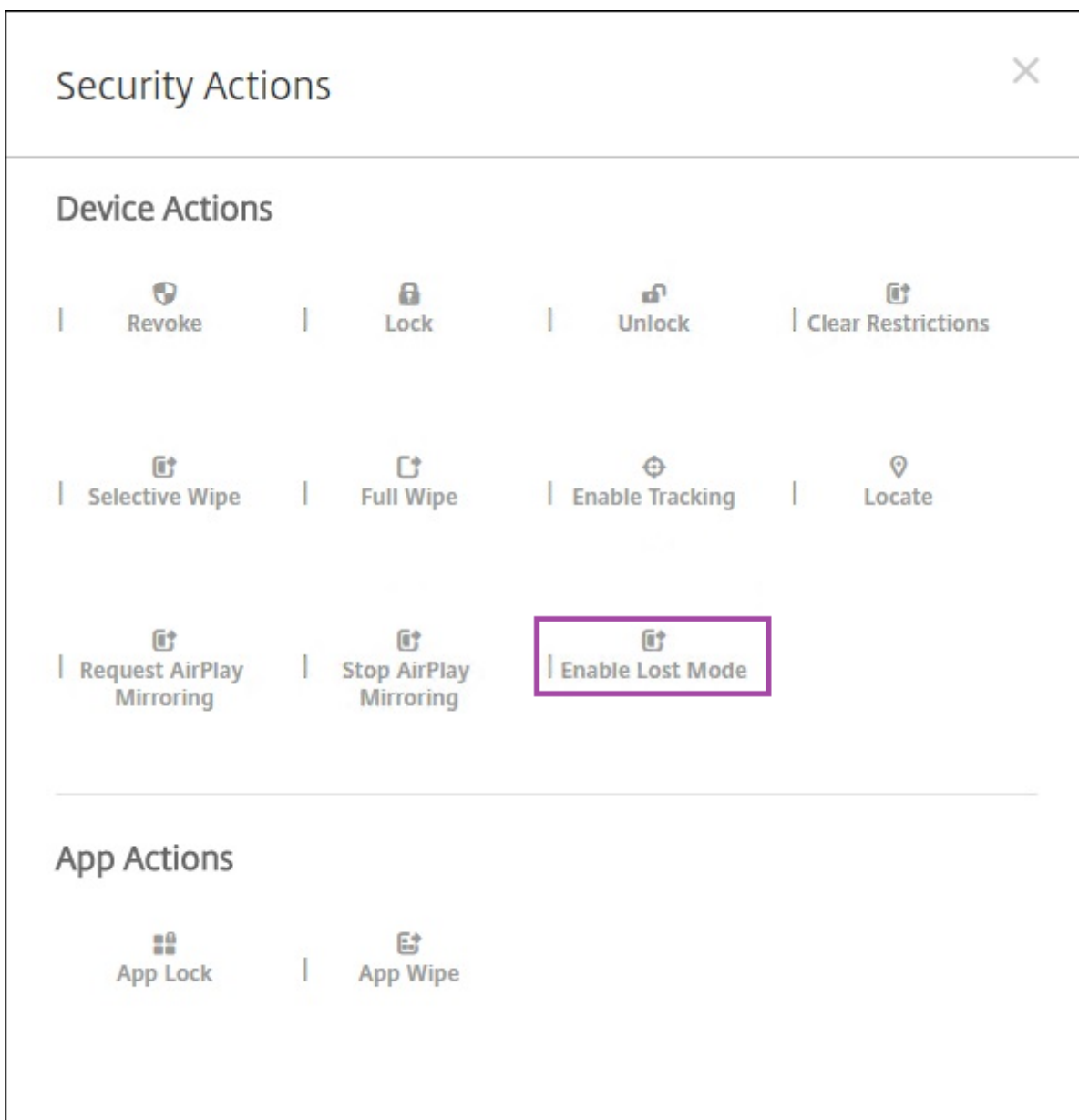
Você também pode usar a caixa **Ações de segurança** para verificar o status de um dispositivo para um usuário cuja conta está desabilitada ou foi excluída do Active Directory. A presença das ações Desbloqueio de aplicativo ou Cancelar apagamento de aplicativos indica que os aplicativos estão atualmente bloqueados ou apagados.

Colocar dispositivos iOS no Modo Perdido

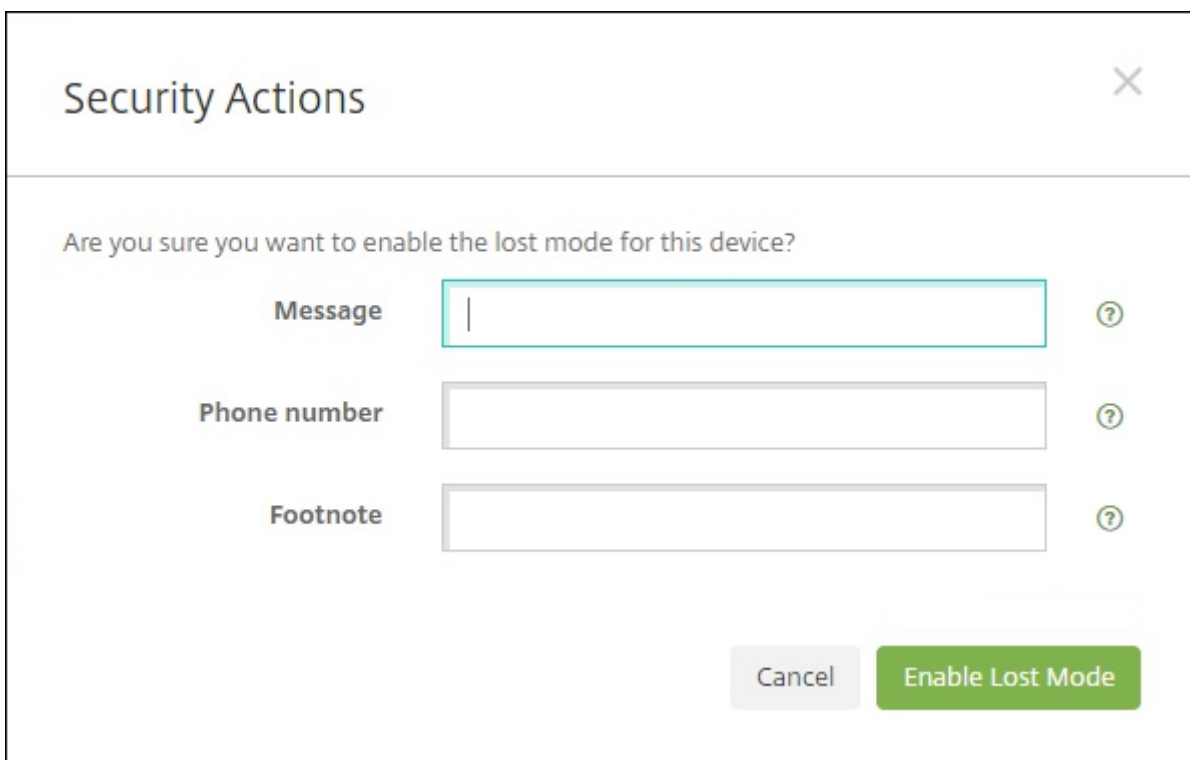
A propriedade de dispositivo Modo Perdido do XenMobile coloca um dispositivo iOS no Modo Perdido. Ao contrário do Modo perdido gerenciado da Apple, o Modo perdido do XenMobile não requer que um usuário realize nenhuma destas duas ações para ativar a localização de seu dispositivo: definir a configuração **Buscar iPhone/iPad** ou ativar os Serviços de localização para o Citrix Secure Hub.

No Modo perdido do XenMobile, somente o XenMobile Server pode desbloquear o dispositivo. (Em contraste, se você usar o recurso de bloqueio de dispositivo do XenMobile, os usuários podem desbloquear o dispositivo diretamente usando um código PIN fornecido por você.)

Para ativar ou desativar o Modo perdido: vá para **Gerenciar > Dispositivos**, escolha um dispositivo iOS supervisionado e clique em **Segurança**. Em seguida, clique em **Ativar modo perdido** ou **Desativar modo perdido**.

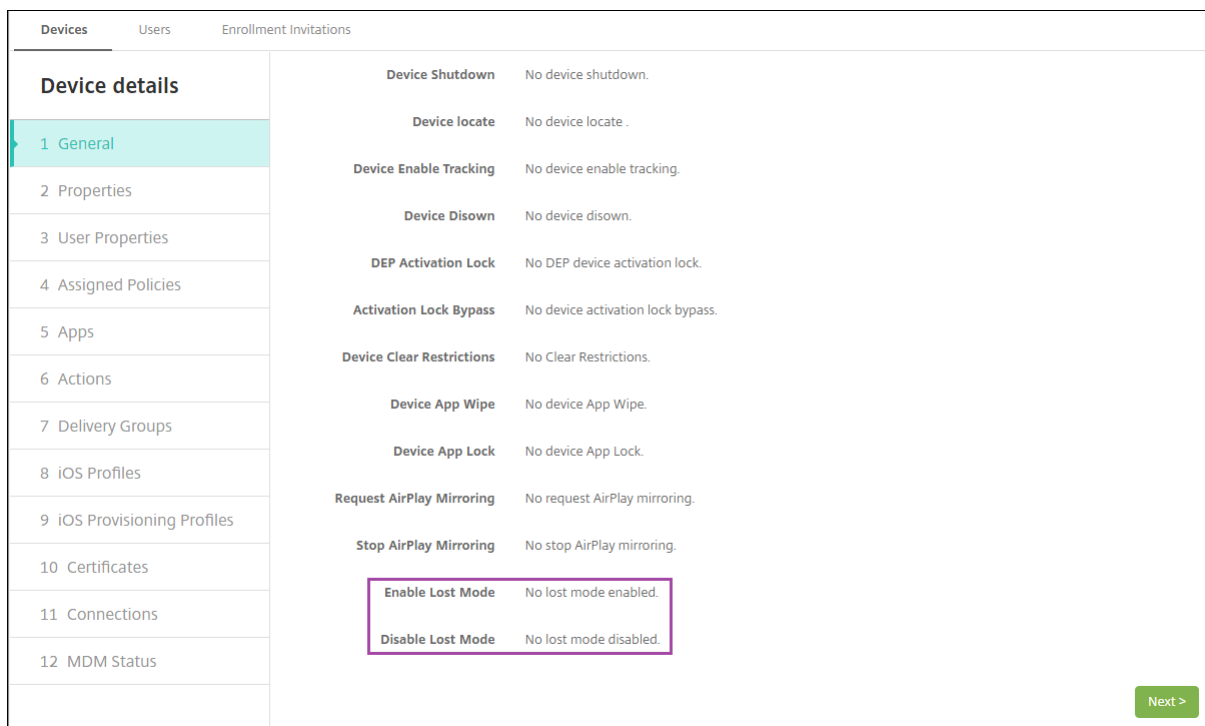


Se você clicar em **Ativar Modo Perdido**, digite informações para aparecer no dispositivo quando estiver no modo perdido.



Use qualquer um dos seguintes métodos para verificar o status do Modo perdido:

- Na janela **Ações de segurança**, verifique se o botão é **Desativar modo perdido**.
- Em **Gerenciar > Dispositivos**, na guia **Geral**, em **Segurança**, veja a última ação Ativar modo perdido ou Desativar modo perdido.



Device details	Setting	Status
1 General	Device Shutdown	No device shutdown.
2 Properties	Device locate	No device locate.
3 User Properties	Device Enable Tracking	No device enable tracking.
4 Assigned Policies	Device Disown	No device disown.
5 Apps	DEP Activation Lock	No DEP device activation lock.
6 Actions	Activation Lock Bypass	No device activation lock bypass.
7 Delivery Groups	Device Clear Restrictions	No Clear Restrictions.
8 iOS Profiles	Device App Wipe	No device App Wipe.
9 iOS Provisioning Profiles	Device App Lock	No device App Lock.
10 Certificates	Request AirPlay Mirroring	No request AirPlay mirroring.
11 Connections	Stop AirPlay Mirroring	No stop AirPlay mirroring.
12 MDM Status	Enable Lost Mode	No lost mode enabled.
	Disable Lost Mode	No lost mode disabled.

- Em **Gerenciar > Dispositivos**, na guia **Propriedades**, confirme que o valor da configuração de **Modo perdido de MDM ativado** esteja correta.

Devices	Users	Enrollment Invitations
Device details		
1 General	Activation lock enabled	No
2 Properties	Hardware encryption capabilities	Block and file levels encryption
3 User Properties	Internal storage encrypted	No
4 Assigned Policies	Jailbroken/Rooted	No
5 Apps	MDM lost mode enabled	No
6 Actions	Passcode compliant	Yes
7 Delivery Groups	Passcode compliant with configuration	Yes
8 iOS Profiles	Passcode present	No
9 iOS Provisioning Profiles	Supervised	No
10 Certificates	- Storage space Add	
11 Connections	Available storage space	10.92 GB
12 MDM Status	Total storage space	12.28 GB ×
	- System information Add	
	Active iTunes account	Yes
	Cloud backup enabled	No
		Back Next >

Se você ativar o Modo perdido do XenMobile em um dispositivo iOS, o console XenMobile também mudará, da seguinte maneira:

- Em **Configurar > Ações**, a lista **Ações** não inclui estas ações automatizadas: **Revogar o dispositivo**, **Apagar seletivamente o dispositivo** e **Apagar completamente o dispositivo**.
- Em **Gerenciar > Dispositivos**, a lista **Ações de segurança** não inclui mais as ações de dispositivo **Revogar** e **Apagamento seletivo**. Você ainda pode usar uma ação de segurança para executar uma ação de **Apagamento completo**, conforme necessário.

Para iPads com iOS 7 e versões posteriores: o iOS acrescenta as palavras “iPad perdido” ao conteúdo digitado na caixa **Mensagem** na tela **Ações de segurança**.

Para iPhones com iOS 7 e versões posteriores: se você deixar a **Mensagem** vazia e fornecer um número de telefone, a Apple exibirá a mensagem “Ligar para o proprietário” na tela de bloqueio do dispositivo.

Ignorar bloqueio de ativação do iOS

Bloqueio de ativação é um recurso do Buscar iPhone/iPad que impede a reativação de um dispositivo supervisionado perdido ou roubado. O Bloqueio de Ativação requer o ID Apple e a senha do usuário para que alguém possa desativar Buscar iPhone/iPad, apagar o dispositivo ou reativar o dispositivo. Para os dispositivos de propriedade da organização, ignorar um bloqueio de ativação é necessário, por exemplo, para redefinir ou realocar dispositivos.

Para ativar o Bloqueio de Ativação, você configura e implanta a política do dispositivo de Opções XenMobile MDM. Você pode gerenciar um dispositivo a partir do console XenMobile sem as credenciais Apple do usuário. Para desviar do requisito de credenciais Apple de um bloqueio de ativação, execute a ação de segurança Ignorar Bloqueio de Ativação a partir do console XenMobile.

Por exemplo, se o usuário retorna um telefone perdido ou para configurar o dispositivo antes ou após um apagamento completo: quando o telefone pede as credenciais de conta do iTunes, você pode ignorar essa etapa emitindo a ação de segurança Ignorar Bloqueio de Ativação no console XenMobile.

Requisitos do dispositivo para o desvio de bloqueio de ativação

- iOS 7.1 (versão mínima)
- Supervisionados por meio do Apple Configurator ou Apple DEP
- Configurado com uma conta do iCloud
- Buscar iPhone/iPad ativado
- Registrado no XenMobile
- A política de dispositivo de Opções do MDM, com o bloqueio de ativação habilitado, é implantada nos dispositivos

Para ignorar um bloqueio de ativação antes de emitir um apagamento completo de um dispositivo:

1. Acesse **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Segurança** e em **Ignorar bloqueio de ativação**.
2. Apagar o dispositivo. A tela de bloqueio de ativação não aparece durante a configuração do dispositivo.

Para ignorar um bloqueio de ativação depois de emitir um apagamento completo de um dispositivo:

1. Redefinir ou apagar o dispositivo. A tela de bloqueio de ativação aparece durante a configuração do dispositivo.
2. Acesse **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Segurança** e em **Ignorar bloqueio de ativação**.
3. Toque no botão Voltar no dispositivo. É exibida a tela de início.

Tenha em mente o seguinte:

- Aconselhe seus usuários a não desativarem Buscar iPhone/iPad. Não execute um apagamento completo a partir do dispositivo. Em ambos os casos, o usuário é solicitado a digitar a senha da conta do iCloud. Após a validação da conta, o usuário não verá uma tela Ativar iPhone/iPad depois de apagar todo o conteúdo e configurações.
- Para um dispositivo com um código de desvio do bloqueio de ativação gerado e com o bloqueio de ativação ativado: se você não pode ignorar a página Ativar iPhone/iPad após um apagamento completo, não é necessário excluir o dispositivo do XenMobile. Você ou o usuário pode entrar em contato com o suporte da Apple para desbloquear o dispositivo diretamente.

- Durante um inventário de hardware, o XenMobile consulta um dispositivo para obter um código de desvio de bloqueio de Ativação. Se um código de desvio estiver disponível, o dispositivo o envia para o XenMobile. Em seguida, para remover o código de desvio do dispositivo, envie a ação de segurança Ignorar Bloqueio de Ativação a partir do console XenMobile. Nesse ponto, o XenMobile Server e a Apple têm o código de desvio necessário para desbloquear o dispositivo.
- A ação de segurança Ignorar Bloqueio de Ativação utiliza a disponibilidade de um serviço Apple. Se a ação não funcionar, você pode desbloquear um dispositivo da seguinte maneira. No dispositivo, insira manualmente as credenciais da conta do iCloud. Ou deixe o campo do nome do usuário vazio e digite o código de desvio no campo da senha. Para ver o código de desvio, vá para **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Editar** e clique em **Propriedades**. O **código de desvio do bloqueio de ativação** está em **Informações de segurança**.

Dispositivos compartilhados

November 30, 2020

O XenMobile permite configurar dispositivos que podem ser compartilhados por vários usuários. O recurso de dispositivos compartilhados permite que, por exemplo, médicos em hospitais usem qualquer dispositivo próximo para acessar aplicativos e dados, em vez de precisar transportar um dispositivo específico. Você também pode deslocar os trabalhadores em áreas como aplicação da lei, varejo e fabricação para compartilhar dispositivos para reduzir os custos com equipamentos.

Pontos principais sobre dispositivos compartilhados

Você pode usar qualquer um dos dispositivos iOS e Android compatíveis como dispositivos compartilhados. Para obter uma lista de dispositivos compatíveis, consulte [Sistemas operacionais compatíveis de dispositivos](#).

Registro MDM

- Disponível em tablets e telefones iOS e Android. Não é compatível com o registro básico do Programa de implantação da Apple para um dispositivo compartilhado do XenMobile Enterprise. Use um Programa de Implantação da Apple autorizado para registrar um dispositivo compartilhado neste modo.
- Não é compatível com autenticação de certificado de cliente, PIN da Citrix, Touch ID, entropia de usuário e autenticação de dois fatores.

Registro MDM+MAM

- Disponível apenas em dispositivos iOS e Android.
- Compatível apenas com autenticação de nome de usuário e senha do Active Directory.
- Não é compatível com autenticação de certificado de cliente, código secreto do Secure Hub, Touch ID, entropia de usuário e autenticação de dois fatores.
- Não é compatível com registro Somente MAM. Os dispositivos devem se registrar no MDM.
- Compatível apenas com Secure Mail, Secure Web e os aplicativos móveis ShareFile. Não é compatível com aplicativos HDX.
- Suporta somente usuários do Active Directory. Não oferece suporte a grupos e usuários locais.
- Para atualizar para MDM+MAM, requer um novo registro dos dispositivos compartilhados somente MDM existentes.
- Os usuários não podem compartilhar aplicativos nativos nos dispositivos.
- Depois de baixados durante o primeiro registro, os aplicativos móveis de produtividade não são baixados novamente durante o login do usuário
- No Android, para isolar os dados de cada usuário por motivos de segurança, defina a política **Não permitir dispositivos com root** no console XenMobile como **Ativada**.

Pré-requisitos para registrar dispositivos compartilhados

Antes de poder registrar dispositivos compartilhados, você deve fazer o seguinte:

- Crie uma função de usuário de registro de dispositivo compartilhado. Veja [Configuração de funções com RBAC](#).
- Crie um usuário do dispositivo compartilhado. Veja [Para adicionar, editar, desbloquear ou excluir contas de usuários](#).
- Crie um grupo de entrega que contenha as políticas, os aplicativos e as ações base que você deseja aplicar ao usuário de registro de dispositivo compartilhado. Veja [Implantar recursos](#).

Pré-requisitos para registro MDM+MAM

1. Crie um grupo do Active Directory. Dê a ele um nome descritivo, nesse caso **Shared Device Enrollers**.
2. Adicione ao grupo os usuários do Active Directory que registram dispositivos compartilhados. Se você desejar uma nova conta para esse fim, crie um novo usuário do Active Directory (por exemplo, **sdenroll**) e adicione-o ao grupo do Active Directory.

Configuração de um dispositivo compartilhado

Siga estas etapas para configurar um dispositivo compartilhado.

1. No console XenMobile, clique na engrenagem no canto superior direito. A página **Settings** é exibida.
2. Clique em **Controle de acesso baseado em função** e clique em **Adicionar**. A tela **Adicionar função** é exibida.
3. Crie uma função de usuário de registro de dispositivo compartilhado chamada **Usuário de registro de dispositivo compartilhado** com permissões de **Assistente de registro de dispositivos compartilhados** em **Acesso autorizado**. Não se esqueça de expandir **Dispositivos** nos **Recursos do console** e selecionar **Apagamento seletivo do dispositivo**. Essa configuração garante que os aplicativos e as políticas provisionadas por meio da conta do assistente de registro de dispositivos compartilhados sejam excluídos por meio do Secure Hub quando o registro do dispositivo é cancelado.

Em **Aplicar Permissões**, mantenha a configuração padrão, **Para todos os grupos de usuários**, ou atribua permissões a grupos de usuários específicos do Active Directory com **Para grupos de usuários específicos**.

Settings > Role-Based Access Control > Add Role

Add Role

- 1 Role Info
- 2 Assignment

Role Info

RBAC name*

RBAC template: Select a template [Apply]

Authorized access

- Admin console access
- Self Help Portal access
- Shared devices enroller
- Remote Support access
- Public api access

Console features

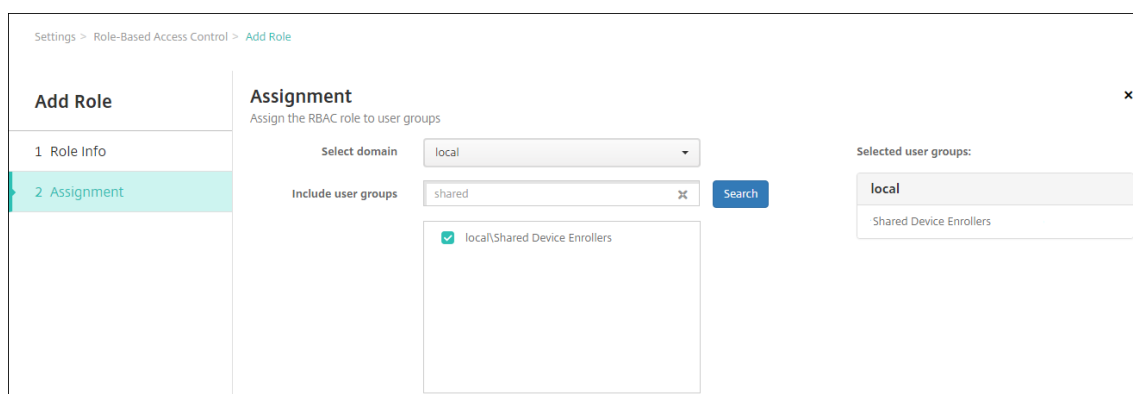
- Dashboard
- Reporting
- Devices
 - Full Wipe device
 - Clear Restriction
 - Selective Wipe device
 - View locations
 - Lock device
 - Unlock device

Apply permissions

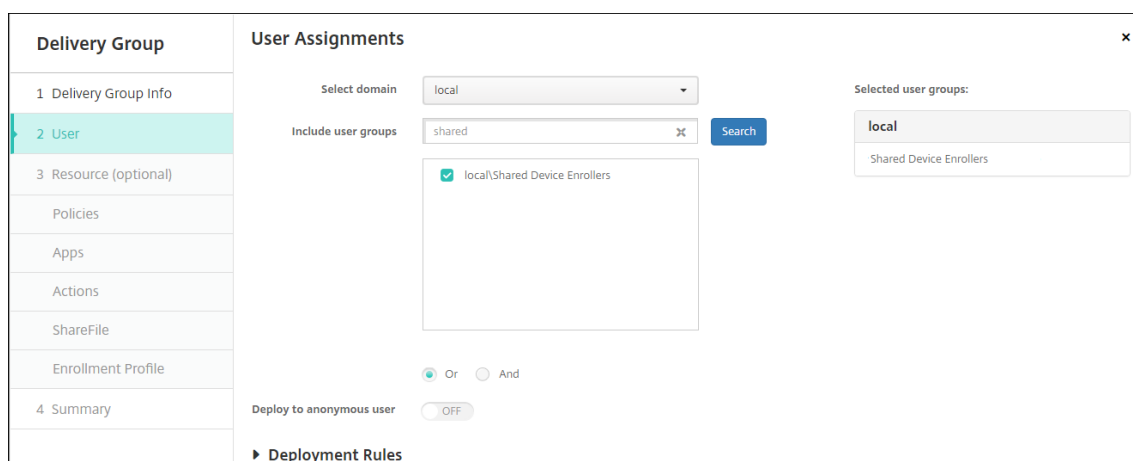
- To all user groups
- To specific user groups

Next >

Clique em **Avançar** para ir para a tela **Atribuição**. Atribua a função de registro de dispositivo compartilhado ao grupo do Active Directory para os usuários de registro de dispositivos compartilhados, criados na Etapa 1, em Pré-requisitos. Na imagem a seguir, **citrix.lab** é o domínio do Active Directory e o **Shared Device Enrollers** é o grupo do Active Directory.



4. Crie um grupo de entrega que contenha as políticas, os aplicativos e as ações base que você deseja aplicar ao dispositivo quando um usuário não estiver conectado. Em seguida, associe esse grupo de entrega ao grupo do Active Directory do usuário de registro de dispositivo compartilhado.



5. Instale o Secure Hub no dispositivo compartilhado e registre-o no XenMobile usando a conta de usuário de registro de dispositivo compartilhado. Agora você pode exibir e gerenciar o dispositivo por meio do console XenMobile. Para obter mais informações, consulte [Registrar dispositivos](#).
6. Para aplicar diferentes políticas ou fornecer mais aplicativos aos usuários autenticados, você deve criar um grupo de entrega associado a esses usuários e implantado somente em dispositivos compartilhados. Quando você criar os grupos, configure regras de implantação para garantir que os pacotes sejam implantados em dispositivos compartilhados. Para obter mais informações, consulte [Implantar recursos](#).
7. Para interromper o compartilhamento do dispositivo, realize um apagamento seletivo para remover a conta de usuário de registro de dispositivo compartilhado do dispositivo. Remova todos os aplicativos e políticas implementados no dispositivo.

Experiência do usuário de dispositivos compartilhados

Registro MDM

Os usuários veem somente os recursos disponíveis para eles e têm a mesma experiência em todos os dispositivos compartilhados. As políticas de registro e os aplicativos do dispositivo compartilhado sempre permanecem no dispositivo. Quando um usuário que não está registrado em dispositivos compartilhados faz login no Secure Hub, as políticas e os aplicativos dessa pessoa são implantados no dispositivo. Quando esse usuário se desconectar, todas as políticas e aplicativos que não fazem parte do registro do dispositivo compartilhado são removidos. Os recursos de registro de dispositivo compartilhado permanecem intactos.

Registro MDM+MAM

O Secure Mail e o Secure Web são implantados no dispositivo quando registrados pelo usuário de registro de dispositivo compartilhado. Os dados do usuário são mantidos de forma protegida no dispositivo. Os dados não são expostos para outros usuários quando eles fazem login no Secure Mail e no Secure Web.

Somente um usuário por vez pode fazer login no Secure Hub. O usuário anterior deve fazer logout antes que o próximo usuário possa fazer login. Por motivos de segurança, o Secure Hub não armazena as credenciais do usuário em dispositivos compartilhados, portanto, os usuários devem digitar as credenciais deles sempre que fizerem login. O Secure Hub bloqueia novos logins até que remova as políticas, aplicativos e dados associados ao usuário anterior.

O registro de dispositivo compartilhado não altera o processo de atualização de aplicativos. Você pode enviar por push atualizações para os usuários de dispositivo compartilhado como sempre, e os usuários de dispositivo compartilhado podem atualizar aplicativos diretamente nos dispositivos deles.

Políticas recomendadas do Secure Mail

- Para o melhor desempenho do Secure Mail, defina **Max sync period** com base no número de usuários que compartilham o dispositivo. Não é recomendável permitir a sincronização ilimitada.

Número de usuários compartilhando o dispositivo	Período máximo recomendado de sincronização
21–25	1 semana ou menos
6–20	2 semanas ou menos
5 ou menos	1 mês ou menos

- Bloqueie **Enable contact export** para evitar a exposição dos contatos de um usuário a outros usuários que compartilham o dispositivo.
- No iOS, somente as configurações a seguir podem ser definidas por usuário. Todas as outras configurações são comuns entre os usuários que compartilham o dispositivo:
 - Notificações
 - Assinatura
 - Ausência Temporária
 - Período de Sincronização de Email
 - S/MIME
 - Verificar ortografia

XenMobile AutoDiscovery Service

August 20, 2021

O serviço AutoDiscovery simplifica o processo de registro para os usuários por meio da descoberta de URL baseada em e-mail. O serviço AutoDiscovery também oferece recursos como verificação de registro, certificate pinning e outros benefícios para os clientes do Citrix Workspace. O serviço, hospedado no Citrix Cloud, é uma parte importante de muitas implantações do XenMobile.

Com o serviço AutoDiscovery, os usuários:

- Podem usar suas credenciais de rede corporativa para registrar seus dispositivos.
- Não precisam inserir detalhes sobre o endereço do XenMobile Server.
- Digitam seus nomes de usuário no formato UPN (nome principal do usuário). Por exemplo, `user@mycompany.com`.

Recomendamos que você use o serviço AutoDiscovery em ambientes de alta segurança. O serviço AutoDiscovery oferece suporte a certificate pinning de chave pública, o que evita ataques man-in-the-middle. Certificate pinning garante que o certificado assinado pela sua empresa seja usado quando os clientes Citrix se comunicam com o XenMobile. Para configurar o certificate pinning para seus sites XenMobile, entre em contato com o Suporte Citrix. Para obter informações sobre certificate pinning, consulte [Certificate pinning](#).

Para acessar o serviço AutoDiscovery, vá para <https://adsui.cloud.com> (comercial) ou <https://adsui.cem.cloud.us> (governo).

Pré-requisitos

- O novo serviço AutoDiscovery no Citrix Cloud requer a versão mais recente do Secure Hub:

- Para iOS, Secure Hub versão 21.1.0 ou posterior
- Para Android, Secure Hub versão 21.2.1 ou posterior

Dispositivos com versões anteriores do Secure Hub podem sofrer interrupções no serviço.

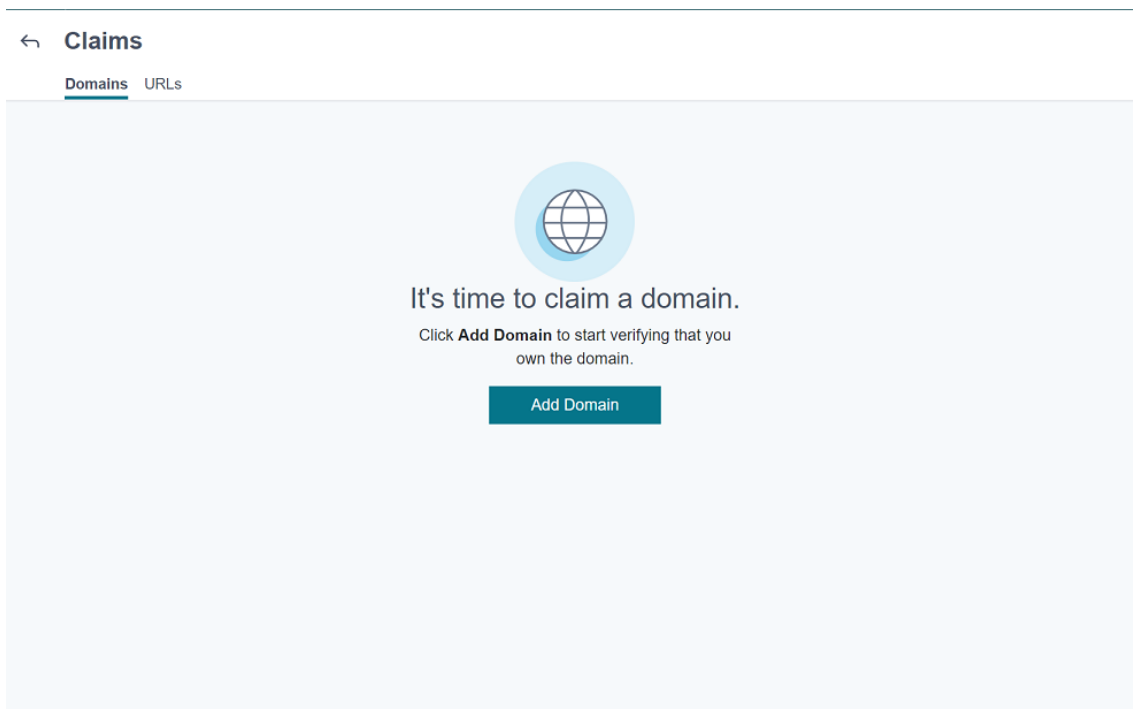
- Para acessar o novo serviço AutoDiscovery, você deve ter uma conta de administrador do Citrix Cloud com acesso completo. O serviço AutoDiscovery não suporta contas de administrador com acesso personalizado. Se você não tiver uma conta, consulte [Registrar-se no Citrix Cloud](#).

A Citrix migrou todos os registros do AutoDiscovery existentes para o Citrix Cloud sem interrupção no serviço. Os registros migrados não aparecem automaticamente no novo console. Você deve recuperar domínios no novo serviço AutoDiscovery para provar propriedade. Para obter mais informações, consulte [CTX312339](#).

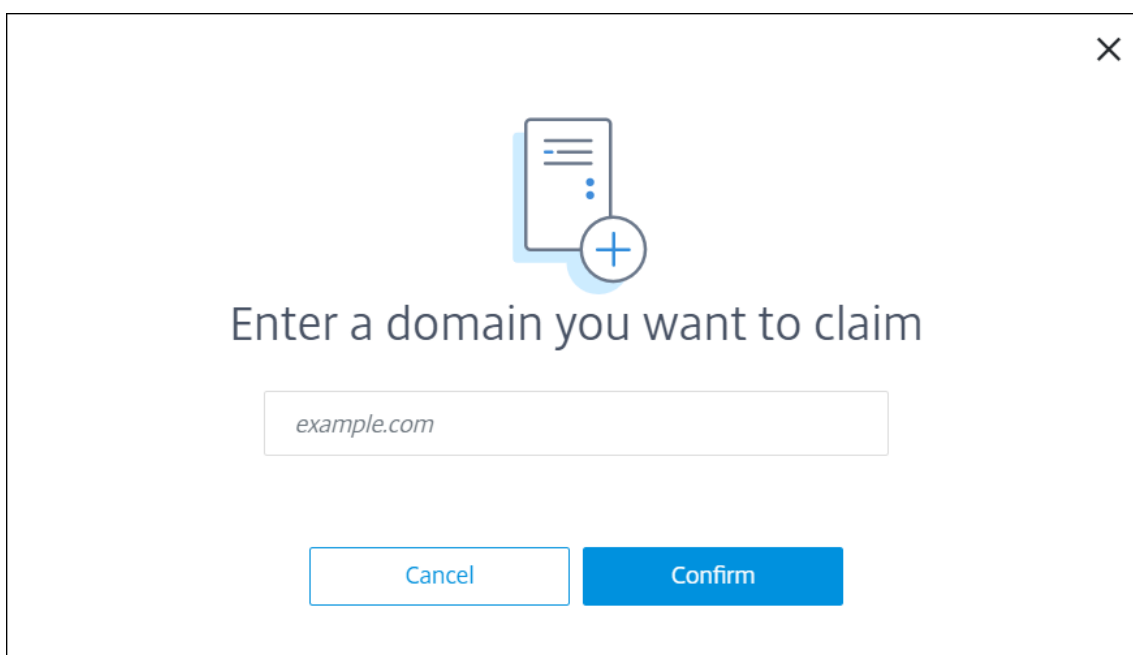
- Antes de começar a usar o serviço AutoDiscovery para suas implantações do Endpoint Management, verifique e reivindique seu domínio. Você pode reivindicar até 10 domínios. A reivindicação associa o domínio verificado ao serviço AutoDiscovery. Para reivindicar mais de 10 domínios, abra um tíquete SRE ou entre em contato com o Suporte Técnico da Citrix.
- Use a configuração da porta MAM em vez do FQDN do Citrix Gateway para direcionar o tráfego MAM para seu data center. Se você inserir um nome de domínio totalmente qualificado juntamente com a porta do seu Citrix Gateway, o dispositivo cliente usa a configuração da **Porta MAM**.
- Se um bloqueador de anúncios impedir que o site seja aberto, certifique-se de desativar o bloqueador de anúncios para todo o site.

Reivindicar um domínio

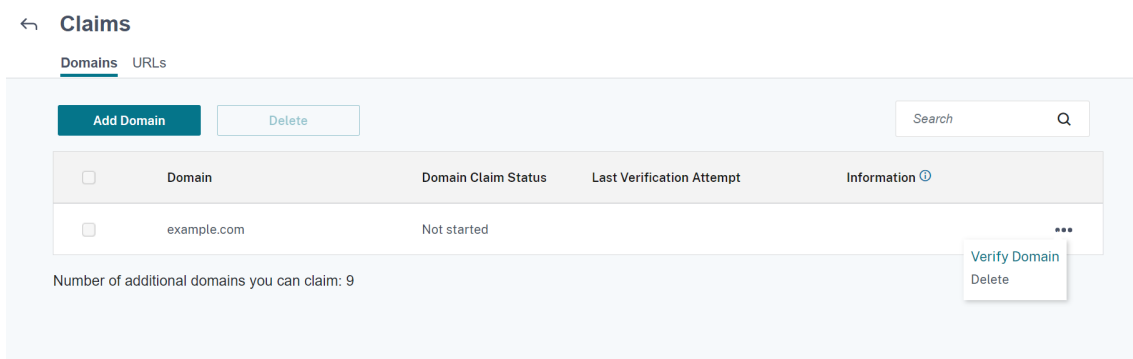
1. Na guia **Reivindicações > Domínios**, clique em **Adicionar domínio**.



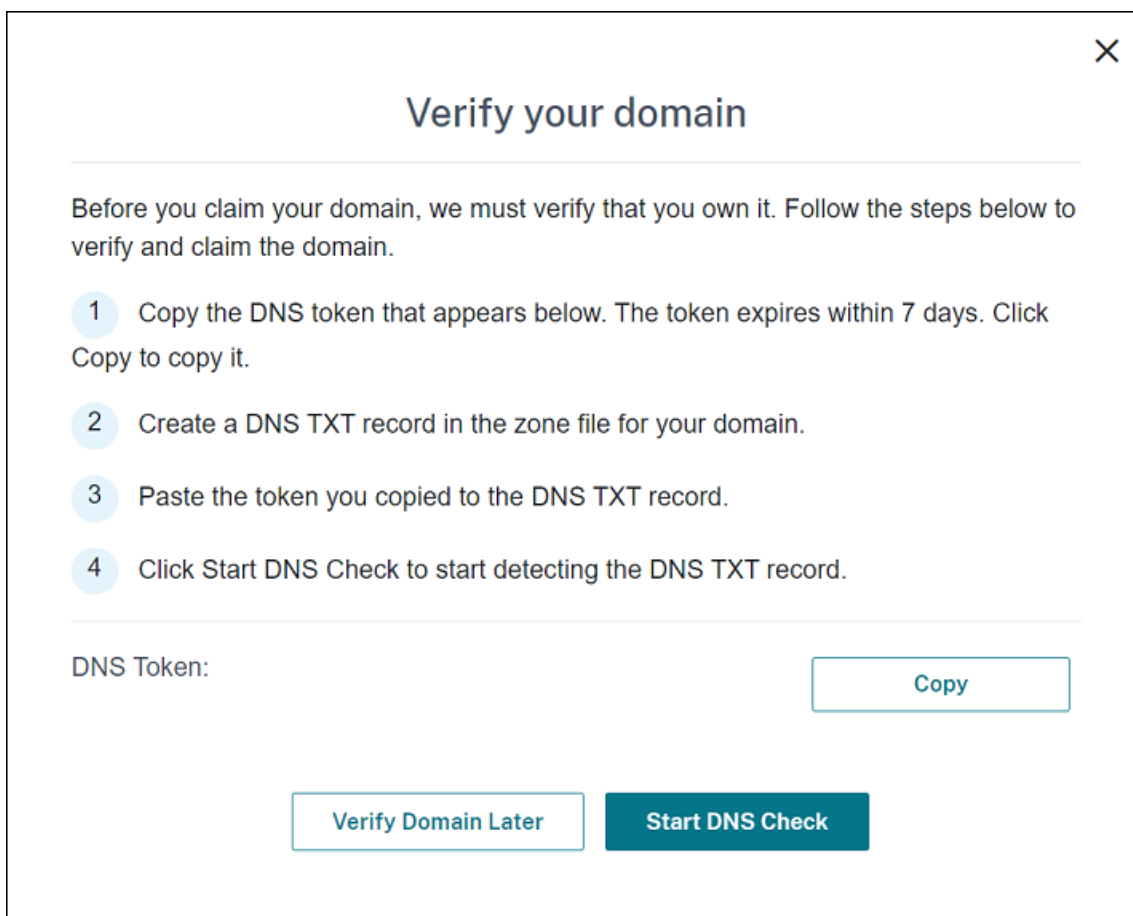
2. Na caixa de diálogo exibida, insira o nome do domínio do seu ambiente XenMobile e, em seguida, clique em **Avançar**. Seu domínio aparece em **Reivindicações > Domínios**.



3. No domínio adicionado, clique no menu de reticências e selecione **Verify Domain** para iniciar o processo de verificação. A página **Verify Domain** é exibida.

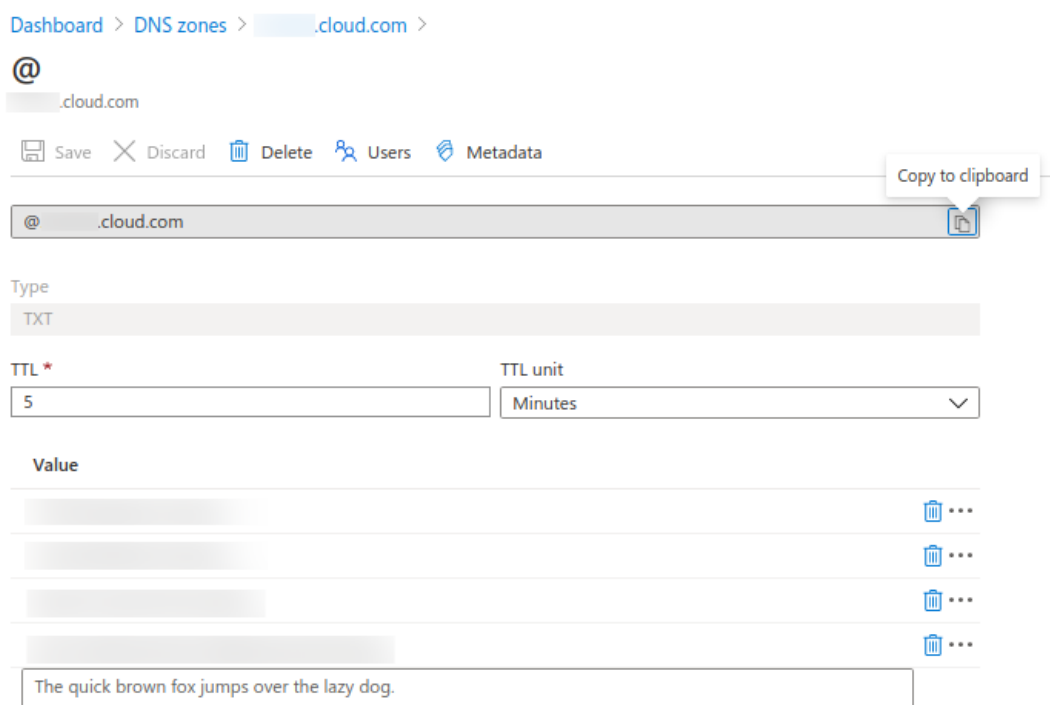


4. Na página **Verify your domain**, siga as instruções para verificar se você possui o domínio.



- Clique em **Copy** para copiar o token DNS para a área de transferência.
- Crie um registro TXT de DNS no arquivo de zona para o seu domínio. Para isso, vá para o portal do provedor de hospedagem do seu domínio e adicione o token DNS que você copiou.

A captura de tela a seguir mostra um portal de provedor de hospedagem de domínio. Seu portal pode parecer diferente.



- c) No Citrix Cloud, na página **Verify your domain**, clique em **Start DNS Check** para começar a detectar seu registro TXT de DNS. Se você quiser verificar o domínio mais tarde, clique em **Verify Domain Later**.

O processo de verificação geralmente leva cerca de uma hora. No entanto, pode demorar até dois dias para retornar uma resposta. Você pode sair e fazer login novamente durante a verificação de status.

Após a conclusão da configuração, o status do seu domínio muda de **Pending** para **Verified**.

5. Depois de reivindicar seu domínio, forneça informações sobre o serviço AutoDiscovery. Clique no menu de reticências no domínio que você adicionou e clique em **Add Endpoint Management Info**. A página **AutoDiscovery Service Information** é exibida.
6. Insira as seguintes informações e clique em **Save**.
 - **Endpoint Management Server FQDN:** insira o nome de domínio totalmente qualificado do XenMobile Server. Por exemplo: `example.xml.cloud.com`. Essa configuração é usada para o tráfego de controle MDM e MAM.
 - **Citrix Gateway FQDN:** insira o nome de domínio totalmente qualificado do Citrix Gateway, no formato FQDN ou FQDN:porta. Por exemplo: `example.com`. Essa configuração é usada para direcionar o tráfego MAM para o seu data center. Para implantações Somente MDM, deixe este campo em branco.

Nota:

A Citrix recomenda que você use a configuração da **porta MAM** em vez do **FQDN do Citrix Gateway** para controlar o tráfego MAM. Se você inserir um nome de domínio totalmente qualificado juntamente com a porta do seu Citrix Gateway, o dispositivo cliente usa a configuração da **Porta MAM**.

- **Instance Name:** insira o nome da instância do XenMobile Server que você configurou acima. Se você não tiver certeza sobre o nome da sua instância, deixe o valor padrão, **zdm**.
- **MDM Port:** insira a porta usada para o tráfego de controle do MDM e o registro MDM. Para serviços baseados em nuvem, o padrão é 443.
- **MAM Port:** insira a porta usada para o tráfego de controle do MAM, registro MAM, registro iOS e enumeração de aplicativo. Para serviços baseados em nuvem, o padrão é 8443.

Solicitar Descoberta Automática para dispositivos Windows

Se você planeja registrar dispositivos Windows, faça o seguinte:

1. Entre em contato com o Suporte Citrix e crie uma solicitação de suporte para habilitar a Descoberta Automática do Windows.
2. Obtenha um certificado SSL não curinga assinado publicamente para [enterpriseenrollment.mycompany.com](#). A parte [mycompany.com](#) é o domínio que contém as contas que os usuários usam para se registrar. Anexe o certificado SSL no formato .pfx e sua senha à solicitação de suporte criada na etapa anterior.

Para usar mais de um domínio para registrar dispositivos Windows, você também pode usar um certificado multidomínio com a seguinte estrutura:

- Um SubjectDN com um CN que especifica o domínio principal ao qual ele serve (por exemplo, [enterpriseenrollment.mycompany1.com](#)).
 - Os SANs adequados para os domínios restantes (por exemplo, [enterpriseenrollment.mycompany2.com](#), [enterpriseenrollment.mycompany3.com](#) e assim por diante).
3. Crie um nome canônico (CNAME) em seu registro DNS e mapeie o endereço de seu certificado SSL ([enterpriseenrollment.mycompany.com](#)) para [autodisc.xm.cloud.com](#).

Quando um usuário de dispositivo Windows se registra usando um UPN, o servidor de registro Citrix:

- Fornece os detalhes do seu XenMobile Server.
- Indica ao dispositivo para solicitar um certificado válido do XenMobile.

Nesse ponto, você pode registrar todos os dispositivos suportados. Prossiga para a próxima seção para se preparar para entregar recursos aos dispositivos.

Políticas de dispositivo

April 26, 2021

Você pode configurar como o XenMobile interage em seus dispositivos por meio de políticas. Apesar de muitas políticas serem comuns a todos os dispositivos, cada dispositivo tem um conjunto de políticas específicas ao seu sistema operacional. Como resultado, você poderá encontrar diferenças entre plataformas e até mesmo entre dispositivos com Android de diferentes fabricantes.

Para obter uma descrição resumida de cada política de dispositivo, consulte Resumos de políticas de dispositivo neste artigo.

Nota:

Se o seu ambiente estiver configurado com Objetos de Política de Grupo (GPOs):

Quando você configurar políticas de dispositivo do XenMobile para o Windows 10, lembre-se da regra a seguir. Se uma política em um ou mais dispositivos Windows 10 registrados for conflitante, a política alinhada ao GPO terá precedência.

Para ver a quais políticas o contêiner do Android Enterprise dá suporte, consulte [Android Enterprise](#).

Pré-requisitos

- Crie os grupos de entrega que você planeja usar.
- Instale todos os certificados AC necessários.

Adicionar uma política de dispositivo

As etapas básicas para criar uma política de dispositivo são as seguintes:

1. Nomeie e descreva a política.
2. Configure a política para uma ou mais plataformas.
3. Crie regras de implantação (opcional).
4. Atribua a política a grupos de entrega.
5. Configure o cronograma de implantação (opcional).

Para criar e gerenciar políticas de dispositivos, acesse **Configurar > Políticas de dispositivo**.

<input type="checkbox"/>	Policy name	Type	Created on	Last updated on	Status
<input type="checkbox"/>	K--Scheduling	Scheduling	8/12/17 6:43 AM	8/12/17 6:43 AM	
<input type="checkbox"/>	K--AppInv	Software Inventory	8/12/17 6:45 AM	8/12/17 6:45 AM	
<input type="checkbox"/>	K--Webclip	Mdm Weblink	8/12/17 6:46 AM	8/12/17 6:46 AM	
<input type="checkbox"/>	K--Passcode	Password	8/12/17 6:47 AM	8/12/17 6:47 AM	
<input type="checkbox"/>	K--Wifi	Wifi	8/12/17 6:47 AM	8/12/17 6:47 AM	
<input type="checkbox"/>	K--T&C	Terms Conditions	8/12/17 6:48 AM	8/12/17 6:48 AM	

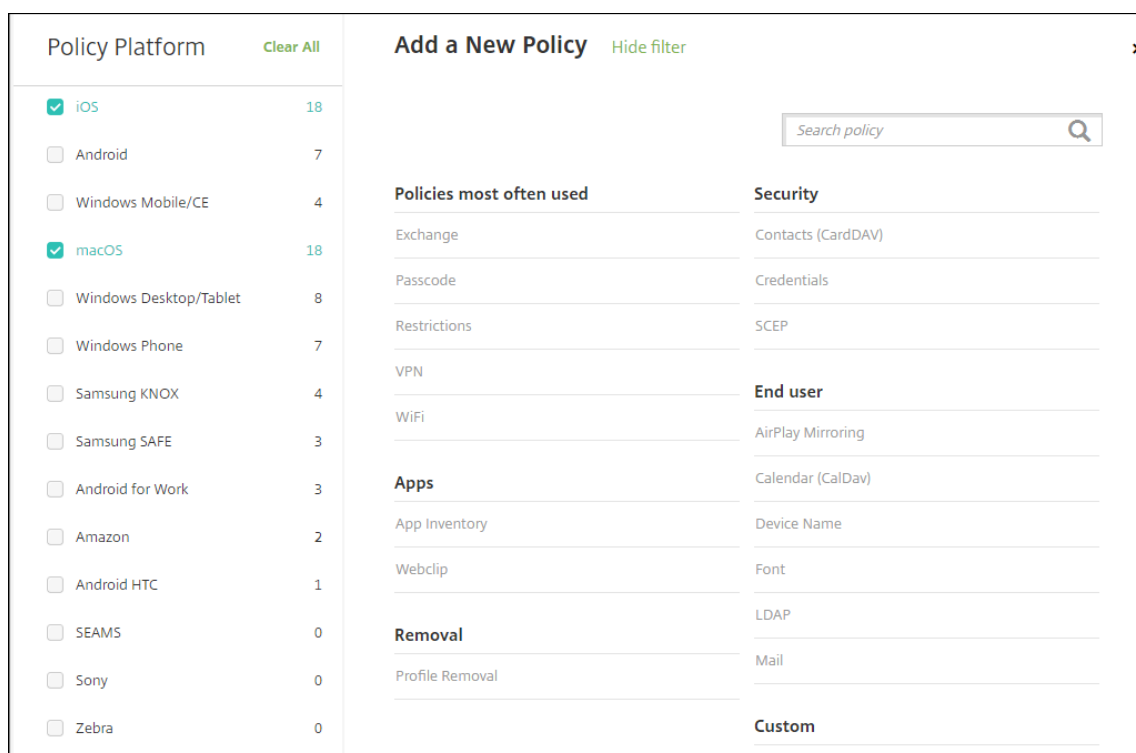
Para adicionar uma política:

1. Na página **Políticas de dispositivo**, clique em **Adicionar**. A página **Adicionar uma Nova Política** é exibida.

Policy Platform	Count
<input type="checkbox"/> iOS	45
<input type="checkbox"/> Android	20
<input type="checkbox"/> Windows Mobile/CE	20
<input type="checkbox"/> macOS	18
<input type="checkbox"/> Windows Desktop/Tablet	17
<input type="checkbox"/> Windows Phone	16
<input type="checkbox"/> Samsung KNOX	10
<input type="checkbox"/> Samsung SAFE	9
<input type="checkbox"/> Android for Work	6
<input type="checkbox"/> Amazon	3
<input type="checkbox"/> Android HTC	1
<input type="checkbox"/> SEAMS	1
<input type="checkbox"/> Sony	1
<input type="checkbox"/> Zebra	1

Policies most often used	Security
Exchange	Android for Work App Restrictions
Location	App Lock
Passcode	App Restrictions
Restrictions	BitLocker
Scheduling	Contacts (CardDAV)
Terms & Conditions	Copy Apps to Samsung Container
VPN	Credentials
WiFi	Defender
	Kiosk
Network access	Managed Domains
APN	SCEP
Cellular	Samsung MDM License Key
Connection Manager	

2. Clique em uma ou mais plataformas para exibir uma lista das políticas de dispositivo para as plataformas selecionadas. Clique em um nome de política para continuar adicionando a política.



Você também pode digitar o nome da política na caixa de pesquisa. Conforme você digita, possíveis correspondências são exibidas. Se a sua política estiver na lista, clique nela. Somente a política selecionada permanece nos resultados. Clique nela para abrir a página **Informações sobre a política** referente a essa política.

3. Selecione as plataformas que você deseja incluir na política. As páginas de configuração das plataformas selecionadas são exibidas na Etapa 5.
4. Preencha a página **Informações sobre a política** e clique em **Avançar**. A página **Informações sobre a política** reúne as informações, como o nome da política, para ajudá-lo a identificar e rastrear as políticas. Essa página é semelhante para todas as políticas.
5. Preencha as páginas de plataforma. As páginas de plataforma são exibidas para cada plataforma selecionada na Etapa 3. Essas páginas são diferentes para cada política. Uma política pode ser diferente entre as plataformas. Nem todas as políticas se aplicam a todas as plataformas.

Algumas páginas incluem tabelas de itens. Para excluir um item existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de lixeira no lado direito. Na caixa de diálogo de confirmação, clique em **Excluir**.

Para editar um item existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta no lado direito.

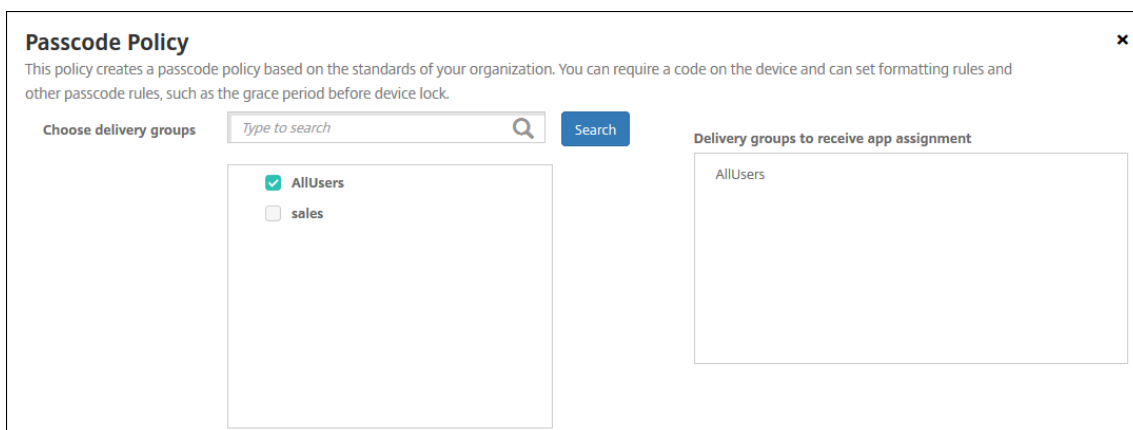
Para configurar regras de implantação, atribuições e cronograma

Para obter mais informações sobre como configurar as regras de implantação, incluindo ilustrações, consulte [Implantar recursos](#).

1. Na página da plataforma, expanda **Regras de implantação** e defina estas configurações: A guia **Base** é exibida por padrão.
 - Nas listas, clique nas opções para determinar quando a política deve ser implantada. Você pode optar por implantar a política quando todas as condições forem atendidas ou quando qualquer condição for atendida. A opção padrão é **Tudo**.
 - Clique em **Nova regra** para definir as condições.
 - Nas listas, clique nas condições, como **Propriedade do dispositivo** e **BYOD**.
 - Clique em **Nova regra** novamente se você desejar adicionar mais condições. Você pode adicionar quantas condições desejar.
2. Clique na guia **Avançado** para combinar as regras com as opções booleanas. As condições que você escolheu na guia **Base** são exibidas.
3. Você pode usar a lógica booleana mais avançada para combinar, editar ou adicionar regras.
 - Clique em **AND**, **OR** ou **NOT**.
 - Nas listas, selecione as condições que você deseja adicionar à regra. Em seguida, clique no sinal de mais (+) no lado direito para adicionar a condição à regra.

A qualquer momento, clique para selecionar uma condição e, em seguida, clique em **EDITAR** para alterar a condição ou em **Excluir** para removê-la.
 - Clique em **Nova regra** para adicionar outra condição.
4. Clique em **Avançar** para ir até a próxima página de plataforma ou, quando todas as páginas da plataforma estiverem preenchidas, até a página **Atribuições**.
5. Na página **Atribuições**, selecione os grupos de entrega aos quais você deseja aplicar a política. Se você clicar em um grupo de entrega, o grupo será exibido na caixa **Grupos de entrega que receberão a atribuição de aplicativos**.

Grupos de entrega que receberão a atribuição de aplicativos não aparece até que você selecione um grupo de entrega.



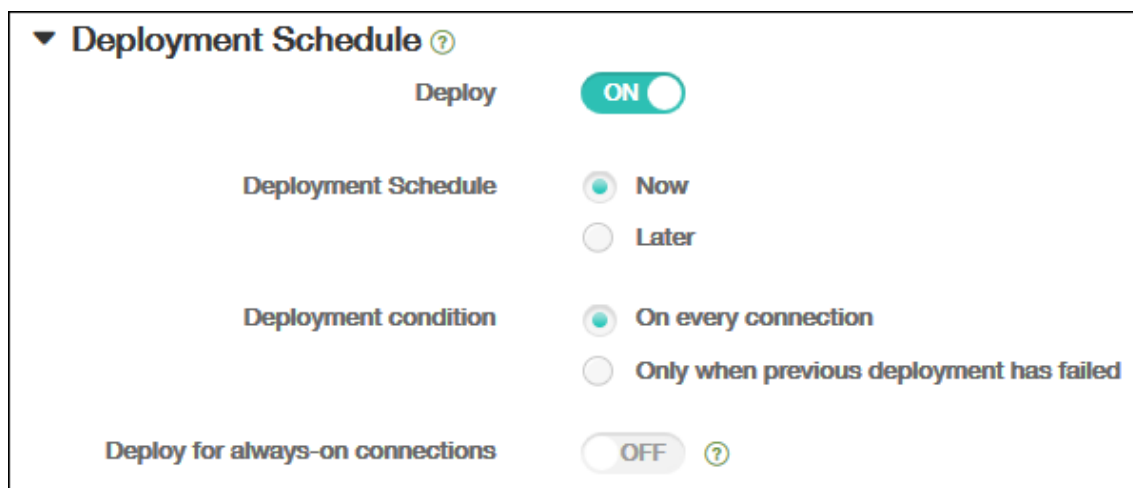
6. Na página **Atribuições**, expanda o **Cronograma de implantação** e depois defina as seguintes configurações:

- Ao lado de **Implantar**, clique em **I** para agendar a implantação ou em **O** para impedi-la. A opção padrão é **I**.
- Ao lado do **Cronograma de implantação**, clique em **Agora** ou em **Mais tarde**. A opção padrão é **Agora**.
- Se você clicar em **Mais tarde**, clique no ícone de calendário e selecione a data e a hora da implantação.
- Ao lado de **Condição de implantação**, clique em **Em cada conexão** ou em **Somente quando a implantação anterior tiver falhado**. A opção padrão é **Em cada conexão**.
- Ao lado de **Implantar para conexões permanentes**, clique em **I** ou **O**. A opção padrão é **O**.

Nota:

Essa opção será aplicável quando você tiver configurado a chave de implantação em segundo plano do cronograma em **Configurações > Propriedades do servidor**. A opção sempre conectada não está disponível para dispositivos iOS.

O cronograma de implantação que você configura é o mesmo para todas as plataformas. Todas as alterações feitas se aplicam a todas as plataformas, exceto **Implantar para conexões permanentes**, que não se aplica ao iOS.



7. Clique em **Salvar**.

A política é exibida na tabela **Políticas de dispositivo**.

Remover uma política de dispositivo de um dispositivo

As etapas para remover uma política de dispositivo de um dispositivo dependem da plataforma.

- Android

Para remover uma política de dispositivo de um dispositivo Android, use a política de dispositivo de desinstalação do XenMobile. Para obter informações, consulte [Política de dispositivo de desinstalação do XenMobile](#).

- iOS e macOS

Para remover uma política de dispositivo de um dispositivo iOS ou macOS, use a política de dispositivo de remoção de perfil. Em dispositivos iOS e macOS, todas as políticas fazem parte do perfil MDM. Assim, você pode criar uma política de dispositivo de remoção de perfil apenas para a política que deseja remover. O resto das políticas e o perfil permanecem no dispositivo. Para obter informações, consulte [Política de dispositivo de remoção de perfil](#).

- Windows 10

Você não pode remover diretamente uma política de dispositivo de um dispositivo Desktop ou Tablet com Windows 10. No entanto, você pode usar um dos seguintes métodos:

- Cancelar o registro do dispositivo e, em seguida, enviar por push um novo conjunto de políticas para o dispositivo. Depois, os usuários se registram novamente para continuar.
- Enviar uma ação de segurança por push para limpar seletivamente o dispositivo específico. Essa ação remove todos os aplicativos e dados corporativos do dispositivo. Em seguida, você remove a política de dispositivo de um grupo de entrega que contém

apenas esse dispositivo e envia o grupo de entrega para o dispositivo por push. Depois, os usuários se registram novamente para continuar.

- SO Chrome

Para remover uma política de dispositivo de um dispositivo Chrome OS, você pode remover a política de dispositivo de um grupo de entrega que contém apenas esse dispositivo. Em seguida, você envia o grupo de entrega para o dispositivo por push.

Editar uma política de dispositivo

Para editar uma política, selecione a caixa de seleção ao lado de uma política para mostrar o menu de opções acima da lista de políticas. Ou clique em uma política na lista para exibir o menu de opções no lado direito da lista.

Device Policies						
	Policy name	Type	Created on	Last updated on	Status	
<input type="checkbox"/>	K--Scheduling	Scheduling	8/12/17 6:43 AM	8/12/17 6:43 AM		
<input checked="" type="checkbox"/>	K--AppInv	Software Inventory	8/12/17 6:45 AM	8/12/17 6:45 AM		
<input type="checkbox"/>	K--Webclip	Mdm Weblink				
<input type="checkbox"/>	K--Passcode	Password				
<input type="checkbox"/>	K--Wifi	Wifi				
<input type="checkbox"/>	K--T&C	Terms Conditions				
<input type="checkbox"/>	K--Location	Locationservices				
<input type="checkbox"/>	K--EAS	Exchange				
<input type="checkbox"/>	K--AppLock	Applock				

Edit
Delete

Deployment

0
Installed

0
Pending

0
Failed

Show more >

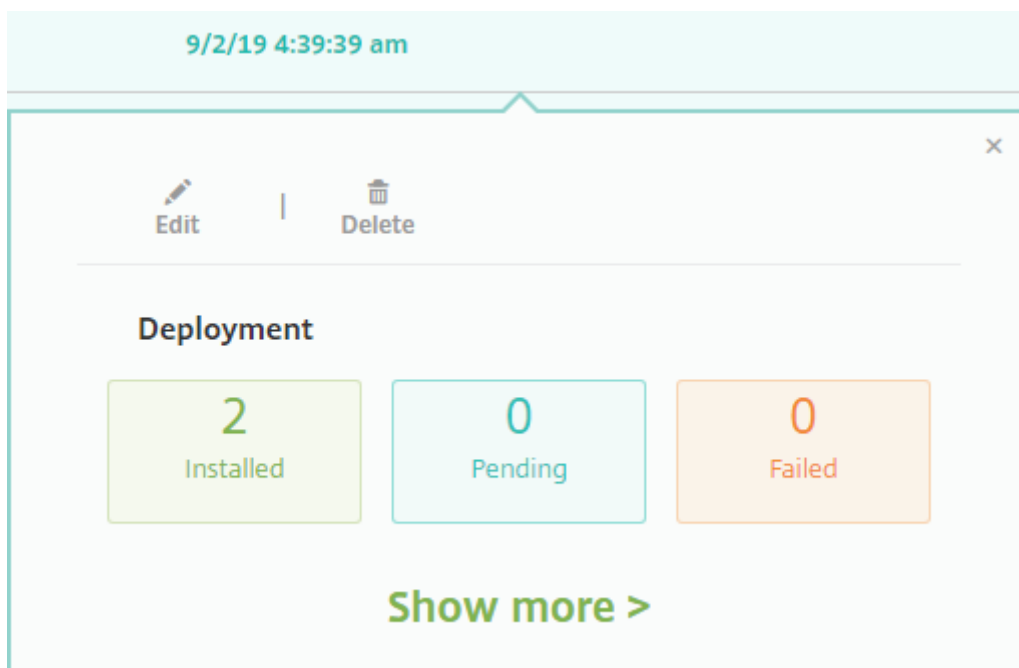
Para exibir os detalhes da política, clique em **Mostrar mais**.

Para editar as configurações de uma política de dispositivo, clique em **Editar**.

Se você clicar em **Excluir**, é exibida uma caixa de diálogo de confirmação. Clique em **Excluir** novamente para excluir a política.

Verificar o status de implantação da política

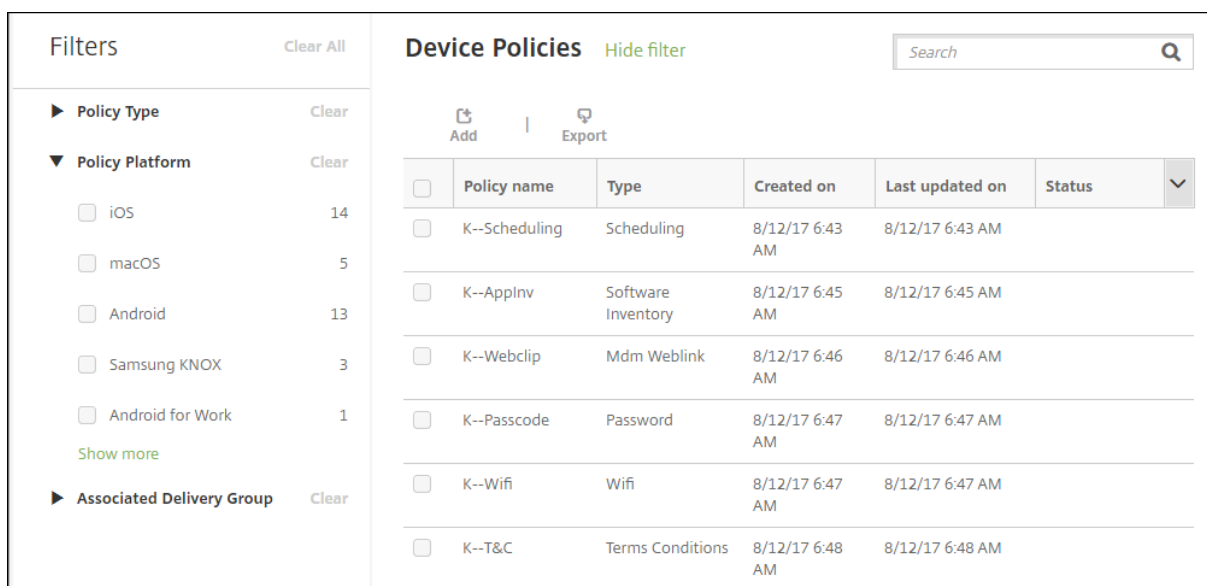
Clique em uma linha de política na página **Configurar > Políticas de dispositivo** para verificar o seu status de implantação.



Quando uma implantação de política está pendente, os usuários podem atualizar a política do Secure Hub tocando em **Preferências > Informações do dispositivo > Atualizar política**.

Filtrar a lista de políticas de dispositivo adicionadas

Você pode filtrar a lista de políticas adicionadas por tipos de política, plataformas e grupos de entrega associados. Na página **Configurar > Políticas de dispositivos**, clique em **Mostrar Filtro**. Na lista, selecione as caixas de seleção relativas aos itens que deseja ver.



Clique em **SALVAR ESTA EXIBIÇÃO** para salvar um filtro. O nome do filtro, em seguida, é exibida em

um botão abaixo do botão **SALVAR ESTA EXIBIÇÃO**.

Resumos de políticas de dispositivo

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Espelhamento de AirPlay	Adiciona dispositivos AirPlay específicos (como outro computador Mac) aos dispositivos iOS. Você também tem a opção de adicionar dispositivos a uma lista de permissão de dispositivos supervisionados. Essa opção limita os usuários a apenas os dispositivos AirPlay na lista de permissão.
AirPrint	Adiciona impressoras AirPrint à lista de impressoras AirPrint nos dispositivos iOS. Essa política facilita o suporte aos ambientes nos quais as impressoras e os dispositivos estão em sub-redes diferentes.
Permissões do aplicativo Enterprise Android	Configura como as solicitações para aplicativos do Android Enterprise nos perfis de trabalho lidam com o que o Google chama de permissões “perigosas”.
Restrições de aplicativos Android Enterprise	Atualiza as restrições associadas aos aplicativos Android.
APN	Determina as configurações usadas para conectar os seus dispositivos ao General Packet Radio Service (GPRS) de uma operadora de telefonia específica. Essa configuração já está definida na maioria dos novos telefones. Use essa política se sua organização não usar um APN de consumidor para conexão com a Internet de um dispositivo móvel.
Acesso aos aplicativos	Define uma lista dos aplicativos necessários, opcionais ou evitados no dispositivo. Você pode criar uma ação automatizada para reagir à conformidade do dispositivo com essa lista de aplicativos.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Atributos de aplicativo	Especifica atributos, como o ID de um pacote de aplicativo gerenciado ou um identificador de VPN por aplicativo, para dispositivos iOS.
Configuração do aplicativo	Define remotamente várias configurações e comportamentos de aplicativos que dão suporte à configuração gerenciada. Para fazer isso, você deve implantar um arquivo de configuração XML (chamado de lista de propriedades, ou plist) nos dispositivos iOS. Ou você pode implantar pares de chave/valor no Windows 10 phone, área de trabalho ou dispositivos de tablet.
Inventário de aplicativos	Coleta um inventário dos aplicativos em dispositivos gerenciados. O XenMobile compara então o inventário com todas as políticas de acesso aos aplicativos implantadas nesses dispositivos. Dessa forma, você pode detectar aplicativos que estão em uma lista de permissão ou de bloqueio de acesso a aplicativo e tomar as devidas providências.
Bloqueio de aplicativo	Define uma lista de aplicativos que os usuários podem ou não executar em determinados dispositivos Android ou iOS.
Uso de rede de aplicativos	Define regras de uso de rede para especificar como os aplicativos gerenciados usam redes, como redes de dados celulares, nos dispositivos iOS. As regras se aplicam somente aos aplicativos gerenciados. Os aplicativos gerenciados são aqueles que você implanta nos dispositivos de usuários por meio do XenMobile.
Restrições de aplicativo	Cria listas de bloqueio de aplicativos que você deseja impedir que os usuários instalem em dispositivos Samsung Knox. Você também pode criar listas de permissão de aplicativos que os usuários podem instalar.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Desinstalação de aplicativo	Remove aplicativos dos dispositivos do usuário.
Restrições de desinstalação de aplicativo	Especifica os aplicativos que os usuários podem ou não desinstalar.
Notificações de aplicativos	Controla como os usuários do iOS recebem notificações de aplicativos especificados.
Atualizar automaticamente aplicativos gerenciados	Controla como os aplicativos gerenciados instalados são atualizados em dispositivos Android Enterprise.
BitLocker	Ajusta as configurações disponíveis na interface do BitLocker em dispositivos Windows 10.
Navegador	Define se os dispositivos dos usuários podem usar o navegador ou quais funções de navegador os dispositivos podem usar.
Calendário (CalDav)	Adiciona uma conta de calendário (CalDAV) a dispositivos iOS ou macOS. A conta CalDAV permite que os usuários sincronizem dados de agendamento com qualquer servidor compatível com CalDAV.
Celular	Define as configurações de rede celular.
Gerenciador de conexões	Especifica as configurações de conexão dos aplicativos que se conectam automaticamente à Internet e a redes privadas. Essa política está disponível somente em Windows Pocket PCs.
Contatos (CardDAV)	Adiciona uma conta de contato do iOS (CardDAV) a dispositivos iOS ou macOS. A conta CardDAV permite que os usuários sincronizem dados de contato com qualquer servidor compatível com CardDAV.
Controlar atualizações do sistema operacional	Implanta as mais recentes atualizações de sistema operacional em dispositivos supervisionados com suporte.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Copiar aplicativos para o contêiner da Samsung	Copia os aplicativos que já estão instalados em um dispositivo para um contêiner KNOX em dispositivos Samsung com suporte. Os aplicativos copiados para o contêiner KNOX ficam disponíveis somente quando os usuários fazem login no contêiner KNOX.
Credenciais	Permite que autenticação integrada com sua configuração de PKI no XenMobile. Por exemplo, com uma entidade PKI, um keystore, um provedor de credenciais ou um certificado de servidor.
XML personalizado	Personaliza recursos como provisionamento de dispositivos, habilitação de recursos do dispositivo, configuração do dispositivo e gerenciamento de falhas.
Defender	Define configurações do Windows Defender no Windows 10 para desktop e tablet.
Excluir arquivos e pastas	Exclui arquivos e pastas específicos dos dispositivos Windows Mobile/CE.
Excluir chaves e valores do registro	Exclui chaves e valores específicos do registro dos dispositivos Windows Mobile/CE.
Atestado de integridade de dispositivo	Requer que os dispositivos Windows 10 informem o estado da sua integridade. Para que eles enviem dados específicos e informações de tempo de execução para o serviço de atestado de integridade (HAS) para análise. O HAS cria e retorna um Certificado de Atestado de Integridade que o dispositivo envia para o XenMobile. Quando o XenMobile recebe o Certificado de Atestado de Integridade, com base no conteúdo daquele certificado, ele pode implantar ações automáticas que você configurou.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Nome do dispositivo	Define os nomes em dispositivos iOS e macOS para que você possa identificá-los. Você pode usar macros, texto ou uma combinação de ambos para definir um nome de dispositivo.
Configuração de educação	Configura os dispositivos de instrutor e estudante para uso com o Apple Educação. Se os instrutores usam o aplicativo de Sala de Aula, é necessária a política do dispositivo Configuração de Educação.
Hub empresarial	Distribui aplicativos a Windows Phones por meio da loja Enterprise Hub Company. O XenMobile é compatível somente com uma política do Hub Empresarial para um modo do Secure Hub para Windows Phone. Por exemplo, não crie várias políticas do Hub Empresarial com versões diferentes do Secure Home para XenMobile Enterprise Edition. Você pode implantar a política inicial do Hub Empresarial somente durante registro do dispositivo.
Exchange	Ativa os emails do ActiveSync para o cliente de email nativo no dispositivo.
Arquivos	Adiciona os arquivos de script ao XenMobile que executam determinadas funções para usuários. Ou você pode adicionar arquivos de documento que deseja que os usuários do dispositivo Android tenham acesso em seus dispositivos. Quando você adiciona o arquivo, pode também especificar o diretório no qual deseja que o arquivo seja armazenado no dispositivo.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
FileVault	Esta política permite que você ative a criptografia do dispositivo FileVault em dispositivos macOS registrados. Você também pode controlar o número de vezes que um usuário pode ignorar a configuração do FileVault durante o logon. Disponível para macOS 10.7 ou versões posteriores.
Firewall	Define as configurações de firewall. Você fornece os endereços IP, as portas e os nomes de host que deseja permitir ou bloquear nos dispositivos. Você também pode definir o proxy e as configurações de redirecionamento do proxy.
Fonte	Adiciona mais fontes para dispositivos iOS e macOS. As fontes devem ser TrueType (.TTF) ou OpenType (.OTF). O XenMobile não dá suporte a coleções de fontes (.TTC ou .OTC).
Layout da tela inicial	Especifica o layout de aplicativos e pastas para a tela inicial do iOS em dispositivos supervisionados iOS 9.3 e versões posteriores.
Importar perfil de iOS e macOS	Importa arquivos XML de configuração de dispositivo para dispositivos iOS e macOS para o XenMobile. O arquivo contém as políticas de segurança do dispositivo e as restrições que você prepara por meio do Apple Configurator.
Gerenciamento de proteção do teclado	Controla os recursos disponíveis para os usuários antes que eles desbloqueiem a proteção do teclado do dispositivo e o keyguard do Work Challenge. Você também pode controlar os recursos de proteção do teclado do dispositivo para dispositivos totalmente gerenciados e dedicados. Por exemplo, você pode desativar recursos de tela de bloqueio, como desbloqueio por impressão digital, agentes confiáveis e notificações.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Quiosque	Restringe o uso do aplicativo em dispositivos Samsung SAFE. Você pode limitar os aplicativos disponíveis a um ou mais aplicativos específicos. Essa política é útil para dispositivos corporativos que foram criados para executar somente um tipo ou classe específico de aplicativos. Esta política também permite que você escolha imagens personalizadas para a tela inicial do dispositivo e papéis de parede de bloqueio de tela no modo de quiosque.
Configuração do Launcher	Especifica as configurações para o Citrix Launcher nos dispositivos Android, como os aplicativos permitidos e uma imagem de logotipo personalizado para o ícone do Launcher.
LDAP	Oferece informações sobre um servidor LDAP a ser usado nos dispositivos iOS, incluindo qualquer informação de conta necessária como o nome de host do servidor LDAP. A política também fornece um conjunto de políticas de pesquisa de LDAP a serem usadas ao consultar o servidor LDAP.
Localização	Permite geolocalizar dispositivos em um mapa, desde que o aparelho esteja com o GPS ativado no Secure Hub. Depois de implantar essa política no dispositivo, você pode enviar um comando de localização a partir do XenMobile Server. O dispositivo responde com as suas coordenadas de localização. O XenMobile também oferece suporte a políticas de geocerca e de rastreamento.
Email	Configura uma conta de email em dispositivos iOS ou macOS.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Domínios gerenciados	Define os domínios gerenciados que se aplicam a emails e ao navegador Safari. Os domínios gerenciados ajudam você a proteger dados corporativos ao controlar quais aplicativos podem abrir documentos baixados de domínios usando o Safari. Para dispositivos supervisionados iOS 8 e versões posteriores, você pode especificar as URLs ou os subdomínios para controlar como os usuários podem abrir documentos, anexos e downloads do navegador.
Opções de MDM	Gerencia o bloqueio de ativação Buscar iPhone e iPad em dispositivos supervisionados iOS 7.0 e versões posteriores.
Informações sobre a organização	Especifica as informações da organização para mensagens de alerta que o XenMobile implanta em dispositivos iOS.
Código secreto	Impõe um código PIN ou senha em um dispositivo gerenciado. Você pode definir a complexidade e os tempos limite do código secreto no dispositivo.
Ponto de acesso pessoal	Permite que os usuários se conectem à internet quando não estão dentro do alcance de uma rede WiFi. Os usuários se conectam por meio da conexão de dados celulares no seu dispositivo iOS, usando a funcionalidade de ponto de acesso pessoal.
Remoção de perfil	Remove o perfil de aplicativo dos dispositivos iOS ou macOS.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Perfil de provisionamento	Especifica um perfil de provisionamento de distribuição empresarial para enviar para os dispositivos. Quando você desenvolve assina com código um aplicativo empresarial iOS, você geralmente inclui um perfil de provisionamento. A Apple requer que o perfil para o aplicativo seja executado em um dispositivo iOS. Se um perfil de configuração estiver ausente ou tiver expirado, o aplicativo falhará quando um usuário tocar para abri-lo.
Remoção de perfil de provisionamento	Remove perfis de provisionamento do iOS.
Proxy	Especifica as configurações de proxy HTTP globais para dispositivos que executam o Windows Mobile/CE e o iOS. Você pode implantar somente uma política de proxy HTTP global por dispositivo.
Registro	Define as chaves e os valores do registro que permitem administrar dispositivos Windows Mobile/CE. O Registro do Windows Mobile/CE armazena dados sobre as definições de aplicativos, drivers, preferências do usuário e configurações.
Suporte remoto	Fornece a você o acesso remoto aos dispositivos Samsung KNOX. O Remote Support não está mais disponível para novos clientes desde 1º de janeiro de 2019. Os clientes existentes podem continuar a usar o produto, no entanto, a Citrix não fornecerá melhorias ou correções.
Restrições	Fornece centenas de opções para bloquear e controlar recursos e funcionalidades em dispositivos gerenciados. Exemplos de opções de restrição: desativar a câmera ou o microfone, impor regras de roaming e forçar o acesso a serviços de terceiros, como lojas de aplicativos.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Roaming	Configura se deve ser permitida voz e o roaming de dados em dispositivos iOS e Windows Mobile/CE. Se o roaming de voz está desativado, o roaming de dados é automaticamente desativado.
Chave de licença MDM Samsung	Especifica a chave interna do Enterprise License Management (ELM) Samsung que você precisa implantar em um dispositivo antes de implantar as políticas e restrições do SAFE. O XenMobile também suporta o serviço Enterprise Firmware Over-The-Air (E-FOTA) da Samsung. O XenMobile dá suporte às políticas do Samsung for Enterprise (SAFE) e do Samsung KNOX e as estende.
Programação	Obrigatória nos dispositivos Android e Windows Mobile para se conectar de volta ao XenMobile Server para gerenciamento do MDM, envio por push de aplicativos e implantação de políticas. Se você não enviar essa política a dispositivos e não ativar o Google FCM, um dispositivo não poderá se conectar de volta ao servidor.
SCEP	Configura dispositivos iOS e macOS para recuperar um certificado de um servidor SCEP externo. Você também pode fornecer um certificado para o dispositivo usando SCEP de uma PKI que esteja conectada ao XenMobile. Para fazer isso, crie uma entidade de PKI e um provedor de PKI em modo distribuído.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Conta SSO	Cria contas de logon único (SSO) para que os usuários façam logon somente uma vez para acessar o XenMobile e seus recursos internos da empresa. Os usuários não precisam armazenar nenhuma credencial no dispositivo. O XenMobile usa as credenciais do usuário empresarial da conta SSO entre aplicativos, incluindo os aplicativos da App Store. Essa política é compatível com a autenticação Kerberos. Disponível para o iOS.
Criptografia de armazenamento	Criptografa armazenamento interno e externo. Em alguns dispositivos, essa política impede que os usuários usem um cartão de armazenamento nos respectivos dispositivos.
Calendários inscritos	Adiciona um calendário inscrito à lista de calendários nos dispositivos iOS. Inscreva-se em um calendário antes de adicioná-lo à lista de calendários inscritos nos dispositivos dos usuários.
Termos e condições	Requer que os usuários aceitem as políticas específicas da empresa que regem as conexões à rede corporativa. Quando os usuários registram seus dispositivos no XenMobile, eles devem aceitar os termos e condições para registrar os dispositivos. Não aceitar os termos e condições cancela o processo de registro.

Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Túnel	Usada somente para suporte remoto. O suporte remoto permite que o pessoal da central de ajuda assuma o controle remotamente de dispositivos móveis gerenciados Windows CE e Android. O suporte remoto não está disponível para implantações do XenMobile Server em cluster no local. O Remote Support não está mais disponível para novos clientes desde 1º de janeiro de 2019. Os clientes existentes podem continuar a usar o produto, no entanto, a Citrix não fornecerá melhorias ou correções.
VPN	Fornecer acesso a sistemas de backend que usam a tecnologia de Gateway VPN de legado. Esta política fornece detalhes de conexão gateway VPN que você pode implantar nos dispositivos. XenMobile é compatível com vários provedores de VPN, incluindo Cisco AnyConnect, Juniper e Citrix VPN. Se o seu gateway VPN der suporte a esta opção, você poderá vincular essa política a uma CA e ativar VPN sob demanda.
Papel de parede	Adiciona um arquivo .png ou .jpg para definir o papel de parede na tela de bloqueio ou na tela inicial de um dispositivo iOS, ou em ambas. Para usar papéis de parede diferentes em iPads e iPhones, crie políticas diferentes de papéis de parede e implantá-las nos usuários apropriados.
Filtro de conteúdo Web	Filtra conteúdo web nos dispositivos iOS. O XenMobile usa a função de filtro automático da Apple e os sites que você adiciona a listas de permissão e de bloqueio. Disponível somente para dispositivos supervisionados iOS.

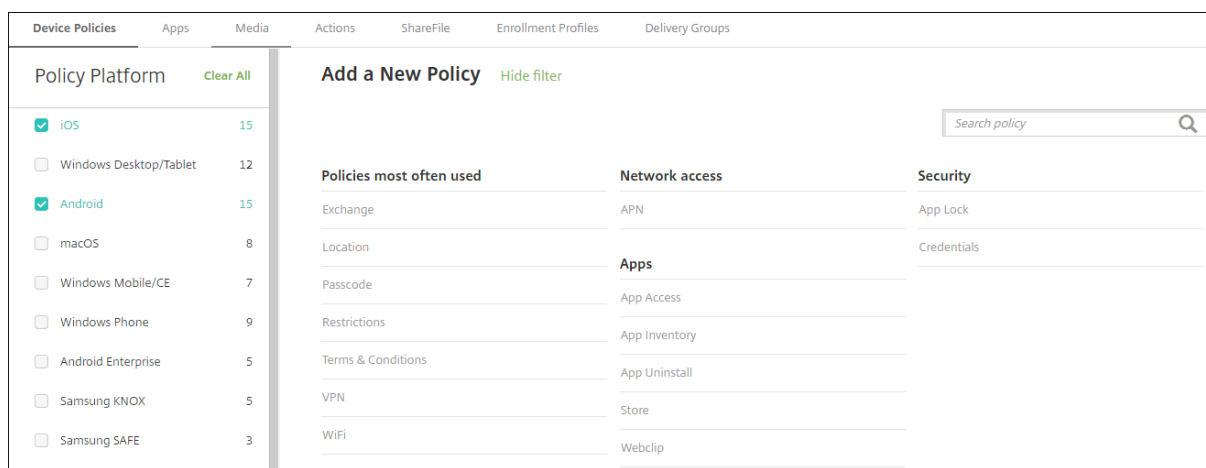
Nome da Política de Dispositivo	Descrição da Política de Dispositivo
Clip web	Insere atalhos ou cliques Web em sites para que apareçam junto com aplicativos nos dispositivos de usuários. Você pode especificar seus próprios ícones para representar os cliques Web para dispositivos iOS, macOS e Android. O tablet Windows requer somente um rótulo e uma URL.
WiFi	Permite que os administradores implantem detalhes do roteador de WiFi em dispositivos gerenciados. Os detalhes do roteador incluem SSID, dados de autenticação e dados de configuração.
Certificado Windows CE	Cria e fornece certificados Windows Mobile/CE de uma PKI externa para os dispositivos de usuários.
Proteção de informações do Windows	Especifica os aplicativos que exigem a Proteção de informações do Windows no nível de imposição definido na política. A política é para dispositivos supervisionados Windows 10 versão 1607 e versões posteriores.
XenMobile Store	Especifica se um clip Web da XenMobile Store aparece na tela inicial dos dispositivos do usuário.
Opções do XenMobile	Configura o comportamento do Secure Hub quando ele se conecta ao XenMobile a partir de dispositivos Android e Windows Mobile/CE.
Desinstalação do XenMobile	Desinstala o XenMobile dos dispositivos Android e Windows Mobile/CE. Quando implantada, essa política remove o XenMobile de todos os dispositivos no grupo de implantação.

Políticas de dispositivo por plataforma

January 22, 2021

Para exibir as políticas disponíveis por plataforma:

1. No console XenMobile, vá para **Configurar > Políticas de dispositivo**.
2. Clique em **Adicionar**.
3. Cada plataforma de dispositivo é exibida em uma lista no painel **Plataforma de política**. Se esse painel não estiver aberto, clique em **Mostrar filtro**.
4. Para ver uma lista de todas as políticas disponíveis para uma plataforma, selecione a plataforma. Para ver uma lista das políticas que estão disponíveis para várias plataformas, selecione cada uma dessas plataformas. Uma política aparece na lista somente se ela se aplicar a cada plataforma selecionada.



A versão mais recente do XenMobile é compatível com políticas de dispositivo para as seguintes plataformas:

- Amazon
- Android
- Android Enterprise
- Android Zebra
- SO Chrome
- iOS
- macOS
- Samsung SAFE
- Samsung KNOX
- Windows 10 Desktop/Tablet
- Telefone Windows 10
- Windows Mobile/CE

Para obter detalhes sobre os dispositivos com suporte na versão mais recente do XenMobile, consulte [Plataformas de dispositivo com suporte](#).

Nota:

Se o seu ambiente estiver configurado com Objetos de Política de Grupo (GPOs):

Quando você configurar políticas de dispositivo do XenMobile para o Windows 10, lembre-se da regra a seguir. Se uma política em um ou mais dispositivos Windows 10 registrados for conflitante, a política alinhada ao GPO terá precedência.

Política de dispositivo de espelhamento de AirPlay

April 26, 2021

O recurso Apple AirPlay permite que os usuários espelhem exatamente o que está no monitor de um dispositivo em outro computador Mac.

Você pode adicionar uma política de dispositivo do XenMobile para adicionar dispositivos específicos AirPlay (como outro computador Mac) aos dispositivos iOS. Você também tem a opção de adicionar dispositivos a uma lista de permissão de dispositivos supervisionados, o que limita os usuários a somente os dispositivos AirPlay na lista de permissão. Para obter informações sobre como colocar um dispositivo no modo Supervisionado, consulte [Para colocar um dispositivo iOS no modo Supervisionado usando o Apple Configurator](#).

Nota:

Antes de prosseguir, verifique se você tem os IDs de dispositivo e todas as senhas de todos os dispositivos que deseja adicionar.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

AirPlay Mirroring Policy

This policy lets you specify specific AirPlay devices to add to users' iOS and macOS devices. For supervised devices, you have the option of specifying a list of whitelisted AirPlay devices.

AirPlay Password

Device Name * Password * Add

Whitelist ID

Device ID * Add

Policy Settings

Remove policy Select date Duration until removal (in hours)

Allow user to remove policy Always

- **Senha do AirPlay:** para cada dispositivo que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
 - **ID do dispositivo:** insira o endereço de hardware (endereço Mac) no formato xx:xx:xx:xx:xx:xx. Esse campo não diferencia maiúsculas de minúsculas.
 - **Senha:** insira uma senha opcional para o dispositivo.
 - Clique em **Adicionar** para adicionar o dispositivo ou em **Cancelar** para cancelar a adição do dispositivo.
- **ID da lista branca:** essa lista é ignorada para dispositivos não supervisionados. Os IDs de dispositivo nessa lista são os únicos dispositivos AirPlay disponíveis para os dispositivos dos usuários. Para cada dispositivo AirPlay que você desejar adicionar à lista, clique em **Adicionar** e faça o seguinte:

Nota:

O console XenMobile Server inclui os termos “lista negra” e “lista branca”. Estamos alterando esses termos em uma próxima versão para “lista de bloqueio” e “lista de permissão”.

- **ID do dispositivo:** digite o ID do dispositivo no formato xx:xx:xx:xx:xx:xx. Esse campo não diferencia maiúsculas de minúsculas.
 - Clique em **Adicionar** para adicionar o dispositivo ou em **Cancelar** para cancelar a adição do dispositivo.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra.

Configurações do macOS

- **Senha do AirPlay:** para cada dispositivo que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
 - **ID do dispositivo:** insira o endereço de hardware (endereço Mac) no formato xx:xx:xx:xx:xx:xx. Esse campo não diferencia maiúsculas de minúsculas.
 - **Senha:** insira uma senha opcional para o dispositivo.
 - Clique em **Adicionar** para adicionar o dispositivo ou em **Cancelar** para cancelar a adição do dispositivo.
- **ID da lista branca:** essa lista é ignorada para dispositivos não supervisionados. Os IDs de dispositivo nessa lista são os únicos dispositivos AirPlay disponíveis para os dispositivos do usuário. Para cada dispositivo AirPlay que você desejar adicionar à lista, clique em **Adicionar** e faça o seguinte:
 - **ID do dispositivo:** digite o ID do dispositivo no formato xx:xx:xx:xx:xx:xx. Esse campo não diferencia maiúsculas de minúsculas.
 - Clique em **Adicionar** para adicionar o dispositivo ou em **Cancelar** para cancelar a adição do dispositivo.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra.
 - **Permitir que o usuário remova a política:** você pode selecionar quando os usuários podem remover a política do dispositivo. Selecione **Sempre**, **Código secreto obrigatório** ou **Nunca** no menu. Se você selecionar **Código secreto obrigatório**, digite um código secreto no campo **Código secreto de remoção**.
 - **Escopo do perfil:** selecione se esta política se aplica a um **Usuário** ou a um **Sistema** in-

teiro. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

Política de dispositivo do AirPrint

April 23, 2020

Você pode adicionar uma política de dispositivo ao XenMobile para adicionar impressoras AirPrint à lista de impressoras AirPrint nos dispositivos iOS. Essa política facilita o suporte aos ambientes nos quais as impressoras e os dispositivos estão em sub-redes diferentes.

Essa política se aplica ao iOS 7.0 e versões posteriores.

Nota:

Verifique se você tem o endereço IP e o caminho do recurso de cada impressora.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

- **Destino do AirPrint:** para cada destino do AirPrint que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
 - **Endereço IP:** insira o endereço IP da impressora AirPrint.
 - **Caminho do recurso:** insira o Caminho do Recurso associado à impressora. Esse valor corresponde ao parâmetro do registro `_ipps.tcp Bonjour`. Por exemplo, `printers/-Canon_MG5300_series` ou `printers/Xerox_Phaser_7600`.
 - Clique em **Salvar** para adicionar a impressora ou em **Cancelar** para cancelar a adição da impressora.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Política de configurações gerenciadas do Android Enterprise

May 24, 2021

A política de dispositivo de configurações gerenciadas do Android Enterprise controla várias opções de configuração de aplicativos e restrições de aplicativos. O desenvolvedor do aplicativo define as opções e dicas de ferramentas disponíveis para um aplicativo. Se uma dica de ferramenta mencionar o uso de um “valor modelo”, use a macro XenMobile correspondente. Para obter mais informações, consulte [Visão geral da configuração remota](#) (no site do desenvolvedor Android) e [Macros](#).

Os parâmetros de configuração do aplicativo podem incluir itens como:

- Configurações de e-mail do aplicativo
- Permitir ou bloquear URLs para um navegador da Web
- Opção para controlar a sincronização de conteúdo do aplicativo através de uma conexão celular ou apenas por uma conexão Wi-Fi

Para obter informações sobre as configurações exibidas para seus aplicativos, entre em contato com o desenvolvedor do aplicativo.

Pré-requisitos

- Conclua as tarefas de configuração do Android Enterprise no Google e conecte o Android Enterprise ao Google Play gerenciado. Para obter mais informações, consulte [Android Enterprise](#).
- Adicione aplicativos Android Enterprise ao XenMobile. Para obter mais informações, consulte [Adição de aplicativos ao XenMobile](#).

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Requisitos para VPNs por aplicativo

Para criar uma VPN por aplicativo para AE, você precisa executar etapas extras, além de configurar a política de configurações gerenciadas do Android Enterprise. Além disso, você deve verificar se os seguintes pré-requisitos foram atendidos:

- Citrix Gateway no local
- Os seguintes aplicativos estão instalados no dispositivo:
 - Citrix SSO
 - Citrix Secure Hub

Um fluxo de trabalho geral para configurar uma VPN por aplicativo para dispositivos AE:

1. Configure um perfil VPN como descrito neste artigo.

2. Configure o Citrix ADC para aceitar o tráfego da VPN por aplicativo. Para obter detalhes, consulte [Configuração de VPN completa no Citrix Gateway](#).

Configurações do Android Enterprise

Depois que você optar por adicionar uma política de dispositivo de configurações gerenciadas do Android Enterprise, será exibida uma solicitação para selecionar um aplicativo. Se não houver nenhum aplicativo do Android Enterprise adicionado ao XenMobile, você não poderá continuar.

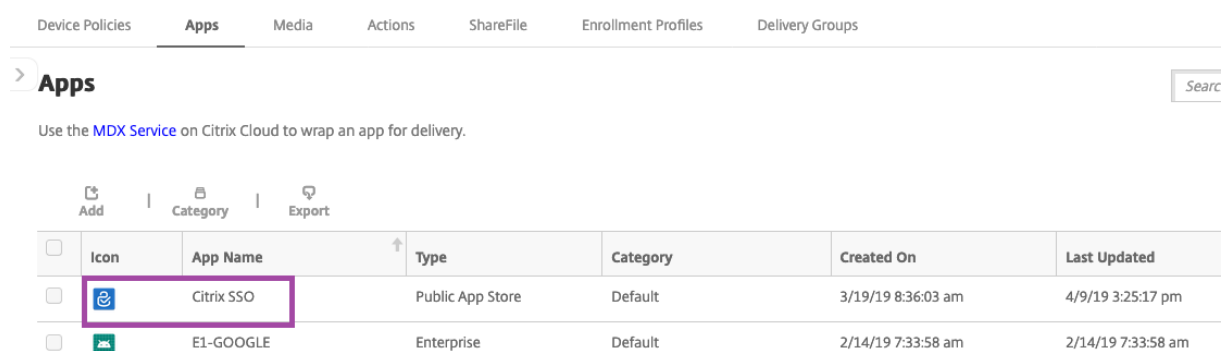
Depois de selecionar um aplicativo, defina as configurações de política. As configurações são específicas para cada aplicativo.

Android Enterprise Managed Configurations	Android Enterprise Managed Configurations
1 Policy Info	This policy lets you control a variety of app configuration options and app restrictions. The options available for an app and the tooltips are defined by the app developer. If a tooltip mentions using a "templated value", use the corresponding Endpoint Management macro instead.
2 Platforms Clear All	Restrictions for importing documents <input type="checkbox"/> Box <input type="checkbox"/> DropBox <input type="checkbox"/> Drive
<input checked="" type="checkbox"/> Android Enterprise	Restrictions for sharing the DocuSign app <input type="checkbox"/> Box <input type="checkbox"/> DropBox <input type="checkbox"/> Drive <input type="checkbox"/> Evernote
3 Assignment	Restrictions for sharing envelopes and documents <input type="checkbox"/> Box <input type="checkbox"/> DropBox <input type="checkbox"/> Drive <input type="checkbox"/> Evernote

Configurar perfis VPN para Android Enterprise

Disponibilize perfis VPN para dispositivos Android Enterprise usando o aplicativo Citrix SSO com a política de dispositivo de configuração gerenciada do Android Enterprise.

Comece adicionando o Citrix SSO ao console XenMobile como um aplicativo da Google Play Store. Consulte [Acrescentar um aplicativo de loja de aplicativos pública](#).

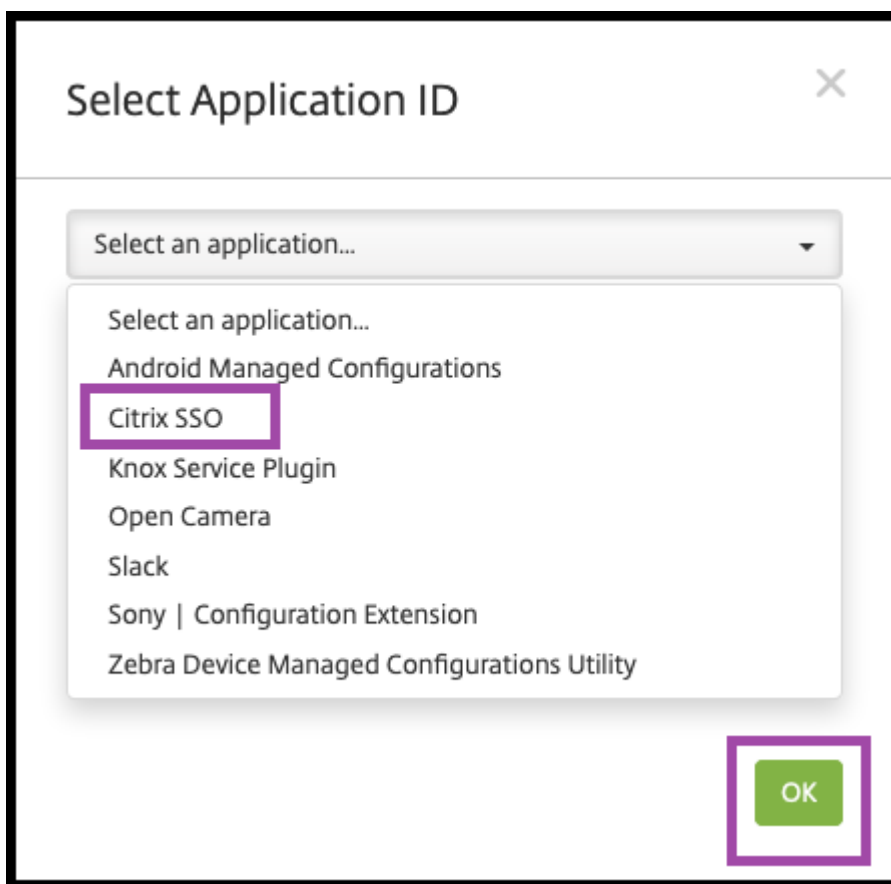


Criar uma configuração gerenciada do Android Enterprise para o Citrix SSO

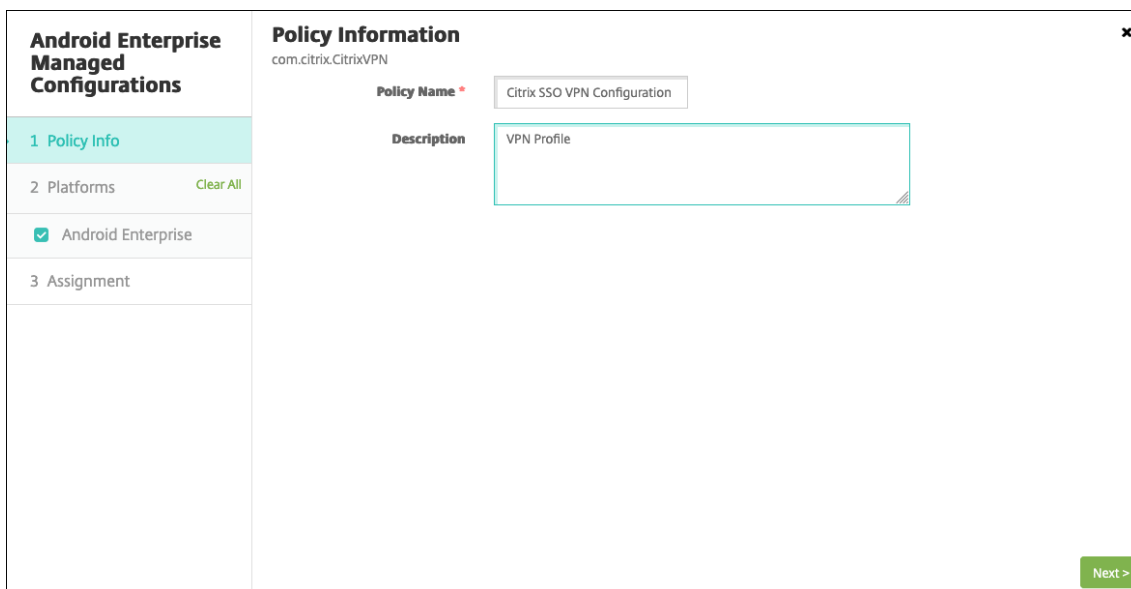
Configure a política de dispositivo de configurações gerenciadas do Android Enterprise para Citrix SSO para criar perfis VPN. Os dispositivos que têm o aplicativo Citrix SSO instalado e a política implantada têm acesso aos perfis VPN criados por você.

Você precisa do seu Citrix Gateway FQDN e da porta.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. Clique em **Add**.
2. Selecione **Android Enterprise**. Clique em **Configurações gerenciadas do Android Enterprise**.
3. Quando a janela **Selecionar ID do aplicativo** for exibida, escolha **Citrix SSO** na lista e clique em **OK**.



4. Digite um nome e uma descrição para a configuração da sua Citrix SSO VPN. Clique em **Avançar**.



5. Configure os parâmetros de perfil VPN.
 - **Nome do perfil VPN.** Digite um nome para o perfil VPN. Se você estiver criando mais de um perfil VPN, use um nome exclusivo para cada um. Se você não fornecer um nome, o

endereço colocado no campo **Endereço do servidor** será usado como o nome do perfil VPN.

- **Endereço do servidor(*)**. Digite o seu Citrix Gateway FQDN. Se a porta do Citrix Gateway não for 443, digite a porta também. Use formato de URL. Por exemplo, <https://gateway.mycompany.com:8443>.
- **Nome de usuário (opcional)**. Forneça o nome de usuário que os usuários finais usam para se autenticar no Citrix Gateway. Você pode usar a macro XenMobile {user.username} para este campo. (Consulte [Macros](#).) Se você não fornecer um nome de usuário, os usuários serão solicitados a fornecer um nome de usuário quando se conectarem ao Citrix Gateway.
- **Senha (opcional)**. Forneça a senha que os usuários finais usam para se autenticar no Citrix Gateway. Se você não fornecer uma senha, os usuários serão solicitados a fornecer uma senha quando se conectarem ao Citrix Gateway.
- **Alias de certificado (opcional)**. Digite um alias de certificado. O alias do certificado facilita o acesso do aplicativo ao certificado. Quando o mesmo alias de certificado é usado com a política de dispositivo de Credenciais, o aplicativo recupera o certificado e autentica a VPN sem qualquer ação dos usuários.
- **Tipo VPN por aplicativo (opcional)**. Se você estiver usando VPN por aplicativo para restringir quais aplicativos usam a VPN, você pode configurar esse parâmetro. Se você selecionar **Permitir**, o tráfego de rede para os nomes de pacotes de aplicativos relacionados na **lista de aplicativos PerAppVPN** será roteado através da VPN. O tráfego de rede de todos os outros aplicativos é roteado fora da VPN. Se você selecionar **Não permitir**, o tráfego de rede para os nomes de pacotes de aplicativos relacionados na **lista de aplicativos PerAppVPN** será roteado por fora da VPN. O tráfego de rede de todos os outros aplicativos é roteado através da VPN. O padrão é **Permitir**.
- **Lista de aplicativos PerAppVPN**. Uma lista de aplicativos cujo tráfego é permitido ou bloqueado na VPN, dependendo do valor do **Tipo de VPN por aplicativo**. Liste os nomes dos pacotes de aplicativos separados por vírgula ou ponto e vírgula. Os nomes dos pacotes de aplicativos diferenciam maiúsculas e minúsculas e devem aparecer nesta lista exatamente como aparecem na loja de aplicativos Google Play. Esta lista é opcional. Mantenha esta lista vazia para o provisionamento de VPN em todo o dispositivo.
- **Perfil VPN padrão**. Digite o nome do perfil VPN a ser usado quando os usuários tocarem no switch de conexão na interface de usuário do aplicativo Citrix SSO em vez de tocar em um perfil específico. Se esse campo for deixado vazio, o perfil principal será usado para conexão. Se apenas um perfil estiver configurado, ele será marcado como perfil padrão. Para VPN sempre conectada, esse campo deve ser definido como o nome do perfil VPN a ser usado para estabelecer VPN sempre conectada.

- **Desativar perfis de usuário.** Se essa configuração estiver ON, os usuários não poderão criar suas próprias VPNs em seus dispositivos. Se essa configuração estiver OFF, os usuários poderão criar suas próprias VPNs em seus dispositivos. O padrão é OFF.
- **Bloquear servidores não confiáveis.** Esta definição está OFF quando utiliza um certificado auto-assinado para o Citrix Gateway ou quando o certificado raiz para a AC que emite o certificado Citrix Gateway não está na lista de AC do sistema. Se essa configuração estiver ON, o sistema operacional Android valida o certificado Citrix Gateway. Se a validação falhar, a conexão não será permitida. O valor padrão é ON.

The screenshot shows the 'Policy Information' configuration page. On the left, there is a sidebar titled 'Android Enterprise Managed Configurations' with a list of steps: 1 Policy Info (highlighted), 2 Platforms (with a 'Clear All' link), 3 Assignment, and a checked checkbox for 'Android Enterprise'. The main area is titled 'Policy Information' and shows 'Policy Name' as 'Citrix SSO VPN Configuration' and 'Description' as 'VPN Profile'. A 'Next >' button is located at the bottom right of the main area.

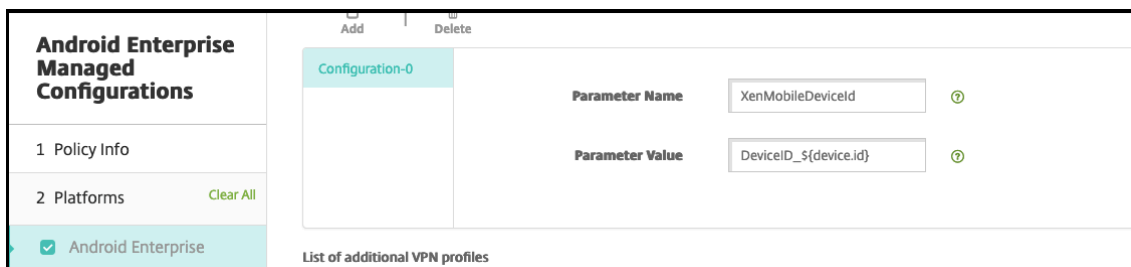
6. Opcionalmente, crie parâmetros personalizados. Os parâmetros personalizados **XenMobileDeviceID** e **UserAgent** são suportados. Selecione a configuração VPN atual e clique em **Adicionar**.

The screenshot shows the 'Custom Parameters' configuration page. On the left, there is a sidebar titled 'Android Enterprise Managed Configurations' with a list of steps: 1 Policy Info, 2 Platforms (with a 'Clear All' link), and a checked checkbox for 'Android Enterprise'. The main area is titled 'Custom Parameters' and shows 'Add' and 'Delete' buttons. A 'Configuration' button is highlighted, and a message says 'Click 'Add' to add new Configuration'.

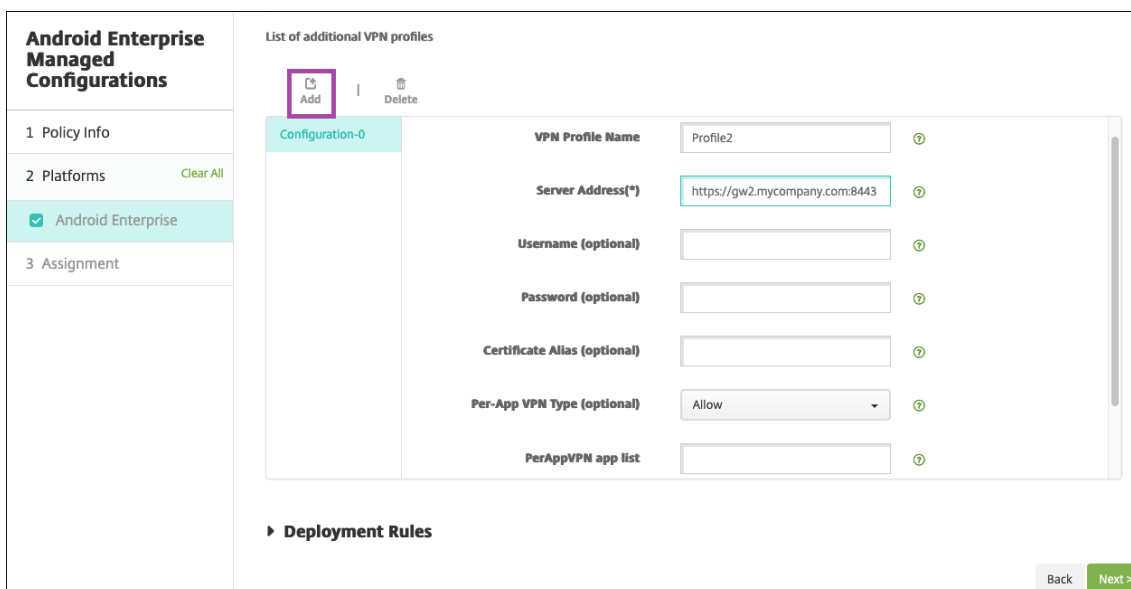
- a) Crie um parâmetro personalizado:

- **Nome do parâmetro.** Digite **XenMobileDeviceId**. Esse campo é o ID do dispositivo a ser usado para a Verificação de Acesso à Rede com base no registro do dispositivo no XenMobile. Se o XenMobile registrar e gerenciar o dispositivo, a conexão VPN será permitida. Caso contrário, a autenticação será negada no momento do estabelecimento da VPN.

- **Valor do parâmetro** Para o XenMobile determinar o estado de registro e gerenciamento dos dispositivos, o valor de XenMobileDeviceId é definido como `DeviceID_${ device.id }`.



- a) Para criar outro parâmetro personalizado, clique em **Adicionar** novamente. Crie o parâmetro personalizado.
 - **Nome do parâmetro.** Digite **UserAgent**. O texto é anexado ao cabeçalho HTTP do User-Agent para executar uma verificação extra no Citrix Gateway. O valor desse texto é anexado ao cabeçalho HTTP do User-Agent pelo aplicativo Citrix SSO enquanto se comunica com o Citrix Gateway.
 - **Valor do parâmetro.** Digite o texto que deseja anexar ao cabeçalho HTTP do User-Agent. O texto deve estar em conformidade com as especificações HTTP do User-Agent.
7. Opcionalmente, crie mais configurações de perfil VPN. Clique em **Adicionar** abaixo da lista de configurações. Uma nova configuração aparece na lista. Selecione a nova configuração e repita a etapa 5 e, opcionalmente, a etapa 6.



8. Quando você tiver criado todos os perfis VPN desejados, clique em **Avançar**.
9. Configure regras de implantação para essa configuração gerenciada para o Citrix SSO.

10. Clique em **Salvar**.

A configuração gerenciada para o Citrix SSO agora aparece na sua lista de políticas de dispositivo configuradas.

Para habilitar “sempre conectada” para os perfis VPN que você configurou, defina a [Políticas de dispositivo das opções de XenMobile](#).

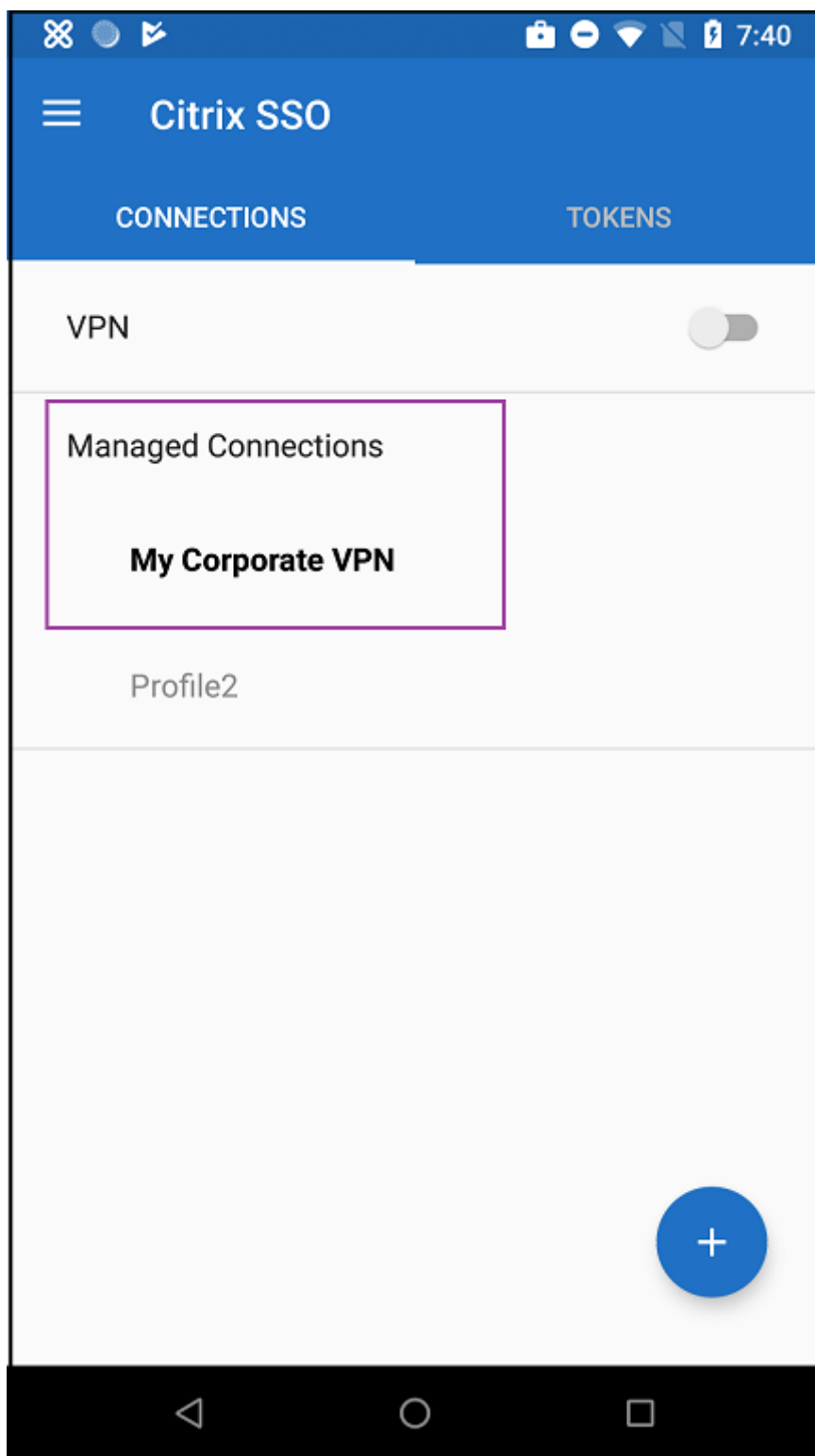
Nota:

O Citrix Secure Hub 19.5.5 ou posterior é necessário para VPN sempre conectada para Android Enterprise.

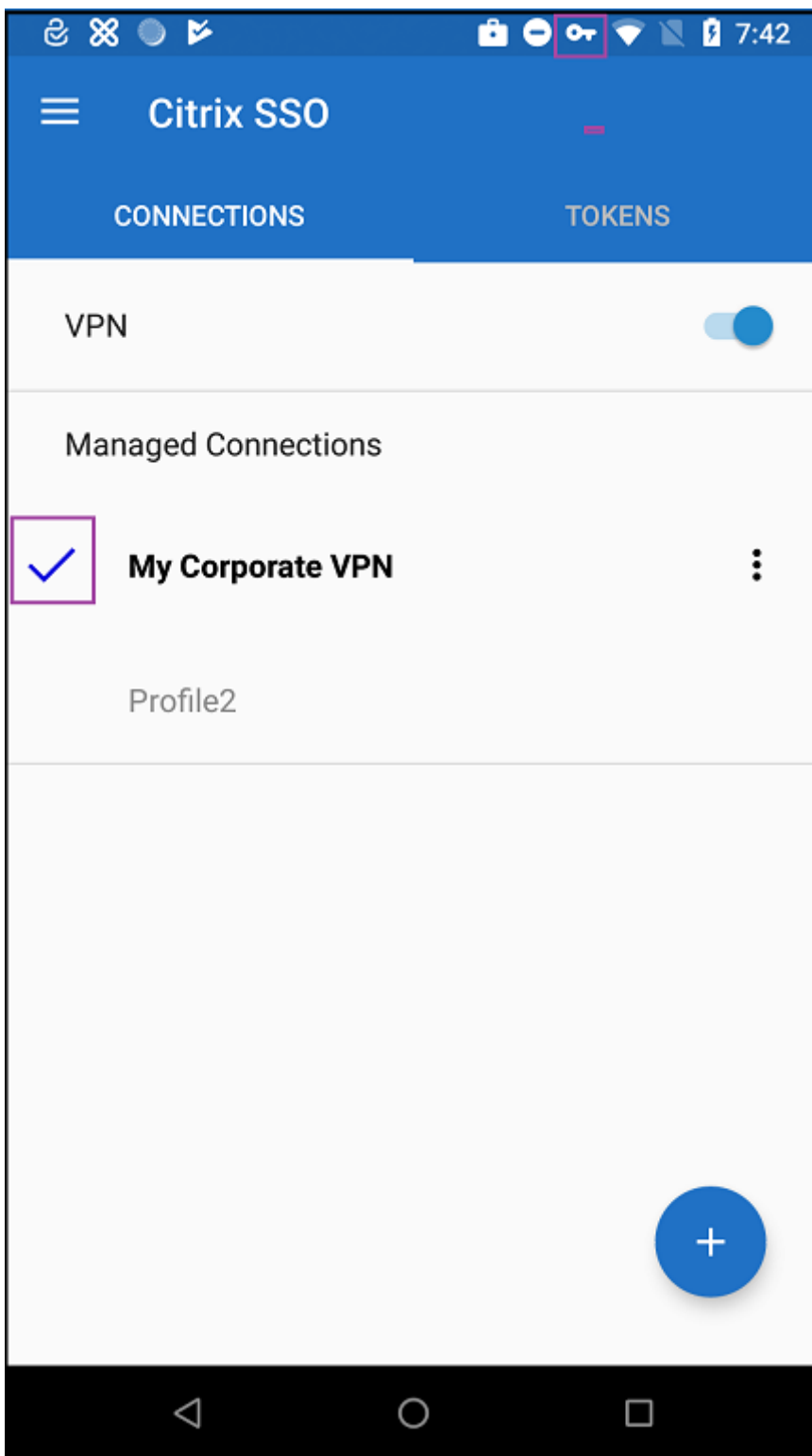
Acessar perfis VPN a partir do dispositivo

Para acessar os perfis VPN criados, os usuários do Android Enterprise instalam o Citrix SSO da Google Play Store.

O perfil ou perfis VPN que você configurou são exibidos na área **Conexões gerenciadas** do aplicativo. Os usuários tocam no perfil VPN para se conectarem usando esse perfil VPN.



Após os usuários terem se autenticado e conectado, uma marca de seleção será exibida ao lado do perfil VPN. O ícone de chave indica que a VPN está conectada.



Gerenciar dispositivos Zebra Android usando Zebra OEMConfig

Gerencie dispositivos Zebra Android usando a ferramenta administrativa Zebra Technologies OEMConfig. Para obter informações sobre o aplicativo Zebra OEMConfig, consulte o [Site da Zebra Technologies](#).

XenMobile suporta Zebra OEMConfig versão 9.2 e superior. Para obter informações sobre os requisitos de sistema para instalar o Zebra OEMConfig em dispositivos, consulte [Configuração do OEMConfig](#) no site da Zebra Technologies.

Comece adicionando o aplicativo Zebra OEMConfig ao console XenMobile como um aplicativo da loja Google Play. Consulte [Acrescentar um aplicativo de loja de aplicativos pública](#).

Criar uma configuração gerenciada do Android Enterprise para o aplicativo Zebra OEMConfig

Configure a política de dispositivo de configurações gerenciadas do Android Enterprise para o aplicativo Zebra OEMConfig. A política se aplica aos dispositivos Zebra que têm o aplicativo Zebra OEMConfig instalado e a política implantada.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. Clique em **Add**.
2. Selecione **Android Enterprise**. Clique em **Configurações gerenciadas do Android Enterprise**.
3. Quando a janela **Selecionar ID do aplicativo** for exibida, escolha **ZebraOEMConfig powered by MX** na lista e clique em **OK**.
4. Digite um nome e uma descrição para a configuração Zebra OEMConfig. Clique em **Avançar**.
5. Digite um nome para a configuração Zebra OEMConfig.
6. Configure os parâmetros disponíveis. Por exemplo:
 - Para desativar a câmera na parte frontal do dispositivo, selecione **Camera Configuration** e defina **Use of Front Camera** como **Off**.
 - Para alterar o formato de hora dos dispositivos, selecione **Click Configuration** e defina **Time Format** como **12** para formato de 12 horas ou **24** para formato de 24 horas.

Para obter uma lista e descrições de todas as configurações disponíveis, consulte [Configurações gerenciadas Zebra](#) no site da Zebra Technologies.

1. Opcionalmente, crie mais configurações Zebra OEMConfig. Clique em **Adicionar** abaixo da lista de configurações. Uma nova configuração aparece na lista. Selecione a nova configuração e configure os parâmetros.
2. Após criar todas as configurações Zebra OEMConfig desejadas, clique em **Avançar**.
3. Configure regras de implantação para essa configuração gerenciada para o Zebra OEMConfig.
4. Clique em **Salvar**.

Permissões do aplicativo Enterprise Android

November 30, 2020

Você pode configurar como as solicitações para aplicativos Android Enterprise nos perfis de trabalho lidam com o que o Google chama de permissões “perigosas”. Você controla se o usuário é solicitado a conceder ou negar a solicitação de permissão do aplicativo. Este recurso se aplica a dispositivos que executam o Android 7.0 e posterior.

O Google define permissões perigosas como permissões que dão ao aplicativo acesso a dados ou recursos que envolvem as informações particulares do usuário ou que podem afetar os dados armazenados do usuário ou a operação de outros aplicativos. Por exemplo, a capacidade de ler os contatos do usuário é uma permissão perigosa.

Você pode configurar um estado global que controla o comportamento de todas as solicitações de permissões perigosas para os aplicativos do Android Enterprise em perfis de trabalho. Você também pode controlar o comportamento de solicitações de permissões perigosas para grupos de permissão individual, conforme definido pelo Google, para cada aplicativo. Essas configurações individuais substituem o estado global.

Para obter informações sobre como o Google define grupos de permissões, consulte “Grupos de permissões” neste [Guia de desenvolvedores do Android](#).

Por padrão, os usuários são solicitados a conceder ou negar solicitações de permissões perigosas.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do Android Enterprise

Android for Work App Permissions

- 1 Policy Info
- 2 Platforms
- 2.1 Android for Work
- 3 Assignment

Android for Work App Permissions ✕

This policy lets you specify the behavior when Android for Work apps request dangerous permissions.

Global State * Prompt

Calendar

App *	Grant Status	Add
Gmail	Grant	+

Camera

App *	Grant Status	Add
WhatsApp Messenger	Deny	+

Contacts

App *	Grant Status	Add
Gmail	Prompt	+
WhatsApp Messenger	Deny	+

Location

App *	Grant Status	Add
		+

Microphone

App *	Grant Status	Add
		+

Back Next >

- **Estado global:** controla o comportamento de todas as solicitações de permissões perigosas. Na lista, clique em **Solicitar**, **Conceder** ou **Negar**.
 - **Solicitar:** os usuários são solicitados a conceder ou negar solicitações de permissões perigosas.
 - **Conceder:** todas as solicitações de permissões perigosas são concedidas. O usuário não é solicitado.
 - **Negar:** todas as solicitações de permissões perigosas são negadas. O usuário não é solicitado.

O padrão é **Solicitar**.

- Defina um comportamento individual para cada grupo de permissões, para cada aplicativo. Para configurar o comportamento de um grupo de permissões: clique em **Adicionar** e, em **Aplicativo**, escolha um aplicativo na lista. Se você configurar aplicativos do sistema Android Enterprise, clique em **Adicionar novo** e insira o nome do pacote de aplicativos que você ativou na política de dispositivo Restrições. Em Estado de concessão, escolha **Solicitar**, **Conceder** ou **Negar**. Esse estado de concessão substitui o estado global.
 - **Solicitar:** os usuários são solicitados a conceder ou negar solicitações de permissões perigosas desse grupo de permissões para este aplicativo.
 - **Conceder:** as solicitações de permissões perigosas desse grupo de permissões para este aplicativo são concedidas. O usuário não é solicitado.
 - **Negar:** solicitações de permissões perigosas deste grupo de permissões para este aplicativo são negadas. O usuário não é solicitado.

O padrão é **Solicitar**.

- Clique em **Salvar** ao lado do aplicativo e do estado de concessão.
- Para adicionar mais aplicativos ao grupo de permissões, clique em **Adicionar** novamente e repita essas etapas.
- Quando você terminar de definir os estados de concessão para todos os grupos de permissões desejados, clique em **Avançar**.

Política de dispositivo do APN

April 23, 2020

Você pode adicionar uma política de dispositivo de Nome de Ponto de Acesso (APN) personalizado a dispositivos iOS, Android e Windows Mobile/CE. Use essa política se sua organização não usar um APN de consumidor para conexão com a Internet de um dispositivo móvel. Uma política de APN determina as configurações usadas para conectar os seus dispositivos a um GPRS da operadora de telefonia específica. Essa configuração já está definida na maioria dos telefones mais recentes.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

The screenshot shows the 'APN Policy' configuration page. On the left, a sidebar lists '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'iOS', 'Android', and 'Windows Mobile/CE' are all checked. The main content area is titled 'APN Policy' and contains the following fields and options:

- APN ***: An empty text input field.
- User name**: A text input field containing 'administrator'.
- Password**: A text input field with masked characters (dots).
- Server proxy address**: An empty text input field.
- Server proxy port**: An empty text input field.
- Remove policy**: Two radio button options: 'Select date' (selected) and 'Duration until removal (in hours)'. Below the second option is a text input field with a calendar icon.

At the bottom right of the form, there are 'Back' and 'Next >' buttons.

- **APN:** digite o nome do ponto de acesso. Ele deve corresponder a um APN aceito pelo iOS, ou a política falhará.
- **Nome de usuário:** essa cadeia de caracteres especifica o nome de usuário desse APN. Se o nome do usuário estiver ausente, o dispositivo solicitará a cadeia de caracteres durante a instalação do perfil.

- **Senha:** A senha do usuário para este APN. Para fins de ofuscação, a senha é codificada. Se ela estiver ausente da carga, o dispositivo solicitará a senha durante a instalação do perfil.
- **Endereço do servidor proxy:** o endereço IP ou a URL do proxy do APN.
- **Porta do servidor proxy:** o número da porta do proxy do APN. Ele será necessário se você tiver inserido um endereço de servidor proxy.
- Em **Configurações de política**, ao lado de **Remover política**, clique em **Selecionar data** ou em **Duração até remoção (em horas)**.
 - Se você clicar em **Selecionar data**, clique no calendário para selecionar a data específica para remoção.
 - Na lista **Permitir que o usuário remova a política**, clique em **Sempre**, **Senha obrigatória** ou **Nunca**.
 - Se você clicar em **Senha obrigatória**, ao lado de **Senha de remoção**, digite a senha necessária.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do Android

The screenshot displays the 'APN Policy' configuration screen. On the left, a sidebar lists '1 Policy Info', '2 Platforms', and '3 Assignment'. Under 'Platforms', 'Android' is selected with a checkmark. The main content area shows the following fields: 'APN *' (empty), 'User name' (administrator), 'Password' (masked with dots), 'Server' (empty), 'APN type' (empty), 'Authentication type' (None), 'Server proxy address' (empty), 'Server proxy port' (empty), and 'MMSC' (empty). At the bottom right, there are 'Back' and 'Next >' buttons.

- **APN:** digite o nome do ponto de acesso. Ele deve corresponder a um APN aceito do Android, ou a política falhará.
- **Nome de usuário:** essa cadeia de caracteres especifica o nome de usuário desse APN. Se o nome do usuário estiver ausente, o dispositivo solicitará a cadeia de caracteres durante a instalação do perfil.

- **Senha:** A senha do usuário para este APN. Para fins de ofuscação, a senha é codificada. Se ela estiver ausente da carga, o dispositivo solicitará a senha durante a instalação do perfil.
- **Servidor:** essa configuração, que é anterior aos smartphones, geralmente está vazia. Ela faz referência a um servidor de gateway Wireless Application Protocol (WAP) para telefones que não puderam acessar ou renderizar sites da web comuns.
- **Tipo de APN:** essa configuração deve coincidir com o uso pretendido da operadora para o ponto de acesso. Trata-se de uma cadeia de caracteres separada por vírgulas de especificadores do serviço do APN e deve coincidir com as definições publicadas da operadora sem fio. Alguns exemplos:
 - *. Todo o tráfego passa por esse ponto de acesso.
 - mms. Todo o tráfego multimídia passa por esse ponto de acesso.
 - padrão. Todo o tráfego, incluindo multimídia, passa por esse ponto de acesso.
 - supl. A localização de plano de usuário segura é associada ao GPS assistido.
 - dun. A rede de Conexão discada está desatualizada e raramente deve ser usada.
 - hipri. Redes de alta prioridade.
 - fota. O firmware por rede celular é usado para receber as atualizações de firmware.
- **Tipo de autenticação:** na lista, clique no tipo de autenticação a ser usado. O padrão é Nenhum.
- **Endereço do servidor proxy:** o endereço IP ou a URL do proxy HTTP de APN da operadora.
- **Porta do servidor proxy:** o número da porta do proxy do APN. Ele será necessário se você tiver inserido um endereço de servidor proxy.
- **MMSC:** o endereço do Servidor de Gateway MMS fornecido pela operadora.
- **Endereço do proxy MMS (Multimedia Messaging Server):** esse é o servidor do serviço de mensagens multimídia do tráfego MMS. O MMS sucedeu o SMS para enviar mensagens maiores com conteúdo multimídia, como imagens ou vídeos. Esses servidores exigem protocolos específicos (como MM1, ... MM11).
- **Porta MMS:** a porta usada para o proxy MMS.

Configurações do Windows Mobile/CE

APN Policy	APN Policy
1 Policy Info	This policy creates a custom Access Point Name (APN) on the device. Use this policy if your organization does not use a consumer APN to connect to the Internet from a mobile device.
2 Platforms	<p>APN * <input type="text"/></p> <p>Network <input type="text" value="Built-in office"/></p> <p>User name <input type="text"/></p> <p>Password <input type="text"/></p>
<input type="checkbox"/> iOS <input type="checkbox"/> Android <input checked="" type="checkbox"/> Windows Mobile/CE	<p>► Deployment Rules</p>
3 Assignment	

- **APN:** digite o nome do ponto de acesso. Ele deve corresponder a um APN aceito do Android, ou a política falhará.
- **Rede:** na lista, clique no tipo de rede a ser usada. O padrão é **Escritório interno**.

- **Nome de usuário:** essa cadeia de caracteres especifica o nome de usuário desse APN. Se o nome do usuário estiver ausente, o dispositivo solicitará a cadeia de caracteres durante a instalação do perfil.
- **Senha:** A senha do usuário para este APN. Para fins de ofuscação, a senha é codificada. Se ela estiver ausente da carga, o dispositivo solicitará a senha durante a instalação do perfil.

Política de dispositivo de acesso aos aplicativos

April 23, 2020

A política de dispositivo de acesso aos aplicativos no XenMobile permite definir uma lista de aplicativos cuja instalação é necessária no dispositivo, que podem ser instalados no dispositivo ou que não devem ser instalados no dispositivo. Você pode criar uma ação automatizada para reagir à conformidade do dispositivo com essa lista de aplicativos. Você pode criar políticas de acesso aos aplicativos para dispositivos iOS, Android e Windows Mobile/CE.

Você pode configurar somente um tipo de política de acesso por vez. Você pode adicionar uma política de qualquer lista de aplicativos necessários, aplicativos sugeridos ou aplicativos proibidos, mas não uma mistura na mesma política de acesso aos aplicativos. Se você criar uma política para cada tipo de lista, recomendamos que você nomeie cada política cuidadosamente, para que saiba qual política no XenMobile se aplica à qual lista de aplicativos.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações da plataforma

- **Política de acesso:** clique em **Obrigatório**, **Sugerido** ou **Proibido**. O padrão é **Obrigatório**.
- Para adicionar um ou mais aplicativos à lista, clique em **Adicionar** e faça o seguinte:
 - **Nome do aplicativo:** insira um nome de aplicativo.
 - **Identificador de aplicativo:** insira um identificador de aplicativo opcional.
 - Clique em **Salvar** ou em **Cancelar**.
 - Repita essas etapas para cada aplicativo que você deseja adicionar.

Política de dispositivo de atributos de aplicativo

April 23, 2020

A política de dispositivos de atributos de aplicativo permite especificar atributos, como um ID do pacote do aplicativo gerenciado ou um identificador de VPN por aplicativo, para dispositivos iOS.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

App Attributes Policy	Policy Information
1 Policy Info	This policy lets you specify the attributes you want to add to apps on iOS devices.
2 Platforms	Policy Name * <input type="text"/>
<input checked="" type="checkbox"/> iOS	Description <input type="text"/>
3 Assignment	

- **ID de pacote de aplicativos gerenciados:** na lista, clique em um ID de pacote de aplicativo ou em **Adicionar novo**.
 - Se você clicar em **Adicionar novo**, digite o código do pacote de aplicativos no campo exibido.
- **Identificador VPN por aplicativo:** na lista, clique no identificador VPN por aplicativo.

Política de dispositivo de configuração de aplicativo

April 23, 2020

Você pode configurar remotamente aplicativos que suportam configuração gerenciada implantando:

- Um arquivo de configuração XML (chamado de lista de propriedades, ou plist) nos dispositivos iOS
- Ou pares de chave/valor para dispositivos de telefone, tablet ou desktop do Windows 10.

A configuração especifica várias definições e comportamentos no aplicativo. O XenMobile envia a configuração para os dispositivos quando o usuário instala o aplicativo. As definições e os comportamentos reais que você pode configurar dependem do aplicativo e estão além do escopo deste artigo.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

<p>App Configuration Policy</p> <p>1 Policy Info</p> <p>2 Platforms</p> <p><input checked="" type="checkbox"/> iOS</p> <p><input checked="" type="checkbox"/> Windows Phone</p> <p><input checked="" type="checkbox"/> Windows Desktop/Tablet</p> <p>3 Assignment</p>	<p>App Configuration Policy</p> <p>This policy lets you specify key/value configuration parameters for an app. XenMobile pushes the app configuration to the device when the app gets installed. For iOS devices, after you enter the dictionary content, you can check the syntax.</p> <p>Identifier * <input type="text" value="Make a selection"/></p> <p>Dictionary content *</p> <div style="border: 1px solid #ccc; height: 80px; width: 100%;"></div> <p><input type="button" value="Check Dictionary"/></p> <p>► Deployment Rules</p>
--	--

- **Identificador:** na lista, clique no aplicativo que você deseja configurar ou em **Adicionar novo** para adicionar um novo aplicativo à lista.
 - Se você clicar em **Adicionar novo**, digite o identificador do aplicativo no campo exibido.
- **Conteúdo do dicionário:** digite ou copie e cole as informações de configuração da lista de propriedades XML (plist).
- Clique em **Verificar dicionário**. O XenMobile verifica o XML. Se não houver nenhum erro, você verá **XML válido** abaixo da caixa de conteúdo. Se algum erro de sintaxe for exibido abaixo da caixa de conteúdo, você deverá corrigi-lo antes de continuar.

Configurações do Windows Phone ou Desktop/Tablet

<p>App Configuration Policy</p> <p>1 Policy Info</p> <p>2 Platforms</p> <p><input type="checkbox"/> iOS</p> <p><input checked="" type="checkbox"/> Windows Phone</p> <p><input checked="" type="checkbox"/> Windows Desktop/Tablet</p> <p>3 Assignment</p>	<p>App Configuration Policy</p> <p>This policy lets you specify key/value configuration parameters for an app. XenMobile pushes the app configuration to the device when the app gets installed.</p> <p><input type="text" value="Make a selection"/></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 40%;">Parameter name *</td> <td style="width: 40%;">Value *</td> <td style="width: 20%; text-align: right;"><input type="button" value="Add"/></td> </tr> </table> <p>► Deployment Rules</p>	Parameter name *	Value *	<input type="button" value="Add"/>
Parameter name *	Value *	<input type="button" value="Add"/>		

<p>App Configuration Policy</p> <p>1 Policy Info</p> <p>2 Platforms</p> <p><input type="checkbox"/> iOS</p> <p><input type="checkbox"/> Windows Phone</p> <p><input checked="" type="checkbox"/> Windows Desktop/Tablet</p> <p>3 Assignment</p>	<p>App Configuration Policy</p> <p>This policy lets you specify key/value configuration parameters for an app. XenMobile pushes the app configuration to the device when the app gets installed.</p> <p><input type="text" value="Make a selection"/></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 40%;">Parameter name *</td> <td style="width: 40%;">Value *</td> <td style="width: 20%; text-align: right;"><input type="button" value="Add"/></td> </tr> </table> <p>► Deployment Rules</p>	Parameter name *	Value *	<input type="button" value="Add"/>
Parameter name *	Value *	<input type="button" value="Add"/>		

- Na lista **Fazer uma seleção**, clique no aplicativo que você deseja configurar ou em **Adicionar novo** para adicionar um novo aplicativo à lista.
 - Se você clicar em **Adicionar novo**, digite o nome da família do pacote no campo exibido.
- Para cada parâmetro de configuração que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
 - **Nome do parâmetro:** Digite o nome de chave para uma configuração de aplicativo para o dispositivo Windows. Para obter informações sobre as configurações de aplicativo Windows, consulte a documentação da Microsoft.
 - **Valor:** Digite o valor do parâmetro especificado.
 - Clique em **Adicionar** para adicionar o parâmetro ou em **Cancelar** para cancelar a adição do parâmetro.

Política de dispositivo de inventário de aplicativos

July 10, 2020

A política de inventário de aplicativos permite que você colete um inventário dos aplicativos em dispositivos gerenciados. O XenMobile pode então comparar o inventário com todas as políticas de acesso aos aplicativos implantadas nesses dispositivos. Dessa forma, você pode detectar aplicativos que aparecem em uma lista de permissão ou bloqueio de aplicativo e tomar as devidas providências.

Você pode criar as políticas de acesso a aplicativos para dispositivos iOS, macOS, Android, Android Enterprise, Windows Desktop/Tablet, Windows Phone ou Windows Mobile/CE.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações da plataforma

App Inventory Policy

This policy lets you collect an inventory of the apps on managed devices so you can detect apps that appear on an app blacklist or whitelist and take action accordingly.

ios

► Deployment Rules

Back Next >

- Para cada plataforma que você selecionar, mantenha a configuração padrão ou altere a configuração para **O**. O padrão é **On**.

Política de dispositivo de bloqueio de aplicativo

July 10, 2020

A Política de dispositivo de bloqueio de aplicativo define uma lista de aplicativos que podem ser executados em um dispositivo ou uma lista de aplicativos cuja execução é bloqueada em um dispositivo. Você pode configurar essa política para os dispositivos Android e iOS, mas a maneira exata pela qual a política funciona é diferente em cada plataforma. Por exemplo, você não pode bloquear vários aplicativos em um dispositivo iOS.

Da mesma forma, em dispositivos iOS, você pode selecionar apenas um aplicativo iOS por política. Isso significa que os usuários só são capazes de usar o dispositivo para executar um único aplicativo. Eles não podem realizar outras atividades no dispositivo, exceto as opções permitidas especificamente quando a política de bloqueio de aplicativo é aplicada.

Além disso, os dispositivos iOS devem ser supervisionados para enviar por push políticas de bloqueio de aplicativo.

Embora a política de dispositivo funcione na maioria dos dispositivos Android L e M, o bloqueio de aplicativo não funciona em dispositivos Android N ou de versões posteriores porque o Google não utilizava mais a API.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

App Lock Policy	App Lock Policy
1 Policy Info	This policy lets you define a list of apps that are allowed to run on a device, or a list of apps that are blocked from running on a device.
2 Platforms	<p>App bundle ID * <input type="text" value="Make a selection"/></p> <p>Options</p> <p>Disable touch screen <input checked="" type="checkbox"/> ON iOS 7.0+</p> <p>Disable device rotation sensing <input type="checkbox"/> OFF iOS 7.0+</p> <p>Disable volume buttons <input type="checkbox"/> OFF iOS 7.0+</p> <p>Disable ringer switch <input type="checkbox"/> OFF iOS 7.0+</p> <p>Disable sleep/wake button <input type="checkbox"/> OFF iOS 7.0+</p> <p>Disable auto lock <input type="checkbox"/> OFF iOS 7.0+</p> <p>Enable VoiceOver <input type="checkbox"/> OFF iOS 7.0+</p> <p>Enable zoom <input type="checkbox"/> OFF iOS 7.0+</p>
<input checked="" type="checkbox"/> iOS	
<input checked="" type="checkbox"/> Android	
3 Assignment	

- **ID do pacote de aplicativos:** na lista, clique no aplicativo ao qual esta política se aplica ou clique em **Adicionar novo** para adicionar um novo aplicativo à lista. Se você selecionar **Adicionar novo**, digite o nome do aplicativo no campo exibido.
- **Opções:** cada uma das opções a seguir se aplica somente ao iOS 7.0 ou versões posteriores. Em cada opção, o padrão é **O**, exceto para a opção Desativar tela de toque, que é **I** por padrão.
 - Desativar tela de toque
 - Desativar sensor de rotação do dispositivo
 - Desativar botões de volume
 - Desativar botão de toque

Quando Desativar botão de toque está **I**, o comportamento do toque depende da posição do botão quando foi desativado pela primeira vez.
 - Desativar botão soneca/despertador
 - Desativar bloqueio automático
 - Desativar VoiceOver
 - Ativar zoom
 - Ativar inversão de cores
 - Ativar o AssistiveTouch
 - Ativar fala de seleção
 - Ativar áudio mono
- **Opções ativadas pelo usuário:** cada uma das opções a seguir se aplica somente ao iOS 7.0 ou

versões posteriores. Para cada opção, o padrão é **O**.

- Permitir ajuste do VoiceOver
- Permitir ajuste do zoom
- Permitir ajuste da inversão de cores
- Permitir ajuste do AssistiveTouch

• Configurações de política

- **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do Android

Nota:

Você não pode bloquear o aplicativo de configurações do Android usando a política de dispositivo de bloqueio de aplicativo.

The screenshot shows the 'App Lock Policy' configuration window. On the left, a sidebar lists '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', 'Android' is selected with a checkmark, while 'iOS' is unselected. The main area is titled 'App Lock Policy' and contains the following settings:

- Lock message:** An empty text input field.
- Unlock password:** An empty text input field.
- Prevent uninstall:** A toggle switch set to 'OFF'.
- Lock screen:** An empty text input field with a green 'Browse' button to its right.
- Enforce:** Two radio buttons: 'Blacklist' (selected) and 'Whitelist'.
- Apps:** A section with a search bar labeled 'App name' and an 'Add' button.

• Parâmetros de bloqueio de aplicativo

- **Mensagem de bloqueio:** digite a mensagem que os usuários veem quando tentam abrir um aplicativo bloqueado.
- **Senha de desbloqueio:** digite a senha para desbloquear o aplicativo.
- **Impedir desinstalação:** selecione se os usuários têm permissão para desinstalar aplicativos. O padrão é **Off**.
- **Tela de bloqueio:** selecione a imagem que aparece na tela de bloqueio do dispositivo clicando em Procurar e navegando para a localização do arquivo.
- **Impor:** clique em **Lista negra** para criar uma lista de aplicativos que não têm permissão para serem executados em dispositivos ou clique em **Lista branca** para criar uma lista de

aplicativos que podem ser executados em dispositivos.

Nota:

O console XenMobile Server inclui os termos “lista negra” e “lista branca”. Estamos alterando esses termos em uma próxima versão para “lista de bloqueio” e “lista de permissão”.

- **Aplicativos:** clique em **Adicionar** e faça o seguinte:
 - **Nome do aplicativo:** na lista, clique no nome do aplicativo para adicioná-lo às listas de permissão ou bloqueio, ou clique em **Adicionar novo** para adicionar um novo aplicativo à lista de aplicativos disponíveis.
 - Se você selecionar **Adicionar novo**, digite o nome do aplicativo no campo exibido.
 - Clique em **Salvar** ou em **Cancelar**.
 - Repita essas etapas para cada aplicativo que você deseja adicionar às listas de permissão ou bloqueio.

Política de dispositivo de uso de rede de aplicativos

April 23, 2020

Você pode definir regras de uso de rede para especificar como os aplicativos gerenciados usam redes, como redes de dados celulares, nos dispositivos iOS. As regras se aplicam somente aos aplicativos gerenciados. Aplicativos gerenciados são aqueles que você implanta nos dispositivos dos usuários usando o XenMobile. Eles não incluem aplicativos que os usuários baixaram diretamente para os dispositivos deles sem que fossem implantados usando o XenMobile ou aqueles já instalados nos dispositivos quando eles foram registrados no XenMobile.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

- **Permitir dados celulares de roaming:** selecione se os aplicativos especificados podem usar uma conexão de dados celulares enquanto estiverem em roaming. O padrão é **Off**.
- **Permitir dados celulares:** selecione se os aplicativos especificados podem usar uma conexão de dados celulares. O padrão é **Off**.
- **Correspondências de identificador de aplicativo:** para cada aplicativo que você desejar adicionar à lista, clique em **Adicionar** e faça o seguinte:
 - **Identificador de aplicativo:** insira um identificador de aplicativo.
 - Clique em **Salvar** para salvar o aplicativo na lista ou em **Cancelar** para não salvar.

Política de dispositivo de notificações de aplicativo

April 23, 2020

A política de notificações de aplicativos permite controlar como os usuários de iOS recebem notificações de aplicativos especificados. Essa política é compatível em dispositivos com o iOS 9.3 ou versões posteriores.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

App Bundle Identifier	Allow Notifications	Show in Notification Center	Badge App Icon	Sounds	Show on Lock Screen	Show in Car Play	Enable Critical Alert	Unlocked Alert Style	Save	Cancel
App Store	ON	ON	ON	ON	ON	ON	OFF	Alerts		

Policy Settings

Remove policy: Select date
 Duration until removal (in hours)

Allow user to remove policy: Always

Profile scope: System (iOS 9.3+)

- **Identificador do pacote de aplicativos:** especifique os aplicativos aos quais você deseja aplicar essa política.
- **Permitir notificações:** selecione **I** para permitir notificações.
- **Mostrar no Centro de notificação:** selecione **I** para mostrar notificações no Centro de Notificação dos dispositivos dos usuários.
- **Ícone de Aviso nos Aplicativos:** selecione **I** para mostrar um ícone de aviso do aplicativo com as notificações.
- **Sons:** selecione **I** para incluir sons com as notificações.
- **Mostrar na tela de bloqueio:** selecione **I** para mostrar notificações na tela de bloqueio dos dispositivos do usuário.
- **Exibir em Car Play:** se **I**, as notificações serão exibidas no Apple CarPlay. Disponível no iOS 12 e posterior. O padrão é **Ativado**.
- **Ativar alerta crítico:** se **I**, um aplicativo pode marcar uma notificação como uma notificação crítica que ignora as configurações de Não Perturbe e de toque. Disponível no iOS 12 e posterior. O padrão é **Desativado**.
- **Estilo de alerta desbloqueado:** na lista, selecione **Nenhum**, **Banner** ou **Alertas** para configurar a aparência dos alertas desbloqueados.

- **Configurações de política**

- **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.
- **Escopo do perfil:** selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Esta opção está disponível apenas no iOS 9.3 e posterior.

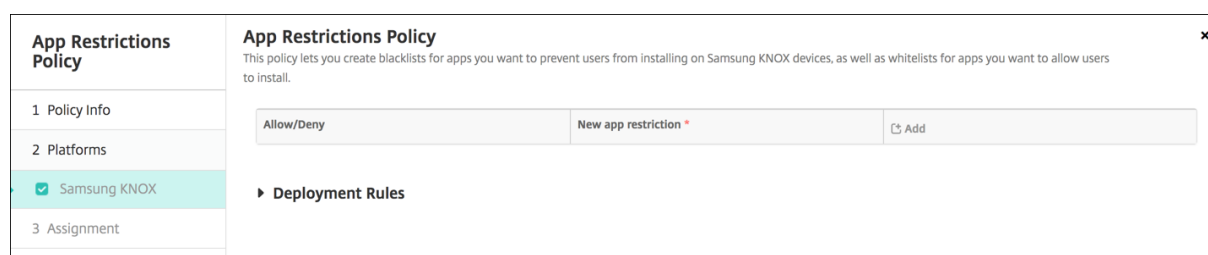
Política de dispositivo de restrições de aplicativo

July 10, 2020

Você pode criar listas de bloqueio de aplicativos que deseja impedir que os usuários instalem em dispositivos Samsung KNOX. Você também pode criar listas de permissão de aplicativos que deseja permitir que os usuários instalem.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do Samsung KNOX



Para cada aplicativo que você desejar adicionar à lista Permitir ou Negar, clique em **Adicionar** e faça o seguinte:

- **Permitir ou negar:** selecione se os usuários têm permissão para instalar o aplicativo.
- **Nova restrição de aplicativo:** digite o ID de pacote do aplicativo; por exemplo, com.kmdm.af.crackle.
- Clique em **Salvar** para salvar o aplicativo na lista Permitir ou Negar ou clique em **Cancelar** para não salvar.

Política de dispositivo de encapsulamento de aplicativo

April 23, 2020

Importante:

A política de encapsulamento de aplicativo é usado somente para suporte remoto. Para obter informações sobre o Suporte Remoto, consulte [Opções de suporte e suporte remoto](#). O Remote Support não está mais disponível para novos clientes desde 1º de janeiro de 2019. Os clientes existentes podem continuar a usar o produto, no entanto, a Citrix não fornecerá melhorias ou correções.

Os túneis de aplicativos foram projetados para aumentar a continuidade do serviço e a confiabilidade de transferência de dados de seus aplicativos móveis. Os túneis de aplicativo definem os parâmetros de proxy entre o componente de cliente de qualquer aplicativo do dispositivo móvel e o componente de servidor de aplicativos. Você também pode usar os túneis de aplicativo para criar túneis de suporte remoto para um dispositivo a fim de oferecer suporte ao gerenciamento. Você pode configurar a política de encapsulamento de aplicativo para dispositivos Android e Windows Mobile/CE.

Qualquer tráfego de aplicativo enviado por meio de um túnel definido nesta política passa pelo XenMobile antes de ser redirecionado para o servidor que executa o aplicativo.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do Android

Tunnel Policy	Tunnel Policy
1 Policy Info	This policy lets you configure an app tunnel. While doing so, you can choose if the tunnel will be used for the remote support app.
2 Platforms	<p>Use this tunnel for remote support <input type="checkbox"/> OFF</p> <p>Connection configuration</p> <p>Connection initiated by <input type="text" value="Device"/> ⓘ</p> <p>Maximum connections per device * <input type="text" value="1"/> ⓘ</p> <p>Define connection time out <input type="checkbox"/> OFF ⓘ</p> <p>Block cellular connections passing by this tunnel <input type="checkbox"/> OFF ⓘ</p> <p>App device parameters</p> <p>Client port * <input type="text"/> ⓘ</p> <p>App server parameters</p> <p>IP address or server name * <input type="text"/></p> <p>Server port * <input type="text"/></p>
<input checked="" type="checkbox"/> Android	
<input checked="" type="checkbox"/> Windows Mobile/CE	
3 Assignment	

- **Usar este túnel para suporte remoto:** selecione se o túnel será usado para suporte remoto.

As etapas de configuração são diferentes, dependendo se você selecionou o suporte remoto.

- Se você não selecionar o suporte remoto, faça o seguinte:
 - **Conexão iniciada por:** clique em **Dispositivo** ou **Servidor** para especificar a origem que inicia a conexão.
 - **Máximo de conexões por dispositivo:** digite um número para especificar quantas conexões TCP simultâneas o aplicativo pode estabelecer. Esse campo só se aplica às conexões iniciadas pelo dispositivo.
 - **Definir o tempo limite de conexão:** selecione se deseja definir um período de tempo durante o qual um aplicativo pode ficar ocioso antes do túnel ser fechado.
 - * **Tempo limite de conexão:** se você configurar **Definir o tempo limite de conexão** como **Ativado**, digite o período de tempo em segundos durante o qual um aplicativo pode ficar ocioso antes do túnel ser fechado.
 - **Bloquear conexões celulares que passam por este túnel:** selecione se o túnel está bloqueado durante o roaming.

Nota:

Conexões Wi-Fi e USB não serão bloqueadas.

- **Porta do cliente:** digite o número da porta. Na maioria dos casos, esse valor é o mesmo para a porta do servidor.
- **Endereço IP ou nome do servidor:** digite o endereço IP ou nome do servidor do aplicativo. Esse campo só se aplica às conexões iniciadas pelo dispositivo.
- **Porta do servidor:** digite o número de porta do servidor.
- Se você selecionar o suporte remoto, faça o seguinte:
 - **Usar este túnel para suporte remoto:** defina como **Ativado**.
 - **Definir o tempo limite de conexão:** selecione se deseja definir um período de tempo durante o qual um aplicativo pode ficar ocioso antes do túnel ser fechado.
 - * **Tempo limite de conexão:** se você configurar **Definir o tempo limite de conexão** como **Ativado**, digite o período de tempo em segundos durante o qual um aplicativo pode ficar ocioso antes do túnel ser fechado.
 - **Usar conexão SSL:** selecione se deseja usar uma conexão SSL segura para este túnel.
 - **Bloquear conexões celulares que passam por este túnel:** selecione se o túnel está bloqueado durante o roaming. Esta configuração não bloqueia conexões WiFi e USB.

Configurações do Windows Mobile/CE

Tunnel Policy	Tunnel Policy
1 Policy Info	This policy lets you configure an app tunnel. While doing so, you can choose if the tunnel will be used for the remote support app.
2 Platforms	<p>Use this tunnel for remote support <input type="checkbox"/> OFF</p> <p>Connection configuration</p> <p>Connection initiated by Device <input type="text"/> ?</p> <p>Protocol Generic TCP <input type="text"/> ?</p> <p>Maximum connections per device * 1 <input type="text"/> ?</p> <p>Define connection time out OFF <input type="text"/> ?</p> <p>Block cellular connections passing by this tunnel OFF <input type="text"/> ?</p> <p>App device parameters</p> <p>Redirect to XenMobile Through app settings <input type="text"/></p> <p>Client port * <input type="text"/> ?</p> <p>App server parameters</p> <p>IP address or server name * <input type="text"/></p>
<input type="checkbox"/> Android <input checked="" type="checkbox"/> Windows Mobile/CE	
3 Assignment	

- **Usar este túnel para suporte remoto:** selecione se o túnel será usado para suporte remoto.

As etapas de configuração são diferentes, dependendo se você selecionou o suporte remoto.

- Se você não selecionar o suporte remoto, faça o seguinte:
 - **Conexão iniciada por:** clique em **Dispositivo** ou **Servidor** para especificar a origem que inicia a conexão.
 - **Protocolo:** na lista, clique no protocolo a ser usado. O padrão é o **TCP genérico**.
 - **Máximo de conexões por dispositivo:** digite um número para especificar quantas conexões TCP simultâneas o aplicativo pode estabelecer. Esse campo só se aplica às conexões iniciadas pelo dispositivo.
 - **Definir o tempo limite de conexão:** selecione se deseja definir um período de tempo durante o qual um aplicativo pode ficar ocioso antes do túnel ser fechado.
 - * **Tempo limite de conexão:** se você configurar **Definir o tempo limite de conexão** como **Ativado**, digite o período de tempo em segundos durante o qual um aplicativo pode ficar ocioso antes do túnel ser fechado.
 - **Bloquear conexões celulares que passam por este túnel:** selecione se o túnel está bloqueado durante o roaming.

Nota:
Conexões Wi-Fi e USB não serão bloqueadas.
 - **Redirecionar para o XenMobile:** na lista, clique na opção de conexão do dispositivo ao XenMobile. O padrão é **Através de configurações de aplicativo**.
 - * Se você selecionar **Usando um alias local**, digite o alias no **Alias local**. O padrão é

localhost.

- * Se você selecionar **Um intervalo de endereços IP**, digite o endereço IP inicial em **Intervalo de endereços IP de** e digite o endereço IP final em **Intervalo de endereços IP para**.
- **Porta do cliente:** digite o número da porta. Na maioria dos casos, esse valor é o mesmo para a porta do servidor.
- **Endereço IP ou nome do servidor:** digite o endereço IP ou nome do servidor do aplicativo. Esse campo só se aplica às conexões iniciadas pelo dispositivo.
- **Porta do servidor:** digite o número de porta do servidor.
- Se você selecionar o suporte remoto, faça o seguinte:
 - **Usar este túnel para suporte remoto:** defina como **Ativado**.
 - **Definir o tempo limite de conexão:** selecione se deseja definir um período de tempo durante o qual um aplicativo pode ficar ocioso antes do túnel ser fechado.
 - * **Tempo limite de conexão:** se você configurar **Definir o tempo limite de conexão** como **Ativado**, digite o período de tempo em segundos durante o qual um aplicativo pode ficar ocioso antes do túnel ser fechado.
 - **Usar conexão SSL:** selecione se deseja usar uma conexão SSL segura para este túnel.
 - **Bloquear conexões celulares que passam por este túnel:** selecione se o túnel está bloqueado durante o roaming. As conexões Wi-Fi e USB não são bloqueadas.

Política de dispositivo de desinstalação de aplicativo

April 23, 2020

Você pode criar uma política de desinstalação de aplicativo para as plataformas iOS, Android, Samsung KNOX, Android Enterprise, Windows Desktop/Tablet e Windows Mobile/CE. Uma política de desinstalação de aplicativo permite que você remova aplicativos dos dispositivos do usuário por uma série de razões. Talvez você não deseje mais oferecer compatibilidade com determinados aplicativos, sua empresa pode desejar substituir os aplicativos existentes por aplicativos semelhantes de diferentes fornecedores e assim por diante.

Os aplicativos são removidos quando essa política é implantada nos dispositivos dos usuários. Com exceção dos dispositivos Samsung KNOX, os usuários recebem um prompt para desinstalar o aplicativo. Os usuários de dispositivos Samsung KNOX não recebem um aviso para desinstalar o aplicativo.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

App Uninstall Policy	App Uninstall Policy
1 Policy Info	This policy lets you specify which apps need to be uninstalled. You can perform silent removal only on Samsung KNOX devices. If you don't find the app in the list, use the package name.
2 Platforms	Managed app bundle ID * <input type="text" value="Make a selection"/>
<input checked="" type="checkbox"/> iOS	► Deployment Rules
<input checked="" type="checkbox"/> Android	
<input checked="" type="checkbox"/> Samsung KNOX	
<input checked="" type="checkbox"/> Android for Work	
<input checked="" type="checkbox"/> Windows Phone	
<input checked="" type="checkbox"/> Windows Desktop/Tablet	
<input checked="" type="checkbox"/> Windows Mobile/CE	
3 Assignment	

- **ID de pacote de aplicativos gerenciados:** na lista, clique em um aplicativo existente ou em **Adicionar novo**. Se não houver nenhum aplicativo configurado para essa plataforma, a lista estará vazia e você deverá adicionar um novo aplicativo.
 - Quando você clica em **Adicionar**, aparece um campo em que você pode digitar um nome de aplicativo.

Todas as outras configurações da plataforma

- **Aplicativos a desinstalar:** para cada aplicativo que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
 - **Nome do aplicativo:** na lista, clique em um aplicativo existente ou em **Adicionar novo** para adicionar um novo nome de aplicativo. Se não houver nenhum aplicativo configurado para essa plataforma, a lista estará vazia e você deverá adicionar novos aplicativos.
 - Clique em **Adicionar** para adicionar o aplicativo ou em **Cancelar** para cancelar a adição do aplicativo.

Desinstalar um aplicativo corporativo automaticamente depois que o aplicativo da loja de aplicativos pública correspondente for instalado

Você pode configurar o XenMobile para remover a versão corporativa dos aplicativos Citrix após a instalação da versão da loja de aplicativos pública. Esse recurso evita que os dispositivos dos usuários tenham dois ícones de aplicativo idênticos após a instalação da versão da loja de aplicativos pública.

Uma condição de implantação para a Política de dispositivo de desinstalação de aplicativo dispara o XenMobile para remover aplicativos mais antigos de dispositivos de usuários durante a instalação da nova versão. Esse recurso está disponível somente para dispositivos iOS gerenciados conectados a um XenMobile Server no modo empresarial (XME).

Para configurar uma regra de implantação com a condição Nome do aplicativo instalado:

- Especifique o **ID do pacote de aplicativos gerenciados** para o aplicativo Empresarial.
- Adicionar uma regra: Clique em **Nova regra** e, em seguida, como mostrado no exemplo, escolha **Nome do aplicativo instalado e é igual a**. Digite a ID do pacote de aplicativo para o aplicativo de loja de aplicativos pública.

No exemplo, quando o aplicativo da loja de aplicativos pública (com.citrix.mail.ios) é instalado em um dispositivo nos grupos de entrega especificados, o XenMobile remove a versão Empresarial (com.citrix.mail).

Política de dispositivo de restrições de desinstalação de aplicativo

April 23, 2020

Você pode especificar os aplicativos que os usuários podem ou não podem desinstalar em um dispositivo Samsung SAFE ou Amazon.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações Samsung SAFE ou Amazon

- **Configurações de restrição de desinstalação de aplicativo:** para cada regra de aplicativo que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
 - **Nome do aplicativo:** na lista, clique em um aplicativo ou em **Adicionar novo** para adicionar um novo aplicativo.
 - **Regra:** selecione se os usuários podem desinstalar o aplicativo. O padrão é permitir a desinstalação.
 - Clique em **Salvar** ou em **Cancelar**.

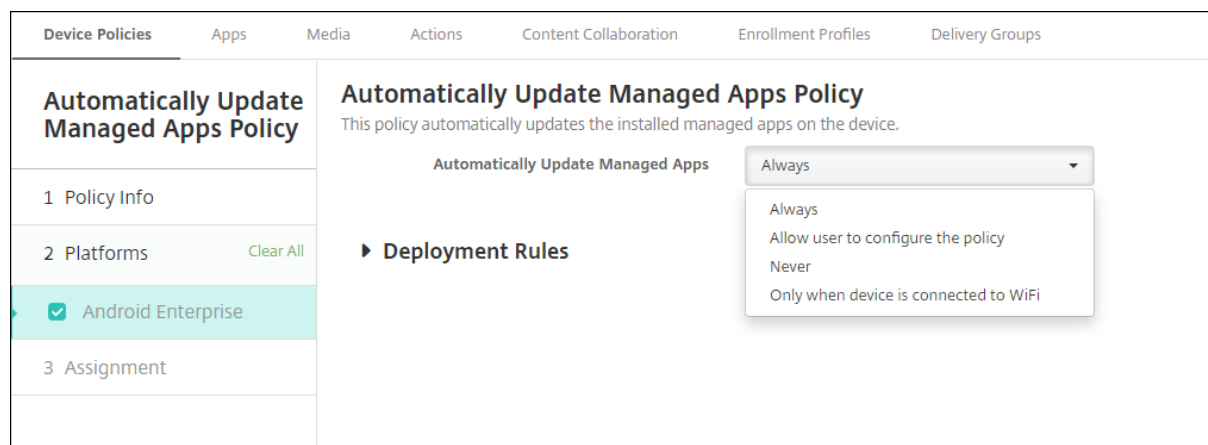
Política de dispositivo de atualizar automaticamente aplicativos gerenciados

January 22, 2021

Esta política controla como os aplicativos gerenciados instalados são atualizados em dispositivos Android Enterprise. Você pode restringir a capacidade dos usuários de permitir atualizações automáticas de aplicativos em seus dispositivos. Se você permitir que os usuários controlem atualizações au-

tomáticas de aplicativos em seus dispositivos, eles definem as políticas de atualização de aplicativo automática na loja gerenciada do Google Play.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).



Defina **Atualizar automaticamente aplicativos gerenciados**.

- **Sempre:** habilita atualizações automáticas de aplicativos. **Sempre** é o padrão.
- **Permitir que o usuário configure a política:** permite que o usuário configure a política de atualização automática de aplicativos para o dispositivo na loja gerenciada do Google Play.
- **Nunca:** desativa as atualizações automáticas de aplicativos.
- **Somente quando o dispositivo está conectado a WiFi:** permite atualizações automáticas de aplicativos somente quando o dispositivo está conectado ao Wi-Fi.

Política de dispositivo BitLocker

April 23, 2020

O Windows 10 inclui um recurso de criptografia de disco chamado BitLocker, que fornece proteções de arquivos e sistemas adicionais contra o acesso não autorizado de um dispositivo Windows perdido ou roubado. Para obter mais proteção, você pode usar o BitLocker com chips TPM (Trusted Platform Module), versão 1.2 ou posterior. Um chip TPM manipula operações criptográficas e gera, armazena e limita o uso de chaves criptográficas.

Começando com o Windows 10, compilação 1703, as políticas do MDM podem controlar o BitLocker. Você pode usar a política de dispositivo de BitLocker no XenMobile para definir as configurações disponíveis no Assistente de BitLocker nos dispositivos Windows 10. Por exemplo, em um dispositivo com o BitLocker habilitado, o BitLocker pode solicitar aos usuários como eles querem desbloquear sua unidade na inicialização, como fazer backup de sua chave de recuperação e como desbloquear

uma unidade fixa. A configuração da política do dispositivo BitLocker também configura se o seguinte deve ocorrer ou não:

- Ativar o BitLocker em dispositivos sem chip TPM
- Mostrar opções de recuperação na interface BitLocker.
- Negar acesso de gravação a uma unidade fixa ou removível quando o BitLocker não está habilitado.

Nota:

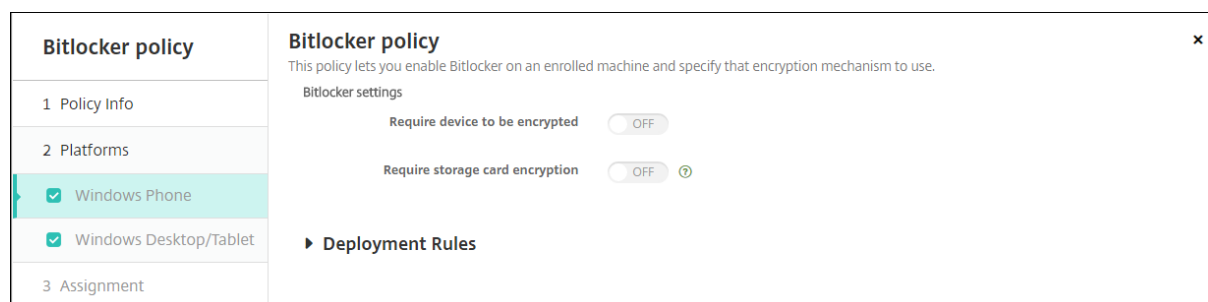
Depois de a criptografia BitLocker ter sido iniciada em um dispositivo, você não pode alterar posteriormente as configurações de BitLocker no dispositivo por meio da implantação de uma atualização da política BitLocker no dispositivo.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Requisitos

- A política de dispositivo BitLocker requer o Windows 10 Enterprise Edition.
- Antes de implantar a política do dispositivo BitLocker, prepare seu ambiente para o uso do BitLocker. Para obter informações detalhadas da Microsoft, incluindo requisitos e configuração do sistema BitLocker, consulte [BitLocker](#) e os artigos abaixo daquele nó.

Configurações do Windows Phone



- **Exigir que o dispositivo seja criptografado:** determina se os usuários devem para ativar a criptografia de BitLocker em um cartão de sistema do Windows Phone. Se o valor for **Ativado**, os dispositivos mostram uma mensagem após a conclusão do registro, indicando que a empresa requer criptografia do dispositivo. Se o usuário optar por não gerenciar a criptografia do dispositivo, o usuário não terá acesso para gravar na placa de sistema. Se o valor for **Desativado**, o usuário não é solicitado e a política de BitLocker determina se o dispositivo está criptografado. O padrão é **Desativado**.

- **Exigir criptografia de cartão de armazenamento:** determina se os usuários devem ativar a criptografia de BitLocker em um cartão de armazenamento do Windows Phone. Se o valor for **Ativado**, a criptografia de cartão de armazenamento é necessária para obter a permissão de gravação no cartão. O padrão é **Desativado**.

Configurações do Windows Desktop e Tablet

The screenshot shows the BitLocker policy configuration window. On the left, a navigation pane lists '1 Policy Info', '2 Platforms' (with 'Windows Phone' and 'Windows Desktop/Tablet' checked), and '3 Assignment'. The main content area is titled 'BitLocker policy' and includes a description: 'This policy lets you enable BitLocker on an enrolled machine and specify that encryption mechanism to use.' Below this, several settings are listed with toggle switches and help icons:

- BitLocker settings:** 'Require device to be encrypted' is set to OFF.
- Encryption settings:** 'Configure encryption methods' is set to OFF.
- OS drive settings:** 'Require additional authentication at startup' is set to OFF.
- PIN length:** 'Minimum PIN length' is set to 6.
- OS drive recovery settings:** 'Configure OS drive recovery' is set to OFF.
- Customize preboot recovery message and URL:** 'Customize preboot recovery message and URL' is set to OFF.
- Fixed drive recovery settings:** 'Configure fixed drive recovery' is set to OFF.
- Fixed drive settings:** 'Block write access to fixed drives not using BitLocker' is set to OFF.
- Removable drive settings:** 'Block write access to removable drives not using BitLocker' is set to OFF.
- Other drive settings:** 'Prompt for other disk encryption' is set to OFF.

- **Exigir que o dispositivo seja criptografado:** determina se os usuários devem para ativar a criptografia de BitLocker em um cartão de sistema do Windows Desktop ou Tablet. Se o valor for **Ativado**, os dispositivos mostram uma mensagem após a conclusão do registro, indicando que a empresa requer criptografia do dispositivo. Se o valor for **Desativado**, o usuário não é solicitado e o BitLocker usa as configurações de política. O padrão é **Desativado**.
- **Configurar métodos de criptografia:** determina os métodos de criptografia a serem usados para tipos de unidade específicos. Se o valor for **Desativado**, o Assistente para BitLocker solicita ao usuário para identificar o método de criptografia a ser usado para um tipo de unidade. O método de criptografia para todas as unidades padrão é XTS-AES de 128 bits. O método de criptografia para as unidades removíveis é AES-CBC de 128 bits. Se o valor for **Ativado**, o BitLocker usa o método de criptografia especificado na política. Se o valor for **Ativado**, essas configurações adicionais são exibidas: **unidade do sistema operacional**, **unidade fixa** e **unidade removível**. Escolha o método de criptografia padrão para cada tipo de unidade. O padrão é **Desativado**.

- **Exigir autenticação adicional na inicialização:** Especifica a autenticação adicional necessária durante a inicialização do dispositivo. Especifica se deseja permitir BitLocker em dispositivos que não têm um chip TPM também. Se o valor for **Desativado**, os dispositivos sem TPM não podem usar criptografia BitLocker. Para obter informações sobre TPM, consulte o artigo da Microsoft, [Visão geral da tecnologia Trusted Platform Module](#). Se o valor for **Ativado**, as seguintes configurações adicionais são exibidas. O padrão é **Desativado**.
 - **Bloquear o BitLocker em dispositivos sem chip TPM:** em um dispositivo sem chip TPM, o BitLocker exige que os usuários criem uma senha de desbloqueio ou uma chave de inicialização. A chave de inicialização é armazenada em uma unidade USB, que o usuário deve conectar ao dispositivo antes da inicialização. A senha de desbloqueio tem um mínimo de oito caracteres. O padrão é **Desativado**.
 - **Inicialização TPM:** em um dispositivo com TPM, há quatro modos de desbloquear: somente TPM, TPM + PIN, TPM + chave, e TPM + PIN + chave. A inicialização do TPM é para o modo somente TPM, no qual as chaves de criptografia são armazenadas no chip TPM. Este modo não exige que um usuário forneça dados de desbloqueio adicionais. O dispositivo do usuário desbloqueie automaticamente durante a reinicialização, usando a chave de criptografia do chip TPM. O padrão é **Permitir TPM**.
 - **PIN de inicialização TPM:** esta configuração é o modo de desbloqueio TPM + PIN. Um PIN pode ter até 20 dígitos. Use a configuração de **Comprimento mínimo do PIN** para especificar o tamanho mínimo do PIN. Um usuário configura um PIN durante a instalação do BitLocker e fornece o PIN durante a inicialização do dispositivo.
 - **Chave de inicialização TPM:** esta configuração é o modo de desbloqueio TPM + Chave. A chave de inicialização é armazenada em uma unidade USB ou outra unidade removível, que o usuário deve conectar ao dispositivo antes da inicialização.
 - **Chave de inicialização TPM e PIN:** esta configuração é o modo de desbloqueio TPM + PIN + Chave.

Se o desbloqueio for bem-sucedido, o sistema operacional inicia o carregamento. Se o desbloqueio falhar, o dispositivo entra no modo de recuperação.
- **Comprimento mínimo do PIN:** o tamanho mínimo do PIN de inicialização do TPM. O padrão é **6**.
- **Configurar recuperação da unidade do sistema operacional:** se a etapa de desbloqueio falhar, o BitLocker solicita ao usuário a chave de recuperação configurada. Essa configuração define as opções de recuperação da unidade do sistema operacional, disponíveis para os usuários que não tenham a senha de desbloqueio ou a chave de inicialização USB. O padrão é **Desativado**.
 - **Permitir agente de recuperação de dados baseado em certificado:** especifica se deseja ou não permitir um agente de recuperação de dados baseado em certificado. Adicione um

agente de recuperação de dados das Políticas de chave pública, que está localizado no Console de Gerenciamento de Política de Grupo (GPMC) ou no Editor de Política de Grupo Local. Para obter mais informações sobre agentes de recuperação de dados, consulte o artigo Microsoft [Configurações da Política de Grupo do BitLocker](#). O padrão é **Desativado**.

- **Criar senha de recuperação de 48 bits para recuperação da unidade do sistema operacional:** especifica se você deseja permitir ou exigir que os usuários usem uma senha de recuperação. O BitLocker gera a senha e a armazena em um arquivo ou conta do Microsoft Cloud. O padrão é **Permitir senha de 48 dígitos**.
- **Criar chave de recuperação de 256 bits:** especifica se você deseja permitir ou exigir que os usuários usem uma chave de recuperação. Uma chave de recuperação é um arquivo BEK, que é armazenado em uma unidade USB. O padrão é **Permitir uma chave de recuperação de 256 bits**.
- **Ocultar opções de recuperação da unidade do sistema operacional:** especifica se você deseja mostrar ou ocultar as opções de recuperação na interface do BitLocker. Se o valor for **Ativado**, nenhuma opção de recuperação aparece na interface BitLocker. Nesse caso, registre os dispositivos no Active Directory, salve as opções de recuperação no Active Directory e defina **Salvar informações de recuperação no AD DS** para **Ativado**. O padrão é **Desativado**.
- **Salvar informações de recuperação no AD DS:** especifica se deseja salvar as opções de recuperação nos Serviços de Domínio do Active Directory. O padrão é **Desativado**.
- **Configurar informações de recuperação armazenadas no AD DS:** especifica se deseja armazenar a senha de recuperação do BitLocker ou a senha de recuperação e o pacote de chaves nos Serviços do Domínio Active Directory. Armazenar o pacote de chaves dá suporte à recuperação de dados de uma unidade que está fisicamente corrompida. O padrão é **Senha de recuperação de backup**.
- **Ativar BitLocker depois de armazenar as informações de recuperação no AD DS:** especifica se deseja impedir que os usuários ativem o BitLocker, a menos que o dispositivo esteja conectado ao domínio e o backup das informações de recuperação de BitLocker no Active Directory seja bem-sucedido. Se estiver **Ativado**, um dispositivo deve ser ingressado no domínio antes de iniciar o BitLocker. O padrão é **Desativado**.
- **Personalizar mensagem de recuperação de pré-inicialização e URL:** especifica se o BitLocker mostra uma mensagem personalizada e a URL na tela de recuperação. Se o valor for **Ativado**, as seguintes configurações adicionais são exibidas: **Usar mensagem de recuperação e URL padrão**, **Usar mensagem de recuperação vazia e URL**, **Usar mensagem personalizada de recuperação** e **Usar URL de recuperação personalizada**. Se o valor for **Desativado**, são exibidas a mensagem de recuperação de padrão e a URL. O padrão é **Desativado**.
- **Configurar recuperação da unidade fixa:** configura as opções de recuperação aos usuários

para uma unidade fixa de criptografia BitLocker. O BitLocker não exibe uma mensagem aos usuários sobre a criptografia de unidade fixa. Para desbloquear uma unidade durante a inicialização, um usuário fornece uma senha ou um cartão inteligente. As configurações de desbloqueio de inicialização, que não estão nesta política, aparecem na interface BitLocker quando um usuário habilita a criptografia BitLocker em uma unidade fixa. Para obter informações sobre as configurações relacionadas, consulte **Configurar recuperação da unidade do sistema operacional**, anteriormente nessa lista. O padrão é **Desativado**.

- **Bloquear acesso de gravação a unidades fixas que não usam BitLocker:** Se **Ativado**, os usuários podem gravar em unidades fixas somente quando essas unidades são criptografadas com o BitLocker. O padrão é **Desativado**.
- **Bloquear acesso de gravação a unidades removíveis que não usam BitLocker:** Se **Ativado**, os usuários podem gravar em unidades removíveis somente quando essas unidades são criptografadas com o BitLocker. Defina essa configuração dependendo se a sua organização permite ou não o acesso de gravação em unidades removíveis de outra organização. O padrão é **Desativado**.
- **Solicitar outra criptografia de disco:** permite que você desabilite a mensagem de aviso para outra criptografia de disco em dispositivos. O padrão é **Desativado**.

Política de dispositivo de navegador

April 23, 2020

Você pode criar políticas de dispositivo de navegador para dispositivos Samsung SAFE ou Samsung KNOX para definir se os dispositivos do usuário podem usar o navegador ou para limitar as funções do navegador que os dispositivos podem usar.

Nos dispositivos Samsung, você pode desativar completamente o navegador ou pode ativar ou desativar pop-ups, JavaScript, cookies, preenchimento automático e decidir se deseja impor avisos de fraude.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do Samsung SAFE e do Samsung KNOX

- **Desativar navegador:** selecione se o navegador Samsung deve ser desativado completamente nos dispositivos dos usuários. O padrão é **O**, o que permite que os usuários usem o navegador. Quando você desativa o navegador, as opções a seguir desaparecem.
- **Desativar pop-up:** selecione se mensagens pop-up são permitidas no navegador.

- **Desativar Javascript:** selecione se JavaScript pode ser executado no navegador.
- **Desativar cookies:** selecione se você deseja permitir cookies.
- **Desativar preenchimento automático:** selecione se os usuários têm permissão para ativar a função de preenchimento automático do navegador.
- **Forçar aviso de fraude:** selecione se um aviso deverá ser exibido quando os usuários visitarem um site fraudulento ou comprometido.

Política de dispositivo de calendário (CalDav)

April 23, 2020

Você pode adicionar uma política de dispositivo no XenMobile para adicionar uma conta de calendário (CalDAV) aos dispositivos iOS ou macOS dos usuários para permitir que eles sincronizem dados de agendamento com qualquer servidor compatível com CalDAV.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

- **Descrição da conta:** digite uma descrição da conta. Este campo é obrigatório.
- **Nome do host:** digite o endereço do servidor CalDAV. Este campo é obrigatório.
- **Porta:** digite a porta à qual o servidor CalDAV deve se conectar. Este campo é obrigatório. O padrão é **8443**.
- **URL principal:** digite a URL base do calendário do usuário.
- **Nome de usuário:** digite o nome de usuário de login. Este campo é obrigatório.
- **Senha:** digite uma senha de usuário opcional.
- **Usar SSL:** selecione se uma conexão SSL com o servidor CalDAV deve ser usada. O padrão é **On**.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do macOS

- **Descrição da conta:** digite uma descrição da conta. Este campo é obrigatório.
- **Nome do host:** digite o endereço do servidor CalDAV. Este campo é obrigatório.
- **Porta:** digite a porta à qual o servidor CalDAV deve se conectar. Este campo é obrigatório. O padrão é **8443**.
- **URL principal:** digite a URL base do calendário do usuário.
- **Nome de usuário:** digite o nome de usuário de login. Este campo é obrigatório.
- **Senha:** digite uma senha de usuário opcional.
- **Usar SSL:** selecione se uma conexão SSL com o servidor CalDAV deve ser usada. O padrão é **On**.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra.
 - **Permitir que o usuário remova a política:** você pode selecionar quando os usuários podem remover a política do dispositivo. Selecione **Sempre**, **Código secreto obrigatório** ou **Nunca** no menu. Se você selecionar **Código secreto obrigatório**, digite um código secreto no campo **Código secreto de remoção**.
 - **Escopo do perfil:** selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

Política de dispositivo celular

April 23, 2020

Essa política permite que você defina as configurações da rede celular em um dispositivo iOS.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

- **Anexar APN**

- **Nome:** um nome para essa configuração.
- **Tipo de autenticação:** na lista, clique em Protocolo CHAP (**CHAP**) ou em Protocolo PAP (**PAP**). O padrão é **PAP**.
- **Username e Password:** o nome do usuário e a senha que deseja usar para autenticação.
- **APN**
 - **Nome:** um nome para a configuração Nome do ponto de acesso (APN).
 - **Tipo de autenticação:** na lista, clique em **CHAP** ou **PAP**. O padrão é **PAP**.
 - **Username e Password:** o nome do usuário e a senha que deseja usar para autenticação.
 - **Servidor proxy:** o endereço de rede do servidor proxy.
 - **Porta do servidor proxy:** a porta do servidor proxy.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Política de dispositivo do gerenciador de conexões

April 23, 2020

No XenMobile, você pode especificar as configurações de conexão dos aplicativos que se conectam automaticamente à Internet e a redes privadas. Essa política está disponível somente em Windows Pocket PCs.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do Windows Mobile/CE

Nota:

Escritório interno significa que todas as conexões estão na intranet da sua empresa. **Internet integrada** significa que todas as conexões são para a Internet.

- **Aplicativos que se conectam a uma rede privada usam automaticamente:** na lista, clique em **Escritório interno** ou **Internet integrada**. O padrão é **Escritório interno**.
- **Aplicativos que se conectam à Internet automaticamente usam:** na lista, clique em **Escritório interno** ou **Internet integrada**. O padrão é **Escritório interno**.

Política de dispositivo de agendamento de conexão

April 23, 2020

Importante:

A Citrix recomenda que você use o Firebase Cloud Messaging (FCM) para controlar as conexões de dispositivos Android, Android Enterprise e Chrome OS com o XenMobile Server. Para obter informações sobre como usar o FCM, consulte [Firebase Cloud Messaging](#).

Se você optar por não usar o FCM, poderá criar políticas de agendamento de conexão para controlar como e quando os dispositivos do usuário se conectam ao XenMobile Server.

Você pode especificar que os usuários conectem os dispositivos deles manualmente ou que os dispositivos se conectem em um período de tempo definido.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações da plataforma

- **Exigir que os dispositivos se conectem:** clique na opção que você deseja definir para esse agendamento.
 - **Sempre:** manter a conexão ativa de forma permanente. O XenMobile no dispositivo do usuário tenta se reconectar ao servidor XenMobile após uma perda de conexão de rede e monitorará a conexão mediante a transmissão de pacotes de controle em intervalos regulares. A Citrix recomenda esta opção para segurança otimizada. Quando você escolher **Sempre**, use também para a **Política de Túnel** do dispositivo, a configuração **Definir tempo limite de conexão**, para garantir que a conexão não esteja esgotando a bateria. Ao manter a conexão ativa, você pode enviar comandos de segurança por push, como apagar ou bloquear o dispositivo sob demanda. Você também deve selecionar a opção **Cronograma de implantação Implantar para conexões permanentes** em cada política implantada no dispositivo.
 - **Nunca:** conectar manualmente. Os usuários têm de iniciar a conexão no XenMobile, nos seus dispositivos. A Citrix não recomenda essa opção para implantações de produção, pois ela impede que você implante políticas de segurança nos dispositivos e, portanto, os usuários nunca receberão novos aplicativos ou políticas.
 - **A cada:** conectar no intervalo designado. Quando essa opção está em vigor e você envia uma política de segurança, como um bloqueio ou um apagamento, o XenMobile processa a ação no dispositivo na próxima vez em que ele se conectar. Quando você seleciona essa opção, o campo **Conectar a cada N minutos** é exibido, em que você deve digitar o número de minutos após o qual o dispositivo deve reconectar. O padrão é **20**.

- **Definir programação:** quando ativada, o XenMobile no dispositivo do usuário tenta se reconectar ao XenMobile Server após uma perda de conexão de rede e monitora a conexão mediante a transmissão de pacotes de controle em intervalos regulares no período de tempo que você definir. Consulte Definição de um período de tempo de conexão, mais adiante, para saber como definir um período de tempo de conexão.
 - * **Manter a conexão permanente durante estas horas:** os dispositivos dos usuários devem estar conectados durante o período de tempo definido.
 - * **Exigir uma conexão dentro de cada um destes intervalos:** os dispositivos dos usuários devem ser conectados pelo menos uma vez em qualquer um dos períodos de tempo definidos.
 - * **Usar hora do dispositivo local em vez de UTC:** sincronizar os períodos de tempo definidos para o horário local do dispositivo em vez do Tempo Universal Coordenado (UTC).

Definição de um período de tempo de conexão

Quando você ativa as opções a seguir, é exibida uma linha do tempo na qual você pode definir os períodos de tempo que desejar. Você pode ativar uma ou ambas as opções para exigir uma conexão permanente durante horários específicos ou para exigir uma conexão em determinados períodos de tempo. Cada quadrado na linha do tempo é 30 minutos, portanto, se você desejar uma conexão entre 8:00 e 9:00 da manhã todo dia da semana, clique nos dois quadrados na linha do tempo entre 8 e 9 da manhã todo dia da semana.

Por exemplo, as duas linhas do tempo na figura a seguir exigem uma conexão permanente entre 8:00 e 9:00 da manhã todo dia da semana, uma conexão permanente entre 12:00 da manhã de sábado e 1:00 da manhã de domingo e pelo menos uma conexão todo dia da semana entre 5:00 e 8:00 da manhã ou entre 10:00 da manhã e 11:00 da noite.

- **Nome do host:** digite o endereço do servidor CardDAV. Este campo é obrigatório.
- **Porta:** digite a porta à qual o servidor CardDAV deve se conectar. Este campo é obrigatório. O padrão é **8443**.
- **URL principal:** digite a URL base do calendário do usuário.
- **Nome de usuário:** digite o nome de usuário de login. Este campo é obrigatório.
- **Senha:** digite uma senha de usuário opcional.
- **Usar SSL:** selecione se uma conexão SSL com o servidor CardDAV deve ser usada. O padrão é **On**.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do macOS

- **Descrição da conta:** digite uma descrição da conta. Este campo é obrigatório.
- **Nome do host:** digite o endereço do servidor CardDAV. Este campo é obrigatório.
- **Porta:** digite a porta à qual o servidor CardDAV deve se conectar. Este campo é obrigatório. O padrão é **8443**.
- **URL principal:** digite a URL base do calendário do usuário.
- **Nome de usuário:** digite o nome de usuário de login. Este campo é obrigatório.
- **Senha:** digite uma senha de usuário opcional.
- **Usar SSL:** selecione se uma conexão SSL com o servidor CardDAV deve ser usada. O padrão é **On**.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra.

- **Permitir que o usuário remova a política:** você pode selecionar quando os usuários podem remover a política do dispositivo. Selecione **Sempre**, **Código secreto obrigatório** ou **Nunca** no menu. Se você selecionar **Código secreto obrigatório**, digite um código secreto no campo **Código secreto de remoção**.
- **Escopo do perfil:** selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

Política de dispositivo Controlar atualizações do sistema operacional

August 10, 2020

A política de dispositivo Controlar atualizações do sistema operacional permite que você implemente:

- As atualizações mais recentes do sistema operacional a dispositivos iOS com supervisão.
A política de dispositivos de Atualização de SO só funciona para dispositivos supervisionados e registrados no Programa de Implantação da Apple.
- As atualizações mais recentes de sistema operacional e aplicativo para dispositivos macOS registrados em DEP com macOS 10.11.5 e versões posteriores.
- As atualizações do sistema operacional mais recentes a dispositivos Samsung SAFE com supervisão.

Nos dispositivos Samsung SAFE, o XenMobile envia a política Controlar atualizações do sistema operacional para o Secure Hub, que então aplica a política ao dispositivo. A página **Gerenciar > Dispositivos** é exibida quando o XenMobile Server envia a política e quando o dispositivo recebe a política.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

Device Policies	Apps	Media	Actions	ShareFile	Enrollment Profiles	Delivery Groups
<div style="border: 1px solid #ccc; padding: 10px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <div style="width: 25%;"> <p>Control OS Update</p> <p>1 Policy Info</p> <p>2 Platforms</p> <p><input checked="" type="checkbox"/> iOS</p> <p><input checked="" type="checkbox"/> macOS</p> <p><input checked="" type="checkbox"/> Samsung SAFE</p> <p>3 Assignment</p> </div> <div style="width: 75%;"> <p>Control OS Update ✕</p> <p>This policy lets you push the latest OS updates to supervised devices and force installation.</p> <p>OS update options *</p> <p><input type="radio"/> Download only ⓘ</p> <p><input checked="" type="radio"/> Download and/or install ⓘ</p> <p>OS update frequency (1-365 days) * <input type="text" value="7"/> ⓘ</p> <p>▶ Deployment Rules</p> </div> </div> </div>						

- **Opções de atualização do sistema operacional:** ambas as opções baixam as mais recentes atualizações de sistema operacional para dispositivos supervisionados de acordo com a **frequência de atualização do SO**. O dispositivo solicita que os usuários instalem atualizações. O aviso é visível depois que o usuário desbloqueia o dispositivo.
- **Frequência de atualização do SO:** determina com que frequência o XenMobile verifica e atualiza o sistema operacional do dispositivo. O padrão é **7** dias.

Configurações do macOS

<div style="border: 1px solid #ccc; padding: 10px;"> <div style="display: flex; justify-content: space-between; align-items: center;"> <div style="width: 25%;"> <p>Control OS Update</p> <p>1 Policy Info</p> <p>2 Platforms</p> <p><input checked="" type="checkbox"/> iOS</p> <p><input checked="" type="checkbox"/> macOS</p> <p><input checked="" type="checkbox"/> Samsung SAFE</p> <p>3 Assignment</p> </div> <div style="width: 75%;"> <p>Control OS Update ✕</p> <p>This policy lets you push the latest OS updates to supervised devices and force installation.</p> <p>OS update options *</p> <p><input checked="" type="radio"/> Download and/or install ⓘ</p> <p><input type="radio"/> Download only and notify ⓘ</p> <p>OS update frequency (1-365 days) * <input type="text" value="7"/> ⓘ</p> <p>▶ Deployment Rules</p> </div> </div> </div>						
---	--	--	--	--	--	--

- **Opções de atualização do sistema operacional:** ambas as opções baixam as mais recentes atualizações de sistema operacional para macOS de acordo com a **frequência de atualização do OS**. Você pode optar por instalar as atualizações ou notificar o usuário por meio da loja de aplicativos que as atualizações estão disponíveis.
- **Frequência de atualização do SO:** determina com que frequência o XenMobile verifica e atualiza o sistema operacional do dispositivo. O padrão é **7** dias.

Obter status para ações de atualização do iOS e do macOS

No iOS e macOS, o XenMobile não implementa a política de controle de atualizações do sistema operacional nos dispositivos. Em vez disso, o XenMobile usa a política para enviar esses comandos do MDM para dispositivos:

- Cronograma de verificação de atualização do SO: solicita que o dispositivo execute uma verificação em segundo plano de atualizações do sistema operacional. (opcional para iOS)
- Atualização de SO disponível: consulta o dispositivo para obter uma lista de atualizações do sistema operacional disponíveis.
- Planejar atualização de SO: solicita que o dispositivo execute atualizações do macOS, atualizações de aplicativos ou ambas. Assim, o sistema operacional do dispositivo determina quando deve baixar ou instalar as atualizações do sistema operacional e do aplicativo.

A página **Gerenciar > Dispositivos > Detalhes do dispositivo (Geral)** mostra o status das verificações de atualizações agendadas e disponíveis do sistema operacional e atualizações agendadas do macOS e do aplicativo.

Para obter mais detalhes sobre o status das ações de atualização, vá para a página **Gerenciar > Dispositivos > Detalhes do dispositivo (Grupos de entrega)**.

Status	Action	Channel/User	Date
Success	Get Available OS Update Sent	SYSTEM	10/6/17 1:34:53 pm
Success	Schedule OS Update Scan Acknowledged	SYSTEM	10/6/17 1:34:53 pm
Success	Schedule OS Update Scan Sent	SYSTEM	10/6/17 1:34:53 pm
Success	Software inventory response	macos	10/6/17 1:34:20 pm
Done	Software inventory requested	macos	10/6/17 1:34:20 pm
Success	Mobileconfig response : MacOS DEP Webclip OSX (Profile already installed)	macos	10/6/17 1:34:20 pm

Para obter detalhes como atualizações disponíveis do sistema operacional e a última tentativa de instalação, vá para a página **Gerenciar > Dispositivos > Detalhes do dispositivo (Propriedades)**.

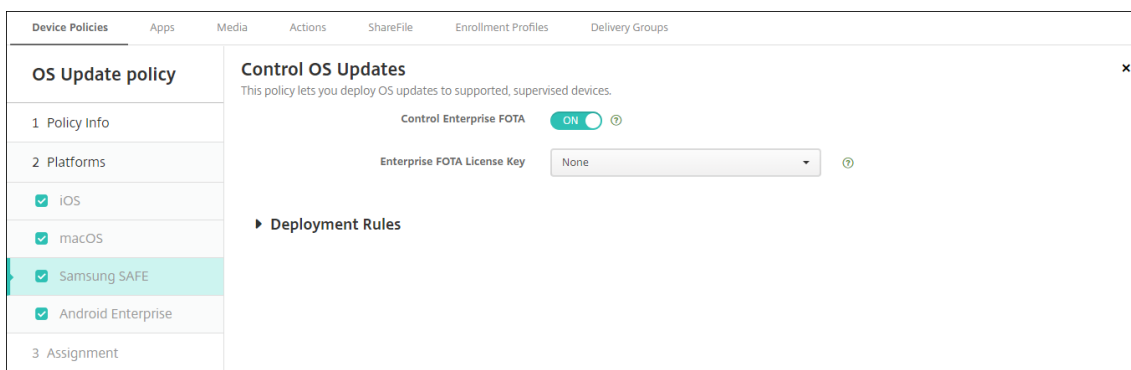
Device details	DEP account name	DEP Account FR	
1 General	DEP profile assigned	10/6/17 1:08:16 pm	
	DEP profile pushed	10/6/17 1:08:16 pm	
	DEP registration by	@outlook.com	
	DEP registration date	1/20/17 4:42:06 pm	
	Description	MB 12.0 SPACE GRAY/1.1GHZ/8GB/256GB-FRA	
	Device model	MacBook	
	Device name	FranckD MacBook	
	Model ID	MacBook8,1	
	OS Update Install Failure Message		
	OS Update Install Status	Success	×
2 Properties	OS Update is Critical	No	
	OS Update Last Install Attempt	10/6/17 1:35:15 pm	
3 User Properties	OS Update Version	macOS Sierra Update, iTunes	
	Operating system build	16B2657	
4 Assigned Policies			
5 Apps			
6 Media			
7 Actions			
8 Delivery Groups			
9 Certificates			
10 Connections			

Device details	Properties																																	
1 General	<table border="1"> <thead> <tr> <th colspan="2">-- Custom</th> <th>Add</th> </tr> </thead> <tbody> <tr> <td>AutoCheckEnabled</td> <td>true</td> <td></td> </tr> <tr> <td>AutomaticAppInstallationEnabled</td> <td>false</td> <td></td> </tr> <tr> <td>AutomaticOSInstallationEnabled</td> <td>false</td> <td></td> </tr> <tr> <td>AutomaticSecurityUpdatesEnabled</td> <td>true</td> <td></td> </tr> <tr> <td>BackgroundDownloadEnabled</td> <td>true</td> <td></td> </tr> <tr> <td>CatalogURL</td> <td>https://swscan.apple.com/content/catalogs/others/index-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog.gz</td> <td></td> </tr> <tr> <td>IsDefaultCatalog</td> <td>true</td> <td></td> </tr> <tr> <td>PerformPeriodicCheck</td> <td>true</td> <td></td> </tr> <tr> <td>PreviousScanDate</td> <td>2017-10-06T11:28:41Z</td> <td></td> </tr> <tr> <td>PreviousScanResult</td> <td>0</td> <td></td> </tr> </tbody> </table>	-- Custom		Add	AutoCheckEnabled	true		AutomaticAppInstallationEnabled	false		AutomaticOSInstallationEnabled	false		AutomaticSecurityUpdatesEnabled	true		BackgroundDownloadEnabled	true		CatalogURL	https://swscan.apple.com/content/catalogs/others/index-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog.gz		IsDefaultCatalog	true		PerformPeriodicCheck	true		PreviousScanDate	2017-10-06T11:28:41Z		PreviousScanResult	0	
	-- Custom		Add																															
	AutoCheckEnabled	true																																
	AutomaticAppInstallationEnabled	false																																
	AutomaticOSInstallationEnabled	false																																
	AutomaticSecurityUpdatesEnabled	true																																
	BackgroundDownloadEnabled	true																																
	CatalogURL	https://swscan.apple.com/content/catalogs/others/index-10.12-10.11-10.10-10.9-mountainlion-lion-snowleopard-leopard.merged-1.sucatalog.gz																																
	IsDefaultCatalog	true																																
	PerformPeriodicCheck	true																																
PreviousScanDate	2017-10-06T11:28:41Z																																	
PreviousScanResult	0																																	
2 Properties																																		
3 User Properties																																		
4 Assigned Policies																																		
5 Apps																																		
6 Media																																		
7 Actions																																		
8 Delivery Groups																																		
9 Certificates																																		
10 Connections																																		

Configurações do Samsung SAFE

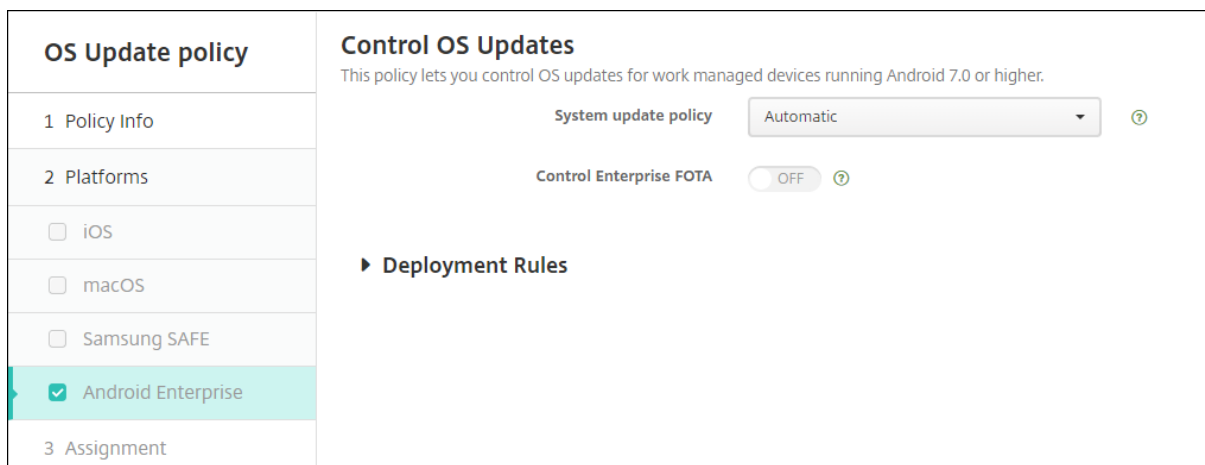
O Samsung Enterprise FOTA, também conhecido como E-FOTA, permite determinar quando os dispositivos são atualizados e a versão do firmware a ser usada. Para usar o E-FOTA:

1. Crie uma política de dispositivo chave de licença de MDM Samsung com as chaves e as informações de licença que você recebeu da Samsung. Para obter mais informações, consulte [Política de dispositivo de chave de licença MDM Samsung](#).
2. Crie uma política de dispositivo de controle de atualizações do sistema operacional para habilitar o Enterprise FOTA.



- **Ativar Enterprise FOTA:** defina como **Ativado**.
- **Chave de licença Enterprise FOTA:** selecione o nome da política de dispositivo de chave de licença Samsung MDM.

Configurações do Android Enterprise



- **Política de atualização do sistema.** Determina quando ocorrem atualizações do sistema. Instala **automaticamente** uma atualização quando disponível. **Em janela** instala a atualização automaticamente dentro da janela de manutenção diária especificada na **Hora de início** e **Hora de término**. **Adiar** permite que um usuário adie uma atualização por até 30 dias.
 - **Hora de início.** O início do período da janela de manutenção, medido como o número de minutos (**0 - 1440**) a contar da meia-noite na hora local do dispositivo. O padrão é **0**.
 - **Hora de término.** O fim do período da janela de manutenção, medido como o número de minutos (**0 - 1440**) a contar da meia-noite na hora local do dispositivo. O padrão é **120**.
- **Controlar Enterprise FOTA.** Permite controlar atualizações para dispositivos Samsung que utilizam o serviço Samsung Enterprise Firmware-Over-the-Air (FOTA). Para dispositivos Android Enterprise executando Samsung Knox 3.0 ou posterior. O padrão é **Desativado**.
- **Chave de licença do Enterprise FOTA.** Quando **Controlar Enterprise FOTA** está **ligado**, a **chave de licença do Enterprise FOTA** permite especificar a chave de licença a ser usada para

atualizações do Samsung FOTA. Para dispositivos Android Enterprise executando Samsung Knox 3.0 ou posterior. O padrão é **Nenhum**. A chave pode ser definida usando a política de dispositivo de **chave de licença MDM Samsung**. Veja [Política de dispositivo de chave de licença MDM Samsung](#).

Política de dispositivo Copiar aplicativos para o contêiner da Samsung

November 30, 2020

Para aplicativos que já estão instalados em um dispositivo, você pode especificar a cópia de aplicativos para um contêiner do KNOX em dispositivos Samsung com suporte. Para obter informações sobre dispositivos com suporte, consulte o artigo da Samsung [Devices built on Knox](#).

Os aplicativos copiados para o contêiner KNOX ficam disponíveis somente quando os usuários fazem login no contêiner KNOX.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Pré-requisitos

- Registre o dispositivo no XenMobile.
- Implante as chaves MDM da Samsung (ELM e KLM). Para saber como fazer isso, consulte [Política de dispositivo de chave de licença MDM Samsung](#).
- Instale aplicativos no dispositivo.
- Inicialize o KNOX no dispositivo para copiar os aplicativos para o contêiner do KNOX.

Configurações da plataforma

- **Novo aplicativo:** para cada aplicativo que você deseja adicionar à lista, clique em **Adicionar** e faça o seguinte:
 - Digite um ID de pacote; por exemplo, com.mobewolf.lacingart para o aplicativo LacingArt.
 - Clique em **Salvar** ou em **Cancelar**.

Política de dispositivo de credenciais

December 22, 2020

As políticas de dispositivo de Credenciais apontam para uma PKI configurada no XenMobile. Por exemplo, sua configuração PKI pode incluída na entidade PKI, um keystore, um provedor de credenciais ou um certificado de servidor. Para obter mais informações sobre as credenciais, consulte [Certificação e autenticação](#).

Cada plataforma com suporte exige um conjunto diferente de valores, que são descritos neste artigo.

Nota:

Antes de criar esta política, você precisa ter as informações de credencial que planeja usar para cada plataforma, além de quaisquer certificados e senhas.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

The screenshot shows the 'Credentials Policy' configuration page. On the left is a navigation menu with sections '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', several operating systems are listed with checkboxes: iOS (checked), macOS (checked), Android (checked), Android for Work (checked), Windows Phone (checked), Windows Desktop/Tablet (checked), and Windows Mobile/CE (checked). The main content area is titled 'Credentials Policy' and includes a descriptive paragraph: 'This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.' Below this are several configuration fields: 'Credential type' is a dropdown menu set to 'Certificate (.cer, .crt, .der and .pem)'; 'Credential name' is an empty text input field; 'The credential file path' is a text input field with a green 'Browse' button; 'Remove policy' has two radio button options: 'Select date' (selected) and 'Duration until removal (in hours)'; 'Allow user to remove policy' is a dropdown menu set to 'Always'. At the bottom, there is a section for 'Deployment Rules' with a right-pointing arrow.

Faça as seguintes configurações:

- **Tipo de credencial:** na lista, clique no tipo de credencial a ser usado com esta política e insira as seguintes informações para a credencial selecionada:
 - **Certificado**
 - * **Nome da credencial:** insira um nome exclusivo para a credencial.
 - * **O caminho do arquivo de credencial:** selecione o arquivo de credencial clicando em Procurar e navegando para a localização do arquivo.
 - **Keystore**
 - * **Nome da credencial:** insira um nome exclusivo para a credencial.
 - * **O caminho do arquivo de credencial:** selecione o arquivo de credencial clicando em Procurar e navegando para a localização do arquivo.
 - * **Senha:** Insira a senha do keystore para a credencial.

- **Certificado de servidor**
 - * **Certificado de servidor:** na lista, clique no certificado a ser usado.
- **Provedor de credenciais**
 - * **Provedor de credenciais:** na lista, clique no nome do provedor de credenciais.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do macOS

Credentials Policy	Credentials Policy
1 Policy Info	This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.
2 Platforms	<p>Credential type: Certificate (.cer, .crt, .der and .pem)</p> <p>Credential name *</p> <p>The credential file path <input type="text"/> <input type="button" value="Browse"/></p>
<input type="checkbox"/> iOS <input checked="" type="checkbox"/> macOS <input checked="" type="checkbox"/> Android <input checked="" type="checkbox"/> Android for Work <input checked="" type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Desktop/Tablet <input checked="" type="checkbox"/> Windows Mobile/CE	<p>Policy Settings</p> <p>Remove policy: <input checked="" type="radio"/> Select date <input type="radio"/> Duration until removal (in hours)</p> <p>Allow user to remove policy: Always</p> <p>Profile scope: User macOS 10.7+</p>
3 Assignment	

Faça as seguintes configurações:

- **Tipo de credencial:** na lista, clique no tipo de credencial a ser usado com esta política e insira as seguintes informações para a credencial selecionada:
 - **Certificado**
 - * **Nome da credencial:** insira um nome exclusivo para a credencial.
 - * **O caminho do arquivo de credencial:** selecione o arquivo de credencial clicando em **Procurar** e navegando para a localização do arquivo.
 - **Keystore**
 - * **Nome da credencial:** insira um nome exclusivo para a credencial.
 - * **O caminho do arquivo de credencial:** selecione o arquivo de credencial clicando em **Procurar** e navegando para a localização do arquivo.
 - * **Senha:** Insira a senha do keystore para a credencial.

- **Certificado de servidor**
 - * **Certificado de servidor:** na lista, clique no certificado a ser usado.
- **Provedor de credenciais**
 - * **Provedor de credenciais:** na lista, clique no nome do provedor de credenciais.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra.
 - **Permitir que o usuário remova a política:** você pode selecionar quando os usuários podem remover a política do dispositivo. Selecione **Sempre**, **Código secreto obrigatório** ou **Nunca** no menu. Se você selecionar **Código secreto obrigatório**, digite um código secreto no campo **Código secreto de remoção**.
 - **Escopo do perfil:** selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

Configurações do Android

Credentials Policy	Credentials Policy
1 Policy Info	This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.
2 Platforms	<p>Credential type: <input type="text" value="Certificate (.cer, .crt, .der and .pem)"/></p> <p>The credential file path: <input type="text"/> <input type="button" value="Browse"/></p> <p>► Deployment Rules</p>
<input type="checkbox"/> iOS <input type="checkbox"/> macOS <input checked="" type="checkbox"/> Android <input checked="" type="checkbox"/> Android for Work <input checked="" type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Desktop/Tablet <input checked="" type="checkbox"/> Windows Mobile/CE	
3 Assignment	

Faça as seguintes configurações:

- **Tipo de credencial:** na lista, clique no tipo de credencial a ser usado com esta política e insira as seguintes informações para a credencial selecionada:
 - **Certificado**
 - * **Nome da credencial:** digite um nome exclusivo para a credencial.

- * **O caminho do arquivo de credencial:** selecione o arquivo de credencial clicando em Procurar e navegando para a localização do arquivo.
- **Keystore**
 - * **Nome da credencial:** digite um nome exclusivo para a credencial.
 - * **O caminho do arquivo de credencial:** selecione o arquivo de credencial clicando em **Procurar** e navegando para a localização do arquivo.
 - * **Senha:** digite a senha do keystore para a credencial.
- **Certificado de servidor**
 - * **Certificado de servidor:** na lista, clique no certificado a ser usado.
- **Provedor de credenciais**
 - * **Provedor de credenciais:** na lista, clique no nome do provedor de credenciais.

Configurações do Android Enterprise

Credentials Policy	Credentials Policy
1 Policy Info	This policy lets you deliver certificates to devices. On iOS, certificates such as a certificate for wi-fi authentication can also be used as part of another policy. For Windows phones, only Windows 10 and later supervised devices support the policy.
2 Platforms	<p>Remove credentials <input type="checkbox"/> OFF</p> <p>Apply to fully managed devices with a work profile <input type="checkbox"/> OFF</p> <p>Credential type Certificate (.cer, .crt, .der and .p... ▾</p> <p>The credential file path <input type="text"/> <input type="button" value="Browse"/></p> <p>► Deployment Rules</p>
<input checked="" type="checkbox"/> iOS	
<input checked="" type="checkbox"/> macOS	
<input checked="" type="checkbox"/> Android (legacy DA)	
<input checked="" type="checkbox"/> Android Enterprise	
<input checked="" type="checkbox"/> Windows Phone	
<input checked="" type="checkbox"/> Windows Desktop/Tablet	
<input checked="" type="checkbox"/> Windows Mobile/CE	
3 Assignment	

Defina essas configurações para determinar como o XenMobile aplica as configurações de credenciais:

- **Remover credenciais:** defina como **Ativado** para definir as seguintes configurações. O padrão é **Desativado**.
 - **Remover credenciais do usuário:** remove certificados do keystore gerenciado. O padrão é **Desativado**.
 - **Remover certificados raiz confiáveis:** desinstala todos os certificados de CA que não sejam do sistema. O padrão é **Desativado**.
- **Aplicar a dispositivos totalmente gerenciados com um perfil de trabalho:** permite que você defina as configurações de política de credenciais para dispositivos totalmente gerenci-

ados com perfis de trabalho. Quando essa configuração estiver **Ativada**, selecione uma das seguintes configurações:

- **Perfil de trabalho:** as configurações de credenciais que você configura se aplicam apenas ao perfil de trabalho no dispositivo.
- **Gerenciar dispositivo:** as configurações de credenciais que você configura se aplicam somente ao dispositivo.
- **Ambos:** as configurações de credenciais que você configurar se aplicam ao perfil de trabalho e ao dispositivo.

Quando essa configuração estiver **Desativada**, as configurações de credenciais que você configurar se aplicarão somente ao dispositivo. O padrão é **Desativado**.

Defina as configurações de credencial:

- **Tipo de credencial:** na lista, clique no tipo de credencial a ser usado com esta política e insira as seguintes informações para a credencial selecionada:
 - **Certificado**
 - * **O caminho do arquivo de credencial:** selecione o arquivo de credencial clicando em **Procurar** e navegando para a localização do arquivo.
 - **Keystore**
 - * **O caminho do arquivo de credencial:** selecione o arquivo de credencial clicando em **Procurar** e navegando para a localização do arquivo.
 - * **Alias de certificado:** um alias de certificado facilita o acesso ao certificado pelos aplicativos. Configure um alias de certificado na política de dispositivo de Configuração gerenciada do Android Enterprise. Em seguida, digite o alias no campo **Alias de certificado** na política de dispositivo de Credenciais. Os aplicativos recuperam o certificado e autenticam a VPN sem qualquer ação por parte dos usuários.
 - * **Senha:** digite a senha do keystore para a credencial.
 - **Certificado de servidor**
 - * **Certificado de servidor:** na lista, clique no certificado a ser usado.
 - **Provedor de credenciais**
 - * **Alias de certificado:** um alias de certificado facilita o acesso ao certificado pelos aplicativos. Configure um alias de certificado na política de dispositivo de Configuração gerenciada do Android Enterprise. Em seguida, digite o alias no campo **Alias de certificado** na política de dispositivo de Credenciais. Os aplicativos recuperam o certificado e autenticam a VPN sem qualquer ação por parte dos usuários.
 - * **Provedor de credenciais:** na lista, clique no nome do provedor de credenciais.
 - * **Aplicativos que devem usar os certificados** para especificar aplicativos que têm acesso silencioso às credenciais desse provedor, clique em **Adicionar**, selecione um aplicativo e clique em **Salvar**.

Configurações do Windows Desktop/Tablet

Credentials Policy	Credentials Policy
1 Policy Info	This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.
2 Platforms	<p>Certificate Type: <input type="text" value="ROOT"/></p> <p>Store device: <input type="text" value="root"/></p> <p>Location: <input type="text" value="System"/></p> <p>Credential type: <input type="text" value="Certificate (.cer, .crt, .der and .pem)"/></p> <p>Credential file path: <input type="text"/> <input type="button" value="Browse"/></p>
<input type="checkbox"/> iOS <input type="checkbox"/> macOS <input type="checkbox"/> Android <input type="checkbox"/> Android for Work <input type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Desktop/Tablet <input checked="" type="checkbox"/> Windows Mobile/CE	<p>► Deployment Rules</p>
3 Assignment	

- **Tipo de Certificado:** na lista, clique em **RAIZ** ou **CLIENTE**.
- Se você clicar em **RAIZ**, defina estas configurações:
 - **Dispositivo de armazenamento:** na lista, clique em **raiz**, **Meu** ou **CA** referente à localização do repositório de certificados para a credencial. **Meu** armazena o certificado em repositórios de certificados dos usuários.
 - **Localização:** em Tablets Windows 10, **Sistema** é a única localização.
 - **Tipo de credencial:** em Tablets Windows 10, **Certificado** é o único tipo de credencial.
 - **Caminho do arquivo de credencial:** selecione o arquivo de credencial clicando em **Procurar** e navegando para a localização do arquivo.
- Se você clicar em **CLIENTE**, defina estas configurações:
 - **Localização:** em Tablets Windows 10, **Sistema** é a única localização.
 - **Tipo de credencial:** em Tablets Windows 10, **Keystore** é o único tipo de credencial.
 - **Nome da credencial:** digite o nome da credencial. Este campo é obrigatório.
 - **Caminho do arquivo de credencial:** selecione o arquivo de credencial clicando em **Procurar** e navegando para a localização do arquivo.
 - **Senha:** digite a senha associada à credencial. Este campo é obrigatório.

Configurações do Windows Mobile/CE

Credentials Policy	Credentials Policy
1 Policy Info	This policy lets you deliver certificates to devices. On iOS, the certificates, such as a certificate for WiFi authentication, can also be used as part of another policy. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.
2 Platforms	<p>Store device: <input type="text" value="root"/></p> <p>Credential type: <input type="text" value="Certificate (.cer, .crt, .der and .pem)"/></p> <p>Credential file path: <input type="text"/> <input type="button" value="Browse"/></p> <p>► Deployment Rules</p>
<input type="checkbox"/> iOS <input type="checkbox"/> macOS <input type="checkbox"/> Android <input type="checkbox"/> Android for Work <input type="checkbox"/> Windows Phone <input type="checkbox"/> Windows Desktop/Tablet <input checked="" type="checkbox"/> Windows Mobile/CE	
3 Assignment	

- **Dispositivo de armazenamento:** na lista, clique na localização do repositório de certificados para a credencial. O padrão é **raiz**. As opções são:
 - **Autoridades confiáveis de execução privilegiada:** os aplicativos assinados com um certificado pertencente a esse repositório serão executados com nível de confiança privilegiada.
 - **Autoridades confiáveis de execução não privilegiada:** os aplicativos assinados com um certificado pertencente a esse repositório serão executados com nível de confiança normal.
 - **SPC (Certificado de Editor de Software):** o Software Publishing Certificate (SPC) é usado para assinar arquivos .cab.
 - **raiz:** um repositório de certificados que contém certificados raiz.
 - **CA:** um repositório de certificados que contém informações de criptografia, incluindo autoridades de certificação intermediárias.
 - **MEU:** um repositório de certificados que contém certificados pessoais do usuário final.
- **Tipo de credencial:** certificado é o único tipo de credencial para telefones Windows Mobile/CE.
- **O caminho do arquivo de credencial:** selecione o arquivo de credencial clicando em **Procurar** e navegando para a localização do arquivo.

Política de dispositivo de XML personalizado

April 1, 2021

Você pode criar políticas de XML personalizado no XenMobile para personalizar os seguintes recursos em dispositivos Windows e Zebra Android com suporte e dispositivos Android Enterprise:

- Provisionamento, o que inclui configurar o dispositivo e ativar ou desativar recursos

- Configuração do dispositivo, o que inclui permitir que os usuários alterem configurações e parâmetros do dispositivo
- Atualizações de software, incluindo o fornecimento de novos softwares ou correções de bugs a serem carregados no dispositivo, entre eles softwares do sistema e aplicativos
- Gerenciamento de falhas, o que inclui receber relatórios de erro e status do dispositivo

Nota:

Ao criar seu conteúdo XML, use o caractere % com cautela. O caractere % é um caractere reservado XML, usado apenas para o escape de caracteres especiais XML. Para usar % em um nome, codifique-o como %25.

Para dispositivos Windows, crie sua configuração de XML personalizado usando a API Open Mobile Alliance Device Management (OMA DM) no Windows. A criação do XML personalizado com a API OMA DM está além do escopo deste tópico. Para obter mais informações sobre como usar a API OMA DM, consulte [OMA Device Management](#) no site Microsoft Developer Network.

Para dispositivos Android Zebra e Android Enterprise, crie sua configuração de XML personalizado usando o MX Management System (MXMS). A criação do XML personalizado com a API MXMS está além do escopo deste artigo. Para obter mais informações sobre como usar o MXMS, consulte [About MX](#) no site do Zebra.

Nota:

Para telefones Windows 10 RS2, depois que uma política de XML personalizado ou de Restrições que desativa o Internet Explorer é implantada no telefone, o navegador permanece ativado. Para resolver esse problema, reinicie o telefone. Esse é um problema de terceiros.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do Windows Phone, Windows Desktop/Tablet, Zebra Android e Android Enterprise

- **Conteúdo XML:** digite ou recorte e cole o código XML personalizado que você deseja adicionar à política.

Depois que você clica em **Avançar**, o XenMobile verifica a sintaxe do conteúdo XML. Todos os erros de sintaxe são exibidos abaixo da caixa de conteúdo. Corrija todos os erros antes de continuar.

Se não houver nenhum erro de sintaxe, a página de atribuição **Política de XML personalizado** será exibida.

Política de dispositivo do Defender

April 23, 2020

O Windows Defender é uma proteção contra malware incluída com o Windows 10. Você pode usar a política de dispositivo do XenMobile, Defender, para configurar a política do Microsoft Defender para o Windows 10 para desktop e tablet.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do Windows Desktop e Tablet

Defender	Defender
1 Policy Info	This policy configures Windows Defender settings in Windows 10 for desktop and tablet.
2 Platforms	Allows scanning of archives <input type="radio"/> OFF
<input checked="" type="checkbox"/> Windows Desktop/Tablet	Allows cloud protection <input checked="" type="radio"/> ON
3 Assignment	Allows a full scan of removable drives <input checked="" type="radio"/> ON
	Allows Windows Defender Real-time Monitoring functionality <input checked="" type="radio"/> ON
	Allows scanning of network files <input checked="" type="radio"/> ON
	Allows user access to the Windows Defender UI <input checked="" type="radio"/> ON
	Excluded extensions <input type="text"/>
	Excluded paths <input type="text"/>
	Excluded processes <input type="text"/>
	Submit samples consent <input type="text" value="Send safe samples"/>

- **Permite exame de arquivos:** permite ou proíbe que o Defender examine arquivos armazenados. O padrão é **Desativado**.
- **Permite proteção da nuvem:** permite ou proíbe que o Defender envie informações à Microsoft sobre atividades de malware. O padrão é **Ativado**.
- **Permite exame completo de unidades removíveis:** permite ou proíbe que o Defender examine unidades removíveis, como pen drives. O padrão é **Ativado**.
- **Permite funcionalidade de monitoramento em tempo real do Windows Defender:** o padrão é **Ativado**.
- **Permite exame de arquivos de rede:** permite ou proíbe que o Defender examine arquivos de rede. O padrão é **Ativado**.
- **Permite o acesso do usuário à interface de usuário do Windows Defender:** especifica se os usuários podem acessar a interface de usuário do Windows Defender. Essa configuração entrará em vigor da próxima vez em que o dispositivo do usuário for iniciado. Se essa configuração for **Desativado**, os usuários não receberão notificações do Windows Defender. O padrão é **Ativado**.

- **Extensões excluídas:** as extensões a serem excluídas de exames em tempo real ou agendados. Para separar extensões, use o caractere |. Por exemplo, “lib|obj”.
- **Caminhos excluídos:** os caminhos a serem excluídos de exames em tempo real ou agendados. Para separar caminhos, use o caractere |. Por exemplo, “C:\Exemplo\C:\Exemplo1”.
- **Processos excluídos:** os processos a serem excluídos de exames em tempo real ou agendados. Para separar processos, use o caractere |. Por exemplo, “C:\Exemplo.exe\C:\Exemplo1.exe”.
- **Enviar consentimento de amostras:** controla se é ou não necessário enviar à Microsoft arquivos que possam exigir análise adicional para determinar se eles são mal-intencionados. Opções: **Sempre avisar**, **Enviar amostras seguras**, **Nunca enviar**, **Enviar todas as amostras**. O padrão é **Enviar amostras seguras**.

Política de dispositivo de excluir arquivos e pastas

April 23, 2020

Você pode criar uma política no XenMobile para excluir arquivos e pastas específicos dos dispositivos Windows Mobile/CE.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do Windows Mobile/CE

- **Arquivos e pastas a serem excluídos:** para cada arquivo ou pasta que você deseja excluir, clique em Adicionar e faça o seguinte:
 - **Caminho:** digite o caminho para o arquivo ou a pasta.
 - **Tipo:** na lista, clique em Arquivo ou Pasta. O padrão é Arquivo.
 - Clique em **Salvar** para salvar o arquivo ou a pasta, ou clique em **Cancelar** para não salvar.

Política de dispositivo Excluir chaves e valores do Registro

April 23, 2020

Você pode criar uma política no XenMobile para excluir chaves e valores específicos do Registro dos dispositivos Windows Mobile/CE.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do Windows Mobile/CE

- **Chaves e valores de Registro a serem excluídos:** para cada chave e valor do Registro que você desejar excluir, clique em **Adicionar** e faça o seguinte:
 - **Chave:** digite o caminho da chave do Registro. Esse é um campo obrigatório. O caminho da chave do Registro deve começar com HKEY_CLASSES_ROOT\, HKEY_CURRENT_USER\, HKEY_LOCAL_MACHINE\ ou HKEY_USERS\.
 - **Valor:** digite o nome do valor a ser excluído ou deixe esse campo em branco para excluir a chave do Registro inteira.
 - Clique em **Salvar** para salvar a chave e o valor ou clique em **Cancelar** para não salvar.

Política de dispositivo de Atestado de Integridade de Dispositivo

November 30, 2020

No XenMobile, você pode exigir que os dispositivos Windows 10 relatem o estado da sua integridade fazendo com que esses dispositivos enviem dados específicos e informações de tempo de execução para o Serviço de Atestado de Integridade (HAS) para análise. O HAS cria e retorna um Certificado de Atestado de Integridade que o dispositivo envia para o XenMobile. Quando o XenMobile recebe o Certificado de Atestado de Integridade, com base no conteúdo do Certificado de Atestado de Integridade, ele pode implantar ações automáticas que você configurou anteriormente.

Os dados verificados pelo HAS são:

- AIK presente
- Status de Bit Locker
- Depuração de inicialização ativada
- Versão da lista de revisões do Gerenciador de inicialização
- Integridade do código ativada
- Versão da lista de revisões de integridade do código
- Política do programa de implantação da Apple
- Driver ELAM carregado
- Emitido em
- Depuração de kernel ativada
- PCR
- Redefinir contagem
- Reiniciar contagem
- Modo de segurança ativado
- Hash SBCEP
- Inicialização segura ativada

- Sinalização de teste ativada
- VSM ativado
- WinPE ativado

Para obter mais informações, consulte a página [Device HealthAttestation CSP](#) da Microsoft.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Para configurar DHA usando o Microsoft Cloud

Adicione uma política de atestado de integridade do dispositivo e defina essa configuração para cada plataforma escolhida:

- **Ativar atestado de integridade de dispositivo:** selecione se pretende exigir o Atestado de Integridade de Dispositivo. O padrão é **Off**.

Para configurar o DHA usando um servidor DHA do Windows no local

Para habilitar o DHA no local, você primeiro configura um servidor DHA. Em seguida, você cria uma política do XenMobile Server para habilitar o serviço DHA local.

1. Para configurar um servidor DHA, você instala a função de servidor DHA em uma máquina executando o Windows Server 2016 Technical Preview 5 ou posterior. Para obter instruções, consulte [Configurar um servidor de atestado de integridade de dispositivo no local](#).
2. Adicione uma política de atestado de integridade do dispositivo e defina estas configurações:
 - **Ativar atestado de integridade do dispositivo: ON.**
 - **Configurar o serviço de atestado de integridade no local: ON.**
 - **FQDN do Serviço DHA no local:** digite o nome de domínio totalmente qualificado do servidor DHA que você configurou.
 - **Versão da API DHA no local:** selecione a versão do serviço DHA instalado no servidor DHA.

Política de dispositivo de nome do dispositivo

April 23, 2020

Você pode definir os nomes nos dispositivos iOS e macOS supervisionados para que você possa identificá-los facilmente. Você pode usar macros, texto ou uma combinação de ambos para definir o nome do dispositivo. Por exemplo, para definir o nome do dispositivo como o número de série do dispositivo, você usaria `$(device.serialnumber)`. Para definir o nome do dispositivo como uma

combinação do nome do usuário e do seu domínio, você usaria `${user.username}@exemplo.com`. Para obter informações sobre macros, consulte [Macros no XenMobile](#).

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do iOS e do MacOS

Device Name Policy	Device Name Policy This policy lets you apply a name on a supervised device on iOS and macOS devices. Available in iOS 8 and later.
1 Policy Info	Device name * <input type="text"/>
2 Platforms	▶ Deployment Rules
<input checked="" type="checkbox"/> iOS	
<input checked="" type="checkbox"/> macOS	
3 Assignment	

- **Nome do dispositivo:** digite a macro, uma combinação de macros ou uma combinação de macros e texto para nomear cada dispositivo de forma exclusiva. Por exemplo, use `${device.serialnumber}` para definir os nomes de dispositivo como o número de série de cada dispositivo ou use `${device.serialnumber} ${user.username}` para incluir o nome do usuário no nome do dispositivo.

Política de dispositivo Configuração de Educação

November 30, 2020

A Política de dispositivo Configuração de Educação define:

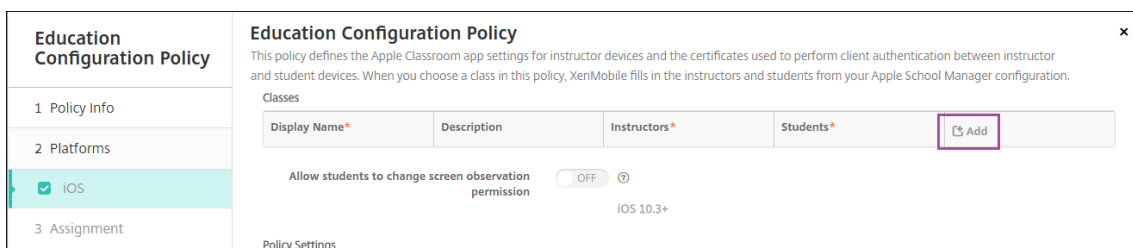
- As configurações de aplicativo Sala de Aula da Apple para dispositivos de instrutores.
- Os certificados usados para realizar a autenticação de cliente entre os dispositivos do instrutor e do aluno.

Quando você escolhe uma aula nessa política, o console XenMobile preenche a configuração de instrutores e alunos com a configuração do Apple School Manager. Crie uma política se as configurações do aplicativo Apple Sala de Aula nesta política forem iguais para todas as classes.

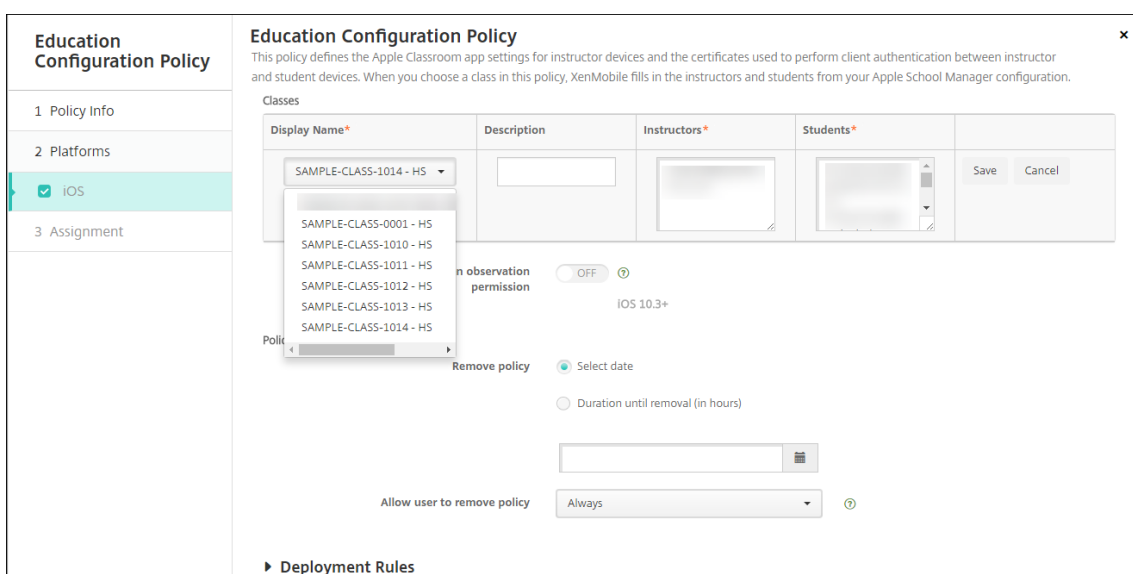
Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

- **Classes:** para adicionar uma classe, clique em **Adicionar**.



Depois, clique na lista **Nome de exibição**. É exibida uma lista de classes obtidas da sua conta do Apple School Manager conectada.



Quando você escolhe uma classe de **nome de exibição**, o XenMobile preenche as informações de instrutores e alunos. Continue adicionando classes.

Education Configuration Policy

This policy defines the Apple Classroom app settings for instructor devices and the certificates used to perform client authentication between instructor and student devices. When you choose a class in this policy, XenMobile fills in the instructors and students from your Apple School Manager configuration.

Classes

Display Name*	Description	Instructors*	Students*	Add
SAMPLE-CLASS-0001 - HS		@appleid.citrix.com, @appleid.citrix.com	@appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com	
SAMPLE-CLASS-1010 - HS		@appleid.citrix.com	@appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com	
SAMPLE-CLASS-1011 - HS		@appleid.citrix.com	@appleid.citrix.com	
SAMPLE-CLASS-1012 - HS		@appleid.citrix.com	@appleid.citrix.com, @appleid.citrix.com, @appleid.citrix.com	

Allow students to change screen observation permission ON ⓘ
IOS 10.3+

Policy Settings

Remove policy Select date
 Duration until removal (in hours)

- **Permitir que os alunos modifiquem a permissão de observação de tela:** Se **Ativado**, os alunos registrados em aulas gerenciadas podem escolher se querem permitir que seus professores observem a tela de seus dispositivos. O padrão é **Desativado**.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra.

Para editar informações de classes na política

Você pode adicionar uma descrição para uma classe (o “nome de exibição” no aplicativo Sala de Aula). Você também pode adicionar ou remover instrutores e alunos. O XenMobile não salva essas alterações na sua conta Apple School Manager. Para obter mais informações, consulte “Gerenciar informações do instrutor, aluno e classe” em [Integração com os recursos do Apple Educação](#).

Passa o mouse sobre a coluna **Adicionar** da classe que deseja editar e, em seguida, clique no ícone de lápis.

Education Configuration Policy

- 1 Policy Info
- 2 Platforms
- 3 iOS
- 3 Assignment

Education Configuration Policy ✕

This policy defines the Apple Classroom app settings for instructor devices and the certificates used to perform client authentication between instructor and student devices. When you choose a class in this policy, XenMobile fills in the instructors and students from your Apple School Manager configuration.

Classes

Display Name*	Description	Instructors*	Students*	
SAMPLE-CLASS-0001 - HS		@appleid.citrix.com, pleid.citrix.com	appleid.citrix.com, appleid.citrix.com, leid.citrix.com, pleid.citrix.com, appleid.citrix.com, pleid.citrix.com, in@appleid.citrix.com	➕ Add

Para excluir uma classe da política, passe o mouse sobre a coluna **Adicionar** da classe que deseja excluir e clique no ícone de lixeira.

Política de dispositivo do Hub Empresarial

April 23, 2020

Uma política de dispositivo do hub empresarial para Windows Phone permite distribuir aplicativos por meio da loja do hub empresarial.

Antes de criar a política, o seguinte é necessário:

- Um certificado de assinatura AET (.aetx) da DigiCert
- O aplicativo Citrix Company Hub assinado usando a ferramenta de assinatura de aplicativos da Microsoft (XapSignTool.exe)

Nota:

O XenMobile é compatível somente com uma política do Hub Empresarial para um modo do Secure Hub para Windows Phone. Por exemplo, para carregar o Secure Hub para Windows Phone para XenMobile Enterprise Edition, você não deve criar várias políticas do Hub Empresarial com versões diferentes do Worx Home para XenMobile Enterprise Edition. Você pode implantar somente a política inicial do Hub Empresarial durante registro do dispositivo.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do Windows Phone

Enterprise Hub Policy	Enterprise Hub Policy
1 Policy Info	To create the Enterprise Hub policy for Windows Phone app distribution through the Enterprise Hub Company store, you need the AET (.aetx) signing certificate from Symantec. You also need to have obtained and signed the Citrix Company Hub app using the Microsoft app signing tool (XapSignTool.exe).
2 Platforms	Upload .aetx file <input type="text"/> <input type="button" value="Browse"/>
<input checked="" type="checkbox"/> Windows Phone	Upload signed Enterprise Hub app <input type="text"/> <input type="button" value="Browse"/>
3 Assignment	
	► Deployment Rules

- **Upload de arquivo .aetx:** selecione o arquivo .aetx clicando em **Procurar** e navegando até a localização do arquivo.
- **Carregar o aplicativo de hub empresarial:** selecione o aplicativo Hub Enterprise clicando em **Procurar** e navegando até a localização do aplicativo.

Política de dispositivo do Exchange

January 22, 2021

Você pode usar a política de dispositivo do Exchange ActiveSync para configurar um cliente de email em dispositivos dos usuários e permitir que eles acessem emails corporativos hospedados no Exchange. Você pode criar políticas para iOS, macOS, Android Enterprise, Samsung SAFE, Samsung KNOX, Windows Phone e Windows Tablet. Cada plataforma exige um conjunto diferente de valores, que são descritos em detalhes nas seções a seguir.

Para criar essa política, você precisa do nome do host ou endereço IP do Exchange Server. Para obter informações sobre as configurações do ActiveSync, consulte o artigo da Microsoft [ActiveSync CSP](#).

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

Exchange Policy	Exchange Policy
1 Policy Info	This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.
2 Platforms	
<input checked="" type="checkbox"/> iOS	Exchange ActiveSync account name *
<input checked="" type="checkbox"/> macOS	Exchange ActiveSync host name *
<input checked="" type="checkbox"/> Android HTC	Use SSL <input checked="" type="checkbox"/> ON
<input checked="" type="checkbox"/> Android TouchDown	Domain
<input checked="" type="checkbox"/> Android for Work	User
<input checked="" type="checkbox"/> Samsung SAFE	Email address
<input checked="" type="checkbox"/> Samsung KNOX	Password
<input checked="" type="checkbox"/> Windows Phone	Email sync interval
<input checked="" type="checkbox"/> Windows Desktop/Tablet	Identity credential (keystore or PKI credential)
	Authorize email move between accounts <input type="checkbox"/> OFF

- **Nome de conta do Exchange ActiveSync:** digite a descrição da conta de email exibida nos dispositivos do usuário.
- **Nome do host do Exchange ActiveSync:** digite o endereço do servidor de email.
- **Usar SSL:** selecione se as conexões entre os dispositivos dos usuários e o Exchange Server devem ser protegidas. O padrão é **On**.
- **Domínio:** insira o domínio no qual o Exchange Server reside. Você pode usar a macro de sistema \$user.domainname nesse campo para procurar automaticamente os nomes de domínio dos usuários.
- **Usuário:** especifique o nome do usuário da conta de usuário do Exchange. Você pode usar a macro de sistema \$user.username nesse campo para procurar automaticamente os nomes dos usuários.
- **Endereço de email:** especifique o endereço de email completo. Você pode usar a macro de sistema \$user.mail nesse campo para procurar automaticamente as contas de email dos usuários.
- **Usar OAuth:** se definido como **On**, a conexão usará OAuth para autenticação. O padrão é **Off**. Essa opção se aplica ao iOS 12.0 e posterior.
- **Senha:** digite uma senha opcional para a conta de usuário do Exchange. Essa configuração não aparece quando **Usar OAuth** está **On**.
- **Intervalo de sincronização de emails:** na lista, escolha com que frequência o email é sincronizado com o Exchange Server. O padrão é **3 dias**.
- **Credencial de identidade (keystore ou PKI):** na lista, clique em uma credencial de identidade opcional se você tiver configurado um provedor de identidade para o XenMobile. Esse campo só é necessário quando o Exchange exige uma autenticação de certificado cliente. O padrão é **Nenhum**.
- **Autorizar a mudança de emails entre contas:** selecione se os usuários têm permissão para mover emails dessa conta para outra conta, além de encaminhar e responder de uma conta

diferente. O padrão é **Off**.

- **Enviar email somente do aplicativo de email:** selecione se os usuários têm restrições no aplicativo de correio do iOS para enviar emails. O padrão é **Off**.
- **Desativar a sincronização de emails recentes:** selecione se os usuários devem ser impedidos de sincronizar endereços recentes. O padrão é **Off**. Essa opção se aplica somente ao iOS 6.0 e versões posteriores.
- **Ativar assinatura S/MIME:** selecione se esta conta suporta ou não a assinatura S/MIME. O padrão é **On**. Quando definido como **On**, os campos abaixo são exibidos.
 - **Credencial de identidade de assinatura:** escolha a credencial de assinatura a ser usada.
 - **Usuário de assinatura S/MIME substituível:** se definido como **On**, os usuários podem ativar e desativar a assinatura S/MIME nas configurações de seus dispositivos. O padrão é **Off**. Essa opção se aplica ao iOS 12.0 e posterior.
 - **UUID de certificado de assinatura S/MIME substituível pelo usuário:** se definido como **On**, os usuários podem selecionar, nas configurações de seus dispositivos, a credencial de assinatura a ser usada. O padrão é **Off**. Essa opção se aplica ao iOS 12.0 e posterior.
- **Ativar criptografia S/MIME:** selecione se essa conta é compatível com a criptografia S/MIME. O padrão é **Off**. Quando definido como **On**, os campos abaixo são exibidos.
 - **Credencial de identidade de criptografia:** escolha a credencial de criptografia a ser usada.
 - **Ativar comutador de S/MIME por mensagem:** quando definido como **On**, mostra aos usuários uma opção para ativar ou desativar a criptografia S/MIME para cada mensagem que redigem. O padrão é **Off**.
 - **Criptografia S/MIME como padrão substituível pelo usuário:** se definido como **On**, os usuários podem, nas configurações de seus dispositivos, selecionar se S/MIME permanecerá ativa como padrão. O padrão é **Off**. Essa opção se aplica ao iOS 12.0 e posterior.
 - **UUID de certificado de criptografia S/MIME substituível pelo usuário:** se definido como **On**, os usuários podem ativar e desativar a identidade da criptografia de S/MIME e a criptografia nas configurações de seus dispositivos. O padrão é **Off**. Essa opção se aplica ao iOS 12.0 e posterior.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do macOS

Exchange Policy	Exchange Policy
1 Policy Info	This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.
2 Platforms	
<input type="checkbox"/> iOS	Exchange ActiveSync account name *
<input checked="" type="checkbox"/> macOS	User *
<input checked="" type="checkbox"/> Android HTC	Email address *
<input checked="" type="checkbox"/> Android TouchDown	Password
<input checked="" type="checkbox"/> Android for Work	Internal Exchange host
<input checked="" type="checkbox"/> Samsung SAFE	Internal server port
<input checked="" type="checkbox"/> Samsung KNOX	Internal server path
<input checked="" type="checkbox"/> Windows Phone	Use SSL for internal Exchange host <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Windows Desktop/Tablet	External Exchange host
3 Assignment	External server port
	External server path

- **Nome de conta do Exchange ActiveSync:** digite a descrição da conta de email exibida nos dispositivos do usuário.
- **Usuário:** especifique o nome do usuário da conta de usuário do Exchange. Você pode usar a macro de sistema \$user.username nesse campo para procurar automaticamente os nomes dos usuários.
- **Endereço de email:** especifique o endereço de email completo. Você pode usar a macro de sistema \$user.mail nesse campo para procurar automaticamente as contas de email dos usuários.
- **Usar OAuth:** se definido como **On**, a conexão usará OAuth para autenticação. O padrão é **Off**. Essa opção se aplica ao macOS 10.14 e posterior.
- **URL de login do OAuth:** especifica o URL a ser carregado em uma exibição da Web para autenticar usando o OAuth quando o Serviço de Descoberta Automática não for usado. Esse campo aparece quando **Usar OAuth** está definido como **On**.
- **Senha:** digite uma senha opcional para a conta de usuário do Exchange. Essa configuração não aparece quando **Usar OAuth** está **On**.
- **Host interno do Exchange:** se desejar que os nomes de host interno e externo do Exchange sejam diferentes, digite um nome de host interno do Exchange opcional.
- **Porta de servidor interno:** se você desejar que as portas de servidor interno e externo do Exchange sejam diferentes, digite um número de porta de servidor interno do Exchange opcional.
- **Caminho de servidor interno:** se você desejar que os caminhos de servidor interno e externo do Exchange sejam diferentes, digite um caminho de servidor interno do Exchange opcional.

- **Usar SSL para host interno do Exchange:** selecione se as conexões entre os dispositivos dos usuários e o host interno do Exchange devem ser protegidas. O padrão é **On**.
- **Host externo do Exchange:** se você deseja que os nomes de host interno e externo do Exchange sejam diferentes, digite um nome de host externo do Exchange opcional.
- **Porta do servidor externo:** se você deseja que as portas de servidor interno e externo do Exchange sejam diferentes, digite um número de porta opcional do servidor externo do Exchange.
- **Caminho de servidor externo:** se você deseja que os caminhos de servidor interno e externo do Exchange sejam diferentes, digite um caminho de servidor externo do Exchange opcional.
- **Usar SSL para host externo do Exchange:** selecione se as conexões entre os dispositivos dos usuários e o host interno do Exchange devem ser protegidas. O padrão é **On**.
- **Permitir Mail Drop:** selecione se os usuários têm permissão para compartilhar arquivos sem fio entre dois Macs, sem a necessidade de conexão com uma rede existente. O padrão é **Off**.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra.
 - **Permitir que o usuário remova a política:** você pode selecionar quando os usuários podem remover a política do dispositivo. Selecione **Sempre**, **Código secreto obrigatório** ou **Nunca** no menu. Se você selecionar **Código secreto obrigatório**, digite um código secreto no campo **Código secreto de remoção**.
 - **Escopo do perfil:** selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

Android Enterprise

Exchange Policy	Exchange Policy
1 Policy Info	This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.
2 Platforms	<p>Server name or IP address *</p> <input type="text"/>
<input type="checkbox"/> iOS	Domain <input type="text"/>
<input type="checkbox"/> macOS	User ID * <input type="text"/>
<input type="checkbox"/> Android HTC	Password <input type="text"/>
<input type="checkbox"/> Android TouchDown	Email address <input type="text"/>
<input checked="" type="checkbox"/> Android for Work	Identity credential (keystore or PKI) <input type="text" value="None"/>
<input checked="" type="checkbox"/> Samsung SAFE	
<input checked="" type="checkbox"/> Samsung KNOX	► Deployment Rules

- **Nome ou endereço IP do servidor:** digite o nome de host ou o endereço IP do Exchange Server.
- **Domínio:** digite o domínio no qual o Exchange Server reside. Você pode usar a macro de sistema \$user.domainname nesse campo para procurar automaticamente os nomes de domínio dos usuários.
- **ID do usuário:** especifique o nome do usuário da conta de usuário do Exchange. Você pode usar a macro de sistema \$user.username nesse campo para procurar automaticamente os nomes dos usuários.
- **Senha:** digite uma senha opcional para a conta de usuário do Exchange.
- **Endereço de email:** especifique o endereço de email completo. Você pode usar a macro de sistema \$user.mail nesse campo para procurar automaticamente as contas de email dos usuários.
- **Credencial de identidade (keystore ou PKI):** na lista, clique em uma credencial de identidade opcional se você tiver configurado um provedor de identidade para o XenMobile. Esse campo só é necessário quando o Exchange exige uma autenticação de certificado cliente. O padrão é **Nenhum**.

Configurações do Samsung SAFE e do Samsung KNOX

Exchange Policy	Exchange Policy
1 Policy Info	This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.
2 Platforms	
<input type="checkbox"/> iOS	Server name or IP address *
<input type="checkbox"/> macOS	Domain
<input type="checkbox"/> Android HTC	User ID *
<input type="checkbox"/> Android TouchDown	Password
<input type="checkbox"/> Android for Work	Email address *
<input checked="" type="checkbox"/> Samsung SAFE	Identity credential (keystore or PKI) None
<input checked="" type="checkbox"/> Samsung KNOX	Use SSL connection <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Windows Phone	Sync contacts <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Windows Desktop/Tablet	Sync calendar <input checked="" type="checkbox"/>
	Default account <input checked="" type="checkbox"/>

- **Nome ou endereço IP do servidor:** digite o nome de host ou o endereço IP do Exchange Server.
- **Domínio:** digite o domínio no qual o Exchange Server reside. Você pode usar a macro de sistema \$user.domainname nesse campo para procurar automaticamente os nomes de domínio dos usuários.
- **ID do usuário:** especifique o nome do usuário da conta de usuário do Exchange. Você pode usar a macro de sistema \$user.username nesse campo para procurar automaticamente os nomes dos usuários.
- **Senha:** digite uma senha opcional para a conta de usuário do Exchange.
- **Endereço de email:** especifique o endereço de email completo. Você pode usar a macro de sistema \$user.mail nesse campo para procurar automaticamente as contas de email dos usuários.
- **Credencial de identidade (keystore ou PKI):** na lista, clique em uma credencial de identidade opcional se você tiver configurado um provedor de identidade para o XenMobile. Esse campo só é necessário quando o Exchange exige uma autenticação de certificado cliente.
- **Usar conexão SSL:** selecione se as conexões entre os dispositivos dos usuários e o Exchange Server devem ser protegidas. O padrão é **On**.
- **Sincronizar os contatos:** selecione se a sincronização dos contatos dos usuários entre os dispositivos e o Exchange Server deve ser ativada. O padrão é **On**.
- **Sincronizar o calendário:** selecione se a sincronização do calendário dos usuários entre os dispositivos e o Exchange Server deve ser ativada. O padrão é **On**.
- **Conta padrão:** selecione se as contas do Exchange dos usuários devem ser o padrão para envio de email dos respectivos dispositivos. O padrão é **On**.

Configurações do Windows Phone e do Windows Desktop/Tablet

Exchange Policy	Exchange Policy
1 Policy Info	This policy configures Microsoft Exchange ActiveSync so users can run Exchange email on their devices. When you create this policy, you need the host name or IP address for the Exchange Server.
2 Platforms	
<input type="checkbox"/> iOS	Account name or display name *
<input type="checkbox"/> macOS	Server name or IP address *
<input type="checkbox"/> Android HTC	Domain
<input type="checkbox"/> Android TouchDown	User ID or user name *
<input type="checkbox"/> Android for Work	Email address *
<input type="checkbox"/> Samsung SAFE	Use SSL connection <input type="radio"/> OFF
<input type="checkbox"/> Samsung KNOX	Sync items
<input type="checkbox"/> Windows Phone	Past days to sync
<input checked="" type="checkbox"/> Windows Desktop/Tablet	Frequency
	Logging level

Nota:

Essa política não permite que você defina a senha do usuário. Os usuários devem definir esse parâmetro nos dispositivos deles depois que você enviar a política por push.

- **Nome da conta ou nome de exibição:** digite o nome de conta do Exchange ActiveSync.
- **Nome ou endereço IP do servidor:** digite o nome de host ou o endereço IP do Exchange Server.
- **Domínio:** insira o domínio no qual o Exchange Server reside. Você pode usar a macro de sistema \$user.domainname nesse campo para procurar automaticamente os nomes de domínio dos usuários.
- **ID de usuário ou nome de usuário:** especifique o nome do usuário da conta de usuário do Exchange. Você pode usar a macro de sistema \$user.username nesse campo para procurar automaticamente os nomes dos usuários.
- **Endereço de email:** especifique o endereço de email completo. Você pode usar a macro de sistema \$user.mail nesse campo para procurar automaticamente as contas de email dos usuários.
- **Usar conexão SSL:** selecione se as conexões entre os dispositivos dos usuários e o Exchange Server devem ser protegidas. O padrão é **Off**.
- **Últimos dias para sincronizar:** na lista, clique em quantos dias no passado todo o conteúdo do dispositivo deve ser sincronizado com o Exchange Server. O padrão é **Todo o conteúdo**.
- **Frequência:** na lista, clique na agenda a ser usada durante a sincronização dos dados que são enviados para o dispositivo do Exchange Server. O padrão é **Quando chega**.
- **Nível de log:** na lista, clique em **Desativado**, **Básico** ou **Avançado** para especificar o nível de detalhes do registro em log da atividade do Exchange. O **padrão é Desativado**.

Política de dispositivo de arquivo

May 6, 2021

Você pode adicionar e implantar arquivos para que os usuários acessem em seus dispositivos Android e Android Enterprise. Você especifica o diretório onde deseja armazenar o arquivo no dispositivo. Por exemplo, você deseja que os usuários recebam um documento da empresa ou um arquivo .pdf. Implante o arquivo em dispositivos e informe aos usuários onde o arquivo está localizado.

Os dispositivos Android não suportam a execução de scripts nativamente. Os usuários precisam de software de terceiros para executar scripts.

Você pode adicionar os seguintes tipos de arquivo com essa política:

- Arquivos baseados em texto (.xml, .html, .py e assim por diante)
- Outros arquivos, como documentos, fotos, planilhas ou apresentações
- Para Windows Mobile e Windows CE somente: Arquivos de script criados com MortScript

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do Android Enterprise

Files Policy

This policy lets you upload files and executable scripts to devices.

File to be imported * Browse

File type

File

Script

Replace macro expressions OFF ?

Destination folder ?

Destination file name ?

If file exists ?

Copy file only if different

Do not copy

► Deployment Rules

- **Arquivo a ser importado:** para selecionar o arquivo a ser importado, clique em **Procurar** e navegue até o local do arquivo.
- **Tipo de arquivo:** selecione **Arquivo** ou **Script**.
- **Executar imediatamente:** quando você seleciona **Script**, a opção **Executar imediatamente** aparece. Nada acontece quando você habilita essa configuração. Os usuários devem executar o script manualmente.- **Substituir expressões de macro:** selecione se você deseja substituir nomes de token de macro em um script por uma propriedade de dispositivo ou usuário. Para ver a sintaxe de macro, consulte Macros. O padrão é **Off**.
- **Pasta de destino:** na lista, selecione a localização na qual o arquivo enviado deve ser armazenado ou clique em **Adicionar nova** para escolher uma localização de arquivo não listada. Você pode usar a macro %XenMobile Folder%\ ou %Flash Storage%\ como o início de um identificador de caminho.
- **Nome do arquivo de destino:** opcional. Se você precisar alterar um nome de arquivo antes de implantá-lo em um dispositivo, digite o nome do arquivo.
- **Se o arquivo existir:** na lista, selecione se deseja copiar um arquivo existente. O padrão é **Copiar o arquivo somente se for diferente**.

Configurações do Android

- **Arquivo a ser importado:** selecione o arquivo a ser importado clicando em **Procurar** e navegando até a localização do arquivo.
- **Tipo de arquivo:** selecione **Arquivo** ou **Script**.
- **Executar imediatamente:** quando você seleciona **Script**, a opção **Executar imediatamente** aparece. Nada acontece quando você habilita essa configuração. Os usuários devem executar o script manualmente. - **Substituir expressões de macro:** selecione se você deseja substituir nomes de token de macro em um script por uma propriedade de dispositivo ou usuário. O padrão é **Off**.
- **Pasta de destino:** na lista, selecione a localização na qual o arquivo enviado deve ser armazenado ou clique em **Adicionar nova** para escolher uma localização de arquivo não listada. Além disso, você pode usar a macro %XenMobile Folder%\ ou %Flash Storage%\ como o início de um identificador de caminho.
- **Nome do arquivo de destino:** opcionalmente, digite um nome diferente para o arquivo se ele for alterado antes de ser implantado em um dispositivo.
- **Copiar arquivo somente se for diferente:** na lista, selecione se o arquivo deverá ser copiado se for diferente do arquivo existente. O padrão é copiar o arquivo somente se ele for diferente.

Configurações do Windows Mobile/CE

- **Arquivo a ser importado:** selecione o arquivo a ser importado clicando em Procurar e navegando até a localização do arquivo.
- **Tipo de arquivo:** selecione **Arquivo** ou **Script**.
- **Executar imediatamente:** quando você seleciona **Script**, **Executar imediatamente** aparece. Selecione se o script deve ser executado quando o arquivo é carregado. O padrão é **Off**.
- **Substituir expressões de macro:** selecione se você deseja substituir nomes de token de macro em um script com uma propriedade de dispositivo ou usuário. O padrão é **Off**.
- **Pasta de destino:** na lista, selecione a localização na qual o arquivo enviado deve ser armazenado ou clique em **Adicionar nova** para escolher uma localização de arquivo não listada. Além disso, você pode usar qualquer uma das macros abaixo como o início de um identificador de caminho:
 - %Flash Storage%\
 - %XenMobile Folder%\
 - %Program Files%\
 - %My Documents%\
 - %Windows%\
- **Nome do arquivo de destino:** opcionalmente, digite um nome diferente para o arquivo se ele for alterado antes de ser implantado em um dispositivo.
- **Copiar arquivo somente se for diferente:** na lista, selecione se o arquivo deverá ser copiado

se for diferente do arquivo existente. O padrão é copiar o arquivo somente se ele for diferente.

- **Arquivo somente leitura:** selecione se o arquivo deve ser somente leitura. O padrão é **Off**.
- **Arquivo oculto:** selecione se o arquivo não deve ser mostrado na lista de arquivos. O padrão é **Off**.

Política de dispositivo FileVault

August 31, 2018

O recurso de Criptografia de disco do FileVault do macOS protege o volume do sistema, criptografando seu conteúdo. Com o FileVault ativado em um dispositivo macOS, um usuário efetua login com a senha da conta sempre que o dispositivo é iniciado. Se o usuário perde a sua senha, uma chave de recuperação permite desbloquear o disco e redefinir sua senha.

A política do dispositivo XenMobile, FileVault, habilita as telas de configuração do usuário do FileVault e define as configurações, como as chaves de recuperação. Para obter mais informações sobre o FileVault, consulte o site de suporte da Apple, <https://support.apple.com>.

Para adicionar a política FileVault, acesse **Configurar > Políticas de dispositivo**.

Configurações do macOS

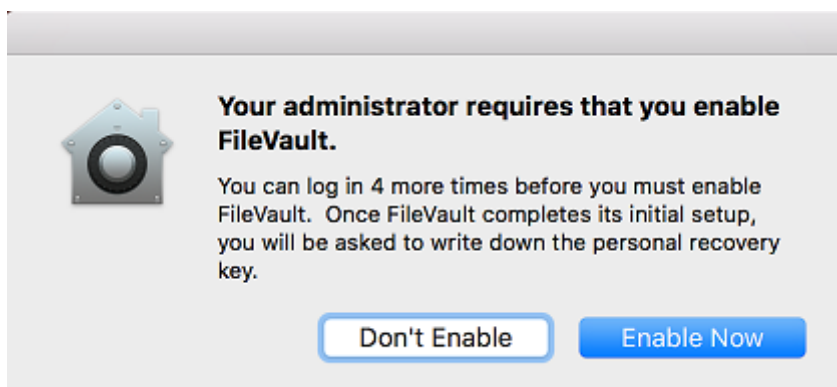
FileVault Policy	FileVault Policy
1 Policy Info	This policy lets you enable FileVault device encryption on enrolled macOS devices.
2 Platforms	Prompt for FileVault setup during logout <input type="radio"/> OFF ⓘ
<input checked="" type="checkbox"/> macOS	Maximum times to skip FileVault setup <input type="text" value="0"/> ⓘ
3 Assignment	Recovery key type <input type="text" value="Personal recovery key"/> ⓘ
	Show personal recovery key <input checked="" type="radio"/> ON ⓘ
	▶ Deployment Rules

- **Solicitar a configuração do FileVault durante o logout:** se estiver **I**, solicita que o usuário ative o FileVault durante os próximos N logouts, conforme especificado pela opção **Número máximo de vezes para ignorar a configuração do FileVault**. Se o valor for **0**, o aviso de senha do FileVault não aparecerá.

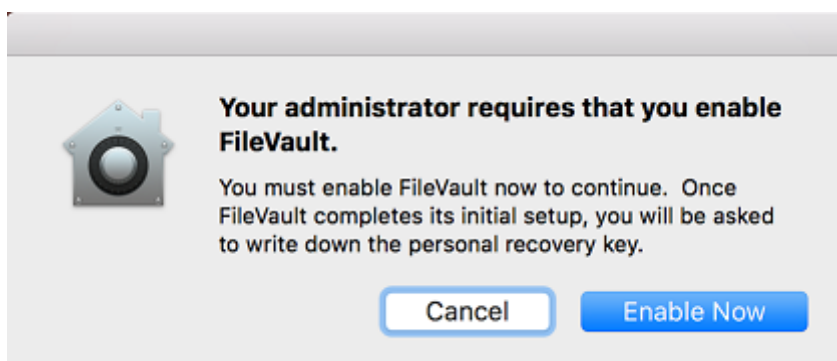
Depois de implantar a política FileVault com essa configuração ativada, a seguinte tela aparece quando um usuário faz o logoff do dispositivo. A tela dá ao usuário a opção de ativar o FileVault antes de logoff.

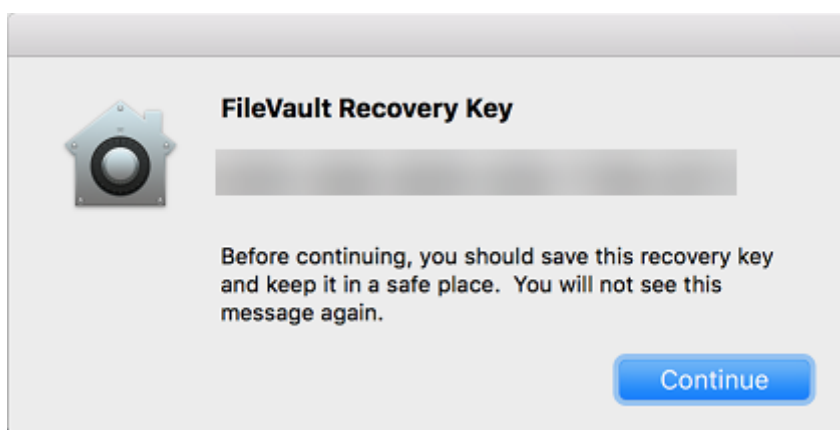


Se o valor **Número máximo de vezes para ignorar a configuração do FileVault** não for 0: depois que você implantar a política do FileVault com essa configuração desativada e, quando o usuário fizer logon, a tela a seguir será exibida.



Se o valor **Número máximo de vezes para ignorar a configuração do FileVault** for 0 ou o usuário tiver ignorado a configuração do número máximo de vezes, a tela a seguir será exibida.





Política de dispositivo de fonte

April 23, 2020

Você pode adicionar uma política de dispositivo ao XenMobile para adicionar mais fontes aos dispositivos iOS e macOS. As fontes devem ser TrueType (.ttf) ou OpenType (.oft). Coleções de fontes (.ttc ou .otc) não são compatíveis.

Para o iOS, essa política se aplica somente ao iOS 7.0 e versões posteriores.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

- **Nome visível para o usuário:** digite o nome que os usuários veem nas respectivas listas de fonte.
- **Arquivo de fonte:** selecione o arquivo de fonte a ser adicionado aos dispositivos dos usuários clicando em **Procurar** e navegando até a localização do arquivo.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do macOS

- **Nome visível para o usuário:** digite o nome que os usuários veem nas respectivas listas de fonte.
- **Arquivo de fonte:** selecione o arquivo de fonte a ser adicionado aos dispositivos dos usuários clicando em **Procurar** e navegando até a localização do arquivo.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra.
 - **Permitir que o usuário remova a política:** você pode selecionar quando os usuários podem remover a política do dispositivo. Selecione **Sempre**, **Código secreto obrigatório** ou **Nunca** no menu. Se você selecionar **Código secreto obrigatório**, digite um código secreto no campo **Código secreto de remoção**.
 - **Escopo do perfil:** selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

Política de dispositivo de layout de tela inicial

April 1, 2021

Você pode especificar o layout de aplicativos e pastas para a tela inicial do iOS. A política de dispositivo de layout da tela inicial é para dispositivos supervisionados iOS 9.3 e versões posteriores.

Importante:

Implantar várias políticas de layout da tela inicial em um dispositivo resulta em um erro do iOS no dispositivo. Essa limitação é aplicável independentemente de você definir a tela inicial usando essa política do XenMobile ou usando o Apple Configurator.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

- Para cada uma das áreas da tela que você deseja configurar (como **Dock** ou **Página 1**), clique em **Adicionar**.
- **Tipo:** escolha **Aplicativo**, **Pasta** ou **Clip web**.

A configuração **Uso restrito do aplicativo > Permitir apenas alguns aplicativos** em [Política de dispositivo de restrições](#) pode impedir que os cliques web apareçam corretamente na tela inicial. Para que os cliques web apareçam corretamente, siga um destes procedimentos:

- Defina **Uso restrito do aplicativo** para **Permitir todos os aplicativos** ou **Não permitir alguns aplicativos**.
- Com **Uso restrito do aplicativo** definido como **Permitir apenas alguns aplicativos**, adicione um aplicativo com o ID do pacote `com.apple.webapp` para permitir cliques web.

- **Nome para exibição:** o nome que aparece na tela inicial do aplicativo ou pasta.

- **Valor:** para aplicativos, digite o identificador do pacote. Para pastas, digite uma lista de identificadores de pacote separados por vírgulas. Para clips web, digite o ID do pacote `com.apple.webClip.managed` e configure o URL do clip web na política de clip web. Se existir mais de um valor clip web com o mesmo URL, o comportamento fica indefinido nos dispositivos iOS 11.3 e posteriores.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.
 - **Escopo do perfil:** selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Esta opção está disponível apenas no iOS 9.3 e posterior.

Política de dispositivo de importação do perfil de iOS e macOS

April 23, 2020

Você pode importar arquivos XML de configuração de dispositivo para dispositivos iOS e macOS para o XenMobile. O arquivo contém as políticas de segurança do dispositivo e as restrições que você prepara com o Apple Configurator.

Você pode colocar um dispositivo iOS no modo supervisionado no Apple Configurator, como descrito posteriormente neste artigo. Para obter mais informações sobre como usar o Apple Configurator para criar um arquivo de configuração, consulte a página [Configurator Support](#) da Apple.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do iOS e do MacOS

Import iOS & macOS Profile Policy	Import iOS & macOS Profile Policy This policy lets you import a device configuration XML file for either iOS or macOS. The file contains device security policies and restrictions that you prepare with the Apple Configurator.
1 Policy Info	ios configuration profile <input type="text"/> <input type="button" value="Browse"/>
2 Platforms	▶ Deployment Rules
<input checked="" type="checkbox"/> iOS	
<input checked="" type="checkbox"/> macOS	
3 Assignment	

- **Perfil de configuração do iOS** ou **Perfil de configuração do macOS**: para selecionar o arquivo de configuração para importar, clique em **Procurar** e navegue até a localização do arquivo.

Colocar um dispositivo iOS no modo Supervisionado com o Apple Configurator

Para usar o Apple Configurator, você precisa de um computador Apple que execute o macOS 10.7.2 ou versões posteriores.

Importante:

Colocar um dispositivo no modo supervisionado instala a versão selecionada do iOS no dispositivo, apagando completamente os dados ou os aplicativos do usuário armazenados anteriormente.

1. Instale o Apple Configurator pelo iTunes.
2. Conecte o dispositivo iOS ao seu computador Apple.
3. Inicie o Apple Configurator. O Configurator mostra que você tem um dispositivo a ser preparado para supervisão.
4. Para preparar o dispositivo para supervisão:
 - a) Mude o controle de **Supervision** para **On**. A Citrix recomenda que você escolha essa configuração se pretender manter o controle contínuo do dispositivo reaplicando uma configuração regularmente.
 - b) Opcionalmente, forneça um nome para o dispositivo.
 - c) No iOS, clique em **Latest** para obter a versão mais recente do iOS que você deseja instalar.
5. Quando você estiver pronto para preparar o dispositivo para supervisão, clique em **Prepare**.

Política de dispositivo de gerenciamento de keyguard

December 22, 2020

O Android keyguard gerencia as telas de bloqueio de dispositivo e de Work Challenge. Esta política permite que você gerencie recursos para o keyguard do perfil de trabalho do Android Enterprise e a proteção de teclado avançada do dispositivo. Você pode controlar:

- Gerenciamento de proteção do teclado em dispositivos de perfil de trabalho. Você pode especificar os recursos disponíveis para os usuários antes que eles desbloqueiem a proteção do teclado do dispositivo e o keyguard do Work Challenge. Por exemplo, por padrão, os usuários podem usar o desbloqueio por impressão digital e exibir notificações não editadas na tela de bloqueio.

- Gerenciamento de proteção do teclado em dispositivos totalmente gerenciados e dedicados. Você pode especificar os recursos disponíveis, como agentes de confiança e câmera segura, antes que desbloqueiem a tela de proteção do teclado. Ou, você pode optar por desativar todos os recursos de proteção do teclado.
- Gerenciamento de proteção do teclado em dispositivos totalmente gerenciados com perfis de trabalho. Você pode usar uma política de Gerenciamento de proteção do teclado para aplicar configurações separadas ao dispositivo e ao perfil de trabalho.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do Android Enterprise

Keyguard Management Policy	Keyguard Management Policy
1 Policy Info	Android keyguard manages the device and work challenge lock screens. This policy lets you control the features available to users before they unlock the device keyguard and the work challenge keyguard.
2 Platforms	
<input checked="" type="checkbox"/> Android Enterprise	
3 Assignment	
	<p>Apply to fully managed devices with a work profile <input type="checkbox"/> OFF</p> <p>Work profile keyguard features</p> <p>Disable trust agents <input type="checkbox"/> OFF ?</p> <p>Disable biometric authentication <input type="checkbox"/> OFF ?</p> <p>Disable fingerprint unlock <input type="checkbox"/> OFF ?</p> <p>Disable face authentication <input type="checkbox"/> OFF ?</p> <p>Disable iris authentication <input type="checkbox"/> OFF ?</p> <p>Disable unredacted notifications <input type="checkbox"/> OFF ?</p> <p>Fully managed device keyguard features</p> <p>Disable all keyguard features <input type="checkbox"/> OFF ?</p> <p>Disable trust agents <input type="checkbox"/> OFF ?</p> <p>Disable biometric authentication <input type="checkbox"/> OFF ?</p> <p>Disable fingerprint unlock <input type="checkbox"/> OFF ?</p> <p>Disable face authentication <input type="checkbox"/> OFF ?</p> <p>Disable iris authentication <input type="checkbox"/> OFF ?</p> <p>Disable all notifications <input type="checkbox"/> OFF ?</p> <p>Disable unredacted notifications <input type="checkbox"/> OFF ?</p> <p>Disable secure camera <input type="checkbox"/> OFF ?</p>

- **Aplicar a dispositivos totalmente gerenciados com um perfil de trabalho:** permite que você defina as configurações de política de dispositivo de Gerenciamento de proteção do teclado para dispositivos totalmente gerenciados com perfis de trabalho.

Quando essa configuração está **Ativada**, você pode aplicar configurações separadas ao dispositivo e ao perfil de trabalho em dispositivos totalmente gerenciados com perfis de trabalho.

Quando essa configuração está **Desativada**, você pode aplicar configurações a dispositivos com perfil de trabalho ou dispositivos totalmente gerenciados. As configurações definidas para perfis de trabalho só se aplicam a dispositivos com perfil de trabalho. As configu-

rações definidas para dispositivos totalmente gerenciados aplicam-se apenas a dispositivos totalmente gerenciados.

O padrão é **Desativado**.

- **Recursos de proteção do teclado de perfil de trabalho:** controla se os seguintes recursos estão disponíveis antes que um usuário desbloqueie a proteção do teclado do perfil de trabalho (tela de bloqueio).
 - **Desativar agentes de confiança:** se **Desativado**, os agentes de confiança podem operar em telas seguras de proteção do teclado quando um desafio é definido no perfil de trabalho. Defina como **Ativado** para desativar todos os agentes de confiança no perfil de trabalho. O padrão é **Desativado**.
 - **Desativar a autenticação biométrica:** se **Desativado**, a autenticação biométrica estará disponível em telas seguras de proteção do teclado quando um desafio for definido no perfil de trabalho. Defina como **Ativado** para desativar a autenticação biométrica no perfil de trabalho. Essa configuração desabilita o desbloqueio por impressão digital, autenticação facial e autenticação por íris. O padrão é **Desativado**. Para Android 9.0 e posterior.
 - **Desativar o desbloqueio por impressão digital:** se **Ativado**, o desbloqueio por impressão digital não estará disponível em telas seguras de proteção do teclado quando um desafio for definido no perfil de trabalho. Defina como **Desativado** para habilitar o desbloqueio por impressão digital no perfil de trabalho. O padrão é **Desativado**.
 - **Desabilitar autenticação facial:** se **Desativado**, a autenticação facial estará disponível em telas seguras de proteção do teclado quando um desafio for definido no perfil de trabalho. Defina como **Ativado** para desativar a autenticação facial no perfil de trabalho. O padrão é **Desativado**. Para Android 9.0 e posterior.
 - **Desabilitar autenticação por íris:** se **Desativado**, a autenticação por íris estará disponível em telas seguras de proteção do teclado quando um desafio for definido no perfil de trabalho. Defina como **Ativado** para desativar a autenticação por íris no perfil de trabalho. O padrão é **Desativado**. Para Android 9.0 e posterior.
 - **Desativar notificações não editadas:** se **Desativado**, as notificações editadas e não editadas aparecerão nas telas seguras de proteção do teclado. Defina como **Ativado** para desativar notificações não editadas e mostrar somente notificações editadas. O padrão é **Desativado**.
- **Recursos de proteção de teclado de dispositivo totalmente gerenciado:** controla se os seguintes recursos estão disponíveis antes que um usuário desbloqueie a proteção do teclado do dispositivo (tela de bloqueio). Esses recursos se aplicam a dispositivos totalmente gerenciados ou dedicados.
 - **Desativar todos os recursos de proteção do teclado:** se **Desativado**, todas as personalizações atuais e futuras de proteção do teclado estarão disponíveis nas telas seguras de proteção do teclado. Defina como **Ativado** para desativar todas as personalizações de

proteção do teclado. O padrão é **Desativado**.

- **Desativar agentes de confiança:** se **Desativado**, os agentes de confiança podem operar nas telas seguras de proteção do teclado. Defina como **Ativado** para desativar os agentes de confiança. O padrão é **Desativado**.
- **Desativar a autenticação biométrica:** se **Desativado**, a autenticação biométrica estará disponível em telas seguras de proteção do teclado quando um desafio for definido no dispositivo. Defina como **Ativado** para desativar a autenticação biométrica no dispositivo. Isso desabilita o desbloqueio por impressão digital, autenticação facial e autenticação por íris. O padrão é **Desativado**. Para Android 9.0 e posterior.
- **Desativar o desbloqueio por impressão digital:** se **Desativado**, o desbloqueio por impressão digital estará disponível em telas seguras de proteção do teclado quando um desafio for definido no dispositivo. Defina como **Ativado** para desativar o desbloqueio por impressão digital no dispositivo. O padrão é **Desativado**.
- **Desabilitar autenticação facial:** se **Desativado**, a autenticação facial estará disponível em telas seguras de proteção do teclado quando um desafio for definido no dispositivo. Defina como **Ativado** para desativar a autenticação facial no dispositivo. O padrão é **Desativado**. Para Android 9.0 e posterior.
- **Desabilitar autenticação por íris:** se **Desativado**, a autenticação por íris estará disponível em telas seguras de proteção do teclado quando um desafio for definido no dispositivo. Defina como **Ativado** para desativar a autenticação por íris no dispositivo. O padrão é **Desativado**. Para Android 9.0 e posterior.
- **Desativar todas as notificações:** se **Desativado**, todas as notificações aparecerão nas telas seguras de proteção do teclado. Defina como **Ativado** para mostrar todas as notificações. O padrão é **Desativado**.
- **Desativar notificações não editadas:** se **Desativado**, as notificações editadas e não editadas aparecerão nas telas seguras de proteção do teclado. Defina como **Ativado** para desativar notificações não editadas e mostrar somente notificações editadas. O padrão é **Desativado**.
- **Desativar câmera segura:** se **Desativado**, a câmera segura estará disponível em telas seguras de proteção do teclado. Defina como **Ativado** para desativar a câmera segura. O padrão é **Desativado**.

Política de dispositivo do quiosque

November 30, 2020

A política de quiosque permite restringir dispositivos no modo quiosque ao limitar os aplicativos que podem ser executados. O XenMobile não controla qual parte do dispositivo bloqueia no modo de quiosque. O dispositivo gerencia as configurações do modo de quiosque depois que você implanta a

política.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Para colocar um dispositivo Samsung SAFE no modo de quiosque

1. Ative a chave de API do Samsung SAFE no dispositivo móvel, conforme descrito em [Políticas de dispositivo de chave de licença MDM Samsung](#). Esta etapa permite que você habilite as políticas em dispositivos Samsung SAFE.
2. Ative o Firebase Cloud Messaging para dispositivos Android, conforme descrito em [Firebase Cloud Messaging](#). Esta etapa permite que dispositivos Android se conectem ao XenMobile.
3. Adicione uma política de dispositivo do Quiosque, conforme descrito na próxima seção.
4. Atribua essas três políticas de dispositivo aos grupos de entrega apropriados. Considere se você deseja incluir outras políticas, como de inventário de aplicativos, nesses grupos de entrega.

Para remover os dispositivos móveis do modo de Quiosque, crie uma política de dispositivo que tenha o **Modo de quiosque** definido como **Desativar**. Atualize os grupos de entrega para remover a política de quiosque que ativou o modo de quiosque e para adicionar a política de quiosque que desativa o modo de quiosque.

Para adicionar uma política de dispositivo

Todos os aplicativos que você especificar para o Modo de quiosque já deverão estar instalados nos dispositivos do usuário.

Algumas opções se aplicam somente à API do Samsung Mobile Device Management (MDM) 4.0 e posterior.

Configurações do Samsung SAFE

Você pode especificar que apenas um aplicativo, ou aplicativos específicos, pode ser utilizado. Essa política é útil para dispositivos corporativos que foram projetados para executar somente um tipo ou classe específico de aplicativos. A política também permite que você escolha imagens personalizadas para a tela inicial do dispositivo e papéis de parede da tela de bloqueio para quando o dispositivo estiver no Modo de quiosque.

- **Modo de quiosque:** clique em **Ativar** ou **Desativar**. O padrão é **Ativar**. Quando você clica em **Desativar**, todas as opções a seguir desaparecem.
- **Pacote de inicializador:** a Citrix recomenda deixar esse campo em branco, a menos que você tenha desenvolvido um inicializador interno para permitir que os usuários abram os aplicativos

de Quiosque. Se você usar um inicializador interno, digite o nome completo do pacote de aplicativos do inicializador.

- **Número de telefone de emergência:** digite um número de telefone opcional. Qualquer um pode usar esse método para contatar sua empresa para localizar um dispositivo perdido. Aplica-se somente ao MDM 4.0 e versões posteriores.
- **Permitir barra de navegação:** selecione se deseja permitir que os usuários visualizem e usem a barra de navegação no Modo de quiosque. Aplica-se somente ao MDM 4.0 e versões posteriores. O padrão é **On**.
- **Permitir modo de várias janelas:** selecione se deseja permitir que os usuários usem várias janelas enquanto estão no Modo de quiosque. Aplica-se somente ao MDM 4.0 e versões posteriores. O padrão é **On**.
- **Permitir barra de status:** selecione se deseja permitir que os usuários visualizem a barra de status no Modo de quiosque. Aplica-se somente ao MDM 4.0 e versões posteriores. O padrão é **On**.
- **Permitir barra de sistema:** selecione se deseja permitir que os usuários visualizem a barra de sistema no Modo de quiosque. O padrão é **On**.
- **Permitir gerenciador de tarefas:** selecione se deseja permitir que os usuários visualizem e usem o gerenciador de tarefas no Modo de quiosque. O padrão é **On**.
- **Alterar código secreto SAFE comum:** essa configuração ajuda a proteger contra alterações inadvertidas no campo Código secreto SAFE comum. Quando essa configuração é **Off**, não é possível alterar o campo Código secreto SAFE comum. O padrão é **Off**.
- **Código secreto SAFE comum:** se você definir uma política de código secreto geral para todos os dispositivos Samsung SAFE, digite este código secreto opcional neste campo.
- **Papéis de parede**
 - **Definir um papel de parede para a página inicial:** selecione se deseja usar uma imagem personalizada para a tela inicial no Modo de quiosque. O padrão é **Off**.
 - * **Imagem da página inicial:** ao ativar a opção **Definir um papel de parede para a página inicial**, selecione o arquivo de imagem clicando em **Procurar** e navegando até a localização do arquivo.
 - **Definir um papel de parede de bloqueio:** selecione se deseja usar uma imagem personalizada para a tela de bloqueio no Modo de quiosque. O padrão é **Off**. Aplica-se somente ao MDM 4.0 e versões posteriores.
 - * **Imagem de bloqueio:** ao ativar a opção **Definir um papel de parede de bloqueio**, selecione o arquivo de imagem clicando em **Procurar** e navegando até a localização do arquivo.
- **Aplicativos:** para cada propriedade de usuário que você desejar adicionar ao Modo de quiosque, clique em **Adicionar** e faça o seguinte:
 - **Novo aplicativo a ser adicionado:** digite o nome completo do aplicativo a ser adicionado. Por exemplo, com.android.calendar permite aos usuários usar o aplicativo de calendário

do Android.

- Clique em **Salvar** para adicionar o aplicativo ou em **Cancelar** para cancelar a adição do aplicativo.

Configurações do Android Enterprise

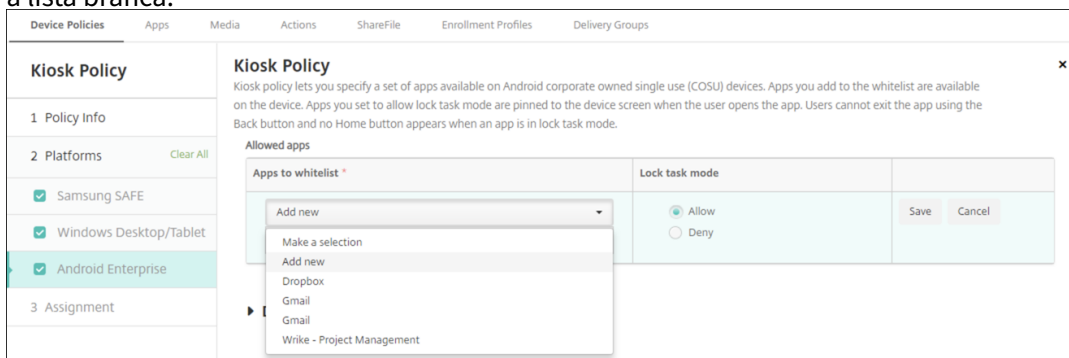
Você pode permitir aplicativos e definir o modo de bloqueio de tarefa em dispositivos Android Enterprise dedicados, também conhecidos como dispositivos corporativos para uso único (COSU, Corporate Owned Single Use). Por padrão, os serviços Secure Hub e Google Play estão na lista de permissão.

Para permitir um aplicativo, clique em **Adicionar**. Você pode permitir vários aplicativos. Para obter mais informações, consulte [Android Enterprise](#).

Nota:

O console XenMobile Server inclui os termos “lista negra” e “lista branca”. Estamos alterando esses termos em uma próxima versão para “lista de bloqueio” e “lista de permissão”.

- **Aplicativos para lista branca:** insira o nome do pacote do aplicativo que você deseja colocar na lista branca ou selecione o aplicativo na lista.
 - Clique em **Adicionar novo** para inserir o nome do pacote do aplicativo aprovado para mostrar na lista.
 - Selecione o aplicativo existente na lista. A lista mostra aplicativos que estão carregados no XenMobile Server. Por padrão, os serviços Secure Hub e Google Play são acrescentados à lista branca.



- **Modo de bloqueio de tarefa:** escolha **Permitir** para definir o aplicativo a ser fixado na tela do dispositivo quando o usuário iniciar o aplicativo. Escolha **Negar** para que o aplicativo não seja fixado. Por padrão, os serviços Secure Hub e Google Play são permitidos. O padrão é **Permitir**.

Quando um aplicativo está no modo de bloqueio de tarefa, ele é fixado na tela do dispositivo quando o usuário o abre. O botão Início não aparece e o botão Voltar fica desativado. O usuário sai do aplicativo usando uma ação programada no aplicativo, como logoff.

Política de dispositivos de configuração de Launcher para Android

April 23, 2020

O Citrix Launcher permite que você personalize a experiência do usuário para dispositivos Android implantados pelo XenMobile. O Citrix Launcher e a política do dispositivo de configuração do Launcher não são compatíveis com o Android Enterprise.

Você pode adicionar uma política de Configuração para controlar estes recursos do Citrix Launcher:

- Gerenciar dispositivos Android para que os usuários possam acessar somente os aplicativos que você especificar.
- Opcionalmente, especifique uma imagem de logotipo personalizado para o ícone do Citrix Launcher e uma imagem de plano de fundo personalizado para o Citrix Launcher.
- Especifique uma senha que os usuários devem digitar para sair do Launcher.

Apesar do Citrix Launcher permitir aplicar essas restrições no nível de dispositivo, o iniciador concede aos usuários a flexibilidade operacional de que necessitam por meio do acesso incorporado às configurações de dispositivos como configurações de WiFi, Bluetooth e de código secreto de dispositivo. O Citrix Launcher não foi criado com a intenção de ser uma camada extra de segurança além da que a plataforma de dispositivo já fornece.

Depois de ter implantado o Citrix Launcher, o XenMobile o instala, substituindo o iniciador padrão do Android.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do Android

Launcher Configuration Policy	Launcher Configuration Policy						
1 Policy Info	This policy lets you define a configuration of an Android device launcher. Launcher app configuration						
2 Platforms	Define a logo image <input type="checkbox"/> OFF ⓘ						
<input checked="" type="checkbox"/> Android	Define a background image <input type="checkbox"/> OFF ⓘ						
3 Assignment	Allowed apps						
	<table border="1"><thead><tr><th>App name</th><th>Package name *</th><th>⊞ Add</th></tr></thead><tbody><tr><td></td><td></td><td></td></tr></tbody></table>	App name	Package name *	⊞ Add			
App name	Package name *	⊞ Add					
	Password <input type="password"/> ⓘ						
	▶ Deployment Rules						

- **Definir uma imagem de logotipo:** selecione se deve ser usada uma imagem de logotipo personalizada para o ícone do Citrix Launcher. O padrão é **Off**.
- **Imagem de logotipo:** ao ativar a opção **Definir uma imagem de logotipo**, selecione o arquivo de imagem clicando em **Procurar** e navegar para a localização do arquivo. Tipos de arquivo suportados são PNG, JPG, GIF, JPEG e GIF.

- **Definir uma imagem de fundo:** selecione se deve ser usada uma imagem personalizada para o fundo do Citrix Launcher. O padrão é **Off**.
- **Imagem de fundo:** ao ativar a opção **Definir uma imagem de fundo**, selecione o arquivo de imagem clicando em **Procurar** e navegando para a localização do arquivo. Tipos de arquivo suportados são PNG, JPG, GIF, JPEG e GIF.
- **Aplicativos permitidos:** para cada aplicativo que você deseja permitir no Citrix Launcher, clique em **Adicionar** e faça o seguinte:
 - **Novo aplicativo a ser adicionado:** digite o nome completo do aplicativo a ser adicionado. Por exemplo, com.android.calendar para o aplicativo de calendário do Android.
 - Clique em **Salvar** para adicionar o aplicativo ou em **Cancelar** para cancelar a adição do aplicativo.
- **Senha:** a senha que um usuário deve digitar para sair do Citrix Launcher.

Política de dispositivo do LDAP

April 23, 2020

Crie uma política de LDAP para os dispositivos iOS no XenMobile para fornecer informações sobre um servidor LDAP a ser usado, incluindo qualquer informação de conta necessária. A política também fornece um conjunto de políticas de pesquisa de LDAP a serem usadas ao consultar o servidor LDAP.

Você precisa do nome do host LDAP antes de configurar essa política.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

- **Descrição da conta:** insira uma descrição opcional da conta.
- **Nome de usuário da conta:** insira um nome de usuário opcional.
- **Senha da conta:** insira uma senha opcional. Use esse campo somente com perfis criptografados.
- **Nome do host LDAP:** insira o nome de host do servidor LDAP. Este campo é obrigatório.
- **Usar SSL:** selecione se uma conexão SSL com o servidor LDAP deve ser usada. O padrão é **On**.
- **Configurações de Pesquisa:** adicione configurações de pesquisa a serem usadas ao consultar o servidor LDAP. Você pode inserir quantas configurações de pesquisa desejar, mas deve adicionar pelo menos uma configuração para tornar a conta útil. Clique em **Adicionar** e faça o seguinte:
 - **Descrição:** digite uma descrição da configuração da pesquisa. Este campo é obrigatório.

- **Escopo:** escolha **Base**, **Um nível** ou **Subárvore** para definir o quão profunda a pesquisa na árvore LDAP deve ser. O padrão é **Base**.
 - * **Base** pesquisa o nó para o qual a base de pesquisa aponta.
 - * **Um nível** pesquisa o nó Base e um nível abaixo dele.
 - * **Subárvore** pesquisa o nó Base, além de todos os seus filhos, independentemente da profundidade.
- **Base de pesquisa:** digite o caminho para o nó no qual a pesquisa deve ser iniciada. Por exemplo, ou=people ou 0=example corp. Este campo é obrigatório.
- Clique em **Salvar** para adicionar a configuração de pesquisa ou em **Cancelar** para cancelar a inclusão dessa configuração.
- Repita essas etapas para cada configuração de pesquisa que você deseja adicionar.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do macOS

- **Descrição da conta:** insira uma descrição opcional da conta.
- **Nome de usuário da conta:** insira um nome de usuário opcional.
- **Senha da conta:** insira uma senha opcional. Use esse campo somente com perfis criptografados.
- **Nome do host LDAP:** insira o nome de host do servidor LDAP. Este campo é obrigatório.
- **Usar SSL:** selecione se uma conexão SSL com o servidor LDAP deve ser usada. O padrão é **On**.
- **Configurações de Pesquisa:** adicione configurações de pesquisa a serem usadas ao consultar o servidor LDAP. Você pode inserir quantas configurações de pesquisa desejar, mas deve adicionar pelo menos uma configuração para tornar a conta útil. Clique em **Adicionar** e faça o seguinte:
 - **Descrição:** digite uma descrição da configuração da pesquisa. Este campo é obrigatório.
 - **Escopo:** escolha **Base**, **Um nível** ou **Subárvore** para definir o quão profunda a pesquisa na árvore LDAP deve ser. O padrão é **Base**.
 - * **Base** pesquisa o nó para o qual a base de pesquisa aponta.
 - * **Um nível** pesquisa o nó Base e um nível abaixo dele.
 - * **Subárvore** pesquisa o nó Base, além de todos os seus filhos, independentemente da profundidade.
 - **Base de pesquisa:** digite o caminho para o nó no qual a pesquisa deve ser iniciada. Por exemplo, ou=people ou 0=example corp. Este campo é obrigatório.

- Clique em **Salvar** para adicionar a configuração de pesquisa ou em **Cancelar** para cancelar a inclusão dessa configuração.
- Repita essas etapas para cada configuração de pesquisa que você deseja adicionar.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra.
 - **Permitir que o usuário remova a política:** você pode selecionar quando os usuários podem remover a política do dispositivo. Selecione **Sempre**, **Código secreto obrigatório** ou **Nunca** no menu. Se você selecionar **Código secreto obrigatório**, digite um código secreto no campo **Código secreto de remoção**.
 - **Escopo do perfil:** selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

Política de dispositivo de localização

May 6, 2021

Crie políticas de dispositivo de localização no XenMobile para impor fronteiras geográficas. Quando os usuários violam o limite definido, também chamado de *geocerca*, o XenMobile pode realizar certas ações. Por exemplo, você pode configurar a política para emitir uma mensagem de aviso para os usuários quando eles ultrapassam o perímetro definido. Você também pode configurar a política para limpar os dados corporativos dos usuários quando eles ultrapassarem um perímetro, seja imediatamente ou após determinado tempo. Para obter informações sobre as ações de segurança, como a ativação de rastreamento e localização de um dispositivo, consulte [Ações de segurança](#).

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

Location Policy	Location Policy
1 Policy Info	This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.
2 Platforms	Device agent configuration
<input checked="" type="checkbox"/> iOS	Location Timeout: <input type="text" value="1"/> <input type="text" value="Minutes"/>
<input checked="" type="checkbox"/> Android	Tracking duration: <input type="text" value="6"/> <input type="text" value="Hours"/>
3 Assignment	Accuracy: <input type="text" value="328"/> <input type="text" value="Feet"/>
	Report if Location Services are disabled: <input type="radio"/> OFF
	Geofencing: <input type="radio"/> OFF
	▶ Deployment Rules

- **Tempo limite de localização:** digite um numeral e, na lista, clique em **Segundos** ou **Minutos** para definir a frequência com a qual o XenMobile tenta corrigir a localização do dispositivo. Os valores válidos são de 60 a 900 segundos ou de 1 a 15 minutos. O padrão é 1 minuto.
- **Duração de rastreamento:** digite um numeral e, na lista, clique em **Horas** ou **Minutos** para definir por quanto tempo o XenMobile rastreia o dispositivo. Os valores válidos são de 1 a 6 horas ou de 10 a 360 minutos. O padrão é 6 horas.
- **Precisão:** digite um numeral e, na lista, clique em **Metros**, **Pés** ou **Jardas** para definir a proximidade a um dispositivo que o XenMobile usa para rastreá-lo. Os valores válidos são de 10 a 5000 jardas ou metros ou de 30 a 15000 pés. O padrão é 328 pés.
- **Informar se os serviços de localização estiverem desativados:** selecione se o dispositivo envia um relatório para o XenMobile quando o GPS está desativado. O padrão é **Off**.
- **Cerca geográfica**

Geofencing	<input checked="" type="checkbox"/>
Radius	<input type="text" value="16400"/> <input type="text" value="Feet"/>
Center point latitude*	<input type="text" value="0.000000"/>
Center point longitude*	<input type="text" value="0.000000"/>
Warn user on perimeter breach	<input type="radio"/> OFF ?
Wipe corporate data on perimeter breach	<input type="radio"/> OFF

Quando você ativar a Geocerca, defina estas configurações:

- **Raio:** digite um numeral e, na lista, clique nas unidades a serem usadas para medir o raio. O padrão é 16.400 pés. Valores válidos para o raio são:
 - 164 a 164000 pés

- 50 a 50000 metros
- 54 a 54680 jardas
- 1 a 31 milhas
- **Latitude do ponto central:** digite uma latitude, como 37.787454, para definir a latitude do ponto central da geocerca.
- **Longitude do ponto central:** digite uma longitude, como 122.402952, para definir a longitude do ponto central da geocerca.
- **Avisar ao usuário sobre a violação do perímetro:** selecione se uma mensagem de aviso deverá ser emitida quando os usuários violarem o perímetro definido. O padrão é **Off**. Nenhuma conexão com o XenMobile é necessária para exibir a mensagem de aviso.
- **Apagar dados corporativos em caso de violação de perímetro:** selecione se os dispositivos dos usuários deverão ser apagados quando eles violarem o perímetro. O padrão é **Off**. Quando você ativa essa opção, o campo **Atraso no apagamento local** é exibido.
 - Digite um numeral e, na lista, clique em **Segundos** ou **Minutos** para definir o período de tempo a aguardar antes de limpar os dados corporativos dos dispositivos dos usuários. Isso oferece aos usuários a oportunidade de retornar para o local permitido antes que o XenMobile apague seletivamente os dispositivos deles. O padrão é 0 segundo.

Configurações do Android

Location Policy	Location Policy
1 Policy Info	This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters. Device agent configuration
2 Platforms	Poll interval: 10 Minutes
<input type="checkbox"/> iOS	Report if Location Services is disabled: OFF
<input checked="" type="checkbox"/> Android	Geofencing: OFF
3 Assignment	Deployment Rules

- **Intervalo de sondagem:** digite um numeral e, na lista, clique em **Minutos**, **Horas** ou **Dias** para definir a frequência com a qual o XenMobile tenta fixar a localização do dispositivo. Os valores válidos são de 1 a 1440 minutos, de 1 a 24 horas ou qualquer número de dias. O padrão é 10 minutos. Definir esse valor como menos de 10 minutos pode afetar negativamente a duração da bateria do dispositivo.
- **Informar se os serviços de localização estiverem desativados:** selecione se o dispositivo envia um relatório para o XenMobile quando o GPS está desativado. O padrão é **Off**.
- **Cerca geográfica**

Geofencing ON

Radius Feet

Center point latitude*

Center point longitude*

Warn user on perimeter breach OFF ?

Device connects to XenMobile for policy refresh

- Perform no action on perimeter breach
- Wipe corporate data on perimeter breach
- Lock device locally

Quando você ativar a Geocerca, defina estas configurações:

- **Raio:** digite um numeral e, na lista, clique nas unidades a serem usadas para medir o raio. O padrão é 16.400 pés. Valores válidos para o raio são:
 - 164 a 164000 pés
 - 1 a 50 quilômetros
 - 50 a 50000 metros
 - 54 a 54680 jardas
 - 1 a 31 milhas
- **Latitude do ponto central:** digite uma latitude, como 37.787454, para definir a latitude do ponto central da geocerca.
- **Longitude do ponto central:** digite uma longitude, como 122.402952, para definir a longitude do ponto central da geocerca.
- **Avisar ao usuário sobre a violação do perímetro:** selecione se uma mensagem de aviso deverá ser emitida quando os usuários violarem o perímetro definido. O padrão é **Off**. Nenhuma conexão com o XenMobile é necessária para exibir a mensagem de aviso.
- **O dispositivo se conecta ao XenMobile para atualização de política:** selecione uma das seguintes opções para quando os usuários violarem o perímetro:
 - **Não realizar nenhuma ação em caso de violação do perímetro:** não fazer nada. Esse é o padrão.
 - **Apagar dados corporativos em caso de violação de perímetro:** apagar os dados corporativos depois de um período de tempo especificado. Quando você ativa essa opção, o campo **Atraso no apagamento local** é exibido.
 - * Digite um numeral e, na lista, clique em Segundos ou Minutos para definir o período de tempo a aguardar antes de limpar os dados corporativos dos dispositivos dos usuários. Isso oferece aos usuários a oportunidade de retornar para o local permitido antes que o XenMobile apague seletivamente os dispositivos deles. O padrão é 0 segundo.

- **Atraso no bloqueio:** bloquear os dispositivos dos usuários após um período de tempo especificado. Quando você ativa essa opção, o campo **Atraso no bloqueio** é exibido.
 - * Digite um numeral e, na lista, clique em Segundos ou Minutos para definir o período de tempo a aguardar antes de bloquear os dispositivos dos usuários. Isso oferece aos usuários a oportunidade de retornar para o local permitido antes que o XenMobile bloqueie os dispositivos deles. O padrão é 0 segundo.

Configurações do Android Enterprise

Para que o acompanhamento de localização do Android funcione, certifique-se de que os seguintes requisitos sejam atendidos:

- Android 8.5 ou posterior
- A configuração Permitir compartilhamento de localização ativada na política de dispositivo de Restrições para Android Enterprise
- Agendamento de conexões (recomendado para Firebase Cloud Messaging)

Location Policy	Location Policy
1 Policy Info	This policy lets you set geographic perimeters for devices, such as radius, latitude and longitude, and you can track the locations and movements of the devices. You can then perform a selective or full wipe if the device breaches the parameters.
2 Platforms	Apply to fully managed devices with a work profile <input type="checkbox"/> OFF
<input checked="" type="checkbox"/> iOS	Managed device
<input checked="" type="checkbox"/> Android (legacy DA)	Location Mode <input type="text" value="Off"/> ⓘ
<input checked="" type="checkbox"/> Android Enterprise	Managed profile
3 Assignment	Report if Location Services is disabled <input type="checkbox"/> OFF
	Geofencing <input type="checkbox"/> OFF

Aplicar a dispositivos totalmente gerenciados com um perfil de trabalho

Para dispositivos totalmente gerenciados com perfis de trabalho, apenas a configuração do modo de localização está disponível.

- **Aplicar a dispositivos totalmente gerenciados com um perfil de trabalho:** permite que você defina o modo de localização para dispositivos totalmente gerenciados com perfis de trabalho. Quando essa configuração estiver ativada, defina a configuração do modo de localização:
 - **Modo de localização:** especifique o grau de detecção de localização a ser ativado. Você pode usar a ação de segurança Localizar somente quando o modo de localização estiver definido como **Alta precisão** ou **Economia de bateria**. O padrão é **Alta precisão**.
 - * **Alta precisão:** ativa todos os métodos de detecção de localização, incluindo GPS, redes e outros sensores.

- * **Apenas sensores:** ativa apenas GPS e outros sensores.
- * **Economia de bateria:** ativa apenas o provedor de localização de rede.
- * **Desativado:** desativa a detecção de localização.

Quando **Aplicar a dispositivos totalmente gerenciados com um perfil de trabalho** está desativado, as configurações se aplicam ao dispositivo gerenciado e ao perfil de trabalho, conforme mostrado nas seções a seguir. O padrão é **Desativado**.

Dispositivo gerenciado

- **Modo de localização:** especifique o grau de detecção de localização a ser ativado. Você pode usar a ação de segurança Localizar somente quando o modo de localização estiver definido como Alta Precisão ou Economia de Bateria. O padrão é Alta Precisão.
 - **Alta precisão:** ativa todos os métodos de detecção de localização, incluindo GPS, redes e outros sensores.
 - **Apenas sensores:** ativa apenas GPS e outros sensores.
 - **Economia de bateria:** ativa apenas o provedor de localização de rede.
 - **Desativado:** desativa a detecção de localização.
- **Cerca geográfica:**

The screenshot shows the configuration for Geofencing. The 'Geofencing' toggle is turned ON. The 'Poll interval' is set to 10 minutes. The 'Radius' is set to 16400 feet. The 'Center point latitude' and 'Center point longitude' are both set to 0.000000. The 'Warn user on perimeter breach' toggle is turned OFF. Under 'Device connects to Endpoint Management for policy refresh', the option 'Perform no action on perimeter breach' is selected.

Quando você ativar a Geocerca, defina estas configurações:

- **Intervalo de sondagem:** digite um numeral e clique em **Minutos**, **Horas** ou **Dias** para definir a frequência com que o XenMobile Server tenta determinar a localização do dispositivo. Os valores válidos são 1 a 1440 minutos, 1 a 24 horas ou qualquer número de dias. O padrão é **10**

minutos. Definir esse valor abaixo de 10 minutos pode afetar negativamente a autonomia da bateria do dispositivo.

- **Raio:** digite um numeral e clique nas unidades a serem usadas para medir o raio. O padrão é **16400 pés (5000 metros)**. Valores válidos para o raio são:
 - 164 a 164000 pés
 - 1 a 50 quilômetros
 - 50 a 50000 metros
 - 54 a 54680 jardas
 - 1 a 31 milhas
- **Latitude do ponto central:** digite uma latitude, como 37.787454, para definir a latitude do ponto central da geocerca. Para buscar o valor, vá para **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Segurança** e em **Localizar**. Depois de localizar o dispositivo, o XenMobile Server relata a localização do dispositivo na página do dispositivo **Detalhes > Geral em Segurança**.
- **Longitude do ponto central:** digite uma longitude, como 122.402952, para definir a longitude do ponto central da geocerca.
- **Avisar ao usuário sobre a violação do perímetro:** selecione se uma mensagem de aviso deverá ser emitida quando os usuários violarem o perímetro definido. O padrão é **Off**. Nenhuma conexão com o XenMobile Server é necessária para exibir a mensagem de aviso.
- **O dispositivo se conecta ao XenMobile Server para atualização de política:** selecione uma das seguintes opções para quando os usuários violarem o perímetro:
 - **Não realizar nenhuma ação em caso de violação do perímetro:** não fazer nada. Essa configuração é a padrão.
 - **Apagar dados corporativos em caso de violação de perímetro:** apagar os dados corporativos depois de um período de tempo especificado. Quando você ativa essa opção, o campo **Atraso no apagamento local** é exibido.
 - * Digite um numeral e clique em **Segundos** ou **Minutos** para definir o período de tempo a aguardar antes de limpar os dados corporativos dos dispositivos dos usuários. Esse período de espera dá aos usuários a oportunidade de retornar para o local permitido antes que o XenMobile Server apague seletivamente os dispositivos deles. O padrão é **0 segundo**.
 - **Bloquear dispositivo localmente:** bloquear os dispositivos dos usuários após um período de tempo especificado. Quando você ativa essa opção, o campo **Atraso no bloqueio** é exibido.
 - * Digite um numeral e clique em **Segundos** ou **Minutos** para definir o período de tempo a aguardar antes de bloquear os dispositivos dos usuários. Esse período de espera dá aos usuários a oportunidade de retornar para o local permitido antes que o XenMobile

Server bloqueie os dispositivos deles. O padrão é **0 segundo**.

Perfil gerenciado

- **Informa se os serviços de localização estão desativados:** selecione se o dispositivo deve enviar um relatório para o XenMobile Server quando o usuário desliga o GPS. O padrão é **Off**.
- **Cerca geográfica:** veja as configurações no artigo em [Dispositivo gerenciado](#).

Política de dispositivo de email

April 23, 2020

Você pode adicionar uma política de dispositivo de email ao XenMobile para configurar uma conta de email em dispositivos iOS ou macOS.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do iOS e do MacOS

Mail Policy	Mail Policy
1 Policy Info	This configuration allows you to set email parameters. Note that when applied to a supervised device, you need to configure Email address and User name fields.
2 Platforms	Account description *
<input checked="" type="checkbox"/> iOS	Account type IMAP
<input checked="" type="checkbox"/> macOS	Path prefix
3 Assignment	User display name *
	Email address *
	Incoming email
	Email server host name *
	Email server port * 143
	User name *
	Authentication type Password
	Password

- **Descrição da conta:** digite uma descrição da conta que é exibida nos aplicativos Email e Configurações. Este campo é obrigatório.
- **Tipo de conta:** escolha **IMAP** ou **POP** para selecionar o protocolo a ser usado para contas de usuário. O padrão é **IMAP**. Quando você seleciona **POP**, a opção de prefixo de **Caminho** a seguir desaparece.
- **Prefixo de caminho:** digite **INBOX** ou o prefixo de caminho da sua conta de email IMAP. Este campo é obrigatório.

- **Nome para exibição do usuário:** digite o nome do usuário completo a ser usado para mensagens e outras finalidades. Este campo é obrigatório.
- **Endereço de email:** digite o endereço de email completo da conta. Este campo é obrigatório.
- **Configurações de email de entrada**
 - **Nome de host do servidor de email:** digite o nome do host ou endereço IP do servidor de email de entrada. Este campo é obrigatório.
 - **Porta do servidor de email:** digite o número da porta de servidor de email de entrada. O padrão é **143**. Este campo é obrigatório.
 - **Nome de usuário:** digite o nome de usuário da conta de email. Esse nome é geralmente o mesmo que o endereço de email até o caractere @. Este campo é obrigatório.
 - **Tipo de autenticação:** escolha o tipo de autenticação que deve ser usado. O padrão é **Senha**. Quando **Nenhum** está selecionado, o campo **Senha** a seguir desaparece.
 - **Senha:** digite uma senha opcional para o servidor de email de entrada.
 - **Usar SSL:** selecione se o servidor de email de entrada usa a autenticação Secure Socket Layer. O padrão é **Off**.
- **Configurações de email de saída**
 - **Nome de host do servidor de email:** digite o nome do host ou endereço IP do servidor de email de saída. Este campo é obrigatório.
 - **Porta do servidor de email:** digite o número da porta de servidor de email de saída. Se não houver porta, você não digitará um número da porta, pois a porta padrão para o protocolo especificado será usada.
 - **Nome de usuário:** digite o nome de usuário da conta de email. Esse nome é geralmente o mesmo que o endereço de email até o caractere @. Este campo é obrigatório.
 - **Tipo de autenticação:** escolha o tipo de autenticação para usar. O padrão é **Senha**.
 - **Senha:** digite uma senha opcional para o servidor de email de saída.
 - **Senha de saída idêntica à de entrada:** selecione se as senhas de entrada e de saída são iguais. O padrão é **Off**, o que significa que as senhas são diferentes.
 - **Usar SSL:** selecione se o servidor de email de saída usa a autenticação Secure Socket Layer. O padrão é **Off**.
- **Política**
 - **Autorizar a mudança de emails entre contas:** selecione se os usuários têm permissão para mover emails dessa conta para outra conta, além de encaminhar e responder de uma conta diferente. O padrão é **Off**.
 - **Enviar email somente do aplicativo de email:** selecione se os usuários têm restrições no aplicativo de email do iOS para enviar emails.
 - **Desativar a sincronização de emails recentes:** selecione se os usuários devem ser impedidos de sincronizar endereços recentes. O padrão é **Off**. Essa opção se aplica somente ao iOS 6.0 e versões posteriores.
 - **Permitir Mail Drop:** selecione se deseja permitir o uso do Apple Mail Drop para disposi-

tivos que executam o iOS 9.2 e versões posteriores. O padrão é **Off**.

- **Ativar assinatura S/MIME:** selecione se esta conta suporta ou não a assinatura S/MIME. O padrão é **On**. Quando definido como **On**, os campos abaixo são exibidos.
 - * **Credencial de identidade de assinatura:** escolha a credencial de assinatura a ser usada.
 - * **Usuário de assinatura S/MIME substituível:** se definido como **On**, os usuários podem ativar e desativar a assinatura S/MIME nas configurações de seus dispositivos. O padrão é **Off**. Essa opção se aplica ao iOS 12.0 e posterior.
 - * **UUID de certificado de assinatura S/MIME substituível pelo usuário:** se definido como **On**, os usuários podem selecionar, nas configurações de seus dispositivos, a credencial de assinatura a ser usada. O padrão é **Off**. Essa opção se aplica ao iOS 12.0 e posterior.
- **Ativar criptografia S/MIME:** selecione se essa conta é compatível com a criptografia S/MIME. O padrão é **Off**. Quando definido como **On**, os campos abaixo são exibidos.
 - * **Credencial de identidade de criptografia:** escolha a credencial de criptografia a ser usada.
 - * **Ativar comutador de S/MIME por mensagem:** quando definido como **On**, mostra aos usuários uma opção para ativar ou desativar a criptografia S/MIME para cada mensagem que redigem. O padrão é **Off**.
 - * **Criptografia S/MIME como padrão substituível pelo usuário:** se definido como **On**, os usuários podem, nas configurações de seus dispositivos, selecionar se S/MIME permanecerá ativa como padrão. O padrão é **Off**. Essa opção se aplica ao iOS 12.0 e posterior.
 - * **UUID de certificado de criptografia S/MIME substituível pelo usuário:** se definido como **On**, os usuários podem ativar e desativar a identidade da criptografia de S/MIME e a criptografia nas configurações de seus dispositivos. O padrão é **Off**. Essa opção se aplica ao iOS 12.0 e posterior.
- **Configurações de política**
 - **Remover política:** para remover a política posteriormente, você pode configurar o parâmetro de remoção da política na data definida em **Selecionar data** ou no período em **Duração até remoção (em horas)**.
 - **Permitir que o usuário remova a política:** permite que os usuários removam a política de email **Sempre**, apenas com um **Código secreto obrigatório** ou **Nunca**.
 - **Escopo do perfil:** somente para macOS, escolha se a política se aplica com base no nível do **Usuário** ou em todo o **Sistema**.

Política de dispositivo de domínios gerenciados

April 26, 2021

Você pode definir os domínios gerenciados que se aplicam a emails e ao navegador Safari. Os domínios gerenciados ajudam você a proteger dados corporativos ao controlar quais aplicativos podem abrir documentos baixados de domínios usando o Safari.

Para dispositivos iOS 8 e versões posteriores no modo supervisionado, especifique as URLs ou os subdomínios para controlar como os usuários podem abrir documentos, anexos e downloads do navegador. Para iOS 9.3 e versões posteriores em dispositivos supervisionados, você pode especificar as URLs das quais os usuários podem salvar senhas no Safari.

Para ver as etapas sobre como configurar um dispositivo iOS para o modo supervisionado, consulte [Para colocar um dispositivo iOS no modo Supervisionado usando o Apple Configurator](#).

Quando um usuário envia um email para um destinatário cujo domínio não está na lista de domínios de email gerenciados, a mensagem é sinalizada no dispositivo do usuário para avisá-lo que ele está enviando uma mensagem para alguém fora de seu domínio corporativo.

Para itens como documentos, anexos ou downloads: quando um usuário abre um item usando o Safari de um domínio Web que está na lista de domínios Web gerenciados, o aplicativo corporativo adequado abre o item. Se o item não for originário de um domínio Web na lista de domínios Web gerenciados, o usuário não conseguirá abrir o item com um aplicativo corporativo. Ele deverá usar um aplicativo pessoal e não gerenciado.

Para dispositivos supervisionados, mesmo se você não especificar domínios de preenchimento automático de senha do Safari: se o dispositivo estiver configurado como multiusuários efêmeros, os usuários não poderão salvar as senhas. No entanto, se o dispositivo não estiver configurado como multiusuários efêmeros, os usuários poderão salvar todas as senhas.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

Para especificar domínios:

Formato	Descrição
<code>example.com</code>	Trate qualquer caminho sob <code>example.com</code> como gerenciado, mas não <code>site.example.com/</code> .

Formato	Descrição
<code>foo.example.com</code>	Trate qualquer caminho sob <code>foo.example.com</code> como gerenciado, mas não <code>example.com/</code> ou <code>bar.example.com/</code> .
<code>*.example.com</code>	Trate qualquer caminho sob <code>foo.example.com</code> ou <code>bar.example.com</code> como gerenciado, mas não <code>example.com/</code> .
<code>example.com/sub</code>	Tratar <code>example.com/sub</code> e qualquer caminho sob ele como gerenciado, mas não <code>example.com/</code> .
<code>foo.example.com/sub</code>	Trate qualquer caminho sob <code>foo.example.com/sub</code> como gerenciado, mas não <code>example.com</code> , <code>example.com/sub</code> , <code>foo.example.com/</code> ou <code>bar.example.com/sub</code> .
<code>*.example.com/sub</code>	Trate qualquer caminho sob <code>foo.example.com/sub</code> ou <code>bar.example.com/sub</code> como gerenciado, mas não <code>example.com</code> ou <code>foo.example.com/</code> .

Regras:

- Barras à esquerda e à direita de “www.” em URLs são ignoradas quando os domínios são comparados.
- Se uma entrada contiver um número de porta, somente os endereços que especificam esse número de porta são considerados gerenciados. Caso contrário, somente as portas padrão são consideradas gerenciadas (porta 80 para http e porta 443 para https). Por exemplo, o padrão `*.example.com:8080` corresponde a `https://site.example.com:8080/page.html`, mas não a `https://site.example.com/page.html`, enquanto o padrão `*.example.com` corresponde a `https://site.example.com/page.html` e `https://site.example.com/page.html`, mas não a `https://site.example.com:8080/page.html`.
- As definições de domínio Web gerenciado do Safari são cumulativas. Os padrões definidos por todas as cargas de domínio Web gerenciado do Safari são usados para realizar a correspondência com uma solicitação de URL.

Configurações:

- **Domínios gerenciados**

- **Domínios de email não marcados:** para cada domínio de email que você deseja incluir na lista, clique em **Adicionar** e faça o seguinte:
 - * **Domínio de email gerenciado:** digite o domínio de email.
 - * Clique em **Salvar** para salvar o domínio de email ou em **Cancelar** para não salvar.
- **Domínios Web Safari gerenciados:** para cada domínio Web que você deseja incluir na lista, clique em **Adicionar** e faça o seguinte:
 - * **Domínio Web gerenciado:** digite o domínio Web.
 - * Clique em **Salvar** para salvar o domínio Web ou em **Cancelar** para não salvar.
- **Domínios de preenchimento automático de senha do Safari:** para cada domínio de preenchimento automático que você deseja incluir na lista, clique em **Adicionar** e faça o seguinte:
 - * **Domínio de preenchimento automático de senha do Safari:** digite o domínio de preenchimento automático.
 - * Clique em **Salvar** para salvar o domínio de preenchimento automático ou clique em **Cancelar** para não salvar.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Políticas de dispositivo das opções de MDM

April 26, 2021

Você pode criar uma política de dispositivo no XenMobile para gerenciar o Bloqueio de ativação buscar iPhone/iPad nos dispositivos de telefone supervisionados iOS 7.0 e versões posteriores. Para ver as etapas sobre como configurar um dispositivo iOS para o modo supervisionado, consulte [Para colocar um dispositivo iOS no modo Supervisionado usando o Apple Configurator](#).

Bloqueio de ativação é um recurso do Buscar iPhone/iPad que impede a reativação de um dispositivo supervisionado perdido ou roubado. O Bloqueio de Ativação requer o ID Apple e a senha do usuário antes que qualquer pessoa possa desligar o Buscar iPhone/iPad, apagar o dispositivo ou reativar o dispositivo. Para os dispositivos de propriedade da organização, ignorar um bloqueio de ativação é necessário, por exemplo, para redefinir ou realocar dispositivos.

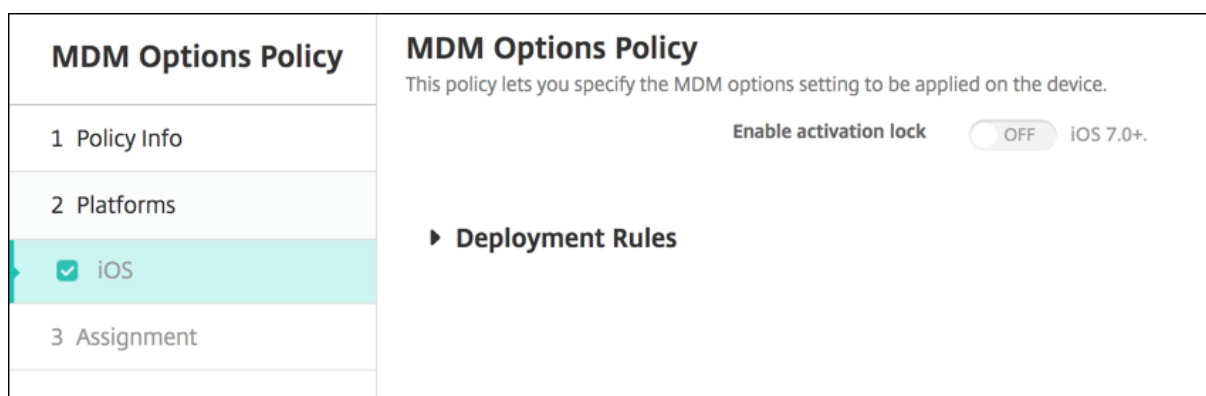
Para ativar o Bloqueio de Ativação, você configura e implanta a política do dispositivo de Opções XenMobile MDM. Você pode gerenciar um dispositivo a partir do console XenMobile sem as credenciais

Apple do usuário. Para desviar do requisito de credenciais Apple de um bloqueio de ativação, execute a ação de segurança Ignorar Bloqueio de Ativação a partir do console XenMobile.

Por exemplo, se o usuário retorna um telefone perdido ou para configurar o dispositivo antes ou após um apagamento completo: quando o telefone pede as credenciais de conta do iTunes, você pode ignorar essa etapa emitindo a ação de segurança Ignorar Bloqueio de Ativação no console XenMobile.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS



- **Ativar bloqueio de ativação:** selecione se o bloqueio de ativação deve ser ativado nos dispositivos nos quais você implantar essa política. O padrão é **Off**.

Depois de ativar o Bloqueio de Ativação, implantando a política do dispositivo de opções do MDM: a Ação de Segurança **Ignorar bloqueio de ativação** aparece quando você seleciona esses dispositivos na página **Gerenciar > Dispositivos** e clica em **Segurança**. O desvio do bloqueio de ativação permite que você remova o bloqueio de ativação de dispositivos supervisionados antes da ativação do dispositivo sem saber o ID Apple e a senha dos usuários do dispositivo. Você pode enviar um desvio do bloqueio de ativação a um dispositivo antes ou depois de um apagamento completo. Para obter mais informações, consulte [Ignorar bloqueio de ativação do iOS](#) no artigo de ações de segurança.

Política de dispositivo de informação da organização

April 23, 2020

Você pode adicionar uma política de dispositivo no XenMobile para especificar as informações da sua organização para mensagens de alerta que são enviadas por push do XenMobile para dispositivos iOS. A política está disponível para dispositivos iOS 7 e versões posteriores.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

- **Nome:** digite o nome da organização que executa o XenMobile.
- **Endereço:** digite o endereço da organização.
- **Telefone:** digite o número de telefone de suporte da organização.
- **Email:** digite o endereço de email de suporte.
- **Magic:** digite uma palavra ou uma frase que descreva os serviços gerenciados pela organização.

Política de dispositivo de código secreto

November 30, 2020

Crie uma política de código secreto no XenMobile com base nos padrões da sua organização. Você pode exigir códigos secretos nos dispositivos dos usuários e definir várias regras de formatação e de código secreto. Você pode criar políticas para iOS, macOS, Android, Samsung KNOX, Android Enterprise, Windows Phone e Windows Desktop/Tablet. Cada plataforma exige um conjunto diferente de valores, que são descritos neste artigo.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

Passcode Policy	Passcode Policy
1 Policy Info	This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.
2 Platforms	<p>Passcode required <input checked="" type="checkbox"/></p> <p>Passcode requirements</p> <p>Minimum length <input type="text" value="6"/></p> <p>Allow simple passcodes <input checked="" type="checkbox"/></p> <p>Required characters <input type="checkbox"/></p> <p>Minimum number of symbols <input type="text" value="0"/></p> <p>Passcode security</p> <p>Device lock grace period (minutes of inactivity) <input type="text" value="None"/></p> <p>Lock device after (minutes of inactivity) (0-999) <input type="text" value="None"/></p> <p>Passcode expiration in days (1-730) <input type="text" value="0"/></p> <p>Previous passcodes saved (0-50) <input type="text" value="0"/></p>
3 Assignment	

- **Código secreto obrigatório:** selecione essa opção para exigir um código secreto e para exibir as opções de configuração de uma política de dispositivo de código secreto do iOS. A página se expande para permitir que você defina as configurações dos requisitos de código secreto, segurança do código secreto e configurações de política.
- **Requisitos de código secreto**
 - **Tamanho mínimo:** na lista, clique no tamanho mínimo do código secreto. O padrão é **6**.
 - **Permitir código secreto simples:** selecione se códigos secretos simples são permitidos. Códigos secretos simples são um conjunto de caracteres repetidos ou sequenciais. O padrão é **On**.
 - **Caracteres obrigatórios:** selecione se será obrigatório que os códigos secretos tenham pelo menos uma letra. O padrão é **Off**.
 - **Número mínimo de símbolos:** na lista, clique no número de símbolos que o código secreto deve conter. O padrão é **0**.
- **Segurança do código secreto**
 - **Período de tolerância de bloqueio do dispositivo (minutos de inatividade):** na lista, clique no período de tempo antes que os usuários tenham que digitar um código secreto para desbloquear um dispositivo bloqueado. O padrão é **Nenhum**.
 - **Bloquear dispositivos após (minutos de inatividade):** na lista, clique no período de tempo durante o qual um dispositivo pode ficar inativo antes de ser bloqueado. O padrão é **Nenhum**.
 - **Expiração de código secreto em dias (1-730):** digite o número de dias após os quais o código secreto expira. Os valores válidos são de 1 a 730. O padrão é **0**, o que significa que a senha nunca expira.
 - **Senhas anteriores salvas (0-50):** digite o número de senhas usadas a serem salvas. Os usuários não conseguem usar nenhuma senha encontrada nessa lista. Os valores válidos são de 0 a 50. O padrão é **0**, o que significa que os usuários podem reutilizar senhas.
 - **Máximo de falhas em tentativas de login:** na lista, clique no número de vezes que um usuário pode não conseguir fazer login com êxito antes que o dispositivo seja totalmente apagado. O padrão é **Não definido**.

Configurações do macOS

Passcode Policy	Passcode Policy
1 Policy Info	This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.
2 Platforms	<p>Passcode required <input type="checkbox"/> OFF</p> <p>Passcode security</p> <p>Delay after failed sign-on attempts, in minutes <input type="text"/></p> <p>Policy Settings</p> <p>Profile scope <input type="text" value="User"/> macOS 10.7+</p> <p>► Deployment Rules</p>
<input type="checkbox"/> iOS	
<input checked="" type="checkbox"/> macOS	
<input checked="" type="checkbox"/> Android	
<input checked="" type="checkbox"/> Samsung KNOX	
<input checked="" type="checkbox"/> Android for Work	
<input checked="" type="checkbox"/> Windows Phone	
<input checked="" type="checkbox"/> Windows Desktop/Tablet	
3 Assignment	

- **Código secreto obrigatório:** selecione essa opção para exigir um código secreto e para exibir as opções de configuração de uma política de dispositivo de código secreto do iOS. A página se expande para permitir que você defina as configurações dos requisitos de código secreto, segurança do código secreto e configurações de política.
- Se você não ativar **Senha necessária**, ao lado de **Atraso após tentativas de login com falha, em minutos**, digite o número de minutos de atraso antes de permitir que os usuários reinsiram o código secreto.
- Se você ativar **Senha necessária**, defina as seguintes configurações:
- **Requisitos de código secreto**
 - **Tamanho mínimo:** na lista, clique no tamanho mínimo do código secreto. O padrão é **6**.
 - **Permitir código secreto simples:** selecione se códigos secretos simples são permitidos. Códigos secretos simples são um conjunto de caracteres repetidos ou sequenciais. O padrão é **On**.
 - **Caracteres obrigatórios:** selecione se será obrigatório que os códigos secretos tenham pelo menos uma letra. O padrão é **Off**.
 - **Número mínimo de símbolos:** na lista, clique no número de símbolos que o código secreto deve conter. O padrão é **0**.
- **Segurança do código secreto**
 - **Período de tolerância de bloqueio do dispositivo (minutos de inatividade):** na lista, clique no período de tempo antes que os usuários tenham que digitar um código secreto para desbloquear um dispositivo bloqueado. O padrão é **Nenhum**.
 - **Bloquear dispositivos após (minutos de inatividade):** na lista, clique no período de tempo durante o qual um dispositivo pode ficar inativo antes de ser bloqueado. O padrão é **Nenhum**.
 - **Expiração de código secreto em dias (1-730):** digite o número de dias após os quais o código secreto expira. Os valores válidos são de 1 a 730. O padrão é **0**, o que significa que

a senha nunca expira.

- **Senhas anteriores salvas (0-50):** digite o número de senhas usadas a serem salvas. Os usuários não conseguem usar nenhuma senha encontrada nessa lista. Os valores válidos são de 0 a 50. O padrão é **0**, o que significa que os usuários podem reutilizar senhas.
- **Máximo de falhas em tentativas de login:** na lista, clique no número de vezes que um usuário pode não conseguir fazer login depois que o dispositivo é bloqueado. O padrão é **Não definido**.
- **Atraso após tentativas de login com falha, em minutos:** digite o número de minutos de atraso antes de permitir que um usuário reinsira um código secreto.
- **Forçar redefinição do código secreto:** na próxima vez que um usuário se autenticar, ele deve redefinir seu código de secreto.
- **Configurações de política**
 - **Escopo do perfil:** selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

Configurações do Android

<p>Passcode Policy</p> <p>1 Policy Info</p> <p>2 Platforms</p> <p><input type="checkbox"/> iOS</p> <p><input type="checkbox"/> macOS</p> <p><input checked="" type="checkbox"/> Android</p> <p><input checked="" type="checkbox"/> Samsung KNOX</p> <p><input checked="" type="checkbox"/> Android for Work</p> <p><input checked="" type="checkbox"/> Windows Phone</p> <p><input checked="" type="checkbox"/> Windows Desktop/Tablet</p> <p>3 Assignment</p>	<p>Passcode Policy</p> <p>This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.</p> <p>Passcode Required <input type="checkbox"/> OFF</p> <p>Encryption</p> <p>Enable encryption <input type="checkbox"/> OFF A 3.0+</p> <p>Samsung SAFE</p> <p>Use same passcode across all users <input type="checkbox"/> OFF</p> <p>► Deployment Rules</p>
---	--

Nota:

A configuração padrão para o Android é **Off**.

- **Código secreto obrigatório:** selecione essa opção para exigir um código secreto e para exibir as opções de configuração de uma política de dispositivo de código secreto do Android. A página se expande para permitir que você defina as configurações de requisitos de código secreto, segurança do código secreto, criptografia e Samsung SAFE.
- **Requisitos de código secreto**
 - **Tamanho mínimo:** na lista, clique no tamanho mínimo do código secreto. O padrão é 6.

- **Reconhecimento biométrico:** selecione se o reconhecimento biométrico deve ser ativado. Se você habilitar essa opção, o campo Caracteres obrigatórios ficará oculto. O padrão é **Off**.
- **Caracteres obrigatórios:** na lista, clique em Sem restrição, Letras e números, Apenas números ou Apenas letras para configurar como os códigos secretos são compostos. O padrão é Sem restrição.
- **Regras avançadas:** selecione se regras avançadas de código secreto devem ser aplicadas. Essa opção está disponível para o Android 3.0 e versões posteriores. O padrão é **Off**.
- Quando você habilitar **Regras avançadas**, em cada uma das seguintes listas, clique no número mínimo de cada tipo de caractere que uma senha deve conter:
 - * **Símbolos:** o número mínimo de símbolos.
 - * **Letras:** o número mínimo de letras.
 - * **Letras minúsculas:** o número mínimo de letras minúsculas.
 - * **Letras maiúsculas:** o número mínimo de letras maiúsculas.
 - * **Números ou símbolos:** o número mínimo de números ou símbolos.
 - * **Números:** o número mínimo de números.

- **Segurança do código secreto**

- **Bloquear dispositivos após (minutos de inatividade):** na lista, clique no período de tempo durante o qual um dispositivo pode ficar inativo antes de ser bloqueado. O padrão é **Nenhum**.
- **Expiração de código secreto em dias (1-730):** digite o número de dias após os quais o código secreto expira. Os valores válidos são de 1 a 730. O padrão é **0**, o que significa que a senha nunca expira.
- **Senhas anteriores salvas (0-50):** digite o número de senhas usadas a serem salvas. Os usuários não conseguem usar nenhuma senha encontrada nessa lista. Os valores válidos são de 0 a 50. O padrão é **0**, o que significa que os usuários podem reutilizar senhas.
- **Máximo de falhas em tentativas de login:** na lista, clique no número de vezes que um usuário pode não conseguir fazer login depois que o dispositivo é apagado. O padrão é **Não definido**.

- **Criptografia**

- **Ativar criptografia:** selecione se a criptografia deve ser ativada. Essa opção está disponível para o Android 3.0 e versões posteriores. A opção está disponível independentemente da configuração da **Senha necessária**.

Para criptografar seus dispositivos, os usuários devem começar com uma bateria carregada e manter o dispositivo conectado durante o período de uma hora ou mais que é decorrido para a criptografia. Se o processo de criptografia for interrompido, eles poderão perder alguns ou todos os dados nos dispositivos deles. Depois que um dispositivo é criptografado, o processo não pode ser revertido exceto por uma redefinição de fábrica,

que apaga todos os dados no dispositivo.

- **Samsung SAFE**

Nota:

Como solução alternativa para desativar o reconhecimento facial ou de íris em dispositivos Samsung SAFE: crie uma política de dispositivo Restrições para o Samsung SAFE. Na política Restrições, ative **Desativar Aplicativos** e adicione `com.samsung.android.bio.face.service` ou `com.samsung.android.server.iris` à tabela. Em seguida, implante a política de restrições.

- **Usar o mesmo código secreto para todos os usuários:** selecione se o mesmo código secreto deve ser usado para todos os usuários. O padrão é **Off**. Esta configuração aplica-se somente aos dispositivos Samsung SAFE e está disponível independentemente da configuração de **Senha necessária**.
- Quando você ativar a opção **Usar o mesmo código secreto para todos os usuários**, digite o código secreto a ser usado por todos os usuários no campo **Código secreto**.
- Quando você ativar a **Senha requerida**, configure as seguintes configurações do SAFE da Samsung:
 - * **Caracteres alterados:** digite o número de caracteres que os usuários devem alterar em seus códigos secretos anteriores. O padrão é **0**.
 - * **Número de vezes em que um caractere pode ocorrer:** digite o número máximo de vezes que um caractere pode ocorrer em um código secreto. O padrão é **0**.
 - * **Tamanho da sequência alfabética:** digite o tamanho máximo de uma sequência alfabética em um código secreto. O padrão é **0**.
 - * **Tamanho da sequência numérica:** digite o tamanho máximo de uma sequência numérica em um código secreto. O padrão é **0**.
 - * **Permitir que os usuários tornem a senha visível:** selecione se os usuários podem tornar visíveis os códigos secretos deles. O padrão é **On**.
 - * **Configure a autenticação biométrica.** Selecione a autenticação biométrica deve ser ativada. O padrão é **Off**. Se você configurá-la como **On**, você pode definir essas opções:
 - **Permitir impressão digital.** Selecione para permitir que os usuários se autenticem usando a impressão digital.
 - **Permitir íris.** Selecione para permitir que os usuários se autenticem usando a íris.
 - * **Cadeias de caracteres proibidas:** crie cadeias de caracteres proibidas para impedir que os usuários usem cadeias de caracteres inseguras que sejam fáceis de adivinhar, como “senha”, “pwd”, “bemvindo”, “123456”, “111111” e assim por diante. Para cada cadeia de caracteres que você desejar negar, clique em **Adicionar** e faça o seguinte:
 - **Cadeias de caracteres proibidas:** digite as cadeias de caracteres que os usuários

não podem usar.

- Clique em **Salvar** para adicionar a cadeia de caracteres ou em **Cancelar** para cancelar a adição da cadeia de caracteres.

Configurações do Samsung KNOX

Passcode Policy	Passcode Policy
1 Policy Info	This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.
2 Platforms	Passcode requirements
<input type="checkbox"/> iOS	Minimum length <input type="text" value="6"/>
<input type="checkbox"/> macOS	Allow users to make password visible <input type="checkbox"/> OFF
<input type="checkbox"/> Android	Forbidden Strings
<input checked="" type="checkbox"/> Samsung KNOX	Forbidden strings <input type="text"/> <input type="button" value="Add"/>
<input checked="" type="checkbox"/> Android for Work	Minimum number of
<input checked="" type="checkbox"/> Windows Phone	Changed characters * <input type="text" value="0"/>
<input checked="" type="checkbox"/> Windows Desktop/Tablet	Symbols * <input type="text" value="0"/>
3 Assignment	Maximum number of
	Number of times a character can occur * <input type="text" value="0"/>
	Alphabetic sequence length * <input type="text" value="0"/>
	Numeric sequence length * <input type="text" value="0"/>

• Requisitos de código secreto

- **Tamanho mínimo:** na lista, clique no tamanho mínimo do código secreto. O padrão é **6**.
- **Permitir que os usuários tornem a senha visível:** selecione se os usuários podem tornar a senha visível.
- **Cadeias de caracteres proibidas:** crie cadeias de caracteres proibidas para impedir que os usuários usem cadeias de caracteres inseguras que sejam fáceis de adivinhar, como “senha”, “pwd”, “bemvindo”, “123456”, “111111” e assim por diante. Para cada cadeia de caracteres que você deseja negar, clique em Adicionar e faça o seguinte:
 - * **Cadeias de caracteres proibidas:** digite as cadeias de caracteres que os usuários não podem usar.
 - * Clique em **Salvar** para adicionar a cadeia de caracteres ou em **Cancelar** para cancelar a adição da cadeia de caracteres.

• Número mínimo de

- **Caracteres alterados:** digite o número de caracteres que os usuários devem alterar em seus códigos secretos anteriores. O padrão é **0**.
- **Símbolos:** digite o número mínimo de símbolos necessários em um código secreto. O padrão é **0**.

• Número máximo de

- **Número de vezes em que um caractere pode ocorrer:** digite o número máximo de vezes que um caractere pode ocorrer em um código secreto. O padrão é **0**.

- **Tamanho da sequência alfabética:** digite o tamanho máximo de uma sequência alfabética em um código secreto. O padrão é **0**.
- **Tamanho da sequência numérica:** digite o tamanho máximo de uma sequência numérica em um código secreto. O padrão é **0**.
- **Segurança do código secreto**
 - **Bloquear dispositivos após (minutos de inatividade):** na lista, clique no número de segundos durante os quais um dispositivo pode ficar inativo antes de ser bloqueado. O padrão é **Nenhum**.
 - **Expiração de código secreto em dias (1-730):** digite o número de dias após os quais o código secreto expira. Os valores válidos são de 1 a 730. O padrão é **0**, o que significa que a senha nunca expira.
 - **Senhas anteriores salvas (0-50):** digite o número de senhas usadas a serem salvas. Os usuários não conseguem usar nenhuma senha encontrada nessa lista. Os valores válidos são de 0 a 50. O padrão é **0**, o que significa que os usuários podem reutilizar senhas.
 - **Se o número de tentativas de login for excedido, o dispositivo é bloqueado:** na lista, clique no número de vezes que um usuário pode não conseguir fazer login depois que o dispositivo é bloqueado. O padrão é **Não definido**.
 - **Se o número de tentativas de login for excedido, o dispositivo é apagado:** na lista, clique no número de vezes que um usuário pode não conseguir fazer login com êxito, após as quais o contêiner do KNOX (juntamente com os dados do KNOX) é apagado do dispositivo. Os usuários precisam reinicializar o contêiner KNOX após a limpeza. O padrão é **Não definido**.

Configurações do Android Enterprise

The screenshot displays the configuration interface for a Passcode Policy. On the left, a sidebar lists various policy categories, with 'Passcode Policy' selected. The main area contains the following settings:

- Device passcode required:** A toggle switch set to 'ON'.
- Show apps and shortcuts while passcode is not in compliance:** A toggle switch set to 'OFF'.
- Passcode requirements for device passcode:**
 - Minimum length:** A dropdown menu set to '6'.
- Allow users to make password visible (Knox 3.0+):** A toggle switch set to 'OFF'.
- Biometric recognition:** A toggle switch set to 'OFF'.
- Required characters:** A dropdown menu set to 'Numbers only'.
- Forbidden Strings (Knox 3.0+):** An empty text input field.

At the bottom right, there are 'Back' and 'Next >' buttons.

Em dispositivos Android Enterprise, você pode exigir um código secreto para o dispositivo, um desafio

de segurança para o perfil de trabalho do Android Enterprise ou ambos.

Nos dispositivos que executam o Android 8.0 ou posterior e o Samsung Knox 3.0 ou posterior, defina as configurações para o Samsung Knox na página **Android Enterprise**. Nos dispositivos que executam versões anteriores do Android ou Samsung Knox, utilize a página **Samsung Knox**.

Nota:

Quando dispositivos executando o Samsung Knox 3.0 estão registrados como dispositivos de perfil de trabalho, as configurações de código secreto do dispositivo para Knox 3.0 e posterior não se aplicam ao código secreto do dispositivo, mesmo que você as defina.

- **Código secreto do dispositivo obrigatório:** requer um código secreto no dispositivo. Quando esta configuração estiver **On**, defina as configurações em **Requisitos de código secreto do dispositivo** e **Segurança de código secreto do dispositivo**. O padrão é **Desativado**.
- **Mostrar aplicativos e atalhos mesmo que o código secreto não esteja em conformidade:** quando essa configuração estiver **Ativada**, os aplicativos e atalhos no dispositivo não ficam ocultos, mesmo quando o código secreto não está em conformidade. Quando esta configuração está **Desativada**, os aplicativos e atalhos ficam ocultos quando o código secreto não está em conformidade. Se você ativar essa configuração, a Citrix recomenda que você crie uma ação automatizada para marcar o dispositivo como sem conformidade quando o código secreto não estiver em conformidade. O padrão é **Desativado**.
- **Requisitos de código secreto do dispositivo**
 - **Tamanho mínimo:** especifica o tamanho mínimo do código secreto. O padrão é 6.
 - **Permitir que os usuários tornem a senha visível:** para dispositivos com Samsung Knox 3.0 e posterior que tenham uma chave de licença Knox válida configurada. Somente para dispositivos totalmente gerenciados. Essa configuração não se aplica a dispositivos registrados como dispositivos de perfil de trabalho. Permite que os usuários tornem a senha visível. O padrão é **Desativado**.
 - **Reconhecimento biométrico:** ativa o reconhecimento biométrico. Se essa configuração for **On**, o campo **Caracteres obrigatórios** ficará oculto. O padrão é **Off**.
 - **Caracteres obrigatórios:** especifica os tipos de caracteres necessários para os códigos secretos. Na lista, escolha **Sem Restrição**, **Letras e números**, **Apenas números** ou **Apenas letras**. Use **Sem restrições** somente para dispositivos que executam o Android 7.0. Android 7.1 e versões posteriores não oferecem suporte à configuração **Sem restrições**. O padrão é **Letras e números**.
 - **Cadeias de caracteres proibidas:** para dispositivos com Samsung Knox 3.0 e posterior que tenham uma chave de licença Knox válida configurada. Somente para dispositivos totalmente gerenciados. Essa configuração não se aplica a dispositivos registrados como dispositivos de perfil de trabalho. Especifica as cadeias de caracteres que os usuários não podem usar como código secreto. Crie cadeias de caracteres proibidas para impedir que os usuários usem cadeias de caracteres inseguras que sejam fáceis de adivinhar, como

“senha”, “pwd”, “bemvindo”, “123456”, “111111” e assim por diante. Para cada cadeia de caracteres que você deseja negar: clique em **Adicionar**, digite a cadeia de caracteres que você não quer que os usuários usem e clique em **Salvar** para adicionar a cadeia de caracteres, ou clique em **Cancelar** para cancelar a adição da cadeia de caracteres.

- **Regras avançadas:** aplica regras avançadas para os tipos de caracteres que podem estar presentes em códigos secretos. Quando essa configuração estiver **On**, defina as configurações em **Número mínimo de** e **Número máximo de**. Essa configuração não está disponível para dispositivos Android anteriores ao Android 5.0. O padrão é **Off**.
- **Número mínimo de:**
 - * **Símbolos:** especifica o número mínimo de símbolos. O padrão é **0**.
 - * **Letras:** especifica o número mínimo de letras. O padrão é **0**.
 - * **Letras minúsculas:** especifica o número mínimo de letras minúsculas. O padrão é **0**.
 - * **Letras maiúsculas:** especifica o número mínimo de letras maiúsculas. O padrão é **0**.
 - * **Números ou símbolos:** especifica o número mínimo de números ou símbolos. O padrão é **0**.
 - * **Números:** especifica o número mínimo de números. O padrão é **0**.
 - * **Caracteres alterados:** para dispositivos com Samsung Knox 3.0 e posterior que tenham uma chave de licença Knox válida configurada. Somente para dispositivos totalmente gerenciados. Essa configuração não se aplica a dispositivos registrados como dispositivos de perfil de trabalho. Especifica o número de caracteres que os usuários devem alterar em seus códigos secretos anteriores. O padrão é **0**.
- **Número máximo de:** para dispositivos com Samsung Knox 3.0 e posterior que tenham uma chave de licença Knox válida configurada. Somente para dispositivos totalmente gerenciados. Essa configuração não se aplica a dispositivos registrados como dispositivos de perfil de trabalho.
 - * **Número de vezes em que um caractere pode ocorrer:** especifica o número máximo de vezes que um caractere pode ocorrer em um código secreto. O padrão é **0**, o que significa que não há limite máximo.
 - * **Tamanho da sequência alfabética:** especifica o tamanho máximo de uma sequência alfabética em um código secreto. O padrão é **0**, o que significa que não há limite máximo.
 - * **Tamanho da sequência numérica:** especifica o tamanho máximo de uma sequência numérica em um código secreto. O padrão é **0**, o que significa que não há limite máximo.
- **Segurança de código secreto do dispositivo:**
 - **Limpar o dispositivo depois de (tentativas de logon malsucedidas):** especifica o número de vezes que um usuário pode errar ao fazer login antes que o dispositivo seja totalmente apagado. O padrão é **Não definido**.
 - **Bloquear dispositivos após (minutos de inatividade) (0-999):** especifica o número de

minutos que um dispositivo pode ficar inativo antes de ser bloqueado. O padrão é **Nenhum**.

- **Expiração de código secreto em dias (1-730):** especifica o número de dias após os quais o código secreto expira. Os valores válidos são 1 a 730. O padrão é **0**, o que significa que a senha nunca expira.
- **Senhas anteriores salvas (0-50):** especifica o número de senhas usadas a serem salvas. Os usuários não conseguem usar nenhuma senha encontrada nessa lista. Os valores válidos são 0 a 50. O padrão é **0**, o que significa que os usuários podem reutilizar as senhas.
- **Bloquear o dispositivo depois de (tentativas de logon malsucedidas):** para dispositivos com Samsung Knox 3.0 e posterior que tenham uma chave de licença Knox válida configurada. Somente para dispositivos totalmente gerenciados. Essa configuração não se aplica a dispositivos registrados como dispositivos de perfil de trabalho. Especifica o número de vezes que um usuário pode errar ao fazer logon, após o qual o dispositivo será bloqueado. O padrão é **Não definido**.
- **Desafio de segurança do perfil de trabalho:** exigir que os usuários concluam um desafio de segurança para acesso a aplicativos em execução em um perfil de trabalho do Android Enterprise. Para dispositivos que executam o Android 7.0 e versões posteriores. Quando essa configuração estiver **Ativada**, defina as configurações em **Requisitos de código secreto para desafio de segurança de perfil de trabalho** e **Segurança de código secreto para desafio de segurança de perfil de trabalho**. O padrão é **Desativado**.
- **Requisitos de código secreto para desafio de segurança de perfil de trabalho:**
 - **Tamanho mínimo:** especifica o tamanho mínimo do código secreto. O padrão é 6.
 - **Permitir que os usuários tornem a senha visível:** para dispositivos com Knox 3.0 e posterior que tenham uma chave de licença Knox válida configurada. Permite que os usuários tornem a senha visível. O padrão é **Desativado**.
 - **Reconhecimento biométrico:** ativa o reconhecimento biométrico. Se essa configuração for **On**, o campo **Caracteres obrigatórios** ficará oculto. O padrão é **Off**.
 - **Caracteres obrigatórios:** especifica os tipos de caracteres necessários para os códigos secretos. Na lista, escolha **Sem Restrição**, **Letras e números**, **Apenas números** ou **Apenas letras**. Use **Sem restrições** somente para dispositivos que executam o Android 7.0. Android 7.1 e versões posteriores não oferecem suporte à configuração **Sem restrições**. O padrão é **Letras e números**.
 - **Cadeias de caracteres proibidas:** para dispositivo com Knox 3.0 e posterior que tenha uma chave de licença Knox válida configurada. Especifica as cadeias de caracteres que os usuários não podem usar como código secreto. Crie cadeias de caracteres proibidas para impedir que os usuários usem cadeias de caracteres inseguras que sejam fáceis de adivinhar, como “senha”, “pwd”, “bemvindo”, “123456”, “111111” e assim por diante. Para cada cadeia de caracteres que você deseja negar: clique em **Adicionar**, digite a cadeia de caracteres que você não quer que os usuários usem e clique em **Salvar** para adicionar a cadeia

de caracteres, ou clique em **Cancelar** para cancelar a adição da cadeia de caracteres.

- **Regras avançadas:** aplica regras avançadas para os tipos de caracteres que podem estar presentes em códigos secretos. Quando essa configuração estiver **On**, defina as configurações em **Número mínimo de** e **Número máximo de**. Essa configuração não está disponível para dispositivos Android anteriores ao Android 5.0. O padrão é **Off**.
- **Número mínimo de:**
 - * **Símbolos:** especifica o número mínimo de símbolos. O padrão é **0**.
 - * **Letras:** especifica o número mínimo de letras. O padrão é **0**.
 - * **Letras minúsculas:** especifica o número mínimo de letras minúsculas. O padrão é **0**.
 - * **Letras maiúsculas:** especifica o número mínimo de letras maiúsculas. O padrão é **0**.
 - * **Números ou símbolos:** especifica o número mínimo de números ou símbolos. O padrão é **0**.
 - * **Números:** especifica o número mínimo de números. O padrão é **0**.
 - * **Caracteres alterados:** para dispositivos com Knox 3.0 e posterior que tenham uma chave de licença Knox válida configurada. Especifica o número de caracteres que os usuários devem alterar em seus códigos secretos anteriores. O padrão é **0**.
- **Número máximo de:** para dispositivos com Knox 3.0 e posterior que tenham uma chave de licença Knox válida configurada.
 - * **Número de vezes em que um caractere pode ocorrer:** especifica o número máximo de vezes que um caractere pode ocorrer em um código secreto. O padrão é **0**, o que significa que não há limite máximo.
 - * **Tamanho da sequência alfabética:** especifica o tamanho máximo de uma sequência alfabética em um código secreto. O padrão é **0**, o que significa que não há limite máximo.
 - * **Tamanho da sequência numérica:** especifica o tamanho máximo de uma sequência numérica em um código secreto. O padrão é **0**, o que significa que não há limite máximo.
- **Ativar código secreto unificado:** se **Ativado**, os usuários usarão um código secreto para seus dispositivos e perfis de trabalho. Se **Desativado**:
 - * Os usuários devem usar códigos secretos diferentes para o dispositivo e para o perfil de trabalho.
 - * A configuração **Use one lock** no dispositivo, que os usuários definem se quiserem usar um código secreto para o dispositivo e perfil de trabalho, está desativada. O usuário não pode ativá-la.
 - * Se o requisito de código secreto para o desafio de segurança do perfil de trabalho for mais complexo do que o código secreto do dispositivo, os usuários com a configuração **Use one lock** ativada serão solicitados a alterar o código secreto do perfil de trabalho.O padrão é **Off**. Disponível a partir do Android 9.0.

- **Segurança de código secreto para desafio de segurança de perfil de trabalho**
 - **Limpar o contêiner após (tentativas de logon malsucedidas):** especifica o número de vezes que um usuário pode errar ao fazer logon, após o qual o perfil de trabalho e seus dados serão apagados do dispositivo. Os usuários precisam reinicializar o perfil de trabalho após efetuar a limpeza. O padrão é **Não definido**.
 - **Bloquear contêiner após (minutos de inatividade):** especifica o número de minutos que um dispositivo pode ficar inativo antes de o perfil de trabalho ser bloqueado. O padrão é **Nenhum**.
 - **Expiração de código secreto em dias (1-730):** especifica o número de dias após os quais o código secreto expira. Os valores válidos são 1 a 730. O padrão é **0**, o que significa que a senha nunca expira.
 - **Senhas anteriores salvas (0-50):** especifica o número de senhas usadas a serem salvas. Os usuários não conseguem usar nenhuma senha encontrada nessa lista. Os valores válidos são 0 a 50. O padrão é **0**, o que significa que os usuários podem reutilizar senhas.
 - **Bloquear o contêiner depois de (tentativas de logon malsucedidas):** para dispositivos com Knox 3.0 e posterior que tenham uma chave de licença Knox válida configurada. Especifica o número de vezes que um usuário pode errar ao fazer logon, após o qual o dispositivo será bloqueado. O padrão é **Não definido**.

Configurações do Windows Phone

Passcode Policy	Passcode Policy
1 Policy Info	This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.
2 Platforms	<p>Passcode required <input checked="" type="checkbox"/></p> <p>Allow simple passcodes <input type="checkbox"/></p> <p>Passcode requirements</p> <p>Minimum length <input type="text" value="6"/></p> <p>Characters required <input type="text" value="Letters only"/></p> <p>Minimum number of symbols <input type="text" value="1"/></p> <p>Passcode security</p> <p>Lock device after (minutes of inactivity) (0-999) <input type="text" value="0"/></p> <p>Passcode expiration in 0-730 days * <input type="text" value="0"/></p> <p>Previous passwords saved (0-50) <input type="text" value="0"/> ⓘ</p> <p>Maximum failed sign-on attempts before wipe (0-999) * <input type="text" value="0"/></p>
<input type="checkbox"/> iOS <input type="checkbox"/> macOS <input type="checkbox"/> Android <input type="checkbox"/> Samsung KNOX <input type="checkbox"/> Android for Work <input checked="" type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Desktop/Tablet	
3 Assignment	

- **Código secreto obrigatório:** selecione essa opção para não exigir um código secreto para dispositivos Windows Phone. A configuração padrão é **I**, o que exige um código secreto. A página é recolhida e as opções a seguir desaparecem quando você desativa essa configuração.
- **Permitir código secreto simples:** selecione se códigos secretos simples são permitidos. Códigos secretos simples são um conjunto de caracteres repetidos ou sequenciais. O padrão é **O**.

- **Requisitos de código secreto**

- **Tamanho mínimo:** na lista, clique no tamanho mínimo do código secreto. O padrão é **6**.
- **Caracteres obrigatórios:** na lista, clique em **Numérico ou alfanumérico**, **Apenas letras** ou **Apenas números** para configurar como os códigos secretos são compostos. O padrão é **Apenas letras**.
- **Número mínimo de símbolos:** na lista, clique no número de símbolos que o código secreto deve conter. O padrão é **1**.

- **Segurança do código secreto**

- **Bloquear dispositivos após (minutos de inatividade):** clique no número de minutos durante os quais um dispositivo pode ficar inativo antes de ser bloqueado. O padrão é **0**.
- **Expiração de código secreto em 0-730 dias:** digite o número de dias após os quais o código secreto expira. Os valores válidos são de 0 a 730. O padrão é **0**, o que significa que a senha nunca expira.
- **Senhas anteriores salvas (0-50):** digite o número de senhas usadas a serem salvas. Os usuários não conseguem usar nenhuma senha encontrada nessa lista. Os valores válidos são de 0 a 50. O padrão é **0**, o que significa que os usuários podem reutilizar senhas.
- **Máximo de falhas em tentativas de login antes de apagamento (0-999):** digite o número de vezes que um usuário pode não conseguir fazer login depois que os dados corporativos são apagados do dispositivo. O padrão é **0**.

Configurações do Windows Desktop/Tablet

Passcode Policy	Passcode Policy
1 Policy Info	This policy creates a passcode policy based on the standards of your organization. You can require a code on the device and can set formatting rules and other passcode rules, such as the grace period before device lock.
2 Platforms	<p>Passcode required <input checked="" type="checkbox"/></p> <p>Passcode security</p> <p>Lock device after (minutes of inactivity) (0-999) <input type="text" value="0"/></p> <p>Passcode expiration in 0-730 days * <input type="text" value="0"/></p> <p>Previous passwords saved (0-24) <input type="text" value="0"/> ⓘ</p> <p>Passcode requirements</p> <p>Minimum length <input type="text" value="6"/></p> <p>► Deployment Rules</p>
3 Assignment	

- **Não permitir login de conveniência:** selecione se os usuários têm permissão para acessar os dispositivos deles com senhas de imagem ou logins biométricos. O padrão é **Off**.
- **Tamanho mínimo do código secreto:** na lista, clique no tamanho mínimo do código secreto. O padrão é **6**.
- **Máximo de tentativas do código secreto antes de apagar:** na lista, clique no número de vezes

que um usuário pode não conseguir fazer login depois que os dados corporativos são apagados do dispositivo. O padrão é **4**.

- **Expiração de código secreto em dias (0-730):** digite o número de dias após os quais o código secreto expira. Os valores válidos são de 0 a 730. O padrão é **0**, o que significa que a senha nunca expira.
- **Histórico do código secreto (1-24):** digite o número de códigos secretos usados a serem salvos. Os usuários não conseguem usar nenhum código secreto encontrado nessa lista. Os valores válidos são 1 a 24. Você deve inserir um número entre 1 e 24 nesse campo. O padrão é **0**.
- **Máximo de inatividade antes do bloqueio do dispositivo em minutos (1-999):** digite o período de tempo, em minutos, durante o qual um dispositivo pode ficar inativo antes de ser bloqueado. Os valores válidos são 1 a 999. Você deve inserir um número entre 1 e 999 nesse campo. O padrão é **0**.

Política de dispositivo do ponto de acesso pessoal

April 23, 2020

Você pode permitir que os usuários se conectem à Internet quando não estão ao alcance de uma rede WiFi usando a conexão de dados celulares, por meio da funcionalidade de ponto de acesso pessoal de seus dispositivos iOS. Disponível no iOS 7.0 e versões posteriores.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

- **Desativar ponto de acesso pessoal:** selecione se pretende desativar a funcionalidade de ponto de acesso pessoal em dispositivos do usuário. O padrão é **0**, que desliga o ponto de acesso pessoal em dispositivos de usuários. Esta política não desativa a funcionalidade. Os usuários ainda podem usar o ponto de acesso pessoal em seus dispositivos, mas quando a política é implantada, o ponto de acesso pessoal é desativado para que não permaneça ativado por padrão.

Política de dispositivo de remoção de perfil

April 23, 2020

Você pode criar uma política de dispositivo de remoção de perfil de aplicativo no XenMobile. A política, quando implantada, remove o perfil de aplicativo dos dispositivos iOS ou macOS dos usuários.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

Profile Removal Policy	Profile Removal Policy This policy lets you remove a profile for iOS or macOS from a device.
1 Policy Info	Profile ID * <input type="text" value="This field is mandatory."/>
2 Platforms	Comment <input type="text"/>
<input checked="" type="checkbox"/> iOS	Deployment Rules
<input checked="" type="checkbox"/> macOS	
3 Assignment	

- **ID do perfil:** na lista, clique no ID do perfil do aplicativo. Este campo é obrigatório.
- **Comentário:** digite um comentário opcional.

Configurações do macOS

Profile Removal Policy	Profile Removal Policy This policy lets you remove a profile for iOS or macOS from a device.
1 Policy Info	Profile ID * <input type="text" value="This field is mandatory."/>
2 Platforms	Deployment scope <input type="text" value="User"/> macOS 10.7+
<input type="checkbox"/> iOS	Comment <input type="text"/>
<input checked="" type="checkbox"/> macOS	Deployment Rules
3 Assignment	

- **ID do perfil:** na lista, clique no ID do perfil do aplicativo. Este campo é obrigatório.
- **Alcance da implantação:** na lista, clique em **Usuário** ou **Sistema**. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.
- **Comentário:** digite um comentário opcional.

Política de dispositivo do perfil de provisionamento

April 23, 2020

Quando você desenvolve e assina o código de um aplicativo empresarial iOS, geralmente inclui um perfil de provisionamento de distribuição empresarial, exigido pela Apple para que o aplicativo seja executado em um dispositivo iOS. Se um perfil de configuração estiver ausente ou tiver expirado, o aplicativo falhará quando um usuário tocar para abri-lo.

O principal problema dos perfis de provisionamento é que eles expiram um ano depois de terem sido gerados no Apple Developer Portal e você deve manter o controle das datas de expiração de todos os seus perfis de provisionamento em todos os dispositivos iOS registrados por seus usuários. Rastrear as datas de expiração envolve não apenas o acompanhamento das datas de expiração propriamente ditas, mas também de qual versão do aplicativo está sendo usada por usuários específicos. Duas soluções são enviar por email os perfis de configuração para os usuários ou colocá-los em um portal da Web para download e instalação. Essas soluções funcionam, mas são propensas a erro porque elas exigem que os usuários sigam as instruções em um email ou acessem o portal da Web e baixem o perfil correto para instalá-lo.

Para tornar esse processo transparente para os usuários, no XenMobile, você pode instalar e remover perfis de provisionamento com as políticas de dispositivo. Os perfis ausentes ou expirados são removidos conforme necessário e os perfis atualizados são instalados nos dispositivos de usuários, para que seja preciso apenas tocar em um aplicativo para abri-lo.

Antes de criar uma política de perfil de provisionamento, você deve criar um arquivo de perfil de provisionamento. Para obter mais informações, consulte o artigo da Apple sobre como criar um perfil de provisionamento de desenvolvimento no [Site do desenvolvedor da Apple](#).

Configurações de iOS

Provisioning Profile Policy	Policy Information
1 Policy Info	This policy lets you upload an iOS provisioning profile.
2 Platforms	Policy Name * <input type="text"/>
<input checked="" type="checkbox"/> iOS	Description <input type="text"/>
3 Assignment	

- **Perfil de provisionamento do iOS:** selecione o arquivo de perfil de provisionamento a ser importado clicando em **Procurar** e navegando até a localização do arquivo.

Política de dispositivo da remoção de perfil de provisionamento

October 26, 2020

Você pode remover os perfis de provisionamento do iOS com as políticas de dispositivo. Para obter mais informações sobre perfis de provisionamento, consulte [Política de dispositivo do perfil de provisionamento](#).

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

- **Perfil de provisionamento do iOS:** na lista, clique no perfil de provisionamento que deseja remover.
- **Comentário:** opcionalmente, adicione um comentário.

Política de dispositivo de proxy

June 15, 2021

Você pode adicionar uma política de dispositivo no XenMobile para especificar as configurações de proxy HTTP global dos dispositivos que executam o Windows Mobile/CE e o iOS 6.0 ou versões posteriores. Você pode implantar somente uma política de proxy HTTP global por dispositivo.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Pré-requisitos

Antes de implantar essa política, defina todos os dispositivos iOS para os quais você deseja atribuir um proxy HTTP global no modo Supervisionado. Para obter detalhes, consulte [Para colocar um dispositivo iOS no modo Supervisionado usando o Apple Configurator](#) ou [Implantar dispositivos através do Programa de Implantação da Apple](#).

Defina regras de implantação para registrar dispositivos antes de enviar a política de proxy para os dispositivos.

Configurações de iOS

- **Configuração de proxy:** clique em **Manual** ou **Automática** para selecionar como o proxy será configurado nos dispositivos dos usuários.
 - Se você clicar em **Manual**, defina estas configurações:
 - * **Nome do host ou endereço IP do servidor proxy:** digite o nome do host ou o endereço IP do servidor proxy. Este campo é obrigatório.
 - * **Porta do servidor proxy:** digite o número da porta do servidor proxy. Este campo é obrigatório.
 - * **Nome de usuário:** digite um nome de usuário opcional para autenticação no servidor proxy.
 - * **Senha:** digite uma senha opcional para autenticação no servidor proxy.
 - Se você clicar em **Automático**, defina estas configurações:
 - * **URL PAC do Proxy:** digite a URL do arquivo PAC que define a configuração de proxy.
 - * **Permitir conexão direta se o PAC estiver inacessível:** selecione se os usuários terão permissão para se conectarem diretamente com o destino se o arquivo PAC estiver inacessível. O padrão é **On**. Essa opção está disponível somente no iOS 7.0 e versões posteriores.
- **Permitir ignorar o proxy para acessar redes cativas:** selecione se o proxy pode ser ignorado para o acesso a redes cativas. O padrão é **Off**.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do Windows Mobile/CE

- **Rede:** na lista, clique no tipo de rede a ser usada. O padrão é **Escritório interno**. As opções possíveis são:
 - Escritório definido pelo usuário
 - Internet definida pelo usuário
 - Escritório interno
 - Internet interna
- **Rede:** na lista, clique no protocolo de conexão de rede a ser usado. O padrão é **HTTP**. As opções possíveis são:
 - HTTP

- WAP
- SOCKS 4
- SOCKS 5
- **Nome do host ou endereço IP do servidor proxy:** digite o nome do host ou o endereço IP do servidor proxy. Este campo é obrigatório.
- **Porta do servidor proxy:** digite o número da porta do servidor proxy. Este campo é obrigatório. O padrão é **80**.
- **Nome de usuário:** digite um nome de usuário opcional para autenticação no servidor proxy.
- **Senha:** digite uma senha opcional para autenticação no servidor proxy.
- **Nome de domínio:** digite um nome de domínio opcional.
- **Ativar:** selecione se o proxy deve ser ativado. O padrão é **On**.

Política de dispositivo do Registro

April 23, 2020

O Registro do Windows Mobile/CE armazena dados sobre as definições de aplicativos, drivers, preferências do usuário e configurações. No XenMobile, você pode definir as chaves e os valores do registro que permitem administrar dispositivos Windows Mobile/CE.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do Windows Mobile/CE

Para cada chave do registro ou par chave/valor do registro que você deseja adicionar, clique em **Adicionar** e faça o seguinte:

- **Caminho da chave do Registro:** digite o caminho completo da chave do registro. Por exemplo, digite **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows** para especificar a rota para a chave do Windows a partir da chave raiz HKEY_LOCAL_MACHINE.
- **Nome do valor do registro:** digite o nome do valor da chave do registro. Por exemplo, digite **ProgramFilesDir** para adicionar esse nome de valor ao caminho de chave do registro HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion. Se você deixar esse campo em branco, isso significará que você está adicionando uma chave do registro e não um par chave/valor do registro.
- **Tipo:** na lista, clique no tipo de dados do valor. O padrão é **DWORD**. As opções possíveis são:
 - **DWORD:** um inteiro não assinado de 32 bits.
 - **Cadeia de caracteres:** qualquer cadeia de caracteres.

- **Cadeia de caracteres estendida:** um valor de cadeia de caracteres que pode conter variáveis de ambiente como %TEMP% ou %USERPROFILE%.
- **Binário:** quaisquer dados binários arbitrários.
- **Valor:** digite o valor associado ao nome do valor do Registro. Por exemplo, para especificar o valor de ProgramFilesDir, digite **C:\Program Files**.
- Clique em **Salvar** para salvar as informações de chave do registro ou em **Cancelar** para não salvá-las.

Suporte remoto à política de dispositivo

October 26, 2020

Nota:

Para implantações do XenMobile Server no local: o suporte remoto permite que o pessoal da central de ajuda assuma o controle remotamente de dispositivos móveis gerenciados Windows CE e Android. Conversão de tela é compatível com somente dispositivos Samsung KNOX.

O suporte remoto não é suportado para implantações do XenMobile Server em cluster no local.

Para obter mais informações, consulte [Opções de suporte e suporte remoto](#).

Crie uma política de suporte remoto no XenMobile para conceder a você acesso remoto aos dispositivos Windows e Android compatíveis. Você pode configurar dois tipos de suporte:

- **Básico**, que permite exibir informações de diagnóstico sobre o dispositivo, como informações do sistema, processos em execução, gerenciador de tarefas (uso da memória e da CPU), conteúdo da pasta do software instalado e assim por diante.
- **Premium**, que permite controlar remotamente a tela do dispositivo, incluindo:
 - controlar cores (na janela principal ou em uma janela flutuante separada)
 - estabelecer uma sessão de Voice-over-IP (VoIP) entre o suporte técnico e o usuário
 - definir configurações
 - criar uma sessão de chat entre o suporte técnico e o usuário

Para implementar essa política, você deve fazer o seguinte:

- Instale o aplicativo XenMobile Remote Support no seu ambiente.
- Configure um túnel de aplicativo de suporte remoto. Para obter detalhes, consulte [Política de dispositivo de encapsulamento de aplicativo](#).
- Configure uma política de dispositivo de suporte remoto do Samsung KNOX, conforme descrito neste tópico.
- Implante a política de suporte remoto do túnel de aplicativo e a política de suporte remoto do Samsung KNOX para os dispositivos do usuário.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do Android e Windows CE

Remote Support Policy	Remote Support Policy This policy lets you enable premium remote support on Samsung KNOX devices to let administrators troubleshoot devices remotely.
1 Policy Info	Remote support <input checked="" type="radio"/> Basic remote support <input type="radio"/> Premium remote support
2 Platforms	
<input checked="" type="checkbox"/> Samsung KNOX	▶ Deployment Rules
3 Assignment	

- **Suporte remoto:** selecione **Suporte remoto básico** ou **Suporte remoto premium**. O padrão é o **Suporte remoto básico**.

Política de dispositivo de restrições

August 20, 2021

Essa política de dispositivo de restrições permite ou restringe certos recursos ou funcionalidades nos dispositivos dos usuários, como a câmera. Você também pode definir restrições de segurança, bem como restrições sobre conteúdo de mídia e restrições sobre os tipos de aplicativos que os usuários podem e não podem instalar. A maior parte das configurações de restrição têm **I**, ou *permite* como padrão. As exceções principais estão no recurso Segurança do iOS - Forçar e em todos os recursos do Tablet Windows, que têm **O** ou *restringe* como padrão.

Para telefones Windows 10 RS2, depois que uma política de XML personalizado ou de Restrições que desativa o Internet Explorer é implantada no telefone, o navegador permanece ativado. Para resolver esse problema, reinicie o telefone. Esse é um problema de terceiros.

Dica:

Qualquer opção para a qual você selecionar **I** significa que o usuário pode executar a operação ou usar o recurso. Por exemplo:

Câmera. Se **I**, o usuário poderá usar a câmera no seu dispositivo. Se **O**, o usuário não poderá usar a câmera no seu dispositivo.

Capturas de tela. Se **I**, o usuário pode fazer capturas de tela no seu dispositivo. Se **O**, o usuário não pode fazer capturas de tela no seu dispositivo.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte a [Política de dispositivo de VPN](#).

Configurações de iOS

Algumas configurações de política de restrições do iOS se aplicam somente a versões específicas do iOS, conforme observado aqui e na página da política de Restrições do console XenMobile.

As configurações de política de restrições do iOS podem ser aplicadas quando o dispositivo está registrado no modo de registro do usuário, modo não supervisionado (MDM completo) ou modo supervisionado. A tabela a seguir mostra os modos de registro disponíveis para cada configuração de política de restrições para iOS 13 e posterior.

Como observado na tabela, algumas configurações que estavam anteriormente disponíveis no modo não supervisionado e supervisionado estão disponíveis apenas no modo supervisionado começando com o iOS 13. Aplicam-se as seguintes regras:

- Se um dispositivo iOS 13+ supervisionado for registrado no XenMobile, as configurações se aplicam ao dispositivo.
- Se um dispositivo iOS 13+ não supervisionado for registrado no XenMobile, as configurações não se aplicam ao dispositivo.
- Se um dispositivo iOS 12 (ou inferior) que já estiver registrado no XenMobile for atualizar para o iOS 13, não haverá alterações. As configurações se aplicam ao dispositivo como antes da atualização.

Para obter informações para configurar um dispositivo iOS para o modo supervisionado, consulte [Para colocar um dispositivo iOS no modo Supervisionado usando o Apple Configurator](#).

Configuração	Registro do usuário	Não supervisionado	Supervisionado
Permitir controles de hardware			
Câmera	Não	Sim	Sim
FaceTime	Não	Não (novo no iOS 13)	Sim
Capturas de tela	Sim	Não	Sim
Permitir que o aplicativo Classroom observe remotamente as telas do alunos	Não	Não	Sim
Permitir que o aplicativo Classroom execute AirPlay e Exibir tela sem avisar	Não	Não	Sim
Fluxos de foto	Não	Sim	Sim
Fluxos de fotos compartilhadas	Não	Sim	Sim
Discagem por voz	Não	Sim	Sim
Siri	Sim	Sim	Sim
Permitir enquanto o dispositivo estiver bloqueado	Sim	Sim	Sim
Filtro de linguagem indecorosa da Siri	Não	Não	Sim
Instalação de aplicativos	Não	Não (novo no iOS 13)	Sim
Permitir busca em segundo plano durante roaming	Não	Sim	Sim
Permitir aplicativos			
iTunes Store	Não	Não (novo no iOS 13)	Sim
Compras no aplicativo	Não	Sim	Sim

Configuração	Registro do usuário	Não supervisionado	Supervisionado
Exigir senha do iTunes para compras	Não	Sim	Sim
Safari	Não	Não (novo no iOS 13)	Sim
Preenchimento automático	Não	Não (novo no iOS 13)	Sim
Forçar aviso de fraude	Sim	Sim	Sim
Ativar JavaScript	Não	Sim	Sim
Bloquear pop-ups	Não	Sim	Sim
Aceitar cookies	Não	Sim	Sim
Rede - Permitir ações do iCloud			
Documentos e dados do iCloud	Não	Não (novo no iOS 13)	Sim
Backup do iCloud	Não	Sim	Sim
Chaveiro de fotos do iCloud	Não	Sim	Sim
Biblioteca de fotos do iCloud	Não	Sim	Sim
Segurança - Força			
Backups criptografados	Sim	Sim	Sim
Rastreamento de anúncios limitado	Não	Sim	Sim
Código secreto no primeiro emparelhamento do AirPlay	Sim	Sim	Sim
Apple Watch emparelhado para usar detecção de pulso	Sim	Sim	Sim

Configuração	Registro do usuário	Não supervisionado	Supervisionado
Compartilhamento de documentos gerenciados com AirDrop	Sim	Sim	Sim
Segurança - Permitir			
Aceitar certificados SSL não confiáveis	Não	Sim	Sim
Atualização automática de definições de segurança do certificado	Não	Sim	Sim
Documentos de aplicativos gerenciados em aplicativos não gerenciados	Sim	Sim	Sim
Aplicativos não gerenciados leem contatos gerenciados	Não	Não	Sim
Aplicativos gerenciados gravam contatos não gerenciados	Não	Não	Sim
Documentos de aplicativos não gerenciados em aplicativos gerenciados	Sim	Sim	Sim
Envio de informações de diagnóstico para a Apple	Sim	Sim	Sim
Touch ID para desbloquear o dispositivo	Não	Sim	Sim

Configuração	Registro do usuário	Não supervisionado	Supervisionado
Notificações do Passbook quando o dispositivo está bloqueado	Não	Sim	Sim
Handoff	Não	Sim	Sim
Sincronização do iCloud para aplicativos gerenciados	Sim	Sim	Sim
Backup para livros da empresa	Sim	Sim	Sim
Sincronização de notas e destaques para livros da empresa	Sim	Sim	Sim
Resultados de Internet no Spotlight	Não	Sim	Sim
Confiança de aplicativo empresarial	Não	Sim	Sim
Apenas configurações supervisionadas - Permitir			
Apagar todo o conteúdo e configurações	Não	Não	Sim
Configuração de restrições	Não	Não	Sim
Podcasts	Não	Não	Sim
Instalação de perfis de configuração	Não	Não	Sim
Modificação de impressão digital	Não	Não	Sim

Configuração	Registro do usuário	Não supervisionado	Supervisionado
Instalação de aplicativos do dispositivo	Não	Não	Sim
Atalhos de teclado	Não	Não	Sim
Apple Watch pareado	Não	Não	Sim
Modificação de código secreto	Não	Não	Sim
Modificação do nome do dispositivo	Não	Não	Sim
Modificação do papel de parede	Não	Não	Sim
Download automático de aplicativos	Não	Não	Sim
AirDrop	Não	Não	Sim
iMessage	Não	Não	Sim
Conteúdo gerado pelo usuário da Siri	Não	Não	Sim
iBooks	Não	Não	Sim
Remoção de aplicativos	Não	Sim	Sim
Game Center	Não	Não (novo no iOS 13)	Sim
Adicionar amigos	Não	Não	Sim
Jogos multiplayer	Não	Não (novo no iOS 13)	Sim
Modificando configurações de conta	Não	Não	Sim
Modificando configurações de dados celulares do aplicativo	Não	Não	Sim

Configuração	Registro do usuário	Não supervisionado	Supervisionado
Modificando configurações de dados celulares do aplicativo	Não	Não	Sim
Modificando configurações de Encontrar meus amigos	Não	Não	Sim
Emparelhamento com hosts não Configurator	Não	Não	Sim
Teclados intuitivos	Não	Não	Sim
Teclado com correção automática	Não	Não	Sim
Teclado com corretor ortográfico	Não	Não	Sim
Pesquisa de definições	Não	Não	Sim
ID de pacote único de aplicativos			
Notícias	Não	Não	Sim
Serviço Apple Music	Não	Não	Sim
iTunes Radio	Não	Não	Sim
Modificação de notificações	Não	Não	Sim
Uso restrito do aplicativo	Não	Não	Sim
Modificação de submissão de diagnóstico	Não	Não	Sim
Modificação de Bluetooth	Não	Não	Sim
Permitir ditado	Não	Não	Sim

Configuração	Registro do usuário	Não supervisionado	Supervisionado
Entrar somente em redes Wi-Fi instaladas por uma política de Wi-Fi	Não	Não	Sim
Permitir que o aplicativo Classroom execute AirPlay e Exibir tela sem avisar	Não	Não	Sim
Permitir que o aplicativo Classroom bloquear um aplicativo e bloquear o dispositivo sem avisar	Não	Não	Sim
Entrar automaticamente em aulas do aplicativo Classroom sem avisar	Não	Não	Sim
Permitir AirPrint	Não	Não	Sim
Permitir armazenamento de credenciais do AirPrint no Keychain	Não	Não	Sim
Permitir descoberta de impressoras AirPrint usando iBeacons	Não	Não	Sim
Permitir o AirPrint em destinos com certificados confiáveis	Não	Não	Sim
Adicionando configurações de VPN	Não	Não	Sim

Configuração	Registro do usuário	Não supervisionado	Supervisionado
Modificando configurações de plano de dados celulares	Não	Não	Sim
Removendo aplicativos do sistema	Não	Não	Sim
Configurando novos dispositivos próximos	Não	Não	Sim
Permitir o modo restrito de USB	Não	Não	Sim
Forçar atualizações de software atrasadas	Não	Não	Sim
Atraso forçado de atualização de software	Não	Não	Sim
Forçar solicitação de permissão de sala de aula para sair das aulas	Não	Não	Sim
Forçar data e hora automáticas	Não	Não	Sim
Preenchimento automático da senha	Não	Não	Sim
Solicitações de proximidade de senha	Não	Não	Sim
Compartilhamento de senha	Não	Não	Sim
Segurança - Mostrar na tela de bloqueio			
Centro de controle	Sim	Sim	Sim
Notificação	Sim	Sim	Sim
Exibição de hoje	Sim	Sim	Sim

Configuração	Registro do usuário	Não supervisionado	Supervisionado
Conteúdo de mídia - Permitir			
Música, podcasts e material do iTunes U explícitos	Não	Não (novo no iOS 13)	Sim
Conteúdo sexual explícito em iBooks	Não	Sim	Sim
Região de classificações	Não	Sim	Sim
Filmes	Não	Sim	Sim
Programas de TV	Não	Sim	Sim
Aplicativos	Não	Sim	Sim

- **Permitir controles de hardware**

- **Câmera:** permitir que os usuários usem a câmera nos dispositivos deles.
 - * **FaceTime:** permitir que os usuários usem o FaceTime nos respectivos dispositivos. Para dispositivos iOS supervisionados.
- **Capturas de tela:** permitir que os usuários façam capturas de tela nos dispositivos deles.
 - * **Permitir que o aplicativo Sala de Aula observe remotamente as telas dos alunos:** se essa restrição não estiver selecionada, o professor não poderá usar o aplicativo Sala de Aula para observar remotamente as telas dos alunos. A configuração padrão está selecionada, um professor pode usar o aplicativo Sala de Aula para observar as telas dos alunos. A configuração de **Permitir que o aplicativo Sala de Aula execute o AirPlay e Exibir Tela sem solicitar** determina se os alunos receberão uma solicitação para conceder a permissão ao professor. Para dispositivos iOS supervisionados.
 - * **Permitir que o aplicativo Sala de Aula execute o AirPlay e Exibir Tela sem solicitar:** se essa restrição estiver marcada, o instrutor pode executar o AirPlay e exibir a tela no dispositivo de um aluno sem pedir permissão. O padrão é desmarcado. Para dispositivos iOS supervisionados.
- **Fluxos de foto:** permitir que os usuários usem o MyPhotoStream para compartilhar fotos usando o iCloud com todos os dispositivos iOS deles.
- **Fluxos de fotos compartilhados:** permitir que os usuários usem o Compartilhamento de fotos do iCloud para compartilhar fotos com colegas de trabalho, amigos e família.
- **Discagem por voz:** ativa a discagem por voz nos dispositivos do usuário.
- **Siri:** permite que os usuários usem a Siri.

- * **Permitir enquanto o dispositivo estiver travado:** permitir que os usuários usem a Siri enquanto os dispositivos deles estão bloqueados.
 - * **Filtro de linguagem indecorosa da Siri:** Ativar o filtro de linguagem indecorosa da Siri. O padrão é restringir esse recurso, o que significa que nenhum filtro de linguagem indecorosa é usado.
Para obter mais informações sobre Siri e segurança, consulte [Políticas da Siri e de ditado](#).
 - **Instalação de aplicativos:** Permitir que os usuários instalem aplicativos. Para dispositivos iOS supervisionados.
 - **Permitir busca em segundo plano durante roaming:** permite que os dispositivos sincronizem automaticamente as contas de correio com o iCloud enquanto estiverem em roaming. Quando **O**, desativa as atividades de busca global em segundo plano quando um telefone iOS está em roaming. O padrão é **Ativado**.
- **Permitir aplicativos**
 - **iTunes Store:** Permitir que os usuários acessem a iTunes Store. Para dispositivos iOS supervisionados.
 - **Compras no aplicativo:** Permitir que os usuários façam compras no aplicativo.
 - * **Exigir senha do iTunes para compras:** Exigir uma senha para compras no aplicativo. O padrão é restringir esse recurso, o que significa que nenhuma senha é necessária para compras no aplicativo.
 - **Safari:** permitir que os usuários acessem o Safari. Para dispositivos iOS supervisionados.
 - * **Preenchimento automático:** Permitir que os usuários configurem o preenchimento automático de nomes de usuário e senhas no Safari.
 - * **Forçar aviso de fraude:** se essa configuração estiver ativada e os usuários visitarem um site de phishing suspeito, o Safari os alertará. O padrão é restringir esse recurso, o que significa que nenhum aviso é emitido.
 - * **Ativar JavaScript:** permitir a execução de JavaScript no Safari.
 - * **Bloquear pop-ups:** bloquear pop-ups durante a exibição de sites. O padrão é restringir esse recurso, o que significa que pop-ups não são bloqueados.
 - **Aceitar cookies:** definir a extensão da aceitação de cookies. Na lista, escolha uma opção para permitir ou restringir cookies. A opção padrão é **Sempre**, o que permite que todos os sites salvem cookies no Safari. Outras opções são **Somente site atual**, **Nunca** e **Somente dos sites visitados**.
 - **Rede - Permitir ações do iCloud**
 - **Documentos e dados do iCloud:** permitir que os usuários sincronizem documentos e dados com o iCloud. Para dispositivos iOS supervisionados.
 - **Backup do iCloud:** permitir que os usuários façam backup dos dispositivos deles no iCloud.

- **Chaves do iCloud:** permitir que os usuários armazenem senhas, informações da rede Wi-Fi e informações de cartão de crédito, entre outras, em Chaves do iCloud.
- **Biblioteca de fotos na nuvem:** permitir que os usuários acessem suas respectivas bibliotecas de fotos do iCloud.

- **Segurança - Força**

O padrão é restringir os recursos a seguir, o que significa que nenhum dos recursos de segurança é ativado.

- **Backups criptografados:** forçar a criptografia dos backups no iCloud.
- **Rastreamento de anúncios limitado:** bloquear o acompanhamento de anúncios direcionados.
- **Código secreto no primeiro emparelhamento do AirPlay:** exigir que os dispositivos compatíveis com o AirPlay sejam verificados com um código de uso único na tela antes que possam usar o AirPlay.
- **Apple Watch emparelhado para usar detecção de pulso:** exigir que um Apple Watch emparelhado use a **Detecção de Pulso**.
- **Compartilhamento de documentos gerenciados com AirDrop:** definir essa opção como **Ativado** faz com que o AirDrop apareça como um destino não gerenciado.

- **Segurança - Permitir**

- **Aceitar certificados SSL não confiáveis:** permitir que os usuários aceitem certificados SSL não confiáveis de sites.
- **Atualização automática de definições de segurança do certificado:** permitir que certificados confiáveis sejam atualizados automaticamente.
- **Documentos de aplicativos gerenciados em aplicativos não gerenciados:** permitir que os usuários movam dados de aplicativos gerenciados (corporativos) para aplicativos não gerenciados (pessoais).
- **Documentos de aplicativos não gerenciados em aplicativos gerenciados:** permitir que os usuários movam dados de aplicativos não gerenciados (pessoais) para aplicativos não gerenciados (corporativos).
- **Envio de informações de diagnóstico para a Apple:** permitir que dados de diagnóstico anônimos sobre os dispositivos dos usuários sejam enviados para a Apple.
- **Touch ID para desbloquear o dispositivo:** permitir que os usuários usem as impressões digitais deles para desbloquear os respectivos dispositivos.
- **Notificações do Passbook quando o dispositivo está bloqueado:** permitir que notificações do Passbook apareçam na tela de bloqueio.
- **Handoff:** permitir que os usuários transfiram as atividades de um dispositivo iOS para outro dispositivo iOS próximo.
- **Sincronização do iCloud para aplicativos gerenciados:** permitir que os usuários sincronizem aplicativos gerenciados com o iCloud.

- **Backup para livros da empresa:** permitir o backup de livros da empresa para o iCloud.
 - **Sincronização de notas e destaques para livros da empresa:** permitir que as notas e os destaques que os usuários adicionaram aos livros da empresa sejam sincronizados com o iCloud.
 - **Confiança de aplicativo empresarial:** permitir que aplicativos empresariais sejam confiáveis. Aplicativos empresariais são todos os aplicativos personalizados para sua organização. Eles podem ser feitos internamente ou podem ser desenvolvidos e comprados de um fornecedor externo. Para obter informações adicionais, consulte [Instalar aplicativos empresariais personalizados no iOS](#).
 - **Resultados de Internet no Spotlight:** permitir que o Spotlight mostre os resultados da pesquisa da Internet, bem como do dispositivo.
 - **Aplicativos não gerenciados leem contatos gerenciados:** Opcional. Disponível somente se **Documentos de aplicativos gerenciados em aplicativos não gerenciados** estiver desativado. Se esta política estiver ativada, os aplicativos não gerenciados poderão ler dados dos contatos das contas gerenciadas. O padrão é **Desativado**. Disponível a partir do iOS 12.
 - **Aplicativos gerenciados gravam contatos não gerenciados:** Opcional. Se habilitado, permite que aplicativos gerenciados gravem contatos nos contatos de contas não gerenciadas. Se **Documentos de aplicativos gerenciados em aplicativos não gerenciados** estiver habilitado, essa restrição não terá efeito. O padrão é **Desativado**. Disponível a partir do iOS 12.
- **Apenas configurações supervisionadas - Permitir**

Estas configurações se aplicam somente a dispositivos supervisionados. Para conhecer as etapas para configurar um dispositivo iOS para o modo supervisionado, consulte [Para colocar um dispositivo iOS no modo Supervisionado usando o Apple Configurator](#).

- **Apagar todo o conteúdo e configurações:** permitir que os usuários apaguem todo o conteúdo e as configurações dos dispositivos deles.
- **Configuração de restrições:** permitir que os usuários configurem os controles dos pais nos dispositivos deles.
- **Podcasts:** permitir que os usuários baixem e sincronizem podcasts.
- **Instalação de perfis de configuração:** permitir que os usuários instalem um perfil de configuração diferente daquele implantado por você.
- **Modificação de impressão digital:** permitir que os usuários alterem ou apaguem a impressão digital Touch ID deles.
- **Instalação de aplicativos do dispositivo:** permitir que os usuários instalem aplicativos. Desabilitar essa configuração impede que os usuários finais instalem novos aplicativos. A App Store é desativada e seu ícone é removido da tela inicial.

- **Atalhos de teclado:** permitir que os usuários criem atalhos de teclado personalizados para palavras ou frases que usam com frequência.
- **Apple Watch pareado:** permitir que os usuários emparelhem um Apple Watch com um dispositivo supervisionado.
- **Modificação de código secreto:** permitir que os usuários alterem a senha em um dispositivo supervisionado.
- **Modificação do nome do dispositivo:** permitir que os usuários alterem o nome do seu dispositivo.
- **Modificação do papel de parede:** permitir que os usuários alterem o papel de parede nos dispositivos deles.
- **Download automático de aplicativos:** permitir que aplicativos sejam baixados.
- **AirDrop:** permitir que os usuários compartilhem fotos, vídeos, sites, locais e mais com dispositivos iOS próximos.
- **iMessage:** permitir que os usuários enviem mensagens de texto sobre WiFi usando o iMessage.
- **Conteúdo gerado pelo usuário de Siri:** permitir que a Siri consulte conteúdo gerado pelo usuário na Web. Os consumidores, e não os jornalistas tradicionais; produzem conteúdo gerado pelo usuário. Por exemplo, o conteúdo encontrado no Twitter ou no Facebook é gerado pelo usuário.
- **iBooks:** permitir que os usuários usem o aplicativo iBooks.
- **Remoção de aplicativos:** permitir que usuários removam aplicativos dos dispositivos deles.
- **Game Center:** permitir que os usuários joguem jogos online usando o Game Center nos dispositivos deles.
 - * **Adicionar amigos:** Permitir que os usuários enviem uma notificação a um amigo para jogar um jogo.
 - * **Jogos multiplayer:** permitir que os usuários iniciem jogos multiplayer nos dispositivos deles.
- **Modificando configurações de conta:** permitir que os usuários modifiquem as configurações de conta do respectivo dispositivo.
- **Modificando configurações de dados celulares do aplicativo:** permitir que os usuários modifiquem a forma como os aplicativos usam dados celulares.
- **Modificando configurações de Encontrar Meus Amigos:** permitir que os usuários alterem as respectivas configurações de Encontrar Meus Amigos.

- **Emparelhamento com hosts não Configurator:** permitir que o administrador controle a quais dispositivos o dispositivo de um usuário pode ser emparelhado. Desativar essa configuração impede o emparelhamento, exceto com o host de supervisão que executa o Apple Configurator. Se nenhum certificado de host de supervisão estiver configurado, todo o emparelhamento será desativado.
- **Teclados intuitivos:** permitir que os dispositivos dos usuários usem teclados intuitivos para sugerir palavras conforme eles digitam. Desative essa opção em situações como durante a administração de testes padronizados testes, nas quais você não deseja que os usuários tenham acesso a palavras sugeridas.
- **Teclado com correção automática:** permitir que os dispositivos dos usuários usem o teclado com correção automática. Desative essa opção em situações como durante a administração de testes padronizados testes, nas quais você não deseja que os usuários tenham acesso à correção automática.
- **Teclado com corretor ortográfico:** permitir que os dispositivos dos usuários usem o corretor ortográfico enquanto digitam. Desative essa opção em situações como durante a administração de testes padronizados testes, nas quais você não deseja que os usuários tenham acesso ao corretor ortográfico.
- **Pesquisa de definições:** permitir que os dispositivos dos usuários usem a pesquisa de definições durante a digitação. Desative essa opção em situações como durante a administração de testes padronizados testes, nas quais você não deseja que os usuários consigam pesquisar definições conforme digitam.
- **ID de pacote único de aplicativos:** criar uma lista de aplicativos que têm permissão para manter o controle sobre o dispositivo e impedir a interação com os outros aplicativos ou funções.
Para adicionar um aplicativo, clique em **Adicionar**, digite um **nome de aplicativo** e clique em **Salvar**. Repita esse processo para cada aplicativo que você desejar adicionar.
- **News:** permitir que os usuários usem o aplicativo News.
- **Serviço Apple Music:** permitir que os usuários usem o serviço Apple Music. Se você não permitir o serviço Apple Music, o aplicativo Música será executado no modo clássica.
- **iTunes Radio:** permitir que os usuários usem o iTunes Radio.
- **Modificação de notificações:** permitir que os usuários modifiquem configurações de notificação.
- **Uso de aplicativos restritos:** permitir que os usuários usem todos os aplicativos ou usem ou não aplicativos com base nos IDs de pacote que você fornecer. Aplica-se somente a dispositivos supervisionados. Se você selecionar **Permitir apenas alguns aplicativos**, adicione um aplicativo com o ID de pacote `com.apple.webapp` para permitir clips web.

Nota:

Apartir do iOS 11, a Apple introduziu alterações nas políticas que estão disponíveis para restrições de aplicativos. A Apple não permite mais remover o acesso ao aplicativo Configurações e ao aplicativo Telefone restringindo o pacote de aplicativos iOS apropriado.

Depois de configurar a política de dispositivo de restrições para bloquear alguns aplicativos e, em seguida, implantar a política: se mais tarde você desejar permitir alguns ou todos os aplicativos, a alteração e implantação da política de dispositivo de restrições não alteram as restrições. Nesse caso, o iOS não aplica as alterações ao perfil de iOS. Para continuar, use a política de remoção de perfil para remover o perfil de iOS e, em seguida, implantar a política de dispositivo de restrições atualizada.

Se você alterar essa configuração para **Permitir apenas alguns aplicativos**: antes de implantar essa política, informe os usuários de dispositivos registrados usando o Programa de Implantação da Apple para fazer login em suas contas Apple no Assistente de Instalação. Caso contrário, os usuários podem ter que desativar a autenticação de dois fatores em seus dispositivos para entrar em suas contas da Apple e acessar os aplicativos permitidos.

- **Modificação de submissão de diagnóstico:** permitir que os usuários modifiquem o envio de diagnóstico de aplicativo e configurações de análise no painel **Ajustes > Diagnóstico e Uso**.
- **Modificação de Bluetooth:** permitir que os usuários modifiquem configurações de Bluetooth.
- **Permitir ditado:** supervisionado somente. Se essa restrição for definida como **Desativado**, a entrada de ditado não será permitida, incluindo fala para texto. A configuração padrão é **Ativado**.
- **Entrar somente em redes WiFi instaladas por uma política de WiFi:** opcional Apenas supervisionado. Se esta restrição estiver definida como **Ativado**, o dispositivo pode se juntar a redes Wi-Fi somente quando elas tiverem sido configuradas através de um perfil de configuração. O padrão é **Desativado**.
- **Permitir que o aplicativo Sala de Aula execute o AirPlay e Exibir Tela sem solicitar:** se essa restrição estiver marcada, o instrutor pode executar o AirPlay e exibir a tela no dispositivo de um aluno sem pedir permissão. O padrão é desmarcado. Para dispositivos iOS supervisionados.
- **Permitir que o aplicativo Sala de Aula bloqueie um aplicativo e bloqueie o dispositivo sem solicitar:** se essa restrição estiver definida como **Ativado**, o aplicativo Sala de Aula bloqueará automaticamente os dispositivos do usuário a um aplicativo e bloqueará

o dispositivo sem avisar os usuários. O padrão é **Desativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).

- **Associar automaticamente às classes do aplicativo Sala de Aula sem solicitar:** se essa restrição estiver definida como **Ativado**, o aplicativo Sala de Sula associará automaticamente os usuários às classes, sem avisar os usuários. O padrão é **Desativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
- **Permitir AirPrint:** se essa restrição estiver definida como **Desativado**, os usuários não poderão imprimir com o AirPrint. A configuração padrão é **Ativado**. Quando essa restrição está **Ativada**, estas restrições extras são exibidas. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
 - * **Permitir o armazenamento de credenciais do AirPrint em Chaves:** se essa restrição não estiver selecionada, o nome de usuário e a senha do AirPrint não serão armazenados em Chaves. A configuração padrão é selecionada. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
 - * **Permitir a descoberta de impressoras AirPrint usando iBeacons:** se essa restrição não estiver selecionada, a descoberta do iBeacon de impressoras AirPrint será desativada. Isso evita que sinalizadores falsos do AirPrint Bluetooth causem phishing no tráfego da rede. A configuração padrão é selecionada. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
 - * **Permitir AirPrint apenas para destinos com certificados confiáveis:** se essa restrição for selecionada, os usuários poderão usar o AirPrint para imprimir apenas em destinos com certificados confiáveis. O padrão é desmarcado. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
- **Adicionar configurações de VPN:** se essa restrição estiver definida como **Desativado**, os usuários não poderão criar configurações de VPN. A configuração padrão é **Ativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
- **Modificar as configurações do plano de celular:** se essa restrição estiver definida como **Desativado**, os usuários não poderão modificar as configurações do plano de celular. A configuração padrão é **Ativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
- **Remover aplicativos do sistema:** se essa restrição estiver definida como **Desativado**, os usuários não poderão remover aplicativos de sistema de seus dispositivos. A configuração padrão é **Ativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).
- **Configurando novos dispositivos próximos:** se essa restrição estiver definida como **Desativado**, os usuários não poderão configurar novos dispositivos próximos. A configuração padrão é **Ativado**. Para dispositivos supervisionados executando o iOS 11 (versão mínima).

ima).

- **Permitir modo restrito de USB:** se **Desativado**, o dispositivo sempre poderá se conectar a acessórios USB enquanto estiver bloqueado. O padrão é **Ativado**. Disponível somente para dispositivos supervisionados iOS 11.3 e de versões posteriores.
 - **Forçar atualizações de software atrasadas:** se **Ativado**, adiará a visibilidade do usuário das Atualizações de Software. Com essa restrição em vigor, o usuário não vê uma atualização de software até que o número especificado de dias após a data de lançamento da atualização de software tenha passado. O padrão é **Desativado**. Disponível somente para dispositivos supervisionados iOS 11.3 e de versões posteriores.
 - **Atraso forçado de atualização de software (dias):** permite especificar um número de dias para adiar uma atualização de software no dispositivo. O atraso máximo é de **90** dias. O padrão é **30** dias. Disponível somente para dispositivos supervisionados iOS 11.3 e de versões posteriores.
 - **Forçar solicitação de permissão de sala de aula para sair das aulas:** se **Ativado**, um aluno matriculado em um curso não gerenciado com Sala de aula deve solicitar permissão do professor quando tentar sair do curso. O padrão é **Desativado**. Disponível somente para dispositivos supervisionados iOS 11.3 e de versões posteriores.
 - **Forçar data e hora automáticas:** permite que você defina automaticamente a data e a hora em dispositivos supervisionados. Se **Ativado**, os usuários do dispositivo não poderão desativar **Definir automaticamente em Geral > Data e hora**. O fuso horário no dispositivo é atualizado somente quando o dispositivo pode determinar sua localização. Ou seja, quando um dispositivo tem uma conexão celular ou uma conexão Wi-Fi com serviços de localização habilitados. O padrão é **Desativado**. Disponível somente para dispositivos supervisionados iOS 12 e de versões posteriores.
 - **Preenchimento automático da senha:** opcional. Se desativado, os usuários não poderão usar os recursos Senhas de Preenchimento automático ou Senhas de segurança automáticas. O padrão é **Ativado**. Disponível a partir do iOS 12.
 - **Solicitações de proximidade de senha:** opcional. Se desativado, os dispositivos dos usuários não solicitam senhas de dispositivos próximos. O padrão é **Ativado**. Disponível a partir do iOS 12.
 - **Compartilhamento de senha:** opcional. Se desativado, os usuários não poderão compartilhar suas senhas usando o recurso AirDrop Passwords. O padrão é **Ativado**. Disponível a partir do iOS 12.
- **Segurança - Mostrar na tela de bloqueio**
 - **Centro de Controle:** permitir o acesso ao Centro de Controle na tela de bloqueio. Centro de controle permite que os usuários modifiquem facilmente as configurações de Modo

avião, Wi-Fi, Bluetooth, Modo não perturbe e Bloquear rotação.

- **Notificação:** permitir notificações na tela de bloqueio.
- **Exibição de hoje:** permitir a Exibição de Hoje, que agrega informações como a previsão do tempo e os itens de calendário do dia atual, na tela de bloqueio.

- **Conteúdo de mídia - Permitir**

- **Música, podcasts e material do iTunes U explícitos:** permitir material explícito nos dispositivos dos usuários.
- **Conteúdo sexual explícito em iBooks:** permitir que material explícito seja baixado do iBooks.
- **Região de classificações:** definir a região da qual as classificações de controles dos pais são obtidas. Na lista, clique em um país para definir a região das classificações. O padrão é **Estados Unidos**.
- **Filmes:** definir se filmes são permitidos nos dispositivos dos usuários. Se filmes forem permitidos, como opção, defina o nível de classificação para filmes. Na lista, clique em uma opção para permitir ou restringir filmes no dispositivo. O padrão é Permitir todos os filmes.
- **Programas de TV:** definir se Programas de TV são permitidos nos dispositivos dos usuários. Se programas de TV forem permitidos, como opção, defina o nível de classificação dos programas de TV. Na lista, clique em uma opção para permitir ou restringir programas de TV no dispositivo. O padrão é Permitir todos os programas de TV.
- **Aplicativos:** definir se aplicativos são permitidos nos dispositivos dos usuários. Se aplicativos forem permitidos, como opção, defina o nível de classificação para aplicativos. Na lista, clique em uma opção para permitir ou restringir aplicativos no dispositivo. O padrão é Permitir todos os aplicativos.

- **Configurações de política**

- **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.
- **Escopo do perfil:** selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Esta opção está disponível apenas no iOS 9.3 e posterior.

Configurações do macOS

Restrictions Policy	Restrictions Policy
1 Policy Info	This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.
2 Platforms	Preferences
<input type="checkbox"/> iOS	Restrict items in System Preferences <input type="checkbox"/> OFF
<input checked="" type="checkbox"/> macOS	Apps
<input checked="" type="checkbox"/> Samsung SAFE	Allow use of Game Center <input checked="" type="checkbox"/> ON macOS 10.11+
<input checked="" type="checkbox"/> Samsung KNOX	Allow adding Game Center friends <input checked="" type="checkbox"/> ON
<input checked="" type="checkbox"/> Windows Phone	Allow multiplayer gaming <input checked="" type="checkbox"/> ON
<input checked="" type="checkbox"/> Windows Desktop/Tablet	Allow Game Center account modification <input checked="" type="checkbox"/> ON
<input checked="" type="checkbox"/> Amazon	Allow App Store adoption <input checked="" type="checkbox"/> ON
<input checked="" type="checkbox"/> Windows Mobile/CE	Allow Safari AutoFill <input checked="" type="checkbox"/> ON
3 Assignment	Require admin password to install or update apps <input type="checkbox"/> OFF
	Restrict App Store to software update only <input type="checkbox"/> OFF

- **Preferências**

- **Restringir itens nas preferências do sistema:** permitir ou restringir o acesso do usuário às Preferências do Sistema. O padrão é **O**, que permite aos usuários acesso completo às Preferências do sistema. Se essa opção estiver ativada, defina as seguintes configurações.

- * **Painel de preferências do sistema:** selecionar se as configurações selecionadas são ativadas ou desativadas. O padrão é ativar todas as configurações, que são **I** por padrão.

- Usuários e Grupos
 - Geral
 - Acessibilidade
 - App Store
 - Atualização de Software
 - Bluetooth
 - CDs e DVDs
 - Data e Hora
 - Área de Trabalho e Protetor de Tela
 - Monitores
 - Dock
 - Economia de Energia
 - Extensões
 - FibreChannel
 - iCloud
 - Tinta
 - Contas da Internet
 - Teclado

- Idioma e Texto
- Mission Control
- Mouse
- Rede
- Notificações
- Controles dos Pais
- Impressoras e Scanners
- Perfis
- Segurança e Privacidade
- Compartilhamento
- Som
- Dicción e Fala
- Spotlight
- Disco de Inicialização
- Time Machine
- Trackpad
- Xsan

- **Aplicativos**

- **Permitir o uso do Game Center:** permitir que os usuários joguem jogos online usando o Game Center. O padrão é **On**.
- **Permitir a adição de amigos do Game Center:** permitir que os usuários enviem uma notificação a um amigo para jogar um jogo. O padrão é **On**.
- **Permitir jogos multiplayer:** permitir que os usuários iniciem jogos multiplayer. O padrão é **On**.
- **Permitir modificação de conta do Game Center:** permitir que os usuários modifiquem as próprias configurações de conta do Game Center. O padrão é **On**.
- **Permitir adoção da App Store:** permitir ou restringir que a App Store adote aplicativos que existiam previamente no OS X. O padrão é **Ativado**.
- **Permitir preenchimento automático do Safari:** permitir que o Safari preencha automaticamente campos em sites com senhas, endereços e outras informações básicas que ele armazena. O padrão é **On**.
- **Exigir uma senha para instalar ou atualizar aplicativos:** exigir uma senha de administrador para instalar ou atualizar aplicativos. O padrão é **Off**, o que significa que nenhuma senha de administrador é necessária.
- **Restringir a App Store somente à atualização de software:** restringir a App Store somente a atualizações, o que desativa todas as guias na App Store, exceto as atualizações. O padrão é **Off**, que permite total acesso à App Store.
- **Restringir os aplicativos que podem ser abertos:** restringir ou permitir os aplicativos que os usuários podem usar. O padrão é **O**, o que permite que todos os aplicativos sejam

usados. Se essa opção estiver ativada, defina as seguintes configurações:

- * **Aplicativos permitidos:** clique em **Adicionar**, digite o nome e o ID do pacote de um aplicativo com permissão para iniciar e clique em **Salvar**. Repita essa etapa para cada aplicativo com permissão para iniciar.
- * **Pastas não permitidas:** clique em **Adicionar**, digite o caminho de arquivo para uma pasta à qual você deseja restringir o acesso do usuário (por exemplo, /Application-s/Utilities) e clique em **Salvar**. Repita essa etapa para todas as pastas que você não deseja que os usuários possam acessar.
- * **Pastas permitidas:** clique em **Adicionar**, digite o caminho de arquivo para uma pasta à qual você deseja conceder o acesso do usuário e clique em **Salvar**. Repita essa etapa para todas as pastas que você deseja que os usuários possam acessar.

- **Widgets**

- **Permitir que apenas os seguintes widgets do painel sejam executados:** permitir ou restringir quais widgets do Painel, como Relógio ou Calculadora, os usuários têm permissão para executar. O padrão é **Off**, o que permite que os usuários executem todos os widgets. Se essa opção estiver ativada, defina a seguinte configuração:
 - * **Widgets permitidos:** clique em **Adicionar**, digite o nome e o ID de um widget que tem permissão de execução e clique em **Salvar**. Repita essa etapa para cada widget que você deseja executar no Painel.

- **Mídia**

- **Permitir AirDrop:** permitir que os usuários compartilhem fotos, vídeos, sites, locais e mais com dispositivos iOS próximos.

- **Compartilhamento**

- **Ativar automaticamente novos serviços de compartilhamento:** selecione se os serviços de compartilhamento devem ser ativados automaticamente.
- **Mail:** selecione se uma caixa de correio compartilhada é permitida.
- **Facebook:** selecione se uma conta compartilhada do Facebook é permitida.
- **Serviços de Vídeo - Flickr, Vimeo, Tudou e Youku:** selecione se os serviços de vídeo compartilhados são permitidos.
- **Adicionar ao Aperture:** selecione se a capacidade de adição compartilhada ao Aperture é permitida.
- **Sina Weibo:** selecione se uma conta compartilhada de microblogging do Sina Weibo é permitida.
- **Twitter:** selecione se uma conta compartilhada no Twitter é permitida.
- **Mensagens:** selecione se o acesso compartilhado a mensagens é permitido.
- **Adicionar ao iPhoto:** selecione se a capacidade de adição compartilhada ao iPhoto é permitida.
- **Adicionar à lista de leitura:** selecione se a capacidade de adição compartilhada à Lista de Leitura é permitida.

- **AirDrop:** selecione se uma conta compartilhada no AirDrop é permitida.

- **Funcionalidade**

- **Bloquear imagem da área de trabalho:** selecione se os usuários podem alterar a imagem da área de trabalho. O padrão é **Off**, o que significa que os usuários podem alterar a imagem da área de trabalho.
- **Permitir o uso da câmera:** selecione se os usuários podem usar a câmera nos Macs deles. O padrão é **Off**, o que significa que os usuários não podem usar a câmera.
- **Permitir Apple Music:** permitir que os usuários usem o serviço Apple Music (macOS 10.12 e versões posteriores). Se você não permitir o serviço Apple Music, o aplicativo Música será executado no modo clássica. Aplica-se somente a dispositivos supervisionados. O padrão é **Ativado**.
- **Permitir sugestões de Spotlight:** selecione se os usuários podem usar as Sugestões de Spotlight para pesquisar o respectivo Mac e para fornecer Sugestões de Spotlight da Internet, do iTunes e da App Store. O padrão é **Off**, o que impede que os usuários utilizem as Sugestões do Spotlight.
- **Permitir pesquisa:** selecione se os usuários podem pesquisar as definições de palavras usando o menu de contexto ou o menu de pesquisa do Spotlight. O padrão é **Off**, o que impede que os usuários usem a Pesquisa nos respectivos Macs.
- **Permitir o uso de senha do iCloud para contas locais:** selecione se os usuários podem usar o respectivo ID Apple e senha do iCloud para fazer logon nos Macs deles. Ativar essa política significa que os usuários usam apenas um ID e senha para *todas* as telas de login em seus Macs. O padrão é **On**, o que permite que os usuários usem o ID Apple e a senha do iCloud para acessar os Macs deles.
- **Permitir documentos e dados de iCloud:** selecione se os usuários têm permissão para acessar documentos e dados armazenados no iCloud nos Macs deles. O padrão é **Off**, o que impede que os usuários usem documentos e dados do iCloud nos Macs deles.
 - * **Permitir área de trabalho e documentos iCloud:** (macOS 10.12.4 e posterior) Seleccionada por padrão.
- **Permitir sincronização de chaves do iCloud:** permitir a sincronização de chaves do iCloud (macOS 10.12 e versões posteriores). O padrão é **On**.
- **Permitir Mail do iCloud:** permitir que os usuários usem o iCloud Mail (macOS 10.12 e versões posteriores). O padrão é **On**.
- **Permitir Contatos do iCloud:** permitir que os usuários usem os Contatos do iCloud (macOS 10.12 e versões posteriores). O padrão é **On**.
- **Permitir Calendários do iCloud:** permitir que os usuários usem os Calendários do iCloud (macOS 10.12 e versões posteriores). O padrão é **On**.
- **Permitir Lembretes do iCloud:** permitir que os usuários usem os Lembretes do iCloud (macOS 10.12 e versões posteriores). O padrão é **On**.
- **Permitir Favoritos do iCloud:** permitir que os usuários sincronizem com os Favoritos do

iCloud (macOS 10.12 e versões posteriores). O padrão é **On**.

- **Permitir Notas do iCloud:** permitir que os usuários usem as Notas do iCloud (macOS 10.12 e versões posteriores). O padrão é **On**.
- **Permitir Fotos do iCloud:** se você alterar essa configuração para **Off**, as fotos não baixadas totalmente da biblioteca de fotos do iCloud serão removidas do armazenamento do dispositivo local (macOS 10.12 e posterior). O padrão é **On**.
- **Permitir desbloqueio automático:** para obter informações sobre essa opção e o Apple Watch, consulte <https://www.imore.com/auto-unlock> (macOS 10.12 e posterior). O padrão é **On**.
- **Permitir Touch ID para desbloquear Mac:** (macOS 10.12.4 e posterior). O padrão é **On**.
- **Forçar atualizações de software atrasadas:** se **Ativado**, esta configuração adiará a visibilidade do usuário das Atualizações de Software. Os usuários não veem uma atualização de software até que o número especificado de dias após a data de lançamento da atualização de software tenha passado. O padrão é **Desativado**. Disponível apenas para dispositivos supervisionados que executam o macOS 10.13.4 e posterior.
- **Atraso forçado de atualização de software (dias):** especifica quantos dias adiar uma atualização de software no dispositivo. O máximo é 90 dias. O padrão é **30**. Disponível apenas para dispositivos supervisionados que executam o macOS 10.13.4 e posterior.
- **Preenchimento automático da senha:** opcional. Se desativado, os usuários não poderão usar os recursos Senhas de Preenchimento automático ou Senhas de segurança automáticas. O padrão é **Ativado**. Disponível a partir do macOS 10.14.
- **Solicitações de proximidade de senha:** opcional. Se desativado, os dispositivos dos usuários não solicitam senhas de dispositivos próximos. O padrão é **Ativado**. Disponível a partir do macOS 10.14.
- **Compartilhamento de senha:** opcional. Se desativado, os usuários não poderão compartilhar suas senhas usando o recurso Airdrop Passwords. O padrão é **Ativado**. Disponível a partir do macOS 10.14.

Configurações do Android

- **Câmera:** permitir que os usuários usem a câmera nos dispositivos deles. Se o valor for **Off**, a câmera está desabilitada. O padrão é **Ativado**.

Configurações do Android Enterprise

Restrictions Policy	Restrictions Policy
1 Policy Info	This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.
2 Platforms	Apply to fully managed devices with a work profile <input type="checkbox"/> OFF
<input checked="" type="checkbox"/> iOS	Allow USB actions
<input checked="" type="checkbox"/> macOS	Debugging <input type="checkbox"/> OFF
<input checked="" type="checkbox"/> Android (legacy DA)	File transfer <input type="checkbox"/> OFF
<input checked="" type="checkbox"/> Android Enterprise	Network
<input checked="" type="checkbox"/> Samsung SAFE	Allow VPN Configuration <input checked="" type="checkbox"/> ON ?
<input checked="" type="checkbox"/> Samsung KNOX	Android beam <input checked="" type="checkbox"/> ON ?
<input checked="" type="checkbox"/> Windows Phone	Allow configuring location provider <input checked="" type="checkbox"/> ON ?
<input checked="" type="checkbox"/> Windows Desktop/Tablet	Security
<input checked="" type="checkbox"/> Amazon	Allow use of the status bar <input type="checkbox"/> OFF ?
<input checked="" type="checkbox"/> Windows Mobile/CE	Keep the keyguard from locking the device <input type="checkbox"/> OFF ?
3 Assignment	Don't allow printing <input type="checkbox"/> OFF ?
	Allow Account Management <input type="checkbox"/> OFF ?
	Allow cross profile copy and paste <input type="checkbox"/> OFF ?
	Allow location sharing <input type="checkbox"/> OFF ?
	Allow Non-Google Play apps <input type="checkbox"/> OFF ?
	Allow screen capture <input type="checkbox"/> OFF ?
	Allow use of camera <input type="checkbox"/> OFF ?

Por padrão, as configurações de **Depuração de USB e Fontes desconhecidas** são desativadas em um dispositivo quando ele é registrado no Android Enterprise no modo de perfil de trabalho.

Nos dispositivos com Android 8.0 ou posterior e Samsung Knox 3.0 e posterior, defina as configurações para Samsung Knox e Samsung SAFE na página **Android Enterprise**. Nos dispositivos que executam versões anteriores do Android ou Samsung Knox, utilize as páginas **Samsung Knox** e **Samsung SAFE**.

A Citrix recomenda que você use o Samsung Knox 3.4 ou superior para os recursos de gerenciamento mais recentes do Samsung Knox.

- **Aplicar a dispositivos totalmente gerenciados com um perfil de trabalho:** permite que as

definições de política de restrições sejam configuradas para dispositivos totalmente gerenciados com perfis de trabalho. Quando essa configuração estiver **Ativada**, selecione uma das seguintes configurações:

- **Perfil de trabalho:** as configurações de restrições que você configura se aplicam apenas ao perfil de trabalho no dispositivo.
- **Gerenciar dispositivo:** as configurações de restrições que você configura se aplicam somente ao dispositivo.

Quando essa configuração estiver **Desativada**, as configurações de credenciais configuradas se aplicam ao dispositivo, exceto as configurações que se aplicam explicitamente ao perfil de trabalho. O padrão é **Desativado**.

Quando **Aplicar a dispositivos totalmente gerenciados com um perfil de trabalho** estiver desativado, defina estas configurações:

- **Permitir ações de USB**

- **Depuração:** permite a depuração por USB. O padrão é **Desativado**.
- **Transferência de arquivos:** permite a transferência de arquivos por USB. O padrão é **Desativado**.

- **Rede**

- **Permitir configuração de VPN:** permite que os usuários criem configurações de VPN. Para dispositivos de perfil de trabalho com Android 6 e posterior e para dispositivos totalmente gerenciados. O padrão é **Ativado**.
- **Android Beam:** permitir que os usuários enviem páginas da Web, imagens, vídeos ou outros conteúdos dos dispositivos deles para outro dispositivo usando NFC (comunicação a curta distância). Para MDM 4.0 e posterior. Padrão se **Ativado**.
- **Permitir configuração do provedor de localização:** permite que os usuários ativem o GPS em seus dispositivos. Para Android API 28 e posterior. O padrão é **Ativado**.
- **Permitir compartilhamento de localização:** permite o compartilhamento de localização. Nos perfis gerenciados, o proprietário do dispositivo pode substituir essa configuração. O padrão é **Desativado**.

Dica:

Você pode criar políticas de dispositivo de Localização no XenMobile para impor fronteiras geográficas. Consulte [Política de dispositivo de localização](#).

- **Segurança**

- **Permitir o uso da barra de status:** se definido como **Ativado**, essa configuração habilita a barra de status em dispositivos gerenciados e em dispositivos dedicados (também conhecidos como dispositivos COSU). Isso desabilita notificações, configurações rápidas e

outras sobreposições de tela que permitem escapar do modo de tela inteira. Os usuários podem acessar as configurações do sistema e ver as notificações. Para Android 6.0 e posterior. O padrão é **Desativado**.

- **Impedir que o Keyguard bloqueie o dispositivo:** se definido como **Ativado**, essa configuração desabilita o Keyguard na tela de bloqueio em dispositivos gerenciados e dispositivos dedicados (também conhecidos como dispositivos COSU). O padrão é **Desativado**.
- **Não permitir impressão:** se **Ativado**, a configuração impede que os usuários imprimam em qualquer impressora acessível a partir do dispositivo do usuário. O padrão é **Off**. Disponível para: Android 9 e posterior.
- **Permitir gerenciamento de conta:** permite que a conta seja adicionada no perfil de trabalho e em dispositivos gerenciados. O padrão é **Desativado**.
- **Allow cross profile copy and paste:** permite ou impede o uso da área de transferência para copiar e colar entre aplicativos no perfil do Android Enterprise e aplicativos na área pessoal. O padrão é **Desativado**.
- **Permitir compartilhamento de localização:** permite o compartilhamento de localização. Nos perfis gerenciados, o proprietário do dispositivo pode substituir essa configuração. O padrão é **Desativado**.
- **Permitir aplicativos não Google Play:** permite a instalação de aplicativos de outras lojas diferentes da Google Play. O padrão é **Desativado**.
- **Permitir captura de tela:** permite que os usuários gravem ou façam uma captura da tela do dispositivo. O padrão é **Desativado**.
- **Permitir o uso da câmera:** permite que os usuários tirem fotos e façam vídeos com a câmera do dispositivo. O padrão é **Desativado**.
- **Permitir o controle do usuário das configurações do aplicativo:** permite que os usuários desinstalem aplicativos, desativem aplicativos, limpem o cache e os dados, forcem a interrupção de qualquer aplicativo e cancelem os padrões. O padrão é **Desativado**.
- **Permitir widgets de aplicativo de perfil de trabalho na tela inicial:** se essa configuração estiver **Ativada**, os usuários podem colocar widgets de aplicativos de perfil de trabalho na tela inicial do dispositivo. Se essa configuração for **Desativado**, os usuários não podem colocar widgets de aplicativo de perfil de trabalho na tela inicial do dispositivo. O padrão é **Desativado**.
 - * **Aplicativos cujos widgets serão permitidos:** uma lista dos aplicativos que você deseja permitir na tela inicial. Defina **Permitir widgets de aplicativo de perfil profissional na tela inicial** como **Ativado** e adicione o aplicativo. Clique em **Adicionar** e selecione um aplicativo cujos widgets você deseja permitir na lista na tela inicial. Clique em **Save**. Repita esse processo para permitir mais widgets de aplicativos.
- **Permitir contatos do perfil profissional nos contatos do dispositivo:** mostra contatos do perfil gerenciado do Android Enterprise no perfil pai, para chamadas recebidas (An-

droid 7.0 e posterior). O padrão é **Desativado**.

- **Ativar aplicativos do sistema:** permite que os usuários executem aplicativos de dispositivo pré-instalados. O padrão é **Desativado**. Para habilitar aplicativos específicos, clique em **Adicionar** na tabela **Lista de aplicativos do sistema**.

- * **Lista de aplicativos do sistema:** Uma lista dos aplicativos do sistema que você deseja ativar no dispositivo. Defina **Ativar aplicativos do sistema** como **Ativado** e adicione o nome do pacote do aplicativo. Para procurar o nome do pacote de um aplicativo do sistema, você pode usar o Android Debug Bridge (adb) para chamar o comando gerenciador de pacotes (pm) do Android. Por exemplo, `adb shell "pm list packages -f name"`, onde "name" é parte do nome do pacote. Para obter mais informações, consulte <https://developer.android.com/studio/command-line/adb>. Para dispositivos Android Enterprise, você pode restringir as permissões de aplicativos usando a [política de configurações gerenciadas do Android Enterprise](#).

- **Desativar aplicativos:** Impede que uma lista especificada de aplicativos seja executada nos dispositivos. O padrão é **Desativado**. Para desabilitar um aplicativo instalado, altere a configuração para **Ativado** e clique em **Adicionar** na tabela **Lista de Aplicativos**.

- * **Lista de aplicativos:** uma lista dos aplicativos que você deseja bloquear. Defina **Desativar aplicativos** como **Ativado** e adicione o aplicativo. Digite o nome do pacote do aplicativo. Alterar e implantar uma lista de aplicativos sobrescreve a lista de aplicativos anterior. Por exemplo: se você desativar com.example1 e com.example2 e, posteriormente, alterar a lista para com.example1 e com.example3, o XenMobile habilitará com.example.2.

- **Ativar verificação de aplicativo:** permite que o sistema operacional verifique os aplicativos para detectar comportamentos mal-intencionados. O padrão é **Ativado**.
- **Ativar Google Apps:** permite que os usuários baixem aplicativos do Google Mobile Services para o dispositivo. O padrão é **Ativado**.
- **Permitir que o usuário configure as credenciais do usuário:** especifique se os usuários podem configurar credenciais no armazenamento de keystore gerenciado. O padrão é **Ativado**.

- **Dispositivo totalmente gerenciado.**

- **Permitir vários usuários:** permite que vários usuários usem um dispositivo (MDM 4.0 e posterior). O padrão é **Ativado**.
- **Permitir roaming:** permite que os usuários usem dados celulares enquanto estiverem em roaming. O padrão é O, que desativa o roaming nos dispositivos dos usuários. O padrão é **Desativado**. Quando essa definição está ativada, estas configurações estão disponíveis para dispositivos Samsung SAFE:
 - * **Dados:** permitir que os usuários usem dados celulares para dados.
 - * **Push:** permitir que os usuários usem dados celulares para envio.

- * **Sincronização:** permite que os usuários usem dados celulares para sincronização.
 - * **Chamadas de voz:** permite que os usuários usem dados celulares para chamadas de voz.
 - **Permitir SMS:** permite que os usuários enviem e recebam mensagens SMS. O padrão é **Desativado**.
 - **Backup:** permite que os usuários façam backup de aplicativos e dados do sistema em seus dispositivos. O padrão é **Ativado**.
 - **Bluetooth:** permite que os usuários usem Bluetooth. O padrão é **Ativado**.
 - **Alteração de data e hora:** permite que os usuários alterem a data e hora em seus dispositivos. O padrão é **Ativado**.
 - **Redefinição de fábrica:** permite que os usuários realizem uma redefinição de fábrica em seus dispositivos. O padrão é **Ativado**.
 - **Armazenamento em massa:** permite a transferência de grandes arquivos de dados entre os dispositivos dos usuários e um computador por uma conexão USB. O padrão é **Ativado**.
 - **Microfone:** permite que os usuários usem o microfone em seus dispositivos. O padrão é **Ativado**.
 - **Tethering:** permite que os usuários configurem hotspots portáteis e vinculem dados. O padrão é **Desativado**. Quando essa definição está ativada, estas configurações estão disponíveis para dispositivos Samsung:
 - * **USB:** permite que os usuários compartilhem uma conexão de dados móvel com outro dispositivo usando as suas conexões USB.
 - * **Bluetooth:** permite que os usuários compartilhem uma conexão de dados móvel com outro dispositivo usando as suas conexões Bluetooth.
 - * **Wi-Fi:** permite que os usuários compartilhem uma conexão de dados móvel com outro dispositivo usando as suas conexões Wi-Fi.
 - **Wi-Fi:** permite que usuários se conectem a redes Wi-Fi. O padrão é **Ativado**. Quando essa definição está ativada, estas configurações estão disponíveis:
 - * **Direto:** permite que os usuários se conectem diretamente a outro dispositivo usando as suas conexões Wi-Fi. Apenas para dispositivos Samsung. Para MDM 4.0 e posterior.
 - * **Alteração de estado:** permite que os aplicativos alterem o estado da conectividade Wi-Fi.
- **Samsung SAFE: permite os controles de hardware**
 - **Ativar verificação de inicialização confiável ODE:** usar a verificação de inicialização confiável ODE para estabelecer uma cadeia de confiança do carregador de inicialização com a imagem do sistema. O padrão é **Ativado**.
 - **Permitir apenas chamadas de emergência:** permite que os usuários ativem o modo Somente chamadas de emergência em seus dispositivos. O padrão é **Desativado**.
 - **Permitir recuperação de firmware:** permite que os usuários recuperem o firmware em seus dispositivos. O padrão é **Ativado**.

- **Permitir criptografia rápida:** permite a criptografia somente do espaço de memória usado. Isso contrasta com a criptografia completa de disco, que criptografa todos os dados, incluindo configurações, dados de aplicativo, arquivos baixados e aplicativos, mídia e outros arquivos. O padrão é **Ativado**.
- **Modo de critérios comuns:** coloca o dispositivo no modo de critérios comuns. A configuração Critérios Comuns impõe processos de segurança rigorosos. O padrão é **Ativado**.
- **Faixa de inicialização DOD:** exibe uma mensagem ou uma faixa de mensagem de notificação de uso do sistema aprovado para DoD quando os dispositivos dos usuários são reiniciados. O padrão é **Desativado**.
- **Alterações de configurações:** permite que os usuários alterem as configurações em seus dispositivos totalmente gerenciados. O padrão é **Ativado**.
- **Atualização por rede celular:** permite que os dispositivos dos usuários recebam atualizações de software sem fio (MDM 3.0 e versões posteriores). O padrão é **Ativado**.
- **Dados de segundo plano:** permite que aplicativos sincronizem dados em segundo plano para dispositivos totalmente gerenciados. O padrão é **Ativado**.
- **Área de transferência:** permitir que os usuários copiem dados para a área de transferência nos dispositivos deles.
 - * **Compartilhamento de área de transferência:** permitir que os usuários compartilhem conteúdo da área de transferência entre os respectivos dispositivos e um computador (MDM 4.0 e versões posteriores).
- **Tecla Home:** permite que os usuários usem a tecla **Home** em seus dispositivos totalmente gerenciados. O padrão é **Ativado**.
- **Localização fictícia:** permite que os usuários usem localizações de GPS fictícias. Para dispositivos totalmente gerenciados. O padrão é **Ativado**.
- **NFC:** permite que os usuários usem NFC em seus dispositivos totalmente gerenciados (MDM 3.0 e posterior). O padrão é **Ativado**.
- **Desligar:** permite que os usuários desliguem seus dispositivos totalmente gerenciados (MDM 3.0 e versões posteriores). O padrão é **Ativado**.
- **Cartão SD:** permite que os usuários usem um cartão SD, se disponível, com os seus dispositivos. O padrão é **Ativado**.
- **Discador de voz:** permite que os usuários usem o comunicador de voz em seus dispositivos (MDM 4.0 e versões posteriores). O padrão é **Ativado**.
- **Armazenamento em host:** permite que os dispositivos dos usuários ajam como o host USB quando um dispositivo USB é conectado a seus dispositivos. Em seguida, os dispositivos dos usuários fornecem energia ao dispositivo USB. O padrão é **Ativado**.
- **SBeam:** permite que os usuários compartilhem conteúdo com outras pessoas usando NFC e Wi-Fi Direct (MDM 4.0 e versões posteriores). O padrão é **Ativado**.
- **SVoice:** permite que os usuários usem o assistente pessoal inteligente e navegador de conhecimento em seus dispositivos (MDM 4.0 e versões posteriores). O padrão é **Ativado**.

- **Samsung SAFE: permitir aplicativos**
 - **Reconhecimento de face:** permite que os usuários usem o aplicativo de reconhecimento de face. O padrão é **Ativado**.
 - **Navegador:** permite que os usuários usem o navegador da Web. O padrão é **Ativado**.
 - **Youtube:** permite que os usuários acessem o YouTube. O padrão é **Ativado**.
 - **Google Play/Marketplace:** permite que os usuários acessem o Google Play e o Google Apps Marketplace. O padrão é **Ativado**.
 - **Forçar parada de aplicativos do sistema:** permite que os usuários desativem os aplicativos de sistema pré-instalados (MDM 4.0 e versões posteriores). O padrão é **Ativado**.

- **Samsung SAFE: Network**
 - **MMS de entrada:** permite que os usuários recebam mensagens MMS. O padrão é **Ativado**.
 - **MMS de saída:** permite que os usuários enviem mensagens MMS. O padrão é **Ativado**.
 - **SMS de entrada:** permite que os usuários recebam mensagens SMS. O padrão é **Ativado**.
 - **SMS de saída:** permite que os usuários enviem mensagens SMS. O padrão é **Ativado**.
 - **Configurar redes móveis:** permite que os usuários configurem redes móveis. O padrão é **Ativado**.
 - **Limite por dia (MB):** insira o número de MB de dados móveis que os usuários podem usar por dia. O padrão é 0, o que desativa esse recurso (MDM 4.0 e versões posteriores).
 - **Limite por semana (MB):** insira o número de MB de dados móveis que os usuários podem usar por semana. O padrão é 0, o que desativa esse recurso (MDM 4.0 e versões posteriores).
 - **Limite por mês (MB):** insira o número de MB de dados móveis que os usuários podem usar por mês. O padrão é 0, o que desativa esse recurso (MDM 4.0 e versões posteriores).
 - **Apenas conexões seguras:** permite que os usuários usem somente conexões seguras (MDM 4.0 e versões posteriores). O padrão é **Ativado**.
 - **Gravação de áudio:** permite que os usuários gravem áudio usando os seus dispositivos (MDM 4.0 e versões posteriores). O padrão é **Ativado**.
 - **Gravação de vídeo:** permite que os usuários gravem vídeo usando os seus dispositivos (MDM 4.0 e versões posteriores). O padrão é **Ativado**.

- **Samsung Knox**
 - **Ativar verificação de revogação:** ativa a verificação de certificados revogados. O padrão é **Ativado**.
 - **Mover aplicativos para o contêiner:** permite que os usuários movam aplicativos entre o contêiner Knox e a área pessoal em seus dispositivos. O padrão é **Ativado**.
 - **Impor a Autenticação Multifator:** os usuários devem usar uma impressão digital e outro método de autenticação, como senha ou PIN, para abrir os dispositivos deles. O padrão é **Ativado**.
 - **Ativar keystore TIMA:** o KeyStore TIMA fornece o armazenamento seguro de chaves

baseado em TrustZone para as chaves simétricas. Os pares de chaves e os certificados RSA são roteados para o provedor padrão de armazenamento de chaves para armazenamento. O padrão é **Ativado**.

- **Impor autenticação ao contêiner:** usar uma autenticação separada e diferente daquela usada para desbloquear o dispositivo abrir o contêiner Knox. O padrão é **Ativado**.
- **Lista de compartilhamento:** permite que os usuários compartilhem conteúdo entre aplicativos na lista Compartilhar Via. O padrão é **Ativado**.
- **Ativar Log de Auditoria:** permite a criação de logs de auditoria de eventos para análise forense de um dispositivo. O padrão é **Ativado**.
- **Usar Teclado Seguro:** força os usuários a usar um teclado seguro no contêiner Knox. O padrão é **Ativado**.
- **Autenticação do navegador com cartão inteligente:** ativa a autenticação de navegador nos dispositivos equipados com um leitor de cartão inteligente.

Quando **Aplicar a dispositivos totalmente gerenciados com um perfil de trabalho** estiver ativo e definido como **Perfil de trabalho**, defina estas configurações:

- **Rede**

- **Permitir configuração do provedor de localização:** permite que os usuários ativem o GPS em seus dispositivos. Para Android API 28 e posterior. O padrão é **Ativado**.

- **Segurança**

- **Não permitir impressão:** se **Ativado**, a configuração impede que os usuários imprimam em qualquer impressora acessível a partir do dispositivo do usuário. O padrão é **Off**. Disponível para: Android 9 e posterior.
- **Allow account management:** permite que a conta seja adicionada no perfil profissional e em dispositivos gerenciados. O padrão é **Desativado**.
- **Allow cross profile copy and paste:** permite ou impede o uso da área de transferência para copiar e colar entre aplicativos no perfil do Android Enterprise e aplicativos na área pessoal. O padrão é **Desativado**.
- **Permitir compartilhamento de localização:** permite o compartilhamento de localização. Nos perfis gerenciados, o proprietário do dispositivo pode substituir essa configuração. O padrão é **Desativado**.

Dica:

Você pode criar políticas de dispositivo de Localização no XenMobile para impor fronteiras geográficas. Consulte [Política de dispositivo de localização](#).

- **Permitir aplicativos não Google Play:** permite a instalação de aplicativos de outras lojas diferentes da Google Play. O padrão é **Desativado**.

- **Permitir captura de tela:** permite que os usuários gravem ou façam uma captura da tela do dispositivo. O padrão é **Desativado**.
- **Permitir o uso da câmera:** permite que os usuários tirem fotos e façam vídeos com a câmera do dispositivo. O padrão é **Desativado**.
- **Permitir o controle do usuário das configurações do aplicativo:** permite que os usuários desinstalem aplicativos, desativem aplicativos, limpem o cache e os dados, forcem a interrupção de qualquer aplicativo e cancelem os padrões. O padrão é **Desativado**.
- **Permitir widgets de aplicativo de perfil de trabalho na tela inicial:** se essa configuração estiver **Ativada**, os usuários podem colocar widgets de aplicativos de perfil de trabalho na tela inicial do dispositivo. Se essa configuração for **Desativado**, os usuários não podem colocar widgets de aplicativo de perfil de trabalho na tela inicial do dispositivo. O padrão é **Desativado**.
 - * **Aplicativos cujos widgets serão permitidos:** uma lista dos aplicativos que você deseja permitir na tela inicial. Defina **Permitir widgets de aplicativo de perfil profissional na tela inicial** como **Ativado** e adicione o aplicativo. Clique em **Adicionar** e selecione um aplicativo cujos widgets você deseja permitir na lista na tela inicial. Clique em **Save**. Repita esse processo para permitir mais widgets de aplicativos.
- **Permitir contatos do perfil profissional nos contatos do dispositivo:** mostra contatos do perfil gerenciado do Android Enterprise no perfil pai, para chamadas recebidas (Android 7.0 e posterior). O padrão é **Desativado**.
- **Ativar aplicativos do sistema:** permite que os usuários executem aplicativos de dispositivo pré-instalados. O padrão é **Desativado**. Para habilitar aplicativos específicos, clique em **Adicionar** na tabela **Lista de aplicativos do sistema**.
 - * **Lista de aplicativos do sistema:** Uma lista dos aplicativos do sistema que você deseja ativar no dispositivo. Defina **Ativar aplicativos do sistema** como **Ativado** e adicione o nome do pacote do aplicativo. Para procurar o nome do pacote de um aplicativo do sistema, você pode usar o Android Debug Bridge (adb) para chamar o comando gerenciador de pacotes (pm) do Android. Por exemplo, `adb shell "pm list packages -f name"`, onde "name" é parte do nome do pacote. Para obter mais informações, consulte <https://developer.android.com/studio/command-line/adb>. Para dispositivos Android Enterprise, você pode restringir as permissões de aplicativos usando a política de [permissões de aplicativo Android Enterprise](#).
- **Desativar aplicativos:** Impede que uma lista especificada de aplicativos seja executada nos dispositivos. O padrão é **Desativado**. Para desabilitar um aplicativo instalado, altere a configuração para **Ativado** e clique em **Adicionar** na tabela **Lista de Aplicativos**.

- * **Lista de aplicativos:** uma lista dos aplicativos que você deseja bloquear. Defina **Desativar aplicativos** como **Ativado** e adicione o aplicativo. Digite o nome do pacote do aplicativo. Alterar e implantar uma lista de aplicativos sobrescreve a lista de aplicativos anterior. Por exemplo: se você desativar com.example1 e com.example2 e, posteriormente, alterar a lista para com.example1 e com.example3, o XenMobile habilitará com.example.2.
- **Ativar verificação de aplicativo:** permite que o sistema operacional verifique os aplicativos para detectar comportamentos mal-intencionados. O padrão é **Ativado**.
- **Ativar Google Apps:** permite que os usuários baixem aplicativos do Google Mobile Services para o dispositivo. O padrão é **Ativado**.
- **Não permitir impressão:** se **Ativado**, a configuração impede que os usuários imprimam em qualquer impressora acessível a partir do dispositivo do usuário. O padrão é **Off**. Disponível para: Android 9 e posterior.
- **Permitir que o usuário configure as credenciais:** permite que os usuários definam seus nomes de usuário e senhas. O padrão é **Ativado**.
- **Samsung SAFE: permite os controles de hardware**
 - **Área de transferência:** permitir que os usuários copiem dados para a área de transferência nos dispositivos deles.
 - * **Compartilhamento de área de transferência:** permitir que os usuários compartilhem conteúdo da área de transferência entre os respectivos dispositivos e um computador (MDM 4.0 e versões posteriores).
- **Samsung SAFE: permitir aplicativos**
 - **Navegador:** permite que os usuários usem o navegador da Web. O padrão é **Ativado**.
 - **Youtube:** permite que os usuários acessem o YouTube. O padrão é **Ativado**.
 - **Google Play/Marketplace:** permite que os usuários acessem o Google Play e o Google Apps Marketplace. O padrão é **Ativado**.
- **Samsung Knox**
 - **Ativar verificação de revogação:** ativa a verificação de certificados revogados. O padrão é **Ativado**.
 - **Mover aplicativos para o contêiner:** permite que os usuários movam aplicativos entre o contêiner Knox e a área pessoal em seus dispositivos. O padrão é **Ativado**.
 - **Impor a Autenticação Multifator:** os usuários devem usar uma impressão digital e outro método de autenticação, como senha ou PIN, para abrir os dispositivos deles. O padrão é **Ativado**.
 - **Ativar keystore TIMA:** o KeyStore TIMA fornece o armazenamento seguro de chaves baseado em TrustZone para as chaves simétricas. Os pares de chaves e os certificados RSA

são roteados para o provedor padrão de armazenamento de chaves para armazenamento. O padrão é **Ativado**.

- **Impor autenticação ao contêiner:** usar uma autenticação separada e diferente daquela usada para desbloquear o dispositivo abrir o contêiner Knox. O padrão é **Ativado**.
- **Lista de compartilhamento:** permite que os usuários compartilhem conteúdo entre aplicativos na lista Compartilhar Via. O padrão é **Ativado**.
- **Ativar Log de Auditoria:** permite a criação de logs de auditoria de eventos para análise forense de um dispositivo. O padrão é **Ativado**.
- **Usar Teclado Seguro:** força os usuários a usar um teclado seguro no contêiner Knox. O padrão é **Ativado**.
- **Autenticação do navegador com cartão inteligente:** ativa a autenticação de navegador nos dispositivos equipados com um leitor de cartão inteligente.

Quando **Aplicar a dispositivos totalmente gerenciados com um perfil de trabalho** estiver ativado e definido como **Gerenciar dispositivos**, defina estas configurações:

- **Permitir ações de USB**

- **Depuração:** permite a depuração por USB. O padrão é **Desativado**.
- **Transferência de arquivos:** permite a transferência de arquivos por USB. O padrão é **Desativado**.

- **Rede**

- **Permitir configuração de VPN:** permite que os usuários criem configurações de VPN. Para dispositivos de perfil de trabalho com Android 6 e posterior e para dispositivos totalmente gerenciados. O padrão é **Ativado**.
- **Android Beam:** permitir que os usuários enviem páginas da Web, imagens, vídeos ou outros conteúdos dos dispositivos deles para outro dispositivo usando NFC (comunicação a curta distância). Para MDM 4.0 e posterior. Padrão se **Desativado**.
- **Permitir configuração do provedor de localização:** permite que os usuários ativem o GPS em seus dispositivos. Para Android API 28 e posterior. O padrão é **Ativado**.

- **Segurança**

- **Permitir o uso da barra de status:** se definido como **Ativado**, essa configuração habilita a barra de status em dispositivos gerenciados e em dispositivos dedicados (também conhecidos como dispositivos COSU). Isso desabilita notificações, configurações rápidas e outras sobreposições de tela que permitem escapar do modo de tela inteira. Os usuários podem acessar as configurações do sistema e ver as notificações. Para Android 6.0 e posterior. O padrão é **Desativado**.
- **Impedir que o Keyguard bloqueie o dispositivo:** se definido como **Ativado**, essa configuração desabilita o Keyguard na tela de bloqueio em dispositivos gerenciados e dispositivos dedicados (também conhecidos como dispositivos COSU). O padrão é **Desativado**.
- **Não permitir impressão:** se **Ativado**, a configuração impede que os usuários imprimam em qualquer impressora acessível a partir do dispositivo do usuário. O padrão é **Off**.

Disponível para: Android 9 e posterior.

- **Allow account management:** permite que a conta seja adicionada no perfil profissional e em dispositivos gerenciados. O padrão é **Desativado**.
- **Allow cross profile copy and paste:** permite ou impede o uso da área de transferência para copiar e colar entre aplicativos no perfil do Android Enterprise e aplicativos na área pessoal. O padrão é **Desativado**.
- **Permitir compartilhamento de localização:** permite o compartilhamento de localização. Nos perfis gerenciados, o proprietário do dispositivo pode substituir essa configuração. O padrão é **Desativado**.

Dica:

Você pode criar políticas de dispositivo de Localização no XenMobile para impor fronteiras geográficas. Consulte [Política de dispositivo de localização](#).

- **Permitir aplicativos não Google Play:** permite a instalação de aplicativos de outras lojas diferentes da Google Play. O padrão é **Desativado**.
- **Permitir captura de tela:** permite que os usuários gravem ou façam uma captura da tela do dispositivo. O padrão é **Desativado**.
- **Permitir o uso da câmera:** permite que os usuários tirem fotos e façam vídeos com a câmera do dispositivo. O padrão é **Desativado**.
- **Permitir o controle do usuário das configurações do aplicativo:** permite que os usuários desinstalem aplicativos, desativem aplicativos, limpem o cache e os dados, forcem a interrupção de qualquer aplicativo e cancelem os padrões. O padrão é **Desativado**.
- **Permitir widgets de aplicativo de perfil de trabalho na tela inicial:** se essa configuração estiver **Ativada**, os usuários podem colocar widgets de aplicativos de perfil de trabalho na tela inicial do dispositivo. Se essa configuração for **Desativado**, os usuários não podem colocar widgets de aplicativo de perfil de trabalho na tela inicial do dispositivo. O padrão é **Desativado**.
 - * **Aplicativos cujos widgets serão permitidos:** uma lista dos aplicativos que você deseja permitir na tela inicial. Defina **Permitir widgets de aplicativo de perfil profissional na tela inicial** como **Ativado** e adicione o aplicativo. Clique em **Adicionar** e selecione um aplicativo cujos widgets você deseja permitir na lista na tela inicial. Clique em **Save**. Repita esse processo para permitir mais widgets de aplicativos.
- **Permitir contatos do perfil profissional nos contatos do dispositivo:** mostra contatos do perfil gerenciado do Android Enterprise no perfil pai, para chamadas recebidas (Android 7.0 e posterior). O padrão é **Desativado**.
- **Ativar aplicativos do sistema:** permite que os usuários executem aplicativos de dispositivo pré-instalados. O padrão é **Desativado**. Para habilitar aplicativos específicos, clique em **Adicionar** na tabela **Lista de aplicativos do sistema**.
 - * **Lista de aplicativos do sistema:** Uma lista dos aplicativos do sistema que

you want to activate on the device. Define **Ativar aplicativos do sistema** as **Ativado** and add the package name of the application. To find the package name of an application on the system, you can use the Android Debug Bridge (adb) to run the package manager (pm) command on the Android. For example, `adb shell "pm list packages -f name"`, where "name" is part of the package name. For more information, consult <https://developer.android.com/studio/command-line/adb>. For Android Enterprise devices, you can restrict application permissions using the [policy of configurations managed by Android Enterprise](#).

- **Desativar aplicativos:** Impede que uma lista especificada de aplicativos seja executada nos dispositivos. O padrão é **Desativado**. Para desabilitar um aplicativo instalado, altere a configuração para **Ativado** e clique em **Adicionar** na tabela **Lista de Aplicativos**.
 - * **Lista de aplicativos:** uma lista dos aplicativos que você deseja bloquear. Defina **Desativar aplicativos** como **Ativado** e adicione o aplicativo. Digite o nome do pacote do aplicativo. Alterar e implantar uma lista de aplicativos sobrescreve a lista de aplicativos anterior. Por exemplo: se você desativar com.example1 e com.example2 e, posteriormente, alterar a lista para com.example1 e com.example3, o XenMobile habilitará com.example2.
- **Ativar verificação de aplicativo:** permite que o sistema operacional verifique os aplicativos para detectar comportamentos mal-intencionados. O padrão é **Ativado**.
- **Ativar Google Apps:** permite que os usuários baixem aplicativos do Google Mobile Services para o dispositivo. O padrão é **Ativado**.
- **Dispositivo totalmente gerenciado.**
 - **Permitir vários usuários:** permite que vários usuários usem um dispositivo (MDM 4.0 e posterior). O padrão é **Ativado**.
 - **Permitir roaming:** permite que os usuários usem dados celulares enquanto estiverem em roaming. O padrão é O, que desativa o roaming nos dispositivos dos usuários. O padrão é **Desativado**. Quando essa definição está ativada, estas configurações estão disponíveis para dispositivos Samsung SAFE:
 - * **Dados:** permitir que os usuários usem dados celulares para dados.
 - * **Push:** permitir que os usuários usem dados celulares para envio.
 - * **Sincronização:** permite que os usuários usem dados celulares para sincronização.
 - * **Chamadas de voz:** permite que os usuários usem dados celulares para chamadas de voz.
 - **Permitir SMS:** permite que os usuários enviem e recebam mensagens SMS. O padrão é **Desativado**.
 - **Backup:** permite que os usuários façam backup de aplicativos e dados do sistema em seus dispositivos. O padrão é **Ativado**.
 - **Bluetooth:** permite que os usuários usem Bluetooth. O padrão é **Ativado**.

- **Alteração de data e hora:** permite que os usuários alterem a data e hora em seus dispositivos. O padrão é **Ativado**.
- **Redefinição de fábrica:** permite que os usuários realizem uma redefinição de fábrica em seus dispositivos. O padrão é **Ativado**.
- **Manter a tela do dispositivo ligada:** se esta configuração estiver definida como **Ativado**, a tela do dispositivo permanecerá ligada quando o dispositivo estiver conectado. O padrão é **Desativado**.
- **Armazenamento em massa:** permite a transferência de grandes arquivos de dados entre os dispositivos dos usuários e um computador por uma conexão USB. O padrão é **Ativado**.
- **Microfone:** permite que os usuários usem o microfone em seus dispositivos. O padrão é **Ativado**.
- **Tethering:** permite que os usuários configurem hotspots portáteis e vinculem dados. O padrão é **Desativado**. Quando essa definição está ativada, estas configurações estão disponíveis para dispositivos Samsung:
 - * **USB:** permite que os usuários compartilhem uma conexão de dados móvel com outro dispositivo usando as suas conexões USB.
 - * **Bluetooth:** permite que os usuários compartilhem uma conexão de dados móvel com outro dispositivo usando as suas conexões Bluetooth.
 - * **Wi-Fi:** permite que os usuários compartilhem uma conexão de dados móvel com outro dispositivo usando as suas conexões Wi-Fi.
- **Wi-Fi:** permite que usuários se conectem a redes Wi-Fi. O padrão é **Ativado**. Quando essa definição está ativada, estas configurações estão disponíveis:
 - * **Direto:** permite que os usuários se conectem diretamente a outro dispositivo usando as suas conexões Wi-Fi. Apenas para dispositivos Samsung. Para MDM 4.0 e posterior.
 - * **Alteração de estado:** permite que os aplicativos alterem o estado da conectividade Wi-Fi.
- **Samsung SAFE: permite os controles de hardware**
 - **Ativar verificação de inicialização confiável ODE:** usar a verificação de inicialização confiável ODE para estabelecer uma cadeia de confiança do carregador de inicialização com a imagem do sistema. O padrão é **Ativado**.
 - **Permitir apenas chamadas de emergência:** permite que os usuários ativem o modo Somente chamadas de emergência em seus dispositivos. O padrão é **Desativado**.
 - **Permitir recuperação de firmware:** permite que os usuários recuperem o firmware em seus dispositivos. O padrão é **Ativado**.
 - **Permitir criptografia rápida:** permite a criptografia somente do espaço de memória usado. Isso contrasta com a criptografia completa de disco, que criptografa todos os dados, incluindo configurações, dados de aplicativo, arquivos baixados e aplicativos, mídia e outros arquivos. O padrão é **Ativado**.
 - **Modo de critérios comuns:** coloca o dispositivo no modo de critérios comuns. A configu-

ração Critérios Comuns impõe processos de segurança rigorosos. O padrão é **Ativado**.

- **Faixa de inicialização DOD:** exibe uma mensagem ou uma faixa de mensagem de notificação de uso do sistema aprovado para DoD quando os dispositivos dos usuários são reiniciados. O padrão é **Desativado**.
- **Alterações de configurações:** permite que os usuários alterem as configurações em seus dispositivos totalmente gerenciados. O padrão é **Ativado**.
- **Atualização por rede celular:** permite que os dispositivos dos usuários recebam atualizações de software sem fio (MDM 3.0 e versões posteriores). O padrão é **Ativado**.
- **Dados de segundo plano:** permite que aplicativos sincronizem dados em segundo plano para dispositivos totalmente gerenciados. O padrão é **Ativado**.
- **Área de transferência:** permitir que os usuários copiem dados para a área de transferência nos dispositivos deles.
 - * **Compartilhamento de área de transferência:** permitir que os usuários compartilhem conteúdo da área de transferência entre os respectivos dispositivos e um computador (MDM 4.0 e versões posteriores).
- **Tecla Home:** permite que os usuários usem a tecla **Home** em seus dispositivos totalmente gerenciados. O padrão é **Ativado**.
- **Localização fictícia:** permite que os usuários usem localizações de GPS fictícias. Para dispositivos totalmente gerenciados. O padrão é **Ativado**.
- **NFC:** permite que os usuários usem NFC em seus dispositivos totalmente gerenciados (MDM 3.0 e posterior). O padrão é **Ativado**.
- **Desligar:** permite que os usuários desliguem seus dispositivos totalmente gerenciados (MDM 3.0 e versões posteriores). O padrão é **Ativado**.
- **Cartão SD:** permite que os usuários usem um cartão SD, se disponível, com os seus dispositivos. O padrão é **Ativado**.
- **Armazenamento em host:** permite que os dispositivos dos usuários ajam como o host USB quando um dispositivo USB é conectado a seus dispositivos. Em seguida, os dispositivos dos usuários fornecem energia ao dispositivo USB. O padrão é **Ativado**.
- **Discador de voz:** permite que os usuários usem o comunicador de voz em seus dispositivos (MDM 4.0 e versões posteriores). O padrão é **Ativado**.
- **SBeam:** permite que os usuários compartilhem conteúdo com outras pessoas usando NFC e Wi-Fi Direct (MDM 4.0 e versões posteriores). O padrão é **Ativado**.
- **SVoice:** permite que os usuários usem o assistente pessoal inteligente e navegador de conhecimento em seus dispositivos (MDM 4.0 e versões posteriores). O padrão é **Ativado**.
- **Samsung SAFE: permitir aplicativos**
 - **Reconhecimento de face:** permite que os usuários usem o aplicativo de reconhecimento de face. O padrão é **Ativado**.
 - **Navegador:** permite que os usuários usem o navegador da Web. O padrão é **Ativado**.
 - **Youtube:** permite que os usuários acessem o YouTube. O padrão é **Ativado**.

- **Google Play/Marketplace:** permite que os usuários acessem o Google Play e o Google Apps Marketplace. O padrão é **Ativado**.
- **Samsung SAFE: Network**
 - **MMS de entrada:** permite que os usuários recebam mensagens MMS. O padrão é **Ativado**.
 - **MMS de saída:** permite que os usuários enviem mensagens MMS. O padrão é **Ativado**.
 - **SMS de entrada:** permite que os usuários recebam mensagens SMS. O padrão é **Ativado**.
 - **SMS de saída:** permite que os usuários enviem mensagens SMS. O padrão é **Ativado**.
 - **Configurar redes móveis:** permite que os usuários configurem redes móveis. O padrão é **Ativado**.
 - **Limite por dia (MB):** insira o número de MB de dados móveis que os usuários podem usar por dia. O padrão é 0, o que desativa esse recurso (MDM 4.0 e versões posteriores).
 - **Limite por semana (MB):** insira o número de MB de dados móveis que os usuários podem usar por semana. O padrão é 0, o que desativa esse recurso (MDM 4.0 e versões posteriores).
 - **Limite por mês (MB):** insira o número de MB de dados móveis que os usuários podem usar por mês. O padrão é 0, o que desativa esse recurso (MDM 4.0 e versões posteriores).
 - **Apenas conexões seguras:** permite que os usuários usem somente conexões seguras (MDM 4.0 e versões posteriores). O padrão é **Ativado**.
 - **Gravação de áudio:** permite que os usuários gravem áudio usando os seus dispositivos (MDM 4.0 e versões posteriores). O padrão é **Ativado**.
 - **Gravação de vídeo:** permite que os usuários gravem vídeo usando os seus dispositivos (MDM 4.0 e versões posteriores). O padrão é **Ativado**.
- **Samsung Knox**
 - **Ativar verificação de revogação:** ativa a verificação de certificados revogados. O padrão é **Ativado**.
 - **Mover aplicativos para o contêiner:** permite que os usuários movam aplicativos entre o contêiner Knox e a área pessoal em seus dispositivos. O padrão é **Ativado**.
 - **Impor a Autenticação Multifator:** os usuários devem usar uma impressão digital e outro método de autenticação, como senha ou PIN, para abrir os dispositivos deles. O padrão é **Ativado**.
 - **Ativar keystore TIMA:** o KeyStore TIMA fornece o armazenamento seguro de chaves baseado em TrustZone para as chaves simétricas. Os pares de chaves e os certificados RSA são roteados para o provedor padrão de armazenamento de chaves para armazenamento. O padrão é **Ativado**.
 - **Impor autenticação ao contêiner:** usar uma autenticação separada e diferente daquela usada para desbloquear o dispositivo abrir o contêiner Knox. O padrão é **Ativado**.
 - **Lista de compartilhamento:** permite que os usuários compartilhem conteúdo entre aplicativos na lista Compartilhar Via. O padrão é **Ativado**.
 - **Ativar Log de Auditoria:** permite a criação de logs de auditoria de eventos para análise

forense de um dispositivo. O padrão é **Ativado**.

- **Usar Teclado Seguro:** força os usuários a usar um teclado seguro no contêiner Knox. O padrão é **Ativado**.
- **Autenticação do navegador com cartão inteligente:** ativa a autenticação de navegador nos dispositivos equipados com um leitor de cartão inteligente.

Configurações do Samsung SAFE

Restrictions Policy	Restrictions Policy
1 Policy Info	This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.
2 Platforms	Allow hardware controls
<input type="checkbox"/> iOS	Enable ODE Trusted Boot Verification <input checked="" type="checkbox"/>
<input type="checkbox"/> macOS	Allow Development Mode <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Samsung SAFE	Allow Emergency Calls Only <input type="checkbox"/>
<input checked="" type="checkbox"/> Samsung KNOX	Allow Firmware Recovery <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Windows Phone	Allow Fast Encryption <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Windows Desktop/Tablet	Common Criteria Mode <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Amazon	Factory reset <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Windows Mobile/CE	Date Time Change <input checked="" type="checkbox"/>
3 Assignment	DOD boot banner <input type="checkbox"/>
	Settings changes <input checked="" type="checkbox"/>

Algumas opções estão disponíveis somente em APIs específicas de gerenciamento de dispositivo móvel da Samsung. Essas opções são marcadas com as informações relevantes da versão.

• Permitir controles de hardware

- **Ativar verificação de inicialização confiável ODE:** usar a verificação de inicialização confiável ODE para estabelecer uma cadeia de confiança do carregador de inicialização com a imagem do sistema.
- **Permitir modo de desenvolvimento:** permitir que os usuários ativem as configurações do desenvolvedor nos dispositivos deles.
- **Permitir apenas chamadas de emergência:** permitir que os usuários ativem o modo Somente chamadas de emergência nos dispositivos deles.
- **Permitir recuperação de firmware:** permitir que os usuários recuperem o firmware nos dispositivos deles.
- **Permitir criptografia rápida:** permitir a criptografia somente do espaço de memória usado. Isso contrasta com a criptografia completa de disco, que criptografa todos os dados, incluindo configurações, dados de aplicativo, arquivos baixados e aplicativos, mídia e outros arquivos.
- **Modo Common Criteria:** colocar o dispositivo no Common Criteria Mode. A configuração Critérios Comuns impõe processos de segurança rigorosos.

- **Redefinição de fábrica:** permitir que os usuários realizem uma redefinição de fábrica nos dispositivos deles
- **Alteração de data e hora:** permitir que os usuários alterem a data e hora nos dispositivos deles.
- **Faixa de inicialização DOD:** exibir uma mensagem ou uma faixa de mensagem de notificação de uso do sistema aprovado para DoD quando os dispositivos dos usuários são reiniciados.
- **Alterações de configurações:** permitir que os usuários alterem as configurações nos dispositivos deles.
- **Backup:** permitir que os usuários façam backup de aplicativos e dados do sistema nos dispositivos deles.
- **Atualização por rede celular:** permitir que os dispositivos dos usuários recebam atualizações de software sem fio (MDM 3.0 e versões posteriores).
- **Dados de segundo plano:** permitir que os aplicativos sincronizem dados em segundo plano.
- **Câmera:** permitir que os usuários usem a câmera nos dispositivos deles.
- **Área de transferência:** permitir que os usuários copiem dados para a área de transferência nos dispositivos deles.
 - * **Compartilhamento de área de transferência:** permitir que os usuários compartilhem conteúdo da área de transferência entre os respectivos dispositivos e um computador (MDM 4.0 e versões posteriores).
- **Tecla Home:** permitir que os usuários usem a tecla Home nos dispositivos deles.
- **Microfone:** permitir que os usuários usem o microfone nos dispositivos deles.
- **Localização fictícia:** permitir que os usuários usem localizações de GPS fictícias.
- **NFC:** permitir que os usuários usem NFC (comunicação a curta distância) nos dispositivos deles (MDM 3.0 e versões posteriores).
- **Desligar:** permitir que os usuários desliguem os dispositivos deles (MDM 3.0 e versões posteriores).
- **Capturas de tela:** permitir que os usuários façam capturas de tela nos dispositivos deles.
- **Cartão SD:** permitir que os usuários usem um cartão SD, se disponível, com os dispositivos deles.
- **Discador de voz:** permitir que os usuários usem o comunicador de voz nos dispositivos deles (MDM 4.0 e versões posteriores).
- **SBeam:** permitir que os usuários compartilhem conteúdo com outras pessoas usando NFC e Wi-Fi Direct (MDM 4.0 e versões posteriores).
- **SVoice:** permitir que os usuários usem o assistente pessoal inteligente e navegador de conhecimento nos dispositivos deles (MDM 4.0 e versões posteriores).
- **Permitir vários usuários:** permite que vários usuários usem um dispositivo (MDM 4.0 e posterior). O padrão é **Desativado**.

- **Permitir aplicativos**

- **Navegador:** permitir que os usuários usem o navegador da Web.
- **Youtube:** permitir que os usuários acessem o YouTube.
- **Google Play/Marketplace:** permitir que os usuários acessem o Google Play e o Google Apps Marketplace.
- **Permitir aplicativos não Google Play:** permitir que os usuários baixem aplicativos de outros sites além do Google Play e do Google Apps Marketplace. Se **ativado**, um usuário pode usar as configurações de segurança em seu dispositivo para confiar em aplicativos de fontes desconhecidas.
- **Parar aplicativo do sistema:** permitir que os usuários desativem os aplicativos de sistema pré-instalados (MDM 4.0 e versões posteriores).
- **Desativar aplicativos:** se **Ativado**, impede que uma lista especificada de aplicativos sejam executados em dispositivos Samsung SAFE.

- **Rede**

- **MMS de entrada:** permitir que os usuários recebam mensagens MMS.
- **SMS de entrada:** permitir que os usuários recebam mensagens SMS.
- **MMS de saída:** permitir que os usuários enviem mensagens MMS.
- **SMS de saída:** permitir que os usuários enviem mensagens SMS.
- **Perfis de rede virtual privada para adicionar usuários:**
- **Bluetooth:** permitir que os usuários usem Bluetooth.
 - * **Tethering:** permitir que os usuários compartilhem uma conexão de dados móvel com outro dispositivo usando a conexão Bluetooth.
- **Wi-Fi:** permitir que usuários se conectem a redes Wi-Fi.
 - * **Tethering:** permitir que os usuários compartilhem uma conexão de dados móvel com outro dispositivo usando a conexão Wi-Fi.
 - * **Direto:** permitir que os usuários se conectem diretamente a outro dispositivo usando uma conexão Wi-Fi (MDM 4.0 e versões posteriores).
 - * **Alteração de estado:** permitir que os aplicativos alterem o estado da conectividade Wi-Fi.
 - * **Alterações de política de usuário:** permitir que os usuários alterem as políticas de Wi-Fi. Se essa opção não estiver selecionada, os usuários poderão alterar somente o nome do usuário e a senha do WiFi. Se essa opção estiver selecionada, os usuários poderão alterar as políticas de WiFi.
- **Tethering:** permitir que os usuários compartilhem uma conexão de dados móvel com outro dispositivo.
- **Dados celulares:** permitir que os usuários usem a conexão celular deles para dados.
- **Permitir roaming:** permitir que os usuários usem dados celulares enquanto estiverem em roaming. O padrão é O, que desativa o roaming nos dispositivos dos usuários.
- **Apenas conexões seguras:** permitir que os usuários usem somente conexões seguras

- (MDM 4.0 e versões posteriores).
- **Android Beam:** permitir que os usuários enviem páginas da Web, imagens, vídeos ou outros conteúdos dos dispositivos deles para outro dispositivo usando NFC (MDM 4.0 e versões posteriores).
 - **Gravação de áudio:** permitir que os usuários gravem áudio usando os dispositivos deles (MDM 4.0 e versões posteriores).
 - **Gravação de vídeo:** permitir que os usuários gravem vídeo usando os dispositivos deles (MDM 4.0 e versões posteriores).
 - **Serviços de localização:** permitir que os usuários liguem o GPS nos dispositivos deles.
 - **Limite por dia (MB):** insira o número de MB de dados móveis que os usuários podem usar por dia. O padrão é 0, o que desativa esse recurso (MDM 4.0 e versões posteriores).
 - **Limite por semana (MB):** insira o número de MB de dados móveis que os usuários podem usar por semana. O padrão é 0, o que desativa esse recurso (MDM 4.0 e versões posteriores).
 - **Limite por mês (MB):** insira o número de MB de dados móveis que os usuários podem usar por mês. O padrão é 0, o que desativa esse recurso (MDM 4.0 e versões posteriores).
 - **Permitir ações de USB** permitir a conexão USB entre os dispositivos dos usuários e um computador.
 - **Depuração:** permitir a depuração sobre USB.
 - **Armazenamento em host:** permitir que os dispositivos dos usuários ajam como o host USB quando um dispositivo USB é conectado aos dispositivos deles. Em seguida, os dispositivos dos usuários fornecem energia ao dispositivo USB.
 - **Armazenamento em massa:** permitir a transferência de grandes arquivos de dados entre os dispositivos dos usuários e um computador sobre uma conexão USB.
 - **Reprodutor de mídia Kies:** permitir que os usuários usem a ferramenta Samsung Kies para sincronizar arquivos entre os dispositivos deles e um computador.
 - **Tethering:** permitir que os usuários compartilhem uma conexão de dados móvel com outro dispositivo usando uma conexão USB.
 - **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra.
 - **Permitir que o usuário remova a política:** você pode selecionar quando os usuários podem remover a política do dispositivo. Selecione **Sempre**, **Código secreto obrigatório** ou **Nunca** no menu. Se você selecionar **Código secreto obrigatório**, digite um código secreto no campo **Código secreto de remoção**.

- **Escopo do perfil:** selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

Configurações do Samsung KNOX

Restrictions Policy	Restrictions Policy
1 Policy Info	This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.
2 Platforms	
<input type="checkbox"/> iOS	Allow use of camera <input checked="" type="checkbox"/>
<input type="checkbox"/> macOS	Enable Revocation Check <input checked="" type="checkbox"/>
<input type="checkbox"/> Samsung SAFE	Move Apps To Container <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Samsung KNOX	Enforce Multifactor Authentication <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Windows Phone	Enable TIMA Key store <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Windows Desktop/Tablet	Enforce Auth For Container <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Amazon	Share List <input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Windows Mobile/CE	Enable Audit Log <input checked="" type="checkbox"/>
3 Assignment	Use Secure Keypad <input checked="" type="checkbox"/>
	Enable Google Apps <input checked="" type="checkbox"/>

Essas opções estão disponíveis somente no Samsung KNOX Premium (KNOX 2.0).

- **Permitir o uso da câmera:** permitir que os usuários usem a câmera nos dispositivos deles.
- **Permitir verificação de revogação:** ativar a verificação de certificados revogados.
- **Mover aplicativos para o contêiner:** permitir que os usuários movam aplicativos entre o contêiner KNOX e área pessoal nos dispositivos deles.
- **Impor a Autenticação Multifator:** os usuários devem usar uma impressão digital e outro método de autenticação, como senha ou PIN, para abrir os dispositivos deles.
- **Ativar keystore TIMA:** o KeyStore TIMA fornece o armazenamento seguro de chaves baseado em TrustZone para as chaves simétricas. Os pares de chaves e os certificados RSA são roteados para o provedor padrão de armazenamento de chaves para armazenamento.
- **Impor autenticação ao contêiner:** usar uma autenticação separada e diferente daquela usada para desbloquear o dispositivo abrir o contêiner KNOX.
- **Lista de Compartilhamento:** permitir que os usuários compartilhem conteúdo entre aplicativos na lista Compartilhar Via.
- **Ativar Log de Auditoria:** permitir a criação de logs de auditoria de eventos para análise forense de um dispositivo.
- **Usar Teclado Seguro:** forçar os usuários a usar um teclado seguro no contêiner KNOX.
- **Ativar Google Apps:** permitir que os usuários baixem aplicativos do Google Mobile Services para o contêiner KNOX.
- **Autenticação do navegador com cartão inteligente:** ativar a autenticação de navegador nos

dispositivos equipados com um leitor de cartão inteligente.

Configurações do Windows Phone e do Windows Desktop/Tablet

Restrictions Policy	Restrictions Policy
1 Policy Info	This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.
2 Platforms	<p>WIFI Settings</p> <p>Allow WiFi <input checked="" type="checkbox"/></p> <p>Allow Internet sharing <input checked="" type="checkbox"/></p> <p>Allow auto-connect to WiFi Sense hotspots <input checked="" type="checkbox"/></p> <p>Allow manual configuration <input checked="" type="checkbox"/></p> <p>Connectivity</p> <p>Allow NFC <input checked="" type="checkbox"/></p> <p>Allow bluetooth <input checked="" type="checkbox"/></p> <p>Allow VPN over cellular <input checked="" type="checkbox"/></p> <p>Allow VPN over cellular while roaming <input checked="" type="checkbox"/></p> <p>Allow USB connection <input checked="" type="checkbox"/></p>
<input type="checkbox"/> iOS <input type="checkbox"/> macOS <input type="checkbox"/> Samsung SAFE <input type="checkbox"/> Samsung KNOX <input checked="" type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Desktop/Tablet <input checked="" type="checkbox"/> Amazon <input checked="" type="checkbox"/> Windows Mobile/CE	
3 Assignment	

• Configurações de Wi-Fi

- **Permitir Wi-Fi:** permitir que um dispositivo se conecte a uma rede Wi-Fi. Windows Phone somente.
- **Permitir compartilhamento de Internet:** permitir que um dispositivo compartilhe a respectiva conexão com a Internet com outros dispositivos, transformando-o em um ponto de acesso Wi-Fi.
- **Permitir a conexão automática com pontos de acesso WiFi Sense:** permitir que um dispositivo se conecte automaticamente a pontos de acesso WiFi Sense. Os serviços de localização devem estar ativados para que essa opção funcione. Para obter mais informações sobre o WiFi Sense, consulte as [Perguntas frequentes do WiFi Sense](#) do Windows Phone.
- **Permitir configuração manual:** permitir que os usuários configurem manualmente as conexões Wi-Fi. Windows Phone somente.

• Conectividade

- **Permitir NFC:** permitir que o dispositivo se comunique com uma marca NFC (Comunicação a Curta Distância) ou outro dispositivo de transmissão com tecnologia NFC. Windows Phone somente.
- **Permitir bluetooth:** permitir que o dispositivo se conecte por Bluetooth. Windows Phone somente.
- **Permitir VPN via celular:** permitir que o dispositivo se conecte sobre VPN a uma rede celular.
- **Permitir VPN via celular em roaming:** permitir que o dispositivo se conecte sobre VPN quando ele fizer roaming entre redes celulares.

- **Permitir conexão USB:** permitir que uma área de trabalho acesse o armazenamento de um dispositivo usando uma conexão USB. Windows Phone somente.
- **Permitir roaming de dados celulares:** permitir que os usuários usem dados celulares enquanto estiverem em roaming.
- **Contas**
 - **Permitir conexão de conta da Microsoft:** permitir que o dispositivo use uma conta da Microsoft para autenticação e serviços de conexão não relacionados a email.
 - **Permitir email não Microsoft:** permitir que o usuário adicione contas de email que não são da Microsoft.
- **Pesquisar:** somente Windows Phone.
 - **Permitir que a pesquisa use localização:** permitir que as pesquisas usem o serviço de localização do dispositivo.
 - **Filtro de conteúdo adulto:** permitir conteúdo adulto. O padrão é **Desativado**, o que significa que o conteúdo adulto não é filtrado.
 - **Permitir que o Bing Vision armazene imagens:** permitir que o Bing Vision armazene as imagens capturadas ao realizar pesquisas do Bing Vision.
- **System**
 - **Permitir cartão de armazenamento:** permitir que o dispositivo use um cartão de memória.
 - **Telemetria:** na lista, clique em uma opção para permitir ou restringir envio de informações de telemetria pelo dispositivo. O padrão é **Permitido**. Outras opções são **Não permitido** e **Permitido, exceto para a solicitação de dados secundários**.
 - **Permitir serviços de localização:** permitir os serviços de localização.
 - **Permitir visualização de compilações internas:** permitir que os usuários visualizem as compilações internas da Microsoft.
- **Câmera:** Windows Desktop/Tablet somente
 - **Permitir o uso da câmera:** permitir que os usuários usem a câmera do respectivo dispositivo.
- **Bluetooth:** Windows Desktop/Tablet somente
 - **Permitir modo detectável:** permitir que dispositivos Bluetooth encontrem o dispositivo local.
 - **Nome do dispositivo local:** um nome para o dispositivo local.
- **Segurança:** Windows Phone somente
 - **Permitir a instalação manual do certificado raiz:** permitir que os usuários instalem manualmente um certificado raiz.
 - **Exigir criptografia do dispositivo:** exigir a criptografia do dispositivo. Observe que depois que a criptografia é ativada em um dispositivo, ela não pode ser desativada. O padrão é **Off**.
 - **Permitir copiar e colar:** permitir que os usuários copiem e coletem dados nos dispositivos

deles.

- **Permitir captura de tela:** permitir que os usuários criem capturas de tela nos dispositivos deles.
- **Permitir gravação de voz:** permitir que os usuários usem a gravação de voz nos dispositivos deles.
- **Permitir Salvar como para arquivos do Office:** permitir que os usuários salvem arquivos do Office usando Salvar como.
- **Permitir notificações do centro de ação:** permitir as notificações do Centro de Ação na tela de bloqueio do dispositivo.
- **Permitir Cortana:** permitir que os usuários acessem o Cortana, o assistente pessoal inteligente e navegador de conhecimento.
- **Permitir a sincronização de configurações de dispositivo:** permitir que os usuários sincronizem configurações entre dispositivos Windows Phone 8.1 quando estiverem em roaming.
- **Experiência:** Windows Desktop/Tablet somente
 - **Permitir Cortana:** permitir que os usuários acessem o Cortana, o assistente pessoal inteligente e navegador de conhecimento.
 - **Permitir descoberta do dispositivo:** permitir a descoberta da rede do dispositivo.
 - **Permitir registro manual no MDM:** permitir que os usuários manualmente cancelam o registro de dispositivos no XenMobile MDM.
 - **Permitir a sincronização de configurações de dispositivo:** permitir que os usuários sincronizem configurações entre dispositivos Windows 10 quando estiverem em roaming.
- **Bloqueio acima:** Windows Desktop/Tablet somente
 - **Permitir notificações toast:** permitir notificações na tela de bloqueio. Windows Desktop/Tablet somente
- **Aplicativos**
 - **Permitir o acesso à loja:** permitir que os usuários acessem a Microsoft Store. Windows Phone somente.
 - **Permitir desbloqueio do desenvolvedor:** permitir que os usuários registrem os dispositivos deles com a Microsoft e desenvolvam ou instalem aplicativos que não estão na loja de aplicativos do Windows Phone. Windows Phone somente.
 - **Permitir o acesso do navegador da Web:** permitir o Internet Explorer no dispositivo. Windows Phone somente.
 - **Permitir atualização automática da loja de aplicativos:** permitir que os aplicativos da loja de aplicativos sejam atualizados automaticamente. Windows Desktop/Tablet somente.
- **Privacidade:** Windows Desktop/Tablet somente
 - **Permitir personalização de entrada:** permitir que o serviço de personalização de entrada seja executado, para melhorar as entradas preditivas, como a caneta e o teclado de

toque, com base no que o usuário digita.

- **Configurações:** Windows Desktop/Tablet somente.
 - **Permitir reprodução automática:** permitir que os usuários alterem as configurações de reprodução automática.
 - **Permitir o sensor de dados:** permitir que os usuários alterem as configurações do Sensor de Dados.
 - **Permitir data e hora:** permitir que os usuários alterem as configurações de data e hora.
 - **Permitir idioma:** permitir que os usuários alterem as configurações de idioma.
 - **Permitir energia e suspensão:** permitir que os usuários alterem as configurações de energia e suspensão.
 - **Permitir região:** permitir que os usuários alterem as configurações de região.
 - **Permitir opções de logon:** permitir que os usuários alterem as configurações de entrada de login.
 - **Permitir local de trabalho:** permitir que os usuários alterem as configurações do local de trabalho.
 - **Permitir a sua conta:** permitir que os usuários alterem as configurações da conta.

Configurações do Amazon

Restrictions Policy	Restrictions Policy
1 Policy Info	This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.
2 Platforms	<p>Allow hardware controls</p> <p>Factory reset <input checked="" type="checkbox"/></p> <p>Profiles <input checked="" type="checkbox"/></p> <p>Allow apps</p> <p>Non-Amazon Appstore apps <input checked="" type="checkbox"/></p> <p>Social networks <input checked="" type="checkbox"/></p> <p>Network</p> <p>Bluetooth <input checked="" type="checkbox"/></p> <p>WiFi switch <input checked="" type="checkbox"/></p> <p>WiFi settings <input checked="" type="checkbox"/></p> <p>Cellular data <input checked="" type="checkbox"/></p> <p>Roaming data <input checked="" type="checkbox"/></p>
<input type="checkbox"/> iOS <input type="checkbox"/> macOS <input type="checkbox"/> Samsung SAFE <input type="checkbox"/> Samsung KNOX <input type="checkbox"/> Windows Phone <input type="checkbox"/> Windows Desktop/Tablet <input checked="" type="checkbox"/> Amazon <input checked="" type="checkbox"/> Windows Mobile/CE	
3 Assignment	

- **Permitir controles de hardware**
 - **Redefinição de fábrica:** permitir que os usuários realizem uma redefinição de fábrica nos dispositivos deles
 - **Perfis:** permitir que os usuários alterem o perfil de hardware nos dispositivos deles.
- **Permitir aplicativos**
 - **Aplicativos não Amazon Appstore:** permitir que os usuários instalem aplicativos não Amazon Appstore nos dispositivos deles.

- **Redes sociais:** permitir que os usuários acessem redes sociais nos dispositivos deles.
- **Rede**
 - **Bluetooth:** permitir que os usuários usem Bluetooth.
 - **Comutador de WiFi:** permitir que os aplicativos alterem o estado da conectividade Wi-Fi.
 - **Configurações de WiFi:** permitir que os usuários alterem as configurações de Wi-Fi.
 - **Dados celulares:** permitir que os usuários usem a conexão celular deles para dados.
 - **Dados de roaming:** permitir que os usuários usem dados celulares enquanto estiverem em roaming.
 - **Serviços de localização:** permitir que os usuários usem GPS.
- **Ações USB:**
 - **Depuração:** permitir que os dispositivos dos usuários se conectem por meio de USB a um computador para depuração.

Configurações do Windows Mobile/CE

Restrictions Policy	Restrictions Policy
1 Policy Info	This policy allows or restricts users from using certain features on their devices, such as the camera. You can also set security restrictions, as well as restrictions on media content and on certain types of apps users can and cannot install.
2 Platforms	<p>Bluetooth/infrared beaming (Obex) <input checked="" type="checkbox"/></p> <p>Camera <input checked="" type="checkbox"/></p> <p>WiFi switch <input checked="" type="checkbox"/></p> <p>Bluetooth <input checked="" type="checkbox"/></p> <p>► Deployment Rules</p>
<input type="checkbox"/> iOS	
<input type="checkbox"/> macOS	
<input type="checkbox"/> Samsung SAFE	
<input type="checkbox"/> Samsung KNOX	
<input type="checkbox"/> Windows Phone	
<input type="checkbox"/> Windows Desktop/Tablet	
<input type="checkbox"/> Amazon	
<input checked="" type="checkbox"/> Windows Mobile/CE	
3 Assignment	

- **Bluetooth/feixe infravermelho (Obex):** ativar o OBEX (protocolo OBjectEXchange) sobre Bluetooth ou infravermelho para trocar dados entre dispositivos.
- **Câmera:** permitir a câmera nos dispositivos dos usuários.
- **Comutador de WiFi:** permitir que os usuários alternem entre redes Wi-Fi.
- **Bluetooth:** ativar Bluetooth nos dispositivos dos usuários.
- **Câmera:** permitir a câmera nos dispositivos dos usuários.
- **Comutador de WiFi:** permitir que os usuários alternem entre redes Wi-Fi.
- **Bluetooth:** ativar Bluetooth nos dispositivos dos usuários.

Política de dispositivo em roaming

April 23, 2020

Você pode adicionar uma política de dispositivo no XenMobile para configurar se o roaming de voz e dados é permitido nos dispositivos iOS e Windows Mobile/CE dos usuários. Quando o roaming de voz está desativado, o roaming de dados é automaticamente desativado. Para o iOS, essa política está disponível somente nos dispositivos iOS 5.0 e versões posteriores.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

- **Desativar roaming de voz:** selecione se o roaming de voz deve ser desativado. Quando essa opção está ativada, o roaming de dados é automaticamente desativado. O padrão é **O**, o que permite o roaming de voz.
- **Desativar roaming de dados:** selecione se o roaming de dados deve ser desativado. Essa opção estará disponível somente quando o roaming de voz estiver ativado. O padrão é **O**, o que permite o roaming de dados.

Configurações do Windows Mobile/CE

- **Em roaming**
 - **Usar somente conexão sob demanda:** o dispositivo se conectará ao XenMobile somente se os usuários dispararem manualmente a conexão nos dispositivos deles, ou se um aplicativo móvel solicitar uma conexão forçada (como uma solicitação de correio por push se o Exchange Server tiver sido definido de acordo). Observe que essa opção desativa temporariamente a política padrão de programação de conexão de dispositivo.
 - **Bloquear conexões celulares exceto as gerenciadas pelo XenMobile:** exceto pelo tráfego de dados oficialmente declarado em um túnel de aplicativo do XenMobile ou outras tarefas de gerenciamento de dispositivo do XenMobile, nenhum outro dado é enviado ou recebido pelo dispositivo. Por exemplo, essa opção desativa todas as conexões com a Internet por meio do navegador da Web do dispositivo.
 - **Bloquear todas as conexões celulares gerenciadas pelo XenMobile:** todos os dados de aplicativo em trânsito por meio de um túnel do XenMobile são bloqueados (incluindo o XenMobile Remote Support). O tráfego de dados relacionado ao gerenciamento de dispositivo puro, no entanto, não é bloqueado.
 - **Bloquear todas as conexões celulares com o XenMobile:** nesse caso, até que o dispositivo também seja reconectado por meio de USB, WiFi ou da respectiva rede celular da

operadora de telefonia móvel padrão, não haverá nenhum tráfego em trânsito entre o dispositivo e o XenMobile.

- **Em roaming doméstico**
 - **Ignorar roaming doméstico:** nenhum dado é bloqueado enquanto os usuários estão em roaming doméstico.

Política de dispositivo de chave de licença MDM Samsung

November 30, 2020

Especifica a chave interna do Enterprise License Management (ELM) Samsung que você precisa implantar em um dispositivo antes de implantar as políticas e restrições do SAFE. O XenMobile também suporta o serviço Enterprise Firmware Over-The-Air (E-FOTA) da Samsung. O XenMobile dá suporte às políticas do Samsung for Enterprise (SAFE) e do Samsung KNOX e as estende.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do Samsung SAFE

The screenshot shows the configuration interface for the 'Samsung MDM License Key Policy'. The left sidebar lists policy sections: 1 Policy Info, 2 Platforms (with 'Samsung SAFE', 'Android Enterprise', and 'Samsung KNOX' checked), and 3 Assignment. The main content area is titled 'Samsung MDM License Key Policy' and includes a description: 'For the SAFE platform, use the macro to generate the ELM key. For the KNOX platform, as a prerequisite, you need to purchase a Samsung KNOX Workspace license. You then provide the license key in order to enable the KNOX APIs and deploy KNOX policies and restrictions to devices.' Below this are several input fields: 'ELM license key *' (containing the macro '\${elm.license.key}'), 'Enterprise FOTA Customer ID', 'Enterprise FOTA license', 'Client ID', and 'Client Secret'. Each field has a help icon. At the bottom, there is a 'Deployment Rules' section with a right-pointing arrow.

- **Chave de licença ELM:** o XenMobile preenche previamente esse campo com a macro que gera a chave de licença ELM. Se o campo estiver em branco, digite esta macro `${elm.license.key}`

Definir as configurações do Samsung E-FOTA

O Samsung Enterprise FOTA (E-FOTA) permite determinar quando os dispositivos são atualizados e a versão do firmware a ser usada. O E-FOTA permite que você teste as atualizações antes de implantá-las, para garantir que as atualizações sejam compatíveis com seus aplicativos. Você pode forçar os

dispositivos a atualizarem com a versão de firmware mais recente disponível, sem exigir a interação do usuário.

Samsung suporta E-FOTA para dispositivos Samsung Knox 2.7.1 (versão mínima) que executam firmware autorizado.

O XenMobile suporta a adição de dispositivos do console XenMobile ao Knox E-FOTA One. Para obter mais informações sobre como exportar uma lista de dispositivos do XenMobile, consulte [Exportar a tabela Dispositivos](#). Para obter mais informações sobre como adicionar um dispositivo ao Knox E-FOTA One, consulte a [documentação da Samsung](#).

O XenMobile não oferece suporte à Knox E-FOTA na solução MDM.

Para configurar uma política E-FOTA:

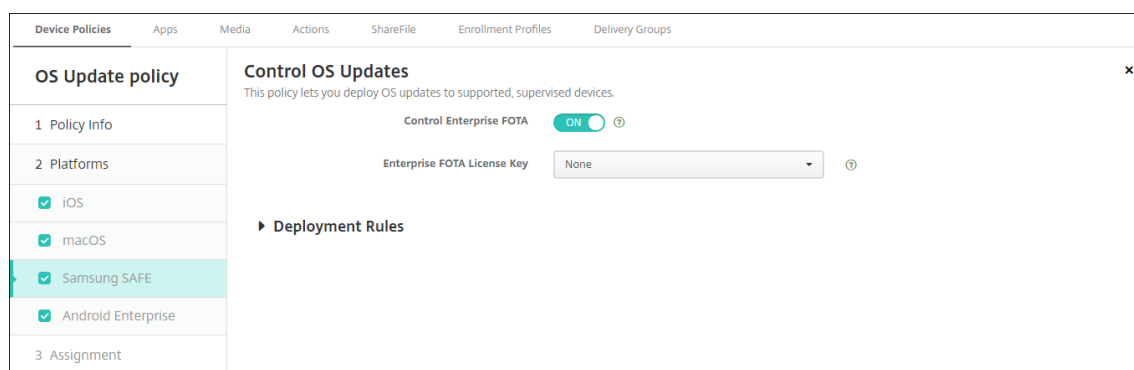
1. Crie uma política de dispositivo chave de licença de MDM Samsung com as chaves e as informações de licença que você recebeu da Samsung. O XenMobile Server valida e registra as informações. Se o XenMobile detectar um problema E-FOTA, uma mensagem de erro aparecerá para indicar o problema. Use o código fornecido para solucionar o problema. Para obter mais informações, consulte [Guias do desenvolvedor](#).

Digite a **chave de licença ELM**: o XenMobile preenche previamente esse campo com a macro que gera a chave de licença ELM. Se o campo estiver em branco, digite esta macro `#{elm.license.key}`

Digite as seguintes informações fornecidas pela Samsung quando você adquiriu um pacote E-FOTA:

- **ID de cliente do Enterprise FOTA**
- **Licença do Enterprise FOTA**
- **ID de cliente**
- **Código secreto do cliente**

2. Opcionalmente, crie uma política de dispositivo de controle de atualização de SO.



- **Ativar Enterprise FOTA:** defina como **Ativado**.

- **Chave de licença Enterprise FOTA:** selecione o nome da política de chave de licença Samsung MDM que você criou na etapa 1.
3. Implante a política de controle de atualização de sistema operacional no Secure Hub.

Configurações do Android Enterprise e Samsung KNOX

The screenshot shows the configuration page for a Samsung MDM License Key Policy. The left sidebar contains a table of contents with sections: 1 Policy Info, 2 Platforms, and 3 Assignment. Under '2 Platforms', there are three checked items: Samsung SAFE, Android Enterprise, and Samsung KNOX. The main content area is titled 'Samsung MDM License Key Policy' and includes a description: 'For the SAFE platform, use the macro to generate the ELM key. For the KNOX platform, as a prerequisite, you need to purchase a Samsung KNOX Workspace license. You then provide the license key in order to enable the KNOX APIs and deploy KNOX policies and restrictions to devices.' Below this is a text input field labeled 'KNOX license key *' and a 'Deployment Rules' section with a right-pointing arrow.

- **Chave de licença KNOX:** Digite a chave de licença KNOX que você obteve da Samsung.

Política de dispositivo de firewall do Samsung SAFE

July 10, 2020

Essa política permite que você defina as configurações de firewall dos dispositivos Samsung. Você insere os endereços IP, as portas e os nomes de host que deseja permitir ou bloquear. Você também pode definir o proxy e as configurações de redirecionamento do proxy.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do Samsung SAFE

- **Permitir/Negar Hosts:** para cada host ao qual você deseja permitir ou negar acesso, clique em **Adicionar** e configure o seguinte:
 - **Nome do host/intervalo de IP:** o nome de host ou o intervalo de endereços IP do site que você deseja afetar.
 - **Porta/intervalo de portas:** a porta ou o intervalo de portas.
 - **Permitir/negar filtro de regra:** clique em **Lista branca** para permitir o acesso ou clique em **Lista negra** para negar o acesso ao site.

Nota:

O console XenMobile Server inclui os termos “lista negra” e “lista branca”. Estamos alterando esses termos em uma próxima versão para “lista de bloqueio” e “lista de permissão”.

- **Configuração de redirecionamento:** para cada proxy que você deseja configurar, clique em **Adicionar** e configure o seguinte:
 - **Nome do host/intervalo de IP:** o nome de host ou o intervalo de endereços IP para o redirecionamento do proxy.
 - **Porta/intervalo de portas:** a porta ou o intervalo de portas para o redirecionamento do proxy.
 - **Proxy IP:** o endereço IP do proxy para o redirecionamento do proxy.
 - **Porta do proxy:** a porta do proxy para o redirecionamento do proxy.
- **Configuração de proxy**
 - **IP do proxy:** o endereço IP do servidor proxy.
 - **Porta:** a porta do servidor proxy.

Política de dispositivo do SCEP

April 1, 2021

Esta política permite que você configure dispositivos iOS e macOS para recuperar um certificado usando o protocolo SCEP de um servidor SCEP externo. Se você deseja entregar um certificado ao dispositivo usando o SCEP de uma PKI que esteja conectada ao XenMobile, deverá criar uma entidade PKI e um provedor PKI no modo distribuído. Para obter detalhes, consulte [Entidades PKI](#).

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

SCEP Policy	SCEP Policy
	This policy lets you create an Simple Certificate Enrollment Protocol (SCEP) profile to enable devices to obtain certificates from a Certificate Authority.
1 Policy Info	URL base *
2 Platforms	Instance name *
<input checked="" type="checkbox"/> iOS	Subject X.500 name (RFC 2253)
<input checked="" type="checkbox"/> macOS	Subject alternative names type
3 Assignment	Maximum retries
	Retry delay
	Challenge password
	Key size (bits)
	Use as digital signature
	Use for key encipherment
	SHA1/MD5 fingerprint (hexadecimal string)

- **URL base:** digite o endereço do servidor SCEP para definir para onde as solicitações SCEP são enviadas: sobre HTTP ou HTTPS. A chave privada não é enviada com a Solicitação de Assinatura de Certificado (CSR), portanto, pode ser seguro enviar a solicitação sem criptografia. No entanto, se a reutilização da senha de uso único for permitida, você deverá usar HTTPS para proteger a senha. Essa etapa é obrigatória.
- **Nome da instância:** digite qualquer cadeia de caracteres que o servidor SCEP reconheça. Por exemplo, isso poderia ser um nome de domínio, como exemplo.org. Se uma AC tiver vários certificados de AC, você poderá usar esse campo para distinguir o domínio necessário. Essa etapa é obrigatória.
- **Nome X.500 da entidade (RFC 2253):** digite a representação de um nome X.500, representado como uma matriz de Identificador de Objeto (OID) e valor. Por exemplo, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, que seria convertido em: [[[“C”, “US”]], [[“O”, “Apple Inc.”]], ..., [[“1.2.5.3”, “bar”]]]. Você pode representar OIDs como números pontilhados com atalhos para o país (C), a localidade (L), o estado (ST), a organização (O), a unidade organizacional (OU) e o nome comum (CN).
- **Tipo de nomes alternativos de assunto:** na lista, clique em um tipo de nome alternativo. A política de SCEP pode especificar um tipo de nome alternativo opcional que fornece os valores exigidos pela autoridade de certificação para a emissão de um certificado. Você pode especificar **Nenhum**, nome **RFC 822**, nome **DNS** ou **URI**.
- **Máximo de repetições:** digite o número de vezes que um dispositivo deve tentar novamente quando o servidor SCEP enviar uma resposta PENDING. O padrão é **3**.
- **Atraso entre cada repetição:** digite o número de segundos de espera entre tentativas subse-

quentes. A primeira nova tentativa é realizada sem atraso. O padrão é **10**.

- **Senha do desafio:** insira um segredo pré-compartilhado.
- **Tamanho da chave (bits):** selecione **2048** ou superior como o tamanho da chave em bits.
- **Usar como assinatura digital:** especifique se você deseja que o certificado seja usado como uma assinatura digital. Se alguém estiver usando o certificado para verificar uma assinatura digital, como para verificar se um certificado foi emitido por uma AC, o servidor SCEP verificaria se o certificado pode ser usado dessa maneira antes de utilizar a chave pública para descryptografar o hash.
- **Usar para codificação de chave:** especifique se você deseja que o certificado seja usado para codificação de chave. Se um servidor estiver usando a chave pública em um certificado fornecido por um cliente para verificar se uma parte dos dados foi criptografada usando a chave privada, o servidor primeiro verificaria se o certificado pode ser usado para codificação de chave. Em caso negativo, a operação falha.
- **Impressão digital SHA1/MD5 (cadeia de caracteres hexadecimal):** se sua AC usar HTTP, use esse campo para fornecer a impressão digital do certificado de AC que o dispositivo usa para confirmar a autenticidade da resposta da AC durante o registro. Você pode inserir uma impressão digital SHA1 ou MD5, ou selecionar um certificado para importar a respectiva assinatura.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do macOS

SCEP Policy	SCEP Policy
1 Policy Info	This policy lets you create an Simple Certificate Enrollment Protocol (SCEP) profile to enable devices to obtain certificates from a Certificate Authority.
2 Platforms	<p>URL base * <input type="text"/></p> <p>Instance name * <input type="text"/></p> <p>Subject X.500 name (RFC 2253) <input type="text"/></p> <p>Subject alternative names type <input type="text" value="None"/></p> <p>Maximum retries <input type="text" value="3"/></p> <p>Retry delay <input type="text" value="10"/></p> <p>Challenge password <input type="text"/></p> <p>Key size (bits) <input type="text" value="1024"/></p> <p>Use as digital signature <input type="radio" value="OFF"/></p> <p>Use for key encipherment <input type="radio" value="OFF"/></p> <p>SHA1/MD5 fingerprint (hexadecimal string) <input type="text"/></p>
<input type="checkbox"/> iOS	
<input checked="" type="checkbox"/> macOS	
3 Assignment	

- **URL base:** digite o endereço do servidor SCEP para definir para onde as solicitações SCEP são enviadas: sobre HTTP ou HTTPS. A chave privada não é enviada com a Solicitação de Assinatura de Certificado (CSR), portanto, pode ser seguro enviar a solicitação sem criptografia. No entanto, se a reutilização da senha de uso único for permitida, você deverá usar HTTPS para proteger a senha. Essa etapa é obrigatória.
- **Nome da instância:** digite qualquer cadeia de caracteres que o servidor SCEP reconheça. Por exemplo, isso poderia ser um nome de domínio, como exemplo.org. Se uma AC tiver vários certificados de AC, você poderá usar esse campo para distinguir o domínio necessário. Essa etapa é obrigatória.
- **Nome X.500 da entidade (RFC 2253):** digite a representação de um nome X.500, representado como uma matriz de Identificador de Objeto (OID) e valor. Por exemplo, /C=US/O=Apple Inc./CN=foo/1.2.5.3=bar, que seria convertido em: [[[“C”, “US”]], [[“O”, “Apple Inc.”]], ..., [[“1.2.5.3”, “bar”]]]. Você pode representar OIDs como números pontilhados com atalhos para o país (C), a localidade (L), o estado (ST), a organização (O), a unidade organizacional (OU) e o nome comum (CN).
- **Tipo de nomes alternativos de assunto:** na lista, clique em um tipo de nome alternativo. A política de SCEP pode especificar um tipo de nome alternativo opcional que fornece os valores exigidos pela autoridade de certificação para a emissão de um certificado. Você pode especificar **Nenhum**, nome **RFC 822**, nome **DNS** ou **URI**.
- **Máximo de repetições:** digite o número de vezes que um dispositivo deve tentar novamente quando o servidor SCEP enviar uma resposta PENDING. O padrão é **3**.

- **Atraso entre cada repetição:** digite o número de segundos de espera entre tentativas subsequentes. A primeira nova tentativa é realizada sem atraso. O padrão é **10**.
- **Senha do desafio:** digite um segredo pré-compartilhado.
- **Tamanho da chave (bits):** selecione **2048** ou superior como o tamanho da chave em bits.
- **Usar como assinatura digital:** especifique se você deseja que o certificado seja usado como uma assinatura digital. Se alguém estiver usando o certificado para verificar uma assinatura digital, como para verificar se um certificado foi emitido por uma AC, o servidor SCEP verificaria se o certificado pode ser usado dessa maneira antes de utilizar a chave pública para descryptografar o hash.
- **Usar para codificação de chave:** especifique se você deseja que o certificado seja usado para codificação de chave. Se um servidor estiver usando a chave pública em um certificado fornecido por um cliente para verificar se uma parte dos dados foi criptografada usando a chave privada, o servidor primeiro verificaria se o certificado pode ser usado para codificação de chave. Em caso negativo, a operação falha.
- **Impressão digital SHA1/MD5 (cadeia de caracteres hexadecimal):** se sua AC usar HTTP, use esse campo para fornecer a impressão digital do certificado de AC que o dispositivo usa para confirmar a autenticidade da resposta da AC durante o registro. Você pode inserir uma impressão digital SHA1 ou MD5, ou selecionar um certificado para importar a respectiva assinatura.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra.
 - **Permitir que o usuário remova a política:** você pode selecionar quando os usuários podem remover a política do dispositivo. Selecione **Sempre**, **Código secreto obrigatório** ou **Nunca** no menu. Se você selecionar **Código secreto obrigatório**, digite um código secreto no campo **Código secreto de remoção**.
 - **Escopo do perfil:** selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

Siri e políticas de ditado

April 15, 2019

Quando os usuários perguntam algo à Siri ou ditam texto em dispositivos iOS gerenciados, a Apple coleta de dados de voz para fins de melhorar a Siri. Os dados de voz a passam por serviços da Apple baseados na nuvem e, portanto, existem fora do contêiner seguro XenMobile. O texto que resultada do ditado, no entanto, permanece no contêiner.

O XenMobile permite que você bloqueie a Siri e os serviços de ditado de acordo com o que determinam suas necessidades de segurança.

Em implantações de MAM, a política **Bloquear ditado** para cada aplicativo é **ativada** por padrão, o que desativa o microfone do dispositivo. Defina como **Desativado** se você quiser permitir o ditado. Você pode encontrar a política no console XenMobile em **Configurar > Aplicativos**. Selecione o aplicativo, clique em **Editar** e, em seguida, clique em **iOS**.

MDX	App Restrictions
1 App Information	Block camera <input checked="" type="checkbox"/> ON ?
2 Platform	Block Photo Library <input checked="" type="checkbox"/> ON ?
<input checked="" type="checkbox"/> iOS	Block mic record <input checked="" type="checkbox"/> ON ?
<input type="checkbox"/> Android	Block dictation <input type="checkbox"/> OFF ?
<input type="checkbox"/> Windows Phone	Block location services <input checked="" type="checkbox"/> ON ?
<input type="checkbox"/> Windows Desktop/Tablet	Block SMS compose <input checked="" type="checkbox"/> ON ?
3 Approvals (optional)	
4 Delivery Group Assignments (optional)	

Em implantações MDM, você também pode desabilitar a Siri com a política da Siri em **Configurar > Políticas de dispositivo**. O uso do Siri é permitido por padrão.

Restrictions Policy	Restrictions Policy
1 Policy Info	This policy allows or restricts users from using certain features on their devices, such as the camera media content and on certain types of apps users can and cannot install.
2 Platforms	Allow hardware controls
<input checked="" type="checkbox"/> iOS	<div style="display: flex; justify-content: space-between;"> <div> <p>Camera <input checked="" type="checkbox"/></p> <p>FaceTime <input checked="" type="checkbox"/></p> <p>Screen shots <input checked="" type="checkbox"/></p> <p>Photo streams <input checked="" type="checkbox"/> iOS 5.0+</p> <p>Shared photo streams <input checked="" type="checkbox"/> iOS 6.0+</p> <p>Voice dialing <input checked="" type="checkbox"/></p> <p>Siri <input checked="" type="checkbox"/></p> <p><input checked="" type="checkbox"/> Allow while device is locked</p> <p><input type="checkbox"/> Siri profanity filter</p> </div> </div>
<input checked="" type="checkbox"/> macOS	
<input checked="" type="checkbox"/> Samsung SAFE	
<input checked="" type="checkbox"/> Samsung KNOX	
<input checked="" type="checkbox"/> Windows Phone	
<input checked="" type="checkbox"/> Windows Desktop/Tablet	
<input checked="" type="checkbox"/> Amazon	
<input checked="" type="checkbox"/> Windows Mobile/CE	

Alguns poucos pontos para levar em consideração ao decidir se deseja permitir a Siri e ditado:

- De acordo com as informações que a Apple divulgou, a Apple mantém dados da Siri e de clip de voz por até dois anos. É atribuído um número aleatório a esses para representar o usuário e os arquivos de voz arquivos são associados a este número aleatório. Para obter mais informações, consulte este artigo da Wired, [Apple reveals how long Siri keeps your data](#).
- Você pode revisar a política de privacidade da Apple acessando **Configurações > Geral > Teclados** em qualquer dispositivo iOS e tocando no link em **Ativar ditado**.

Políticas de dispositivo de conta SSO

April 23, 2020

Crie contas de logon único (SSO) no XenMobile para permitir que os usuários façam logon somente uma vez para acessar o XenMobile e seus recursos internos da empresa de diversos aplicativos. Os usuários não precisam armazenar nenhuma credencial no dispositivo. As credenciais do usuário empresarial da conta SSO são usadas entre aplicativos, incluindo os aplicativos da App Store. Essa política foi desenvolvida para funcionar com um back-end de autenticação Kerberos.

Essa política se aplica ao iOS 7.0 e versões posteriores.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

- **Nome da conta:** insira o nome de conta SSO Kerberos que é exibida nos dispositivos dos usuários. Este campo é obrigatório.
- **Nome principal Kerberos:** insira o nome principal Kerberos. Este campo é obrigatório.
- **Credencial de identidade (keystore ou credencial PKI):** na lista, clique em uma credencial de identidade opcional que pode ser usada para renovar a credencial do Kerberos sem a interação do usuário.
- **Realm Kerberos:** insira o realm Kerberos dessa política. Geralmente, ele é o seu nome de domínio em letras maiúsculas (por exemplo, EXEMPLO.COM). Este campo é obrigatório.
- **URLs permitidas:** para cada URL para a qual você deseja exigir o SSO, clique em **Adicionar** e faça o seguinte:
 - **URL Permitida:** insira uma URL para a qual você deseja exigir o SSO quando um usuário visitar a URL do dispositivo iOS.
Por exemplo, quando um usuário tenta navegar para um site e o site inicia um desafio Kerberos, se esse site não estiver na lista de URLs, o dispositivo iOS não tentará realizar o SSO fornecendo o token Kerberos que o Kerberos pode ter em cache no dispositivo de um login anterior no Kerberos. A correspondência precisa ser exata na parte do host da URL. Por exemplo, <https://shopping.apple.com> é válido, mas https://*.apple.com não é.
Além disso, se o Kerberos não estiver ativado com base no host correspondente, a URL ainda retornará para uma chamada HTTP padrão. Isso pode significar quase qualquer coisa, inclusive um desafio de senha padrão ou um erro HTTP, se a URL estiver configurada para SSO somente usando o Kerberos.
 - Clique em **Adicionar** para adicionar a URL ou em **Cancelar** para cancelar a adição da URL.
- **Identificadores de aplicativo:** para cada aplicativo que tem permissão para usar esse login, clique em **Adicionar** e faça o seguinte:
 - **Identificador de aplicativo:** insira um identificador de aplicativo para um aplicativo que tem permissão para usar esse login. Se você não adicionar nenhum identificador de aplicativo, esse login corresponderá a **todos** os identificadores de aplicativo.
 - Clique em **Adicionar** para adicionar o identificador de aplicativo ou em **Cancelar** para cancelar a adição do identificador de aplicativo.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Política de dispositivo de criptografia de armazenamento

January 22, 2021

Crie políticas de dispositivo de criptografia de armazenamento no XenMobile para criptografar o armazenamento interno e externo, e, dependendo do dispositivo, para impedir que os usuários usem um cartão de armazenamento nos respectivos dispositivos.

Você pode criar políticas para dispositivos Samsung SAFE e Windows Phone. Cada plataforma exige um conjunto diferente de valores, que são descritos em detalhes neste artigo.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Pré-requisitos

Para dispositivos Samsung SAFE, certifique-se de que os seguintes requisitos sejam atendidos antes de configurar esta política:

- Defina a opção Bloqueio de tela nos dispositivos do usuário.
- Conecte dispositivos de usuários e carregue-os pelo menos a 80%.
- Certifique-se de que os dispositivos exijam uma senha contendo números e letras ou símbolos.

Definir as configurações do Samsung SAFE

- **Criptografar armazenamento interno:** selecione se o armazenamento interno deve ser criptografado nos dispositivos dos usuários. O armazenamento interno inclui a memória e o armazenamento interno do dispositivo. O padrão é **On**.
- **Criptografar armazenamento externo:** selecione se o armazenamento externo deve ser criptografado nos dispositivos dos usuários. O padrão é **On**.

Configurações do Windows Phone

- **Exigir criptografia do dispositivo:** selecione se os dispositivos dos usuários devem ser criptografados. O padrão é **Off**.
- **Desativar cartão de armazenamento:** selecione se os usuários devem ser impedidos de usar um cartão de memória nos respectivos dispositivos. O padrão é **Off**.

Política de dispositivo de loja

April 23, 2020

Você pode criar uma política no XenMobile para especificar se os dispositivos iOS, Android ou Tablet Windows exibem um clipe Web do XenMobile Store na tela inicial dos dispositivos.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações da plataforma

Para cada plataforma que você configurar, selecione se o clipe Web da XenMobile Store aparece nos dispositivos dos usuários. O padrão é **On**.

Política de dispositivo de Calendários inscritos

April 23, 2020

Você pode adicionar uma política de dispositivo ao XenMobile para adicionar um calendário inscrito à lista de calendários nos dispositivos iOS. A lista de calendários públicos nos quais você pode se inscrever está disponível em www.apple.com/downloads/macosx/calendars.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Pré-requisito

Você deve estar inscrito em um calendário antes de poder adicioná-lo à lista de calendários inscritos nos dispositivos do usuário.

Configurações de iOS

- **Descrição:** insira uma descrição do calendário. Este campo é obrigatório.
- **URL:** insira a URL do calendário. Você pode inserir um URL `webcal://` ou um link `https://` em um arquivo do iCalendar (.ics). Este campo é obrigatório.
- **Nome de usuário:** insira o nome de usuário de login. Este campo é obrigatório.
- **Senha:** insira uma senha de usuário opcional.

- **Usar SSL:** selecione se deseja usar uma conexão Secure Socket Layer no calendário. O padrão é **Off**.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Política de dispositivo dos termos e condições

April 23, 2020

Crie as políticas de dispositivo dos termos e condições no XenMobile quando desejar que os usuários aceitem as políticas específicas da empresa que regem as conexões à rede corporativa. Quando os usuários registram seus dispositivos no XenMobile, eles visualizam os termos e condições e devem aceitá-los para registrar os dispositivos. Não aceitar os termos e condições cancela o processo de registro.

Você pode criar políticas diferentes para os termos e condições em idiomas diferentes, caso sua empresa tenha usuários internacionais e você deseje que eles aceitem os termos e condições em seus idiomas nativos. Você deve fornecer um arquivo para cada combinação de plataforma e idioma que planeja implantar. Em dispositivos iOS e Android, você deve fornecer arquivos PDF. Em dispositivos Windows, você deve fornecer os arquivos de texto (.txt) e os arquivos de imagem complementares.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do iOS e do Android

- **Arquivo a ser importado:** selecione o arquivo de termos e condições a ser importado clicando em **Procurar** e navegando até a localização do arquivo.
- **Termos e condições padrão:** selecione se este arquivo é o documento padrão para os usuários que são membros de vários grupos com termos e condições diferentes. O padrão é **Off**.

Configurações do Windows Phone e do Tablet Windows

- **Arquivo a ser importado:** selecione o arquivo de termos e condições a ser importado clicando em **Procurar** e navegando até a localização do arquivo.

- **Imagem:** selecione o arquivo de imagem a ser importado clicando em **Procurar** e navegando até a localização do arquivo.
- **Termos e condições padrão:** selecione se este arquivo é o documento padrão para os usuários que são membros de vários grupos com termos e condições diferentes. O padrão é **Off**.

Política de dispositivo de VPN

April 8, 2021

A política de dispositivo de VPN define as configurações de rede virtual privada (VPN) que permitem que os dispositivos do usuário se conectem com segurança a recursos corporativos. Você pode configurar a política de dispositivo de VPN para as seguintes plataformas. Cada plataforma exige um conjunto diferente de valores, que são descritos em detalhes neste artigo.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Requisitos para VPNs por aplicativo

Você configura o recurso VPN por aplicativo para as seguintes plataformas por meio de políticas de VPN:

- iOS
- macOS
- Android (DA legado)
- Samsung SAFE
- Samsung Knox

Para configurar VPNs para dispositivos Android Enterprise, crie uma política de dispositivo de configuração gerenciada do Android Enterprise para o aplicativo Citrix SSO. Consulte [Configurar perfis VPN para Android Enterprise](#).

As opções de VPN por aplicativo estão disponíveis para determinados tipos de conexão. A tabela a seguir indica quando as opções VPN por aplicativo estão disponíveis.

Plataforma	Tipo de conexão	Observação
iOS	Cisco Legacy AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix SSO ou SSL personalizado.	
macOS	Cisco AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA ou SSL personalizado.	
Android (DA legado)	Citrix SSO	
Samsung SAFE	IPSEC, SSL	Tipo de VPN definido como Genérico
Samsung Knox	IPSEC, SSL	Tipo de VPN definido como Genérico

Para criar uma VPN por aplicativo para dispositivos iOS e Android (DA legado) usando o aplicativo Citrix SSO, você precisa executar etapas extras, além da configuração da política de VPN. Além disso, você deve verificar se os seguintes pré-requisitos foram atendidos:

- Citrix Gateway no local
- Os seguintes aplicativos estão instalados no dispositivo:
 - Citrix SSO
 - Citrix Secure Hub

Um fluxo de trabalho geral para configurar uma VPN por aplicativo para dispositivos iOS e Android usando o aplicativo Citrix SSO:

1. Configure uma política de dispositivo de VPN como descrito neste artigo.
 - Para *iOS*, consulte [Configurar o protocolo Citrix SSO para iOS](#). Depois de configurar o protocolo Citrix SSO para iOS por meio de uma política de dispositivo de VPN, você também precisa criar uma política de atributos do aplicativo para associar um aplicativo à política de VPN por aplicativo. Para obter mais informações, consulte [Configurar uma VPN por aplicativo](#).
 - No campo **Tipo de autenticação da conexão**, se você selecionar **Certificado**, deverá primeiro configurar a autenticação baseada em certificado para o Endpoint Management. Consulte [Autenticação de certificado cliente ou certificado e domínio](#).
 - Para *Android (DA legado)*, consulte [Configurar o protocolo Citrix SSO para Android](#).

- No campo **Tipo de autenticação da conexão**, se você selecionar **Certificado** ou **Senha e certificado**, deverá primeiro configurar a autenticação baseada em certificado para o Endpoint Management. Consulte [Autenticação de certificado cliente ou certificado e domínio](#).
- 2. Configure o Citrix ADC para aceitar o tráfego da VPN por aplicativo. Para obter detalhes, consulte [Configuração de VPN completa no Citrix Gateway](#).

Configurações de iOS

Para se preparar para atualizações de dispositivos para o iOS 12:

o tipo de conexão Citrix VPN na política de dispositivo de VPN para iOS não suporta o iOS 12. Execute estas etapas para excluir sua política de dispositivo VPN existente e criar uma política de dispositivo de VPN com o tipo de conexão Citrix SSO:

1. Exclua sua política de dispositivo de VPN para iOS.
2. Adicione uma política de dispositivo de VPN para iOS. Configurações importantes:
 - **Tipo de conexão = Citrix SSO**
 - **Ativar VPN por aplicativo = Ativado**
 - **Tipo de provedor = Túnel de pacote**
3. Adicione uma política de dispositivo de Atributos de Aplicativo para iOS. Para **Identificador VPN por aplicativo**, escolha **iOS_VPN**.

VPN Policy	VPN Policy
1 Policy Info	This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.
2 Platforms	<p>Connection name <input type="text"/></p> <p>Connection type <input type="text" value="L2TP"/></p> <p>Server name or IP address * <input type="text"/></p> <p>User account <input type="text"/></p> <p> <input checked="" type="radio"/> Password authentication <input type="radio"/> RSA SecureID authentication </p> <p>Shared secret <input type="text"/></p> <p>Send all traffic <input type="text" value="OFF"/></p> <p>Proxy configuration <input type="text" value="None"/></p>
<input checked="" type="checkbox"/> iOS <input checked="" type="checkbox"/> macOS <input checked="" type="checkbox"/> Android <input checked="" type="checkbox"/> Samsung SAFE <input checked="" type="checkbox"/> Samsung KNOX <input checked="" type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Desktop/Tablet <input checked="" type="checkbox"/> Amazon	Proxy
3 Assignment	

- **Nome da conexão:** digite um nome para a conexão.
- **Tipo de conexão:** na lista, selecione o protocolo a ser usado para esta conexão. O padrão é **L2TP**.
 - **L2TP:** Protocolo de Encapsulamento de Camada 2 com autenticação de chave pré-compartilhada.

- **PPTP:** Encapsulamento Ponto a Ponto.
- **IPSec:** sua conexão VPN corporativa.
- **Cisco Legacy AnyConnect:** este tipo de conexão requer que o cliente VPN Cisco Legacy AnyConnect esteja instalado no dispositivo do usuário. A Cisco está desativando o cliente Cisco Legacy AnyConnect que foi baseado em uma estrutura VPN agora obsoleta. Para obter mais informações, consulte o artigo de suporte <https://support.citrix.com/article/CTX227708>.
Para usar o cliente Cisco AnyConnect atual, use um **Tipo de conexão de SSL personalizado**. Para ver as configurações necessárias, consulte “Configurar o protocolo SSL personalizado” nesta seção.
- **Juniper SSL:** cliente VPN Juniper Networks SSL.
- **F5 SSL:** cliente VPN F5 Networks SSL.
- **SonicWALL Mobile Connect:** cliente VPN unificado Dell para iOS.
- **Ariba VIA:** cliente Ariba Networks Virtual Internet Access.
- **IKEv2 (somente iOS):** Internet Key Exchange versão 2 somente para iOS.
- **AlwaysOn IKEv2:** acesso sempre ativo usando IKEv2.
- **Configuração dupla de AlwaysOn IKEv2:** acesso sempre ativo usando a configuração dupla IKEv2.
- **Citrix SSO:** cliente Citrix SSO para iOS 12 e posterior.
- **SSL personalizado:** protocolo SSL personalizado. Esse tipo de conexão é necessário para o cliente Cisco AnyConnect que possui um ID de pacote do **com.cisco.anyconnect**. Especifique um **nome de conexão** do **Cisco AnyConnect**. Você também pode implantar a política de VPN e habilitar um filtro de Controle de Acesso da Rede (NAC) para dispositivos iOS. O filtro bloqueia a conexão VPN a dispositivos que têm aplicativos não compatíveis instalados. A configuração requer configurações específicas para a política de VPN do iOS, conforme descrito na seção iOS a seguir. Para obter mais informações sobre outras configurações necessárias para habilitar o filtro NAC, consulte [Controle de Acesso da Rede](#).

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Configurar o protocolo L2TP para iOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- Selecione **Autenticação por senha** ou **Autenticação RSA SecurID**.
- **Segredo compartilhado:** digite a chave secreta compartilhada do IPsec.
- **Enviar todo o tráfego:** selecione se todo o tráfego deve ser enviado sobre a VPN. O padrão é **Off**.

Configurar o protocolo PPTP para iOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- Selecione **Autenticação por senha** ou **Autenticação RSA SecurID**.
- **Nível de criptografia:** na lista, selecione um nível de criptografia. O padrão é **Nenhum**.
 - **Nenhum:** não use criptografia.
 - **Automático:** use o nível de criptografia mais forte compatível com o servidor.
 - **Máximo (128 bits):** use sempre criptografia de 128 bits.
- **Enviar todo o tráfego:** selecione se todo o tráfego deve ser enviado sobre a VPN. O padrão é **Off**.

Configurar o protocolo IPsec para iOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Tipo de autenticação da conexão:** na lista, selecione **Segredo compartilhado** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Segredo Compartilhado**.
- Se você ativar a opção **Segredo compartilhado**, defina as seguintes configurações:
 - **Nome do grupo:** digite um nome de grupo opcional.
 - **Segredo compartilhado:** digite uma chave secreta compartilhada opcional.
 - **Usar autenticação híbrida:** selecione se a autenticação híbrida deve ser usada. Com a autenticação híbrida, o primeiro servidor autentica a si mesmo no cliente e, em seguida, o cliente autentica a si mesmo no servidor. O padrão é **Off**.
 - **Solicitar senha:** selecione se as senhas dos usuários devem ser solicitadas quando eles se conectarem à rede. O padrão é **Off**.
- Se você ativar a opção **Certificado**, configure as seguintes definições:
 - **Credencial de identidade:** na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
 - **Solicitar PIN ao conectar:** selecione se os usuários serão obrigados a inserir o respectivo PIN quando se conectarem à rede. O padrão é **Off**.
 - **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte [Definir as configurações de Ativar VPN sob demanda para iOS](#).
- **Ativar VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**.
- **Correspondência de aplicativo sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do VPN

por aplicativo iniciam a comunicação de rede. O padrão é **Off**.

- **Domínios Safari:** clique em **Adicionar** para adicionar um nome de domínio do Safari.

Configurar o protocolo AnyConnect Cisco legado para iOS

Para fazer a transição do cliente Cisco AnyConnect legado para o novo cliente Cisco AnyConnect, use o protocolo SSL personalizado.

- **Identificador de pacote de provedor:** para o cliente Legacy AnyConnect, o ID do pacote é com.cisco.anyconnect.gui.
- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Grupo:** digite um nome de grupo opcional.
- **Tipo de autenticação da conexão:** na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
 - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
 - Se você ativar a opção **Certificado**, configure as seguintes definições:
 - * **Credencial de identidade:** na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
 - * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **Off**.
 - * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte [Definir as configurações de Ativar VPN sob demanda para iOS](#).
- **Ativar VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Se você ativar essa opção, defina estas configurações:
 - **Correspondência de aplicativo sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede. O padrão é **Off**.
 - **Tipo de provedor:** selecione se a VPN por aplicativo é fornecida como um **Proxy de aplicativo** ou como um **Túnel de pacote**. O padrão é **Proxy de aplicativo**.
 - **Domínios do Safari:** para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
 - * **Domínio:** digite o domínio a ser adicionado.
 - * Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.

Configurar o protocolo Juniper SSL para iOS

- **Identificador de pacote de provedor:** se o seu perfil VPN por aplicativo contiver o identificador de pacote de um aplicativo com vários provedores VPN do mesmo tipo, especifique o provedor a ser usado aqui.
- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Realm:** digite um nome de realm opcional.
- **Função:** digite um nome de função opcional.
- **Tipo de autenticação da conexão:** na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
 - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
 - Se você ativar a opção **Certificado**, configure as seguintes definições:
 - * **Credencial de identidade:** na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
 - * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **Off**.
 - * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte [Definir as configurações de Ativar VPN sob demanda para iOS](#).
- **Ativar VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Se você ativar essa opção, defina estas configurações:
 - **Correspondência de aplicativo sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede. O padrão é **Off**.
 - **Tipo de provedor:** selecione se a VPN por aplicativo é fornecida como um **Proxy de aplicativo** ou como um **Túnel de pacote**. O padrão é **Proxy de aplicativo**.
 - **Domínios do Safari:** para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
 - * **Domínio:** digite o domínio a ser adicionado.
 - * Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.

Configurar o protocolo F5 SSL para iOS

- **Identificador de pacote de provedor:** se o seu perfil VPN por aplicativo contiver o identificador de pacote de um aplicativo com vários provedores VPN do mesmo tipo, especifique o provedor

a ser usado aqui.

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Tipo de autenticação da conexão:** na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
 - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
 - Se você ativar a opção **Certificado**, configure as seguintes definições:
 - * **Credencial de identidade:** na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
 - * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **Off**.
 - * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte [Definir as configurações de Ativar VPN sob demanda para iOS](#).
- **Ativar VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Se você ativar essa opção, defina estas configurações:
 - **Correspondência de aplicativo sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede.
 - **Tipo de provedor:** selecione se a VPN por aplicativo é fornecida como um **Proxy de aplicativo** ou como um **Túnel de pacote**. O padrão é **Proxy de aplicativo**.
 - **Domínios do Safari:** para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
 - * **Domínio:** digite o domínio a ser adicionado.
 - * Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.

Configurar o protocolo SonicWALL para iOS

- **Identificador de pacote de provedor:** se o seu perfil VPN por aplicativo contiver o identificador de pacote de um aplicativo com vários provedores VPN do mesmo tipo, especifique o provedor a ser usado aqui.
- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Grupo ou domínio de login:** digite um grupo ou domínio de login opcional.
- **Tipo de autenticação da conexão:** na lista, selecione **Senha** ou **Certificado** para o tipo de

autenticação dessa conexão. O padrão é **Senha**.

- Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
- Se você ativar a opção **Certificado**, configure as seguintes definições:
 - * **Credencial de identidade:** na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
 - * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **Off**.
 - * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte [Definir as configurações de Ativar VPN sob demanda para iOS](#).
- **Ativar VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Se você definir essa opção como **I**, defina estas configurações:
 - **Correspondência de aplicativo sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede.
 - **Tipo de provedor:** selecione se a VPN por aplicativo é fornecida como um **Proxy de aplicativo** ou como um **Túnel de pacote**. O padrão é **Proxy de aplicativo**.
 - **Domínios do Safari:** para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
 - * **Domínio:** digite o domínio a ser adicionado.
 - * Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.

Configurar o protocolo Ariba VIA para iOS

- **Identificador de pacote de provedor:** se o seu perfil VPN por aplicativo contiver o identificador de pacote de um aplicativo com vários provedores VPN do mesmo tipo, especifique o provedor a ser usado aqui.
- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Tipo de autenticação da conexão:** na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
 - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
 - Se você ativar a opção **Certificado**, configure as seguintes definições:
 - * **Credencial de identidade:** na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.

- * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **Off**.
- * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte [Definir as configurações de Ativar VPN sob demanda para iOS](#).
- **Ativar VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Se você ativar essa opção, defina estas configurações:
 - **Correspondência de aplicativo sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede.
 - **Domínios do Safari:** para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
 - * **Domínio:** digite o domínio a ser adicionado.
 - * Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.

Configurar protocolos IKEv2 para iOS

Essa seção inclui as configurações usadas para os protocolos IKEv2, AlwaysOn IKEv2 e AlwaysOn IKEv2 Dual Configuration. Para o protocolo Configuração dupla de AlwaysOn IKEv2, configure todas essas configurações para redes celulares e Wi-Fi.

- **Permitir que o usuário desative a conexão automática:** para os protocolos AlwaysOn. Selecione se os usuários têm permissão para desativar a conexão automática com a rede em seus dispositivos. O padrão é **Off**.
- **Nome de host ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Identificador local:** o FQDN ou o endereço IP do cliente IKEv2. Este campo é obrigatório.
- **Identificador remoto:** o FQDN ou o endereço IP do servidor VPN. Este campo é obrigatório.
- **Autenticação do dispositivo:** escolha **Segredo compartilhado**, **Certificado** ou **Certificado do dispositivo baseado no identificador do dispositivo** para o tipo de autenticação dessa conexão. O padrão é **Segredo Compartilhado**.
 - Se você escolher **Segredo compartilhado**, digite uma chave secreta compartilhada opcional.
 - Se você escolher **Certificado**, escolha uma **Credencial de identidade** a ser usada. O padrão é **Nenhum**.

- Se você escolher **Certificado do dispositivo baseado no identificador do dispositivo**, escolha o **Tipo de identidade do dispositivo** a ser usado. O padrão é **IMEI**. Para usar essa opção, importe os certificados em massa usando a API REST. Consulte [Carregar certificados para dispositivos iOS em massa com a API REST](#). Disponível somente quando você seleciona **AlwaysOn IKEv2**.
- **Autenticação estendida ativada:** selecione se o Protocolo de autenticação estendido (EAP) deve ser ativado. Se você escolher **I**, digite a **Conta de usuário** e a **Senha de autenticação**.
- **Intervalo de DPD:** escolha quantas vezes um dispositivo par é contactado, para garantir que ele permaneça acessível. O padrão é **Nenhum**. As opções são:
 - **Nenhum:** desative a detecção de par inativo.
 - **Baixo:** entra em contato com o par a cada 30 minutos.
 - **Médio:** entra em contato com o par a cada 10 minutos.
 - **Alto:** entra em contato com o par a cada 1 minuto.
- **Desativar mobilidade e multihoming:** escolha se deseja desativar esse recurso.
- **Usar atributos de sub-rede interna IPv4/IPv6:** escolha se deseja ativar esse recurso.
- **Desativar redirecionamentos:** escolha se deseja desativar redirecionamentos.
- **Ativar keepalive NAT enquanto o dispositivo está no modo de suspensão:** para os protocolos AlwaysOn. Pacotes de keepalive mantêm mapeamentos NAT para conexões IKEv2. O chip envia esses pacotes em intervalos regulares quando o dispositivo está ativo. Se esta configuração for **I**, o chip envia pacotes de keepalive mesmo enquanto o dispositivo estiver no modo de suspensão. O padrão é 20 segundos por Wi-Fi e 110 segundos via rede celular. Você pode alterar o intervalo usando o parâmetro Intervalo de NAT keepalive.
- **Intervalo de keepalive NAT (segundos):** o padrão é 20 segundos.
- **Ativar o Perfect Forward Secrecy:** escolha se deseja ativar este recurso.
- **Endereços IP do servidor DNS:** opcional. Uma lista de configurações de endereços IP de servidores DNS. Esses endereços IP podem incluir uma mistura de endereços IPv4 e IPv6. Clique em **Adicionar** para digitar um endereço.
- **Nome de domínio:** opcional. O domínio principal do túnel.
- **Domínios de pesquisa:** opcional. Uma lista de domínios usada para qualificar totalmente nomes de host de rótulo único.
- **Acrescentar domínios correspondentes suplementares à lista do resolvedor:** opcional. Determina se a lista de domínios correspondentes complementares será ou não adicionada à lista de domínios de pesquisa do resolvedor. O padrão é **Ativado**.

- **Domínios correspondentes suplementares:** opcional. Uma lista de cadeias de domínios usada para determinar as consultas DNS que devem usar as configurações de resolvidor DNS contidas nos endereços de servidor DNS. Essa chave cria uma configuração de DNS dividido em que somente os hosts em determinados domínios resolvem usando o resolvidor DNS do túnel. Os hosts que não estejam em um dos domínios nessa são resolvidos por meio do resolvidor padrão do sistema.

Se esse parâmetro contiver uma cadeia vazia, esta será o domínio padrão. É assim que uma configuração de túnel dividido pode direcionar todas as consultas DNS para os servidores DNS da VPN antes dos servidores DNS primários. Se o túnel VPN for a rota padrão da rede, os servidores DNS listados serão o resolvidor padrão. Nesse caso, a lista de domínios correspondentes suplementares é ignorada.

- **Parâmetros IKE SA e Parâmetros SA filho.** Defina estas configurações para cada opção de parâmetros de Associação de segurança (SA):
 - **Algoritmo de criptografia:** na lista, selecione o algoritmo de criptografia IKE a ser usado. O padrão é **3DES**.
 - **Algoritmo de integridade:** na lista, selecione o algoritmo de integridade a ser usado. O padrão é **SHA1-96**.
 - **Grupo Diffie Hellman:** na lista, selecione o número do grupo Diffie Hellman. O padrão é **2**.
 - **Vida útil ike em minutos:** digite um inteiro entre 10 e 1.440 que representa o tempo de vida SA (intervalo de chaveamento). O padrão é **1440** minutos.
- **Exceções de serviço:** para os protocolos AlwaysOn. Exceções de serviço são serviços do sistema isentos da VPN AlwaysOn. Defina estas configurações de exceções de serviço:
 - **Correio de voz:** na lista, selecione como lidar com a exceção de correio de voz. O padrão é **Permitir tráfego através do túnel**.
 - **AirPrint:** na lista, selecione como lidar com a exceção do AirPrint. O padrão é **Permitir tráfego através do túnel**.
 - **Permitir o tráfego de folha web cativa fora do túnel VPN:** selecione se deseja permitir que os usuários se conectem a pontos de acesso públicos fora do túnel da VPN. O padrão é **Off**.
 - **Permitir o tráfego de todos os aplicativos de rede cativos fora do túnel VPN:** selecione se deseja permitir todos os aplicativos de rede do ponto de acesso fora do túnel da VPN. O padrão é **Off**.
 - **Identificadores de pacote de aplicativos de rede cativos:** para cada identificador de pacote de aplicativos de rede hotspot que os usuários têm permissão para acessar, clique

em **Adicionar** e digite o **Identificador de pacote** de aplicativos de rede hotspot. Clique em **Salvar** para salvar o identificador de pacote de aplicativos.

- **VPN por aplicativo.** Definir estas configurações para tipos de conexão IKEv2.
 - **Ativar VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**.
 - **Correspondência de aplicativo sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede. O padrão é **Off**.
 - **Domínios Safari:** clique em **Adicionar** para adicionar um nome de domínio do Safari.
- **Configuração de proxy:** escolha como a conexão VPN é direcionada por meio de um servidor proxy. O padrão é **Nenhum**.

Configurar o protocolo Citrix SSO para iOS

O cliente Citrix SSO está disponível na Apple Store em <https://apps.apple.com/us/app/citrix-sso/id1333396910>.

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Tipo de autenticação da conexão:** na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
 - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
 - Se você ativar a opção **Certificado**, configure as seguintes definições:
 - * **Credencial de identidade:** na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
 - * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **O**.
 - * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **O**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte [Definir as configurações de Ativar VPN sob demanda para iOS](#).
- **Ativar VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Se você definir essa opção como **I**, defina estas configurações:
 - **Correspondência de aplicativo sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede.

- **Tipo de provedor:** selecione se a VPN por aplicativo é fornecida como um **Proxy de aplicativo** ou como um **Túnel de pacote**. O padrão é **Proxy de aplicativo**.
- **Tipo de provedor:** defina como **Túnel de pacote**.
- **Domínios do Safari:** para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
 - * **Domínio:** digite o domínio a ser adicionado.
 - * Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.
- **XML personalizado:** para cada parâmetro XML personalizado que você deseja adicionar, clique em **Adicionar** e especifique os pares de chave/valor. Os parâmetros disponíveis são:
 - **disableL3:** desativa a VPN de nível de sistema. Permite somente uma VPN por aplicativo. Nenhum **valor** é necessário.
 - **useragent:** associa a esta política de dispositivo todas as políticas do Citrix Gateway que são direcionadas a clientes de plug-in VPN. Para as solicitações iniciadas pelo plug-in, o **valor** dessa chave é anexado automaticamente ao plug-in VPN.

Configurar o protocolo SSL personalizado para iOS

Para fazer a transição do cliente Cisco Legacy AnyConnect para o cliente Cisco AnyConnect:

1. Configure a política de dispositivo de VPN com o protocolo SSL personalizado. Implemente a política em dispositivos iOS.
2. Faça o upload do cliente Cisco AnyConnect de <https://apps.apple.com/us/app/cisco-anyconnect/id1135064690>, adicione o aplicativo ao XenMobile e implemente o aplicativo em dispositivos iOS.
3. Remova a política de dispositivo de VPN antiga de dispositivos iOS.

Configurações:

- **Identificador SSL personalizado (formato DNS inverso):** defina o identificador de pacote. Para o cliente Cisco AnyConnect, use **com.cisco.anyconnect**.
- **Identificador de pacote de provedor:** se o aplicativo especificado em **Identificador SSL personalizado** tiver vários provedores VPN do mesmo tipo (proxy de aplicativo ou túnel de pacote), especifique esse identificador de pacote. Para o cliente Cisco AnyConnect, use **com.cisco.anyconnect**.
- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Tipo de autenticação da conexão:** na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
 - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
 - Se você ativar a opção **Certificado**, configure as seguintes definições:

- * **Credencial de identidade:** na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
- * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **O**.
- * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **O**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte [Definir as configurações de Ativar VPN sob demanda para iOS](#).
- **Ativar VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Se você definir essa opção como **I**, defina estas configurações:
 - **Correspondência de aplicativo sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede.
 - **Tipo de provedor:** um tipo de provedor indica se o provedor é um serviço de VPN ou serviço de proxy. No caso de serviço de VPN, escolha **Túnel de pacote**. No caso de serviço de proxy, escolha **Proxy de aplicativo**. No caso de cliente Cisco AnyConnect, escolha **Túnel de pacote**.
 - **Domínios do Safari:** para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
 - * **Domínio:** digite o domínio a ser adicionado.
 - * Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.
- **XML personalizado:** para cada parâmetro XML personalizado que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
 - **Nome do parâmetro:** digite o nome do parâmetro a ser adicionado.
 - **Valor:** digite o valor associado ao **Nome do parâmetro**.
 - Clique em **Salvar** para salvar o parâmetro ou clique em **Cancelar** para não salvar.

Configurar a política de dispositivo de VPN para suportar NAC

1. O **Tipo de conexão** de **SSL Personalizado** é necessário para configurar o filtro NAC.
2. Especifique um **Nome de conexão** de **VPN**.
3. Para **identificador SSL personalizado**, digite **com.citrix.NetScalerGateway.ios.app**
4. Para **Identificador de pacote de provedor**, digite **com.citrix.netScalergateWay.ios.app.vpnPlugin**

Os valores nas etapas 3 e 4 provêm da instalação necessária do Citrix SSO para a filtragem NAC. Você não configura uma senha de autenticação. Para obter mais informações sobre como usar a função NAC, consulte [Controle de Acesso da Rede](#).

Configurar as opções de Ativar VPN sob demanda para iOS

- **Domínio On Demand:** para cada domínio e ação associada a executar quando os usuários se conectam, clique em **Adicionar** e faça o seguinte:
- **Domínio:** digite o domínio a ser adicionado.
- **Ação:** na lista, selecione uma das ações possíveis:
 - **Sempre estabelecer:** o domínio sempre aciona uma conexão VPN.
 - **Nunca estabelecer:** o domínio nunca aciona uma conexão VPN.
 - **Estabelecer, se necessário:** o domínio dispara uma tentativa de conexão VPN se a resolução de nomes de domínio falhar. Uma falha ocorre quando o servidor DNS não pode resolver o domínio, redireciona para um servidor diferente ou atinge o tempo limite.
 - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.
- **Regras on demand**
 - **Ação:** na lista, selecione a ação a ser tomada. O padrão é **EvaluateConnection**. As ações possíveis são:
 - * **Permitir:** permitir que a VPN sob demanda se conecte quando acionada.
 - * **Conectar:** iniciar incondicionalmente uma conexão VPN.
 - * **Desconectar:** remover a conexão VPN e não se reconectar sob demanda, desde que a regra seja correspondida.
 - * **EvaluateConnection:** avaliar a matriz ActionParameters de cada conexão.
 - * **Ignorar:** manter todas as conexões VPN existentes ativas, mas não se reconectar sob demanda, desde que a regra seja correspondida.
 - **DNSDomainMatch:** para cada domínio em relação ao qual a lista de domínios de pesquisa de um dispositivo pode corresponder que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
 - * **Domínio DNS:** digite o nome de domínio. Você pode usar o prefixo do caractere curinga “*” para correspondência de vários domínios. Por exemplo, *.exemplo.com corresponde a meudominio.exemplo.com, seudominio.exemplo.com e dominiodela.exemplo.com.
 - * Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.
 - **DNSServerAddressMatch:** para cada endereço IP ao qual qualquer um dos servidores DNS especificados da rede pode corresponder que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
 - * **Endereço de servidor DNS:** digite o endereço de servidor DNS que você deseja adicionar. Você pode usar o sufixo do caractere curinga “*” para correspondência de servidores DNS. Por exemplo, 17.* corresponde a qualquer servidor DNS na sub-rede da classe A.
 - * Clique em **Salvar** para salvar o endereço do servidor DNS ou clique em **Cancelar** para não salvar.
 - **InterfaceTypeMatch:** na lista, selecione o tipo de hardware primário de interface de rede

em uso. O padrão é **Não especificado**. Os valores possíveis são:

- * **Não especificado**: corresponde qualquer interface de rede de hardware. Esta opção é o padrão.
- * **Ethernet**: corresponde somente a hardware de interface de rede Ethernet.
- * **WiFi**: corresponde somente a hardware de interface de rede Wi-Fi.
- * **Celular**: corresponde somente a hardware de interface de rede Celular.
- **SSIDMatch**: para cada SSID a ser correspondido em relação à rede atual que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
 - * **SSID**: digite o SSID a ser adicionado. Se a rede não for uma rede Wi-Fi ou se o SSID não for exibido, a correspondência falhará. Deixe essa lista vazia para corresponder a qualquer SSID.
 - * Clique em **Salvar** para salvar o SSID ou clique em **Cancelar** para não salvar.
- **URLStringProbe**: digite uma URL a ser obtida. Se essa URL for obtida com êxito sem redirecionamento, essa regra será correspondida.
- **ActionParameters : Domains**: para cada domínio que EvaluateConnection verifica que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
 - * **Domínio**: digite o domínio a ser adicionado.
 - * Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.
- **ActionParameters : DomainAction**: na lista, selecione o **comportamento da VPN** dos domínios **ActionParameters : Domains** especificados. O padrão é **ConnectIfNeeded**. As ações possíveis são:
 - * **ConnectIfNeeded**: o domínio dispara uma tentativa de conexão VPN se a resolução de nomes de domínio falhar. Uma falha ocorre quando o servidor DNS não pode resolver o domínio, redireciona para um servidor diferente ou atinge o tempo limite.
 - * **NeverConnect**: o domínio nunca aciona uma conexão VPN.
- **ActionParameters : RequiredDNSServers**: para cada endereço IP do servidor DNS que deve ser usado para resolver os domínios especificados, clique em **Adicionar** e faça o seguinte:
 - * **Servidor DNS**: válido somente quando **ActionParameters : DomainAction = ConnectIfNeeded**. Digite o servidor DNS a ser adicionado. Esse servidor não precisa fazer parte da configuração de rede atual do dispositivo. Se o servidor DNS não estiver acessível, uma conexão VPN será estabelecida na resposta. Esse servidor DNS deve ser um servidor DNS interno ou um servidor DNS externo confiável.
 - * Clique em **Salvar** para salvar o servidor DNS ou clique em **Cancelar** para não salvar.
- **ActionParameters : RequiredURLStringProbe**: opcionalmente, digite uma URL HTTP ou HTTPS (preferencial) a ser investigada usando uma solicitação GET. Se o nome do host da URL não puder ser resolvido, se o servidor estiver inacessível ou se o servidor não responder, uma conexão VPN será estabelecida. Válido somente quando **ActionParameters : DomainAction = ConnectIfNeeded**.

- **OnDemandRules : XML content:** digite ou copie e cole as regras on demand da configuração XML.
 - * Clique em **Verificar dicionário** para validar o código XML. Você verá XML válido em texto verde abaixo da caixa de texto **Conteúdo XML** se o XML for válido. Se não for válido, você verá uma mensagem de erro em texto laranja descrevendo o erro.
- **Proxy**
 - **Configuração de proxy:** na lista, selecione como a conexão VPN é direcionada por meio de um servidor proxy. O padrão é **Nenhum**.
 - * Se você ativar a opção **Manual**, configure as seguintes definições:
 - **Nome do host ou endereço IP do servidor proxy:** digite o nome do host ou o endereço IP do servidor proxy. Este campo é obrigatório.
 - **Porta do servidor proxy:** digite o número da porta do servidor proxy. Este campo é obrigatório.
 - **Nome de usuário:** digite um nome de usuário opcional do servidor proxy.
 - **Senha:** digite uma senha opcional do servidor proxy.
 - * Se você configurar **Automático**, defina esta configuração:
 - **URL do servidor proxy:** digite a URL do servidor proxy. Este campo é obrigatório.
- **Configurações de política**
 - Em **Configurações de política**, ao lado de **Remover política**, selecione **Selecionar data** ou em **Duração até remoção (em horas)**.
 - Se você selecionar **Selecionar data**, clique no calendário para selecionar a data específica para remoção.
 - Na lista **Permitir que o usuário remova a política**, selecione **Sempre**, **Senha obrigatória** ou **Nunca**.
 - Se você selecionar **Senha obrigatória**, ao lado de **Senha de remoção**, digite a senha necessária.

Configurar uma VPN por aplicativo

Opções de VPN por aplicativo para o iOS estão disponíveis para estes tipos de conexão: Cisco AnyConnect legado, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix VPN, Citrix SSO e SSL personalizado.

Para configurar uma VPN por aplicativo:

1. Em **Configurar > Políticas de dispositivo**, crie uma política de VPN. Por exemplo:

VPN Policy

1 Policy Info

2 Platforms

iOS

macOS

Android

Samsung SAFE

Samsung KNOX

Windows Phone

Windows Desktop/Tablet

Amazon

3 Assignment

VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

Connection name:

Connection type:

Custom SSL identifier (reverse DNS format) *:

Provider bundle identifier:

Server name or IP address *:

User account:

Authentication type for the connection:

Auth Password:

Per-app VPN

Enable per-app VPN: ON OFF iOS 7.0+

On-demand match app enabled: ON OFF

Provider type:

Safari domains

Back Next >

VPN Policy

1 Policy Info

2 Platforms

iOS

macOS

Android

Samsung SAFE

Samsung KNOX

Windows Phone

Windows Desktop/Tablet

Amazon

3 Assignment

Enable per-app VPN: ON OFF iOS 7.0+

On-demand match app enabled: ON OFF

Provider type:

Safari domains

Domain *: Add

Custom XML

Custom parameters

Parameter name *	Value
<input type="text" value=""/>	<input type="text" value=""/>

Proxy

Proxy configuration:

Policy Settings

Remove policy: Select date Duration until removal (in hours)

Allow user to remove policy:

► Deployment Rules

Back Next >

2. Em **Configurar > Políticas de dispositivo**, crie uma política de atributos de aplicativo para associar um aplicativo à política de VPN por aplicativo. Para **Identificador de VPN por aplicativo**, escolha o nome da política de VPN criado na etapa 1. Para **ID de pacote de aplicativos gerenciados**, escolha a lista de aplicativos ou digite a ID do pacote de aplicativos. (Se você implantar um política de inventário de aplicativos iOS, a lista de aplicativos conterá aplicativos).

App Attributes Policy

1 Policy Info

2 Platforms

iOS

3 Assignment

App Attributes Policy

This policy lets you specify the attributes you want to add to apps on iOS devices.

Managed app bundle ID *:

Per-app VPN identifier:

► Deployment Rules

- **Configurações de política**

- **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do macOS

The screenshot displays the 'VPN Policy' configuration window. On the left, a sidebar lists various platforms, with 'macOS' selected. The main configuration area includes the following fields and options:

- Connection name:** A text input field.
- Connection type:** A dropdown menu currently set to 'L2TP'.
- Server name or IP address:** A text input field.
- User account:** A text input field containing 'administrator'.
- Authentication:** Radio buttons for 'Password authentication' (selected), 'RSA SecureID authentication', 'Kerberos authentication', and 'CryptoCard authentication'.
- Shared secret:** A text input field with masked characters.
- Send all traffic:** A toggle switch currently set to 'OFF'.
- Proxy configuration:** A dropdown menu currently set to 'None'.
- Remove policy:** Radio buttons for 'Select date' (selected) and another unselected option.

At the bottom right, there are 'Back' and 'Next >' buttons.

- **Nome da conexão:** digite um nome para a conexão.
- **Tipo de conexão:** na lista, selecione o protocolo a ser usado para esta conexão. O padrão é L2TP.
 - **L2TP:** Protocolo de Encapsulamento de Camada 2 com autenticação de chave pré-compartilhada.
 - **PPTP:** Encapsulamento Ponto a Ponto.
 - **IPSec:** sua conexão VPN corporativa.
 - **Cisco AnyConnect:** cliente VPN Cisco AnyConnect.
 - **Juniper SSL:** cliente VPN Juniper Networks SSL.
 - **F5 SSL:** cliente VPN F5 Networks SSL.
 - **SonicWALL Mobile Connect:** cliente VPN unificado Dell para iOS.
 - **Ariba VIA:** cliente Ariba Networks Virtual Internet Access.
 - **Citrix VPN:** cliente Citrix VPN.
 - **SSL personalizado:** protocolo SSL personalizado.

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Configurar o protocolo L2TP para macOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- Selecione a **Autenticação de senha**, **Autenticação RSA SecurID**, **Autenticação Kerberos** ou **Autenticação CryptoCard**. O padrão é **Autenticação de senha**.
- **Segredo compartilhado:** digite a chave secreta compartilhada do IPsec.
- **Enviar todo o tráfego:** selecione se todo o tráfego deve ser enviado sobre a VPN. O padrão é **Off**.

Configurar o protocolo PPTP para macOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- Selecione a **Autenticação de senha**, **Autenticação RSA SecurID**, **Autenticação Kerberos** ou **Autenticação CryptoCard**. O padrão é **Autenticação de senha**.
- **Nível de criptografia:** selecione o nível de criptografia desejado. O padrão é **Nenhum**.
 - **Nenhum:** não use criptografia.
 - **Automático:** use o nível de criptografia mais forte compatível com o servidor.
 - **Máximo (128 bits):** use sempre criptografia de 128 bits.
- **Enviar todo o tráfego:** selecione se todo o tráfego deve ser enviado sobre a VPN. O padrão é **Off**.

Configurar o protocolo IPsec para macOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Tipo de autenticação da conexão:** na lista, selecione **Segredo compartilhado** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Segredo Compartilhado**.
 - Se você ativar a autenticação **Segredo compartilhado**, defina as seguintes configurações:
 - * **Nome do grupo:** digite um nome de grupo opcional.
 - * **Segredo compartilhado:** digite uma chave secreta compartilhada opcional.
 - * **Usar autenticação híbrida:** selecione se a autenticação híbrida deve ser usada. Com a autenticação híbrida, o primeiro servidor autentica a si mesmo no cliente e, em seguida, o cliente autentica a si mesmo no servidor. O padrão é **Off**.

- * **Solicitar senha:** selecione se as senhas dos usuários devem ser solicitadas quando eles se conectarem à rede. O padrão é **Off**.
- Se você ativar a autenticação de **Certificado**, defina estas configurações:
 - * **Credencial de identidade:** na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
 - * **Solicitar PIN ao conectar:** selecione se os usuários serão obrigados a inserir o respectivo PIN quando se conectarem à rede. O padrão é **Off**.
 - * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Configurar as opções de Ativar VPN sob demanda.

Configurar o protocolo Cisco AnyConnect para macOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Grupo:** digite um nome de grupo opcional.
- **Tipo de autenticação da conexão:** na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
 - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
 - Se você ativar a opção **Certificado**, configure as seguintes definições:
 - * **Credencial de identidade:** na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
 - * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **Off**.
 - * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Configurar as opções de Ativar VPN sob demanda.
- **Ativar VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Se você ativar essa opção, defina estas configurações:
 - * **Correspondência de aplicativo sob demanda ativada:** selecione se uma conexão VPN por aplicativo é acionada automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede. O padrão é **Off**.
 - * **Domínios do Safari:** para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
 - **Domínio:** digite o domínio a ser adicionado.
 - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.

Configurar o protocolo SSL do Juniper para macOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Realm:** digite um nome de realm opcional.
- **Função:** digite um nome de função opcional.
- **Tipo de autenticação da conexão:** na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
 - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
 - Se você ativar a opção **Certificado**, configure as seguintes definições:
 - * **Credencial de identidade:** na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
 - * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **Off**.
 - * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Definir as configurações de Ativar VPN sob demanda.
- **Ativar VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Se você ativar essa opção, defina estas configurações:
 - **Correspondência de aplicativo sob demanda ativada:** selecione se uma conexão VPN por aplicativo é acionada automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede. O padrão é **Off**.
 - **Domínios do Safari:** para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
 - * **Domínio:** digite o domínio a ser adicionado.
 - * Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.

Configurar o protocolo F5 SSL para macOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Tipo de autenticação da conexão:** na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
 - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
 - Se você ativar a opção **Certificado**, configure as seguintes definições:

- * **Credencial de identidade:** na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
- * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **Off**.
- * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Definir as configurações de Ativar VPN sob demanda.
- **Ativar VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Se você ativar essa opção, defina estas configurações:
 - **Correspondência de aplicativo sob demanda ativada:** selecione se uma conexão VPN por aplicativo é acionada automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede. O padrão é **Off**.
 - **Domínios do Safari:** para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
 - * **Domínio:** digite o domínio a ser adicionado.
 - * Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.

Configurar o protocolo SonicWALL Mobile Connect para macOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Grupo ou domínio de login:** digite um grupo ou domínio de login opcional.
- **Tipo de autenticação da conexão:** na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
 - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
 - Se você ativar a opção **Certificado**, configure as seguintes definições:
 - * **Credencial de identidade:** na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
 - * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **Off**.
 - * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Definir as configurações de Ativar VPN sob demanda.
- **Ativar VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Se você ativar essa opção, defina estas configurações:
 - **Correspondência de aplicativo sob demanda ativada:** selecione se uma conexão VPN

por aplicativo é acionada automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede. O padrão é **Off**.

- **Domínios do Safari:** para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
 - * **Domínio:** digite o domínio a ser adicionado.
 - * Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.

Configurar o protocolo Ariba VIA para macOS

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN.
- **Conta de usuário:** digite uma conta de usuário opcional.
- **Tipo de autenticação da conexão:** na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
 - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
 - Se você ativar a opção **Certificado**, configure as seguintes definições:
 - * **Credencial de identidade:** na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
 - * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **Off**.
 - * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **Off**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Definir as configurações de Ativar VPN sob demanda.
- **Ativar VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Se você ativar essa opção, defina estas configurações:
 - **Correspondência de aplicativo sob demanda ativada:** selecione se uma conexão VPN por aplicativo é acionada automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede. O padrão é **Off**.
 - **Domínios do Safari:** para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
 - * **Domínio:** digite o domínio a ser adicionado.
 - * Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.

Configurar o protocolo SSL personalizado para macOS

- **Identificador SSL personalizado (formato DNS inverso):** digite o identificador SSL no formato de DNS inverso. Este campo é obrigatório.

- **Nome ou endereço IP do servidor:** digite o nome do servidor ou o endereço IP do servidor VPN. Este campo é obrigatório.
- **Conta de usuário:** digite uma conta de usuário opcional.
 - **Tipo de autenticação da conexão:** na lista, selecione **Senha** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Senha**.
 - Se você ativar **Senha**, digite uma senha de autenticação opcional no campo **Senha de autenticação**.
 - Se você ativar a opção **Certificado**, configure as seguintes definições:
 - * **Credencial de identidade:** na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
 - * **Solicitar PIN ao conectar:** selecione se o PIN dos usuários será solicitado quando eles se conectarem à rede. O padrão é **O**.
 - * **Ativar VPN sob demanda:** selecione se deve ser ativado o acionamento de uma conexão VPN quando os usuários se conectarem à rede. O padrão é **O**. Para obter informações sobre como definir as configurações quando a opção **Ativar VPN sob demanda** estiver **I**, consulte Definir as configurações de Ativar VPN sob demanda.
 - **VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. O padrão é **Off**. Se você ativar essa opção, defina estas configurações:
 - * **Correspondência de aplicativo sob demanda ativada:** selecione se as conexões VPN por aplicativo são acionadas automaticamente quando os aplicativos vinculados ao serviço do VPN por aplicativo iniciam a comunicação de rede.
 - * **Domínios do Safari:** para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você deseja incluir, clique em **Adicionar** e faça o seguinte:
 - **Domínio:** digite o domínio a ser adicionado.
 - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.
- **XML personalizado:** para cada parâmetro XML personalizado que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
 - **Nome do parâmetro:** digite o nome do parâmetro a ser adicionado.
 - **Valor:** digite o valor associado ao **Nome do parâmetro**.
 - Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.

Configurar as opções de Ativar VPN sob demanda

- **Domínio On Demand:** para cada domínio e ação associada a ser tomada quando os usuários se conectarem a eles que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
 - **Domínio:** digite o domínio a ser adicionado.
 - **Ação:** na lista, selecione uma das ações possíveis:
 - * **Sempre estabelecer:** o domínio sempre aciona uma conexão VPN.
 - * **Nunca estabelecer:** o domínio nunca aciona uma conexão VPN.
 - * **Estabelecer, se necessário:** o domínio dispara uma tentativa de conexão VPN se a

resolução de nomes de domínio falhar. Uma falha ocorre quando o servidor DNS não pode resolver o domínio, redireciona para um servidor diferente ou atinge o tempo limite.

- Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.

- **Regras on demand**

- **Ação:** na lista, selecione a ação a ser tomada. O padrão é **EvaluateConnection**. As ações possíveis são:

- * **Permitir:** permitir que a VPN sob demanda se conecte quando acionada.
- * **Conectar:** iniciar incondicionalmente uma conexão VPN.
- * **Desconectar:** remover a conexão VPN e não se reconectar sob demanda, desde que a regra seja correspondida.
- * **EvaluateConnection:** avaliar a matriz **ActionParameters** de cada conexão.
- * **Ignorar:** manter todas as conexões VPN existentes ativas, mas não se reconectar sob demanda, desde que a regra seja correspondida.

- **DNSDomainMatch:** para cada domínio em relação ao qual a lista de domínios de pesquisa de um dispositivo do usuário pode corresponder que você deseja adicionar, clique em **Adicionar** e faça o seguinte:

- * **Domínio DNS:** digite o nome de domínio. Você pode usar o prefixo do caractere curinga "*" para correspondência de vários domínios. Por exemplo, *.exemplo.com corresponde a meudominio.exemplo.com, seudominio.exemplo.com e dominiodela.exemplo.com.

- * Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.

- **DNSServerAddressMatch:** para cada endereço IP ao qual qualquer um dos servidores DNS especificados da rede pode corresponder que você deseja adicionar, clique em **Adicionar** e faça o seguinte:

- * **Endereço de servidor DNS:** digite o endereço de servidor DNS que você deseja adicionar. Você pode usar o sufixo do caractere curinga "*" para correspondência de servidores DNS. Por exemplo, 17.* corresponde a qualquer servidor DNS na sub-rede da classe A.

- * Clique em **Salvar** para salvar o endereço do servidor DNS ou clique em **Cancelar** para não salvar.

- **InterfaceTypeMatch:** na lista, clique no tipo de hardware primário de interface de rede em uso. O padrão é **Não especificado**. Os valores possíveis são:

- * **Não especificado:** corresponde qualquer interface de rede de hardware. Esta opção é o padrão.
- * **Ethernet:** corresponde somente a hardware de interface de rede Ethernet.
- * **WiFi:** corresponde somente a hardware de interface de rede Wi-Fi.
- * **Celular:** corresponde somente a hardware de interface de rede Celular.

- **SSIDMatch:** para cada SSID a ser correspondido em relação à rede atual que você deseja

adicionar, clique em **Adicionar** e faça o seguinte.

- * **SSID:** digite o SSID a ser adicionado. Se a rede não for uma rede Wi-Fi ou se o SSID não for exibido, a correspondência falhará. Deixe essa lista vazia para corresponder a qualquer SSID.
- * Clique em **Salvar** para salvar o SSID ou clique em **Cancelar** para não salvar.
- **URLStringProbe:** digite uma URL a ser obtida. Se essa URL for obtida com êxito sem redirecionamento, essa regra será correspondida.
- **ActionParameters : Domains:** para cada domínio que EvaluateConnection verifica que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
 - * **Domínio:** digite o domínio a ser adicionado.
 - * Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.
- **ActionParameters : DomainAction:** na lista, selecione o **comportamento da VPN** dos domínios **ActionParameters : Domains** especificados. O padrão é **ConnectIfNeeded**. As ações possíveis são:
 - * **ConnectIfNeeded:** o domínio dispara uma tentativa de conexão VPN se a resolução de nomes de domínio falhar. Uma falha ocorre quando o servidor DNS não pode resolver o domínio, redireciona para um servidor diferente ou atinge o tempo limite.
 - * **NeverConnect:** o domínio nunca aciona uma conexão VPN.
- **ActionParameters: RequiredDNSServers:** para cada endereço IP do servidor DNS que deve ser usado para resolver os domínios especificados, clique em **Adicionar** e faça o seguinte:
 - * **Servidor DNS:** válido somente quando **ActionParameters : DomainAction = ConnectIfNeeded**. Digite o servidor DNS a ser adicionado. Esse servidor não precisa fazer parte da configuração de rede atual do dispositivo. Se o servidor DNS não estiver acessível, uma conexão VPN será estabelecida na resposta. Esse servidor DNS deve ser um servidor DNS interno ou um servidor DNS externo confiável.
 - * Clique em **Salvar** para salvar o servidor DNS ou clique em **Cancelar** para não salvar.
- **ActionParameters : RequiredURLStringProbe:** opcionalmente, digite uma URL HTTP ou HTTPS (preferencial) a ser investigada usando uma solicitação GET. Se o nome do host da URL não puder ser resolvido, se o servidor estiver inacessível ou se o servidor não responder, uma conexão VPN será estabelecida. Válido somente quando **ActionParameters : DomainAction = ConnectIfNeeded**.
- **OnDemandRules : XML content:** digite ou copie e cole as regras on demand da configuração XML.
 - * Clique em **Verificar dicionário** para validar o código XML. Você verá XML válido em texto verde abaixo da caixa de texto **Conteúdo XML** se o XML for válido. Se não for válido, você verá uma mensagem de erro em texto laranja descrevendo o erro.

- **Proxy**

- **Configuração de proxy:** na lista, selecione como a conexão VPN é direcionada por meio

de um servidor proxy. O padrão é **Nenhum**.

- * Se você ativar a opção **Manual**, configure as seguintes definições:
 - **Nome do host ou endereço IP do servidor proxy:** digite o nome do host ou o endereço IP do servidor proxy. Este campo é obrigatório.
 - **Porta do servidor proxy:** digite o número da porta do servidor proxy. Este campo é obrigatório.
 - **Nome de usuário:** digite um nome de usuário opcional do servidor proxy.
 - **Senha:** digite uma senha opcional do servidor proxy.
- * Se você configurar **Automático**, defina esta configuração:
 - **URL do servidor proxy:** digite a URL do servidor proxy. Este campo é obrigatório.

Configurações do Android

The screenshot shows the 'VPN Policy' configuration window. On the left, a sidebar lists 'Platforms' with 'Android', 'Samsung SAFE', and 'Samsung KNOX' checked. The main configuration area includes:

- Connection name ***: text input field.
- Server name or IP address ***: text input field.
- Connection type**: dropdown menu set to 'Cisco AnyConnect'.
- Identity credential**: dropdown menu set to 'None'.
- Backup VPN server**: text input field.
- User group**: text input field.
- Automatic VPN policy**: toggle switch set to 'OFF'.

Configurar o protocolo Cisco AnyConnect VPN para Android

- **Nome da conexão:** digite um nome para a conexão VPN do Cisco AnyConnect. Este campo é obrigatório.
- **Nome do host ou endereço IP:** digite o nome ou endereço IP do servidor de VPN. Este campo é obrigatório.
- **Credencial de identidade:** na lista, selecione uma credencial de identidade.
- **Servidor VPN de backup:** digite as informações do servidor VPN de backup.
- **Grupo de usuários:** digite as informações do grupo de usuários.
- **Redes Confiáveis**
 - **Política VPN automática:** ative ou desative essa opção para definir a forma como o VPN reage a redes confiáveis e não confiáveis. Se essa opção estiver ativada, defina as seguintes configurações:
 - * **Política de rede confiável:** na lista, selecione a política desejada. O padrão é **Desconectar**. As opções possíveis são:

- **Desconectar:** o cliente encerra a conexão VPN na rede confiável. Essa configuração é a padrão.
- **Conectar:** o cliente inicia uma conexão VPN na rede confiável.
- **Não fazer nada:** o cliente não toma nenhuma ação.
- **Pausar:** quando um usuário estabelece uma sessão VPN fora da rede confiável e, em seguida, entra em uma rede configurada como confiável, a sessão VPN é suspensa. Quando o usuário deixa a rede confiável novamente, a sessão é retomada. Essa configuração elimina a necessidade de estabelecer uma nova sessão VPN após a saída de uma rede confiável.
- * **Política de rede não confiável:** na lista, selecione a política desejada. O padrão é **Conectar**. As opções possíveis são:
 - **Conectar:** o cliente inicia uma conexão VPN na rede não confiável.
 - **Não fazer nada:** o cliente inicia uma conexão VPN na rede não confiável. Esta opção desativa a VPN sempre conectada.
- **Domínios confiáveis:** para cada sufixo de domínio que a interface de rede tem quando o cliente está na rede confiável, clique em **Adicionar** para fazer o seguinte:
 - * **Domínio:** digite o domínio a ser adicionado.
 - * Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.
- **Servidores confiáveis:** para cada endereço de servidor que uma interface de rede tem quando o cliente está na rede confiável, clique em **Adicionar** e faça o seguinte:
 - * **Servidores:** digite o servidor a ser adicionado.
 - * Clique em **Salvar** para salvar o servidor ou clique em **Cancelar** para não salvar.

Configurar o protocolo Citrix SSO para Android

- **Nome da conexão:** digite um nome para a conexão VPN. Este campo é obrigatório.
- **Nome ou endereço IP do servidor:** digite o FQDN ou endereço IP do Citrix Gateway.
- **Tipo de autenticação da conexão:** escolha um tipo de autenticação e preencha qualquer um dos campos que são exibidos para o tipo:
 - **Nome de usuário e Senha:** digite suas credenciais VPN para os **Tipos de autenticação** de **Senha** ou **Senha e certificado**. Opcional. Se você não fornecer as credenciais VPN, o aplicativo Citrix VPN solicitará um nome de usuário e senha.
 - **Credencial de identidade:** é exibida para os **Tipos de autenticação** de **Certificado** ou **Senha e certificado**. Na lista, selecione uma credencial de identidade.
- **Ativar VPN por aplicativo:** selecione se a VPN por aplicativo deve ser ativada. Se você não ativar VPN por aplicativo, todo o tráfego passa pelo do túnel do Citrix VPN. Se você ativar VPN por aplicativo, especifique as configurações a seguir. O padrão é **Off**.

- **Lista branca** ou **lista negra**: se **Lista branca**, todos os aplicativos permitidos passam pelo túnel através dessa VPN. Se **Lista negra**, todos os aplicativos, exceto os aplicativos que estão na lista de bloqueio, passam pelo túnel através dessa VPN.

Nota:

O console XenMobile Server inclui os termos “lista negra” e “lista branca”. Estamos alterando esses termos em uma próxima versão para “lista de bloqueio” e “lista de permissão”.

- **Lista de aplicativos**: especifique os aplicativos permitidos ou bloqueados. Clique em **Adicionar** e, em seguida, digite uma lista separada por vírgulas de nomes de pacote de aplicativo.
- **XML personalizado**: clique em **Adicionar** e, em seguida, digite parâmetros personalizados. O XenMobile é compatível com estes parâmetros para Citrix VPN:
 - **DisableUserProfiles**: Opcional. Para ativar esse parâmetro, digite **Sim** para o **Valor**. Se ativado, o XenMobile não exibirá conexões de VPN adicionadas pelo usuário, e o usuário não poderá adicionar uma conexão. Essa configuração é uma restrição global e se aplica a todos os perfis de VPN.
 - **userAgent**: um valor de cadeia de caracteres. Você pode especificar uma cadeia de caracteres de Agente do Usuário personalizada para enviar em cada solicitação HTTP. A cadeia de caracteres do agente de usuário especificado é acrescentada ao agente de usuário existente do Citrix VPN.

Configurar VPNs para oferecer suporte a NAC

1. Use o **Tipo de conexão** de **SSL Personalizado** para configurar o filtro NAC.
2. Especifique um **Nome de conexão** de **VPN**.
3. Em **XML personalizado**, clique em **Adicionar** e faça o seguinte:
 - **Nome do parâmetro**: digite **XenMobileDeviceId**. Esse campo é o ID do dispositivo a ser usado para a verificação NAC com base no registro do dispositivo no XenMobile. Se o XenMobile registrar e gerenciar o dispositivo, a conexão VPN será permitida. Caso contrário, a autenticação será negada no momento do estabelecimento da VPN.
 - **Valor**: digite **DeviceID_\${device.id}**, que é o valor do parâmetro **XenMobileDeviceId**.
 - Clique em **Salvar** para salvar o parâmetro.

Configurar VPNs para Android Enterprise

Para configurar VPNs para dispositivos Android Enterprise, crie uma política de dispositivo de configuração gerenciada do Android Enterprise para o aplicativo Citrix SSO. Consulte [Configurar perfis VPN para Android Enterprise](#).

Configurações do Samsung SAFE

VPN Policy	VPN Policy
1 Policy Info	This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.
2 Platforms	<p>Connection name * <input type="text" value="K--PPTP"/></p> <p>Vpn Type <input type="text" value="PPTP"/></p> <p>Host name * <input type="text"/></p> <p>User name <input type="text" value="testuser"/></p> <p>Password <input type="password" value="....."/></p> <p>Enable encryption <input type="checkbox"/> OFF</p> <p>► Deployment Rules</p>
<input type="checkbox"/> iOS <input type="checkbox"/> macOS <input checked="" type="checkbox"/> Android <input checked="" type="checkbox"/> Samsung SAFE <input checked="" type="checkbox"/> Samsung KNOX <input type="checkbox"/> Windows Phone <input type="checkbox"/> Windows Desktop/Tablet <input type="checkbox"/> Amazon	
3 Assignment	

- **Nome da conexão:** digite um nome para a conexão.
- **Tipo de VPN:** na lista, selecione o protocolo a ser usado para esta conexão. O padrão é **L2TP com chave pré-compartilhada**. As opções possíveis são:
 - **L2TP com chave pré-compartilhada:** Protocolo de Encapsulamento de Camada 2 com autenticação de chave pré-compartilhada. Essa configuração é a padrão.
 - **L2TP com certificado:** protocolo de encapsulamento de camada 2 com certificado.
 - **PPTP:** Encapsulamento Ponto a Ponto.
 - **IPSec:** sua conexão VPN corporativa. Aplicável a versões de SAFE anteriores à versão 2.0.
 - **Genérico:** uma conexão VPN genérica. Aplicável à versão 2.0 de SAFE ou superiores.

Configure o L2TP com o protocolo de chave pré-compartilhada para o Samsung SAFE

- **Nome do host:** digite o nome do host VPN. Essa opção é necessária.
- **Nome de usuário:** digite um nome de usuário opcional.
- **Senha:** digite uma senha opcional.
- **Chave pré-compartilhada:** digite a chave pré-compartilhada. Essa opção é necessária.

Configurar o L2TP com o protocolo de certificado para o Samsung SAFE

- **Nome do host:** digite o nome do host VPN. Essa opção é necessária.
- **Nome de usuário:** digite um nome de usuário opcional.
- **Senha:** digite uma senha opcional.
- **Credencial de identidade:** na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.

Configurar o protocolo PPTP para o Samsung SAFE

- **Nome do host:** digite o nome do host VPN. Essa opção é necessária.
- **Nome de usuário:** digite um nome de usuário opcional.
- **Senha:** digite uma senha opcional.
- **Ativar criptografia:** selecione se a criptografia deve ser ativada na conexão VPN.

Configurar o protocolo Empresa para o Samsung SAFE

- **Nome do host:** digite o nome do host VPN. Essa opção é necessária.
- **Ativar servidor de backup:** selecione se um servidor VPN de backup deve ser ativado. Se ativado, no **servidor VPN de backup**, digite o FQDN ou o endereço IP do servidor VPN de backup.
- **Ativar autenticação do usuário:** selecione se deseja exigir autenticação do usuário. Se essa opção estiver ativada, defina as seguintes configurações:
 - **Nome de usuário:** digite um nome de usuário.
 - **Senha:** digite a senha de usuário.
- **Nome do grupo:** digite um nome de grupo opcional.
- **Método de autenticação:** na lista, selecione o método de autenticação que deve ser usado. As opções possíveis são:
 - **Certificado:** use a autenticação de certificado. Essa configuração é a padrão. Se selecionada, na lista de **Credenciais de identidade**, selecione a credencial a ser usada. O padrão é **Nenhum**.
 - **Chave pré-compartilhada:** use uma chave pré-compartilhada. Se selecionado, no campo **Chave pré-compartilhada**, digite a chave secreta compartilhada.
 - **RSA híbrido:** use a autenticação híbrida usando certificados RSA.
 - **EAP MD5:** autentique o par EAP no servidor EAP, mas não realize a autenticação mútua.
 - **EAP MSCHAPv2:** use a autenticação de handshake de desafio da Microsoft para autenticação mútua.
- **Certificado de CA:** na lista, selecione o certificado a ser usado. O padrão é **Nenhum**.
- **Ativar rota padrão:** selecione se uma rota padrão deve ser ativada para o servidor VPN. O padrão é **Off**.
- **Ativar a autenticação de cartão inteligente:** selecione se os usuários têm permissão para autenticar usando cartões inteligentes. O padrão é **Off**.
- **Ativar opção móvel:** selecione se a opção móvel deve ser ativada. O padrão é **Off**.
- **Valor do grupo Diffie-Hellman (força da chave):** na lista, selecione a força da chave a ser usada. O padrão é 0.
- **Tipo de túnel dividido:** na lista, selecione o tipo de túnel dividido a ser usado. O padrão é **Automático**. As opções possíveis são:
 - **Automático:** o túnel dividido é usado automaticamente.
 - **Manual:** o túnel dividido é usado sobre o endereço IP e a porta especificados no servidor

VPN.

- **Desativado:** o túnel dividido não é usado.
- **SuiteB Type:** na lista, selecione o nível de criptografia NSA Suite B a ser usado. O padrão é **GCM-128**. As opções possíveis são:
 - **GCM-128:** use a criptografia AES-GCM de 128 bits.
 - **GCM-256:** use a criptografia AES-GCM de 256 bits.
 - **GMAC-128:** use a criptografia AES-GMAC de 128 bits.
 - **GMAC-256:** use a criptografia AES-GMAC de 256 bits.
 - **Nenhum:** não use criptografia.
- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o seguinte:
 - **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
 - Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.

Configurar o protocolo genérico para o Samsung SAFE

- **Nome do host:** digite o nome do host VPN. Essa opção é necessária.
- **Ativar autenticação do usuário:** selecione se deseja exigir autenticação do usuário. Se ativado, em **Senha**, digite a senha do usuário.
- **Nome de usuário:** digite um nome de usuário.
- **Agente de nome de pacote VPN:** o nome ou o ID do pacote da VPN instalada no dispositivo; por exemplo, Mocana ou Pulse Secure.
- **Tipo de conexão VPN:** na lista, selecione **IPSEC** ou **SSL** para o tipo de conexão a ser usado. O padrão é **IPSEC**. As seções a seguir descrevem as definições de configuração de cada tipo de conexão.

Definir configurações de tipo de conexão IPSEC para Samsung SAFE

- **Identidade:** digite um identificador opcional para essa configuração.
- **Tipo de ID de grupo IPsec:** na lista, selecione o tipo de ID de grupo IPsec a ser usado. O padrão é **Padrão**. As opções possíveis são:
 - **Padrão**
 - **Endereço IPv4**
 - **Nome de domínio totalmente qualificado (FQDN)**
 - **FQDN do Usuário**
 - **ID de chave IKE**
- **Versão de IKE:** na lista, selecione a versão do Internet Key Exchange a ser usada. O padrão é **IKEv1**.

- **Método de autenticação:** na lista, selecione o método de autenticação que deve ser usado. O padrão é **Certificado**. As opções possíveis são:
 - **Certificado:** use a autenticação de certificado. Se selecionado, na lista de **Credenciais de identidade**, selecione a credencial a ser usada. O padrão é **Nenhum**.
 - **Chave pré-compartilhada:** use uma chave pré-compartilhada. Se selecionado, no campo **Chave pré-compartilhada**, digite a chave secreta compartilhada.
 - **RSA híbrido:** use a autenticação híbrida usando certificados RSA.
 - **EAP MD5:** autentique o par EAP no servidor EAP, mas não realize a autenticação mútua.
 - **EAP MSCHAPv2:** use a autenticação de handshake de desafio da Microsoft para autenticação mútua.
 - **Autenticação baseada em CAC:** Use um cartão de acesso comum (CAC) para autenticação.
- **Credencial de identidade:** na lista, selecione a credencial de identidade a ser usada. O padrão é **Nenhum**.
- **Certificado de CA:** na lista, selecione o certificado a ser usado.
- **Ativar detecção de perda de conexão:** selecione se você deseja entrar em contato com um par para garantir que ele permaneça ativo. O padrão é **Off**.
- **Ativar rota padrão:** selecione se uma rota padrão deve ser ativada para o servidor VPN.
- **Ativar opção móvel:** selecione se a opção móvel deve ser ativada.
- **Vida útil ike em minutos:** digite o número de minutos antes que a conexão VPN deva ser restabelecida. O padrão é 1440 minutos (24 horas).
- **Vida útil ipsec em minutos:** digite o número de minutos antes que a conexão VPN deva ser restabelecida. O padrão é 1440 minutos (24 horas).
- **Valor do grupo Diffie-Hellman (força da chave):** na lista, selecione a força da chave a ser usada. O padrão é **0**.
- **Modo de troca de chaves IKE Phase 1:** selecione **Principal** ou **Agressivo** para o modo de negociação do IKE Phase 1. O padrão é **Principal**.
 - **Principal:** nenhuma informação é exposta a potenciais invasores durante a negociação, mas é mais lento do que o modo **Agressivo**.
 - **Agressivo:** algumas informações (por exemplo, a identidade dos pares de negociação) são expostas a potenciais invasores durante a negociação, mas é mais rápido do que o modo **Principal**.
- **Valor com Perfect forward secrecy (PFS):** selecione se PFS deve ser usado para exigir que uma nova troca de chaves renegocie uma conexão.
- **Tipo de túnel dividido:** na lista, selecione o tipo de túnel dividido a ser usado. As opções possíveis são:
 - **Automático:** o túnel dividido é usado automaticamente.
 - **Manual:** o túnel dividido é usado sobre o endereço IP e a porta especificados no servidor VPN.

- **Desativado:** o túnel dividido não é usado.
- **Algoritmo de criptografia IPSEC:** uma configuração de VPN que o protocolo IPsec usa.
- **Algoritmo de criptografia IKE:** uma configuração de VPN que o protocolo IPsec usa.
- **Algoritmo de integridade IKE:** uma configuração de VPN que o protocolo IPsec usa.
- **Fornecedor:** um perfil pessoal para agentes genéricos que se comunicam com a API do Knox.
- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o seguinte:
 - **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
 - Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.
- **VPN por aplicativo:** para cada VPN por aplicativo que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
 - **VPN por aplicativo:** a configuração VPN que o aplicativo usa para se comunicar.
 - Clique em **Salvar** para salvar a VPN por aplicativo ou clique em **Cancelar** para não salvar.

Definir configurações de tipo de conexão SSL para o Samsung SAFE

- **Método de autenticação:** na lista, selecione o método de autenticação que deve ser usado. O padrão é **Não aplicável**. As opções possíveis são:
 - **Não Aplicável**
 - **Certificado:** use a autenticação de certificado. Se selecionado, na lista de **Credenciais de identidade**, selecione a credencial a ser usada. O padrão é **Nenhum**.
 - **Autenticação baseada em CAC:** Use um cartão de acesso comum (CAC) para autenticação.
- **Certificado de CA:** na lista, selecione o certificado a ser usado.
- **Ativar rota padrão:** selecione se uma rota padrão deve ser ativada para o servidor VPN.
- **Ativar opção móvel:** selecione se a opção móvel deve ser ativada.
- **Tipo de túnel dividido:** na lista, selecione o tipo de túnel dividido a ser usado. As opções possíveis são:
 - **Automático:** o túnel dividido é usado automaticamente.
 - **Manual:** o túnel dividido é usado sobre o endereço IP e a porta especificados no servidor VPN.
 - **Desativado:** o túnel dividido não é usado.
- **Algoritmo SSL:** digite o algoritmo SSL a ser usado para a negociação cliente-servidor.
- **Fornecedor:** um perfil pessoal para agentes genéricos que se comunicam com a API do Knox.
- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o seguinte:
 - **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
 - Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.

- **VPN por aplicativo:** para cada VPN por aplicativo que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
 - **VPN por aplicativo:** a configuração VPN que o aplicativo usa para se comunicar.
 - Clique em **Salvar** para salvar a VPN por aplicativo ou clique em **Cancelar** para não salvar.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra.
 - **Permitir que o usuário remova a política:** você pode selecionar quando os usuários podem remover a política do dispositivo. Selecione **Sempre**, **Código secreto obrigatório** ou **Nunca** no menu. Se você selecionar **Código secreto obrigatório**, digite um código secreto no campo **Código secreto de remoção**.
 - **Escopo do perfil:** selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

Configurações do Samsung Knox

The screenshot displays the 'VPN Policy' configuration window. On the left, a sidebar lists policy sections: '1 Policy Info', '2 Platforms', and '3 Assignment'. Under '2 Platforms', several operating systems are listed with checkboxes: iOS, macOS, Android, Samsung SAFE, Samsung KNOX (highlighted), Windows Phone, Windows Desktop/Tablet, and Amazon. The main configuration area is titled 'VPN Policy' and includes a descriptive note: 'This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.' Below this, various settings are shown: 'Vpn Type' is set to 'Enterprise'; 'Connection name' and 'Host name' are empty text boxes; 'Enable backup server', 'Enable user authentication', 'Enable default route', 'Enable smartcard authentication', and 'Enable mobile option' are all set to 'OFF'; 'Group name' is an empty text box; 'Authentication method' is set to 'Certificate'; 'Identity credential' is set to 'None'; and 'CA certificate' is set to 'Select certificate'. At the bottom right, there are 'Back' and 'Next >' buttons.

Quando você configura qualquer política para o Samsung Knox, ela se aplica somente no contêiner do Samsung Knox.

- **Tipo de VPN:** na lista, selecione o tipo de conexão VPN a ser configurada. A conexão pode ser

Enterprise (aplicável às versões do Knox anteriores à 2.0) ou **Genérico** (aplicável às versões do Knox 2.0 ou superiores). O padrão é **Empresarial**.

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Configurar o protocolo Empresa para o Samsung Knox

- **Nome da conexão:** digite um nome para a conexão. Este campo é obrigatório.
- **Nome do host:** digite o nome do host VPN. Essa opção é necessária.
- **Ativar servidor de backup:** selecione se um servidor VPN de backup deve ser ativado. Se ativado, no **servidor VPN de backup**, digite o FQDN ou o endereço IP do servidor VPN de backup.
- **Ativar autenticação do usuário:** selecione se deseja exigir autenticação do usuário. Se essa opção estiver ativada, defina as seguintes configurações:
 - **Nome de usuário:** digite um nome de usuário.
 - **Senha:** digite a senha de usuário.
- **Nome do grupo:** digite um nome de grupo opcional.
- **Método de autenticação:** na lista, selecione o método de autenticação que deve ser usado. As opções possíveis são:
 - **Certificado:** use a autenticação de certificado. Para autenticação de certificado, selecione também a credencial a ser usada na lista de **Credenciais de identidade**.
 - **Chave pré-compartilhada:** use uma chave pré-compartilhada. Se selecionado, no campo **Chave pré-compartilhada**, digite a chave secreta compartilhada.
 - **RSA híbrido:** use a autenticação híbrida usando certificados RSA.
 - **EAP MD5:** autentique o par EAP no servidor EAP, mas não realize a autenticação mútua.
 - **EAP MSCHAPv2:** use a autenticação de handshake de desafio da Microsoft para autenticação mútua.
- **Certificado de CA:** na lista, selecione o certificado a ser usado.
- **Ativar rota padrão:** selecione se uma rota padrão deve ser ativada para o servidor VPN.
- **Ativar a autenticação de cartão inteligente:** selecione se os usuários têm permissão para autenticar usando cartões inteligentes. O padrão é **Off**.
- **Ativar opção móvel:** selecione se a opção móvel deve ser ativada.
- **Valor do grupo Diffie-Hellman (força da chave):** na lista, selecione a força da chave a ser usada. O padrão é **0**.
- **Tipo de túnel dividido:** na lista, selecione o tipo de túnel dividido a ser usado. As opções possíveis são:
 - **Automático:** o túnel dividido é usado automaticamente.
 - **Manual:** o túnel dividido é usado sobre o endereço IP e a porta especificados no servidor VPN.
 - **Desativado:** nenhum túnel dividido é usado.
- **SuiteB Type:** na lista, selecione o nível de criptografia NSA Suite B a ser usado. As opções pos-

síveis são:

- **GCM-128:** use a criptografia AES-GCM de 128 bits, que é a configuração padrão.
 - **GCM-256:** use a criptografia AES-GCM de 256 bits.
 - **GMAC-128:** use a criptografia AES-GMAC de 128 bits.
 - **GMAC-256:** use a criptografia AES-GMAC de 256 bits.
 - **Nenhum:** não use criptografia.
- **Rotas de encaminhamento:** clique em **Adicionar** para adicionar qualquer rota de encaminhamento opcional se o servidor VPN corporativo for compatível com várias tabelas de roteamento.

Configurar o protocolo genérico para o Samsung Knox

- **Nome da conexão:** digite um nome para a conexão. Este campo é obrigatório.
- **Agente de nome de pacote VPN:** o nome ou o ID do pacote da VPN instalada no dispositivo; por exemplo, Mocana ou Pulse Secure.
- **Nome do host:** digite o nome do host VPN. Essa opção é necessária.
- **Ativar autenticação do usuário:** selecione se deseja exigir autenticação do usuário. Se essa opção estiver ativada, defina as seguintes configurações:
 - **Nome de usuário:** digite um nome de usuário.
 - **Senha:** digite a senha de usuário.
- **Identidade:** digite um identificador opcional para essa configuração. Aplica-se somente quando **Tipo de conexão VPN = IPSEC**.
- **Tipo de conexão VPN:** na lista, selecione **IPSEC** ou **SSL** para o tipo de conexão a ser usado. O padrão é **IPSEC**. As seções a seguir descrevem as definições de configuração de cada tipo de conexão.
- **Definir as configurações de conexão IPSEC**
 - **Tipo de ID de grupo IPsec:** na lista, selecione o tipo de ID de grupo IPsec a ser usado. O padrão é **Padrão**. As opções possíveis são:
 - * **Padrão**
 - * **Endereço IPv4**
 - * **Nome de domínio totalmente qualificado (FQDN)**
 - * **FQDN do Usuário**
 - * **ID de chave IKE**
 - **Versão de IKE:** na lista, selecione a versão do Internet Key Exchange a ser usada. O padrão é **IKEv1**.
 - **Método de autenticação:** na lista, selecione o método de autenticação que deve ser usado. O padrão é **Certificado**. As opções possíveis são:
 - * **Certificado:** use a autenticação de certificado. Se selecionado, na lista de **Credenciais de identidade**, selecione a credencial a ser usada. O padrão é **Nenhum**.
 - * **Chave pré-compartilhada:** use uma chave pré-compartilhada. Se selecionado, no

campo **Chave pré-compartilhada**, digite a chave secreta compartilhada.

- * **RSA híbrido:** use a autenticação híbrida usando certificados RSA.
 - * **EAP MD5:** autentique o par EAP no servidor EAP, mas não realize a autenticação mútua.
 - * **EAP MSCHAPv2:** use a autenticação de handshake de desafio da Microsoft para autenticação mútua.
 - * **Autenticação baseada em CAC:** Use um cartão de acesso comum (CAC) para autenticação.
- **Certificado de CA:** na lista, selecione o certificado a ser usado.
 - **Ativar detecção de perda de conexão:** selecione se você deseja entrar em contato com um par para garantir que ele permaneça ativo. O padrão é **Off**.
 - **Ativar rota padrão:** selecione se uma rota padrão deve ser ativada para o servidor VPN.
 - **Ativar opção móvel:** selecione se a opção móvel deve ser ativada.
 - **Vida útil ike em minutos:** digite o número de minutos antes que a conexão VPN deva ser restabelecida. O padrão é 1440 minutos (24 horas).
 - **Vida útil ipsec em minutos:** digite o número de minutos antes que a conexão VPN deva ser restabelecida. O padrão é 1440 minutos (24 horas).
 - **Valor do grupo Diffie-Hellman (força da chave):** na lista, selecione a força da chave a ser usada. O padrão é 0.
 - **Modo de troca de chaves IKE Phase 1:** selecione **Principal** ou **Agressivo** para o modo de negociação do IKE Phase 1. O padrão é **Principal**.
 - * **Principal:** nenhuma informação é exposta a potenciais invasores durante a negociação, mas é mais lento do que o modo **Agressivo**.
 - * **Agressivo:** algumas informações (por exemplo, a identidade dos pares de negociação) são expostas a potenciais invasores durante a negociação, mas é mais rápido do que o modo **Principal**.
 - **Valor com Perfect forward secrecy (PFS):** selecione se PFS deve ser usado para exigir que uma nova troca de chaves renegocie uma conexão.
 - **Tipo de túnel dividido:** na lista, selecione o tipo de túnel dividido a ser usado. As opções possíveis são:
 - * **Automático:** o túnel dividido é usado automaticamente.
 - * **Manual:** o túnel dividido é usado sobre o endereço IP e a porta especificados no servidor VPN.
 - * **Desativado:** o túnel dividido não é usado.
 - **SuiteB Type:** na lista, selecione o nível de criptografia NSA Suite B a ser usado. O padrão é **GCM-128**. As opções possíveis são:
 - * **GCM-128:** use a criptografia AES-GCM de 128 bits.
 - * **GCM-256:** use a criptografia AES-GCM de 256 bits.
 - * **GMAC-128:** use a criptografia AES-GMAC de 128 bits.

- * **GMAC-256:** use a criptografia AES-GMAC de 256 bits.
- * **Nenhum:** não use criptografia.
- **Algoritmo de criptografia IPSEC:** uma configuração de VPN que o protocolo IPsec usa.
- **Algoritmo de criptografia IKE:** uma configuração de VPN que o protocolo IPsec usa.
- **Algoritmo de integridade IKE:** uma configuração de VPN que o protocolo IPsec usa.
- **Knox:** configurações somente do Samsung Knox.
- **Fornecedor:** um perfil pessoal para agentes genéricos que se comunicam com a API do Knox.
- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o seguinte:
 - * **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
 - * Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.
- **VPN por aplicativo:** para cada VPN por aplicativo que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
 - * **VPN por aplicativo:** a configuração VPN que o aplicativo usa para se comunicar.
 - * Clique em **Salvar** para salvar a VPN por aplicativo ou clique em **Cancelar** para não salvar.
- **Definir as configurações de conexão SSL**
 - **Método de autenticação:** na lista, clique no método de autenticação que deve ser usado. As opções possíveis são:
 - * **Não aplicável:** nenhum método de autenticação é aplicado. Essa configuração é a padrão.
 - * **Certificado:** use a autenticação de certificado. Essa configuração é a padrão. Se selecionado, na lista de Credenciais de identidade, selecione a credencial a ser usada. O padrão é Nenhum.
 - * **Autenticação baseada em CAC:** Use um cartão de acesso comum (CAC) para autenticação.
 - **Certificado de CA:** na lista, selecione o certificado a ser usado.
 - **Ativar rota padrão:** selecione se uma rota padrão deve ser ativada para o servidor VPN.
 - **Ativar opção móvel:** selecione se a opção móvel deve ser ativada.
 - **Tipo de túnel dividido:** na lista, selecione o tipo de túnel dividido a ser usado. As opções possíveis são:
 - * **Automático:** o túnel dividido é usado automaticamente.
 - * **Manual:** o túnel dividido é usado sobre o endereço IP e a porta especificados.
 - * **Desativado:** nenhum túnel dividido é usado.
 - **Suite B Type:** na lista, selecione o nível de criptografia NSA Suite B a ser usado. O padrão é GCM-128. As opções possíveis são:
 - * **GCM-128:** use a criptografia AES-GCM de 128 bits.

- * **GCM-256:** use a criptografia AES-GCM de 256 bits.
- * **GMAC-128:** use a criptografia AES-GMAC de 128 bits.
- * **GMAC-256:** use a criptografia AES-GMAC de 256 bits.
- * **Nenhuma: não usar criptografia.** Digite o algoritmo SSL a ser usado para a negociação cliente-servidor.
- **Algoritmo SSL:** digite o algoritmo SSL a ser usado para a negociação cliente-servidor.
- **Knox:** configurações somente do Samsung Knox.
- **Fornecedor:** um perfil pessoal para agentes genéricos que se comunicam com a API do Knox.
- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o seguinte:
 - * **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
 - * Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.
- **VPN por aplicativo:** para cada VPN por aplicativo que você deseja adicionar, clique em **Adicionar** e faça o seguinte:
 - * **VPN por aplicativo:** a configuração VPN que o aplicativo usa para se comunicar.
 - * Clique em **Salvar** para salvar a VPN por aplicativo ou clique em **Cancelar** para não salvar.

Configurações do Windows Phone

VPN Policy

This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.

1 Policy Info

2 Platforms

- iOS
- macOS
- Android
- Samsung SAFE
- Samsung KNOX
- Windows Phone
- Windows Desktop/Tablet
- Amazon

3 Assignment

Connection name *

Profile type: Native

VPN server name *

Tunneling protocol *: L2TP

Authentication method *: EAP

EAP method *: TLS

DNS suffix

Trusted networks

Require smart card certificate: OFF

Automatically select client certificate: OFF

Remember credential: OFF

Always-on VPN: OFF

Back Next >

Essas configurações são compatíveis somente em telefones supervisionados com Windows 10 e versões posteriores.

- **Nome da conexão:** insira um nome para a conexão. Este campo é obrigatório.
- **Tipo de perfil:** na lista, selecione **Nativo** ou **Plug-in**. O padrão é **Nativo**. As seções a seguir descrevem as configurações de cada uma dessas opções.
- **Configurações de tipo de perfil nativo:** essas configurações se aplicam à VPN interna nos telefones com Windows dos usuários.
 - **Nome do servidor VPN:** digite o FQDN ou o endereço IP do servidor VPN. Este campo é obrigatório.
 - **Protocolo de encapsulamento:** na lista, selecione o tipo de túnel VPN a ser usado. O padrão é **L2TP**. As opções possíveis são:
 - * **L2TP:** Protocolo de Encapsulamento de Camada 2 com autenticação de chave pré-compartilhada.
 - * **PPTP:** Encapsulamento Ponto a Ponto.
 - * **IKEv2:** Internet Key Exchange versão 2.
 - **Método de autenticação:** na lista, selecione o método de autenticação a ser usado. O padrão é **EAP**. As opções possíveis são:
 - * **EAP:** Extended Authentication Protocol.
 - * **MSChapV2:** use a autenticação de handshake de desafio da Microsoft para autenticação mútua. Esta opção não está disponível quando você seleciona IKEv2 para o tipo de túnel. Quando você seleciona MSChapV2, uma opção **Usar credenciais do Windows automaticamente** aparece. O padrão é **Off**.
 - **Método EAP:** na lista, selecione o método EAP a ser usado. O padrão é o **TLS**. Esse campo não está disponível quando a autenticação MSChapV2 está ativada. As opções possíveis são:
 - * **TLS:** Transport Layer Security
 - * **PEAP:** Protected Extensible Authentication Protocol
 - **Sufixo DNS:** digite o sufixo DNS.
 - **Redes confiáveis:** digite uma lista de redes separadas por vírgula que não exigem uma conexão VPN para acesso. Por exemplo, quando os usuários estiverem na rede sem fio da sua empresa, eles poderão acessar recursos protegidos diretamente.
 - **Exigir um certificado de cartão inteligente:** determine se deve ser exigido um certificado de cartão inteligente. O padrão é O.
 - **Selecionar o certificado cliente automaticamente:** selecione se o certificado cliente a ser usado para autenticação deve ser escolhido automaticamente. O padrão é O. Essa opção não está disponível quando Exigir um certificado de cartão inteligente está ativado.
 - **Lembrar credencial:** selecione se as credenciais devem ser armazenadas em cache. O padrão é O. Quando essa opção está ativada, as credenciais são armazenadas sempre que possível.
 - **VPN sempre conectada:** selecione se a conexão VPN está sempre conectada. O padrão é O. Quando essa opção está ativada, a conexão VPN permanece ativa até que o usuário se

desconecte manualmente.

- **Ignorar para local:** digite o endereço e o número de porta para permitir que os recursos locais ignorem o servidor proxy.
- **Configurar o tipo de protocolo do plugin:** essas configurações se aplicam a plug-ins de VPN obtidos da Windows Store e instalados nos dispositivos dos usuários.
 - **Endereço de servidor:** digite a URL, o nome de host ou o endereço IP do servidor VPN.
 - **ID de aplicativo cliente:** digite o nome de família do pacote do plug-in de VPN.
 - **XML de Perfil de Plug-in:** selecione o perfil de plug-in de VPN personalizado para ser usado clicando em **Procurar** e navegando até a localização do arquivo. Entre em contato com o provedor do plug-in para obter o formato e os detalhes.
 - **Sufixo DNS:** digite o sufixo DNS.
 - **Redes confiáveis:** digite uma lista de redes separadas por vírgula que não exigem uma conexão VPN para acesso. Por exemplo, quando os usuários estiverem na rede sem fio da sua empresa, eles poderão acessar recursos protegidos diretamente.
 - **Lembrar credencial:** selecione se as credenciais devem ser armazenadas em cache. O padrão é O. Quando essa opção está ativada, as credenciais são armazenadas sempre que possível.
 - **VPN sempre conectada:** selecione se a conexão VPN está sempre conectada. O padrão é O. Quando essa opção está ativada, a conexão VPN permanece ativa até que o usuário se desconecte manualmente.
 - **Ignorar para local:** digite o endereço e o número de porta para permitir que os recursos locais ignorem o servidor proxy.

Configurações do Windows Desktop/Tablet

VPN Policy	VPN Policy
1 Policy Info	This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.
2 Platforms	<p>Connection name *</p> <p>Profile type: Native</p> <p>Server address *</p> <p>Remember credential: OFF</p> <p>DNS suffix</p> <p>Tunnel type *: L2TP</p> <p>Authentication method *: EAP</p> <p>EAP method *: TLS</p> <p>Trusted networks</p> <p>Require smart card certificate: OFF</p> <p>Automatically select client certificate: OFF</p> <p>Always-on VPN: OFF</p>
<input type="checkbox"/> iOS <input type="checkbox"/> macOS <input type="checkbox"/> Android <input type="checkbox"/> Samsung SAFE <input type="checkbox"/> Samsung KNOX <input checked="" type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Desktop/Tablet <input type="checkbox"/> Amazon	<p>Back Next ></p>
3 Assignment	

- **Nome da conexão:** insira um nome para a conexão. Este campo é obrigatório.
- **Tipo de perfil:** na lista, selecione **Nativo** ou **Plug-in**. O padrão é **Nativo**.
- **Configurar tipo de perfil nativo:** essas configurações se aplicam à VPN interna nos dispositivos Windows dos usuários.
 - **Endereço de servidor:** digite o FQDN ou o endereço IP do servidor VPN. Este campo é obrigatório.
 - **Lembrar credencial:** selecione se as credenciais devem ser armazenadas em cache. O padrão é **Off**. Quando essa opção está ativada, as credenciais são armazenadas sempre que possível.
 - **Sufixo DNS:** digite o sufixo DNS.
 - **Tipo de túnel:** na lista, selecione o tipo de túnel VPN a ser usado. O padrão é **L2TP**. As opções possíveis são:
 - * **L2TP:** Protocolo de Encapsulamento de Camada 2 com autenticação de chave pré-compartilhada.
 - * **PPTP:** Encapsulamento Ponto a Ponto.
 - * **IKEv2:** Internet Key Exchange versão 2.
 - **Método de autenticação:** na lista, selecione o método de autenticação a ser usado. O padrão é **EAP**. As opções possíveis são:
 - * **EAP:** Extended Authentication Protocol.
 - * **MSChapV2:** use a autenticação de handshake de desafio da Microsoft para autenticação mútua. Esta opção não está disponível quando você seleciona **IKEv2** para o tipo de túnel.
 - **Método EAP:** na lista, selecione o método EAP a ser usado. O padrão é o **TLS**. Esse campo não está disponível quando a autenticação MSChapV2 está ativada. As opções possíveis são:
 - * **TLS:** Transport Layer Security
 - * **PEAP:** Protected Extensible Authentication Protocol
 - **Redes confiáveis:** digite uma lista de redes separadas por vírgula que não exigem uma conexão VPN para acesso. Por exemplo, quando os usuários estiverem na rede sem fio da sua empresa, eles poderão acessar recursos protegidos diretamente.
 - **Exigir um certificado de cartão inteligente:** determine se deve ser exigido um certificado de cartão inteligente. O padrão é **Off**.
 - **Selecionar o certificado cliente automaticamente:** selecione se o certificado cliente a ser usado para autenticação deve ser escolhido automaticamente. O padrão é **Off**. Essa opção não está disponível quando você ativa **Exigir um certificado de cartão inteligente**.
 - **VPN sempre conectada:** selecione se a conexão VPN está sempre conectada. O padrão é **Off**. Quando essa opção está ativada, a conexão VPN permanece ativa até que o usuário se desconecte manualmente.
 - **Ignorar para local:** digite o endereço e o número de porta para permitir que os recursos

locais ignorem o servidor proxy.

- **Configure Plugin profile type:** essas configurações se aplicam a plug-ins de VPN obtidos da Windows Store e instalados nos dispositivos dos usuários.
 - **Endereço de servidor:** digite o FQDN ou o endereço IP do servidor VPN. Este campo é obrigatório.
 - **Lembrar credencial:** selecione se as credenciais devem ser armazenadas em cache. O padrão é **Off**. Quando essa opção está ativada, as credenciais são armazenadas sempre que possível.
 - **Sufixo DNS:** digite o sufixo DNS.
 - **ID de aplicativo cliente:** digite o nome de família do pacote do plug-in de VPN.
 - **XML de Perfil de Plug-in:** selecione o perfil de plug-in de VPN personalizado para ser usado clicando em **Procurar** e navegando até a localização do arquivo. Entre em contato com o provedor do plug-in para obter o formato e os detalhes.
 - **Redes confiáveis:** digite uma lista de redes separadas por vírgula que não exigem uma conexão VPN para acesso. Por exemplo, quando os usuários estiverem na rede sem fio da sua empresa, eles poderão acessar recursos protegidos diretamente.
 - **VPN sempre conectada:** selecione se a conexão VPN está sempre conectada. O padrão é **Off**. Quando essa opção está ativada, a conexão VPN permanece ativa até que o usuário se desconecte manualmente.
 - **Ignorar para local:** digite o endereço e o número de porta para permitir que os recursos locais ignorem o servidor proxy.

Configurações do Amazon

VPN Policy	VPN Policy
1 Policy Info	This policy lets you configure a VPN connection to provide a device-level encrypted connection to the intranet. For Windows Phone, the policy is supported only on Windows 10 and later supervised devices.
2 Platforms	<p>Connection name *</p> <p>Vpn Type: L2TP PSK</p> <p>Server address *</p> <p>User name: administrator</p> <p>Password:</p> <p>L2TP Secret</p> <p>IPSec Identifier</p> <p>IPSec pre-shared key</p> <p>DNS search domains</p> <p>DNS servers</p> <p>Forwarding routes</p>
<input checked="" type="checkbox"/> iOS <input checked="" type="checkbox"/> macOS <input checked="" type="checkbox"/> Android <input checked="" type="checkbox"/> Samsung SAFE <input checked="" type="checkbox"/> Samsung KNOX <input checked="" type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Desktop/Tablet <input checked="" type="checkbox"/> Amazon	<p>► Deployment Rules</p> <p>Back Next ></p>
3 Assignment	

- **Nome da conexão:** insira um nome para a conexão.
- **Tipo de VPN:** selecione o tipo de conexão. As opções possíveis são:
 - **L2TP PSK:** protocolo de encapsulamento de camada 2 com autenticação de chave pré-compartilhada. Essa configuração é a padrão.
 - **L2TP RSA:** protocolo de encapsulamento de camada 2 com autenticação RSA.
 - **IPSEC XAUTH PSK:** Internet Protocol Security com chave pré-compartilhada e autenticação estendida.
 - **IPSEC HYBRID RSA:** Internet Protocol Security com autenticação RSA híbrida.
 - **PPTP:** Encapsulamento Ponto a Ponto.

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Definir as configurações do L2TP PSK para Amazon

- **Endereço de servidor:** digite o endereço IP do servidor VPN.
- **Nome de usuário:** digite um nome de usuário opcional.
- **Senha:** digite uma senha opcional.
- **L2TP secreto:** digite a chave secreta compartilhada.
- **Identificador IPsec:** digite o nome da conexão VPN que os usuários veem nos respectivos dispositivos quando se conectam.
- **Chave pré-compartilhada IPsec:** digite a chave secreta.
- **Domínios de pesquisa DNS:** digite os domínios em relação aos quais a lista de domínios de pesquisa de um dispositivo do usuário pode corresponder.
- **Servidores DNS:** digite os endereços IP dos servidores DNS a serem usados para resolver os domínios especificados.
- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o seguinte:
 - **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
 - Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.

Definir as configurações do L2TP RSA para Amazon

- **Endereço de servidor:** digite o endereço IP do servidor VPN.
- **Nome de usuário:** digite um nome de usuário opcional.
- **Senha:** digite uma senha opcional.
- **L2TP secreto:** digite a chave secreta compartilhada.
- **Domínios de pesquisa DNS:** digite os domínios em relação aos quais a lista de domínios de pesquisa de um dispositivo do usuário pode corresponder.
- **Servidores DNS:** digite os endereços IP dos servidores DNS a serem usados para resolver os domínios especificados.

- **Certificado de servidor:** na lista, selecione o certificado a ser usado.
- **Certificado CA:** na lista, selecione o certificado de AC a ser usado.
- **Credencial de identidade:** na lista, selecione a credencial de identidade a ser usada.
- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o seguinte:
 - **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
 - Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.

Definir as configurações de IPSEC XAUTH PSK para Amazon

- **Endereço de servidor:** digite o endereço IP do servidor VPN.
- **Nome de usuário:** digite um nome de usuário opcional.
- **Senha:** digite uma senha opcional.
- **Identificador IPsec:** digite o nome da conexão VPN que os usuários veem nos respectivos dispositivos quando se conectam.
- **Chave pré-compartilhada IPsec:** digite a chave secreta compartilhada.
- **Domínios de pesquisa DNS:** digite os domínios em relação aos quais a lista de domínios de pesquisa de um dispositivo do usuário pode corresponder.
- **Servidores DNS:** digite os endereços IP dos servidores DNS a serem usados para resolver os domínios especificados.
- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o seguinte:
 - **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
 - Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.

Definir as configurações de IPSEC AUTH RSA para Amazon

- **Endereço de servidor:** digite o endereço IP do servidor VPN.
- **Nome de usuário:** digite um nome de usuário opcional.
- **Senha:** digite uma senha opcional.
- **Domínios de pesquisa DNS:** digite os domínios em relação aos quais a lista de domínios de pesquisa de um dispositivo do usuário pode corresponder.
- **Servidores DNS:** digite os endereços IP dos servidores DNS a serem usados para resolver os domínios especificados.
- **Certificado de servidor:** na lista, selecione o certificado a ser usado.
- **Certificado CA:** na lista, selecione o certificado de AC a ser usado.
- **Credencial de identidade:** na lista, selecione a credencial de identidade a ser usada.

- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o seguinte:
 - **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
 - Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.

Definir as configurações de IPSEC HYBRID RSA para Amazon

- **Endereço de servidor:** digite o endereço IP do servidor VPN.
- **Nome de usuário:** digite um nome de usuário opcional.
- **Senha:** digite uma senha opcional.
- **Domínios de pesquisa DNS:** digite os domínios em relação aos quais a lista de domínios de pesquisa de um dispositivo do usuário pode corresponder.
- **Servidores DNS:** digite os endereços IP dos servidores DNS a serem usados para resolver os domínios especificados.
- **Certificado de servidor:** na lista, selecione o certificado a ser usado.
- **Certificado CA:** na lista, selecione o certificado de AC a ser usado.
- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o seguinte:
 - **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
 - Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.

Definir as configurações de PPTP para Amazon

- **Endereço de servidor:** digite o endereço IP do servidor VPN.
- **Nome de usuário:** digite um nome de usuário opcional.
- **Senha:** digite uma senha opcional.
- **Domínios de pesquisa DNS:** digite os domínios em relação aos quais a lista de domínios de pesquisa de um dispositivo do usuário pode corresponder.
- **Servidores DNS:** digite os endereços IP dos servidores DNS a serem usados para resolver os domínios especificados.
- **Criptografia PPP (MPPE):** selecione se a criptografia de dados deve ser ativada com o Microsoft Point-to-Point Encryption (MPPE). O padrão é **Off**.
- **Rotas de encaminhamento:** se o servidor VPN corporativo for compatível com rotas de encaminhamento, para cada rota de encaminhamento a ser usada, clique em **Adicionar** e faça o seguinte:
 - **Rota de encaminhamento:** digite o endereço IP da rota de encaminhamento.
 - Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.

Política de dispositivo de papel de parede

August 20, 2021

Você pode adicionar um arquivo .png ou .jpg para definir o papel de parede na tela de bloqueio ou na tela inicial de um dispositivo iOS, ou em ambas. Disponível no iOS 7.1.2 e posterior apenas para dispositivos supervisionados. Para usar papéis de parede diferentes em iPads e iPhones, você precisa criar políticas diferentes de papéis de parede e implantá-las nos usuários apropriados.

A tabela a seguir lista a recomendação da Apple para dimensões de imagem para dispositivos iOS.

iPhone

Dispositivo	Dimensões da imagem em pixels
iPhone 12 Pro Max	2778 x 1284
iPhone 12 e iPhone 12 Pro	2532 x 1170
iPhone 12 Mini	2340 x 1080
iPhone 11 Max	2688 x 1242
iPhone 11 Pro	2436 x 1125
iPhone 11	1792 x 828
iPhone XS Max	2688 x 1242
iPhone X, XS	2436 x 1125
iPhone XR	1792 x 828
iPhone SE 2ª geração	1334 x 750
iPhone 7 Plus, 8 Plus	2208 x 1242
iPhone 7, 8	1334 x 750
iPhone 8 Plus	1334 x 750
iPhone 8	1334 x 750

iPad

Dispositivo	Dimensões da imagem em pixels
iPad Pro (1ª, 2ª e 3ª geração de 12,9")	2732 x 2048
iPad Pro de 10,5 polegadas	2224 x 1668

Dispositivo	Dimensões da imagem em pixels
iPad Pro (9,7 polegadas)	1536 x 2048
iPad Air 2	2048 x 1536

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte a [Política de dispositivo de VPN](#).

Configurações de iOS

- **Aplicar a:** na lista, selecione **Tela de bloqueio**, **Tela inicial (lista de ícones)** ou **Telas de bloqueio e inicial** para definir onde o papel de parede deverá ser exibido.
- **Arquivo de papel de parede:** selecione o arquivo de papel de parede clicando em **Procurar** e navegando até a localização do arquivo.

Política de dispositivo de filtro de conteúdo Web

April 26, 2021

Você pode adicionar uma política de dispositivo no XenMobile para filtrar conteúdo Web nos dispositivos iOS usando a função de filtro automático da Apple em conjunto com sites específicos que você adiciona a listas de permissão e de bloqueio. Essa política está disponível somente nos dispositivos iOS 7.0 e versões posteriores no modo Supervisionado. Para obter informações sobre como colocar um dispositivo iOS no modo Supervisionado, consulte [Para colocar um dispositivo iOS no modo Supervisionado usando o Apple Configurator](#).

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

- **Tipo de filtro:** na lista, clique em **Interno** ou **Plug-in**, e siga os procedimentos a seguir da opção que você escolher. O padrão é **Interno**.

Tipo de filtro interno

- **Filtro de conteúdo Web**
 - **Filtro automático ativado:** se a função de filtro automático da Apple deve ou não ser usada para analisar sites de conteúdo impróprio. O padrão é **Off**.

- **URLs permitidas:** essa lista será ignorada quando a opção **Filtro automático ativado** estiver definida como **O**. Quando **Filtro automático ativado** estiver definido como **I**, os itens nessa lista estarão sempre acessíveis, mesmo que o filtro automático permita ou não o acesso. Para cada URL que você deseja adicionar à lista de permissão, clique em **Adicionar** e faça o seguinte:
 - * Digite a URL do site permitido. Você deve adicionar `http://` ou `https://` antes do endereço da web.
 - * Clique em **Salvar** para salvar o site na lista de permissão ou clique em **Cancelar** para não salvá-lo.
- **URLs na lista negra:** os itens nessa lista são sempre bloqueados. Para cada URL que você deseja adicionar à lista de bloqueio, clique em **Adicionar** e faça o seguinte:
 - * Digite a URL do site a ser bloqueado. Você deve adicionar `http://` ou `https://` antes do endereço da web.
 - * Clique em **Salvar** para salvar o site na lista de bloqueio ou clique em **Cancelar** para não salvá-lo.

Nota:

O console XenMobile Server inclui os termos “lista negra” e “lista branca”. Estamos alterando esses termos em uma próxima versão para “lista de bloqueio” e “lista de permissão”.

- **Lista branca de indicadores**

- **Lista branca de indicadores:** especifica os sites que os usuários podem acessar. Para ativar o acesso a sites da web, adicione a URL.
 - * **URL:** a URL de cada site que os usuários podem acessar. Por exemplo, para habilitar o acesso ao armazenamento do Secure Hub, adicione a URL do XenMobile Server à lista de **URLs**. Você deve adicionar `http://` ou `https://` antes do endereço da web. Este campo é obrigatório.
 - * **Pasta de indicadores:** digite um nome de pasta de indicadores opcional. Se esse campo for deixado em branco, o marcador será adicionado ao diretório de marcadores padrão.
 - * **Título:** digite um título descritivo para o site. Por exemplo, digite “Google” para a URL `https://google.com`.
 - * Clique em **Salvar** para salvar o site na lista de permissão ou clique em **Cancelar** para não salvá-lo.

Tipo de filtro de plug-in

- **Nome do filtro:** insira um nome exclusivo para o filtro.
- **Identificador:** insira o ID de pacote do plug-in que fornece o serviço de filtragem.
- **Endereço do serviço:** insira um endereço de servidor opcional. Os formatos válidos são endereço IP, nome de host ou URL.

- **Nome de usuário:** insira um nome de usuário opcional para o serviço.
- **Senha:** insira uma senha opcional para o serviço.
- **Certificado:** na lista, clique em um certificado de identidade opcional a ser usado para autenticar o usuário no serviço. O padrão é **Nenhum**.
- **Filtrar o tráfego de WebKit:** selecione se o tráfego de WebKit deve ser filtrado.
- **Filtrar o tráfego de soquete:** selecione se o tráfego de soquete deve ser filtrado.
- **Dados personalizados:** para cada chave personalizada que você deseja adicionar ao filtro da Web, clique em **Adicionar** e faça o seguinte:
 - **Chave:** digite a chave personalizada.
 - **Valor:** digite um valor para a chave personalizada.
 - Clique em **Salvar** para salvar a chave personalizada ou clique em **Cancelar** para não salvá-la.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Política de dispositivo de clip web

September 10, 2020

Você pode inserir atalhos ou clips web em sites para que apareçam junto aos aplicativos nos dispositivos de usuários. Você pode especificar seus próprios ícones para representar os clips web para dispositivos iOS, iPadOS, macOS e Android. O tablet Windows requer somente um rótulo e uma URL. Nos dispositivos iOS e iPadOS, configure a política de dispositivo de layout de tela inicial para organizar os clips web criados. Se você restringir o acesso a aplicativos no iOS, certifique-se de configurar a política de dispositivo de restrição para permitir clips web. Para obter informações sobre como configurar essas políticas, consulte [Política de dispositivo de layout de tela inicial](#) e [Política de dispositivo de restrições](#).

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações de iOS

- **Rótulo:** digite o rótulo que deve ser exibido com o clip web.

- **URL:** digite a URL associada ao clip web. A URL deve começar com um protocolo, por exemplo, <https://server>.
- **Removível:** selecione se os usuários podem remover o clip web. O padrão é **Off**.
- **Ícone a ser atualizado:** selecione o ícone a ser usado para o clip web clicando em **Procurar** e navegando até a localização do arquivo.
- **Ícone pré-composto:** selecione se o ícone tem efeitos (cantos arredondados, sombra e brilho reflexivo) aplicados a ele. O padrão é **O**, o que adiciona os efeitos.
- **Tela inteira:** selecione se a página da Web vinculada é aberta no modo de tela inteira. O padrão é **Off**.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do macOS

- **Rótulo:** digite o rótulo que deve ser exibido com o clip web.
- **URL:** digite a URL associada ao clip web. A URL deve começar com um protocolo, por exemplo, <https://server>.
- **Ícone a ser atualizado:** selecione o ícone a ser usado para o clip web clicando em **Procurar** e navegando até a localização do arquivo.

Configurações do Android

- **Regra:** selecione se essa política adiciona ou remove um clip web. O padrão é **Adicionar**.
- **Rótulo:** digite o rótulo que deve ser exibido com o clip web.
- **URL:** digite a URL associada ao clip web.
- **Definir um ícone:** selecione se um arquivo de ícone deve ser usado. O padrão é **Off**.
- **Arquivo de ícone:** se a opção **Definir um ícone** estiver definida como **I**, selecione o arquivo de ícone a ser usado clicando em **Procurar** e navegando até a localização do arquivo.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**

- * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
- * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra.
- **Permitir que o usuário remova a política:** você pode selecionar quando os usuários podem remover a política do dispositivo. Selecione **Sempre**, **Código secreto obrigatório** ou **Nunca** no menu. Se você selecionar **Código secreto obrigatório**, digite um código secreto no campo **Código secreto de remoção**.
- **Escopo do perfil:** selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

Configurações do Windows Desktop/Tablet

- **Nome:** digite o rótulo que deve ser exibido com o clip web.
- **URL:** digite a URL associada ao clip web.

Política de dispositivo Wi-Fi

December 22, 2020

Crie políticas de dispositivo de Wi-Fi novas ou existentes no XenMobile usando a página **Configurar > Políticas de dispositivo**. Políticas de Wi-Fi permitem gerenciar como os usuários conectam seus dispositivos a redes Wi-Fi, definindo os itens a seguir:

- Nomes e tipos de redes
- Políticas de autenticação e segurança
- Uso de servidores proxy
- Outros detalhes relacionados a WiFi

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Pré-requisitos

Antes de criar uma política, conclua estas etapas:

- Crie os grupos de entrega que você planeja usar.
- Conheça o nome e o tipo de rede.
- Conheça os tipos de autenticação ou segurança que você planeja usar.
- Conheça as informações do servidor proxy que podem ser necessárias.

- Instale todos os certificados AC necessários.
- Tenha as chaves compartilhadas necessárias.
- Crie a entidade PKI de autenticação baseada em certificado.
- Configure os provedores de credenciais.

Para obter mais informações, consulte [Autenticação](#) e os sub-artigos.

Configurações de iOS

WiFi Policy	WiFi Policy
1 Policy Info	This policy lets you configure a WiFi profile for devices.
2 Platforms	<p>Network type <input type="text" value="Standard"/></p> <p>Network name * <input type="text"/></p> <p>Hidden network (enable if network is open or off) <input type="checkbox" value="OFF"/></p> <p>Auto join (automatically join this wireless network) <input checked="" type="checkbox" value="ON"/></p> <p>Disable Captive Network Detection <input type="checkbox" value="OFF"/></p> <p>Security type <input type="text" value="None"/></p> <p>Proxy configuration <input type="text" value="None"/></p> <p>Fast Lane QoS Marking <input type="text" value="Do not restrict QoS marking"/></p> <p>Remove policy <input checked="" type="radio" value="Select date"/></p>
<input checked="" type="checkbox"/> iOS <input checked="" type="checkbox"/> macOS <input checked="" type="checkbox"/> Android <input checked="" type="checkbox"/> Windows Phone <input checked="" type="checkbox"/> Windows Desktop/Tablet <input checked="" type="checkbox"/> Windows Mobile/CE	<p>Proxy server settings</p> <p>QoS Settings</p> <p>Policy Settings</p>
3 Assignment	

- **Tipo de rede:** na lista, clique em **Padrão**, **Ponto de acesso legado** ou **Hotspot 2.0** para definir o tipo de rede que você planeja usar.
- **Nome da rede:** digite o SSID que é exibido na lista de redes disponíveis do dispositivo. Não se aplica ao **Hotspot 2.0**.
- **Rede oculta (ativar se a rede for aberta ou estiver desligada):** escolha se a rede é oculta.
- **Ingressar automaticamente (ingressar automaticamente nesta rede sem fio):** escolha se o ingresso na rede é automático. Se um dispositivo iOS já estiver conectado a outra rede, ele não entrará nessa rede. O usuário deve se desconectar da rede anterior antes que o dispositivo se conecte automaticamente. O padrão é **On**.
- **Usar endereço MAC estático:** os endereços MAC são identificadores exclusivos que um dispositivo transmite dentro de uma rede. Para aumentar a privacidade, os dispositivos iOS e iPadOS podem usar um endereço MAC diferente sempre que se conectarem a uma rede. Se **Ativado**, o dispositivo sempre usa o mesmo endereço MAC ao se conectar a essa rede. Se **Desativado**, o dispositivo usa um endereço MAC diferente toda vez que se conecta a essa rede. O padrão é **Off**.

- **Tipo de segurança:** na lista, clique no tipo de segurança que você planeja usar. Não se aplica ao **Hotspot 2.0**.
 - Nenhum - não requer configuração adicional.
 - WEP
 - WPA/WPA2 Pessoal
 - Qualquer (Pessoal)
 - WEP Enterprise
 - WPA/WPA2 Enterprise: para a versão mais recente do Windows 10, o uso do WPA-2 Enterprise requer que você configure o SCEP (Simple Certificate Enrollment Protocol). Em seguida, o XenMobile pode enviar o certificado a dispositivos para autenticação no servidor Wi-Fi. Para configurar o SCEP, vá para a página Distribuição de **Configurações > Provedores de credenciais**. Para obter mais informações, consulte [Provedores de credenciais](#).
 - Qualquer (Enterprise)

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Configurações WPA, WPA Pessoal, Qualquer (pessoal) para iOS

Senha: digite uma senha opcional. Se você deixar esse campo em branco, os usuários poderão ser solicitados a inserir as senhas quando fizerem login.

Configurações WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Qualquer (Enterprise) para iOS

Quando você escolhe qualquer uma dessas configurações, as respectivas configurações são listadas após **Configurações do servidor proxy**.

- **Protocolos, tipos de EAP aceitos:** ative os tipos de EAP aos quais você deseja dar suporte e defina as configurações associadas. O padrão é **Off** para cada tipo de EAP disponível.
- **Autenticação interna (TTLS):** *obrigatório somente quando você ativa TTLS*. Na lista, escolha método de autenticação interno a ser usado. As opções são: **PAP**, **CHAP**, **MSCHAP** ou **MSCHAPv2**. O padrão é **MSCHAPv2**.
- **Protocolos, EAP-FAST:** escolha se deseja usar as credenciais de acesso protegido (PACs).
 - Se você escolher **Usar PAC**, escolha se deseja usar um PAC de provisionamento.
 - * Se você escolher **Provisionamento de PAC**, escolha se deseja permitir um handshake TLS anônimo entre o cliente do usuário final e o XenMobile.
 - **Provisionamento de PAC anônimo**
- **Autenticação:**
 - **Nome de usuário:** digite um nome de usuário.

- **Senha por conexão:** escolha se deve ser exigida uma senha toda vez que os usuários fizerem login.
- **Senha:** digite uma senha opcional. Se você deixar esse campo em branco, os usuários poderão ser solicitados a inserir as senhas quando fizerem login.
- **Credencial de identidade (keystore ou credencial PKI):** na lista, escolha o tipo de credencial de identidade. O padrão é **Nenhum**.
- **Identidade externa:** *obrigatório somente quando você ativa PEAP, TTLS ou EAP-FAST.* Digite o nome de usuário visível externamente. Você pode aumentar a segurança digitando um termo genérico, como “anônimo”, para que o nome do usuário não possa ser visto.
- **Exigir um certificado TLS:** escolha se deseja exigir o certificado TLS.
- **Confiança**
 - **Certificados confiáveis:** para adicionar um certificado confiável, clique em **Adicionar** e, para cada certificado que você deseja adicionar, faça o seguinte:
 - * **Aplicativo:** na lista, escolha o aplicativo que você deseja adicionar.
 - * Clique em **Salvar** para salvar o certificado ou em **Cancelar**.
 - **Nomes de certificados de servidor confiáveis:** para adicionar nomes comuns de certificado de servidores confiáveis, clique em **Adicionar** e, para cada nome que você deseja adicionar, adicione o seguinte:
 - * **Certificado:** digite o nome do certificado do servidor. Você pode usar curingas para especificar o nome, como wpa*.exemplo.com.
 - * Clique em **Salvar** para salvar o nome do certificado ou em **Cancelar**.
- **Permitir exceções de confiança:** escolha se a caixa de diálogo de confiança do certificado será exibida nos dispositivos de usuários quando um certificado não for confiável. O padrão é **On**.
- **Configurações do servidor proxy**
 - **Configuração de proxy:** na lista, escolha **Nenhum**, **Manual** ou **Automático** para definir como a conexão VPN cria rotas em um servidor proxy e configure todas as opções adicionais. O padrão é **Nenhum**, que não requer configuração adicional.
 - Se você escolher **Manual**, defina as seguintes configurações:
 - * **Nome do host/endereço IP:** digite o nome do host ou endereço IP do servidor proxy.
 - * **Porta:** digite o número de porta do servidor proxy.
 - * **Nome de usuário:** digite um nome de usuário opcional para autenticação no servidor proxy.
 - * **Senha:** digite uma senha opcional para autenticação no servidor proxy.
 - Se você escolher **Automático**, defina as seguintes configurações:
 - * **URL do servidor:** digite a URL do arquivo PAC que define a configuração de proxy.
 - * **Permitir conexão direta se o PAC estiver inacessível:** escolha se os usuários terão permissão para se conectarem diretamente com o destino se o arquivo PAC estiver inacessível. O padrão é **On**. Essa opção está disponível somente no iOS 7.0 e versões

posteriores.

- **Configurações de política**

- **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**

- * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.

- * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra. Disponível apenas para iOS 6.0 e posterior.

Configurações do macOS

<p>WiFi Policy</p> <p>1 Policy Info</p> <p>2 Platforms</p> <p><input checked="" type="checkbox"/> iOS</p> <p><input checked="" type="checkbox"/> Mac OS X</p> <p><input checked="" type="checkbox"/> Android</p> <p><input checked="" type="checkbox"/> Windows Phone</p> <p><input checked="" type="checkbox"/> Windows Tablet</p> <p>3 Assignment</p>	<p>WiFi Policy</p> <p>This policy lets you configure a WiFi profile for devices.</p> <p>Network type: Standard</p> <p>Network name*: <input type="text"/></p> <p>Hidden network (enable if network is open or off): OFF</p> <p>Auto join (automatically join this wireless network): ON</p> <p>Security type: None</p> <p>Proxy server settings</p> <p>Proxy configuration: None</p> <p>Policy Settings</p> <p>Remove policy: <input checked="" type="radio"/> Select date <input type="radio"/> Duration until removal (in days)</p> <p><input type="text"/></p> <p>Allow user to remove policy: Always</p> <p>Profile scope: User OS X 10.7+</p> <p>► Deployment Rules</p>
--	---

- **Tipo de rede:** na lista, clique em **Padrão**, **Ponto de acesso legado** ou **Hotspot 2.0** para definir o tipo de rede que você planeja usar.
- **Nome da rede:** digite o SSID que é exibido na lista de redes disponíveis do dispositivo. Não se aplica ao **Hotspot 2.0**.
- **Rede oculta (ativar se a rede for aberta ou estiver desligada):** escolha se a rede é oculta.
- **Ingressar automaticamente (ingressar automaticamente nesta rede sem fio):** escolha se o ingresso na rede é automático. Se um dispositivo já estiver conectado a outra rede, ele não

entrará nessa rede. O usuário deve se desconectar da rede anterior antes que o dispositivo se conecte automaticamente. O padrão é **On**.

- **Tipo de segurança:** na lista, clique no tipo de segurança que você planeja usar. Não se aplica ao **Hotspot 2.0**.
 - Nenhum - não requer configuração adicional.
 - WEP
 - WPA/WPA2 Pessoal
 - Qualquer (Pessoal)
 - WEP Enterprise
 - WPA/WPA2 Enterprise
 - Qualquer (Enterprise)

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Configurações WPA, WPA Pessoal, Qualquer (Pessoal) para macOS

- **Senha:** digite uma senha opcional. Se você deixar esse campo em branco, os usuários poderão ser solicitados a inserir as senhas quando fizerem login.

Configurações WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Qualquer (Enterprise) para macOS

Quando você escolhe qualquer uma dessas configurações, as respectivas configurações são listadas após **Configurações do servidor proxy**.

- **Protocolos, tipos de EAP aceitos:** ative os tipos de EAP aos quais você deseja dar suporte e defina as configurações associadas. O padrão é **Off** para cada tipo de EAP disponível.
- **Autenticação interna (TTLS):** *obrigatório somente quando você ativa TTLS*. Na lista, escolha método de autenticação interno a ser usado. As opções são: **PAP**, **CHAP**, **MSCHAP** ou **MSCHAPv2**. O padrão é **MSCHAPv2**.
- **Protocolos, EAP-FAST:** escolha se deseja usar as credenciais de acesso protegido (PACs).
 - Se você selecionar **Usar PAC**, escolha se deseja usar um PAC de provisionamento.
 - * Se você escolher **Provisionamento de PAC**, escolha se deseja permitir um handshake TLS anônimo entre o cliente do usuário final e o XenMobile.
 - **Provisionamento de PAC anônimo**
- **Autenticação:**
 - **Nome de usuário:** digite um nome de usuário.
 - **Senha por conexão:** escolha se deve ser exigida uma senha toda vez que os usuários fizerem login.
 - **Senha:** digite uma senha opcional. Se você deixar esse campo em branco, os usuários poderão ser solicitados a inserir as senhas quando fizerem login.

- **Credencial de identidade (keystore ou credencial PKI):** na lista, escolha o tipo de credencial de identidade. O padrão é **Nenhum**.
- **Identidade externa:** *obrigatório somente quando você ativa PEAP, TTLS ou EAP-FAST.* Digite o nome de usuário visível externamente. Você pode aumentar a segurança digitando um termo genérico como “anônimo” para que o nome do usuário não possa ser visto.
- **Exigir um certificado TLS:** escolha se deseja exigir o certificado TLS.
- **Confiança**
 - **Certificados confiáveis:** para adicionar um certificado confiável, clique em **Adicionar** e, para cada certificado que você deseja adicionar, faça o seguinte:
 - * **Aplicativo:** na lista, escolha o aplicativo que você deseja adicionar.
 - * Clique em **Salvar** para salvar o certificado ou em **Cancelar**.
 - **Nomes de certificados de servidor confiáveis:** para adicionar nomes comuns de certificado de servidores confiáveis, clique em **Adicionar** e, para cada nome que você deseja adicionar, adicione o seguinte:
 - * **Certificado:** digite o nome do certificado do servidor que você deseja adicionar. Você pode usar curingas para especificar o nome, como wpa*.exemplo.com.
 - * Clique em **Salvar** para salvar o nome do certificado ou em **Cancelar**.
- **Permitir exceções de confiança:** escolha se a caixa de diálogo de confiança do certificado será exibida nos dispositivos do usuário quando um certificado não for confiável. O padrão é **On**.
- **Usar como configuração de janela de login:** escolha se deseja usar as mesmas credenciais que inseriu na janela de login para autenticar o usuário.
- **Configurações do servidor proxy**
 - **Configuração de proxy:** na lista, escolha **Nenhum**, **Manual** ou **Automático** para definir como a conexão VPN cria rotas em um servidor proxy e configure todas as opções adicionais. O padrão é **Nenhum**, que não requer configuração adicional.
 - Se você escolher **Manual**, defina as seguintes configurações:
 - * **Nome do host/endereço IP:** digite o nome do host ou endereço IP do servidor proxy.
 - * **Porta:** digite o número de porta do servidor proxy.
 - * **Nome de usuário:** digite um nome de usuário opcional para autenticação no servidor proxy.
 - * **Senha:** digite uma senha opcional para autenticação no servidor proxy.
 - Se você escolher **Automático**, defina as seguintes configurações:
 - * **URL do servidor:** digite a URL do arquivo PAC que define a configuração de proxy.
 - * **Permitir conexão direta se o PAC estiver inacessível:** escolha se os usuários terão permissão para se conectarem diretamente com o destino se o arquivo PAC estiver inacessível. O padrão é **On**. Essa opção está disponível somente no iOS 7.0 e versões posteriores.

Configurações do Android

WiFi Policy	Policy Information
1 Policy Info	This policy lets you configure a WiFi profile for devices.
2 Platforms	Network name* <input type="text"/>
<input checked="" type="checkbox"/> iOS	Authentication <input type="text" value="Open"/>
<input checked="" type="checkbox"/> Mac OS X	Encryption <input type="text" value="WEP"/>
<input checked="" type="checkbox"/> Android	Password <input type="text"/>
<input checked="" type="checkbox"/> Windows Phone	Hidden network (enable if network is open or off) <input type="text" value="OFF"/>
<input checked="" type="checkbox"/> Windows Tablet	► Deployment Rules
3 Assignment	

- **Nome da rede:** digite o SSID que está na lista de redes disponíveis do dispositivo do usuário.
- **Autenticação:** na lista, escolha o tipo de segurança para usar com a conexão Wi-Fi.
 - Aberto
 - Compartilhado
 - WPA
 - WPA-PSK
 - WPA2
 - WPA2-PSK
 - 802.1x EAP

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Configurações abertas e compartilhadas para Android

- **Criptografia:** na lista, escolha **Desativado** ou **WEP**. O padrão é **WEP**.
- **Senha:** digite uma senha opcional.

Configurações WPA, WPA-PSK, WPA2, WPA2-PSK para Android

- **Criptografia:** na lista, escolha **TKIP** ou **AES**. O padrão é **TKIP**.
- **Senha:** digite uma senha opcional.

Configurações 802.1x para Android

- **Tipo de EAP:** na lista, escolha **PEAP**, **TLS** ou **TTLS**. O padrão é **PEAP**.

- **Senha:** digite uma senha opcional.
- **Autenticação fase 2:** na lista, clique em **Nenhum**, **PAP**, **MSCHAP**, **MSCHAPv2** ou **GTC**. O padrão é **PAP**.
- **Identidade:** digite o nome de usuário e o domínio opcionais.
- **Anônimo:** digite o nome de usuário opcional, visível externamente. Você pode aumentar a segurança digitando um termo genérico como “anônimo” para que o nome do usuário não possa ser visto.
- **Certificado de CA:** na lista, escolha o certificado a ser usado.
- **Credencial de identidade:** na lista, escolha a credencial de identidade a ser usada. O padrão é **Nenhum**.
- **Rede oculta (ativar se a rede for aberta ou estiver desligada):** escolha se a rede é oculta.

Configurações do Android Enterprise

WiFi Policy

This policy lets you configure a WiFi profile for devices.

Network name *

Authentication Open

Encryption WEP

Password

Hidden network (enable if network is open or off) OFF

► **Deployment Rules**

- **Nome da rede:** digite o SSID que está na lista de redes disponíveis do dispositivo do usuário.
- **Autenticação:** na lista, escolha o tipo de segurança para usar com a conexão Wi-Fi.
 - Aberto
 - Compartilhado
 - WPA
 - WPA-PSK
 - WPA2
 - WPA2-PSK

- 802.1x EAP

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Configurações abertas e compartilhadas para Android

- **Criptografia:** na lista, escolha **Desativado** ou **WEP**. O padrão é **WEP**.
- **Senha:** digite uma senha opcional.

Configurações WPA, WPA-PSK, WPA2, WPA2-PSK para Android

- **Criptografia:** na lista, escolha TKIP ou AES. O padrão é TKIP.
- **Senha:** digite uma senha opcional.

Configurações 802.1x para Android

- **Tipo de EAP:** na lista, escolha **PEAP**, **TLS** ou **TTLS**. O padrão é **PEAP**.
- **Senha:** digite uma senha opcional.
- **Autenticação fase 2:** na lista, clique em **Nenhum**, **PAP**, **MSCHAP**, **MSCHAPPv2** ou **GTC**. O padrão é **PAP**.
- **Identidade:** digite o nome de usuário e o domínio opcionais.
- **Anônimo:** digite o nome de usuário opcional, visível externamente. Você pode aumentar a segurança digitando um termo genérico como “anônimo” para que o nome do usuário não possa ser visto.
- **Certificado de CA:** na lista, escolha o certificado a ser usado.
- **Credencial de identidade:** na lista, escolha a credencial de identidade a ser usada. O padrão é **Nenhum**.
- **Rede oculta (ativar se a rede for aberta ou estiver desligada):** escolha se a rede é oculta.

Configurações do Windows Phone

WiFi Policy	WiFi Policy
1 Policy Info	This policy lets you configure a WiFi profile for devices.
2 Platforms	<p>Network name * <input type="text"/></p> <p>Authentication <input type="text" value="Open"/></p> <p>Connect if hidden <input type="checkbox" value="OFF"/></p> <p>Connect automatically <input type="checkbox" value="OFF"/></p> <p>Proxy server settings</p> <p>Host name or IP address <input type="text"/></p> <p>Port <input type="text"/></p>
<input type="checkbox"/> iOS	<p>► Deployment Rules</p>
<input type="checkbox"/> macOS	
<input type="checkbox"/> Android	
<input checked="" type="checkbox"/> Windows Phone	
<input checked="" type="checkbox"/> Windows Desktop/Tablet	
<input checked="" type="checkbox"/> Windows Mobile/CE	
3 Assignment	

- **Nome da rede:** digite o SSID que está na lista de redes disponíveis do dispositivo do usuário.
- **Autenticação:** na lista, escolha o tipo de segurança para usar com a conexão Wi-Fi.
 - Aberto
 - WPA Pessoal
 - WPA-2 Pessoal
 - WPA-2 Enterprise: para a versão mais recente do Windows 10, o uso do WPA-2 Enterprise requer que você configure o SCEP. A configuração de SCEP permite que o XenMobile envie o certificado a dispositivos para autenticação no servidor Wi-Fi. Para configurar o SCEP, vá para a página **Distribuição de Configurações > Provedores de credenciais**. Para obter mais informações, consulte [Provedores de credenciais](#).

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Configurações abertas para o Windows Phone

- **Conectar se a rede estiver oculta:** escolha se deseja conectar-se quando a rede está oculta.
- **Conectar automaticamente:** escolha se deseja conectar-se automaticamente à rede.

Configurações WPA Pessoal, WPA-2 Pessoal para Windows Phone

- **Criptografia:** na lista, escolha **AES** ou **TKIP** para definir o tipo de criptografia. O padrão é **AES**.
- **Conectar se a rede estiver oculta:** escolha se deseja conectar-se quando a rede está oculta.
- **Conectar automaticamente:** escolha se deseja conectar-se automaticamente à rede.

Configurações WPA-2 Enterprise para Windows Phone

- **Criptografia:** na lista, escolha **AES** ou **TKIP** para definir o tipo de criptografia. O padrão é **AES**.
- **Tipo de EAP:** na lista, escolha **PEAP-MSCHAPv2** ou **TLS** para definir o tipo de EAP. O padrão é **PEAP-MSCHAPv2**.
- **Conectar se a rede estiver oculta:** escolha se deseja conectar-se quando a rede está oculta.
- **Conectar automaticamente:** escolha se deseja conectar-se automaticamente à rede.
- **Enviar certificado por push via SCEP:** escolha se deseja enviar o certificado por push para os dispositivos de usuários via protocolo SCEP.
- **Provedor de credenciais para SCEP:** na lista, escolha o nome do provedor de credenciais para SCEP. O padrão é **Nenhum**.
- **Configurações do servidor proxy**
 - **Nome do host ou endereço IP:** digite o nome ou endereço IP do servidor proxy.
 - **Porta:** digite o número da porta do servidor proxy.
- **Configurações de política**
 - **Remover política:** escolha um método para agendar a remoção da política. As opções disponíveis são **Selecionar data** e **Duração até remoção (em horas)**
 - * **Selecionar data:** clique no calendário para selecionar a data específica para remoção.
 - * **Duração até remoção (em horas):** digite um número, em horas, até que a remoção da política ocorra.
 - **Permitir que o usuário remova a política:** você pode selecionar quando os usuários podem remover a política do dispositivo. Selecione **Sempre**, **Código secreto obrigatório** ou **Nunca** no menu. Se você selecionar **Código secreto obrigatório**, digite um código secreto no campo **Código secreto de remoção**.
 - **Escopo do perfil:** selecione se esta política se aplica a um **Usuário** ou a um **Sistema** inteiro. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

Configurações do Windows 10

WiFi Policy	WiFi Policy
1 Policy Info	This policy lets you configure a WiFi profile for devices.
2 Platforms	<p>Network name * <input type="text"/></p> <p>Authentication <input type="text" value="Open"/></p> <p>Hidden network (enable if network is open or off) <input type="checkbox" value="OFF"/></p> <p>Connect automatically <input type="checkbox" value="OFF"/></p> <p>Proxy server settings</p> <p>Host name or IP address <input type="text"/></p> <p>Port <input type="text"/></p> <p>► Deployment Rules</p>
<input type="checkbox"/> iOS	
<input type="checkbox"/> macOS	
<input type="checkbox"/> Android	
<input type="checkbox"/> Windows Phone	
<input checked="" type="checkbox"/> Windows Desktop/Tablet	
<input checked="" type="checkbox"/> Windows Mobile/CE	
3 Assignment	

- **Autenticação:** na lista, clique no tipo de segurança para usar com a conexão Wi-Fi.
 - Aberto
 - WPA Pessoal
 - WPA-2 Pessoal
 - WPA Enterprise
 - WPA-2 Enterprise: para a versão mais recente do Windows 10, o uso do WPA-2 Enterprise requer que você configure o SCEP. A configuração de SCEP permite que o XenMobile envie o certificado a dispositivos para autenticação no servidor Wi-Fi. Para configurar o SCEP, vá para a página **Distribuição de Configurações > Provedores de credenciais**. Para obter mais informações, consulte [Provedores de credenciais](#).

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Configurações abertas para o Windows 10

- **Rede oculta (ativar se a rede for aberta ou estiver desligada):** escolha se a rede é oculta.
- **Conectar automaticamente:** escolha se deseja conectar-se automaticamente à rede.

Configurações WPA Pessoal, WPA-2 Pessoal para Windows 10

- **Criptografia:** na lista, escolha **AES** ou **TKIP** para definir o tipo de criptografia. O padrão é **AES**.
- **Rede oculta (ativar se a rede for aberta ou estiver desligada):** escolha se a rede é oculta.
- **Conectar automaticamente:** escolha se deseja conectar-se automaticamente à rede.

Configurações WPA-2 Enterprise para Windows 10

- **Criptografia:** na lista, escolha **AES** ou **TKIP** para definir o tipo de criptografia. O padrão é **AES**.
- **Tipo de EAP:** na lista, escolha **PEAP-MSCHAPv2** ou **TLS** para definir o tipo de EAP. O padrão é **PEAP-MSCHAPv2**.
- **Conectar se a rede estiver oculta:** escolha se a rede está oculta.
- **Conectar automaticamente:** escolha se deseja conectar-se automaticamente à rede.
- **Enviar certificado por push via SCEP:** escolha se deseja enviar o certificado por push para os dispositivos de usuários usando o protocolo SCEP.
- **Provedor de credenciais para SCEP:** na lista, escolha o nome do provedor de credenciais para SCEP. O padrão é **Nenhum**.

Configurações do Windows Mobile/CE

WiFi Policy	WiFi Policy
1 Policy Info	This policy lets you configure a WiFi profile for devices.
2 Platforms	Network name * <input type="text"/> ⓘ
<input type="checkbox"/> iOS	Device-to-device connection (ad-hoc) <input type="checkbox"/> OFF
<input type="checkbox"/> macOS	Network Internet ▾
<input type="checkbox"/> Android	Authentication Open ▾
<input type="checkbox"/> Windows Phone	Encryption WEP ▾
<input type="checkbox"/> Windows Desktop/Tablet	Key provided (automatic) <input type="checkbox"/> OFF
<input checked="" type="checkbox"/> Windows Mobile/CE	Password <input type="text"/>
3 Assignment	Key index 1 ▾
	► Deployment Rules

- **Nome da rede:** digite o SSID que está na lista de redes disponíveis do dispositivo do usuário.
- **Conexão de dispositivo a dispositivo (ad-hoc):** permite que dois dispositivos se conectem diretamente. O padrão é **Desativado**.
- **Rede:** escolha se o dispositivo está conectado a uma fonte de internet externa ou a uma intranet de escritório.
- **Autenticação:** na lista, escolha o tipo de segurança para usar com a conexão Wi-Fi.
 - Aberto
 - WPA Pessoal
 - WPA-2 Pessoal
 - WPA-2 Enterprise

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Configurações abertas para o Windows Mobile/CE

- **Rede oculta (ativar se a rede for aberta ou estiver desligada):** escolha se a rede é oculta.
- **Conectar automaticamente:** escolha se deseja conectar-se automaticamente à rede.

Configurações WPA Pessoal, WPA-2 Pessoal para Windows Mobile/CE

- **Criptografia:** na lista, escolha **AES** ou **TKIP** para definir o tipo de criptografia. O padrão é **AES**.
- **Rede oculta (ativar se a rede for aberta ou estiver desligada):** escolha se a rede é oculta.
- **Conectar automaticamente:** escolha se deseja conectar-se automaticamente à rede.

Configurações WPA-2 Enterprise para Windows Mobile/CE

- **Criptografia:** na lista, escolha **AES** ou **TKIP** para definir o tipo de criptografia. O padrão é **AES**.
- **Tipo de EAP:** na lista, escolha **PEAP-MSCHAPv2** ou **TLS** para definir o tipo de EAP. O padrão é **PEAP-MSCHAPv2**.
- **Conectar se a rede estiver oculta:** escolha se a rede está oculta.
- **Conectar automaticamente:** escolha se deseja conectar-se automaticamente à rede.
- **Enviar certificado por push via SCEP:** escolha se deseja enviar o certificado por push para os dispositivos de usuários usando o protocolo SCEP (Simple Certificate Enrollment Protocol).
- **Provedor de credenciais para SCEP:** na lista, escolha o nome do provedor de credenciais para SCEP. O padrão é **Nenhum**.
- **Chave fornecida (automática):** escolha se a chave fornecida é automaticamente ou não. O padrão é **Desativado**.
- **Senha:** digite a senha nesse campo.
- **Índice de chave:** escolha o índice de chave. As opções disponíveis são **1, 2, 3 e 4**.

Política de dispositivo do certificado do Windows CE

April 23, 2020

Você pode criar uma política de dispositivo no XenMobile para criar e fornecer certificados do Windows Mobile/CE de uma PKI externa para os dispositivos de usuários. Para obter mais informações sobre certificados e entidades PKI, consulte [Certificados](#).

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do Windows CE

- **Provedor de credenciais:** na lista, clique no provedor de credenciais. O padrão é **Nenhum**.
- **Senha gerada no formato PKCS#12:** digite a senha usada para criptografar as credenciais.
- **Pasta de destino:** na lista, clique na pasta de destino da credencial ou em **Adicionar novo** para adicionar uma pasta ainda não presente na lista. As opções predefinidas são:
 - %Flash Storage%\
 - %XenMobile Folder%\
 - %Program Files%\
 - %My Documents%\
 - %Windows%\
- **Nome do arquivo de destino:** digite o nome do arquivo de credencial.

Política de dispositivo Proteção de informações do Windows

July 10, 2020

A Proteção de informações do Windows (WIP), conhecida anteriormente como proteção de dados empresariais (EDP), é uma tecnologia do Windows que oferece proteção contra o possível vazamento de dados corporativos. Vazamentos de dados podem ocorrer por meio do compartilhamento de dados empresariais com aplicativos protegidos não corporativos, entre aplicativos ou fora da rede da sua organização. Para obter mais informações, consulte [Proteger os dados empresariais usando a Proteção de Informações do Windows \(WIP\)](#).

Você pode criar uma política de dispositivo no XenMobile para especificar os aplicativos que requerem Proteção de informações do Windows no nível de execução que você definir. A política Proteção de informações do Windows é para telefones, tablets e desktops supervisionados Windows 10 versão 1607 e posteriores.

O XenMobile inclui alguns aplicativos comuns, e você pode adicionar outros. Especifique para a política um nível de execução que afete a experiência do usuário. Por exemplo, você pode:

- Bloquear qualquer compartilhamento de dados impróprio.
- Avisar sobre o compartilhamento de dados impróprio e permitir que os usuários substituam a política.
- Execute o WIP silenciosamente enquanto registra o log e permite o compartilhamento de dados impróprios.

Para excluir aplicativos da Proteção de informações do Windows, defina os aplicativos em arquivos XML do Microsoft AppLocker e, em seguida, importe esses arquivos para o XenMobile.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do Windows 10

Windows Information Protection Policy		Windows Information Protection Policy																						
1 Policy Info		This policy lets you specify the apps that require Windows Information Protection at the enforcement level you set. The policy is supported only on Windows 10 (RS1 and above). Desktop App																						
2 Platforms		<table border="1"> <thead> <tr> <th>File name *</th> <th>Publisher *</th> <th>Product name *</th> <th>Version *</th> <th>Allowed</th> <th>Add</th> </tr> </thead> <tbody> <tr> <td>explore.exe</td> <td>O= [redacted] L= [redacted] S= [redacted]</td> <td>*</td> <td>*</td> <td>Allowed</td> <td></td> </tr> <tr> <td>notepad.exe</td> <td>O= [redacted] L= [redacted] S= [redacted]</td> <td>*</td> <td>*</td> <td>Allowed</td> <td></td> </tr> </tbody> </table>					File name *	Publisher *	Product name *	Version *	Allowed	Add	explore.exe	O= [redacted] L= [redacted] S= [redacted]	*	*	Allowed		notepad.exe	O= [redacted] L= [redacted] S= [redacted]	*	*	Allowed	
File name *	Publisher *	Product name *	Version *	Allowed	Add																			
explore.exe	O= [redacted] L= [redacted] S= [redacted]	*	*	Allowed																				
notepad.exe	O= [redacted] L= [redacted] S= [redacted]	*	*	Allowed																				
3 Assignment																								

- **Aplicativo de área de trabalho** (Tablet Windows 10), **Aplicativo da loja** (telefone e tablet Windows 10): o XenMobile inclui alguns aplicativos comuns, como mostra o exemplo acima. Você pode editar ou remover esses aplicativos conforme necessário.

Para adicionar outros aplicativos: na tabela **Aplicativo de área de trabalho** ou **Aplicativo da loja**, clique em **Adicionar** e forneça as informações do aplicativo.

Aplicativos **permitidos** podem ler, criar e atualizar dados corporativos. Aplicativos **negados** não podem acessar dados corporativos. Aplicativos **isentos** podem ler dados corporativos, mas não podem criar ou modificar os dados.

- **AppLocker XML:** a Microsoft fornece uma lista de aplicativos que apresentam problemas de compatibilidade com a WIP. Para excluir esses aplicativos da WIP, clique em **Procurar** para carregar a lista. O XenMobile combina o AppLocker XML carregado e os aplicativos de área de trabalho e loja configurados na política enviada ao dispositivo. Para obter mais informações, consulte [Recommended deny list for Windows Information Protection](#).
- **Nível de execução:** selecione uma opção para especificar como você deseja que a Proteção de informações do Windows proteja e gerencie o compartilhamento de dados. O padrão é **Desativado**.
 - * **0-Desl.:** A WIP está desativada e não protege ou audita seus dados.
 - * **1-Silencioso:** A WIP é executada silenciosamente, registra o compartilhamento impróprio de dados e não bloqueia nada. Você pode acessar os logs por meio de [Reporting CSP](#).
 - * **2-Substituir:** A WIP avisa os usuários sobre o compartilhamento de dados potencialmente não seguros. Os usuários podem substituir avisos e compartilhar os dados. Esse modo registra ações, incluindo substituições de usuários, no log de auditoria.
 - * **3-Bloquear:** A WIP impede que os usuários concluam o compartilhamento de dados potencialmente não seguros.

- **Nomes de domínio protegidos:** os domínios que a sua empresa utiliza para identidades de usuários. Essa lista de domínios de identidade gerenciados, junto com o domínio primário, compõem a identidade da sua corporação de gerenciamento. O primeiro domínio da lista é a identidade corporativa principal usada na interface de usuário do Windows. Use “|” para separar itens de lista. Por exemplo: `domain1.com | domain2.com`
- **Certificado de recuperação de dados:** clique em **Procurar** e depois selecione um certificado de recuperação para uso na recuperação de dados de arquivos criptografados. Esse certificado é o mesmo que o certificado do agente de recuperação de dados (DRA) do sistema de arquivos de criptografia (EFS), entregue somente por meio do MDM em vez de pela Política de grupo. Se um certificado de recuperação não estiver disponível, crie-o. Para obter informações, consulte “Criar um certificado de recuperação de dados”, nesta seção.
- **Nomes de domínio de rede:** uma lista de domínios que constituem os limites da empresa. A WIP protege todo o tráfego para os domínios totalmente qualificados nessa lista. Essa configuração, junto com a configuração **Faixa de IP**, detecta se um ponto de extremidade de rede é corporativo ou pessoal em redes privadas. Use uma vírgula para separar itens de lista. Por exemplo: `corp.example.com,region.example.com`
- **Faixa de IP:** uma lista das faixas de IPv4 e IPv6 corporativos que definem os computadores na rede corporativa. A WIP considera esses locais um destino seguro para o compartilhamento de dados corporativos. Use uma vírgula para separar itens de lista. Por exemplo:
`10.0.0.0-10.255.255.255,2001:4898::-2001:4898:7fff:ffff:ffff:ffff:ffff:ffff`
- **A lista de faixas de IP é determinante:** para impedir a detecção automática de intervalos IP pelo Windows, altere essa configuração para **Ativado**. O padrão é **Desativado**.
- **Servidores proxy:** uma lista de servidores proxy que a empresa pode usar para recursos corporativos. Essa configuração será necessária se você usar um proxy na rede. Sem um servidor proxy, os recursos corporativos poderão ficar indisponíveis quando um cliente estiver atrás de um proxy. Por exemplo, recursos podem estar indisponíveis em determinados pontos de acesso WiFi em hotéis e restaurantes. Use uma vírgula para separar itens de lista. Por exemplo:
`proxy.example.com:80;157.54.11.118:443`
- **Servidores proxy internos:** uma lista de servidores proxy pelos quais os seus dispositivos passam para acessar seus recursos de nuvem. Usar esse tipo de servidor indica que os recursos de nuvem com os quais você está se conectando são recursos corporativos. Não inclua nessa lista nenhum dos servidores na configuração de **Servidores proxy** que sejam

usados para o tráfego não protegido pela WIP. Use uma vírgula para separar itens de lista. Por exemplo:

```
example.internalproxy1.com;10.147.80.50
```

- **Recursos de nuvem:** uma lista de recursos de nuvem protegidos pela WIP. Para cada recurso de nuvem, você também pode especificar um servidor proxy na lista de **Servidores proxy** para rotear o tráfego para esse recurso de nuvem. Todo o tráfego roteado através de **Servidores proxy** é tratado como tráfego corporativo. Use uma vírgula para separar itens de lista. Por exemplo:

```
domain1.com:InternalProxy.domain1.com, domain2.com:InternalProxy.  
domain2.com
```

- **Definir exigência de proteção após travamento:** somente para telefones Windows 10. Se for **Ativado**, a política de dispositivo de código secreto também será necessária. Caso contrário, a implantação da política de Proteção de informações do Windows falhará. Além disso, se essa política for **Ativada**, a configuração **Exigir proteção durante bloqueio** será exibida. O padrão é **Desativado**.
- **Exigir proteção durante bloqueio:** somente para telefones Windows 10. Especifica se é preciso criptografar dados corporativos usando uma chave protegida por um PIN de funcionário em um dispositivo bloqueado. Aplicativos não podem ler dados corporativos em um dispositivo bloqueado. O padrão é **Ativado**.
- **Revogar o certificado WIP ao cancelar registro:** especifica se as chaves de criptografia locais de um dispositivo de usuário serão ou não revogadas quando seu registro for cancelado da Proteção de informações do Windows. Depois que as chaves de criptografia forem revogadas, um usuário não poderá acessar dados corporativos criptografados. Se for **Desativado**, as chaves não serão revogadas, e o usuário continuará a ter acesso a arquivos protegidos após o cancelamento do registro. O padrão é **Ativado**.
- **Exibir ícones de sobreposição:** especifica se é necessário incluir a sobreposição de ícones da Proteção de informações do Windows em arquivos corporativos no Explorer e em blocos de aplicativos somente corporativos no menu Iniciar. O padrão é **Desativado**.

Criar um certificado de recuperação de dados

Um certificado de recuperação de dados é necessário para ativar a política de **Proteção de informações do Windows**.

1. No computador que está executando o console XenMobile, abra um prompt de comando e navegue até uma pasta (diferente de Windows\System32) na qual você deseja criar um certificado.

2. Execute este comando:

```
cipher /r:ESFDRA
```

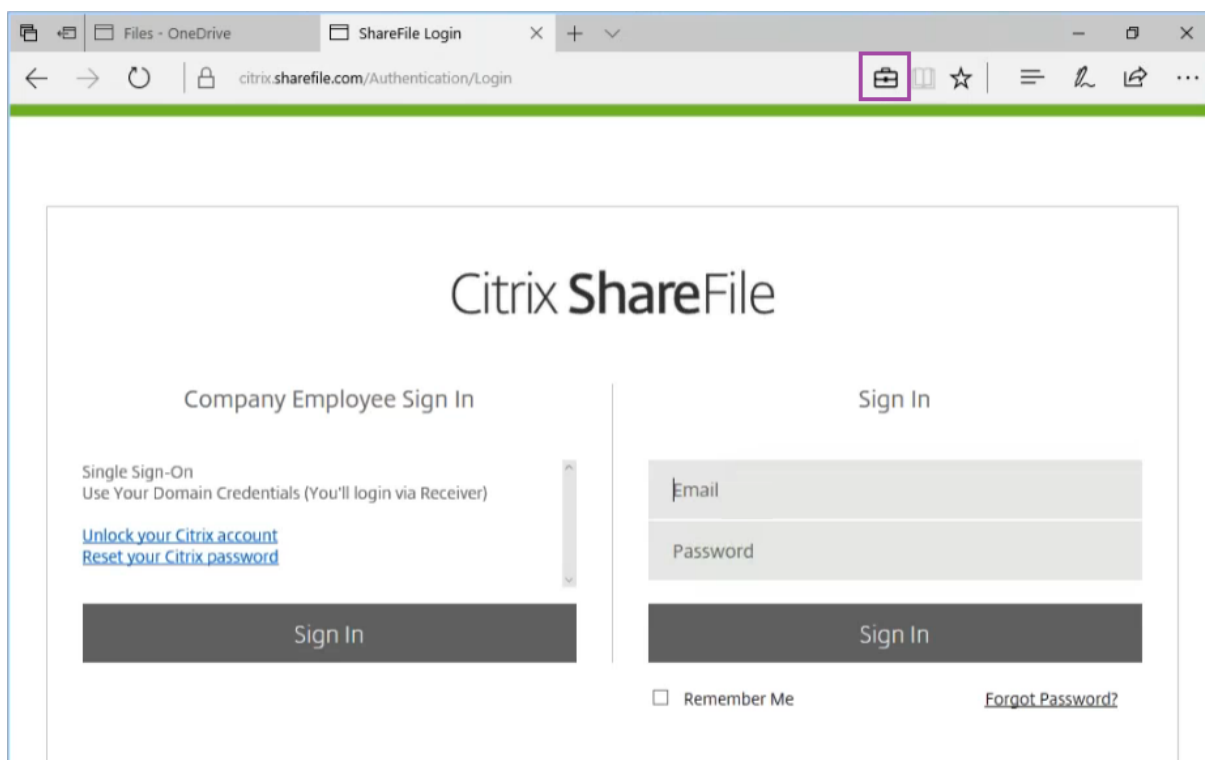
3. Quando solicitado, insira uma senha para proteger o arquivo de chave privada.

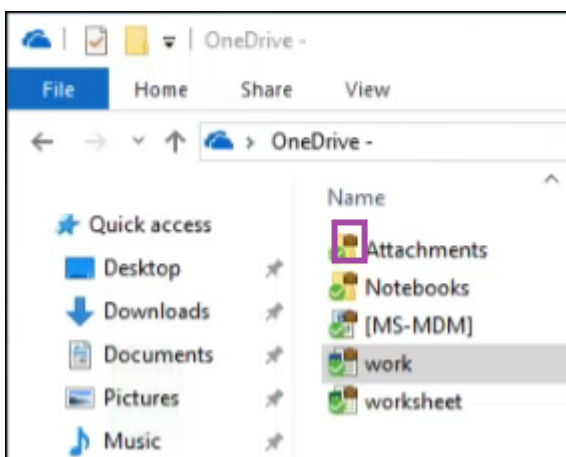
O comando cipher cria um arquivo .cer e .pfx.

4. No console XenMobile, vá para **Configurações > Certificados** e importe o arquivo .cer, que se aplica a tablets e telefones Windows 10.

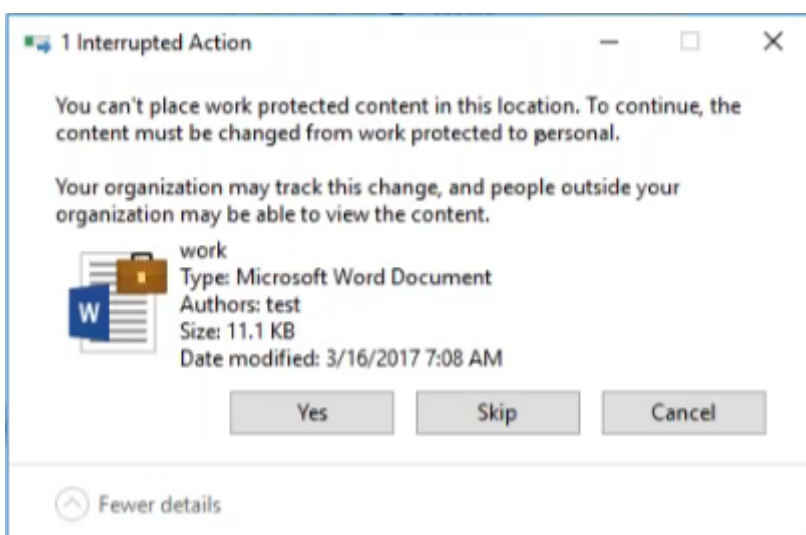
Experiência do usuário

Quando a Proteção de informações do Windows está em vigor, aplicativos e arquivos incluem um ícone:





Se um usuário copiar ou salvar um arquivo protegido em um local não protegido, a seguinte notificação será exibida, dependendo do nível de execução configurado.



Políticas de dispositivo das opções de XenMobile

November 30, 2020

Adicione uma política de opções do XenMobile para configurar o comportamento do Secure Hub quando ele se conecta ao XenMobile de dispositivos Android e Windows Mobile/CE.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Configurações do Android

XenMobile Options Policy

This policy lets you configure parameters for connections to XenMobile.

Device agent configuration

Traybar notification - hide traybar icon OFF

Connection time-out(s) *

Keep-alive interval(s) *

Remote support

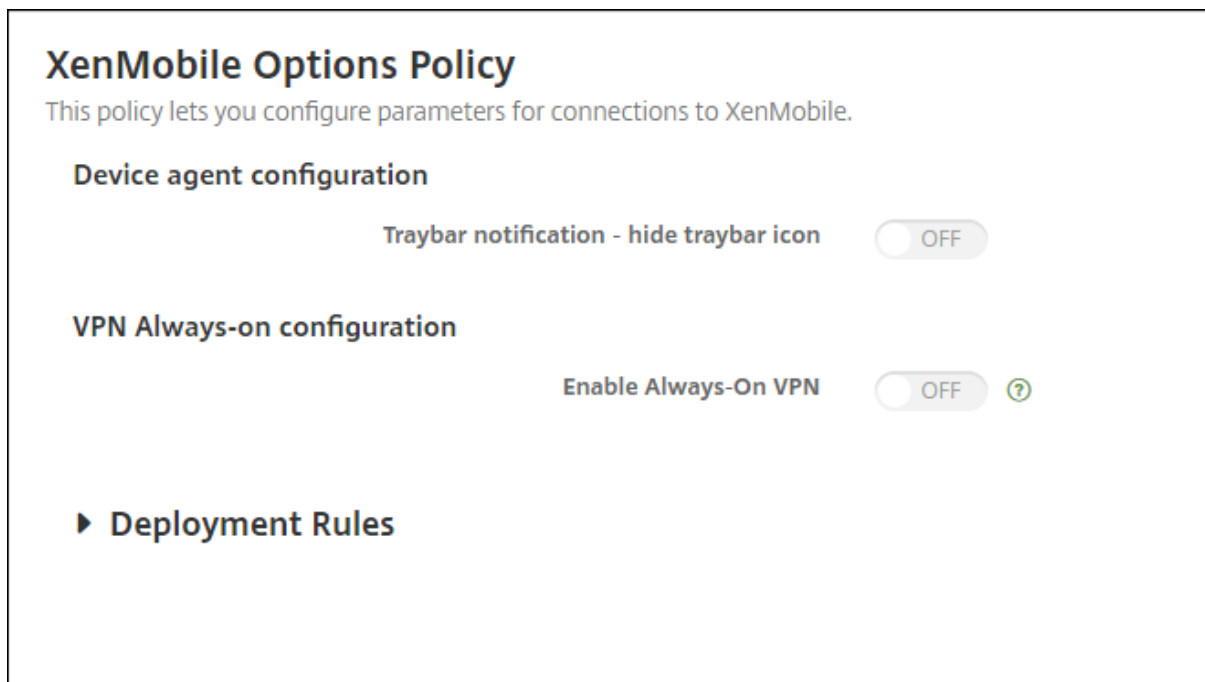
Prompt the user before allowing remote control OFF

Before a file transfer

► **Deployment Rules**

- **Notificação da barra da bandeja - ocultar ícone da barra da bandeja:** selecione se o ícone da barra da bandeja está visível ou oculto. O padrão é **Off**.
- **Tempos limites de conexão:** digite o período de tempo, em segundos, que uma conexão pode ficar inativa antes que ela atinja o tempo limite. O padrão é 20 segundos.
- **Intervalos de persistência de conexões:** digite o período de tempo, em segundos, durante o qual uma conexão deve ser mantida aberta. O padrão é 120 segundos.
- **Avisar ao usuário antes de permitir o controle remoto:** selecione se o usuário deve ser perguntado antes de permitir o controle de suporte remoto. O padrão é **Off**.
- **Antes da transferência de um arquivo:** na lista, clique para selecionar se o usuário deve ser alertado sobre uma transferência de arquivo ou se a permissão do usuário deve ser pedida. Valores disponíveis: **Não avisar ao usuário**, **Avisar ao usuário** e **Pedir permissão do usuário**. O padrão é **Não avisar ao usuário**.

Configurações do Android Enterprise



Com suporte a partir da versão 7 do Android.

- **Notificação da barra da bandeja - ocultar ícone da barra da bandeja:** selecione se o ícone da barra da bandeja está visível ou oculto. O padrão é **Off**.
- **Ativar VPN sempre ativa.** Selecione se a VPN sempre ativa está habilitada ou não. Quando esta definição é **Ativada**, o serviço VPN é iniciado quando o dispositivo é ligado e continua a ser executado enquanto o dispositivo estiver ligado. O padrão é **Desativado**.
- **Pacote de VPN.** Digite o nome do pacote do aplicativo VPN que o dispositivo usa. Por padrão, o nome do pacote do aplicativo Citrix SSO, **com.citrix.CitrixVPN**, é preenchido automaticamente neste campo.

Configurações do Windows Mobile/CE

XenMobile Options Policy	XenMobile Options Policy This policy lets you configure parameters for connections to XenMobile.	
1 Policy Info	Device agent configuration	
2 Platforms	XenMobile backup configuration	Disabled
<input checked="" type="checkbox"/> Android	Connect to the office network	<input checked="" type="checkbox"/> ON
<input checked="" type="checkbox"/> Windows Mobile/CE	Connect to the Internet network	<input checked="" type="checkbox"/> ON
3 Assignment	Connect to the built-in office network	<input checked="" type="checkbox"/> ON
	Connect to the built-in Internet network	<input checked="" type="checkbox"/> ON
	Traybar notification - hide traybar icon	<input type="checkbox"/> OFF
	Connection time-out(s)*	20
	Keep-alive interval(s)*	120
	Remote support	
	Prompt the user before allowing remote control	<input type="checkbox"/> OFF
	Before a file transfer	Do not warn the user
	▶ Deployment Rules	

- **Configuração de agente de dispositivo**
 - **Configuração de backup do XenMobile:** na lista, clique em uma opção para fazer backup da configuração do XenMobile nos dispositivos dos usuários. O padrão é **Desativado**. As opções disponíveis são:
 - * Desativado
 - * Na primeira conexão após a instalação do XenMobile
 - * Na primeira conexão após a reinicialização de cada dispositivo
 - **Conectar à rede do escritório**
 - **Conectar à rede de Internet**
 - **Conectar à rede interna do escritório:** quando essa opção é definida como **I**, o XenMobile detecta automaticamente a rede.
 - **Conectar à rede de Internet interna:** quando essa opção é definida como **I**, o XenMobile detecta automaticamente a rede.
 - **Notificação da barra da bandeja - ocultar ícone da barra da bandeja:** selecione se o ícone da barra da bandeja está visível ou oculto. O padrão é **Off**.
 - **Tempos limites de conexão:** digite o período de tempo, em segundos, que uma conexão

pode ficar inativa antes que ela atinja o tempo limite. O padrão é 20 segundos.

- **Intervalos de persistência de conexões:** digite o período de tempo, em segundos, durante o qual uma conexão deve ser mantida aberta. O padrão é 120 segundos.
- **Suporte remoto**
 - **Avisar ao usuário antes de permitir o controle remoto:** selecione se o usuário deve ser perguntado antes de permitir o controle de suporte remoto. O padrão é **Off**.
 - **Antes da transferência de um arquivo:** na lista, clique para selecionar se o usuário deve ser alertado sobre uma transferência de arquivo ou se a permissão do usuário deve ser pedida. Valores disponíveis: **Não avisar ao usuário**, **Avisar ao usuário** e **Pedir permissão do usuário**. O padrão é **Não avisar ao usuário**.

Política de dispositivo de desinstalação do XenMobile

April 23, 2020

Você pode adicionar uma política de dispositivo no XenMobile para desinstalar o XenMobile dos dispositivos Android e Windows Mobile/CE. Quando implantada, essa política remove o XenMobile de todos os dispositivos no grupo de implantação.

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**. Para obter mais informações, consulte [Políticas de dispositivo](#).

Definir as configurações do Android e do Windows Mobile/CE

- **Desinstalar XenMobile dos dispositivos:** selecione se o XenMobile deve ser desinstalado de cada dispositivo no qual você implantar essa política. O padrão é **Off**.

Adicionar aplicativos

May 24, 2021

A adição de aplicativos ao XenMobile fornece recursos de gerenciamento de aplicativo móvel (MAM). O XenMobile auxilia na entrega de aplicativos, licenciamento de software, configuração e gerenciamento do ciclo de vida do aplicativo.

Aplicativos habilitados para MDX é uma parte importante da preparação da maioria dos tipos de aplicativos para distribuição para dispositivos do usuário. Para obter uma introdução ao MDX, consulte [Sobre o MDX Toolkit](#) e [Visão geral do MAM SDK](#).

- A Citrix recomenda o uso do SDK do MAM para aplicativos habilitados para MDX. Ou você pode continuar com aplicativos preparados com MDX até que o MDX Toolkit seja preterido. Consulte [Substituição](#).
- Você não pode usar o MDX Service ou o MDX Toolkit para preparar os aplicativos móveis de produtividade Citrix. Obtenha os arquivos MDX do aplicativo móvel de produtividade nos downloads da Citrix.

Ao adicionar aplicativos ao console XenMobile, você:

- Define as configurações do aplicativo
- Opcionalmente, organiza os aplicativos em categorias para organizá-los no Secure Hub
- Opcionalmente, define fluxos de trabalho para exigir aprovação antes de permitir que os usuários acessem um aplicativo
- Implanta aplicativos para usuários

Este artigo aborda os fluxos de trabalho gerais para adicionar aplicativos. Consulte os seguintes artigos para detalhes da plataforma:

- [Distribuir aplicativos Android Enterprise](#)
- [Distribuir aplicativos da Apple](#)

Tipos de aplicativos e recursos

A tabela a seguir resume os tipos de aplicativos que você pode implantar com o XenMobile.

Tipo de aplicativo	Fontes	Observações	Consulte
MDX	Aplicativos iOS e Android que você desenvolve para seus usuários. Aplicativos móveis de produtividade Citrix.	Desenvolva aplicativos iOS ou Android com o MAM SDK ou prepare-os com o MDX Service ou Toolkit. Para os aplicativos móveis de produtividade, baixe os arquivos MDX da loja pública nos downloads da Citrix. Em seguida, adicione os aplicativos ao XenMobile.	Acrescentar um aplicativo MDX

Tipo de aplicativo	Fontes	Observações	Consulte
Loja de aplicativos pública	Aplicativos gratuitos ou pagos de lojas de aplicativos públicas, como Google Play ou Apple App Store.	Carregue os aplicativos, habilite os aplicativos para MDX e adicione os aplicativos ao XenMobile.	Acrescentar um aplicativo de loja de aplicativos pública
Web e SaaS.	Sua rede interna (aplicativos Web) ou uma rede pública (SaaS).	O Citrix Workspace oferece logon único móvel para aplicativos SaaS nativos a partir de dispositivos iOS e Android registrados no MDM. Ou use conectores de aplicativo SAML (Security Assertion Markup Language).	Acrescentar um aplicativo Web ou SaaS
Empresarial	Aplicativos privados, incluindo aplicativos Win32, que não são habilitados para MDX. Aplicativos privados do Android Enterprise habilitados para MDX. Os aplicativos empresariais residem em locais de redes de distribuição de conteúdo ou servidores XenMobile.	Adicione os aplicativos ao XenMobile.	Acrescentar um aplicativo empresarial

Tipo de aplicativo	Fontes	Observações	Consulte
Link da Web	Endereços Web da Internet, endereços Web da intranet ou aplicativos Web que não exigem logon único.	Configure links da Web no XenMobile.	Adicionar um link da Web

Ao planejar a distribuição de aplicativos, considere estes recursos:

- Sobre instalações silenciosas
- Sobre aplicativos obrigatórios e opcionais
- Sobre categorias de aplicativos
- Ativar aplicativos do Microsoft Office 365
- Aplicar fluxos de trabalho
- Identidade visual do App store e Citrix Secure Hub

Sobre instalações silenciosas

A Citrix oferece suporte à instalação silenciosa e à atualização de aplicativos iOS, Android Enterprise e Samsung. A instalação silenciosa significa que os usuários não são solicitados a instalar aplicativos que você implanta no dispositivo. Os aplicativos são instalados automaticamente em segundo plano.

Pré-requisitos para implementar a instalação silenciosa:

- Para iOS, coloque o dispositivo iOS gerenciado no modo supervisionado. Para obter detalhes, consulte [Política de dispositivo de importação do perfil de iOS e macOS](#).
- Para o Android Enterprise, os aplicativos são instalados no perfil de trabalho do Android no dispositivo. Para obter detalhes, consulte [Android Enterprise](#).
- Para dispositivos Samsung, ative o Samsung Knox no dispositivo.

Para fazer isso, você define a política de dispositivo de chave de licença MDM Samsung para gerar as chaves de licença ELM Samsung e Knox. Para obter detalhes, consulte [Políticas de dispositivo de chave de licença MDM Samsung](#).

Sobre aplicativos obrigatórios e opcionais

Quando você adiciona aplicativos a um grupo de entrega, escolha se eles são opcionais ou necessários. A Citrix recomenda a implantação de aplicativos conforme **Obrigatório**.

- Aplicativos obrigatórios são instalados silenciosamente nos dispositivos do usuário, minimizando a interação. Ter esse recurso habilitado também permite que os aplicativos sejam atualizados automaticamente.
- Os aplicativos opcionais permitem que os usuários escolham quais aplicativos instalar, mas os usuários devem iniciar a instalação manualmente por meio do Secure Hub.

Para aplicativos marcados como necessários, os usuários podem receber atualizações imediatamente em situações como:

- Carregue um novo aplicativo e marque-o conforme necessário.
- Marque um aplicativo existente conforme necessário.
- Um usuário exclui um aplicativo necessário.
- Está disponível uma atualização do Secure Hub.

Requisitos para a implantação forçada dos aplicativos necessários

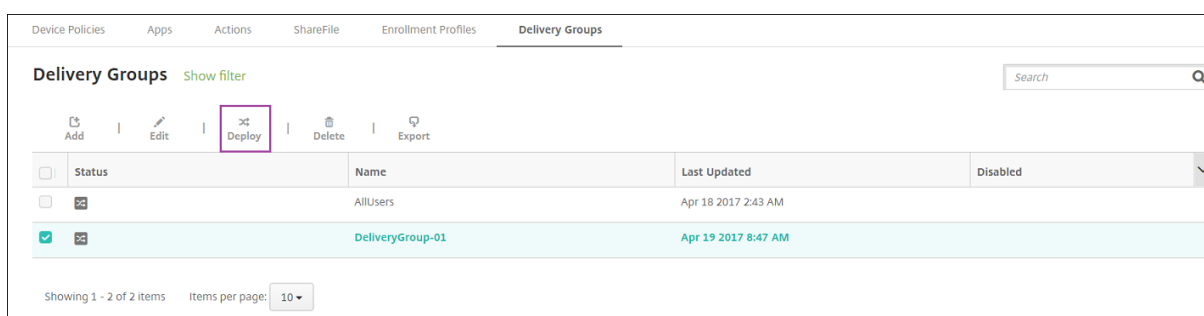
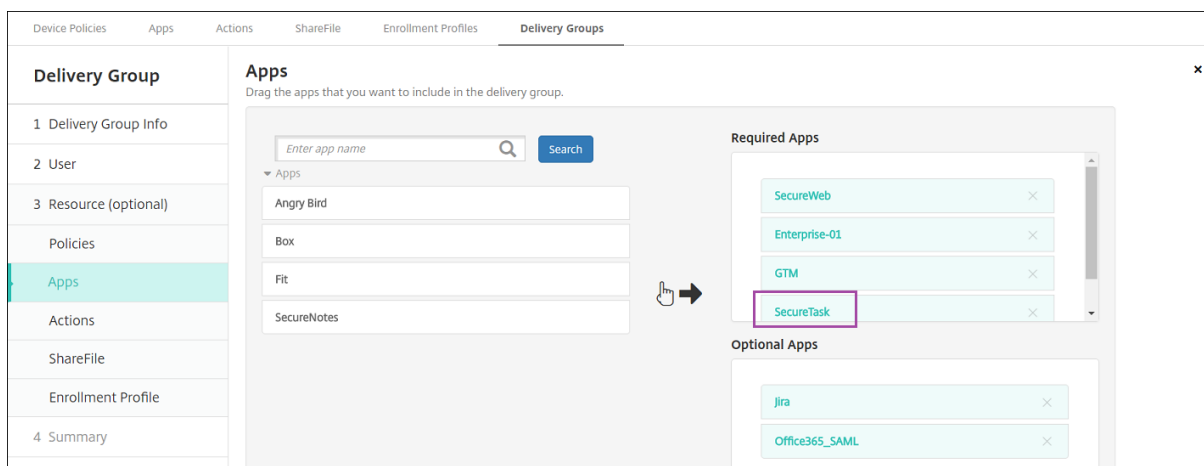
- XenMobile Server 10.6 (versão mínima)
- Secure Hub 10.5.15 para iOS e 10.5.20 para Android (versões mínimas)
- MAM SDK, MDX Service ou MDX Toolkit 10.6 (versão mínima)
- Propriedade personalizada de servidor, `force.server.push.required.apps`

A implantação forçada dos aplicativos necessários está desativada por padrão. Para ativar o recurso, crie uma propriedade personalizada de servidor principal. Defina a **Chave** e o **Nome de exibição** para **`force.server.push.required.apps`** e defina o **Valor** como **verdadeiro**.

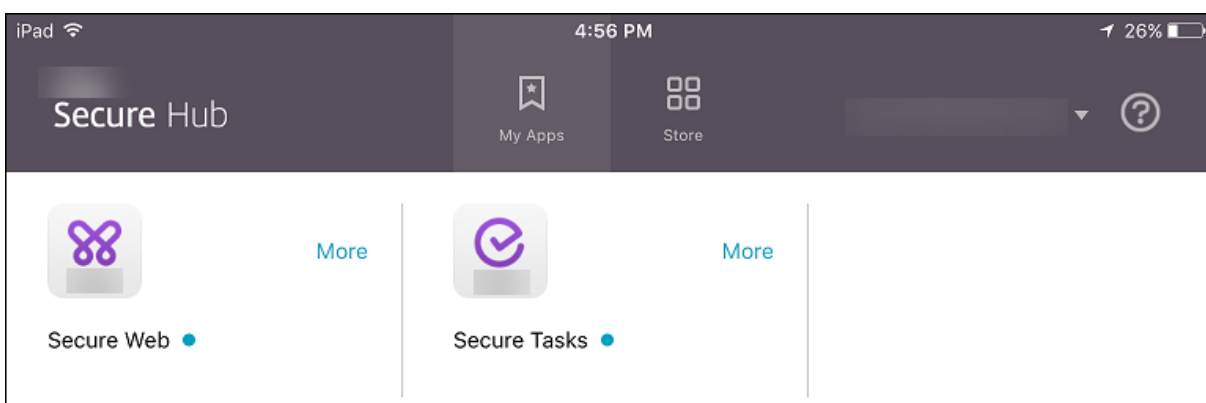
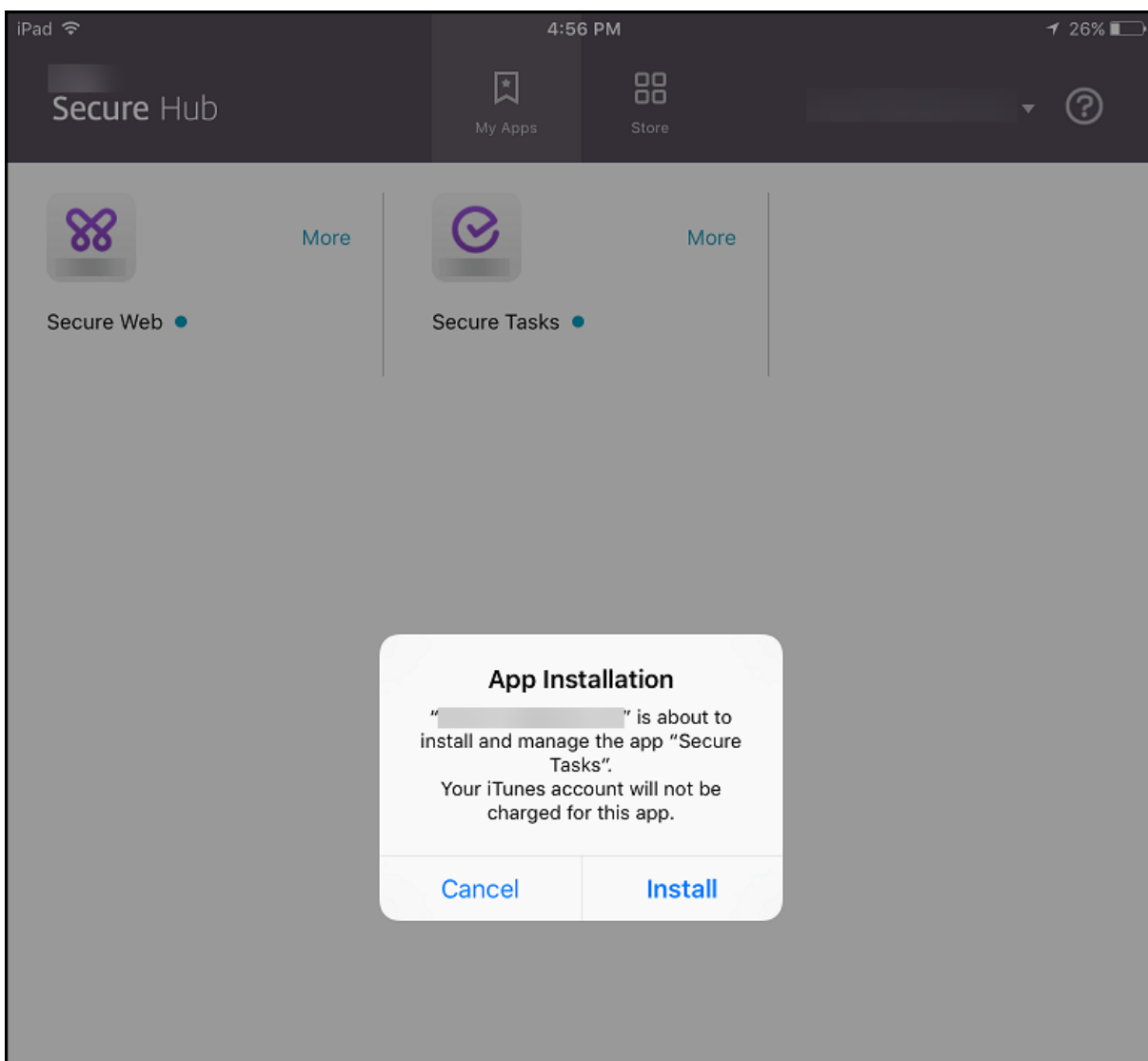
- Após a atualização do XenMobile Server e do Secure Hub: os usuários com dispositivos registrados devem fazer logoff e, em seguida, fazer logon no Secure Hub, uma vez, para obter as atualizações necessárias de implantação de aplicativos.

Exemplos

Os exemplos a seguir mostram a sequência de adicionar um aplicativo chamado Secure Tasks a um grupo de entrega e, em seguida, implantar o grupo de entrega.



Depois que o aplicativo de exemplo, o Secure Tasks, implanta o dispositivo do usuário, o Secure Hub avisa ao usuário para instalar o aplicativo.



Importante:

Os aplicativos obrigatórios habilitados para MDX, incluindo aplicativos corporativos e aplicativos da loja de aplicativos pública, são atualizados imediatamente. A atualização ocorre mesmo se

você configurar uma política MDX para um período de tolerância de atualização do aplicativo e o usuário optar por atualizar o aplicativo posteriormente.

Fluxo de trabalho do aplicativo necessário do iOS para aplicativos empresariais e de lojas públicas

1. Implante o XenMobile App durante o registro inicial. O aplicativo necessário está instalado no dispositivo.
2. Atualize o aplicativo no console XenMobile.
3. Use o console XenMobile para implantar os aplicativos necessários.
4. O aplicativo na tela inicial é atualizado. E, para aplicativos da loja pública, a atualização é iniciada automaticamente. Os usuários não são solicitados a atualizar.
5. Os usuários abrem o aplicativo a partir da tela inicial. Os aplicativos são atualizados imediatamente, mesmo se você definir um período de tolerância de atualização de aplicativo e o usuário tocar para atualizar o aplicativo mais tarde.

Fluxo de trabalho do aplicativo necessário exigido pelo Android para aplicativos empresariais

1. Implante o XenMobile App durante o registro inicial. O aplicativo necessário está instalado no dispositivo.
2. Use o console XenMobile para implantar os aplicativos necessários.
3. O aplicativo está atualizado. (Os dispositivos Nexus solicitam para instalar atualizações, mas dispositivos Samsung fazem uma instalação silenciosa).
4. Os usuários abrem o aplicativo a partir da tela inicial. Os aplicativos são atualizados imediatamente, mesmo se você definir um período de tolerância de atualização de aplicativo e o usuário tocar para atualizar o aplicativo mais tarde. (Os dispositivos Samsung fazem uma instalação silenciosa.)

Fluxo de trabalho do aplicativo necessário do Android para aplicativos de lojas públicas

1. Implante os XenMobile Apps durante o registro inicial. O aplicativo necessário está instalado no dispositivo.
2. Atualize o aplicativo no console XenMobile.
3. Use o console XenMobile para implantar os aplicativos necessários. Ou abra a loja do Secure Hub no dispositivo. O ícone de atualização aparece na loja.
4. A atualização do aplicativo começa imediatamente. (Os dispositivos Nexus solicitam que os usuários instalem a atualização.)
5. Abra o aplicativo a partir da tela inicial. O aplicativo está atualizado. Os usuários não são avisados sobre um período de tolerância. (Os dispositivos Samsung fazem uma instalação silenciosa.)

Desinstalar um aplicativo quando o aplicativo está configurado como obrigatório

Você pode permitir que os usuários desinstalem um aplicativo configurado como obrigatório. Vá para **Configurar > Grupos de Entrega** e mova o aplicativo de **Aplicativos obrigatórios** para **Aplicativos opcionais**.

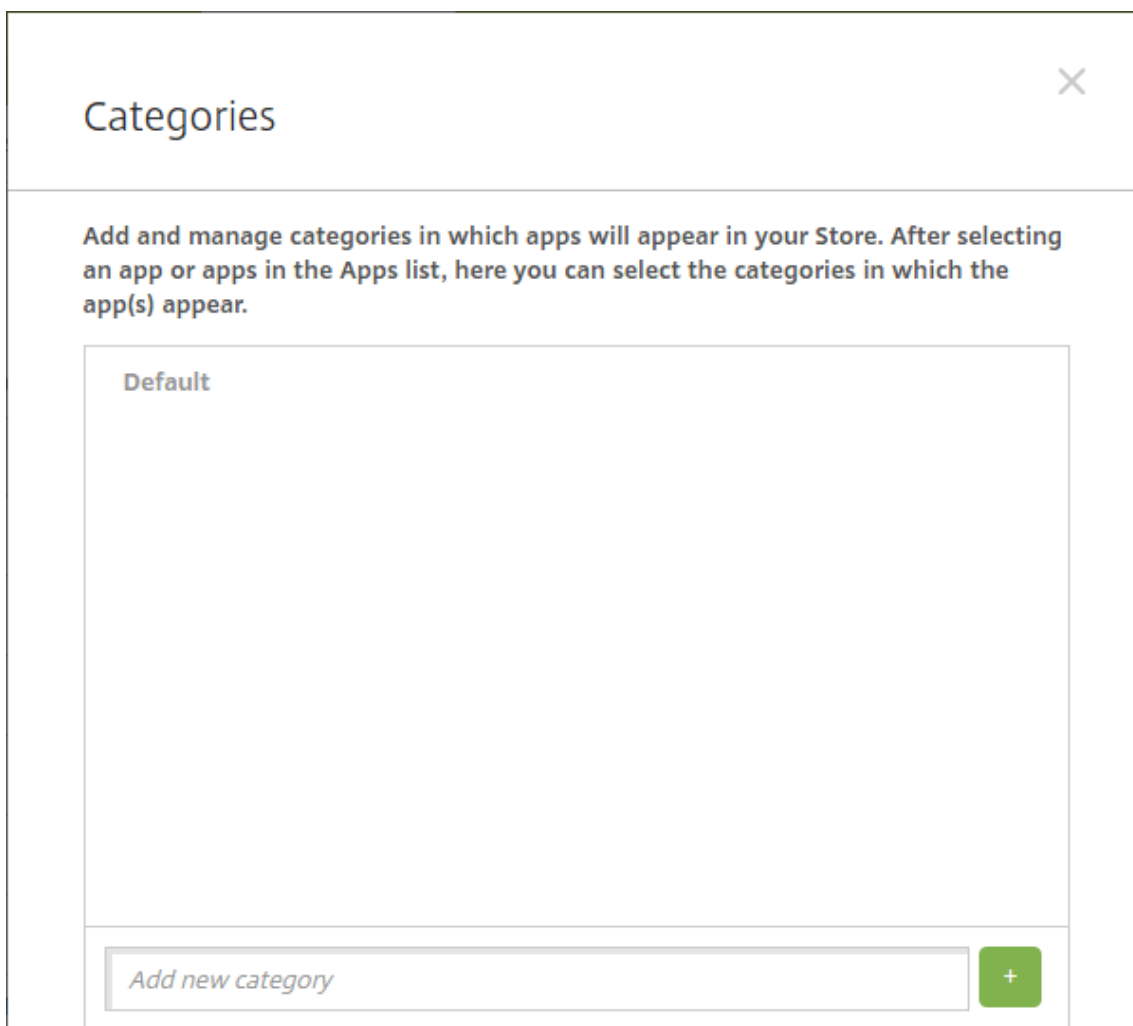
Recomendado: use um grupo de entrega especial para alterar temporariamente um aplicativo para opcional, de modo que usuários específicos possam desinstalar o aplicativo. Assim você pode alterar um aplicativo existente de obrigatório para opcional, implantar o aplicativo no grupo de entrega e desinstalar o aplicativo dos dispositivos. Depois disso, se você quiser que os registros futuros daquele grupo de entrega exijam o aplicativo, você pode definir o aplicativo de volta como obrigatório.

Sobre categorias de aplicativos

Quando os usuários fazem login no Secure Hub, eles recebem uma lista dos aplicativos, links da Web e lojas que você configurou no XenMobile. É possível usar categorias de aplicativos para permitir que os usuários acessem somente determinados aplicativos, lojas ou links da Web. Por exemplo, você pode criar uma categoria Finanças e adicionar à categoria os aplicativos que pertencem somente a finanças. Ou pode configurar uma categoria Vendas à qual atribuir os aplicativos de vendas.

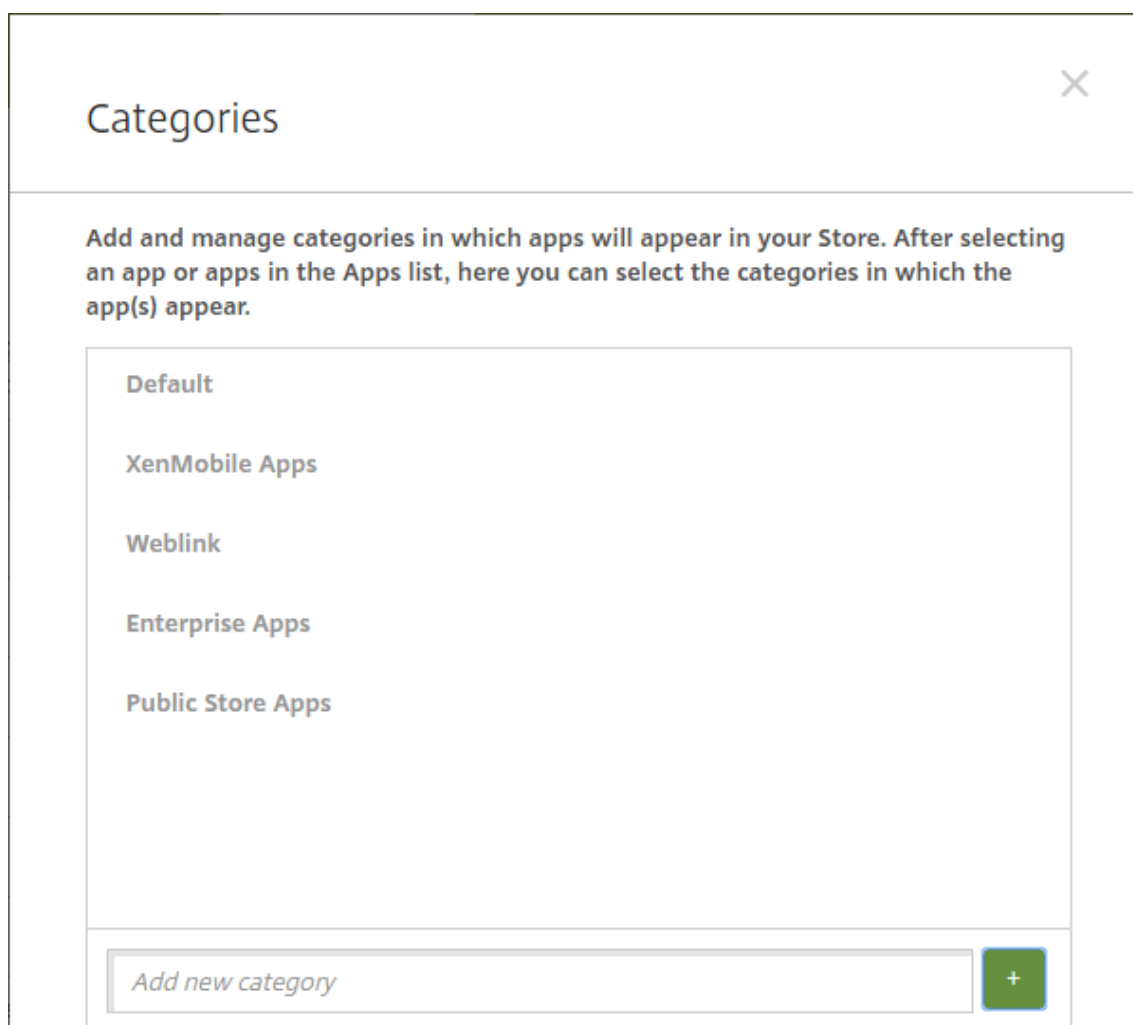
Quando você adicionar ou editar um aplicativo, link da Web ou loja, poderá adicionar o aplicativo a uma ou mais das categorias configuradas.

1. No console XenMobile, clique em **Configurar > Aplicativos > Categoria**. A caixa de diálogo **Categorias** é exibida.



2. Para cada categoria que você deseja adicionar, faça o seguinte:

- Digite o nome da categoria que você deseja adicionar no campo **Adicionar uma nova categoria** na parte inferior da caixa de diálogo. Por exemplo, você pode digitar Aplicativos empresariais para criar uma categoria de aplicativos empresariais.
- Clique no sinal de adição (+) para adicionar a categoria. A categoria recém-criada é adicionada e aparece na caixa de diálogo **Categorias**.



3. Quando terminar de adicionar categorias, feche a caixa de diálogo **Categorias**.
4. Na página **Aplicativos**, você pode colocar um aplicativo existente em uma nova categoria.
 - Selecione o aplicativo que você deseja categorizar.
 - Clique em **Edit**. A página **Informações do Aplicativo** é exibida.
 - Na lista **Categoria do aplicativo**, aplique a nova categoria marcando a caixa de seleção da categoria. Desmarque as caixas de seleção das categorias existentes que você não deseja aplicar ao aplicativo.
 - Clique na guia **Atribuições do grupo de entrega** ou em **Avançar** em cada uma das páginas seguintes para percorrer as páginas de configuração de aplicativo restantes.
 - Clique em **Salvar** na página **Atribuições do grupo de entrega** para aplicar a nova categoria. A nova categoria é aplicada ao aplicativo e é exibida na tabela **Aplicativos**.

Acrescentar um aplicativo MDX

Quando você recebe um arquivo MDX preparado para um aplicativo iOS ou Android, você pode carregar o aplicativo para o XenMobile. Depois de carregar o aplicativo, você pode configurar os detalhes do aplicativo e as configurações de política. Para obter mais informações sobre as políticas de aplicativo que estão disponíveis para cada tipo de plataforma de dispositivo, consulte:

- [Visão geral do SDK MAM](#)
- [Resumo das políticas do MDX](#)

1. No console XenMobile, clique em **Configurar > Aplicativos**. A página **Aplicativos** é exibida.

Icon	App Name	Type	Category	Created On	Last Updated	Disable
	Citrix Secure Web - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	
	Citrix Secure Hub - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	
	Classroom - VPP	Public App Store	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	
	MRF Android Enterprise TD	Enterprise	Default	7/21/17 1:49 PM	7/21/17 1:49 PM	

2. Clique em **Add**. A caixa de diálogo **Adicionar Aplicativo** é exibida.

Click on an app type and then follow the steps to add a deployable app. The app appears in the app table after you complete the steps.

- MDX**
Apps wrapped with the MDX Toolkit to include app policies. You can deploy MDX apps obtained from internal and public stores.
Example: WorxMail
- Public App Store**
Free or paid apps available in a public app store, such as iTunes or Google Play, for download.
Example: GoToMeeting
- Web & SaaS**
Apps accessed from an internal network (Web apps) or over a public network (SaaS). You can create your own apps or choose from a set of app connectors for single sign-on authentication to web apps.
Example: GoogleApps_SAML
- Enterprise**
Native apps not wrapped with the MDX Toolkit and that do not contain the policies found in MDX apps.
Example: Quick-iLaunch
- Web Link**
A Web address (URL) to a public or private site or to a Web app that doesn't require single sign-on.

3. Clique em **MDX**. A página **Informações do aplicativo MDX** é exibida.

4. No painel **Informações do aplicativo**, digite as seguintes informações:

- **Nome:** digite um nome descritivo para o aplicativo. O nome aparecerá em **Nome do aplicativo** na tabela **Aplicativos**.
- **Descrição:** digite uma descrição opcional para o aplicativo.

- **Categoria do aplicativo:** opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte Sobre categorias de aplicativos.
5. Clique em **Avançar**. A página **Plataformas do aplicativo** é exibida.
 6. Em **Plataformas**, selecione as plataformas que você deseja adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.
 7. Para selecionar o arquivo MDX a ser carregado, clique em **Carregar** e navegue para a localização do arquivo.
 8. Na página **Detalhes do aplicativo**, defina estas configurações:
 - **Nome do arquivo:** digite o nome de arquivo associado ao aplicativo.
 - **Descrição do aplicativo:** digite uma descrição para o aplicativo.
 - **Versão do aplicativo:** opcionalmente, digite o número da versão do aplicativo.
 - **ID de pacote:** digite o ID do pacote para o aplicativo, obtido no Google Play Store gerenciado.
 - **Versão do SO mínima:** opcionalmente, digite a versão mais antiga do sistema operacional que o dispositivo pode executar para usar o aplicativo.
 - **Versão do SO máxima:** opcionalmente, digite a versão mais recente do sistema operacional que o dispositivo deve executar para usar o aplicativo.
 - **Dispositivos excluídos:** opcionalmente, digite o fabricante ou os modelos de dispositivos que não podem executar o aplicativo.
 - **Remover aplicativo se o perfil MDM for removido:** selecione se o aplicativo deve ser removido de um dispositivo iOS quando o perfil MDM é removido. O padrão é **On**.
 - **Evitar o backup de dados do aplicativo:** selecione se deseja impedir que usuários façam backup de dados do aplicativo em dispositivos iOS. O padrão é **On**.
 - **Rastreamento de produtos:** especifique qual rastreamento de produto você deseja enviar para os dispositivos iOS. Se você tiver um rastreamento projetado para testes, poderá selecioná-lo e atribuí-lo aos seus usuários. O padrão é **Produção**.
 - **Forçar aplicativo a ser gerenciado:** para um aplicativo que seja instalado como não gerenciado, selecione se deseja solicitar que os usuários permitam que o aplicativo seja gerenciado em dispositivos iOS não supervisionados. O padrão é **On**.
 - **Aplicativo implantado via compra por volume:** selecione se você deseja implantar o aplicativo usando a compra por volume da Apple. Se estiver **Ativado** e você implantar uma versão do MDX do aplicativo e usar a compra por volume para implantar o aplicativo, o Secure Hub mostra somente a instância do volume de compra. O padrão é **Desativado**.
 9. Configure as **Políticas de MDX**. As políticas de MDX variam por plataforma e incluem opções para áreas de política como autenticação, segurança do dispositivo e restrições de aplicativo. No console, cada uma das políticas tem uma dica de ferramenta que descreve a política.

10. Configure as regras de implantação. Para obter informações, consulte [Regras de implantação](#).

11. Expanda **Configuração da loja**.

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

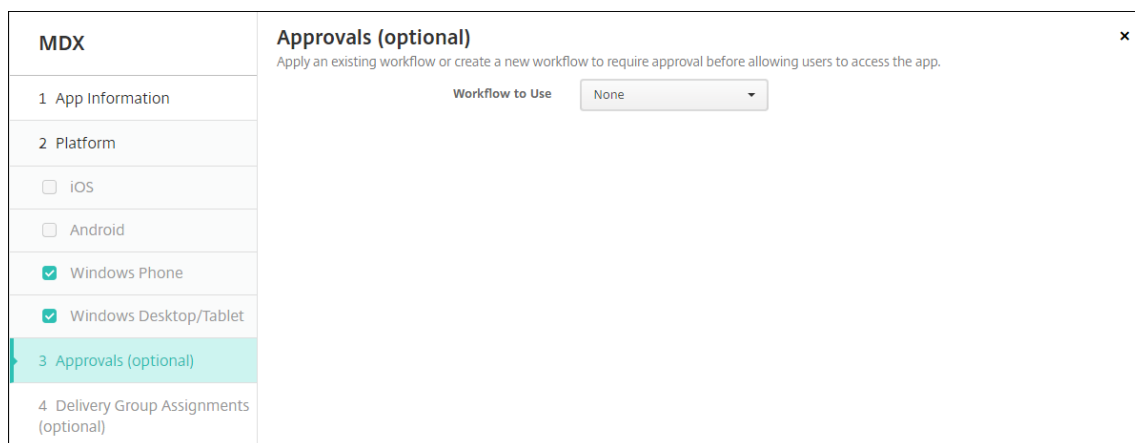
Choose File

Allow app ratings

Allow app comments

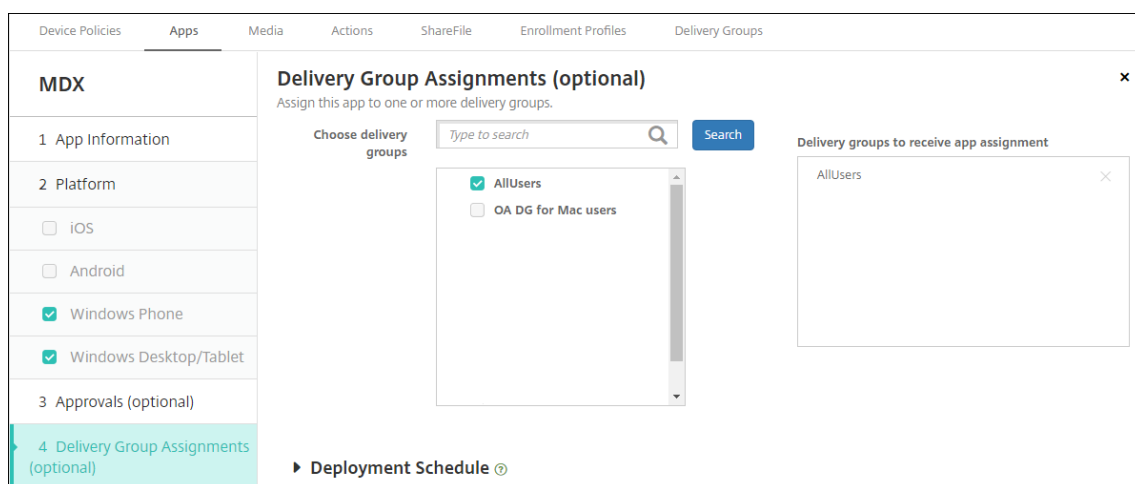
- **Perguntas frequentes sobre o aplicativo:** clique em **Adicionar uma nova pergunta e resposta de Perguntas frequentes** para criar uma Pergunta frequente para o aplicativo.
- **Adicionar capturas de tela para telefones/tablets:** adicionar capturas de tela que aparecem na loja de aplicativos.
- **Permitir classificações do aplicativo:** permitir que os usuários avaliem o aplicativo na loja de aplicativos.
- **Permitir comentários do aplicativo:** permitir que os usuários deixem comentários sobre o aplicativo na loja de aplicativos.

12. Clique em **Avançar**. A página **Aprovações** é exibida.



Para usar fluxos de trabalho para exigir aprovação antes de permitir que os usuários acessem o aplicativo, consulte Aplicar fluxos de trabalho. Se você não quiser configurar fluxos de trabalho de aprovação, continue com a próxima etapa.

13. Clique em **Avançar**. A página **Atribuição de grupo de entrega** é exibida.



14. Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega ou selecione um ou mais grupos. Os grupos que você selecionar aparecerão na lista **Grupos de entrega que receberão a atribuição de aplicativos**.

15. Expanda **Cronograma de implantação** e defina estas configurações:

- **Implantar:** escolha se deseja implantar o aplicativo em dispositivos. O padrão é **On**.
- **Cronograma de implantação:** escolha se deseja implantar o aplicativo **Agora** ou **Mais tarde**. Se você selecionar **Mais tarde**, configure uma data e hora para implantar o aplicativo. O padrão é **Agora**.
- **Condição de implantação:** escolha **Em cada conexão** para implantar o aplicativo sempre que o dispositivo se conectar. Escolha **Somente quando a implantação anterior tiver falhado** para implantar o aplicativo quando o dispositivo não conseguir receber o aplicativo anteriormente. O padrão é **Em cada conexão**.

A opção **Implantar para conexões permanentes** é aplicável quando você tiver configurado a chave de implantação em segundo plano do cronograma em **Configurações > Propriedades do servidor**.

O cronograma de implantação que você configura é o mesmo para todas as plataformas. Todas as alterações feitas se aplicam a todas as plataformas, exceto **Implantar para conexões permanentes**.

16. Clique em **Salvar**.

Acrescentar um aplicativo de loja de aplicativos pública

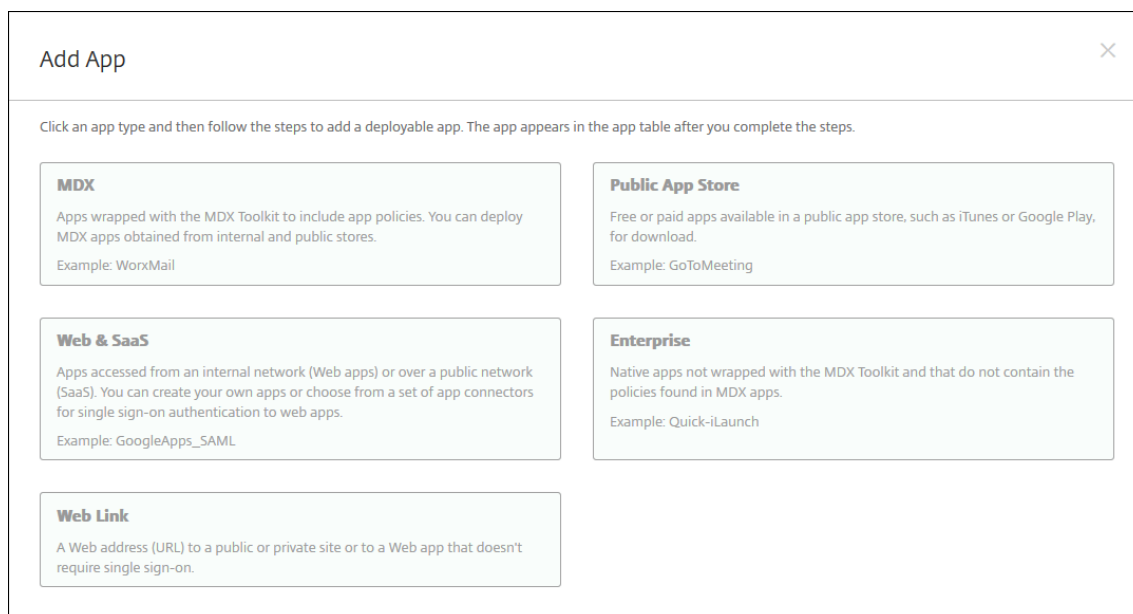
Você pode adicionar ao XenMobile aplicativos gratuitos ou pagos que estão disponíveis em uma loja de aplicativos pública, como o Apple App Store ou Google Play.

Você pode definir as configurações para obter nomes de aplicativo e descrições da Apple App Store. Quando você obtém as informações de aplicativo da loja, o XenMobile substitui o nome existente e a descrição. Configure manualmente as informações do aplicativo do Google Play Store.

Quando você adiciona um aplicativo de loja de aplicativos pública pago para Android Enterprise, pode verificar o status do licenciamento da compra em massa. Esse status é o número total de licenças disponíveis, o número em uso no momento e o endereço de email de cada usuário que consome as licenças. O plano de Compra em Massa do Android Enterprise simplifica o processo de localizar, comprar e distribuir aplicativos e outros dados em massa para uma organização.

Configure as informações do aplicativo e escolha plataformas para entregar o aplicativo a:

1. No console XenMobile, clique em **Configurar > Aplicativos > Adicionar**. A caixa de diálogo **Adicionar Aplicativo** é exibida.



2. Clique em **Loja de aplicativos pública**. A página **Informações do Aplicativo** é exibida.
3. No painel **Informações do aplicativo**, digite as seguintes informações:
 - **Nome:** digite um nome descritivo para o aplicativo. Esse nome aparecerá em **Nome do aplicativo** na tabela **Aplicativos**.
 - **Descrição:** digite uma descrição opcional para o aplicativo.
 - **Categoria do aplicativo:** opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte [Sobre categorias de aplicativos](#).
4. Clique em **Avançar**. A página **Plataformas do aplicativo** é exibida.
5. Em **Plataformas**, selecione as plataformas que você deseja adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Em seguida, defina as configurações do aplicativo para cada plataforma. Consulte:

- Configurar as definições do aplicativo para as aplicações do Google Play
- [Aplicativos da loja de aplicativos gerenciada](#)
- Definir as configurações do aplicativo para aplicativos iOS

Quando terminar de definir as configurações de uma plataforma, defina as regras de implantação da plataforma e a configuração da loja de aplicativos.

1. Configure as regras de implantação. Para obter informações, consulte [Regras de implantação](#).
2. Expanda **Configuração da loja**.

The screenshot shows the 'Store Configuration' section. Under 'App FAQ', there is a button labeled 'Add a new FAQ question and answer'. Below this, the 'App screenshots' section contains five placeholder boxes, each with a 'Choose File' button. At the bottom, there are two toggle switches: 'Allow app ratings' and 'Allow app comments', both of which are currently turned 'ON'.

- **Perguntas frequentes sobre o aplicativo:** clique em **Adicionar uma nova pergunta e resposta de Perguntas frequentes** para criar uma Pergunta frequente para o aplicativo.
- **Adicionar capturas de tela para telefones/tablets:** adicionar capturas de tela que aparecem na loja de aplicativos.
- **Permitir classificações do aplicativo:** permitir que os usuários avaliem o aplicativo na loja de aplicativos.
- **Permitir comentários do aplicativo:** permitir que os usuários deixem comentários sobre o aplicativo na loja de aplicativos.

Configurar as definições do aplicativo para as aplicações do Google Play

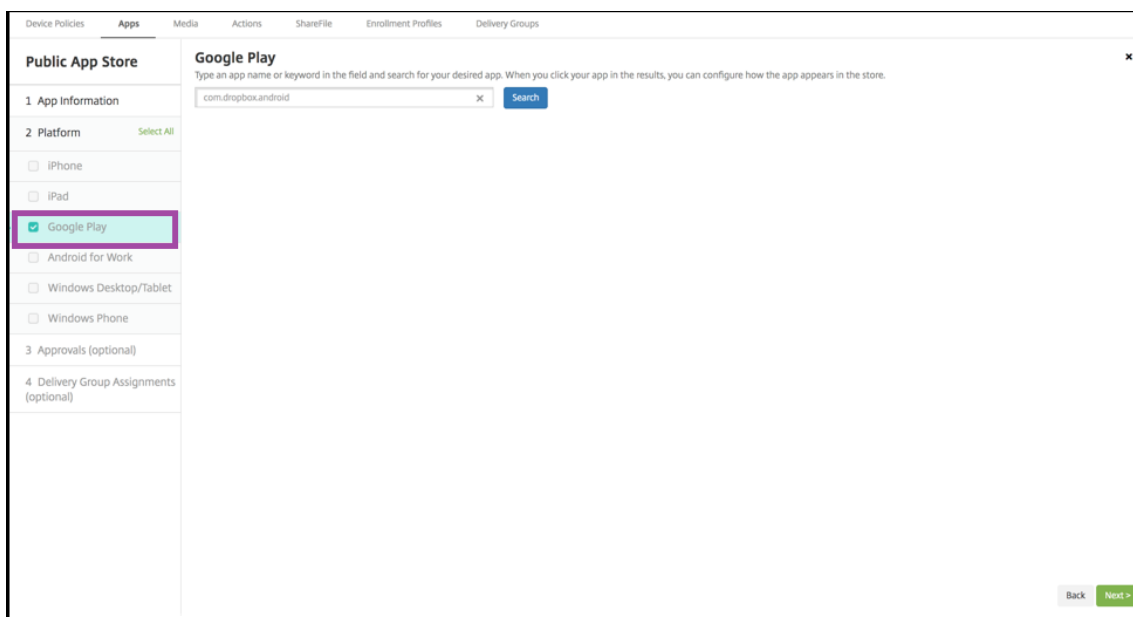
Nota:

Para tornar todos os aplicativos na loja Google Play acessíveis a partir do Google Play gerenciado, use a propriedade do servidor XenMobile, **Acessar todos os aplicativos na loja Google Play gerenciada**. Consulte [Propriedades do servidor](#). Definir esta propriedade como **true** acrescentará os aplicativos da loja pública do Google Play a uma lista de permissão para todos os

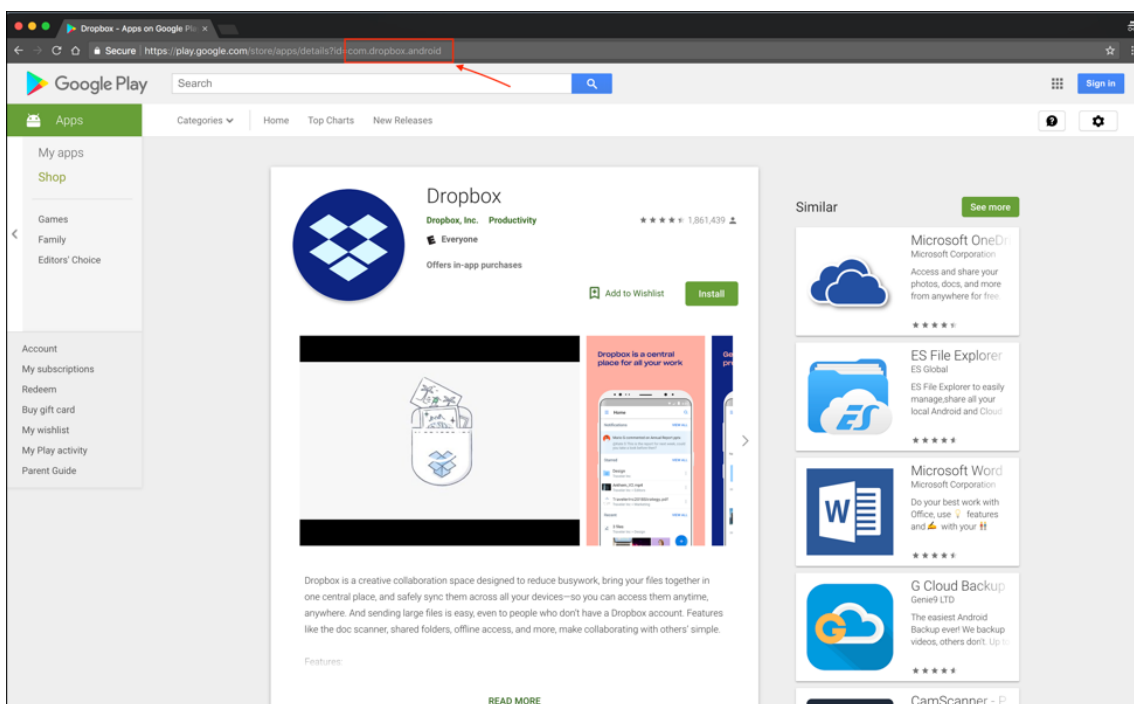
usuários do Android Enterprise. Você pode usar a [Política de dispositivo de restrições](#) para controlar o acesso a esses aplicativos.

A definição de configurações de aplicativos do Google Play Store requer etapas diferentes das de aplicativos de outras plataformas. Você deve configurar manualmente as informações do aplicativo do Google Play Store.

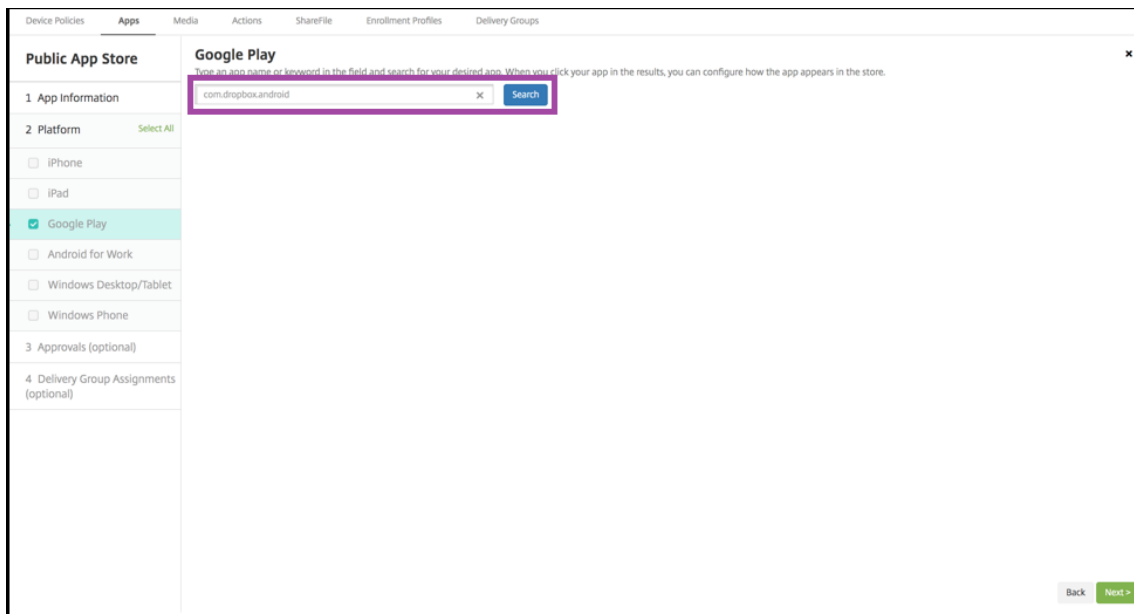
1. Verifique se **Google Play** está selecionado em **Plataformas**.



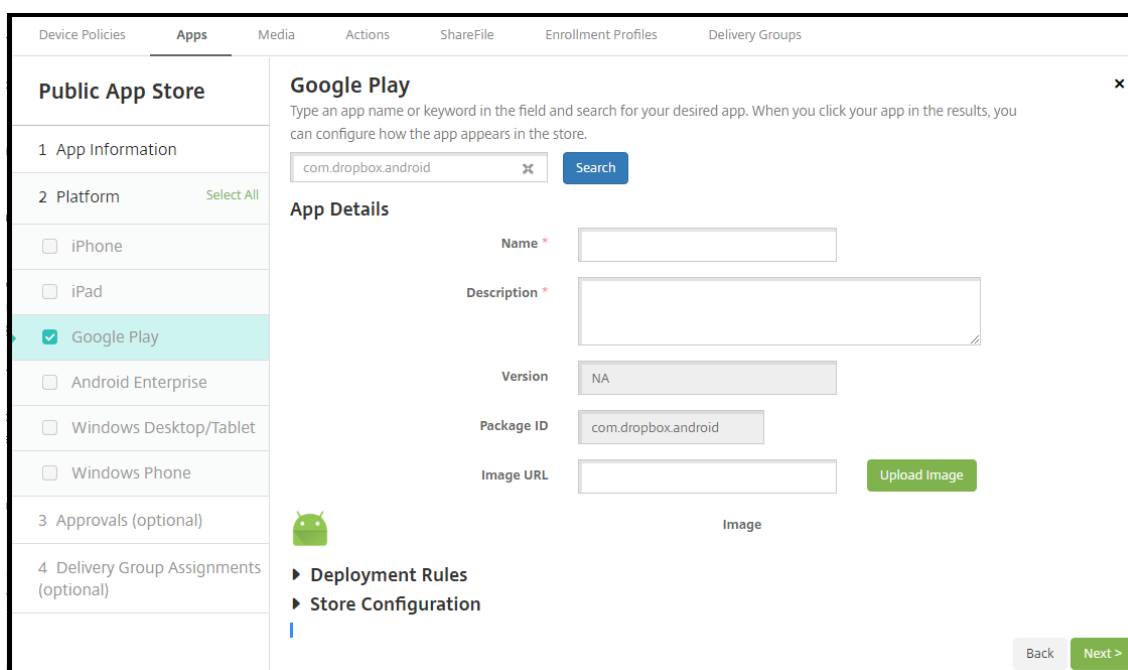
2. Vá para a loja de aplicativos do Google Play. No Google Play Store, copie o ID do pacote. O ID pode ser encontrado na URL do aplicativo.



3. Ao adicionar um aplicativo da Loja de Aplicativos Pública ao console XenMobile Server, cole o ID do pacote na barra de pesquisa. Clique em **Pesquisar**.



4. Se o ID do pacote for válido, uma interface do usuário será exibida, permitindo que você insira detalhes do aplicativo.



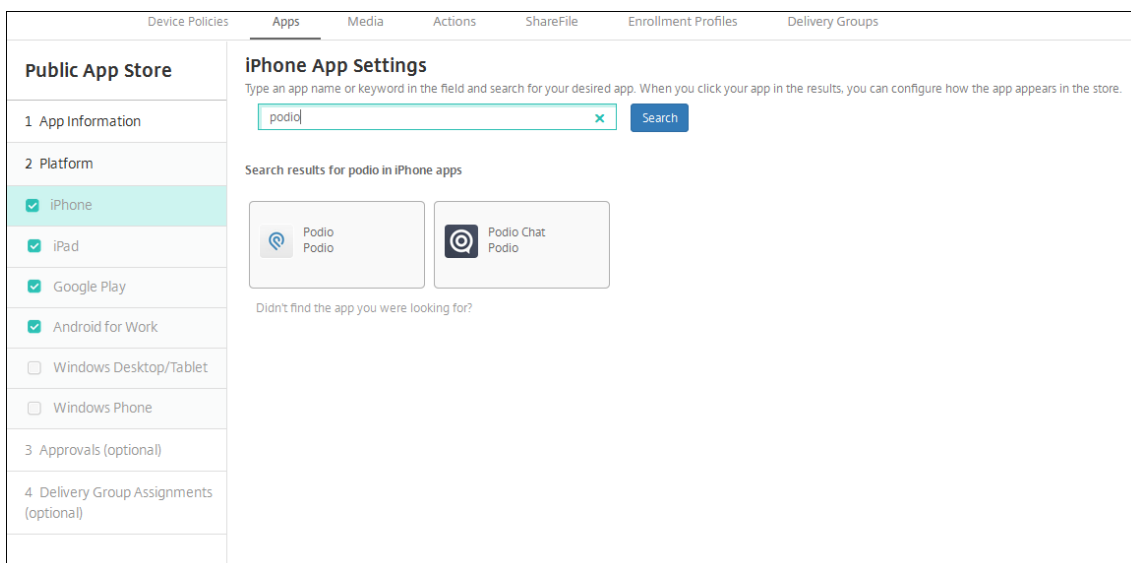
5. Você pode configurar a URL para que a imagem apareça com o aplicativo na loja. Para usar a imagem do Google Play Store:
 - a) Vá para a loja de aplicativos do Google Play. Clique com o botão direito do mouse na imagem do aplicativo e copie o endereço da imagem.
 - b) Cole o endereço da imagem no campo **URL da imagem**.
 - c) Clique em **Carregar imagem**. A imagem aparece ao lado de **Imagem**.

Se você não configurar uma imagem, a imagem genérica do Android aparecerá com o aplicativo.

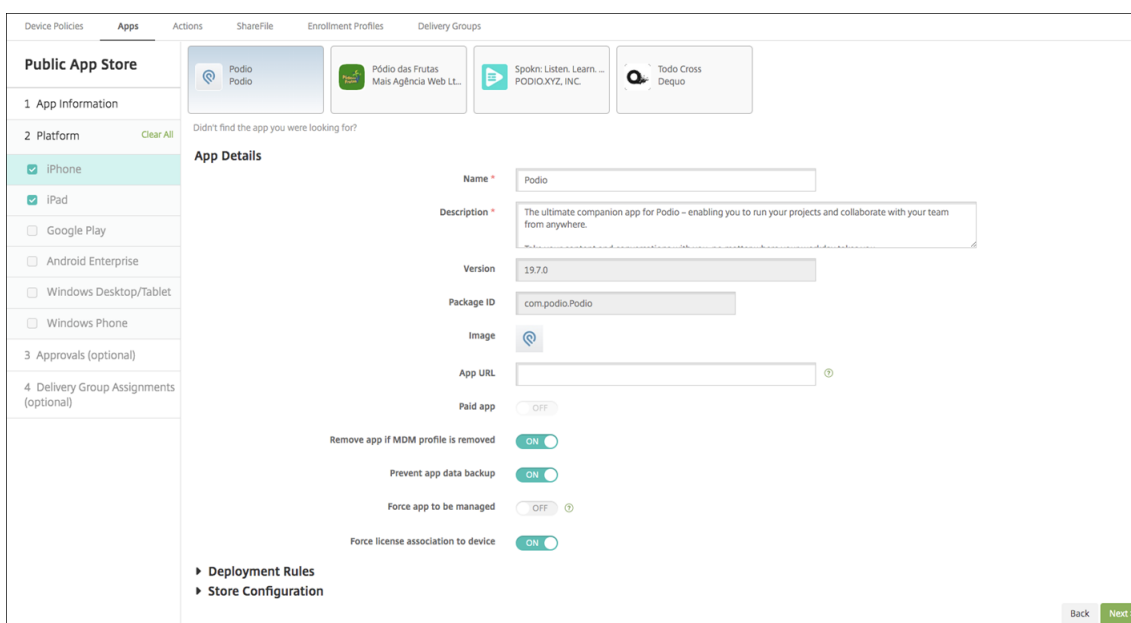
Definir as configurações do aplicativo para aplicativos iOS

1. Digite o nome do aplicativo na caixa de pesquisa e clique em **Pesquisar**. Os aplicativos que correspondem aos critérios de pesquisa são exibidos. Os aplicativos que correspondem aos critérios de pesquisa são exibidos.

A figura a seguir mostra o resultado da pesquisa por **podio** nos aplicativos em um iPhone.



2. Clique no aplicativo que você deseja adicionar.
3. Os campos de **Detalhes do aplicativo** são pré-preenchidos com informações relacionadas ao aplicativo escolhido (incluindo nome, descrição, número da versão e imagem associada).



4. Defina as configurações:
 - Se necessário, altere o nome e a descrição do aplicativo.
 - **Aplicativo pago:** esse campo é configurado previamente e não pode ser alterado.
 - **Remover aplicativo se o perfil MDM for removido:** selecione se o aplicativo deverá ser removido quando o perfil MDM for removido. O padrão é **I**.
 - **Evitar o backup de dados do aplicativo:** selecione se o aplicativo deve ser impedido de realizar o backup de dados. O padrão é **I**.

- **Rastreamento de produtos:** especifique qual rastreamento de produto você deseja enviar para os dispositivos do usuário. Se você tiver um rastreamento projetado para testes, poderá selecioná-lo e atribuí-lo aos seus usuários. O padrão é **Produção**.
 - **Forçar aplicativo a ser gerenciado:** selecione se, quando o aplicativo está instalado e não é gerenciado, os usuários devem ser solicitados a permitir que o aplicativo seja gerenciado em dispositivos não supervisionados. O padrão é **O**. Disponível no iOS 9.0 e versões posteriores.
 - **Forçar associação de licença ao dispositivo:** selecione se um aplicativo que foi desenvolvido com a associação de dispositivo ativada deve ser associado a um dispositivo em vez de a um usuário. Disponível no iOS 9 e versões posteriores. Se o aplicativo que você escolheu não for compatível com a atribuição a um dispositivo, esse campo não poderá ser alterado.
5. Configure as regras de implantação. Para obter informações, consulte [Regras de implantação](#).
 6. Expanda **Configuração da loja**.

▼ Store Configuration

App FAQ

Add a new FAQ question and answer

App screenshots

Choose File

Choose File

Choose File

Choose File

Choose File

Allow app ratings

Allow app comments

- **Perguntas frequentes sobre o aplicativo:** clique em **Adicionar uma nova pergunta e resposta de Perguntas frequentes** para criar uma Pergunta frequente para o aplicativo.

- **Adicionar capturas de tela para telefones/tablets:** adicionar capturas de tela que aparecem na loja de aplicativos.
- **Permitir classificações do aplicativo:** permitir que os usuários avaliem o aplicativo na loja de aplicativos.
- **Permitir comentários do aplicativo:** permitir que os usuários deixem comentários sobre o aplicativo na loja de aplicativos.

7. Para iPhone ou iPad, expanda **Compra por volume**.

a) Para ativar o XenMobile para aplicar uma licença de compra por volume ao aplicativo, na lista **Licença de compra por volume**, clique em **Carregar uma licença de compra por volume**.

b) Na caixa de diálogo que é exibida, importe a licença.

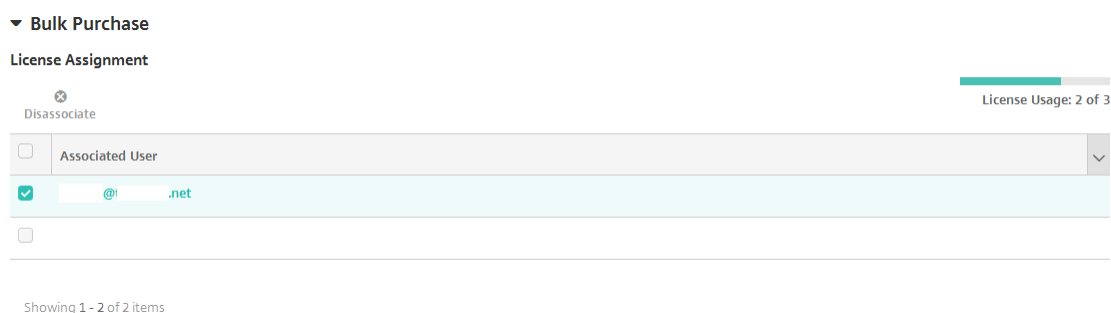
A tabela de Atribuição de licenças mostra o número de licenças em uso para o aplicativo, do total de licenças disponíveis.

Você pode desassociar as licenças de compra por volume para um usuário individual. Isso encerra as atribuições de licença e libera licenças.

8. No Android Enterprise, expanda a seção **Compra em massa**.

A tabela de Atribuição de licenças mostra o número de licenças em uso para o aplicativo, do total de licenças disponíveis.

Você pode selecionar um usuário e clicar em **Desassociar** para encerrar a respectiva atribuição de licença e liberar uma licença para outro usuário. No entanto, você poderá desassociar a licença somente se o usuário não fizer parte de um grupo de entrega que contém o aplicativo específico.



9. Depois que você concluir as configurações de **Compra por volume** ou **Compra em massa**, clique em **Avançar**. A página **Aprovações** é exibida.

Para usar fluxos de trabalho para exigir aprovação antes de permitir que os usuários acessem o aplicativo, consulte Aplicar fluxos de trabalho. Se você não precisar de fluxos de trabalho de aprovação, continue com a próxima etapa.

10. Clique em **Avançar**. A página **Atribuição de grupo de entrega** é exibida.

11. Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega ou selecione um ou mais grupos. Os grupos que você selecionar aparecerão na lista **Grupos de entrega que receberão a atribuição de aplicativos**.

12. Expanda **Cronograma de implantação** e defina estas configurações:

- **Implantar:** escolha se deseja implantar o aplicativo em dispositivos. O padrão é **On**.
- **Cronograma de implantação:** escolha se deseja implantar o aplicativo **Agora** ou **Mais tarde**. Se você selecionar **Mais tarde**, configure uma data e hora para implantar o aplicativo. O padrão é **Agora**.
- **Condição de implantação:** escolha **Em cada conexão** para implantar o aplicativo sempre que o dispositivo se conectar. Escolha **Somente quando a implantação anterior tiver falhado** para implantar o aplicativo quando o dispositivo não conseguir receber o aplicativo anteriormente. O padrão é **Em cada conexão**.

Implantar para conexões permanentes é aplicável quando você tiver configurado a chave de implantação em segundo plano do cronograma em **Configurações > Propriedades do servidor**.

O cronograma de implantação que você configura é o mesmo para todas as plataformas. Todas as alterações feitas se aplicam a todas as plataformas, exceto **Implantar para conexões permanentes**.

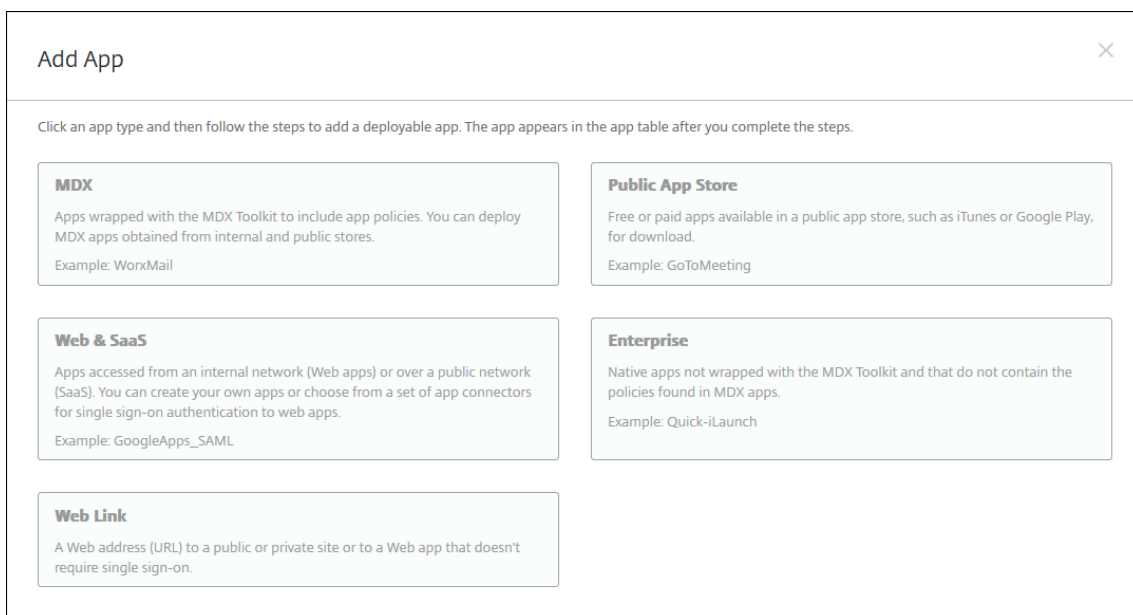
13. Clique em **Salvar**.

Acrescentar um aplicativo Web ou SaaS

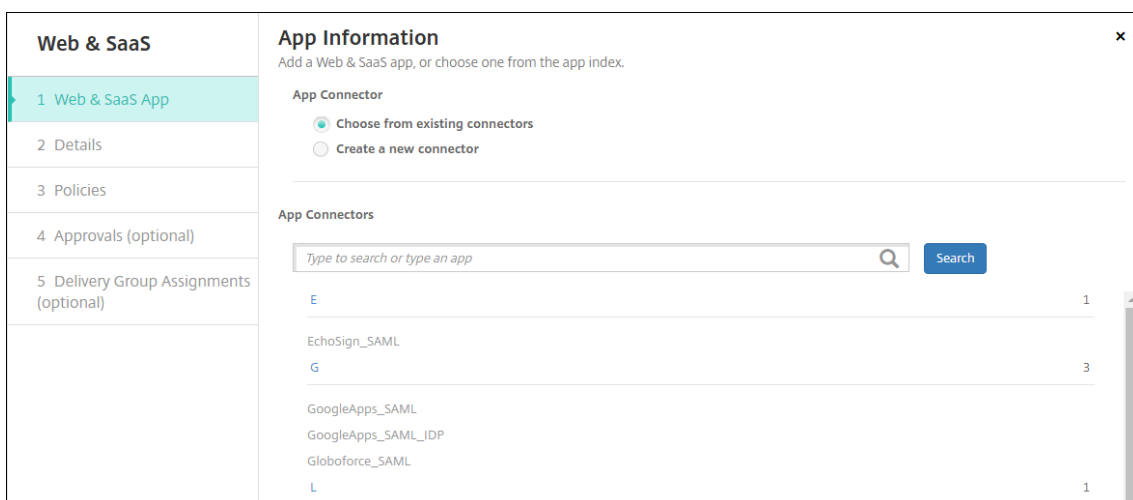
Usando o console XenMobile, você pode oferecer aos usuários a autorização de logon único (SSO) aos seus aplicativos móveis, empresariais, Web e SaaS. Você pode ativar aplicativos para SSO usando modelos de conector de aplicativo. Para obter uma lista dos tipos de conectores disponíveis no XenMobile, consulte [Tipos de conector de aplicativo](#). Você também pode criar seu próprio conector no XenMobile ao adicionar um aplicativo Web ou SaaS.

Se um aplicativo estiver disponível somente para SSO, depois que você salvar as configurações, o aplicativo será exibido na guia **Aplicativos** do console XenMobile.

1. No console XenMobile, clique em **Configurar > Aplicativos > Adicionar**. A caixa de diálogo **Adicionar Aplicativo** é exibida.



2. Clique em **Web e SaaS**. A página **Informações do Aplicativo** é exibida.



3. Configure um aplicativo existente ou novo conector, da seguinte maneira.

Para configurar um conector de aplicativo existente

1. Na página **Informações do aplicativo**, **Escolher dos conectores existentes** já está selecionado, como mostrado anteriormente. Clique no conector que você deseja usar na lista **Conectores de aplicativos**. As informações de conector de aplicativo são exibidas.
2. Defina estas configurações:
 - **Nome do aplicativo:** aceite o nome preenchido previamente ou digite um novo nome.
 - **Descrição do aplicativo:** aceite a descrição preenchida previamente ou digite uma.

- **URL:** aceite a URL preenchida previamente ou digite o endereço Web do aplicativo. Dependendo do conector que você escolher, esse campo poderá conter um espaço reservado que você deve substituir antes que possa continuar para a página seguinte.
- **Nome de domínio:** se aplicável, digite o nome de domínio do aplicativo. Esse campo é obrigatório.
- **O aplicativo está hospedado na rede interna:** selecione se o aplicativo está em execução em um servidor na sua rede interna. Se os usuários se conectarem de uma localidade remota a um aplicativo interno, eles deverão se conectar por meio do Citrix Gateway. Definir essa opção como **I** adiciona a palavra-chave VPN ao aplicativo e permite que os usuários se conectem por meio do Citrix Gateway. O padrão é **O**.
- **Categoria do aplicativo:** na lista, clique em uma categoria opcional a ser aplicada ao aplicativo.
- **Provisionamento de conta de usuário:** selecione se contas de usuário devem ser criadas para o aplicativo. Se você usar o conector Globoforce_SAML, deverá ativar essa opção para garantir a integração perfeita do SSO.
- Se você ativar o **Provisionamento de conta de usuário**, defina estas configurações:
 - **Conta de serviço**
 - * **Nome de usuário:** digite o nome do administrador do aplicativo. Este campo é obrigatório.
 - * **Senha:** digite a senha de administrador do aplicativo. Este campo é obrigatório.
 - **Conta de usuário**
 - * **Quando termina o direito do usuário:** na lista, clique na ação a ser tomada quando os usuários não tiverem mais acesso ao aplicativo. O padrão é **Desativar conta**.
 - **Regra de nome de usuário**
 - * Para cada regra de nome do usuário que você deseja adicionar, faça o seguinte:
 - **Atributos do usuário:** na lista, clique no atributo de usuário a ser adicionado à regra.
 - **Comprimento (caracteres):** na lista, clique no número de caracteres do atributo de usuário a ser usado na regra de nome do usuário. O padrão é **Tudo**.
 - **Regra:** cada atributo de usuário que você adiciona é automaticamente acrescentado à regra de nome do usuário.
- **Requisito de senha**
 - **Comprimento:** digite o comprimento mínimo da senha do usuário. O padrão é **8**.
- **Vencimento de senha**
 - **Validade (dias):** digite o número de dias durante os quais a senha é válida. Os valores válidos são **0 a 90**. O padrão é 90.
 - **Redefinir a senha automaticamente depois de expirar:** selecione se a senha deve ser redefinida automaticamente quando ela expira. O padrão é **O**. Se você não ativar

esse campo, os usuários não poderão abrir o aplicativo após a expiração das senhas.

Para configurar um novo conector de aplicativo

1. Na página **Informações do aplicativo**, selecione **Criar um novo conector**. Os campos de conector de aplicativo são exibidos.

2. Defina estas configurações:

- **Nome:** digite um nome para o conector. Este campo é obrigatório.
- **Descrição:** digite uma descrição para o conector. Este campo é obrigatório.
- **URL de login:** digite ou copie e cole a URL a qual os usuários usam para fazer login no site. Por exemplo, se o aplicativo que você deseja adicionar tiver uma página de logon, abra um navegador da Web e vá para a página de login do aplicativo. Por exemplo, a página pode ser <https://www.example.com/logon>. Este campo é obrigatório.
- **Versão do SAML:** selecione **1.1** ou **2.0**. O padrão é **1.1**.
- **ID da entidade:** digite a identidade do aplicativo SAML.
- **URL do estado do relé:** digite o endereço da Web do aplicativo de SAML. A URL do estado do relé é a URL de resposta do aplicativo.
- **Formato de ID do nome:** selecione **Endereço de email** ou **Não especificado**. O padrão é **Endereço de e-mail**.
- **URL de ACS:** digite a URL do Serviço do Consumidor de Asserção do provedor de identidade ou do provedor de serviços. A URL de ACS oferece aos usuários a capacidade de SSO.

- **Imagem:** selecione se a imagem padrão da Citrix deve ser usada ou se a sua própria imagem do aplicativo deve ser carregada. O padrão é Usar padrão.
 - Para carregar sua própria imagem, clique em **Procurar** e navegue até o local do arquivo. O arquivo deve ser um arquivo .PNG. Não é possível carregar um arquivo JPEG ou GIF. Quando você adicionar um gráfico personalizado, não poderá alterá-lo depois.
3. Quando terminar, clique em **Adicionar**. A página **Detalhes** é exibida.
 4. Clique em **Avançar**. A página **Política de aplicativo** é exibida.

Web & SaaS

App Policy
Fill in app information

1 Web & SaaS App

2 Details

3 Policies

4 Approvals (optional)

5 Delivery Group Assignments (optional)

Device Security

Block jailbroken or rooted **ON**

Network Requirements

WiFi required **OFF**

Internal network required **OFF**

Internal WiFi networks

► Store Configuration

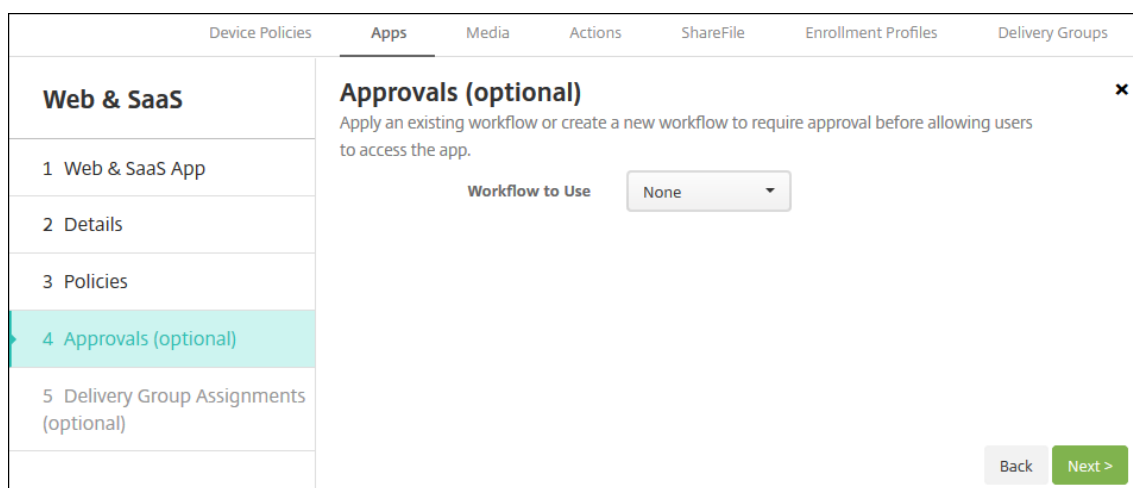
Back Next >

5. Defina estas configurações:
 - **Segurança do dispositivo**
 - **Bloquear com jailbreak ou com root:** selecione se os dispositivos com jailbreak ou root têm o acesso ao aplicativo bloqueado. O padrão é **I**.
 - **Requisitos de rede**
 - **Requer WiFi:** selecione se uma conexão Wi-Fi é necessária para executar o aplicativo. O padrão é **O**.
 - **Requer rede interna:** selecione se uma rede interna é necessária para executar o aplicativo. O padrão é **O**.
 - **Redes de WiFi internas:** se você tiver ativado a opção **Requer WiFi**, digite as redes Wi-Fi internas a serem usadas.
6. Configure as regras de implantação. Para obter informações, consulte [Regras de implantação](#).
7. Expanda **Configuração da loja**.

The screenshot shows the 'Store Configuration' section. Under 'App FAQ', there is a button labeled 'Add a new FAQ question and answer'. Below this, the 'App screenshots' section contains five placeholder boxes, each with a 'Choose File' button. At the bottom, there are two toggle switches: 'Allow app ratings' and 'Allow app comments', both of which are currently turned 'ON'.

- **Perguntas frequentes sobre o aplicativo:** clique em **Adicionar uma nova pergunta e resposta de Perguntas frequentes** para criar uma Pergunta frequente para o aplicativo.
- **Adicionar capturas de tela para telefones/tablets:** adicionar capturas de tela que aparecem na loja de aplicativos.
- **Permitir classificações do aplicativo:** permitir que os usuários avaliem o aplicativo na loja de aplicativos.
- **Permitir comentários do aplicativo:** permitir que os usuários deixem comentários sobre o aplicativo na loja de aplicativos.

8. Clique em **Avançar**. A página **Aprovações** é exibida.



Para usar fluxos de trabalho para exigir aprovação antes de permitir que os usuários acessem o aplicativo, consulte Aplicar fluxos de trabalho.

9. Clique em **Avançar**. A página **Atribuição de grupo de entrega** é exibida.
10. Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega ou selecionar um ou mais grupos. Os grupos que você selecionar aparecerão na lista **Grupos de entrega que receberão a atribuição de aplicativos**.
11. Expanda **Cronograma de implantação** e defina estas configurações:
 - **Implantar**: escolha se deseja implantar o aplicativo em dispositivos. O padrão é **On**.
 - **Cronograma de implantação**: escolha se deseja implantar o aplicativo **Agora** ou **Mais tarde**. Se você selecionar **Mais tarde**, configure uma data e hora para implantar o aplicativo. O padrão é **Agora**.
 - **Condição de implantação**: escolha **Em cada conexão** para implantar o aplicativo sempre que o dispositivo se conectar. Escolha **Somente quando a implantação anterior tiver falhado** para implantar o aplicativo quando o dispositivo não conseguir receber o aplicativo anteriormente. O padrão é **Em cada conexão**.

Implantar para conexões permanentes é aplicável quando você tiver configurado a chave de implantação em segundo plano do cronograma em **Configurações > Propriedades do servidor**.

O cronograma de implantação que você configura é o mesmo para todas as plataformas. Todas as alterações feitas se aplicam a todas as plataformas, exceto **Implantar para conexões permanentes**.

12. Clique em **Salvar**.

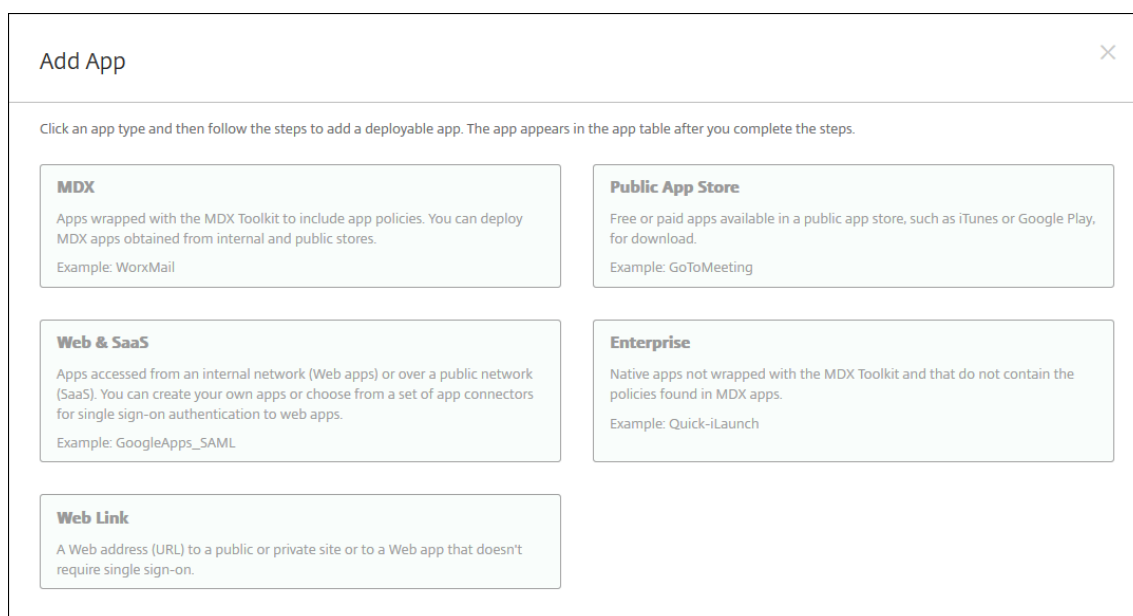
Acrescentar um aplicativo empresarial

Os aplicativos empresariais no XenMobile representam aplicativos nativos que não são preparados com o MAM SDK ou MDX Toolkit. Esses aplicativos não contêm as políticas associadas aos aplicativos MDX. Você pode carregar um aplicativo empresarial na guia **Aplicativos** no console XenMobile. Os aplicativos empresariais são compatíveis com as seguintes plataformas (e tipos de arquivo correspondentes):

- iOS (arquivo .ipa)
- Android (arquivo .apk)
- Samsung Knox (arquivo .apk)
- Android Enterprise (arquivo .apk)
- Consulte também: [Aplicativos privados habilitados para MDX](#)

A adição de aplicativos baixados do Google Play Store como aplicativos empresariais não é suportada. Portanto, adicione aplicativos do Google Play Store como aplicativos da loja de aplicativos pública. Consulte Acrescentar um aplicativo de loja de aplicativos pública.

1. No console XenMobile, clique em **Configurar > Aplicativos > Adicionar**. A caixa de diálogo **Adicionar Aplicativo** é exibida.



2. Clique em **Empresarial**. A página **Informações do Aplicativo** é exibida.
3. No painel **Informações do aplicativo**, digite as seguintes informações:
 - **Nome**: digite um nome descritivo para o aplicativo. Esse nome fica listado em Nome do aplicativo, na tabela Aplicativos.
 - **Descrição**: digite uma descrição opcional para o aplicativo.
 - **Categoria do aplicativo**: opcionalmente, na lista, clique na categoria à qual você deseja

adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte [Sobre categorias de aplicativos](#).

4. Clique em **Avançar**. A página **Plataformas do aplicativo** é exibida.
5. Em **Plataformas**, selecione as plataformas que você deseja adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.
6. Para cada plataforma que você selecionou, selecione o arquivo a ser carregado clicando em **Carregar** e navegando até a localização do arquivo.
7. Clique em **Avançar**. A página de informações do aplicativo da plataforma é exibida.
8. Defina as configurações do tipo de plataforma, como:
 - **Nome do arquivo:** opcionalmente, digite um novo nome para o aplicativo.
 - **Descrição do aplicativo:** opcionalmente, digite uma nova descrição para o aplicativo.
 - **Versão do aplicativo:** você não pode alterar esse campo.
 - **Versão do SO mínima:** opcionalmente, digite a versão mais antiga do sistema operacional que o dispositivo pode executar para usar o aplicativo.
 - **Versão do SO máxima:** opcionalmente, digite a versão mais recente do sistema operacional que o dispositivo deve executar para usar o aplicativo.
 - **Dispositivos excluídos:** opcionalmente, digite o fabricante ou os modelos de dispositivos que não podem executar o aplicativo.
 - **ID de pacote:** Identificador exclusivo do seu aplicativo.
 - **Remover aplicativo se o perfil MDM for removido:** selecione se o aplicativo deve ser removido de um dispositivo quando o perfil MDM é removido. O padrão é **On**.
 - **Evitar o backup de dados do aplicativo:** selecione se o aplicativo deve ser impedido de realizar o backup de dados. O padrão é **On**.
 - **Forçar aplicativo a ser gerenciado:** se você estiver instalando um aplicativo não gerenciado, selecione **I** se quiser que os usuários em dispositivos não supervisionados sejam solicitados a permitir o gerenciamento do aplicativo. Se aceitarem a solicitação, o aplicativo será gerenciado.
9. Configure as regras de implantação. Para obter informações, consulte [Regras de implantação](#).
10. Expanda **Configuração da loja**.

The screenshot shows the 'Store Configuration' section. Under 'App FAQ', there is a button labeled 'Add a new FAQ question and answer'. Below this, the 'App screenshots' section contains five placeholder boxes, each with a 'Choose File' button. At the bottom, there are two toggle switches: 'Allow app ratings' and 'Allow app comments', both of which are currently turned 'ON'.

- **Perguntas frequentes sobre o aplicativo:** clique em **Adicionar uma nova pergunta e resposta de Perguntas frequentes** para criar uma Pergunta frequente para o aplicativo.
- **Adicionar capturas de tela para telefones/tablets:** adicionar capturas de tela que aparecem na loja de aplicativos.
- **Permitir classificações do aplicativo:** permitir que os usuários avaliem o aplicativo na loja de aplicativos.
- **Permitir comentários do aplicativo:** permitir que os usuários deixem comentários sobre o aplicativo na loja de aplicativos.

11. Clique em **Avançar**. A página **Aprovações** é exibida.

Para usar fluxos de trabalho para exigir aprovação antes de permitir que os usuários acessem o aplicativo, consulte Aplicar fluxos de trabalho. Se você não precisar de um fluxo de trabalho de aprovação, continue com a próxima etapa.

12. Clique em **Avançar**. A página **Atribuição de grupo de entrega** é exibida.

13. Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega ou selecione um ou mais grupos. Os grupos que você selecionar aparecerão na lista **Grupos de entrega que receberão a atribuição de aplicativos**.

14. Expanda **Cronograma de implantação** e defina estas configurações:

- **Implantar:** escolha se deseja implantar o aplicativo em dispositivos. O padrão é **On**.
- **Cronograma de implantação:** escolha se deseja implantar o aplicativo **Agora** ou **Mais tarde**. Se você selecionar **Mais tarde**, configure uma data e hora para implantar o aplicativo. O padrão é **Agora**.
- **Condição de implantação:** escolha **Em cada conexão** para implantar o aplicativo sempre que o dispositivo se conectar. Escolha **Somente quando a implantação anterior tiver falhado** para implantar o aplicativo quando o dispositivo não conseguir receber o aplicativo anteriormente. O padrão é **Em cada conexão**.

Implantar para conexões permanentes é aplicável quando você tiver configurado a chave de implantação em segundo plano do cronograma em **Configurações > Propriedades do servidor**.

O cronograma de implantação que você configura é o mesmo para todas as plataformas. Todas as alterações feitas se aplicam a todas as plataformas, exceto **Implantar para conexões permanentes**.

15. Clique em **Salvar**.

Adicionar um link da Web

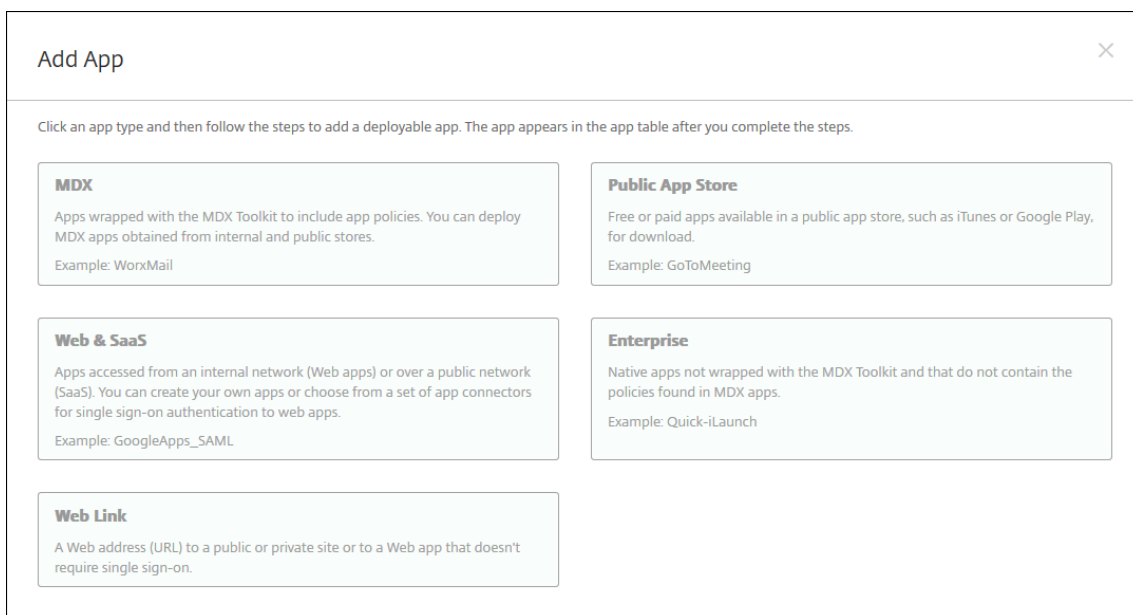
Um link da Web é um endereço Web para um site da Internet ou intranet. Um link da Web também pode apontar para um aplicativo Web que não requer SSO. Depois que você termina de configurar um link da Web, o link é exibido como um ícone na loja de aplicativos. Quando os usuários fazem login no Secure Hub, o link é exibido com a lista de aplicativos e áreas de trabalho disponíveis.

Você pode configurar os links da Web na guia **Aplicativos** do console XenMobile. Quando você termina de configurar um link da Web, o link é exibido como um ícone de link na lista da tabela **Aplicativos**. Quando os usuários fazem login no Secure Hub, o link é exibido com a lista de aplicativos e áreas de trabalho disponíveis.

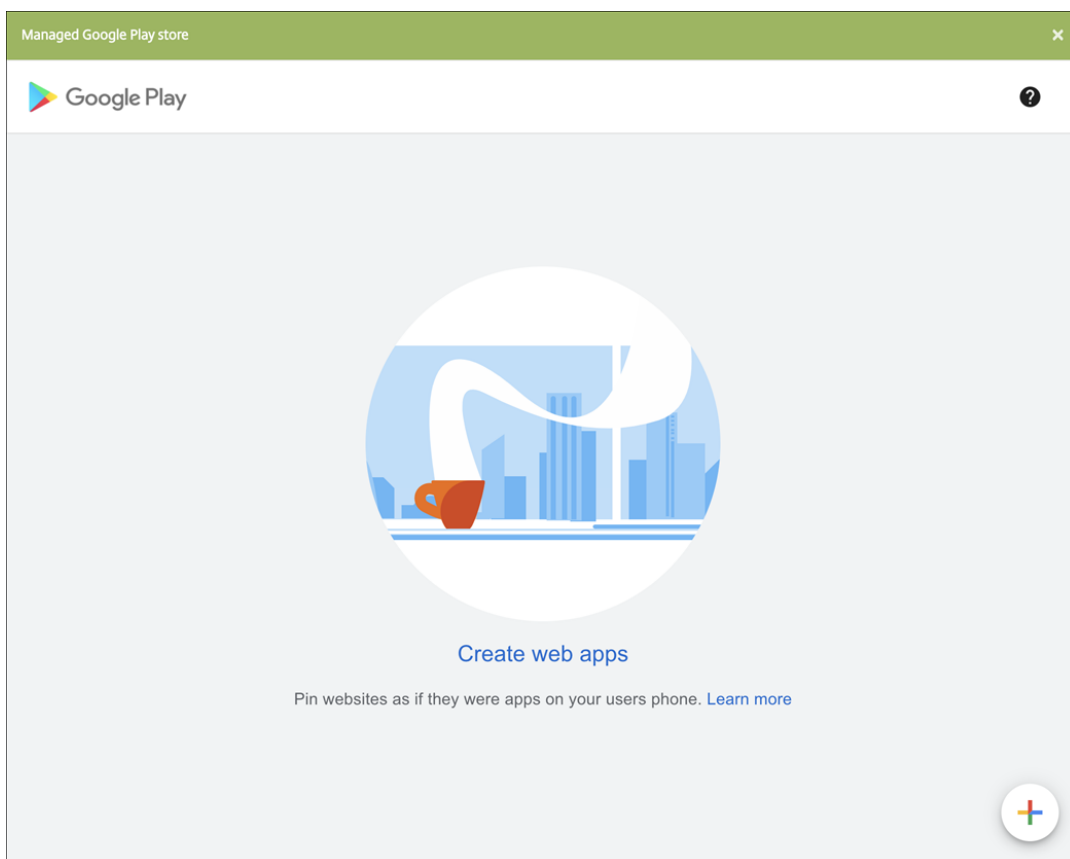
Para adicionar o link, forneça as seguintes informações:

- Nome do link
- Descrição do link
- Endereço da Web (URL)
- Categoria
- Função
- Imagem no formato .png (opcional)

1. No console XenMobile, clique em **Configurar > Aplicativos > Adicionar**. A caixa de diálogo **Adicionar Aplicativo** é exibida.

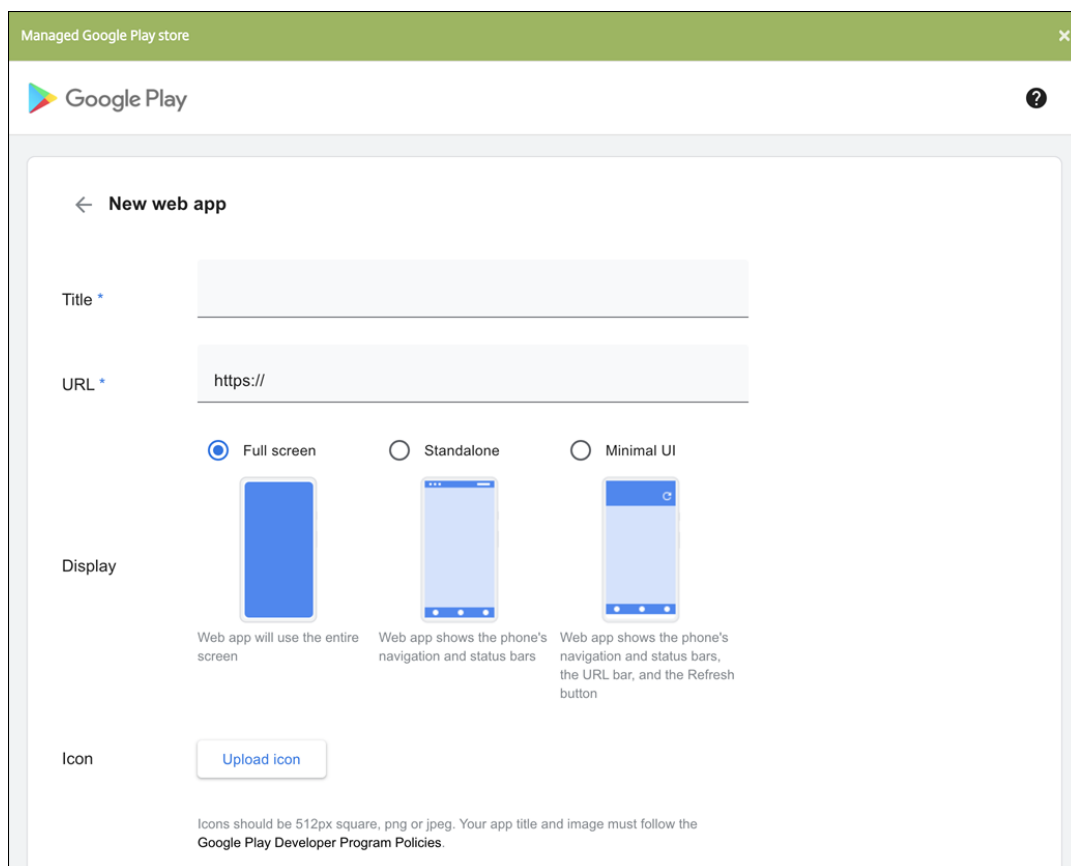


2. Clique em **Link da Web**. A página **Informações do Aplicativo** é exibida.
3. No painel **Informações do aplicativo**, digite as seguintes informações:
 - Nome:** digite um nome descritivo para o aplicativo. Esse nome fica listado em Nome do aplicativo, na tabela Aplicativos.
 - Descrição:** digite uma descrição opcional para o aplicativo.
 - Categoria do aplicativo:** opcionalmente, na lista, clique na categoria à qual você deseja adicionar o aplicativo. Para obter mais informações sobre categorias de aplicativos, consulte Sobre categorias de aplicativos.
4. Clique em **Avançar**. A página **Plataformas do aplicativo** é exibida.
5. Em **Plataformas**, selecione **Outras plataformas**, para adicionar um aplicativo Web para iOS e Android (DA legado), ou selecione **Android Enterprise**. Desmarque a caixa de seleção daqueles que não deseja adicionar.
 - Se você selecionar **Outras plataformas**, continue com a próxima etapa para definir as configurações.
 - Se você selecionar **Android Enterprise**, clique no botão **Carregar** para abrir a loja gerenciada do Google Play. Você não precisa se registrar em uma conta de desenvolvedor para publicar um aplicativo Web. Clique no ícone de **adição** no canto inferior direito para continuar.



Defina estas configurações:

- **Título:** digite o nome do aplicativo Web.
- **URL:** digite o endereço da Web aplicativo.
- **Exibir:** escolha como exibir o aplicativo Web nos dispositivos do usuário. As opções disponíveis são **Tela cheia**, **Autônomo** e **Interface mínima**.
- **Ícone:** carregue sua própria imagem para representar o aplicativo Web.



Quando terminar, clique em **Criar**. Pode levar até 10 minutos para que seu aplicativo Web seja publicado.

6. Para plataformas diferentes do Android Enterprise, defina estas configurações:

- **Nome do aplicativo:** aceite o nome preenchido previamente ou digite um novo nome.
- **Descrição do aplicativo:** aceite a descrição preenchida previamente ou digite uma.
- **URL:** aceite a URL preenchida previamente ou digite o endereço Web do aplicativo. Dependendo do conector que você escolher, esse campo poderá conter um espaço reservado que você deve substituir antes que possa continuar para a página seguinte.
- **O aplicativo está hospedado na rede interna:** selecione se o aplicativo está em execução em um servidor na sua rede interna. Se os usuários se conectarem de uma localidade remota a um aplicativo interno, eles deverão se conectar por meio do Citrix Gateway. Definir essa opção como **I** adiciona a palavra-chave VPN ao aplicativo e permite que os usuários se conectem por meio do Citrix Gateway. O padrão é **O**.
- **Categoria do aplicativo:** na lista, clique em uma categoria opcional a ser aplicada ao aplicativo.
- **Imagem:** selecione se a imagem padrão da Citrix deve ser usada ou se a sua própria imagem do aplicativo deve ser carregada. O padrão é Usar padrão.
 - Para carregar sua própria imagem, clique em **Procurar** e navegue até o local do ar-

quivo. O arquivo deve ser um arquivo .PNG. Não é possível carregar um arquivo JPEG ou GIF. Quando você adicionar um gráfico personalizado, não poderá alterá-lo depois.

- Configure as regras de implantação. Para obter informações, consulte [Regras de implantação](#).
- Expanda **Configuração da loja**.

The screenshot displays the 'Store Configuration' interface. At the top, there is a section for 'App FAQ' with a button labeled 'Add a new FAQ question and answer'. Below this is the 'App screenshots' section, which contains five placeholder boxes, each with a 'Choose File' button. At the bottom of the configuration area, there are two toggle switches: 'Allow app ratings' and 'Allow app comments', both of which are currently turned 'ON'.

- **Perguntas frequentes sobre o aplicativo:** clique em **Adicionar uma nova pergunta e resposta de Perguntas frequentes** para criar uma Pergunta frequente para o aplicativo.
 - **Adicionar capturas de tela para telefones/tablets:** adicionar capturas de tela que aparecem na loja de aplicativos.
 - **Permitir classificações do aplicativo:** permitir que os usuários avaliem o aplicativo na loja de aplicativos.
 - **Permitir comentários do aplicativo:** permitir que os usuários deixem comentários sobre o aplicativo na loja de aplicativos.
- Clique em **Avançar**. A página **Atribuição de grupo de entrega** é exibida.
 - Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega ou selecione um ou mais grupos. Os grupos que você selecionar aparecerão na lista **Grupos de entrega que receberão a atribuição de aplicativos**.

11. Expanda **Cronograma de implantação** e defina estas configurações:

- **Implantar:** escolha se deseja implantar o aplicativo em dispositivos. O padrão é **On**.
- **Cronograma de implantação:** escolha se deseja implantar o aplicativo **Agora** ou **Mais tarde**. Se você selecionar **Mais tarde**, configure uma data e hora para implantar o aplicativo. O padrão é **Agora**.
- **Condição de implantação:** escolha **Em cada conexão** para implantar o aplicativo sempre que o dispositivo se conectar. Escolha **Somente quando a implantação anterior tiver falhado** para implantar o aplicativo quando o dispositivo não conseguir receber o aplicativo anteriormente. O padrão é **Em cada conexão**.

Implantar para conexões permanentes é aplicável quando você tiver configurado a chave de implantação em segundo plano do cronograma em **Configurações > Propriedades do servidor**.

O cronograma de implantação que você configura é o mesmo para todas as plataformas. Todas as alterações feitas se aplicam a todas as plataformas, exceto **Implantar para conexões permanentes**.

12. Clique em **Salvar**.

Ativar aplicativos do Microsoft Office 365

Você pode abrir o contêiner do MDX para permitir que o Secure Mail, Secure Web e Citrix Files transfiram documentos e dados para aplicativos do Microsoft Office 365. Para obter detalhes, consulte [Permitindo Interação Segura com Aplicativos do Office 365](#).

Aplicar fluxos de trabalho

Configure estas definições para atribuir ou criar um fluxo de trabalho:

- **Fluxo de trabalho a ser usado:** na lista, clique em um fluxo de trabalho existente ou clique em **Criar um novo fluxo de trabalho**. O padrão é **Nenhum**.

Se você selecionar **Criar um novo fluxo de trabalho**, defina essas configurações.

- **Nome:** digite um nome exclusivo para o fluxo de trabalho.
- **Descrição:** opcionalmente, digite uma descrição para o fluxo de trabalho.
- **Modelos de aprovação de email:** na lista, selecione o modelo de aprovação a ser atribuído. Quando você clica no ícone de olho à direita deste campo, uma caixa de diálogo é exibida na qual você pode visualizar o modelo.
- **Níveis de aprovação do gerente:** na lista, selecione o número de níveis de aprovação do gerente necessários para esse fluxo de trabalho. O padrão é 1 nível. As opções possíveis são:

- * Não é Necessário
 - * 1 nível
 - * 2 níveis
 - * 3 níveis
- **Selecionar domínio do Active Directory:** na lista, selecione o domínio do Active Directory adequado a ser usado para o fluxo de trabalho.
 - **Encontrar aprovadores necessários adicionais:** digite o nome adicional da pessoa no campo de pesquisa e clique em **Pesquisar**. Os nomes são originários do Active Directory.
 - Quando o nome aparece no campo, selecione a caixa de seleção próxima ao nome. O nome e endereço de email da pessoa aparecem na lista **Aprovadores necessários adicionais selecionados**.

Para remover uma pessoa da lista **Aprovadores necessários adicionais selecionados**, você pode optar por um dos seguintes procedimentos:

- * Clique em **Pesquisar** para ver uma lista de todas as pessoas do domínio selecionado.
- * Digite um nome parcial ou completo na caixa Pesquisar e clique em **Pesquisar** para limitar os resultados da pesquisa.
- * As pessoas da lista **Aprovadores necessários adicionais selecionados** têm marcas de seleção ao lado do respectivo nome na lista de resultados de pesquisa. Percorra a lista e desmarque a caixa de seleção ao lado de cada nome que você deseja remover.

Identidade visual do App store e Citrix Secure Hub

Você pode definir a forma como os aplicativos aparecem na loja e adicionar um logotipo para identificar o Secure Hub e a loja de aplicativos. Esses recursos de identidade visual estão disponíveis para dispositivos iOS e Android.

Antes de começar, verifique se a imagem personalizada está pronta e acessível.

A imagem personalizada deve atender a estes requisitos:

- O arquivo deve estar no formato .png
 - Use um logotipo em branco puro ou texto com um fundo transparente em 72 ppp.
 - O logotipo da empresa não deve exceder esta altura ou largura: 170 pixels x 25 pixels (1x) e 340 pixels x 50 pixels (2x).
 - Dê os seguintes nomes aos arquivos: Header.png e Header@2x.png.
 - Crie um arquivo .zip com os arquivos, não uma pasta que contenha os arquivos.
1. No console XenMobile Server, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida.

2. Em **Cliente**, clique em **Identidade visual do cliente**. A página **Identidade Visual do Cliente** é exibida.

Settings > Client Branding

Client Branding

You can set the way apps appear in the store and add a logo to brand Secure Hub on mobile devices.

Store name*

Default store view

Category

A-Z

Device

Phone

Tablet

Branding file

Note:

- The file must be in .png format (pure white logo/text with transparent background at 72 dpi).
- The company logo should not exceed this height or width: 170px x 25px (1x) + 340px x 50px (2x).
- Files should be named as Header.png and Header@2x.png.

A .zip file should be created from the files, not a folder with the files inside of it.

Faça as seguintes configurações:

- **Nome da loja:** o nome da loja será exibido nas informações da conta do usuário. Alterar o nome também altera a URL usada para acessar os serviços da loja de aplicativos. Geralmente, não é necessário alterar o nome padrão.

Importante:

O nome da loja só pode conter caracteres alfanuméricos.

- **Exibição de armazenamento padrão:** selecione **Categoria** ou **A-Z**. O padrão é **A-Z**
- **Dispositivo:** selecione **Telefone** ou **Tablet**. O padrão é **Telefone**.
- **Arquivo de identidade visual:** selecione uma imagem ou um arquivo .zip de imagens a ser usado para a identidade visual clicando em **Procurar** e navegando até a localização do arquivo.

3. Clique em **Salvar**.

Tipos de conector de aplicativo

August 24, 2018

A tabela a seguir lista os conectores e os tipos de conectores que estão disponíveis no XenMobile quando você adiciona um aplicativo da Web ou SaaS. Você também pode adicionar um novo conector ao XenMobile ao adicionar um aplicativo Web ou SaaS.

A tabela indica se o conector é compatível com o gerenciamento de conta de usuário, o que permite criar novas contas automaticamente ou usando um fluxo de trabalho.

Nome do conector	SSO SAML	Dá suporte ao gerenciamento de conta de usuário
EchoSign_SAML	S	S
Globoforce_SAML		Nota: quando você usar esse conector, ative a opção User Management for Provisioning para garantir a integração perfeita do SSO.
GoogleApps_SAML	S	S
GoogleApps_SAML_IDP	S	S
Lynda_SAML	S	S
Office365_SAML	S	S
Salesforce_SAML	S	S
Salesforce_SAML_SP	S	S
SandBox_SAML	S	
SuccessFactors_SAML	S	
ShareFile_SAML	S	
ShareFile_SAML_SP	S	
WebEx_SAML_SP	S	S

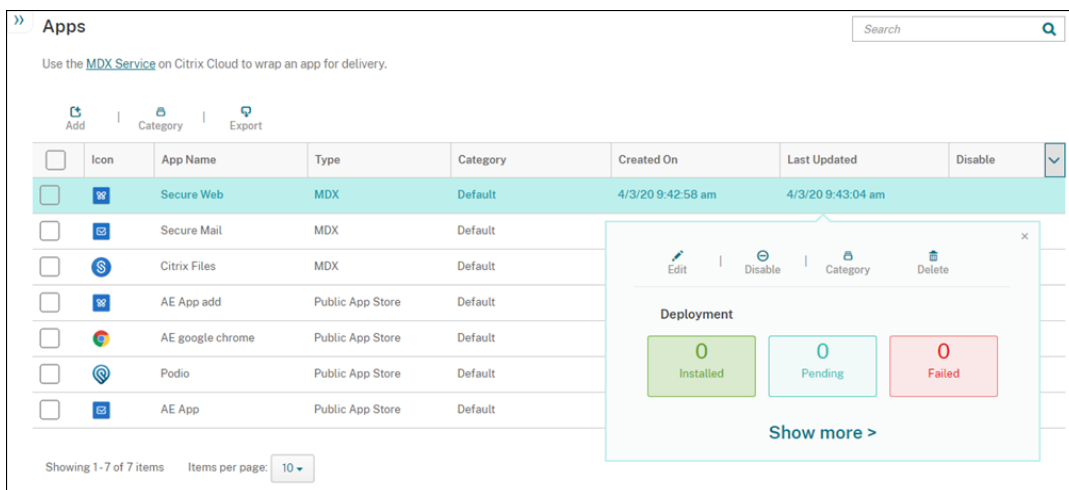
Atualizar aplicativos MDX ou empresariais

April 8, 2021

Para atualizar um aplicativo MDX ou Enterprise no XenMobile, desative o aplicativo no console XenMobile e carregue a nova versão do aplicativo. Você não precisa desativar aplicativos da loja de aplicativos pública, como o Citrix Secure Mail.

1. No console XenMobile, clique em **Configurar > Aplicativos**. A página **Aplicativos** é exibida.
2. Para dispositivos gerenciados (dispositivos registrados no XenMobile para gerenciamento de dispositivos móveis), pule para a etapa 3. Para dispositivos não gerenciados (dispositivos registrados no XenMobile para fins de gerenciamento de aplicativos empresariais), faça o seguinte:

- a) Na tabela **Aplicativos**, marque a caixa de seleção ao lado do aplicativo ou clique na linha que contém o aplicativo que você deseja atualizar.
- b) Clique em **Desativar** no menu que aparece.



- c) Clique em **Desativar** na caixa de diálogo de confirmação. *Desativado* é exibido na coluna **Desativar** do aplicativo.

<input type="checkbox"/>	Icon	App Name	Type	Category	Created On	Last Updated	Disable
<input type="checkbox"/>		Secure Web	MDX	Default	4/3/20 9:42:58 am	4/3/20 9:43:04 am	Disabled
<input type="checkbox"/>		Secure Mail	MDX	Default	4/3/20 9:43:09 am	4/3/20 9:43:16 am	<input type="checkbox"/>

Nota:

Enquanto o aplicativo está desativado, os usuários não podem se reconectar ao aplicativo depois que fazem logoff. Desativar um aplicativo é opcional, mas recomendamos desativar o aplicativo para evitar problemas com a funcionalidade dele. Por exemplo, quando usuários solicitam baixar o aplicativo ao mesmo tempo em que você carrega uma nova versão pode resultar em um problema.

3. Na tabela **Aplicativos**, clique na caixa de seleção ao lado do aplicativo ou clique na linha que contém o aplicativo que você deseja atualizar.
4. Clique em **Editar** no menu exibido. A página **Informações do aplicativo** é exibida com as plataformas que você escolheu originalmente para o aplicativo selecionado.
5. Defina estas configurações:
 - **Nome:** opcionalmente, altere o nome do aplicativo.
 - **Descrição:** opcionalmente, altere a descrição do aplicativo.
 - **Categoria do aplicativo:** opcionalmente, altere a categoria do aplicativo.
6. Clique em **Avançar**. A primeira página selecionada da plataforma é exibida. Faça o seguinte para cada plataforma selecionada:

- a) Escolha o arquivo de substituição que você quer carregar clicando em **Carregar** e navegue para a localização do arquivo. O aplicativo é carregado para o XenMobile.
Se você estiver carregando um aplicativo para o Android Enterprise, uma janela do Google Play gerenciado é exibida. Carregue a nova versão do aplicativo aqui. Para obter mais detalhes, consulte [Distribuir aplicativos Android Enterprise](#).
 - b) Opcionalmente, altere os detalhes de aplicativo e as configurações de política para a plataforma.
 - c) Opcionalmente, configure as regras de implantação e as configurações da XenMobile Store. Para obter informações, consulte Adicionar um aplicativo MDX em [Adicionar aplicativos](#).
7. Clique em **Salvar**. A página **Aplicativos** é exibida.
 8. Se você tiver desativado o aplicativo na Etapa 2, faça o seguinte:
 - a) Na tabela **Aplicativos**, clique para selecionar o aplicativo atualizado e, no menu exibido, clique em **Ativar**.
 - b) Na caixa de diálogo de confirmação exibida, clique em **Ativar**. Os usuários agora podem acessar o aplicativo e recebem um aviso de notificação solicitando que eles atualizem o aplicativo.

Citrix Launcher

July 10, 2020

Substituição do Citrix Launcher

A Citrix removerá o Citrix Launcher da loja de aplicativos em agosto de 2020. Para substituir o Citrix Launcher, você pode usar recursos que já estão disponíveis.

Para provisionar dispositivos como quiosques (dispositivos dedicados):

1. Adicione uma função RBAC que permita que os administradores do XenMobile registrem dispositivos dedicados na sua implantação do XenMobile. Veja [Provisionamento de dispositivos Android Enterprise dedicados](#).
2. Crie um perfil de registro com um **Tipo de inscrição** de **Totalmente gerenciado/Perfil de trabalho**. Veja [Para criar um perfil de registro](#).
3. Crie uma política de dispositivo de quiosque para configurar um aplicativo para fixar na tela do dispositivo ativando a configuração **Bloquear modo tarefa**. Veja [Configurações do Android Enterprise](#).

Sobre o Citrix Launcher

O Citrix Launcher permite que você personalize a experiência do usuário para dispositivos Android implantados pelo XenMobile. A versão mínima do Android com suporte para o gerenciamento do Secure Hub do Citrix Launcher é o Android 4.0.3. O Citrix Launcher e a política do dispositivo de configuração do Launcher não são compatíveis com o Android Enterprise.

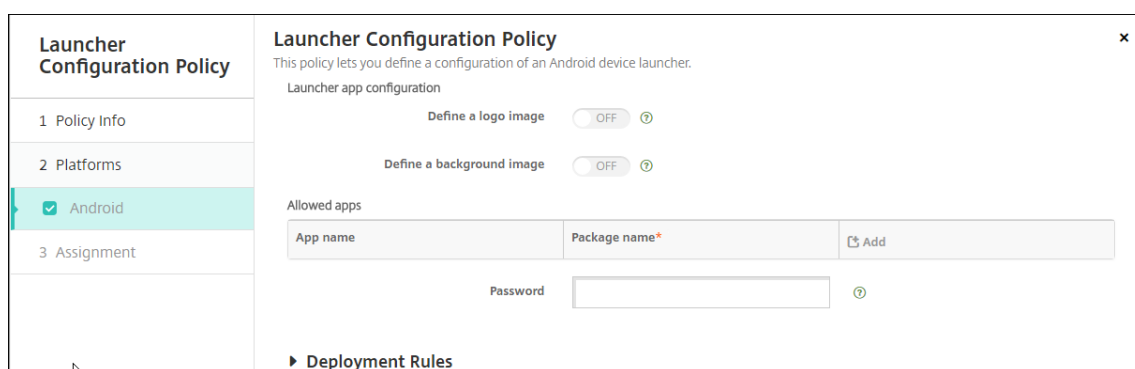
Você pode adicionar uma **Política de Configuração do Launcher** para controlar estes recursos do Citrix Launcher:

- Gerenciar dispositivos Android para que os usuários possam acessar somente os aplicativos que você especificar.
- Opcionalmente, especifique uma imagem de logotipo personalizado para o ícone do Citrix Launcher e uma imagem de plano de fundo personalizado para o Citrix Launcher.
- Especifique uma senha que os usuários devem digitar para sair do Launcher.

Embora o Citrix Launcher permita aplicar essas restrições em nível de dispositivo, o iniciador concede aos usuários acesso incorporado a configurações de dispositivos, como configurações de Wi-Fi, Bluetooth e de código secreto de dispositivo. O Citrix Launcher não foi criado com a intenção de ser uma camada extra de segurança além da que a plataforma de dispositivo já fornece.

Para fornecer o Citrix Launcher para dispositivos Android, siga estes procedimentos gerais.

1. Para baixar o aplicativo Citrix Launcher, acesse <https://www.citrix.com/downloads>. Procure por **Citrix Launcher**. O nome do arquivo é CitrixLauncher.apk. O arquivo está pronto para carregar no XenMobile e não requer preparação.
2. Adicione a política de dispositivo **Política de Configuração do Launcher**. Vá até **Configurar > Políticas de dispositivo**, clique em **Adicionar** e, na caixa de diálogo **Adicionar uma nova política**, comece a digitar **Launcher**. Para obter mais informações, consulte [Política de configuração do Launcher](#).

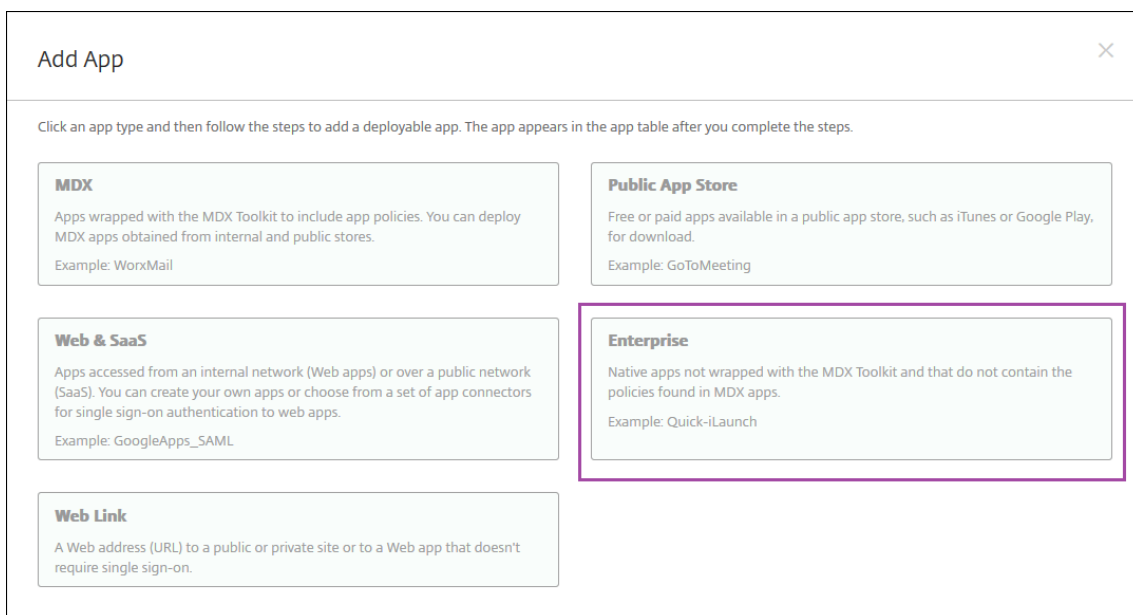


The screenshot shows the 'Launcher Configuration Policy' configuration window. On the left, a sidebar lists '1 Policy Info', '2 Platforms', '3 Assignment', and '4 Deployment Rules', with 'Android' selected under 'Platforms'. The main area is titled 'Launcher Configuration Policy' and contains the following settings:

- Launcher app configuration:**
 - Define a logo image:** OFF (with a help icon)
 - Define a background image:** OFF (with a help icon)
- Allowed apps:** A table with columns for 'App name', 'Package name*', and an 'Add' button.
- Password:** A text input field with a help icon.

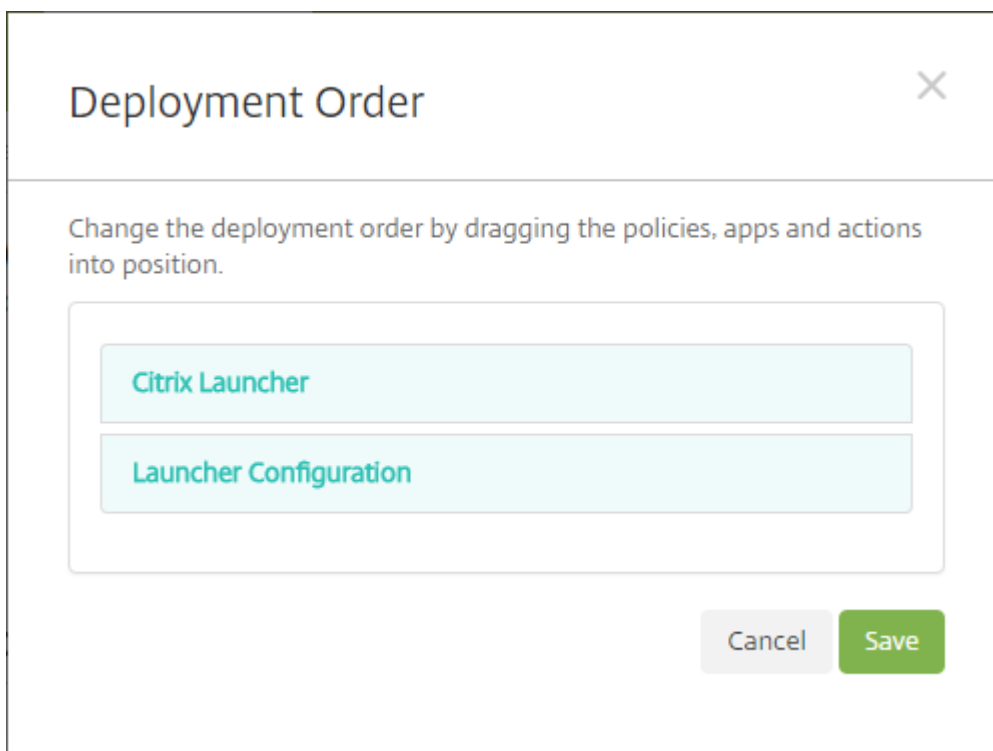
At the bottom, there is a 'Deployment Rules' section with a right-pointing arrow.

3. Adicione o aplicativo Citrix Launcher ao XenMobile como um aplicativo corporativo. Em **Configurar > Aplicativos**, clique em **Adicionar** e, em seguida, clique em **Empresarial**. Para obter mais informações, consulte [Acrescentar um aplicativo empresarial](#).



4. Crie um grupo de entrega para o Citrix Launcher com a configuração a seguir em **Configurar > Grupos de entrega**.

- Na página **Políticas**, adicione a **Política de configuração do Launcher**.
- Na página **Aplicativos**, arraste **Citrix Launcher** até **Aplicativos obrigatórios**.
- Na página **Resumo**, clique em **Ordem de implantação** e verifique se o aplicativo **Citrix Launcher** precede a política **Configuração do Launcher**.



Para obter mais informações, consulte [Implantar recursos](#).

Compra por volume da Apple

November 30, 2020

Você pode gerenciar o licenciamento de aplicativos iOS usando a compra por volume do Apple iOS. A compra por volume simplifica o processo para localizar, comprar e distribuir aplicativos e outros dados em massa para uma organização.

Com a compra por volume, você pode usar o XenMobile para distribuir aplicativos de loja de aplicativos pública.

- A compra por volume não é suportada para registro de MAM. Você deve registrar dispositivos de compra por volume em MDM ou MDM+MAM.
- Não há suporte para compra por volume para aplicativos móveis de produtividade Citrix.
- Embora você possa distribuir os aplicativos de loja pública do XenMobile com a compra por volume, a implantação não é otimizada. São necessárias melhorias no XenMobile e na loja do Secure Hub para resolver as limitações.
- Para obter uma lista de problemas conhecidos com a distribuição de aplicativos da loja pública do XenMobile por meio da compra por volume, consulte este artigo no Citrix [knowledge center](#).

Com a compra por volume, você pode distribuir os aplicativos aplicáveis diretamente para os dispositivos. Ou você pode atribuir conteúdo para seus usuários usando códigos resgatáveis. Você pode fazer as configurações específicas da compra por volume do iOS no XenMobile.

O XenMobile reimporta periodicamente as licenças da compra por volume da Apple para garantir que elas reflitam todas as alterações. Essas alterações se incluem quando você exclui manualmente um aplicativo importado da compra por volume. Por padrão, o XenMobile atualiza a linha de base da licença de compra por volume no mínimo a cada 1440 minutos (24 horas). Você pode alterar o intervalo de linha de base da compra por volume por meio da propriedade do servidor `VPP.baseLine`. Veja [Propriedades do servidor](#).

A configuração **Atualização automática do aplicativo** também depende da propriedade de servidor `VPP.baseLine`, e os aplicativos são atualizados no mesmo cronograma definido nessa propriedade.

Este artigo aborda o uso de compra por volume com licenças gerenciadas, o que permite que você use o XenMobile para distribuir aplicativos. Se você atualmente usa códigos de resgate e deseja mudar para distribuição gerenciada, consulte o documento do Suporte da Apple sobre [Migrar dos códigos de resgate para a distribuição gerenciada com a compra por volume](#).

Para obter informações sobre a compra por volume do iOS, consulte <https://volume.itunes.apple.com/us/store>. Para se registrar na compra por volume, vá para <https://deploy.apple.com/qforms/>

open/register/index/avs. Para acessar sua loja de compra por volume no iTunes, vá para <https://volume.itunes.apple.com/?l=en>.

Depois que você salva as configurações de compra por volume do iOS no XenMobile, os aplicativos comprados aparecem na página **Configurar > Aplicativos** no console XenMobile.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida.
2. Clique em **Compra por volume**. A página de configuração de **Volume Purchase** é exibida.

Name	Suffix	Organization	Country	Expiration Date	User Login
test	Volume Purchase Acct	Citrix Systems	United States	10/24/20 10:43:54 am	

3. Defina estas configurações:
 - **Armazenar a senha de usuário no Secure Hub:** Selecione se um nome do usuário e uma senha devem ser armazenados no Secure Hub para a autenticação do XenMobile. O padrão é armazenar as informações seguras usando este método de segurança.
 - **Propriedade do usuário para mapeamento de país de compra por volume:** digite um código para permitir que os usuários baixem aplicativos de lojas de aplicativos específicas de cada país.

O XenMobile usa esse mapeamento para escolher o pool de propriedades da compra por volume. Por exemplo, se a propriedade do usuário for Estados Unidos, ele não poderá baixar aplicativos se o código de compra por volume for para o Reino Unido. Contate o administrador do plano de compra por volume para obter mais informações sobre o código de mapeamento do país.

4. Para cada conta de compra por volume que você quiser adicionar, clique em **Adicionar**. A caixa de diálogo **Adicionar uma conta de compra de volume** é exibida.
5. Defina estas configurações para cada conta que você adicionar:

Nota:

Se você estiver usando o Apple Configurator 1, carregue um arquivo de licença: vá até **Configurar > Aplicativos**, vá para uma página da plataforma e expanda **Compra por volume**.

- **Nome:** digite o nome da conta de compra por volume.
- **Sufixo:** digite o sufixo a ser exibido com os nomes dos aplicativos obtidos usando a conta de compra por volume. Por exemplo, se você inserir **VP**, o aplicativo Secure Mail é exibido

na lista de aplicativos, como **Secure Mail - VP**.

- **Token da empresa:** Digite ou copie e cole o token de serviço de compra por volume obtido da Apple. Para obter o token: na página **Account Summary** do portal de compra por volume da Apple, clique no botão **Download** para gerar e baixar o arquivo de compra por volume. O arquivo contém o token de serviço e outras informações, como o código do país e a expiração. Salve o arquivo em um local seguro.
- **Login de usuário:** Digite um nome opcional de administrador de conta de compra por volume autorizada usado para importar aplicativos B2B personalizados.
- **Senha de usuário:** Digite a senha de administrador de conta de compra por volume.
- **Atualização automática do aplicativo:** se **Ativado**, os aplicativos de compra por volume serão atualizados automaticamente quando houver uma atualização na Apple Store. O padrão é **Desativado**.

6. Clique em **Salvar** para fechar a caixa de diálogo.

7. Clique em **Salvar** para salvar a configuração de compra por volume.

É exibida uma mensagem que informa que o XenMobile adiciona os aplicativos à lista na página **Configurar > Aplicativos**. Nessa página, observe que os nomes dos aplicativos da sua conta de compra por volume contêm o sufixo que você forneceu na configuração anterior.

Você pode agora definir as configurações do aplicativo de compra por volume e, em seguida, ajustar as suas configurações de política de dispositivo e grupo de entrega para aplicativos de compra por volume. Depois de concluir essas configurações, os usuários podem registrar seus dispositivos. A seguir indica fornecem considerações para esses processos.

- Ao definir as configurações de aplicativo de compra por volume (**Configurar > Aplicativos**), ative **Forçar associação de licença ao dispositivo**. Uma vantagem de usar a compra por volume e o programa de implantação da Apple com dispositivos supervisionados: a capacidade de usar o XenMobile para atribuir o aplicativo no nível de dispositivo (em vez de usuário). Desse modo, você não precisa usar um dispositivo com Apple ID. Além disso, os usuários não recebem um convite para participar da compra por volume da Apple. Os usuários também podem baixar aplicativos sem entrar na respectiva conta do iTunes.

Para exibir as informações de compra por volume do aplicativo, expanda **Compra por volume**. Observe na tabela **Chaves de licença de compra por volume** que a licença está associada a um dispositivo. Se o usuário remove o token e, em seguida, importa-o novamente, a palavra **Oculto** é exibida em vez do número de série, devido a restrições de privacidade da Apple.

Para desassociar uma licença, clique na linha da licença e clique em **Desassociar**.

Se você associar licenças de compra por volume a usuários, o XenMobile integrará os usuários à sua conta de compra por volume e associará o ID do iTunes à conta de compra por volume. A ID do iTunes dos usuários nunca é visível para a sua empresa ou para o servidor XenMobile. Apple transparente cria a associação para manter a privacidade do usuário. Você pode desativar um

usuário da compra por volume da Apple para desassociar todas as licenças da conta do usuário. Para desativar um usuário, vá para **Gerenciar > Dispositivos**.

The screenshot shows the 'User Properties' configuration page in the XenMobile console. On the left, a sidebar lists various configuration options, with '3 User Properties' highlighted. The main area is titled 'User Properties' and contains several input fields: 'User name' (set to 'user123'), 'Password' (with a placeholder 'Enter new password'), and 'Role' (set to 'USER'). Below these is a 'Membership' section with a checkbox for 'local\MSP' and a 'Manage Groups' button. At the bottom, there is a 'Volume Purchase Accounts' section with a checkbox for 'Volume Purchase' and a 'Retire' button. At the bottom right of the page, there are 'Back' and 'Next >' buttons.

- Quando você atribuir um aplicativo a um grupo de entrega, como padrão, o XenMobile identifica o aplicativo como um aplicativo opcional. Para garantir que o XenMobile implante um aplicativo em dispositivos, vá até **Configurar > Grupos de entrega**. Na página **Aplicativos**, mova o aplicativo para a lista **Aplicativos obrigatórios**.
- Quando uma atualização de um aplicativo da loja de aplicativos pública está disponível: quando a compra por volume envia o aplicativo, o aplicativo é atualizado automaticamente nos dispositivos. Para enviar uma atualização para o Secure Hub quando atribuída a um dispositivo e não a um usuário, faça o seguinte. Na página **Configurar > Aplicativos**, em uma página de plataforma, clique em **Verificar se há atualizações** e aplique a atualização.

O XenMobile exibe um Aviso de Expiração de Licença quando os tokens de compra por volume da Apple expirarem.

Aplicativos e áreas de trabalho virtuais através do Citrix Secure Hub

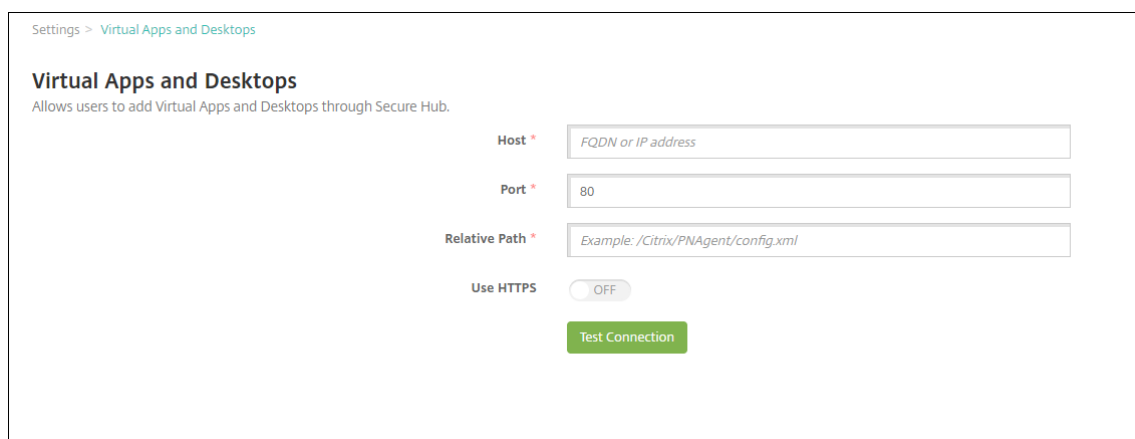
November 30, 2020

O XenMobile pode coletar aplicativos do Virtual Apps and Desktops e disponibilizá-los para usuários

de dispositivos móveis no XenMobile Store. Os usuários assinam os aplicativos diretamente no XenMobile Store e os iniciam do Secure Hub. O Citrix Receiver deve estar instalado nos dispositivos do usuário para iniciar os aplicativos, mas não precisa ser configurado.

Para configurar essa definição, você precisa do nome de domínio totalmente qualificado (FQDN) ou do endereço IP, e do número de porta do site Web Interface ou StoreFront.

1. No console da Web XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida.
2. Clique em **Aplicativos virtuais e desktops**. A página **Aplicativos virtuais e desktops** é exibida.



Settings > Virtual Apps and Desktops

Virtual Apps and Desktops

Allows users to add Virtual Apps and Desktops through Secure Hub.

Host *

Port *

Relative Path *

Use HTTPS

3. Defina estas configurações:
 - **Host:** digite o nome de domínio totalmente qualificado (FQDN) ou o endereço IP do site Web Interface ou do StoreFront.
 - **Porta:** digite o número de porta do site Web Interface ou do StoreFront. O padrão é 80.
 - **Caminho relativo:** digite o caminho. Por exemplo, /Citrix/PNAgent/config.xml
 - **Usar HTTPS:** selecione se a autenticação segura entre o site Web Interface ou do StoreFront e o dispositivo de cliente deve ser ativada. O padrão é **O**.
4. Clique em **Testar conexão** para verificar se o XenMobile pode se conectar ao servidor de aplicativos e áreas de trabalho virtuais especificado.
5. Clique em **Salvar**.

Usar Citrix Content Collaboration com XenMobile

September 10, 2020

O XenMobile tem duas opções para integração com o Citrix Content Collaboration: Citrix Files e conectores de zona de armazenamento. A integração com o Citrix Files ou com conectores de zona de armazenamento requer o XenMobile Enterprise Edition.

Citrix Files

Se você tem o XenMobile Enterprise Edition, pode configurar o XenMobile para fornecer acesso à sua conta do Citrix Files. Essa configuração:

- Permite que usuários móveis acessem o conjunto completo de recursos do Enterprise, como compartilhamento de arquivos, sincronização de arquivos e conectores de zona de armazenamento.
- Pode fornecer ao Citrix Files autenticação de logon único de usuários de XenMobile Apps e políticas abrangentes de controle de acesso.
- Fornece configuração, monitoramento de nível de serviço e monitoramento do uso de licenças do Citrix Files por meio do console XenMobile.

Para obter mais informações sobre como configurar o XenMobile para Citrix Files, consulte [SAML para logon único com Citrix Files](#).

Conectores de zona de armazenamento

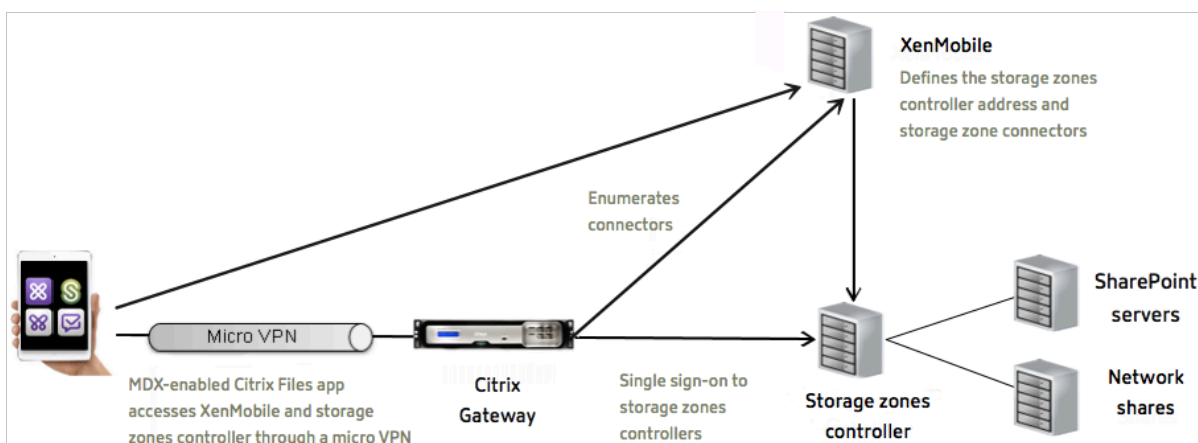
Você pode configurar o XenMobile para fornecer acesso somente aos conectores de zona de armazenamento que você cria por meio do console XenMobile. Essa configuração:

- Fornece aos usuários acesso móvel a repositórios de armazenamento no local existentes, como sites do SharePoint e compartilhamentos de arquivos de rede.
- Não requer que você configure um subdomínio do Citrix Content Collaboration ou hospede dados do Citrix Files.
- Fornece aos usuários acesso móvel aos dados por meio dos aplicativos móveis de produtividade do Citrix Files para iOS e Android. Os usuários podem editar documentos do Microsoft Office. Os usuários também podem visualizar e fazer anotações em arquivos Adobe PDF em dispositivos móveis.
- Está em conformidade com restrições de segurança contra vazamento de informações de usuários fora da rede corporativa.
- Fornece a configuração simples de conectores de zona de armazenamento por meio do console XenMobile. Se mais tarde você decidir usar a funcionalidade completa do Citrix Files com o XenMobile, poderá alterar a configuração no console XenMobile.
- Requer o XenMobile Enterprise Edition.

Apenas para uma XenMobile integração com conectores de zona de armazenamento:

- O Citrix Content Collaboration usa sua configuração de logon único para Citrix Gateway para autenticar com o controlador de zonas de armazenamento.
- O XenMobile não se autentica via SAML porque o plano de controle do Citrix Files não é usado.

O diagrama a seguir mostra a arquitetura de alto nível para o uso do XenMobile com conectores de zona de armazenamento.



Requisitos

- Versões mínimas dos componentes:
 - XenMobile Server 10.5 (no local)
 - ShareFile para iOS (MDX) 5.3
 - ShareFile para Android (MDX) 5.3
 - StorageZone Controller 5.0Este artigo contém instruções sobre como configurar o StorageZone Controller 5.0
- Verifique se o servidor que deverá executar o controlador de zonas de armazenamento atende aos requisitos de sistema. Para obter requisitos, consulte [Requisitos do sistema](#).

Os requisitos de zonas de armazenamento para Citrix Files Data e para zonas de armazenamento Restricted não se aplicam apenas a uma integração XenMobile com conectores de zona de armazenamento.

O XenMobile não dá suporte a conectores Documentum.

- Para executar scripts do PowerShell:
 - Execute os scripts na versão de 32 bits (x86) do PowerShell.

Tarefas de instalação

Execute as tarefas a seguir, na ordem apresentada, para instalar e configurar o controlador de zonas de armazenamento. Estes passos são específicos apenas para uma integração XenMobile com conectores de zona de armazenamento: Alguns desses artigos estão na documentação do controlador de zonas de armazenamento.

1. [Configurar o Citrix ADC para controlador de zonas de armazenamento](#)

Você pode usar o Citrix ADC como um proxy DMZ para controlador de zonas de armazenamento.

2. [Instalar um certificado SSL](#)

Um controlador de zonas de armazenamento que hospeda zonas padrão requer um certificado SSL. Um controlador de zonas de armazenamento que hospeda zonas restritas e usa um endereço interno não requer um certificado SSL.

3. [Preparar seu servidor](#)

É necessário instalar o IIS e ASP.NET para conectores de zona de armazenamento.

4. Instalar o controlador de zonas de armazenamento

5. Preparar o controlador de zonas de armazenamento para usar apenas com conectores de zona de armazenamento

6. [Especificar um servidor proxy para zonas de armazenamento](#)

O console dos controladores de zonas de armazenamento permite que você especifique um servidor proxy para os controladores de zonas de armazenamento. Você também pode especificar um servidor proxy usando outros métodos.

7. [Configurar o controlador de domínio para confiar no controlador de zonas de armazenamento para delegação](#)

Configure o controlador de domínio para oferecer suporte à autenticação NTLM ou Kerberos em compartilhamentos de rede ou sites do SharePoint.

8. Associar um controlador de zonas de armazenamento secundário a uma zona de armazenamento

Para configurar uma de zona de armazenamento para alta disponibilidade, conecte pelo menos dois controladores de zonas de armazenamento a ela.

Instalar o controlador de zonas de armazenamento

1. Baixe e instale o software do controlador de zonas de armazenamento:

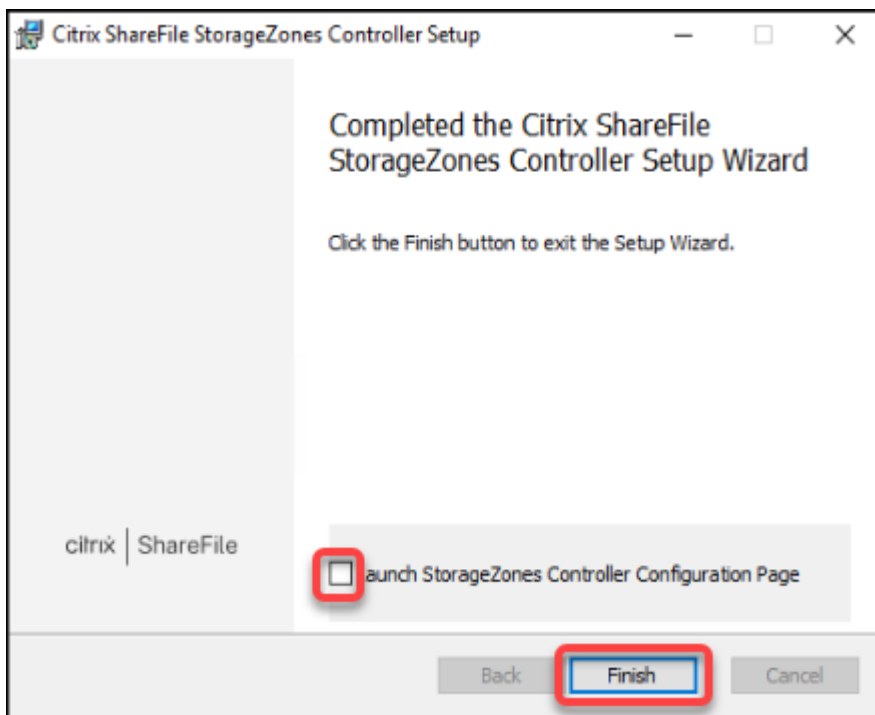
- a) Acesse <https://www.citrix.com/downloads>. Procure por **ShareFile** e faça o download do instalador mais recente do controlador de zonas de armazenamento.
- b) A instalação do controlador de zonas de armazenamento altera o site padrão no servidor para o caminho de instalação do controlador. Ativar a **Autenticação anônima** no site da Web padrão.

2. No servidor em que você deseja instalar o controlador de zonas de armazenamento, execute StorageCenter.msi.

O assistente de instalação do controlador de zonas de armazenamento iniciará.

3. Responda às solicitações:

- Na página **Destination Folder**, se os serviços de informações da Internet (IIS) estiverem instalados no local padrão, mantenha as configurações padrão. Caso contrário, navegue até o local de instalação do IIS.
- Quando a instalação for concluída, desmarque a caixa de seleção **Launch Storage Zones Controller Configuration Page** e, em seguida, clique em **Finish**.



4. Quando solicitado, reinicie o controlador de zonas de armazenamento.
5. Para testar se a instalação foi bem sucedida, navegue para <https://localhost/>. Se a instalação for bem-sucedida, o logotipo Citrix Files será exibido.

Se o logotipo Citrix Files não for exibido, limpe o cache do navegador e tente novamente.

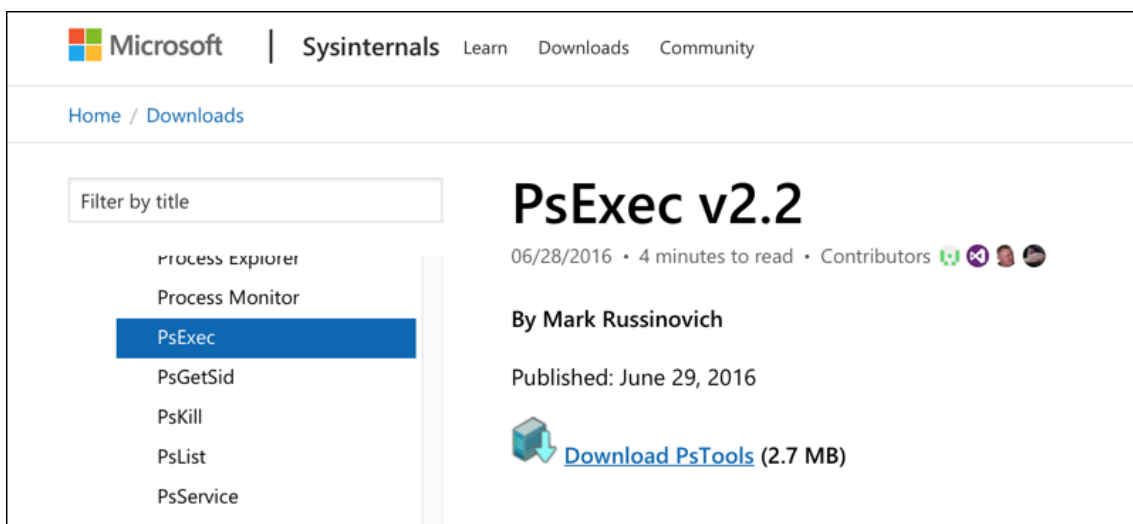
Importante:

Se você planeja clonar o controlador de zonas de armazenamento, capture a imagem de disco antes de continuar configurando o controlador de zonas de armazenamento.

Preparar o controlador de zonas de armazenamento para usar apenas com conectores de zona de armazenamento

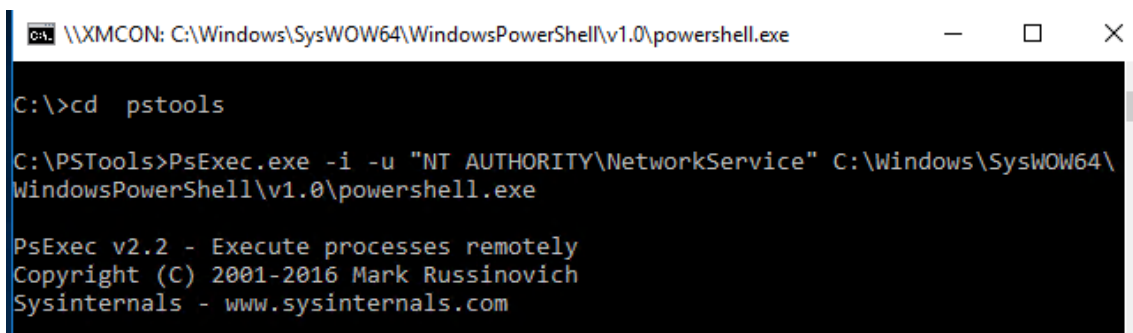
Para uma integração apenas com conectores de zona de armazenamento, você não usa o console administrativo do controlador de zonas de armazenamento. Aquela interface requer uma conta de administrador do Citrix Files, o que não é necessário para esta solução. Como resultado, você pode executar um script do PowerShell para preparar o controlador de zonas de armazenamento para uso sem o plano de controle do Citrix Files. O script faz o seguinte:

- Registra o controlador de zonas de armazenamento atual como um controlador de zonas de armazenamento primário. Mais tarde você pode associar os controladores de zonas de armazenamento secundários ao controlador primário.
 - Cria uma zona e define a senha para ela.
1. No servidor do seu controlador de zonas de armazenamento, baixe a ferramenta PsExec: navegue até Microsoft [Windows Sysinternals](#) e, em seguida, clique em **Download PsTools**. Extraia a ferramenta para a raiz da unidade C.

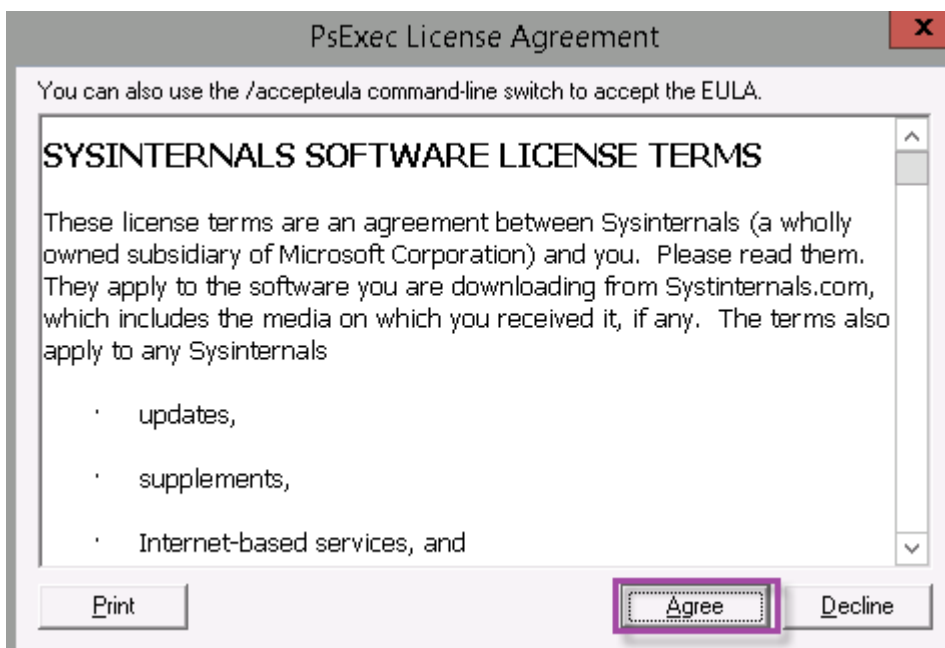


2. Execute a ferramenta PsExec: Abra o aviso de comando como o usuário de administrador e, em seguida, digite o seguinte:

```
1 cd c:\pstools
2 PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64\
  \WindowsPowerShell\v1.0\powershell.exe
3 <!--NeedCopy-->
```



3. Quando solicitado, clique em **Concordar** para executar a ferramenta Sysinternals.



É aberta uma janela do PowerShell.

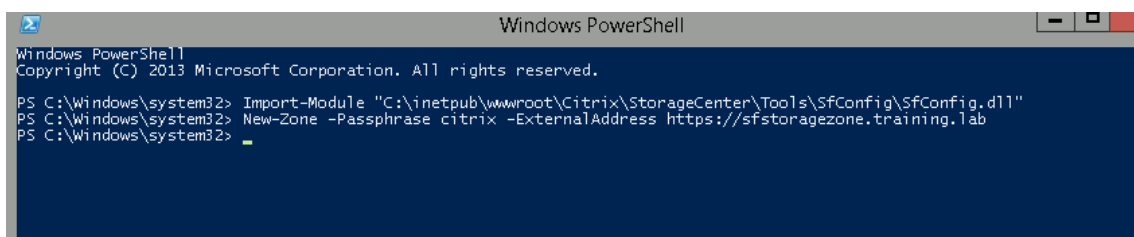
4. Na janela do PowerShell, digite o seguinte:

```
1 Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfig\SfConfig.dll"  
2 New-Zone -Passphrase passphrase -ExternalAddress https://szcfqdn.com  
3 <!--NeedCopy-->
```

Onde:

Passphrase: é a senha que você deseja atribuir o site. Anote-a. Não é possível recuperar a senha por meio do controlador. Se perder a senha, você não poderá reinstalar o controlador de zonas de armazenamento. Associe mais controladores de zonas de armazenamento à zona de armazenamento, ou recupere a zona de armazenamento se o servidor falhar.

ExternalAddress: é o nome de domínio totalmente qualificado externo do servidor do controlador de zonas de armazenamento.



Seu controlador de zonas de armazenamento primário está pronto.

Antes de fazer logon no XenMobile para criar conectores de zona de armazenamento, conclua a configuração a seguir, se aplicável:

[Especificar um servidor proxy para zonas de armazenamento](#)

[Configurar o controlador de domínio para confiar no controlador de zonas de armazenamento para delegação](#)

[Associar um controlador de zonas de armazenamento secundário a uma zona de armazenamento](#)

Para criar conectores de zona de armazenamento, consulte Definir conexões do controlador de zonas de armazenamento no XenMobile.

Associar um controlador de zonas de armazenamento secundário a uma zona de armazenamento

Para configurar uma de zona de armazenamento para alta disponibilidade, conecte pelo menos dois controladores de zonas de armazenamento a ela. Para associar um controlador de zonas de armazenamento secundário a uma zona, instale o controlador de zonas de armazenamento em um segundo servidor. Em seguida, junte esse controlador à zona do controlador principal.

1. Abra uma janela do PowerShell no servidor do controlador de zonas de armazenamento que você deseja associar ao servidor primário.
2. Na janela do PowerShell, digite o seguinte:

```
Join-Zone -Passphrase <passphrase> -PrimaryController <HostnameOrIP>
```

Por exemplo:

```
Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210
```

Definir conexões do controlador de zonas de armazenamento no XenMobile

Antes de adicionar conectores de zona de armazenamento, configure as informações de conexão para cada controlador de zonas de armazenamento habilitado para conectores de zona de armazenamento. Você pode definir controladores de zonas de armazenamento conforme descrito nesta seção ou ao adicionar um conector.

Na sua primeira visita à página **Configurar > ShareFile**, a página resume as diferenças entre o uso de contas do XenMobile para Enterprise e de conectores de zona de armazenamento.

Choose a method for integrating ShareFile with XenMobile or learn more about which mode to select.

	ShareFile Enterprise	StorageZone Connectors Only
Access network shares and SharePoint data from mobile devices	✓	✓
Edit Microsoft Office documents from mobile devices	✓	✓
Preview and annotate Adobe PDF files from mobile devices	✓	✓
Store data in Citrix-managed or customer-managed StorageZones or both	✓	
Securely share files with people inside and outside the enterprise	✓	
Sync files and data across multiple devices	✓	
Access files through the ShareFile website	✓	
Access Office 365 content and Personal Cloud connectors from mobile devices	✓	
Use auditing and reporting capabilities	✓	

[Configure ShareFile Enterprise](#)
[Configure Connectors](#)

Clique em **Configurar conectores** para continuar com as etapas de configuração neste artigo.

StorageZone Connectors Show filter

StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.

<input type="checkbox"/>	Connector Name	Type	StorageZone	Location	Delivery Groups

1. Em **Configurar > ShareFile**, clique em **Gerenciar StorageZones**.

StorageZone Connectors Show filter

StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.

<input type="checkbox"/>	Connector Name	Type	StorageZone	Location	Delivery Groups

2. Em **Gerenciar StorageZones**, adicione as informações de conexão.

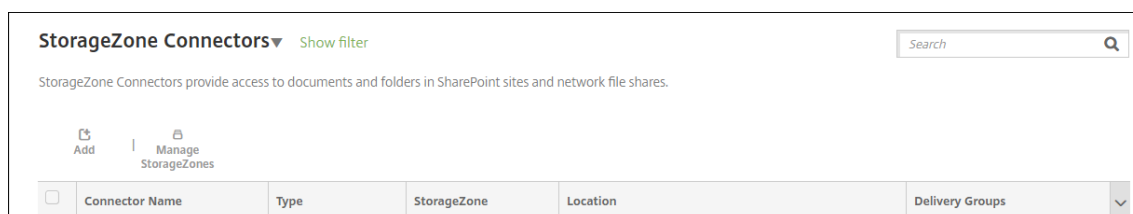
- **Nome:** um nome descritivo para o StorageZone, usado para identificar o StorageZone no XenMobile. Não inclua espaços ou caracteres especiais no nome.
 - **FQDN e porta:** o nome de domínio totalmente qualificado e o número da porta de um controlador de zonas de armazenamento que pode ser alcançada a partir do XenMobile Server.
 - **Conexão segura:** se você usar SSL para conexões com o controlador de zonas de armazenamento, use a configuração padrão, I. Se você não usar SSL para conexões, altere essa configuração para O.
 - **Nome de usuário do administrador e Senha do administrador:** um nome de usuário da conta de serviço de administrador (no formato domínio\administrador) e a respectiva senha. Como alternativa, uma conta de usuário com permissões de leitura e gravação nos controladores de zonas de armazenamento.
3. Clique em **Salvar**.
 4. Para testar a conexão, verifique se o XenMobile Server pode alcançar o nome de domínio totalmente qualificado do controlador de zonas de armazenamento na porta 443.
 5. Para definir outra conexão com o controlador de zonas de armazenamento, clique no botão **Adicionar** em **Gerenciar StorageZones**.

Para editar ou excluir as informações de uma conexão do controlador de zonas de armazena-

mento, selecione o nome da conexão em **Gerenciar StorageZones**. Em seguida, clique em **Editar** ou **Excluir**.

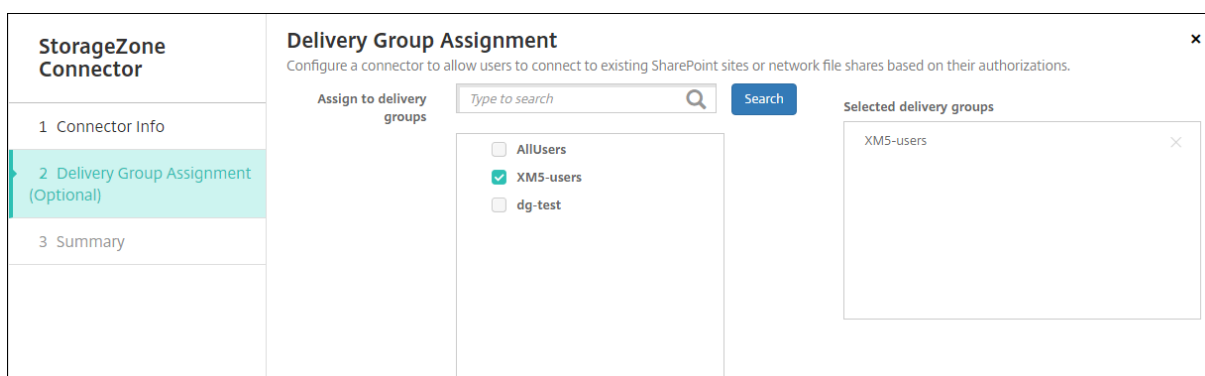
Adicionar um controlador de zonas de armazenamento ao XenMobile

1. Vá até **Configurar > ShareFile** e clique em **Adicionar**.



2. Na página **Informações do Connector**, defina estas configurações:

- **Nome do conector:** um nome que identifica o conector de zona de armazenamento no XenMobile.
 - **Descrição:** observações opcionais sobre esse Connector.
 - **Tipo:** escolha **SharePoint** ou **Rede**.
 - **StorageZone:** escolha as zonas de armazenamento associadas ao conector. Se a zona de armazenamento não estiver na lista, clique em **Gerenciar StorageZones** para definir o controlador de zonas de armazenamento.
 - **Localização:** no SharePoint, especifique a URL do site de nível raiz, o conjunto de sites ou a biblioteca de documentos do SharePoint, no formato <https://sharepoint.company.com>. Para um compartilhamento de rede, especifique o nome de domínio totalmente qualificado do caminho UNC (Uniform Naming Convention), no formato `\\servidor\compartilhamento`.
3. Na página **Atribuição de grupo de entrega**, atribua opcionalmente o Conector a grupos de entrega. Como alternativa, você pode associar conectores a grupos de entrega usando **Configurar > Grupos de entrega**.



1. Na página **Resumo**, você pode rever as opções configuradas. Para ajustar a configuração, clique em **Voltar**.
2. Clique em **Salvar** para salvar o Conector.
3. Teste o conector:

a) Ao prepara os clientes Citrix Files, faça o seguinte:

- Defina a política de Acesso à rede como **Com túnel para a rede interna**.

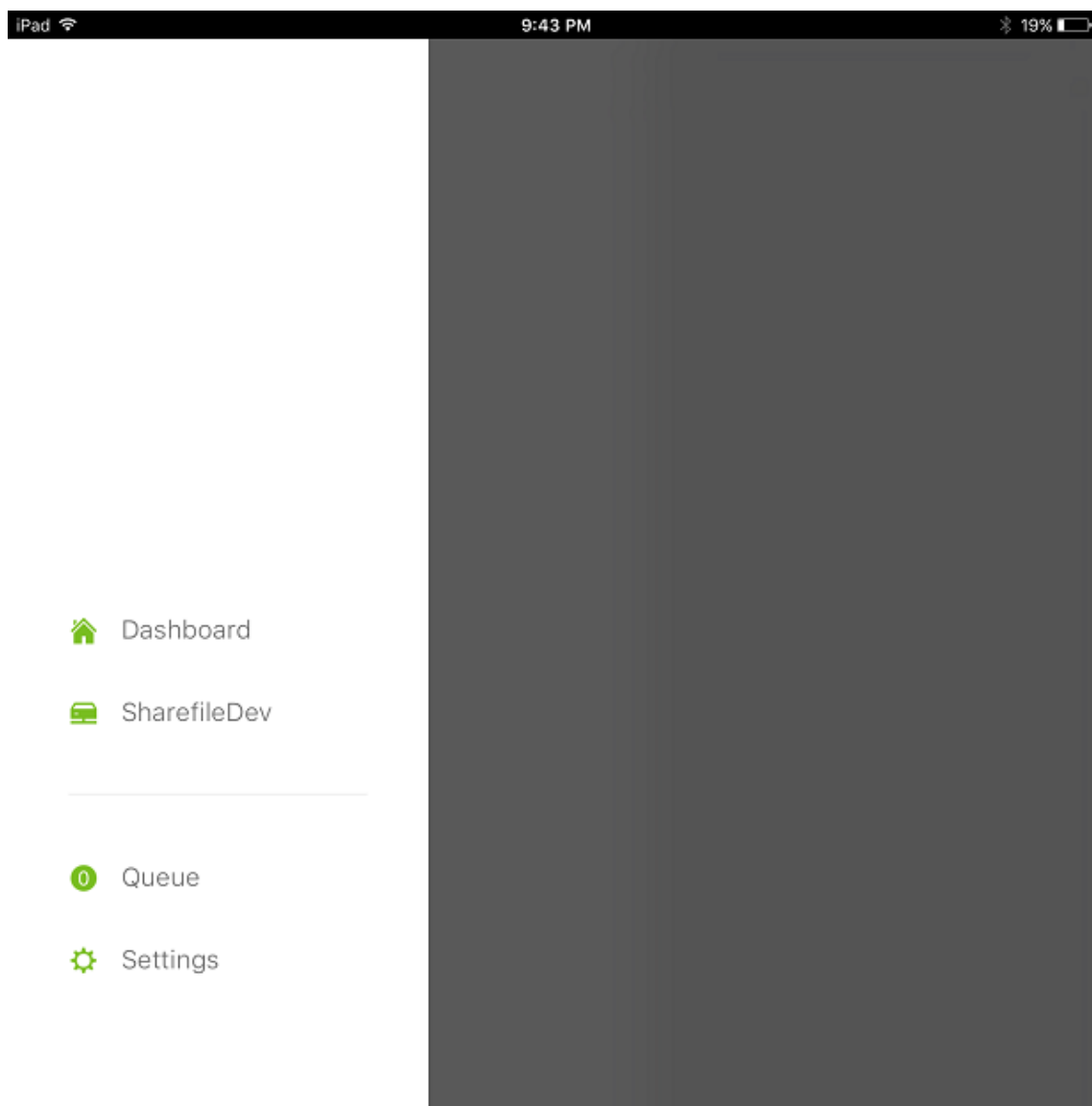
Nesse modo de operação, o framework XenMobile MDX intercepta todo o tráfego de rede do cliente do Citrix Files. O tráfego é redirecionado por meio do Citrix Gateway por meio de uma micro VPN específica para o aplicativo.

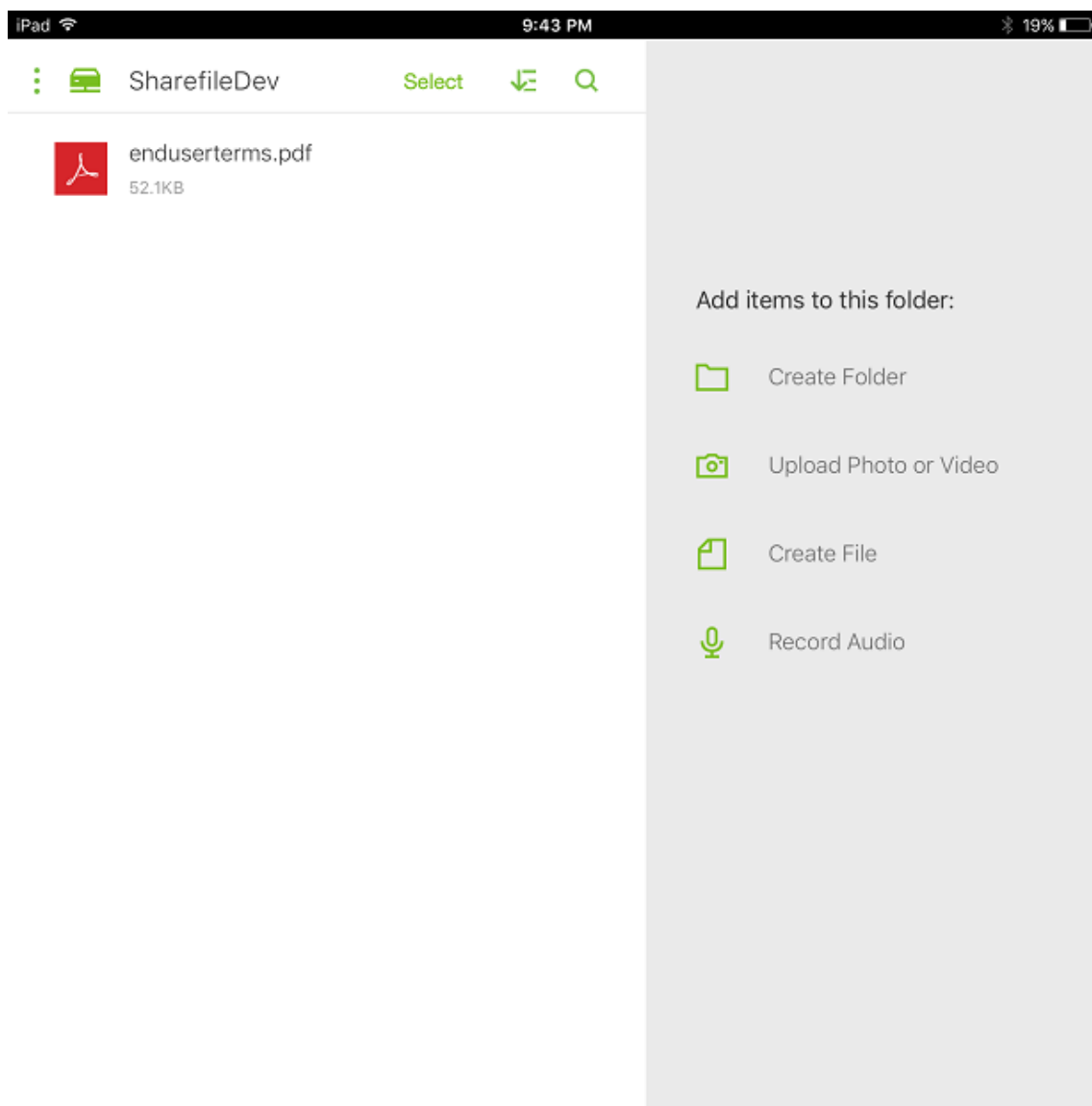
- Defina a política de modo VPN preferido como **Com túnel - SSO de Web**.

Nesse modo de criação de túneis, o framework MDX termina o tráfego SSL/HTTP a partir de um aplicativo MDX. O MDX depois inicia novas conexões para conexões a conexões internas em nome do usuário. Essa configuração de política permite que o framework de MDX detecte e responda aos desafios de autenticação emitidos por servidores da web.

- b) Adicione os clientes Citrix Files ao XenMobile. Para obter detalhes, consulte [Integração e fornecimento de Citrix Files para clientes Endpoint Management](#).
- c) A partir de um dispositivo com suporte, verifique o logon único para o Citrix Files e conectores.

Nos exemplos a seguir, SharefileDev é o nome de um conector.





Filtrar a lista de conectores de zona de armazenamento

Você pode filtrar a lista de conectores de zona de armazenamento por tipo de Conector, grupos de entrega atribuídos e zona de armazenamento.

1. Vá até **Configurar > ShareFile** e clique em **Mostrar filtro**.

StorageZone Connectors Show filter

StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.

[Add](#) | [Manage StorageZones](#)

<input type="checkbox"/>	Connector Name	Type	StorageZone	Location	Delivery Groups
<input type="checkbox"/>	TestNS	NetworkFile	iosDev	\\Kylec-az-sz2\DevTestSZ	XM5-users
<input type="checkbox"/>	TestSP	Sharepoint	iosDev	http://sf-az-sp2013.sfazure.com:80	XM5-users.AllUsers

Showing 1 - 2 of 2 items

2. Expanda os títulos de filtro para fazer seleções. Para salvar um filtro, clique em **Salvar esta exibição**, digite o nome do filtro e clique em **Salvar**.

Filters Clear All

- ▼ **Type** Clear
 - NetworkFile 2
 - Sharepoint 1
- ▶ **Assigned Delivery Groups** Clear
- ▶ **StorageZone** Clear

StorageZone Connectors Hide filter

StorageZone Connectors provide access to documents and folders in SharePoint sites and network file shares.

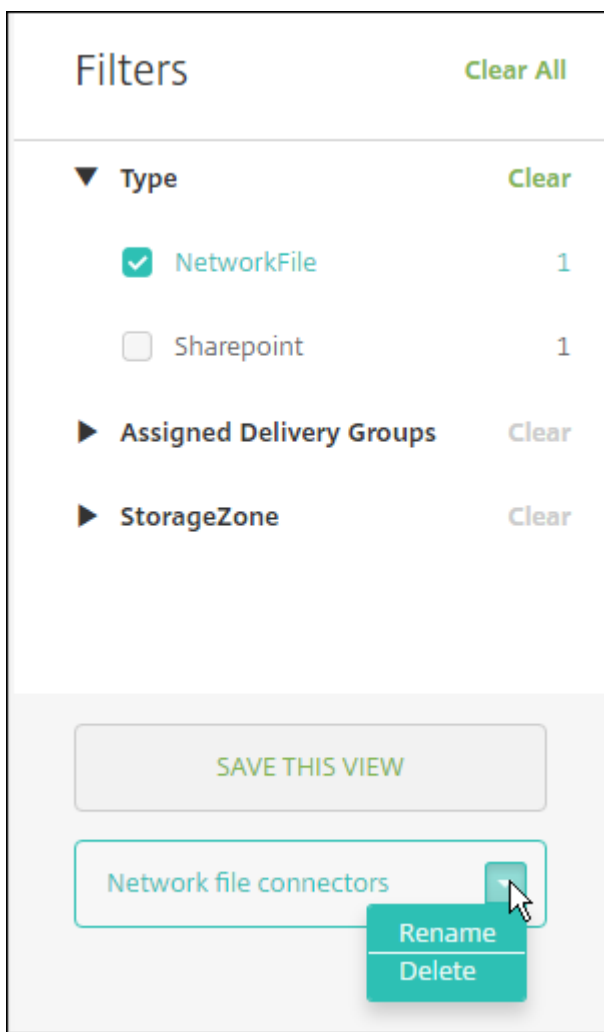
[Add](#) | [Manage StorageZones](#)

<input type="checkbox"/>	Connector Name	Type	StorageZone	Location	Delivery Groups
<input type="checkbox"/>	TestNS	NetworkFile	sz2	\\sz2\Storagezone	XM5-users
<input type="checkbox"/>	testxm	NetworkFile	sz1	\\sz1\Storagezone	XM5-users

Showing 1 - 2 of 2 items

[SAVE THIS VIEW](#)

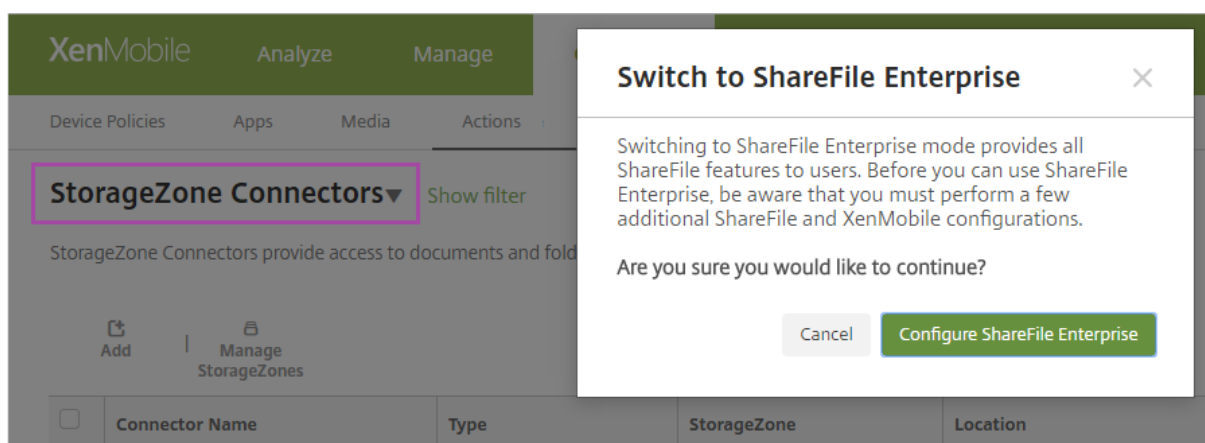
3. Para renomear ou excluir um filtro, clique no ícone de seta ao lado do nome do filtro.



Mudar para Citrix Files

Depois de integrar os conectores de zona de armazenamento ao XenMobile, você pode mudar posteriormente para o conjunto completo de recursos do Enterprise. O uso do conjunto de recursos do Citrix Files requer o XenMobile Enterprise Edition. O XenMobile mantém as configurações de integração existentes do conector de zona de armazenamento.

Vá até **Configurar > ShareFile**, clique no menu suspenso **StorageZone Connectors** e clique em **Configurar ShareFile Enterprise**.



Para obter informações sobre a configuração do Citrix Files, consulte [SAML para logon único com Citrix Files](#).

SmartAccess para aplicativos HDX

April 8, 2021

Esse recurso permite controlar o acesso a aplicativos HDX com base nas propriedades do dispositivo, nas propriedades do usuário de um dispositivo ou nos aplicativos instalados em um dispositivo. Use esse recurso definindo ações automatizadas para marcar o dispositivo como fora de conformidade, para negar acesso a esse dispositivo. Os aplicativos HDX usados com esse recurso são configurados nos aplicativos e áreas de trabalho virtuais usando uma política SmartAccess que nega acesso a dispositivos fora de conformidade. O XenMobile comunica o status do dispositivo ao StoreFront usando uma marca assinada e criptografada. Em seguida, o StoreFront permite ou nega o acesso com base na política de controle de acesso do aplicativo.

Para usar esse recurso, a implantação requer:

- Virtual Apps and Desktops 7.6
- StoreFront 3.7 ou 3.8
- XenMobile Server configurado para reunir aplicativos HDX a partir de um servidor StoreFront
- XenMobile Server configurado com um certificado SAML a ser usado para assinar e criptografar marcas. O mesmo certificado sem a chave privada é carregado no servidor StoreFront.

Para começar a usar este recurso:

- Configure o certificado do XenMobile Server para o repositório do StoreFront
- Configure pelo menos um grupo de entrega de aplicativos e áreas de trabalho virtuais com a política SmartAccess necessária
- Defina a ação automatizada no XenMobile

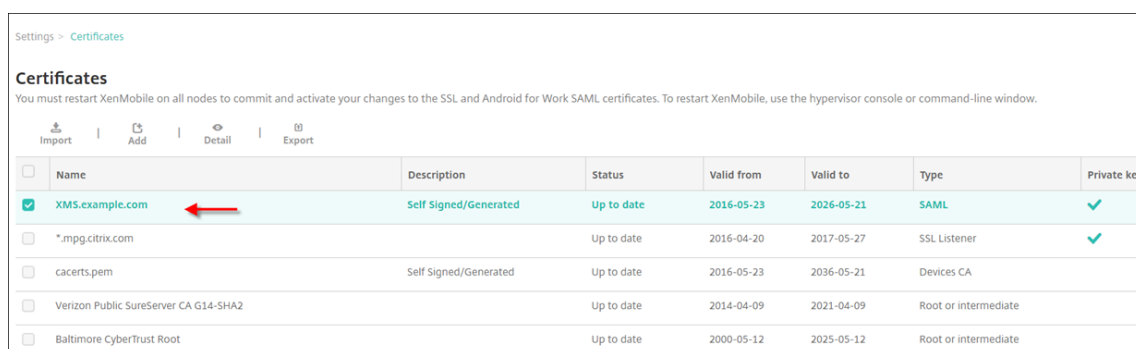
Exporte e configure o certificado do XenMobile Server e carregue-o no repositório do StoreFront

O SmartAccess usa marcas assinadas e criptografadas para se comunicar entre os servidores XenMobile e StoreFront. Para ativar essa comunicação, adicione o certificado do XenMobile Server ao repositório do StoreFront.

Para obter mais informações sobre como integrar o StoreFront e o XenMobile quando o XenMobile estiver ativado com autenticação baseada em domínio e em certificado, consulte o [Support Knowledge Center](#).

Exportar o certificado SAML do XenMobile Server

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida. Clique em **Certificados**.
2. Localize o certificado SAML do XenMobile Server.



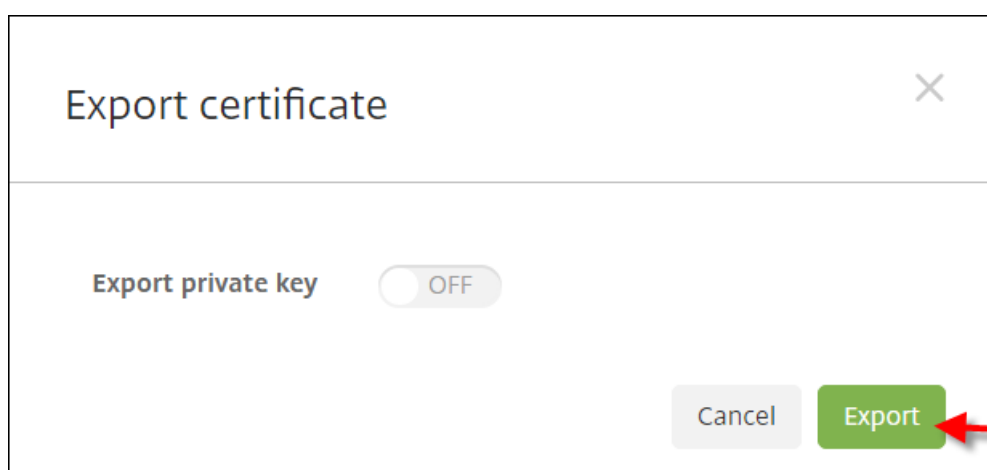
Settings > Certificates

Certificates
You must restart XenMobile on all nodes to commit and activate your changes to the SSL and Android for Work SAML certificates. To restart XenMobile, use the hypervisor console or command-line window.

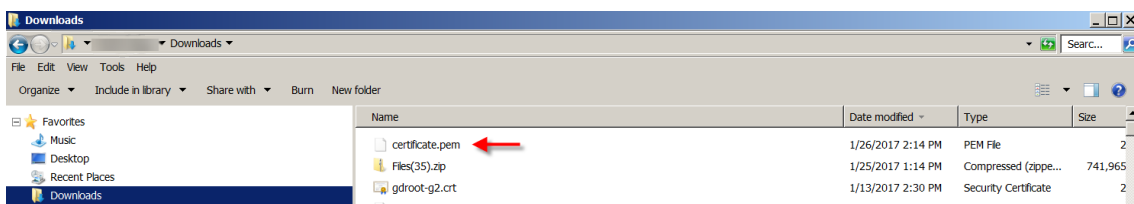
Import | Add | Detail | Export

<input type="checkbox"/>	Name	Description	Status	Valid from	Valid to	Type	Private key
<input checked="" type="checkbox"/>	XMS.example.com	Self Signed/Generated	Up to date	2016-05-23	2026-05-21	SAML	✓
<input type="checkbox"/>	*.mpg.citrix.com		Up to date	2016-04-20	2017-05-27	SSL Listener	✓
<input type="checkbox"/>	cacerts.pem	Self Signed/Generated	Up to date	2016-05-23	2036-05-21	Devices CA	
<input type="checkbox"/>	Verizon Public SureServer CA G14-SHA2		Up to date	2014-04-09	2021-04-09	Root or intermediate	
<input type="checkbox"/>	Baltimore CyberTrust Root		Up to date	2000-05-12	2025-05-12	Root or intermediate	

3. Verifique se a opção **Exportar chave privada** está definida como **O**. Clique em **Exportar** para exportar o certificado para o diretório de download.

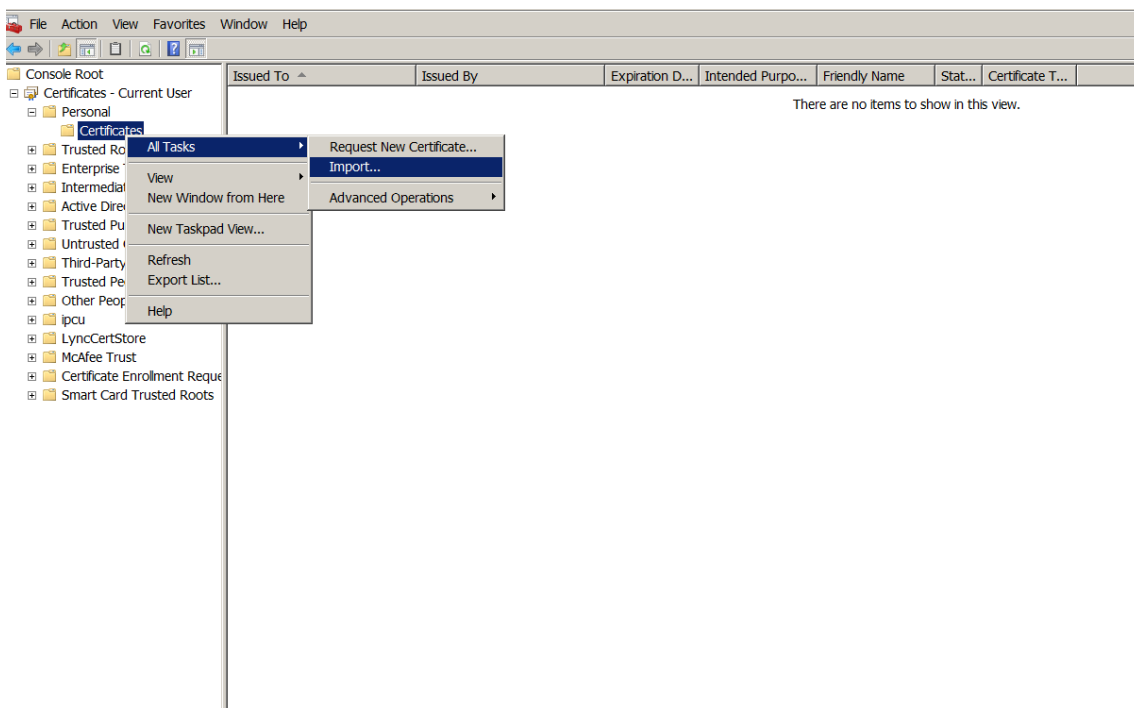


4. Localize o certificado no diretório de download. O certificado está no formato PEM.



Converter o certificado de PEM para CER

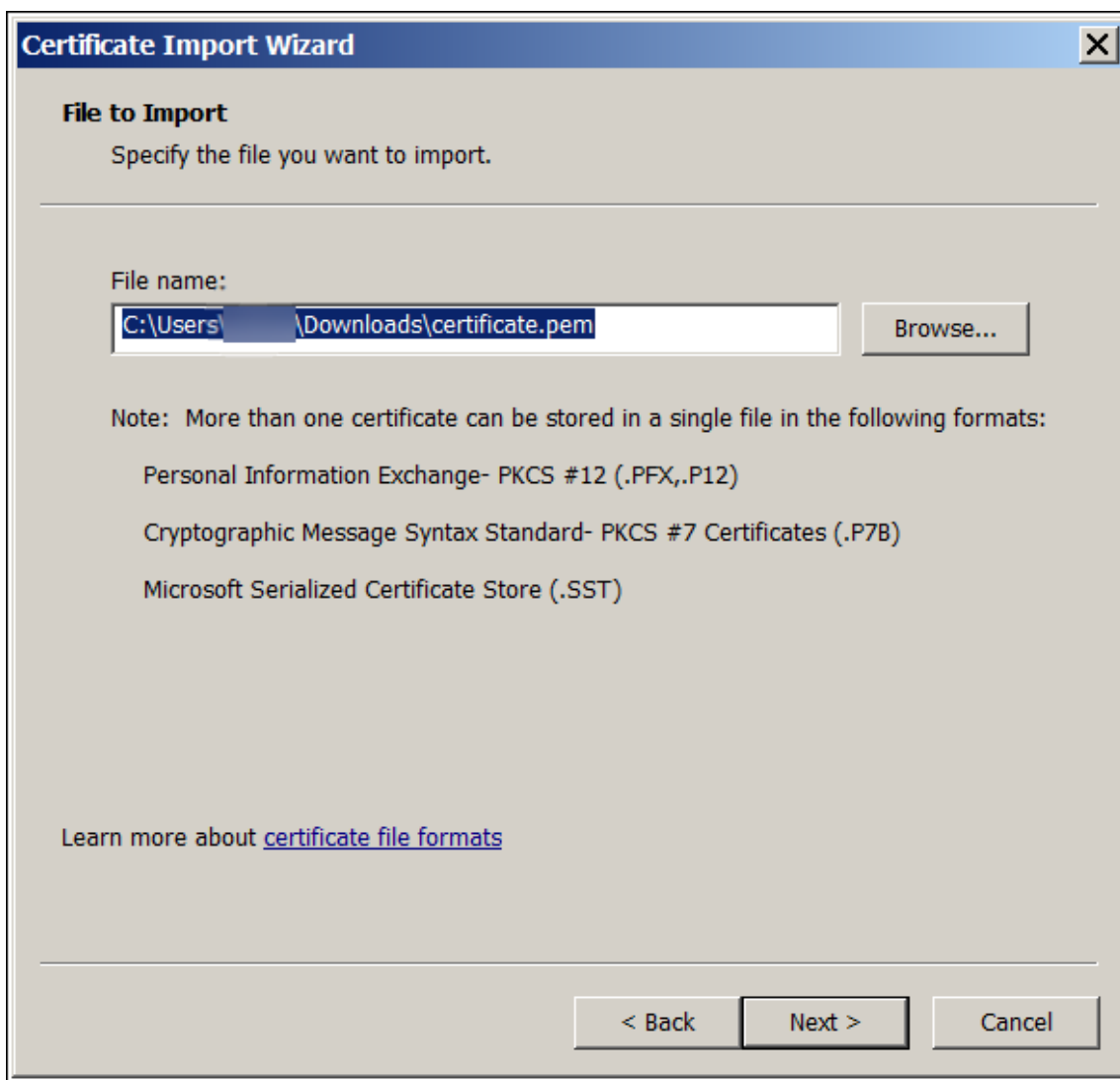
1. Abra o Console de Gerenciamento Microsoft (MMC) e clique com o botão direito do mouse em **Certificados > Todas as tarefas > Importar**.



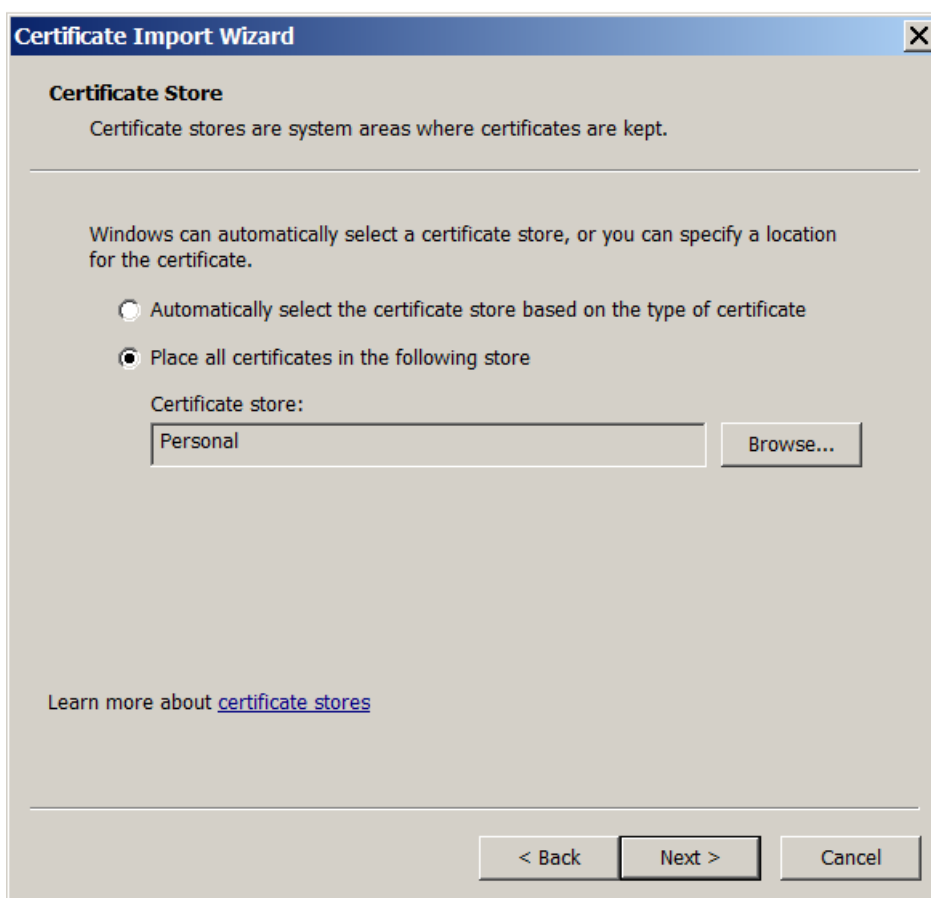
2. Quando o assistente de importação de certificado for exibido, clique em **Avançar**.



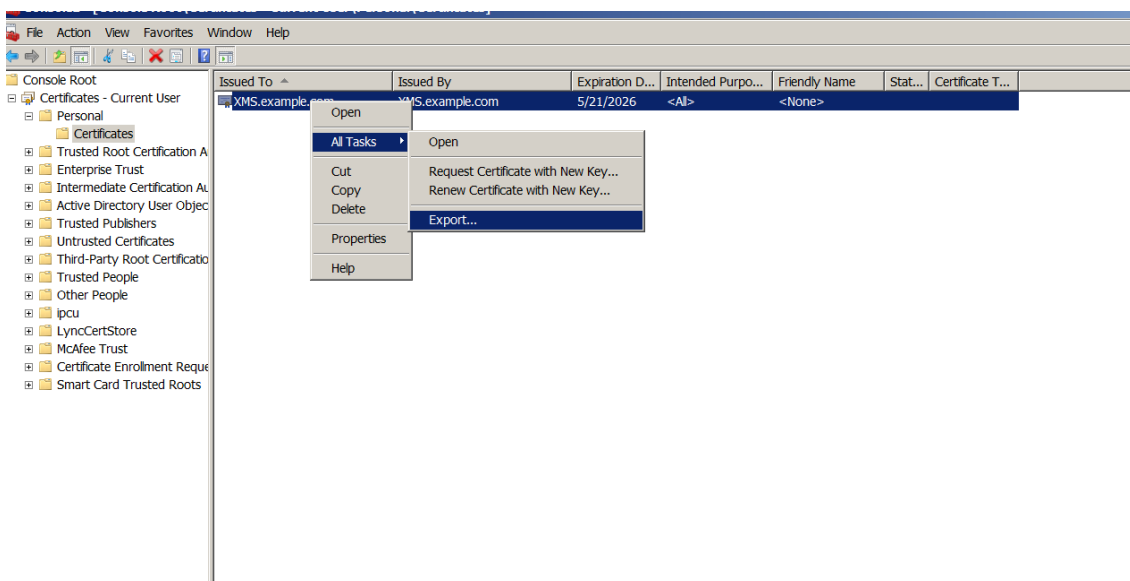
3. Navegue até o certificado no diretório de download.



4. Selecione **Colocar todos os certificados no repositório a seguir** e selecione **Pessoal** como o repositório de certificados. Clique em **Avançar**.



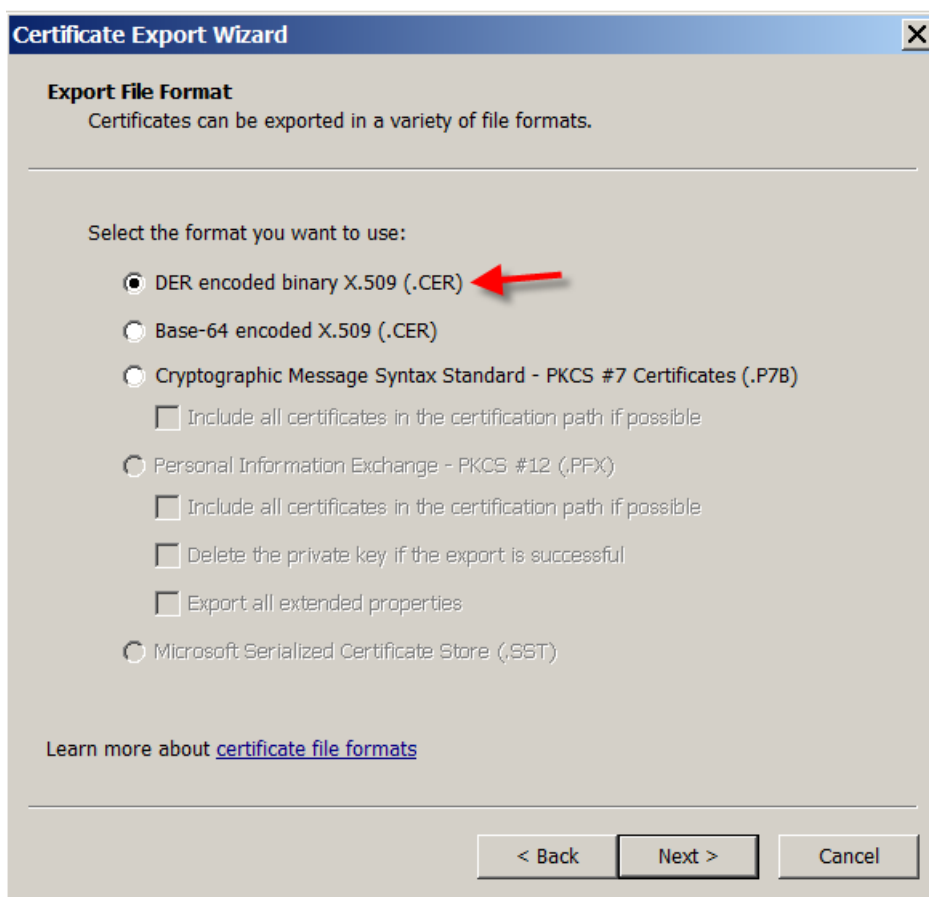
5. Revise suas seleções e clique em **Concluir**. Clique em **OK** na janela de confirmação.
6. No MMC, clique com o botão direito do mouse no certificado e escolha **Todas as tarefas > Exportar**.



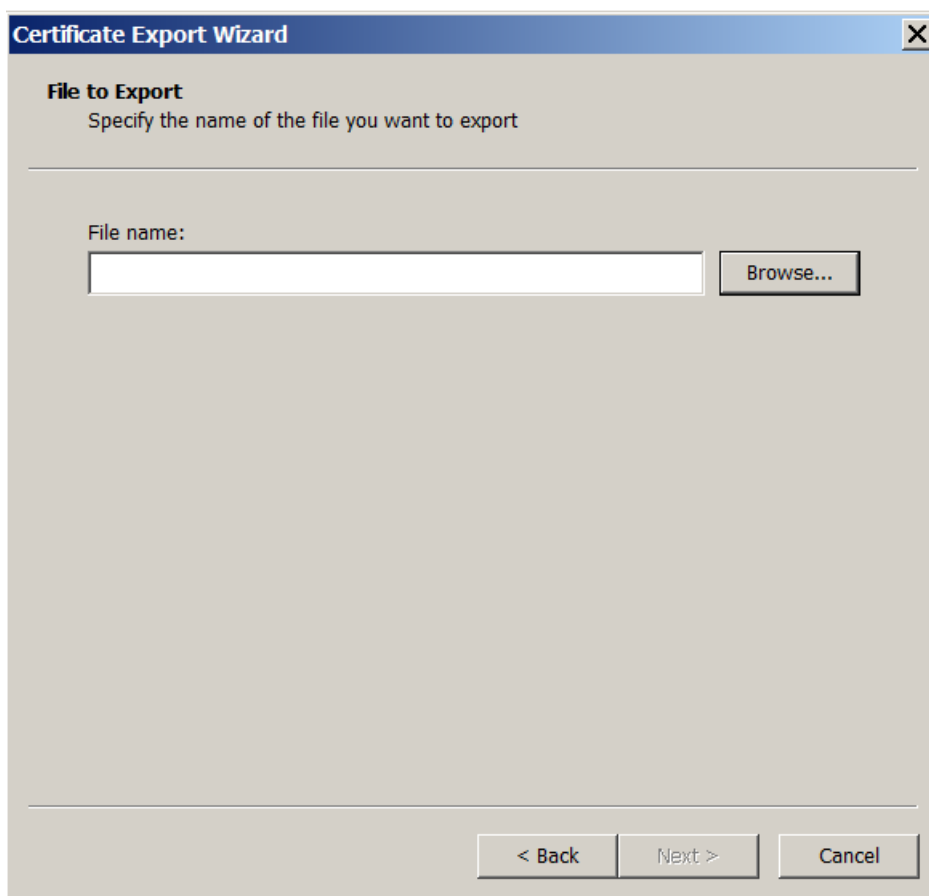
7. Quando o assistente de exportação de certificado for exibido, clique em **Avançar**.



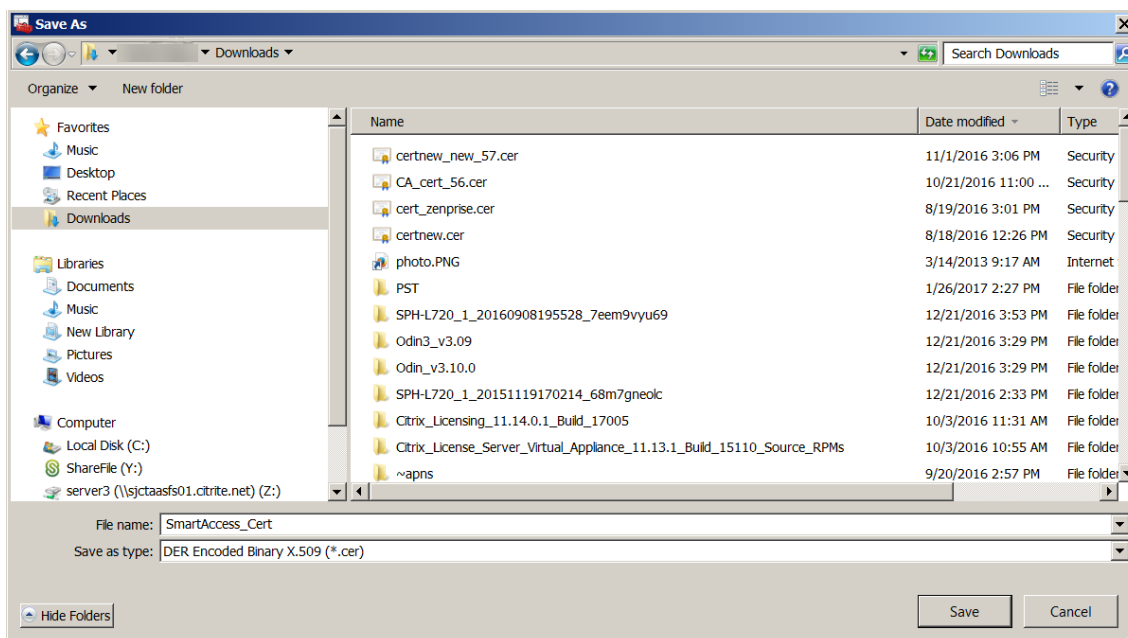
8. Escolha o formato **x.509 binário codificado por DER (.CER)**. Clique em **Avançar**.



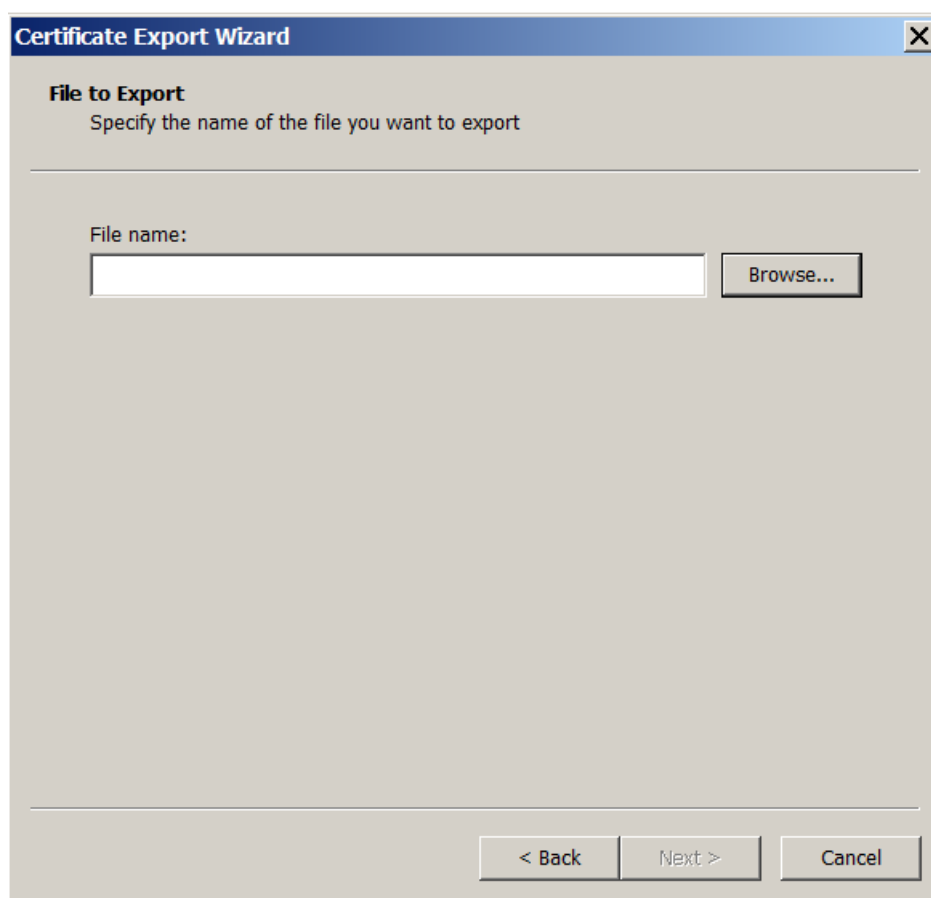
9. Procure o certificado. Digite um nome para o certificado e clique em **Avançar**.



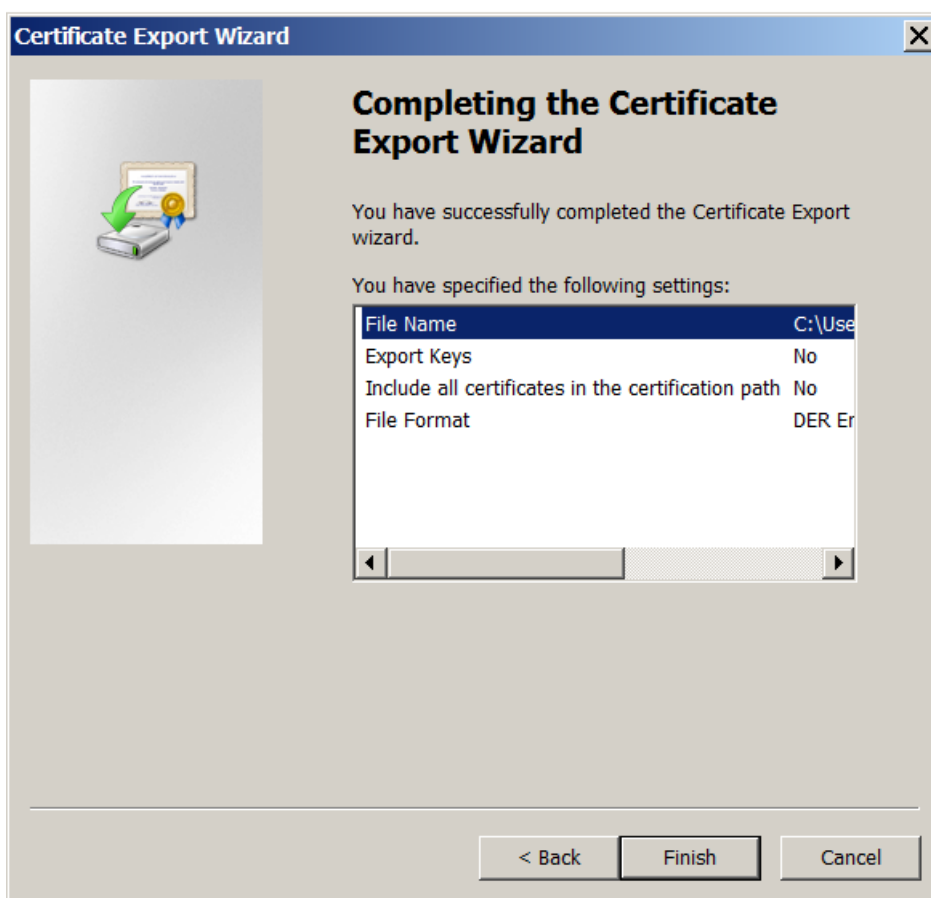
10. Salve o certificado.



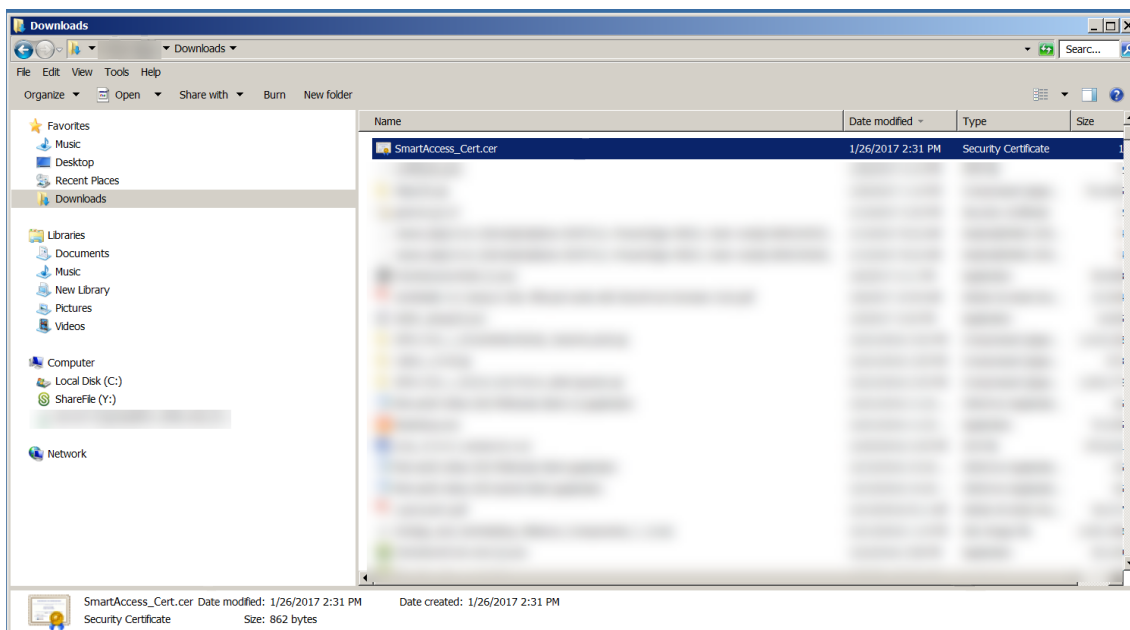
11. Procure o certificado e clique em **Avançar**.



12. Revise suas seleções e clique em **Concluir**. Clique em **OK** na janela de confirmação.

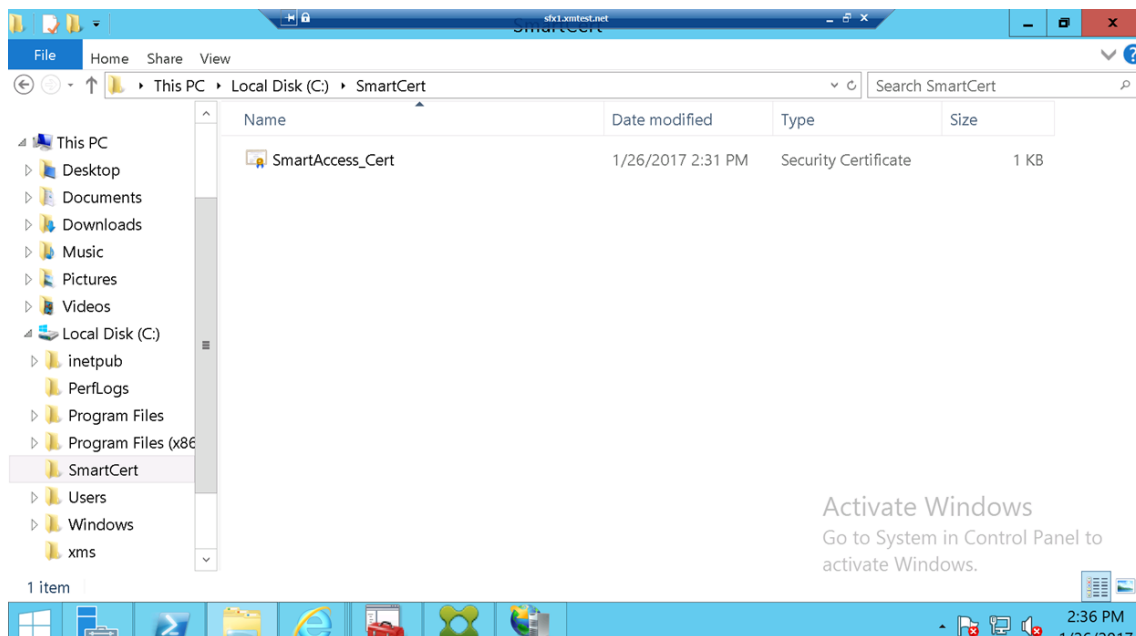


13. Localize o certificado no diretório de download. Observe que o certificado está no formato CER.



Copie o certificado para o Servidor StoreFront

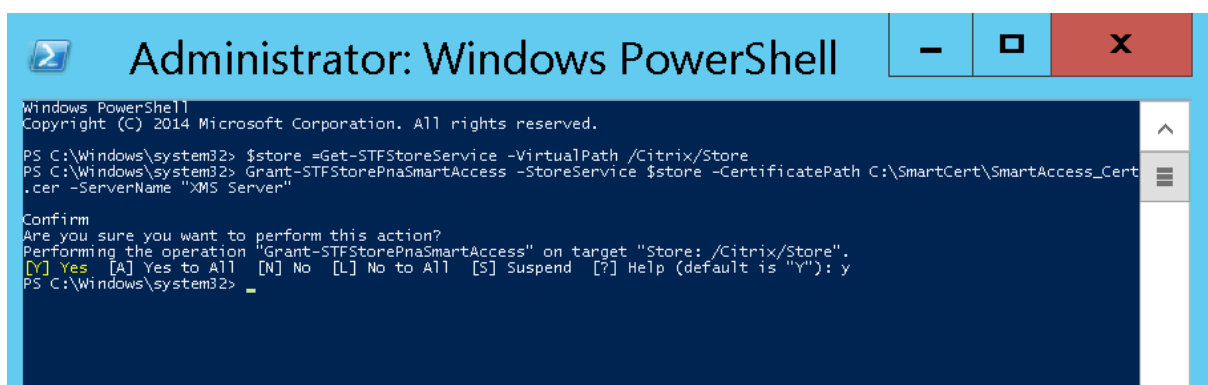
1. No servidor StoreFront, crie uma pasta chamada **SmartCert**.
2. Copie o certificado para a pasta **SmartCert**.



Configure o certificado no repositório do StoreFront

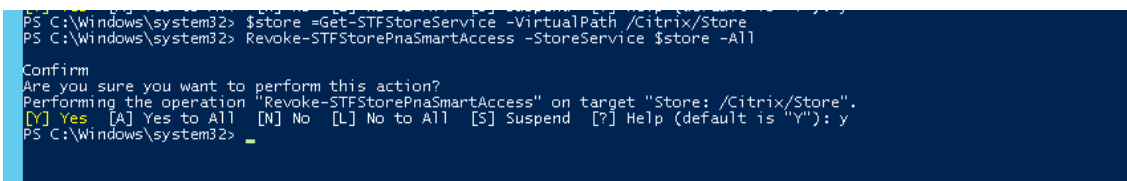
No servidor StoreFront, execute este comando do PowerShell para configurar o certificado do XenMobile Server convertido no repositório:

```
1 Grant-STFStorePnaSmartAccess - StoreService $store -  
CertificatePath "C:\xms\xms.cer" - ServerName "XMS server"  
2 <!--NeedCopy-->
```



Se houver algum certificado existente no repositório StoreFront, execute este comando do PowerShell para revogá-lo:

```
1 Revoke-STFStorePnaSmartAccess - StoreService $store - All
2 <!--NeedCopy-->
```



```
PS C:\Windows\system32> $store = Get-STFStoreService -VirtualPath /Citrix/Store
PS C:\Windows\system32> Revoke-STFStorePnaSmartAccess -StoreService $store -All
Confirm
Are you sure you want to perform this action?
Performing the operation "Revoke-STFStorePnaSmartAccess" on target "Store: /Citrix/Store".
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): y
PS C:\Windows\system32> _
```

Como alternativa, você pode executar qualquer um desses comandos do PowerShell no servidor StoreFront para revogar certificados existentes no repositório do StoreFront:

- Revogar por nome:

```
1 $store = Get-STFStoreService - VirtualPath /Citrix/Store
2
3 Revoke-STFStorePnaSmartAccess - StoreService $store - ServerName "
  My XM Server"
4 <!--NeedCopy-->
```

- Revogar por impressão digital:

```
1 $store = Get-STFStoreService - VirtualPath /Citrix/Store
2
3 Revoke-STFStorePnaSmartAccess - StoreService $store -
  CertificateThumbprint "ReplaceWithThumbprint"
4 <!--NeedCopy-->
```

- Revogar por objeto de servidor:

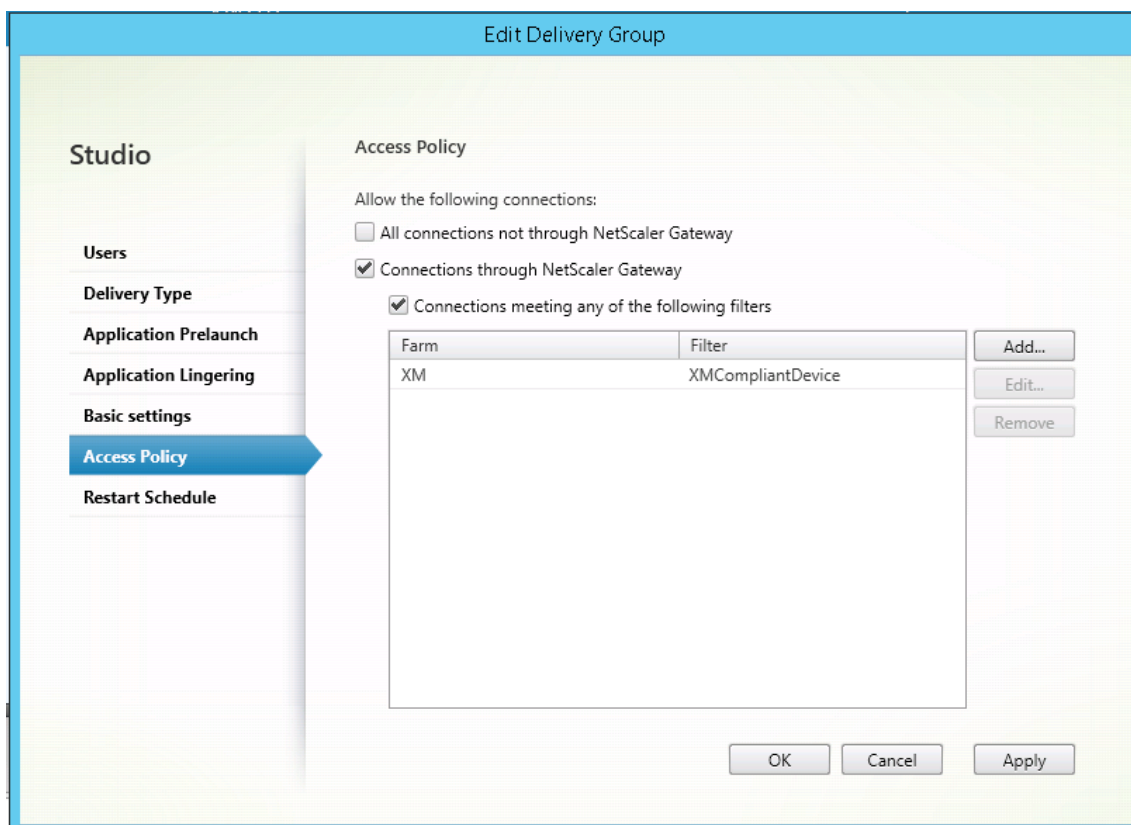
```
1 $store = Get-STFStoreService - VirtualPath /Citrix/Store
2
3 $access = Get-STFStorePnaSmartAccess - StoreService $store
4
5 Revoke-STFStorePnaSmartAccess - StoreService $store - SmartAccess
  $access.AccessConditionsTrusts[0]
6 <!--NeedCopy-->
```

Configure a política SmartAccess para os aplicativos e áreas de trabalho virtuais

Para adicionar a política SmartAccess necessária ao grupo de entrega que fornecer o aplicativo HDX:

1. No servidor de aplicativos e áreas de trabalho virtuais, abra o Citrix Studio.
2. Selecione **Delivery Groups** no painel de navegação do Studio.

3. Selecione um grupo de entrega para o aplicativo ou os aplicativos aos quais você deseja controlar o acesso. Em seguida, selecione **Editar grupo de entrega** no painel **Ações**.
4. Na página **Política de acesso**, selecione **Conexões por meio do NetScaler Gateway** e **Conexão que atende a qualquer um dos seguintes**.
5. Clique em **Adicionar**.
6. Adicione uma política de acesso em que **Farm** seja **XM** e **Filtro** seja **XMCompliantDevice**.



7. Clique em **Aplicar** para aplicar as alterações feitas e deixar a janela aberta ou clique em **OK** para aplicar as alterações e fechar a janela.

Definir ações automatizadas no XenMobile

A política SmartAccess que você define no grupo de entrega de um aplicativo HDX nega o acesso a um dispositivo quando esse dispositivo está fora de conformidade. Use ações automatizadas para marcar o dispositivo como fora de conformidade.

Status	Mode	User name	Device platform	Operating system version	Device model	Last access	Inactivity days	Out of Compliance
<input type="checkbox"/>	MDM MAM	[Redacted]	iOS	8.1	iPad	06/29/2016 10:37:56 am	212 days	
<input type="checkbox"/>	MDM MAM	[Redacted]	iOS	10.2	iPhone	01/27/2017 10:10:59 am	0 day	True

1. No console XenMobile, clique em **Configurar > Ações**. A página **Ações** é exibida.
2. Clique em **Adicionar** para adicionar uma ação. A página **Informações sobre a ação** é exibida.
3. Na página **Informações sobre a ação**, digite um nome e uma descrição para a ação.
4. Clique em **Avançar**. A página **Detalhes da ação** é exibida. No exemplo a seguir, é criado um gatilho que marca imediatamente os dispositivos como fora de conformidade quando eles têm o nome de propriedade do usuário **eng5** ou **eng6**.

Action details

Choose a trigger event and the associated action for that event.

Trigger*

User property

Name

Is

eng5 eng6

Action*

Mark the device as out of compliance

Is

True

0

Hours

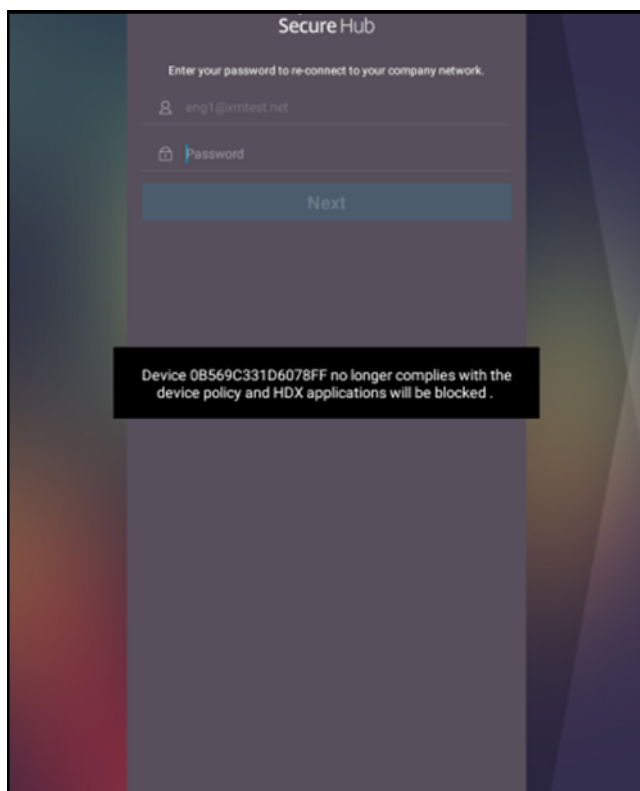
5. Na lista **Gatilho**, escolha **Propriedade do dispositivo**, **Propriedade do usuário** ou **Nome do aplicativo instalado**. O SmartAccess não dá suporte a gatilhos de evento.
6. Na lista **Ação**:
 - Escolha **Marcar o dispositivo como fora de conformidade**.
 - Escolha **Is**.
 - Escolha **True**.
 - Para definir a ação de marcar o dispositivo como fora de conformidade imediatamente quando a condição de gatilho for atendida, defina o período de tempo como **0**.
7. Escolha o grupo ou os grupos de entrega do XenMobile aos quais aplicar essa ação.

8. Reveja o resumo da ação.
9. Clique em **Avançar** e em **Salvar**.

Quando o dispositivo está marcado como fora de conformidade, os aplicativos HDX deixam de ser exibidos no repositório do Secure Hub. O usuário deixa de estar inscrito aos aplicativos. Nenhuma notificação é enviada ao dispositivo e nada no repositório do Secure Hub indica que os aplicativos HDX estavam disponíveis anteriormente.

Se quiser que os usuários sejam notificados quando um dispositivo estiver marcado como fora de conformidade, crie uma notificação e, em seguida, crie uma ação automatizada para enviar essa notificação.

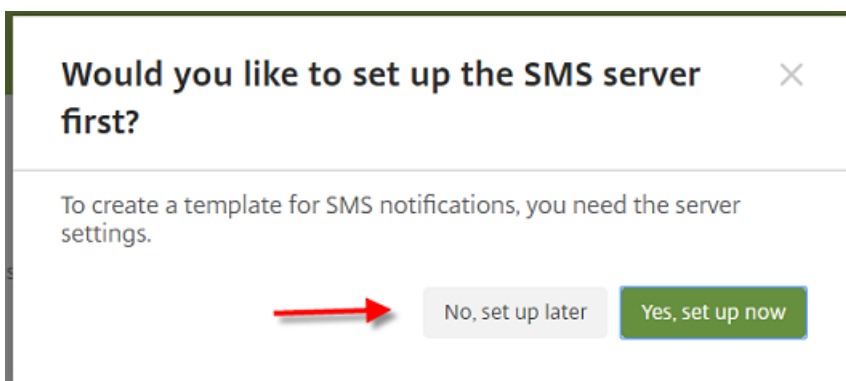
Esse exemplo cria e envia essa notificação quando um dispositivo está marcado como fora de conformidade: “O número de série do dispositivo ou o número de telefone não está mais em conformidade com a política do dispositivo, e os aplicativos HDX serão bloqueados”.



Criar a notificação que os usuários veem quando um dispositivo está marcado como fora de conformidade

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Settings** é exibida.
2. Clique em **Modelos de notificação**. A página **Modelos de notificação** é exibida.

3. Clique em **Adicionar** para acrescentar à página **Modelos de notificação**.
4. Quando solicitado a configurar primeiro o servidor SMS, clique em **Não, configurar mais tarde**.



5. Defina estas configurações:
 - **Nome:** bloqueio de aplicativos HDX
 - **Descrição:** notificação do agente quando o dispositivo está fora de conformidade
 - **Tipo:** notificação Ad Hoc
 - **Secure Hub:** ativado
 - **Mensagem:** o dispositivo `${firstnotnull(device.TEL_NUMBER,device.serialNumber)}` não está mais em conformidade com a política de dispositivo, e os aplicativos HDX serão bloqueados.

The screenshot shows a configuration form for creating an action. The fields are as follows:

- Name***: HDX Application Block
- Description**: (Empty text area)
- Type**: Ad-Hoc Notification (dropdown menu)
Manual sending supported
- SMTP**: Activate (button)
- Sender**: (Empty text field)
- Recipient**: (Empty text field)
- Subject**: (Empty text field)
- Message**: (Empty text area)
- Secure Hub**: Activated (button), Deactivate (button)
- Message***: Device S{firstnotnull(device.TEL_NUMBER,device.serialNumber)} no longer complies with the device policy and HDX applications will be blocked .

6. Clique em **Salvar**.

Crie a ação que envia a notificação quando um dispositivo está marcado como fora de conformidade

1. No console XenMobile, clique em **Configurar > Ações**. A página **Ações** é exibida.
2. Clique em **Adicionar** para adicionar uma ação. A página **Informações sobre a ação** é exibida.
3. Na página **Informações sobre a ação**, insira um nome e uma descrição para a ação:
 - **Nome**: notificação de HDX bloqueado

- **Descrição:** notificação de HDX bloqueado porque o dispositivo está fora de conformidade
4. Clique em **Avançar**. A página **Detalhes da ação** é exibida.
 5. Na lista **Gatilho**:
 - Escolha **Propriedade do dispositivo**.
 - Escolha **Fora de conformidade**.
 - Escolha **Is**.
 - Escolha **True**.

The screenshot shows the 'Actions' configuration page in the XenMobile console. The 'Trigger' section is expanded, showing four dropdown menus: 'Device property', 'Out of compliance', 'Is', and 'True'. The 'Action' section is also expanded, showing five dropdown menus: 'Send notification', 'HDX Application Block', 'Minutes', and 'Days', along with a text input field for 'Preview notification message' containing the value '0'. A 'Next >' button is visible at the bottom right of the form.

6. Na lista **Ação**, especifique as ações que ocorrem quando o gatilho é atendido:
 - Escolha **Enviar notificação**
 - Escolha **Bloco de aplicativos HDX, a notificação que você criou**.
 - Escolha **0**. Definir esse valor como 0 faz com que a notificação seja enviada assim que a condição do gatilho é atendida.
7. Selecione o grupo ou os grupos de entrega do XenMobile aos quais aplicar essa ação. Neste exemplo, escolha **AllUsers**.
8. Reveja o resumo da ação.
9. Clique em **Avançar** e em **Salvar**.

Para obter mais informações sobre como definir ações automatizadas, consulte [Ações automatizadas](#).

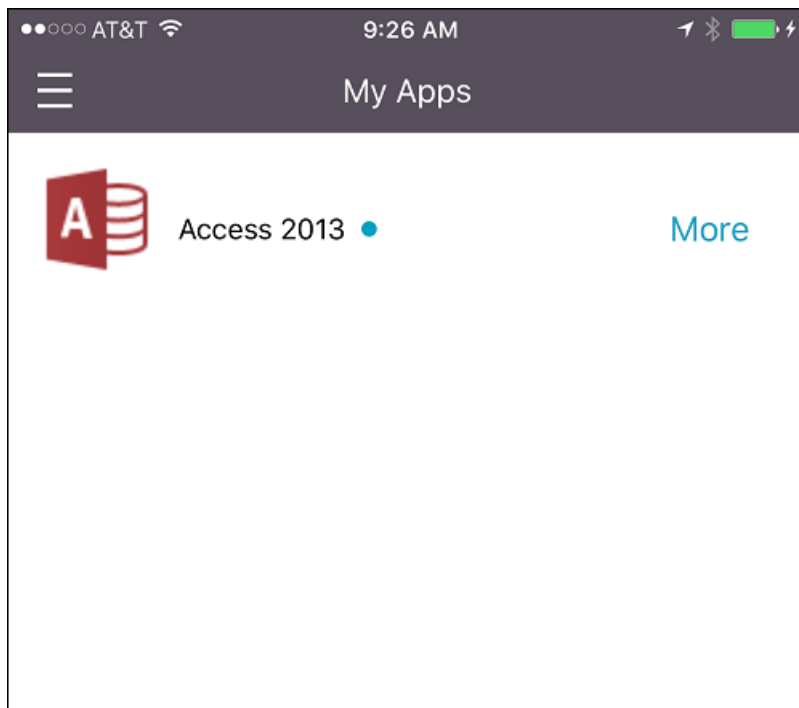
Como os usuários recuperam o acesso a aplicativos HDX

Os usuários podem acessar aplicativos HDX novamente depois que o dispositivo é recolocado em conformidade:

1. No dispositivo, vá até a loja do Secure Hub para atualizar os aplicativos na loja.

2. Vá até o aplicativo e toque em **Adicionar** ao aplicativo.

Depois que o aplicativo for adicionado, ele aparecerá em Meus aplicativos com um ponto azul ao lado, pois é um aplicativo recém-instalado.



Adicionar mídia

December 10, 2020

Você adiciona mídia ao XenMobile para poder implantar a mídia em dispositivos de usuário. Você pode usar o XenMobile para implantar o Apple Books que você obtém por meio da compra por volume da Apple.

Depois de configurar uma conta de compra por volume no XenMobile, seus livros comprados e gratuitos aparecem em **Configurar > Mídia**. Nas páginas de **Mídia**, você configura livros para implantação em dispositivos iOS escolhendo grupos de entrega e especificando regras de implantação.

A primeira vez que um usuário recebe um livro e aceita a licença de compra por volume, os livros implantados são instalados no dispositivo. Os livros aparecem no aplicativo Apple Book. Você não pode desassociar a licença do livro do usuário ou remover o livro do dispositivo. O XenMobile instala livros como mídia necessária. Se um usuário exclui um livro instalado do seu dispositivo, o livro permanece no aplicativo Apple Book, pronto para download.

Pré-requisitos

- Dispositivos iOS
- Configure a compra por volume da Apple no XenMobile, conforme descrito em [Compra por volume da Apple](#).

Configurar livros

Os Apple Books obtidos por meio da compra por volume aparecem na página **Configurar > Mídia**.

The screenshot shows the 'Media' configuration page in XenMobile. It features a navigation bar with tabs for 'Device Policies', 'Apps', 'Media', 'Actions', 'ShareFile', 'Enrollment Profiles', and 'Delivery Groups'. The 'Media' tab is active. Below the navigation bar, there is a search bar and a 'Show filter' link. The main content is a table with the following columns: 'Icon', 'Media Name', 'Type', 'Created On', 'Last Updated', and 'Vpp Account'. The table lists six books, all of which are 'Apple iBooks' and purchased from a 'test' VPP account. At the bottom of the table, it indicates 'Showing 1 - 6 of 6 items' and 'Items per page: 10'.

Icon	Media Name	Type	Created On	Last Updated	Vpp Account
	The Wonderful Wizard of Oz - VPP	Apple iBooks	6/15/17 1:28 PM	6/15/17 1:41 PM	test
	Cool Werewolf Jokes For Kids - VPP	Apple iBooks	6/15/17 1:28 PM	6/15/17 1:28 PM	test
	Science Fiction Stories - VPP	Apple iBooks	6/15/17 1:28 PM	6/15/17 1:32 PM	test
	Coming Out - VPP	Apple iBooks	6/15/17 1:29 PM	6/20/17 10:45 AM	test
	Short Stories - VPP	Apple iBooks	6/15/17 1:29 PM	6/15/17 1:29 PM	test
	A Diamond in My Pocket - VPP	Apple iBooks	6/15/17 1:29 PM	6/20/17 10:39 AM	test

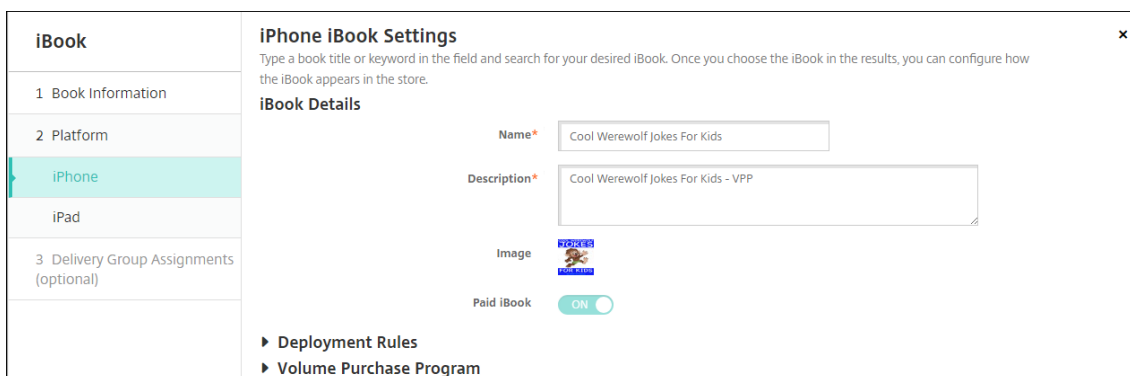
Para configurar um Apple Book para implantação

1. Em **Configurar > Mídia**, selecione um livro e clique em **Editar**. A página **Informações do livro** é exibida.

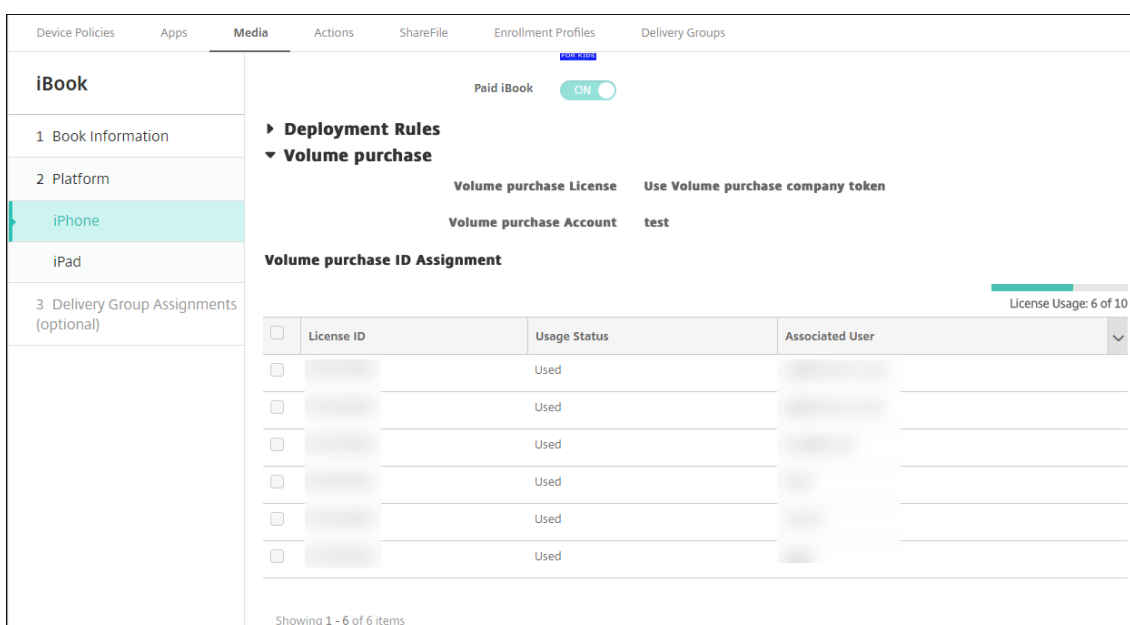
The screenshot shows the 'Book Information' configuration page for an iBook. On the left, there is a sidebar with a list of configuration steps: '1 Book Information' (highlighted), '2 Platform', 'iPhone', 'iPad', and '3 Delivery Group Assignments (optional)'. The main area is titled 'Book Information' and contains two input fields: 'Name' and 'Description'. Both fields are filled with the text 'Cool Werewolf Jokes For Kids - VPP'. There are small circular icons with an 'i' next to each field, likely for information or help.

O **Nome** e **Descrição** são exibidos somente no console XenMobile e logs.

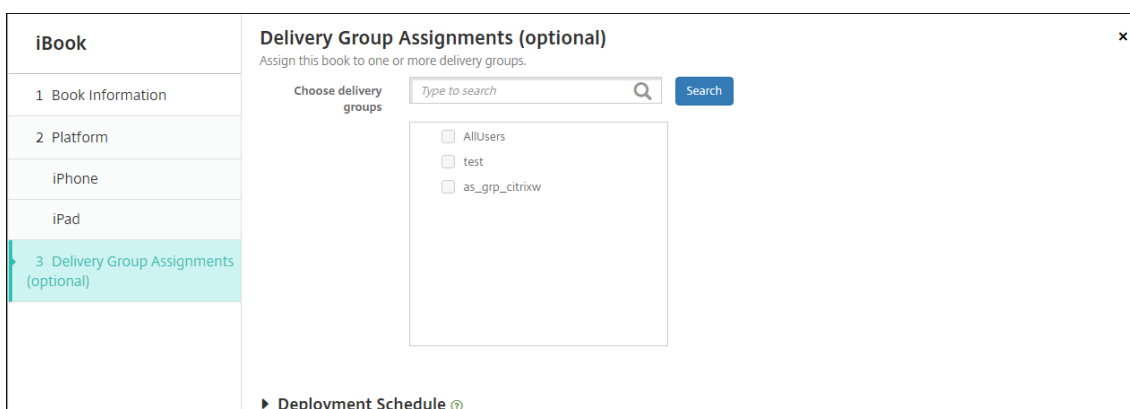
2. Nas páginas de **Configurações iPhone iBook** e **Configurações iPad iBook**: ainda que possa opcionalmente alterar o nome e a descrição do livro, a Citrix recomenda que você não altere essas configurações. A imagem é para sua informação e não é editável. **iBook pago** indica que um livro é adquirido através da compra por volume da Apple.



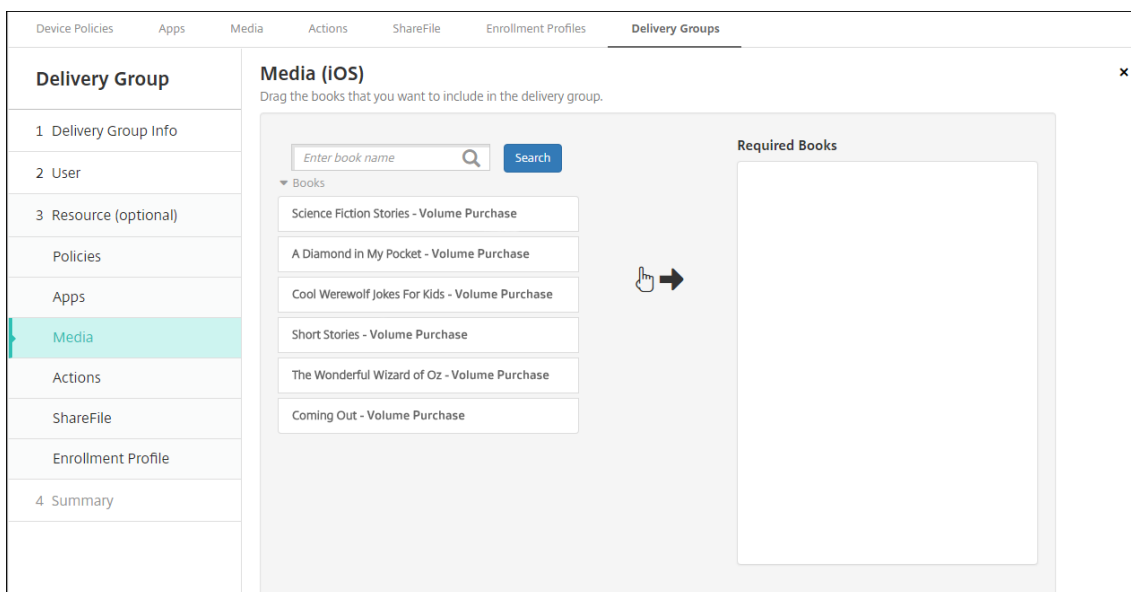
Você também pode especificar regras de implantação ou visualizar informações de compra por volume.



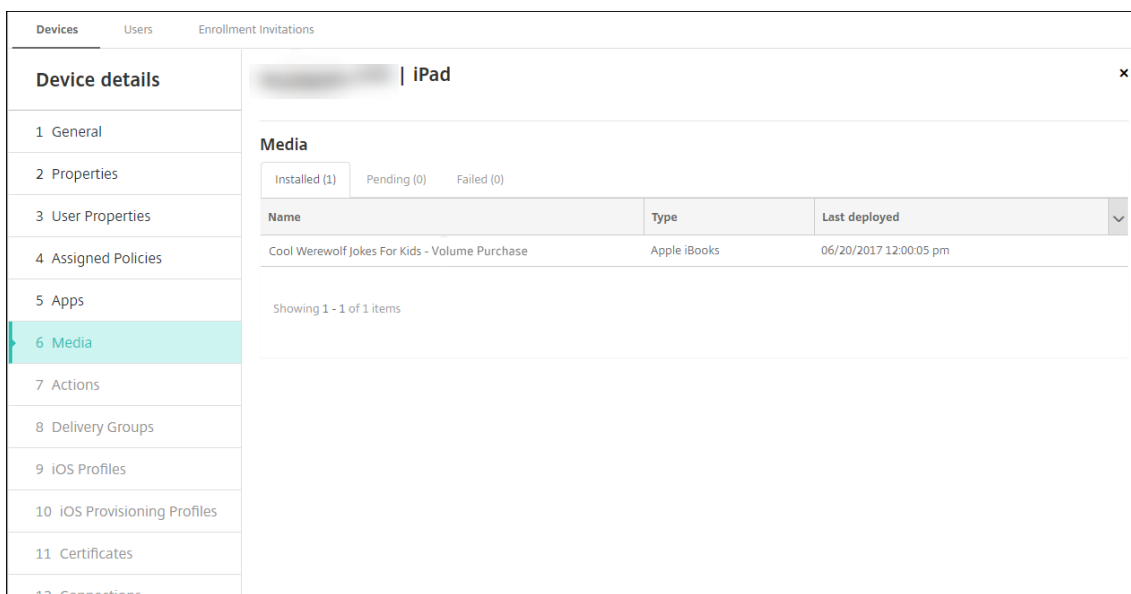
3. Opcionalmente, atribua o livro aos grupos de entrega e defina um cronograma de implantação.



Você também pode atribuir livros a grupos de entrega na guia **Mídia** em **Configurar > Grupos de entrega**. O XenMobile suporta apenas a implantação de livro necessária.



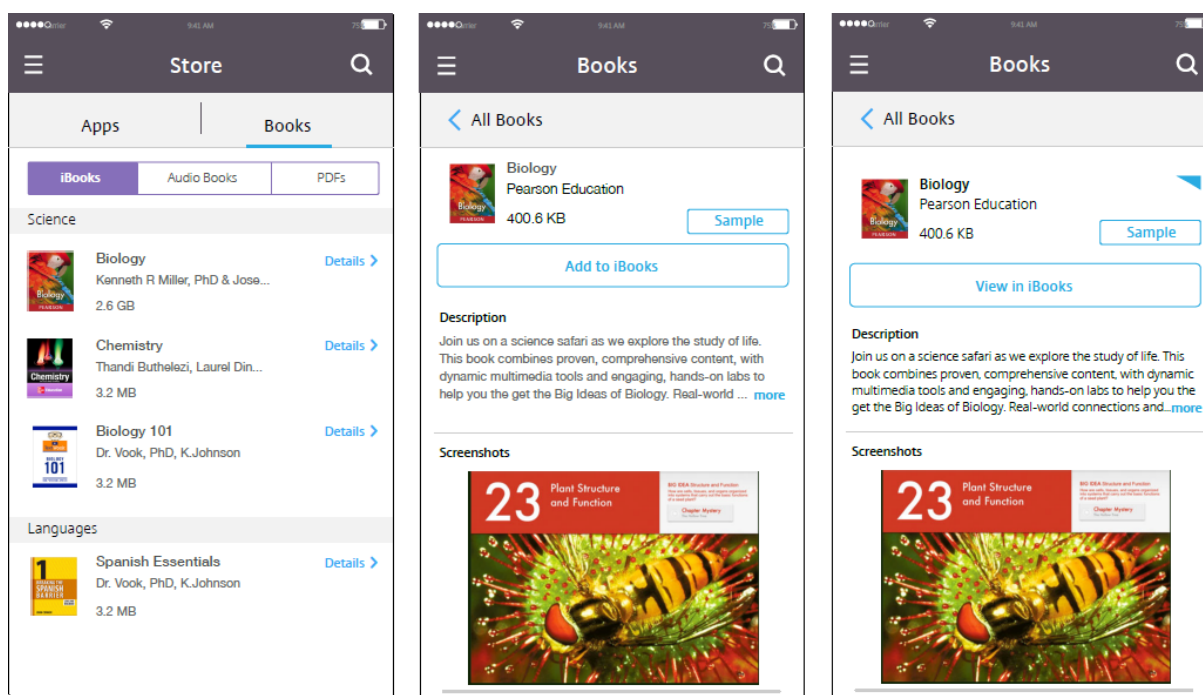
4. Use a guia **Mídia** em **Gerenciar > Dispositivos** para visualizar o status da implantação.



Nota:

Na página **Configurar > Mídia**, se você selecionar um livro e clicar em **Excluir**, o XenMobile remove o livro da lista. No entanto, na próxima vez que o XenMobile se sincronizar com a compra por volume da Apple, o livro reaparecerá na lista, a menos que tenha sido removido da compra por volume da Apple. A exclusão de um livro da lista não remove o livro dos dispositivos.

Os livros aparecem nos dispositivos do usuário, conforme mostrado no exemplo a seguir.



Implantar recursos

April 26, 2021

A configuração e o gerenciamento do dispositivo geralmente envolvem a criação de recursos (políticas, aplicativos e mídias) e ações no console XenMobile e, em seguida, o empacotamento deles usando grupos de entrega. A ordem na qual o XenMobile envia recursos e ações para os dispositivos em um grupo de entrega é chamada de ordem de implantação. Este artigo descreve como:

- Adicionar, gerenciar e implantar grupos de entrega
- Alterar a ordem de implantação de recursos e ações em grupos de entrega
- O XenMobile determina a ordem de implantação quando um usuário está em vários grupos de entrega que têm políticas duplicadas ou conflitantes.

Os grupos de entrega especificam a categoria dos usuários em cujos dispositivos você implanta combinações de políticas, aplicativos, mídias e ações. A inclusão de um grupo de entrega é normalmente baseada nas características dos usuários, como empresa, país, departamento, endereço do escritório, cargo etc. Os grupos de entrega fornecem um maior controle sobre quem recebe quais recursos e quando isso ocorre. Você pode implantar um grupo de entrega para todos ou para um grupo de usuários definido de forma mais restrita.

Implantar em um grupo de entrega significa enviar uma notificação por push a todos os usuários com dispositivos iOS e Windows compatíveis. Esses usuários devem pertencer ao grupo de entrega para

reconectarem-se ao XenMobile. Você pode reavaliar os dispositivos e implantar políticas, aplicativos, mídias e ações que fazem parte de um grupo de entrega.

Para usuários com dispositivos Android: se eles já estiverem conectados, receberão os recursos imediatamente. Caso contrário, com base em suas políticas de agendamento, eles receberão recursos da próxima vez em que se conectarem.

O grupo de entrega padrão AllUsers é criado quando você instala e configura o XenMobile. Ele contém todos os usuários locais e os usuários do Active Directory. Você não pode excluir o grupo AllUsers, mas pode desativá-lo quando não desejar enviar recursos por push para todos os usuários.

Ordem de implantação

Ordem de implantação é a sequência na qual o XenMobile envia recursos para os dispositivos. A ordem de implantação se aplica somente a dispositivos em um grupo de entrega com um perfil de registro configurado para gerenciamento de dispositivo (MDM).

Quando você determina a ordem de implantação, o XenMobile aplica filtros e critérios de controle, como as regras de implantação e o cronograma de implantação, aos recursos. Os recursos incluem políticas, aplicativos, ações e grupos de entrega. Antes de adicionar grupos de entrega, considere como as informações nesta seção se relacionam às suas metas de implantação.

Este é um resumo dos principais conceitos relacionados à ordem de implantação:

- **Ordem de implantação:** a sequência na qual o XenMobile envia recursos (políticas, aplicativos e mídias) e ações para um dispositivo. A ordem de implantação de algumas políticas, como Termos e Condições e Inventário de Software, não afeta outros recursos. A ordem na qual as ações são implantadas não afeta outros recursos, portanto, a respectiva posição é ignorada quando o XenMobile implanta os recursos.
- **Regras de implantação:** o XenMobile usa as regras de implantação que você especifica para as propriedades de dispositivo para filtrar as políticas, os aplicativos, as mídias, as ações e os grupos de entrega. Por exemplo, uma regra de implantação pode especificar o envio por push do pacote de implantação quando um nome de domínio corresponde a um determinado valor.
- **Cronograma de implantação:** o XenMobile usa o cronograma de implantação que você especifica para as políticas, aplicativos, mídias e ações para controlar a implantação desses itens. Você pode especificar que uma implantação ocorra imediatamente, em uma determinada data e hora ou de acordo com as condições de implantação.

A tabela a seguir mostra os critérios de filtro e controle para os vários tipos de objetos e recursos. As regras de implantação são baseadas nas propriedades do dispositivo.

Objeto/recurso	Plataforma do dispositivo	Regra de implantação	Cronograma de implantação	Usuário/grupos
Política de dispositivo	S	S	S	-
Aplicativo	S	S	S	-
Mídia	S	S	S	-
Ação	-	S	S	-
Grupo de entrega	-	S	-	S

É muito provável que, em um ambiente típico, vários grupos de entrega sejam atribuído a um único usuário, com os seguintes resultados possíveis:

- Existem objetos duplicados nos grupos de entrega.
- Uma política específica está configurada de forma diferente em mais de um grupo de entrega que é atribuído a um usuário.

Quando uma dessas situações ocorre, o XenMobile calcula uma ordem de implantação para todos os objetos que ele deve entregar para um dispositivo ou executar. As etapas de cálculo são independentes da plataforma do dispositivo.

Etapas de cálculo

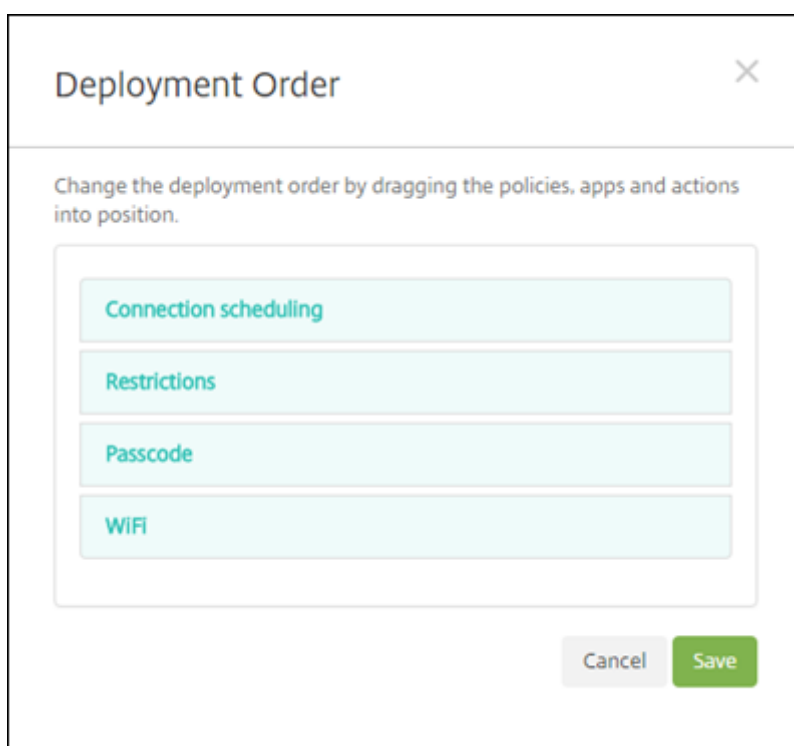
1. Determine todos os grupos de entrega de um usuário específico com base em filtros de usuários, grupos e regras de implantação.
2. Crie uma lista ordenada de todos os recursos (políticas, aplicativos, mídias e ações) dentro de grupos de entrega selecionados. A lista baseia-se nos filtros de plataforma de dispositivo, regras de implantação e agendamento de implantação. O algoritmo de ordenação é o seguinte:
 - a) Coloque os recursos dos grupos de entrega que têm uma ordem de implantação definida pelo usuário antes daqueles que não a têm. A lógica desse posicionamento é descrita após estas etapas.
 - b) Como fator decisivo entre grupos de entrega, ordene os recursos dos grupos de entrega por nome do grupo de entrega. Por exemplo, coloque os recursos do grupo de entrega A antes dos recursos do grupo de entrega B.
 - c) Durante a classificação, se uma ordem de implantação definida pelo usuário for especificada para os recursos de um grupo de entrega, mantenha essa ordem. Caso contrário, classifique os recursos no grupo de entrega por nome do recurso.

d) Se o mesmo recurso aparece mais de uma vez, remova o recurso duplicado.

Os recursos que têm uma ordem definida pelo usuário associada a eles são implantados antes dos recursos sem uma ordem definida pelo usuário. Um recurso pode existir em vários grupos de entrega atribuídos a um usuário. Como indicado nas etapas acima, o algoritmo de cálculo apenas remove recursos redundantes e fornece o primeiro recurso nesta lista. Removendo recursos duplicados deste modo o XenMobile impõe a ordem definida pelo administrador do XenMobile.

Por exemplo, suponha que você tem dois grupos de entrega, desta forma:

- Grupo de entrega, Gerentes de conta 1: com ordem **não especificada** para recursos. Contém as políticas **WiFi** e **Código secreto**.
- Grupo de entrega, Gerentes de conta 2: com ordem **especificada** para recursos. Contém as políticas **Agendamento de conexão**, **Restrições**, **Código secreto** e **WiFi**. Nesse caso, você deseja fornecer a política de **Código secreto** antes de a política **WiFi**.



Se o algoritmo de cálculo tiver classificado grupos de implantação apenas por nome, o XenMobile realizará a implantação nessa ordem, começando com o grupo de entrega Gerentes de conta 1: **WiFi**, **Código secreto**, **Agendamento de conexão** e **Restrições**. O XenMobile ignoraria **Código secreto** e **WiFi**, os dois itens duplicados do grupo de entrega Gerentes de Conta 2.

No entanto, o grupo Gerentes de conta 2 tem uma ordem especificada pelo administrador de implantação. Portanto, o algoritmo de cálculo coloca recursos do grupo de entrega Gerentes de conta 2 mais alto na lista do que os recursos do outro grupo de entrega. Como resultado, o XenMobile implanta as políticas nesta ordem: **Agendamento de conexão**, **Restrição**, **Código secreto** e **WiFi**. O XenMobile ig-

nora as políticas de **Wi-Fi** e **Código secreto** do grupo de entrega Gerentes de conta 1 porque eles são itens duplicados. Portanto, esse algoritmo não respeita a ordem especificada pelo administrador do XenMobile.

Regras de implantação

Configure regras de implantação para fornecer recursos somente quando existirem condições específicas. Você pode configurar regras de implantação básicas ou avançadas.

Ao adicionar uma regra de implantação usando o editor de base, primeiro selecione quando implantar o recurso.

Deployment Rules

Base Advanced

Deploy when All conditions are met. New Rule

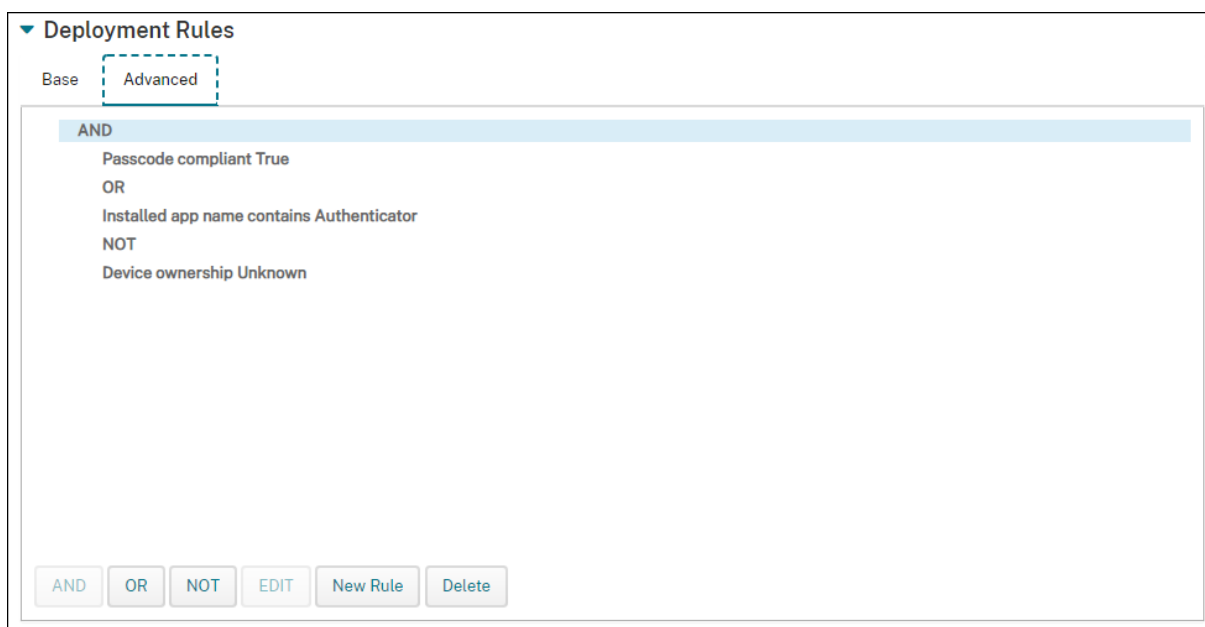
Deploy this resource rega...	only	shareable	✕
Installed app name	is equal to	Secure Hub	✕
Passcode compliant	True		✕
Manage cellular roaming	domestic		✕

- **Todas:** entregar o recurso quando o usuário ou dispositivo atender a todas as condições que você configurar.
- **Qualquer:** entregar o recurso quando o usuário ou dispositivo atender a pelo menos uma das condições que você configurar.

Clique em **Nova regra** para adicionar uma condição. As regras variam de acordo com o recurso que está sendo implantado e a plataforma para a qual você configura o recurso. Existem vários tipos de regras. Você pode optar por implantar o recurso:

- Somente quando a propriedade selecionada existe ou exceto quando a propriedade selecionada existe.
- Quando a propriedade corresponde exatamente ao texto que você digita, a propriedade contém o texto que você digita ou a propriedade não corresponde ao texto que você digita.
- Quando o dispositivo ou usuário está em conformidade com a propriedade selecionada ou não está em conformidade com a propriedade selecionada.
- Quando as propriedades do dispositivo ou usuário correspondem à condição que você seleciona em uma lista predefinida.

Use o editor avançado para criar regras de implantação mais complexas. Existem mais regras para selecionar e você pode combinar diferentes operadores lógicos booleanos ao criar uma regra avançada.



Para adicionar um grupo de entrega

A Citrix recomenda a criação de grupos de entrega antes de criar políticas de dispositivo e perfis de registro.

1. No console, clique em **Configurar > Grupos de entrega**.
2. Na página **Grupos de entrega**, clique em **Adicionar**.
3. Na página **Informações do grupo de entrega**, digite um nome e uma descrição para o grupo de entrega e clique em **Avançar**.

Se um usuário pertencer a vários grupos de entrega que têm perfis de registro diferentes, o nome do grupo de entrega determinará o perfil de registro usado. O XenMobile seleciona o grupo de entrega que aparece por último em uma lista alfabética de grupos de entrega. Para obter mais informações, consulte [Perfis de registro](#).

4. Na página **Atribuições de Usuário**, especifique como gerenciar as atribuições de usuário do grupo de entrega.

Importante:

Não é possível alterar a configuração **Gerenciar atribuições de usuário** depois que o grupo de usuários é criado.

- **Selecionar domínio:** na lista, selecione o domínio do qual escolher usuários.
- **Incluir grupos de usuários:** você pode optar por um dos seguintes procedimentos:
 - Na lista de grupos de usuários, clique em dos grupos que você deseja adicionar. Os grupos selecionados aparecerão na lista **Grupos de usuários selecionados**.
 - Clique em **Pesquisar** para ver uma lista de todos os grupos de usuários no domínio selecionado.
 - Digite um nome de grupo completo ou parcial na caixa de pesquisa e clique em **Pesquisar** para limitar a lista de grupos de usuários.

Para remover um grupo de usuários da lista **Grupos de usuários selecionados**, você pode optar por um dos seguintes procedimentos:

- Na lista **Grupos de usuários selecionados**, clique no **X** ao lado de cada um dos grupos que você deseja remover.
- Clique em **Pesquisar** para ver uma lista de todos os grupos de usuários no domínio selecionado. Role pela lista e desmarque a caixa de seleção de cada um dos grupos que você deseja remover.
- Digite um nome de grupo completo ou parcial na caixa de pesquisa e clique em **Pesquisar** para limitar a lista de grupos de usuários. Role pela lista e desmarque a caixa de seleção de cada um dos grupos que você deseja remover.
- **Ou/E:** selecione se os usuários podem estar em qualquer grupo (Ou) ou se devem estar em todos os grupos (E) para que o recurso seja implantado neles.

- **Implantar para usuário anônimo:** selecione se você deseja implantar para os usuários não autenticados no grupo de entrega. Usuários não autenticados são usuários que você não conseguiu autenticar, mas cujos dispositivos você permitiu se conectarem ao XenMobile de qualquer maneira.

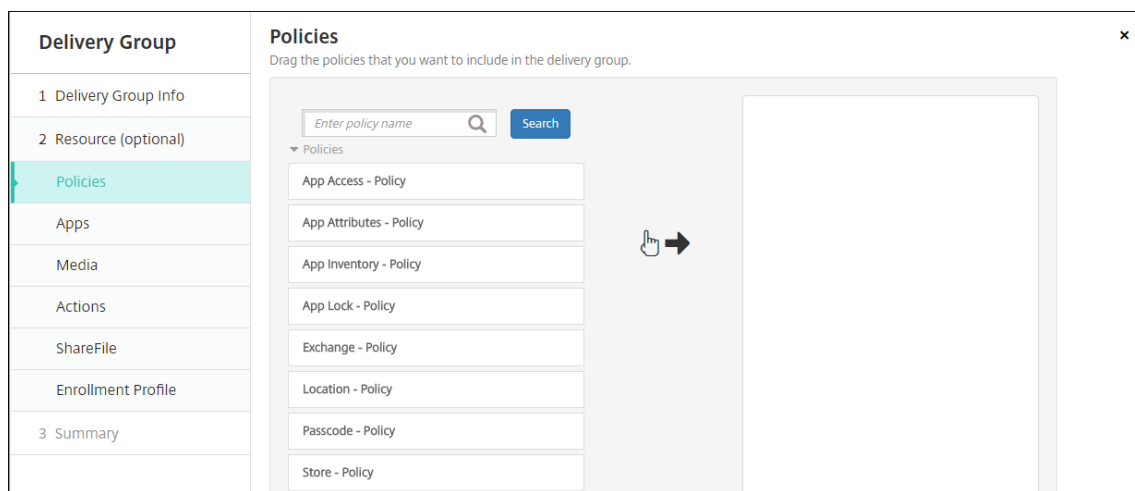
5. Configure as regras de implantação.
6. Clique em **Avançar**. A página de recursos de **Grupo de entrega** é exibida. Adicione opcionalmente políticas, aplicativos ou ações ao grupo de entrega aqui. Para ignorar essa etapa, em **Grupo de entrega**, clique em **Resumo** para ver um resumo da configuração do grupo de entrega.

Para ignorar um recurso, em **Recursos (opcional)**, clique no recurso que você deseja adicionar e siga as etapas para esse recurso.

Para adicionar políticas

1. Para cada política que você deseja adicionar, faça o seguinte:
 - Role pela lista de políticas disponíveis para localizar a política que você deseja adicionar.
 - Ou, para limitar a lista de políticas, digite o nome completo ou parcial da política na caixa de pesquisa e, em seguida, clique em **Pesquisar**.
 - Clique na política que deseja adicionar e arraste-a até a caixa à direita.

Para remover uma política, clique no **X** ao lado do nome da política na caixa à direita.



2. Clique em **Avançar**. A página **Aplicativos** é exibida.

Para adicionar aplicativos

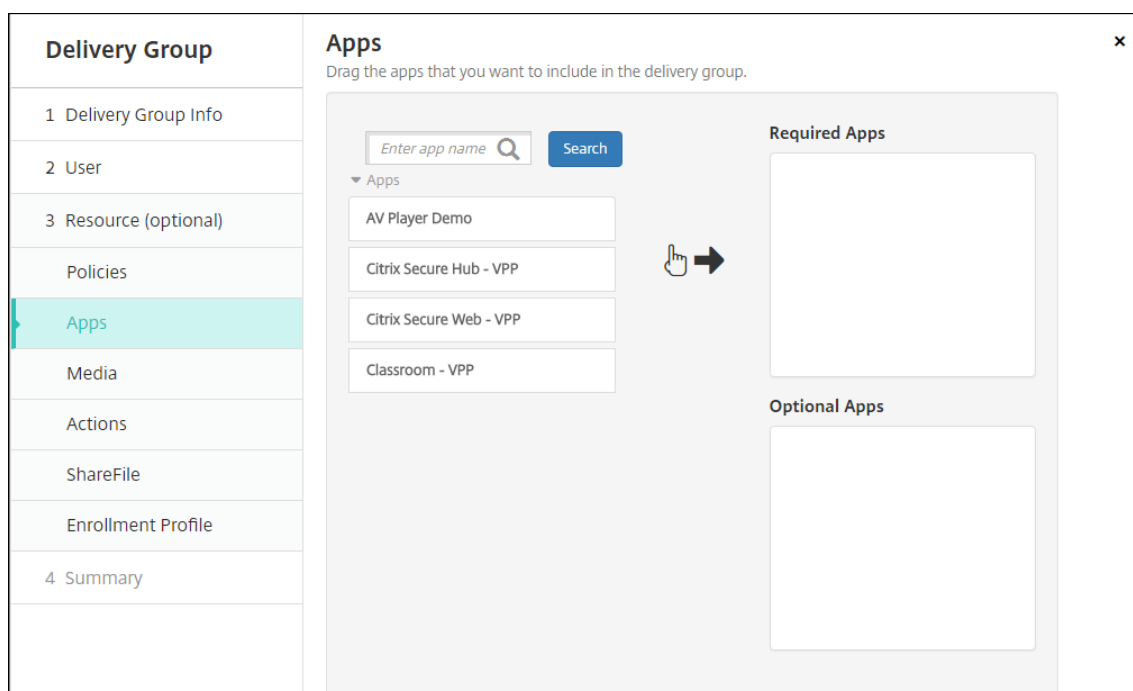
1. Para cada aplicativo que você deseja adicionar, faça o seguinte:

- Role pela lista de aplicativos disponíveis para localizar o aplicativo que você deseja adicionar.
- Ou, para limitar a lista de aplicativos, digite o nome completo ou parcial do aplicativo na caixa de pesquisa e, em seguida, clique em **Pesquisar**.
- Clique no aplicativo que você deseja adicionar e arraste-o até a caixa **Aplicativos obrigatórios** ou até a caixa **Aplicativos opcionais**.

Para aplicativos marcados como necessários, os usuários podem receber atualizações imediatamente em situações como:

- Carregue um novo aplicativo e marque-o conforme necessário.
- Marque um aplicativo existente conforme necessário.
- Quando o usuário exclui um aplicativo necessário.
- Está disponível uma atualização do Secure Hub.

Para obter informações sobre a implantação forçada de aplicativos obrigatórios, incluindo como habilitar o recurso, consulte [Sobre aplicativos obrigatórios e opcionais](#).



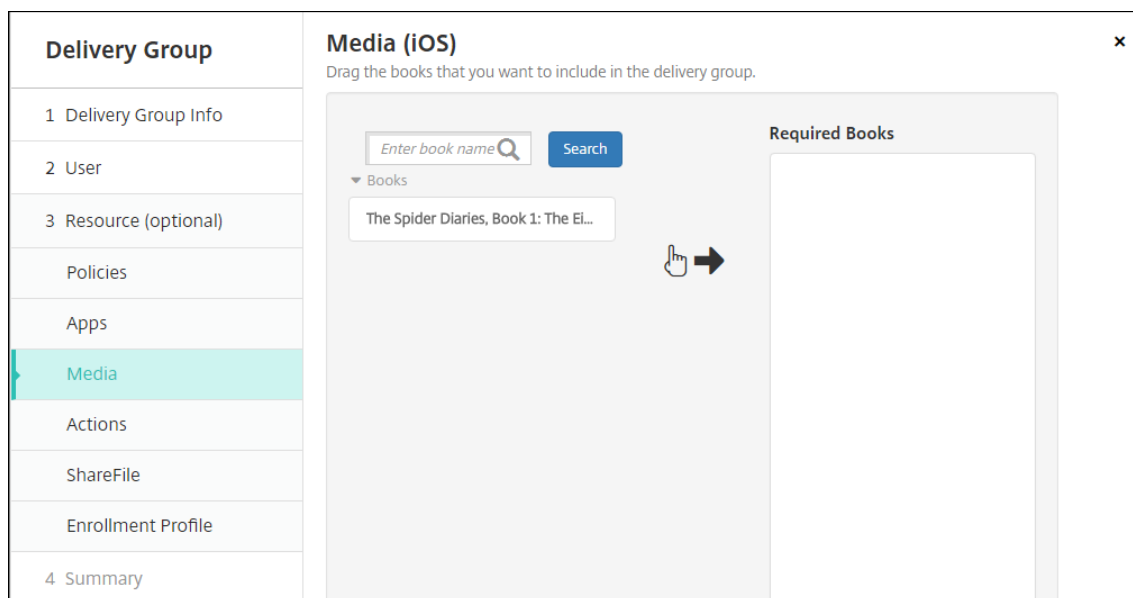
Para remover um aplicativo, clique no **X** ao lado do nome do aplicativo na caixa à direita.

2. Clique em **Avançar**. A página **Mídia** é exibida.

Para adicionar mídias

1. Para cada livro que você deseja adicionar, faça o seguinte:

- Role pela lista de livros disponíveis para localizar o livro que você deseja adicionar.
- Ou, para limitar a lista de livros, digite o nome completo ou parcial de um livro na caixa de pesquisa e, em seguida, clique em **Pesquisar**.
- Clique no livro que você deseja adicionar e arraste-o para a caixa **Livros obrigatórios**.



Para livros marcados como obrigatórios, os usuários recebem atualizações imediatamente em situações como:

- Carregue um novo livro e marque-o como necessário.
- Marque um livro existente como necessário.
- Quando o usuário exclui um livro necessário.
- Está disponível uma atualização do Secure Hub.

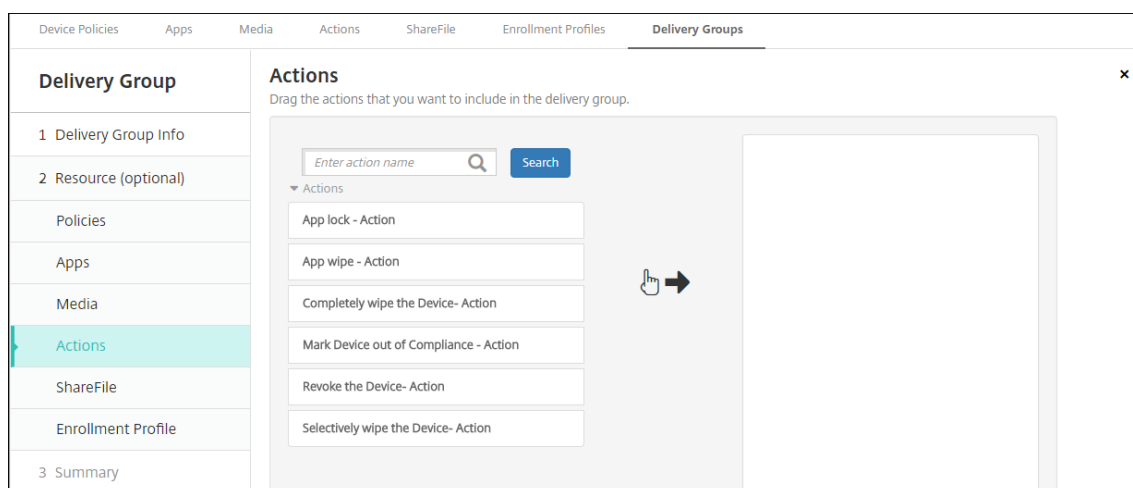
Para remover um livro, clique no **X** ao lado do nome do livro na caixa à direita.

2. Clique em **Avançar**. A página **Ações** é exibida.

Para adicionar ações

1. Para cada ação que você deseja adicionar, faça o seguinte:
 - Role pela lista de ações disponíveis para localizar o aplicativo que você deseja adicionar.
 - Ou, para limitar a lista de ações, digite o nome completo ou parcial da ação na caixa de pesquisa e, em seguida, clique em **Pesquisar**.
 - Clique na ação que deseja adicionar e arraste-a até a caixa à direita.

Para remover uma ação, clique no **X** ao lado do nome da ação na caixa à direita.

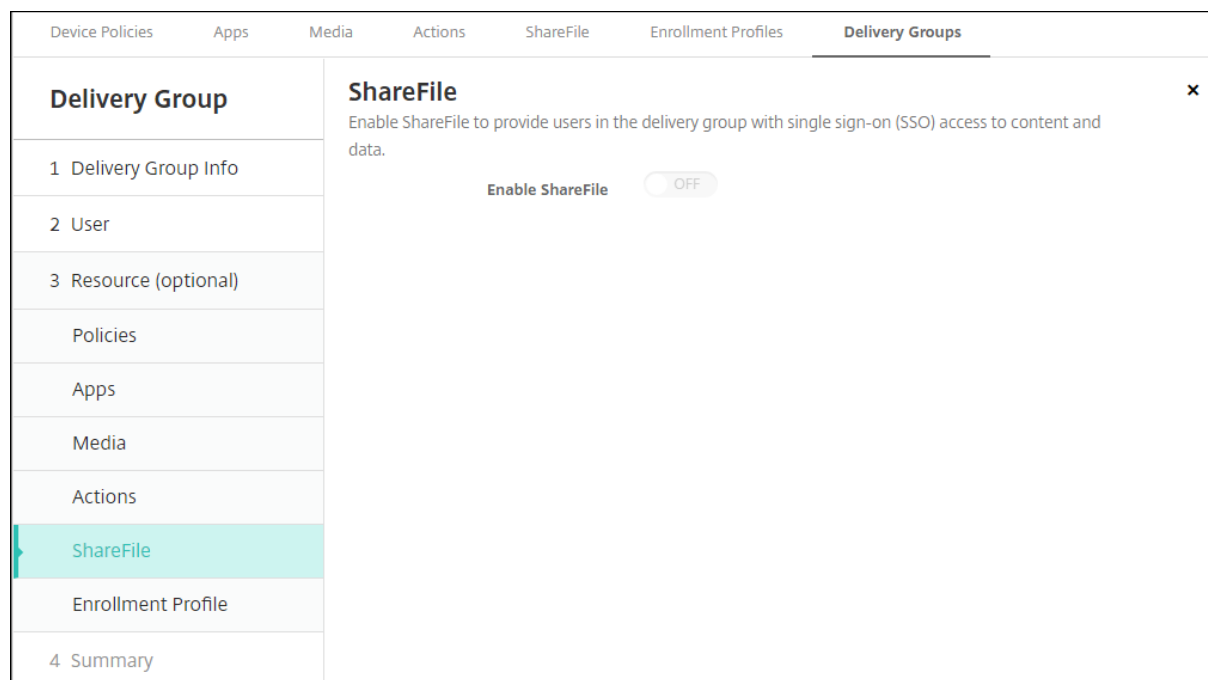


2. Clique em **Avançar**. A página **ShareFile** é exibida.

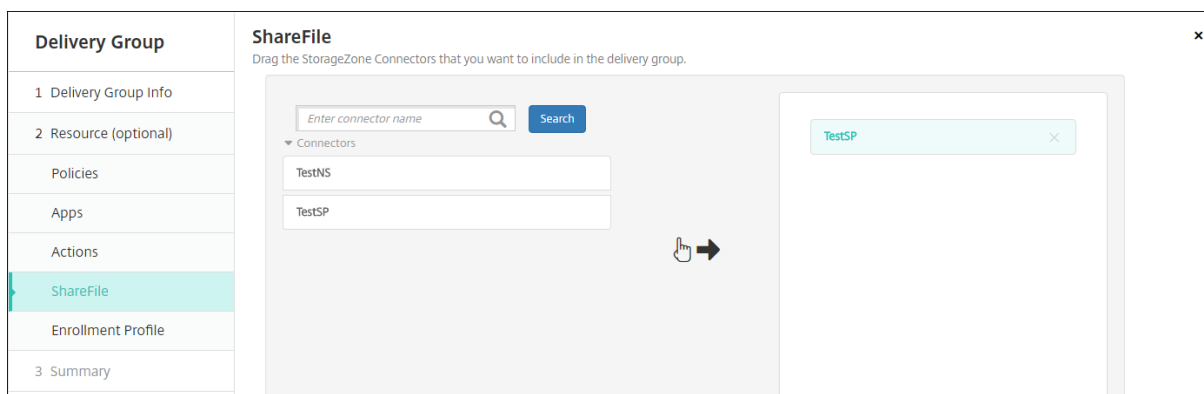
Para aplicar a configuração do Content Collaboration

A página Content Collaboration difere dependendo de você ter configurado o XenMobile (**Configurar > ShareFile**) para contas de empresa ou para conectores de zona de armazenamento.

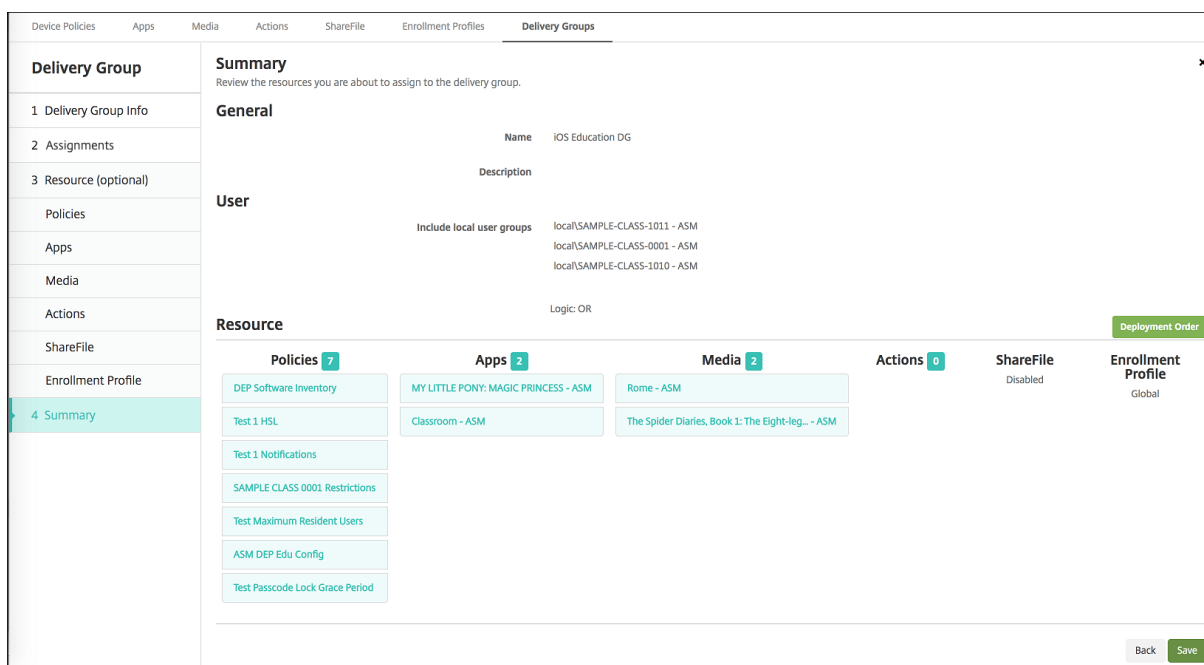
Se tiver configurado para contas de empresa para uso com o XenMobile, defina **Ativar ShareFile** como **I** para fornecer de acesso de logon único ao grupo de entrega para o conteúdo e os dados do Content Collaboration.



Se você tiver configurado os conectores de zona de armazenamento para uso com o XenMobile, selecione os conectores de zona de armazenamento que devem ser incluídos no grupo de entrega.

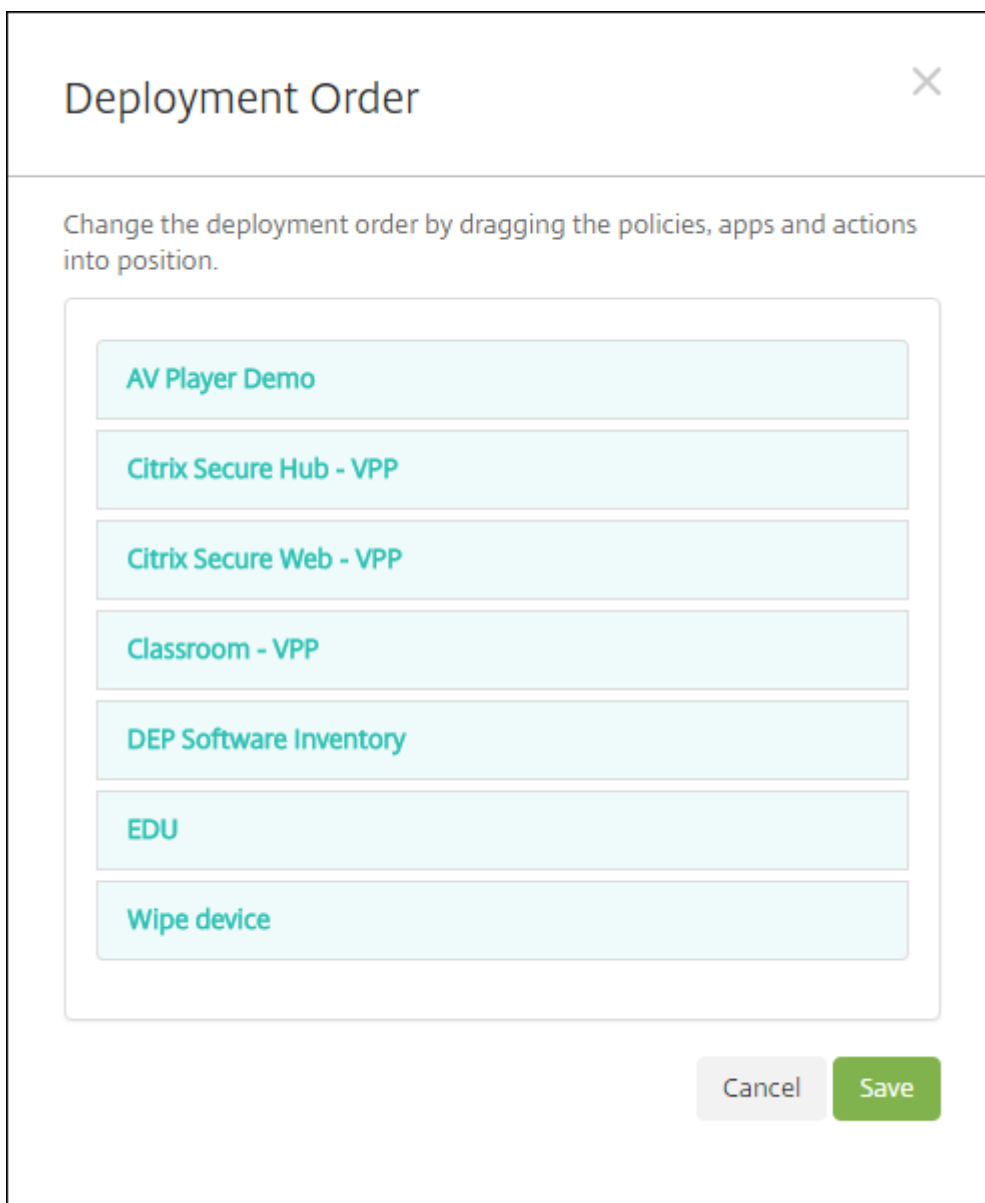


Para revisar as opções configuradas e alterar a ordem de implantação



Na página **Resumo**, você pode verificar as opções que configurou para o grupo de entrega e alterar a ordem de implantação dos recursos. A página Resumo mostra os recursos por categoria. A página Resumo não reflete a ordem de implantação.

1. Clique em **Voltar** para retornar às páginas anteriores e fazer os ajustes necessários na configuração.
2. Clique em **Ordem de implantação** para exibir a ordem de implantação ou para reordenar a implantação. A caixa de diálogo **Ordem de Implantação** é exibida.



3. Clique em um recurso e arraste-o até a localização da qual você deseja implantá-lo. Depois de alterar a ordem de implantação, o XenMobile implanta os recursos na lista de cima para baixo.
4. Clique em **Salvar** para salvar a ordem de implantação.
5. Clique em **Salvar** para salvar o grupo de entrega.

Para editar um grupo de entrega

Você não pode alterar o nome de um grupo de entrega existente. Para atualizar outras configurações: vá para **Configurar > Grupos de entrega**, selecione o grupo que deseja editar e clique em **Editar**.

Para ativar e desativar o grupo de entrega AllUsers

AllUsers é o único grupo de entrega que você pode ativar ou desativar.

Na página **Grupos de entrega**, escolha o grupo de entrega AllUsers marcando a caixa de seleção ao lado de **AllUsers** ou clicando na linha que contém AllUsers. Em seguida, você pode optar por um dos seguintes procedimentos:

- Clique em **Desativar** para desativar o grupo de entrega AllUsers. Esse comando estará disponível somente se AllUsers estiver ativado (o padrão). **Desativado** aparece sob o cabeçalho **Desativado** na tabela do grupo de entrega.
- Clique em **Ativar** para ativar o grupo de entrega AllUsers. Esse comando estará disponível somente se AllUsers estiver desativado. **Desativado** desaparece do cabeçalho **Desativado** na tabela do grupo de entrega.

Para implantar em grupos de entrega

Implantar em um grupo de entrega significa enviar uma notificação por push a todos os usuários com dispositivos iOS, Windows Phone e Tablet Windows. Esses usuários devem pertencer ao grupo de entrega para reconectarem-se ao XenMobile. Dessa forma, você pode reavaliar os dispositivos e implantar aplicativos, políticas e ações.

Para usuários com outros dispositivos de plataformas: se esses dispositivos já estiverem conectados ao XenMobile, eles receberão os recursos imediatamente. Caso contrário, com base em suas políticas de agendamento, eles receberão recursos da próxima vez em que se conectarem.

Para que aplicativos atualizados sejam exibidos na lista Updated Available na XenMobile Store de dispositivos Android, primeiro implante uma política de Inventário de aplicativos nos dispositivos dos usuários.

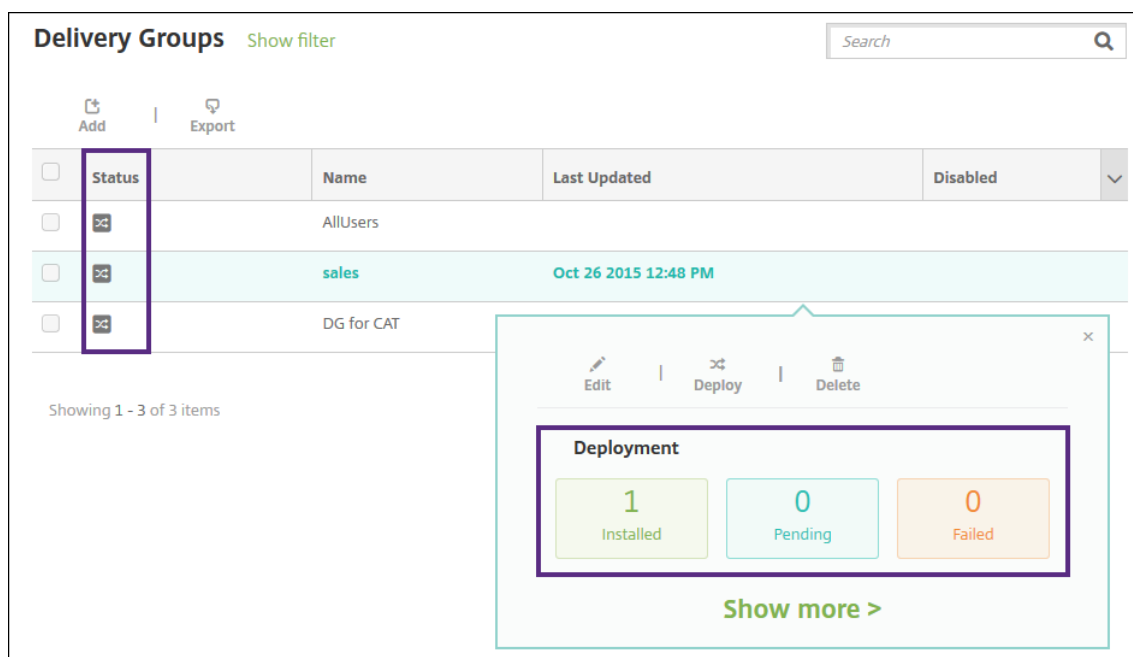
1. Na página **Grupos de entrega**, você pode optar por um dos seguintes procedimentos:
 - Para implantar em mais de um grupo de entrega por vez, marque as caixas de seleção ao lado dos grupos que você deseja implantar.
 - Para implantar em um único grupo de entrega, marque a caixa de seleção ao lado do respectivo nome ou na linha que contém o nome do grupo.
2. Clique em **Implantar**.

Dependendo de como você selecionar um único grupo de entrega, o comando **Implantar** será exibido acima ou à direita do grupo de entrega.

Verifique se os grupos nos quais você deseja implantar aplicativos, políticas e ações estão listados e, em seguida, clique em **Implantar**. Os aplicativos, políticas e ações são implantados para os grupos selecionados com base na plataforma de dispositivo e política de agendamento.

Você pode verificar o status da implantação na página **Grupos de entrega** de uma das seguintes formas:

- Examine o ícone de implantação no cabeçalho **Status** do grupo de entrega, o que indica qualquer falha de implantação.
- Clique na linha que contém o grupo de entrega para exibir uma sobreposição que indica implantações **Instaladas**, **Pendentes** e **Falhas**.



Para excluir grupos de entrega

Você não pode excluir o grupo de entrega AllUsers, mas pode desativá-lo quando não desejar enviar recursos por push para todos os usuários.

1. Na página **Grupos de entrega**, você pode optar por um dos seguintes procedimentos:
 - Para excluir em mais de um grupo de entrega por vez, marque as caixas de seleção ao lado dos grupos que você deseja excluir.
 - Para excluir um único grupo de entrega, marque a caixa de seleção ao lado do respectivo nome ou na linha que contém o nome do grupo.
2. Clique em **Excluir**. A caixa de diálogo **Excluir** é exibida.

Dependendo de como você selecionar um único grupo de entrega, o comando **Excluir** será exibido acima ou à direita do grupo de entrega.

Importante:

Você não pode desfazer uma exclusão.

3. Clique em **Excluir**.

Para exportar a tabela Grupos de Entrega

1. Clique no botão **Exportar** acima da tabela **Grupos de entrega**. O XenMobile extrai as informações na tabela **Grupos de entrega** e converte-as em um arquivo .csv.
2. Abra ou salve o arquivo .csv, seguindo as etapas normais do seu navegador. Você também pode cancelar a operação.

Macros

April 8, 2021

O XenMobile fornece macros como uma forma de preencher dados de propriedades de usuários ou dispositivos no campo de texto dos seguintes itens:

- Políticas
- Notificações
- Modelos de registro
- Ações automatizadas
- Solicitações de assinatura de certificado do provedor de credenciais

O XenMobile substitui uma macro pelos valores de sistema ou de usuário correspondentes. Por exemplo, você pode preencher previamente o valor da caixa de correio de um usuário em um único perfil do Exchange entre milhares de usuários.

Sintaxe de macro

Uma macro pode assumir a seguinte forma:

- `${ type.PROPERTYNAME }`
- `${ type.PROPERTYNAME ['DEFAULT VALUE'] [| FUNCTION [(ARGUMENT1, ARGUMENT2)]] }`

Coloque toda a sintaxe após o cifrão (\$) entre chaves ({}).

- Os nomes qualificados de propriedade fazem referência a uma propriedade de usuário, uma propriedade de dispositivo ou uma propriedade personalizada.
- Os nomes qualificados de propriedade consistem em um prefixo, seguido do nome real da propriedade.
- Propriedades do usuário do formulário `${ user.[PROPERTYNAME] (prefix="user.")}`.

- Propriedades do dispositivo do formulário ``${ device.[PROPERTYNAME] (prefix="device.")}``.
- Nomes de propriedade diferenciam maiúsculas de minúsculas.
- Uma função pode ser uma lista limitada ou um link para uma referência de terceiros que define funções. A seguinte macro para uma mensagem de notificação inclui a função **firstnotnull**:
O dispositivo ``${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}`` foi bloqueado...
- Para macros personalizadas (propriedades que você define), o prefixo é ``${ custom}``. Você pode omitir o prefixo.

Este é um exemplo de macro comum, ``${ user.username}``, que preenche o valor de nome do usuário no campo de texto de uma política. Essa macro é útil para configurar perfis do Exchange ActiveSync e outros perfis usados por vários usuários. O exemplo a seguir mostra como usar macros em uma política do Exchange. A macro para o **Usuário** é ``${ user.username}``. A macro para **Endereço de email** é ``${ user.mail}``.

O exemplo a seguir mostra como usar macros para uma solicitação de assinatura de certificado. A macro para **Nome de entidade** é ``${ CN=$user.username}``. A macro para **Valor** de um **Nome de entidade alternativo** é ``${ $user.userprincipalname}``.

Settings > Credential Providers > Add credential provider

Credential Providers: Certificate Signing Request

Configure the parameters for the key pair that is created during issuance, as well as the parameters of the new certificate.

Key algorithm: RSA

Key size*: 2048

Signature algorithm: SHA256withRSA

Subject name*: CN=Suser.username

Subject alternative names

Type	Value*	Add
User Principal name	Suser.userprincipalname	

O exemplo a seguir mostra como usar macros em um modelo de notificação. O modelo de exemplo define a mensagem enviada a um usuário quando aplicativos HDX são bloqueados devido a um dispositivo não compatível. A macro para a **Mensagem** é:

O dispositivo `${ firstNotNull(device.TEL_NUMBER,device.serialNumber) }` não está mais em conformidade com a política de dispositivo, e os aplicativos HDX serão bloqueados.

Settings > Notification Templates > Add Notification Template

Add Notification Template

Based on the types of templates you choose, you can notify users through supported channels, such as SMTP, SMS and Secure Hub.

Name*: HDX Application Block

Description:

Type: Ad-Hoc Notification
Manual sending supported

Channels

Secure Hub: Activate

Message: Device `${firstNotNull(device.TEL_NUMBER,device.serialNumber)}` no longer complies with the device policy and HDX applications will be blocked.

Para obter mais exemplos de macros utilizadas em notificações, vá para **Configurações > Modelos de notificação**, selecione um modelo predefinido e clique em **Editar**.

O exemplo a seguir mostra uma macro na política de dispositivo Nome do dispositivo. Você pode digitar uma macro, uma combinação de macros ou uma combinação de macros e texto para nomear cada dispositivo de forma exclusiva. Por exemplo, use `${ device.serialnumber }` para definir

o nome de dispositivo de acordo com o número de série de cada dispositivo. Use `${ device.serialnumber }` `${ user.username }` para incluir o nome do usuário no nome do dispositivo. A política de dispositivo Nome do Dispositivo funciona em dispositivos supervisionados iOS e macOS.

Device Name Policy	Device Name Policy x
1 Policy Info	This policy lets you apply a name on a supervised device on iOS and Mac OS X devices. Available in iOS 8 and later.
2 Platforms	Device name* <input type="text" value="\${device.serialnumber}"/>
<input checked="" type="checkbox"/> iOS	▶ Deployment Rules
<input checked="" type="checkbox"/> Mac OS X	
3 Assignment	

Macros para modelos de notificação padrão

Você pode usar as seguintes macros nos modelos de notificação padrão:

- `${ account.SUPPORT_EMAIL }`
- `${ applicationName }`
- `${ enrollment.android.agent.download.url }`
- `${ enrollment.ios.agent.download.url }`
- `${ enrollment.pin }`
- `${ enrollment.url }`
- `${ enrollment.urls }`
- `${ enrollment.ios.url }`
- `${ enrollment.macos.url }`
- `${ enrollment.android.url }`
- `${ enrollment.ios.platform }`
- `${ enrollment.macos.platform }`
- `${ enrollment.android.platform }`
- `${ firstnotnull(device.TEL_NUMBER,device.serialNumber)}`
- `${ firstnotnull(device.TEL_NUMBER,user.mobile)}`
- `${ outofcompliance.reason(smg_block)}`
- `${ outofcompliance.reason(whitelist_blacklist_apps_name)}`

Nota:

O console XenMobile Server inclui os termos “lista negra” e “lista branca”. Estamos alterando esses termos em uma próxima versão para “lista de bloqueio” e “lista de permissão”.

- `${ vpp.account }`
- `${ vpp.appname }`
- `${ vpp.url }`
- `${ zdmserver.hostPath } /enroll`

Macros para políticas específicas

Para a política de dispositivo de Nome do dispositivo (para iOS e macOS), você pode usar essas macros para o **Nome do dispositivo**:

- `${ device.serialnumber }`
- `${ user.username } @example.com`
- `${ device.serialnumber }`
- `${ device.serialnumber }`
- `${ user.username }`
- `${ enrollment.pin }`
- `${ user.dnsroot }`

Para a política de dispositivos clip web, você pode usar esta macro para a **URL**:

- `${ webeas-url }`

Para a política de dispositivo de Chave de licença Samsung MDM, você pode usar essa macro para a **chave de licença ELM**:

- `${ elm.license.key }`

Macros para obter as propriedades internas de dispositivo

Nome de exibição	Macros
ID do dispositivo	<code>\$device.id</code>
GUID do dispositivo	<code>\$device.uniqueid</code>
IMEI do dispositivo	<code>\$device.imei</code>
Família de SO	<code>\$device.OSFamily</code>
Número de série	<code>\$device.serialNumber</code>

Macros para todas as propriedades de dispositivo

A lista a seguir fornece o nome de exibição, o elemento Web e as macros.

Conta suspensa?

- GOOGLE_AW_DIRECTORY_SUSPENDED
- \${device.GOOGLE_AW_DIRECTORY_SUSPENDED}

Código de desvio do bloqueio de ativação

- ACTIVATION_LOCK_BYPASS_CODE
- \${device.ACTIVATION_LOCK_BYPASS_CODE}

Bloqueio de ativação ativado

- ACTIVATION_LOCK_ENABLED
- \${device.ACTIVATION_LOCK_ENABLED}

Conta do iTunes Active

- ACTIVE_ITUNES
- \${device.ACTIVE_ITUNES}

Dispositivo ActiveSync conhecido por MSP

- AS_DEVICE_KNOWN_BY_ZMSP
- \${device.AS_DEVICE_KNOWN_BY_ZMSP}

ID do ActiveSync

- EXCHANGE_ACTIVASYNC_ID
- \${device.EXCHANGE_ACTIVASYNC_ID}

Administrador desativado

- ADMIN_DISABLED
- \${device.ADMIN_DISABLED}

AIK presente?

- WINDOWS_HAS_AIK_PRESENT
- \${device.WINDOWS_HAS_AIK_PRESENT}

API do MDM Amazon disponível

- AMAZON_MDM
- \${device.AMAZON_MDM}

ID do dispositivo Android Enterprise

- GOOGLE_AW_DEVICE_ID
- \${device.GOOGLE_AW_DEVICE_ID}

Dispositivo Android Enterprise habilitado?

- GOOGLE_AW_ENABLED_DEVICE
- \${device.GOOGLE_AW_ENABLED_DEVICE}

Tipo de instalação do Android Enterprise

- GOOGLE_AW_INSTALL_TYPE
- \${device.GOOGLE_AW_INSTALL_TYPE}

Status de assinatura de antispymware

- ANTI_SPYWARE_SIGNATURE_STATUS
- \${device.ANTI_SPYWARE_SIGNATURE_STATUS}

Status de antiSpyware

- ANTI_SPYWARE_STATUS
- \${device.ANTI_SPYWARE_STATUS}

Status de assinatura de antivírus

- ANTI_VIRUS_SIGNATURE_STATUS
- \${device.ANTI_VIRUS_SIGNATURE_STATUS}

Status do antivírus

- ANTI_VIRUS_STATUS
- \${device.ANTI_VIRUS_STATUS}

Código de desvio de trava de ativação DEP ASM

- DEP_ACTIVATION_LOCK_BYPASS_CODE
- \${device.DEP_ACTIVATION_LOCK_BYPASS_CODE}

Chave de caução DEP ASM

- DEP_ESCROW_KEY
- \${device.DEP_ESCROW_KEY}

Marca do recurso

- ASSET_TAG
- \${device.ASSET_TAG}

Verificar atualizações de software automaticamente

- AutoCheckEnabled
- \${device.AutoCheckEnabled}

Baixar automaticamente as atualizações de software em segundo plano

- BackgroundDownloadEnabled

- `#{device.BackgroundDownloadEnabled}`

Instalar automaticamente as atualizações de aplicativos

- `AutomaticAppInstallationEnabled`
- `#{device.AutomaticAppInstallationEnabled}`

Instalar automaticamente as atualizações de SO

- `AutomaticOSInstallationEnabled`
- `#{device.AutomaticOSInstallationEnabled}`

Instalar automaticamente as atualizações de segurança

- `AutomaticSecurityUpdatesEnabled`
- `#{device.AutomaticSecurityUpdatesEnabled}`

Status de atualização automática

- `AUTOUPDATE_STATUS`
- `#{device.AUTOUPDATE_STATUS}`

RAM disponível

- `MEMORY_AVAILABLE`
- `#{device.MEMORY_AVAILABLE}`

Atualizações de software disponíveis

- `AVAILABLE_OS_UPDATE_HUMAN_READABLE`
- `#{device.AVAILABLE_OS_UPDATE_HUMAN_READABLE}`

Espaço de armazenamento disponível

- `FREEDISK`
- `#{device.FREEDISK}`

Bateria de backup

- `BACKUP_BATTERY_PERCENT`
- `#{device.BACKUP_BATTERY_PERCENT}`

Versão de firmware banda básica

- `MODEM_FIRMWARE_VERSION`
- `#{device.MODEM_FIRMWARE_VERSION}`

Bateria carregando

- `BATTERY_CHARGING_STATUS`
- `#{device.BATTERY_CHARGING_STATUS}`

Carregamento da bateria

- BATTERY_CHARGING
- \${device.BATTERY_CHARGING}

Carga de bateria restante

- BATTERY_ESTIMATED_CHARGE_REMAINING
- \${device.BATTERY_ESTIMATED_CHARGE_REMAINING}

Tempo de operação da bateria

- BATTERY_RUNTIME
- \${device.BATTERY_RUNTIME}

Status da bateria

- BATTERY_STATUS
- \${device.BATTERY_STATUS}

Dispositivo BES conhecido por MS

- BES_DEVICE_KNOWN_BY_ZMSP
- \${device.BES_DEVICE_KNOWN_BY_ZMSP}

PIN do BES

- BES_PIN
- \${device.BES_PIN}

ID do agente de servidor BES

- AGENT_ID
- \${device.AGENT_ID}

Nome do servidor BES

- BES_SERVER
- \${device.BES_SERVER}

Versão do servidor BES

- BES_VERSION
- \${device.BES_VERSION}

Informações de BIOS

- BIOS_INFO
- \${device.BIOS_INFO}

Status do BitLocker

- WINDOWS_HAS_BIT_LOCKER_STATUS
- \${device.WINDOWS_HAS_BIT_LOCKER_STATUS}

Endereço MAC Bluetooth

- BLUETOOTH_MAC
- \${device.BLUETOOTH_MAC}

Depuração de inicialização ativada?

- WINDOWS_HAS_BOOT_DEBUGGING_ENABLED
- \${device.WINDOWS_HAS_BOOT_DEBUGGING_ENABLED}

Versão da lista de revisões do Gerenciador de inicialização

- WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION
- \${device.WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION}

Código da operadora

- CARRIER_CODE
- \${device.CARRIER_CODE}

Versão de configurações de operadora

- CARRIER_SETTINGS_VERSION
- \${device.CARRIER_SETTINGS_VERSION}

URL do catálogo

- CatalogURL
- \${device.CatalogURL}

Altitude da rede celular

- GPS_ALTITUDE_FROM_CELLULAR
- \${device.GPS_ALTITUDE_FROM_CELLULAR}

Curso da rede celular

- GPS_COURSE_FROM_CELLULAR
- \${device.GPS_COURSE_FROM_CELLULAR}

Precisão horizontal da rede celular

- GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR
- \${device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR}

Latitude da rede celular

- GPS_LATITUDE_FROM_CELLULAR
- \${device.GPS_LATITUDE_FROM_CELLULAR}

Longitude da rede celular

- GPS_LONGITUDE_FROM_CELLULAR

- `device.GPS_LONGITUDE_FROM_CELLULAR`

Velocidade da rede celular

- `GPS_SPEED_FROM_CELLULAR`
- `device.GPS_SPEED_FROM_CELLULAR`

Tecnologia da rede celular

- `CELLULAR_TECHNOLOGY`
- `device.CELLULAR_TECHNOLOGY`

Carimbo data/hora da rede celular

- `GPS_TIMESTAMP_FROM_CELLULAR`
- `device.GPS_TIMESTAMP_FROM_CELLULAR`

Precisão vertical da rede celular

- `GPS_VERTICAL_ACCURACY_FROM_CELLULAR`
- `device.GPS_VERTICAL_ACCURACY_FROM_CELLULAR`

Alterar a senha no próximo Login?

- `GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN`
- `device.GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN`

ID de dispositivo de cliente

- `CLIENT_DEVICE_ID`
- `device.CLIENT_DEVICE_ID`

Backup de nuvem ativado

- `CLOUD_BACKUP_ENABLED`
- `device.CLOUD_BACKUP_ENABLED`

Integridade do código ativada?

- `WINDOWS_HAS_CODE_INTEGRITY_ENABLED`
- `device.WINDOWS_HAS_CODE_INTEGRITY_ENABLED`

Versão da lista de revisões de integridade do código

- `WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION`
- `device.WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION`

Cor

- `COR`
- `device.COLOR`

Velocidade de CPU

- CPU_CLOCK_SPEED
- \${device.CPU_CLOCK_SPEED}

Tipo de CPU

- CPU_TYPE
- \${device.CPU_TYPE}

Criação de regras

- GOOGLE_AW_DIRECTORY_CREATION_TIME
- \${device.GOOGLE_AW_DIRECTORY_CREATION_TIME}

Atualizações de software críticas

- AVAILABLE_OS_UPDATE_IS_CRITICAL
- \${device.AVAILABLE_OS_UPDATE_IS_CRITICAL}

Rede da operadora atual

- CARRIER
- \${device.CARRIER}

Código do país móvel atual

- CURRENT_MCC
- \${device.CURRENT_MCC}

Código de rede móvel atual

- CURRENT_MNC
- \${device.CURRENT_MNC}

Dados roaming permitido

- DATA_ROAMING_ENABLED
- \${device.DATA_ROAMING_ENABLED}

Data do último backup iCloud

- LAST_CLOUD_BACKUP_DATE
- \${device.LAST_CLOUD_BACKUP_DATE}

Catálogo padrão

- IsDefaultCatalog
- \${device.IsDefaultCatalog}

Nome da conta DEP

- BULK_ENROLLMENT_DEP_ACCOUNT_NAME
- \${device.BULK_ENROLLMENT_DEP_ACCOUNT_NAME}

Política DEP

- WINDOWS_HAS_DEP_POLICY
- \${device.WINDOWS_HAS_DEP_POLICY}

Perfil de DEP atribuído

- PROFILE_ASSIGN_TIME
- \${device.PROFILE_ASSIGN_TIME}

Perfil de DEP enviado

- PROFILE_PUSH_TIME
- \${device.PROFILE_PUSH_TIME}

Perfil de DEP removido

- PROFILE_REMOVE_TIME
- \${device.PROFILE_REMOVE_TIME}

Registro de DEP por

- DEVICE_ASSIGNED_BY
- \${device.DEVICE_ASSIGNED_BY}

Data de registro de DEP

- DEVICE_ASSIGNED_DATE
- \${device.DEVICE_ASSIGNED_DATE}

Descrição

- DESCRIPTION
- \${device.DESCRPTION}

Identificador do dispositivo

- Activesyncid
- \${device.activesyncid}

Modelo do dispositivo

- SYSTEM_OEM
- \${device.SYSTEM_OEM}

Nome do dispositivo

- DEVICE_NAME
- \${device.DEVICE_NAME}

Tipo de dispositivo

- DEVICE_TYPE

- `device.DEVICE_TYPE`

Você pode optar por não perturbe ativado

- `DO_NOT_DISTURB`
- `device.DO_NOT_DISTURB`

Driver ELAM carregado?

- `WINDOWS_HAS_ELAM_DRIVER_LOADED`
- `device.WINDOWS_HAS_ELAM_DRIVER_LOADED`

Conformidade com criptografia

- `ENCRYPTION_COMPLIANCE`
- `device.ENCRYPTION_COMPLIANCE`

ENROLLMENT_KEY_GENERATION_DATE

- `ENROLLMENT_KEY_GENERATION_DATE`
- `device.ENROLLMENT_KEY_GENERATION_DATE`

ID da empresa

- `ENTERPRISEID`
- `device.ENTERPRISEID`

Armazenamento externo 1: espaço disponível

- `EXTERNAL_STORAGE1_FREE_SPACE`
- `device.EXTERNAL_STORAGE1_FREE_SPACE`

Armazenamento externo 1: nome

- `EXTERNAL_STORAGE1_NAME`
- `device.EXTERNAL_STORAGE1_NAME`

Armazenamento externo 1: espaço total

- `EXTERNAL_STORAGE1_TOTAL_SPACE`
- `device.EXTERNAL_STORAGE1_TOTAL_SPACE`

Armazenamento externo 2: espaço disponível

- `EXTERNAL_STORAGE2_FREE_SPACE`
- `device.EXTERNAL_STORAGE2_FREE_SPACE`

Armazenamento externo 2: nome

- `EXTERNAL_STORAGE2_NAME`
- `device.EXTERNAL_STORAGE2_NAME`

Armazenamento externo 2: espaço total

- EXTERNAL_STORAGE2_TOTAL_SPACE
- \${device.EXTERNAL_STORAGE2_TOTAL_SPACE}

Armazenamento externo criptografado

- EXTERNAL_ENCRYPTION
- \${device.EXTERNAL_ENCRYPTION}

FileVault ativado

- IS_FILEVAULT_ENABLED
- \${device.IS_FILEVAULT_ENABLED}

Status de firewall

- DEVICE_FIREWALL_STATUS
- \${device.DEVICE_FIREWALL_STATUS}

Status de firewall

- FIREWALL_STATUS
- \${device.FIREWALL_STATUS}

Versão de firmware

- FIRMWARE_VERSION
- \${device.FIRMWARE_VERSION}

Primeira sincronização

- ZMSP_FIRST_SYNC
- \${device.ZMSP_FIRST_SYNC}

Alias do diretório do Google

- GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS
- \${device.GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS}

Nome de família do Google diretório

- GOOGLE_AW_DIRECTORY_FAMILY_NAME
- \${device.GOOGLE_AW_DIRECTORY_FAMILY_NAME}

Nome do Google Directory

- GOOGLE_AW_DIRECTORY_NAME
- \${device.GOOGLE_AW_DIRECTORY_NAME}

Email principal do Google diretório

- GOOGLE_AW_DIRECTORY_PRIMARY
- \${device.GOOGLE_AW_DIRECTORY_PRIMARY}

ID de usuário do Google diretório

- GOOGLE_AW_DIRECTORY_USER_ID
- \${device.GOOGLE_AW_DIRECTORY_USER_ID}

Altitude GPS

- GPS_ALTITUDE_FROM_GPS
- \${device.GPS_ALTITUDE_FROM_GPS}

Curso de GPS

- GPS_COURSE_FROM_GPS
- \${device.GPS_COURSE_FROM_GPS}

Precisão horizontal do GPS

- GPS_HORIZONTAL_ACCURACY_FROM_GPS
- \${device.GPS_HORIZONTAL_ACCURACY_FROM_GPS}

Latitude de GPS

- GPS_LATITUDE_FROM_GPS
- \${device.GPS_LATITUDE_FROM_GPS}

Longitude do GPS

- GPS_LONGITUDE_FROM_GPS
- \${device.GPS_LONGITUDE_FROM_GPS}

Velocidade do GPS

- GPS_SPEED_FROM_GPS
- \${device.GPS_SPEED_FROM_GPS}

Carimbo data/hora do GPS

- GPS_TIMESTAMP_FROM_GPS
- \${device.GPS_TIMESTAMP_FROM_GPS}

Precisão vertical do GPS

- GPS_VERTICAL_ACCURACY_FROM_GPS
- \${device.GPS_VERTICAL_ACCURACY_FROM_GPS}

ID de dispositivo de hardware

- HW_DEVICE_ID
- \${device.HW_DEVICE_ID}

Recursos de criptografia de hardware

- HARDWARE_ENCRYPTION_CAPS

- `$(device.HARDWARE_ENCRYPTION_CAPS)`

HAS_CONTAINER

- HAS_CONTAINER
- `$(device.HAS_CONTAINER)`

Hash do iTunes armazenar fez logon de conta

- ITUNES_STORE_ACCOUNT_HASH
- `$(device.ITUNES_STORE_ACCOUNT_HASH)`

Rede da operadora inicial

- SIM_CARRIER_NETWORK
- `$(device.SIM_CARRIER_NETWORK)`

Código do país móvel local

- SIM_MCC
- `$(device.SIM_MCC)`

Código de rede móvel local

- SIM_MNC
- `$(device.SIM_MNC)`

ICCID

- ICCID
- `$(device.ICCID)`

Identidade

- AS_DEVICE_IDENTITY
- `$(device.AS_DEVICE_IDENTITY)`

Número IMEI/MEID

- IMEI
- `$(device.IMEI)`

IMSI

- SIM_ID
- `$(device.SIM_ID)`

Armazenamento interno criptografado

- LOCAL_ENCRYPTION
- `$(device.LOCAL_ENCRYPTION)`

Localização de IP

- IP_LOCATION
- \${device.IP_LOCATION}

Endereço IPv4

- IP_ADDRESSV4
- \${device.IP_ADDRESSV4}

Endereço IPv6

- IP_ADDRESSV6
- \${device.IP_ADDRESSV6}

Emitido em

- WINDOWS_HAS_ISSUED_AT
- \${device.WINDOWS_HAS_ISSUED_AT}

Jailbroken/com raiz

- ROOT_ACCESS
- \${device.ROOT_ACCESS}

Depuração de kernel ativada?

- WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED
- \${device.WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED}

Modo de quiosque

- IS_KIOSK
- \${device.IS_KIOSK}

Último endereço IP conhecido

- LAST_IP_ADDR
- \${device.LAST_IP_ADDR}

Última vez de atualização de política

- LAST_POLICY_UPDATE_TIME
- \${device.LAST_POLICY_UPDATE_TIME}

Última data de busca

- PreviousScanDate
- \${device.PreviousScanDate}

Último resultado da busca

- PreviousScanResult
- \${device.PreviousScanResult}

Últimas atualizações de software programadas

- AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME
- \${device.AVAILABLE_OS_UPDATE_INSTALL_LAST_ATTEMPT_TIME}

Última mensagem de falha de atualizações de software agendadas

- AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG
- \${device.AVAILABLE_OS_UPDATE_INSTALL_FAIL_MSG}

Último status de atualizações de software agendadas

- AVAILABLE_OS_UPDATE_INSTALL_STATUS
- \${device.AVAILABLE_OS_UPDATE_INSTALL_STATUS}

Última sincronização

- ZMSP_LAST_SYNC
- \${device.ZMSP_LAST_SYNC}

Serviço de localização ativado

- DEVICE_LOCATOR
- \${device.DEVICE_LOCATOR}

Endereço MAC

- MAC_ADDRESS
- \${device.MAC_ADDRESS}

Conexão de rede de endereço MAC

- MAC_NETWORK_CONNECTION
- \${device.MAC_NETWORK_CONNECTION}

Tipo de endereço MAC

- MAC_ADDRESS_TYPE
- \${device.MAC_ADDRESS_TYPE}

Configuração de caixa de correio

- GOOGLE_AW_DIRECTORY_MAILBOX_SETUP
- \${device.GOOGLE_AW_DIRECTORY_MAILBOX_SETUP}

Bateria principal

- MAIN_BATTERY_PERCENT
- \${device.MAIN_BATTERY_PERCENT}

Modo MDM perdido ativado

- IS_MDM_LOST_MODE_ENABLED

- `device.IS_MDM_LOST_MODE_ENABLED`

MDX_SHARED_ENCRYPTION_KEY

- `MDX_SHARED_ENCRYPTION_KEY`
- `device.MDX_SHARED_ENCRYPTION_KEY`

MEID

- `MEID`
- `device.MEID`

Número de telefone celular

- `TEL_NUMBER`
- `device.TEL_NUMBER`

ID do modelo

- `MODEL_ID`
- `device.MODEL_ID`

Número do modelo

- `MODEL_NUMBER`
- `device.MODEL_NUMBER`

Tipo de adaptador de rede

- `NETWORK_ADAPTER_TYPE`
- `device.NETWORK_ADAPTER_TYPE`

Compilação do sistema operacional

- `SYSTEM_OS_BUILD`
- `device.SYSTEM_OS_BUILD`

Edição do sistema operacional

- `OS_EDITION`
- `device.OS_EDITION`

Idioma do sistema operacional (local)

- `SYSTEM_LANGUAGE`
- `device.SYSTEM_LANGUAGE`

Versão do sistema operacional

- `SYSTEM_OS_VERSION`
- `device.SYSTEM_OS_VERSION`

Endereço da organização

- ORGANIZATION_ADDRESS
- \${device.ORGANIZATION_ADDRESS}

Email da organização

- ORGANIZATION_EMAIL
- \${device.ORGANIZATION_EMAIL}

Magic da organização

- ORGANIZATION_MAGIC
- \${device.ORGANIZATION_MAGIC}

Nome da organização

- ORGANIZATION_NAME
- \${device.ORGANIZATION_NAME}

Número de telefone da organização

- ORGANIZATION_PHONE
- \${device.ORGANIZATION_PHONE}

Fora de conformidade

- OUT_OF_COMPLIANCE
- \${device.OUT_OF_COMPLIANCE}

Propriedade

- CORPORATE_OWNED
- \${device.CORPORATE_OWNED}

Código secreto em conformidade

- PASSCODE_IS_COMPLIANT
- \${device.PASSCODE_IS_COMPLIANT}

Código secreto em conformidade com a configuração

- PASSCODE_IS_COMPLIANT_WITH_CFG
- \${device.PASSCODE_IS_COMPLIANT_WITH_CFG}

Código secreto presente

- PASSCODE_PRESENT
- \${device.PASSCODE_PRESENT}

PCR0

- WINDOWS_HAS_PCR0
- \${device.WINDOWS_HAS_PCR0}

Violação do perímetro

- GPS_PERIMETER_BREACH
- \${device.GPS_PERIMETER_BREACH}

Verificação periódica

- PerformPeriodicCheck
- \${device.PerformPeriodicCheck}

Ponto de acesso pessoal ativado

- PERSONAL_HOTSPOT_ENABLED
- \${device.PERSONAL_HOTSPOT_ENABLED}

Código PIN para geocerca

- PIN_CODE_FOR_GEO_FENCE
- \${device.PIN_CODE_FOR_GEO_FENCE}

Plataforma

- SYSTEM_PLATFORM
- \${device.SYSTEM_PLATFORM}

Nível de plataforma API

- API_LEVEL
- \${device.API_LEVEL}

Nome da política

- POLICY_NAME
- \${device.POLICY_NAME}

Número de telefone principal

- IDENTITY1_PHONENUMBER
- \${device.IDENTITY1_PHONENUMBER}

Operadora de prestadora de SIM primário

- IDENTITY1_CARRIER_NETWORK_OPERATOR
- \${device.IDENTITY1_CARRIER_NETWORK_OPERATOR}

ICCID de SIM principal

- IDENTITY1_ICCID
- \${device.IDENTITY1_ICCID}

Principal IMEI SIM

- IDENTITY1_IMEI

- \${device.IDENTITY1_IMEI}

IMSI de SIM principal

- IDENTITY1_IMSI
- \${device.IDENTITY1_IMSI}

SIM principal em Roaming

- IDENTITY1_ROAMING
- \${device.IDENTITY1_ROAMING}

Conformidade com roaming de SIM primário

- IDENTITY1_ROAMING_COMPLIANCE
- \${device.IDENTITY1_ROAMING_COMPLIANCE}

Nome do produto

- PRODUCT_NAME
- \${device.PRODUCT_NAME}

ID de dispositivo de fornecedor

- PUBLISHER_DEVICE_ID
- \${device.PUBLISHER_DEVICE_ID}

Redefinir contagem

- WINDOWS_HAS_RESET_COUNT
- \${device.WINDOWS_HAS_RESET_COUNT}

Reiniciar contagem

- WINDOWS_HAS_RESTART_COUNT
- \${device.WINDOWS_HAS_RESTART_COUNT}

Modo de segurança ativado?

- WINDOWS_HAS_SAFE_MODE
- \${device.WINDOWS_HAS_SAFE_MODE}

API do Samsung KNOX disponível

- SAMSUNG_KNOX
- \${device.SAMSUNG_KNOX}

Versão de API do Samsung KNOX

- SAMSUNG_KNOX_VERSION
- \${device.SAMSUNG_KNOX_VERSION}

Atestado do Samsung KNOX

- SAMSUNG_KNOX_ATTESTED
- \${device.SAMSUNG_KNOX_ATTESTED}

Data de atualização do atestado do Samsung KNOX

- SAMSUNG_KNOX_ATT_UPDATED_TIME
- \${device.SAMSUNG_KNOX_ATT_UPDATED_TIME}

API Samsung SAFE disponível

- SAMSUNG_MDM
- \${device.SAMSUNG_MDM}

Versão da API do Samsung SAFE

- SAMSUNG_MDM_VERSION
- \${device.SAMSUNG_MDM_VERSION}

Hash SBCP

- WINDOWS_HAS_SBCP_HASH
- \${device.WINDOWS_HAS_SBCP_HASH}

Tela: altura

- SCREEN_HEIGHT
- \${device.SCREEN_HEIGHT}

Tela: número de cores

- SCREEN_NB_COLORS
- \${device.SCREEN_NB_COLORS}

Tela: tamanho

- SCREEN_SIZE
- \${device.SCREEN_SIZE}

Tela: largura

- SCREEN_WIDTH
- \${device.SCREEN_WIDTH}

Tela: Resolução de eixo x

- SCREEN_XDPI
- \${device.SCREEN_XDPI}

Tela: Resolução do eixo Y

- SCREEN_YDPI
- \${device.SCREEN_YDPI}

Número de telefone secundário

- IDENTITY2_PHONENUMBER
- \${device.IDENTITY2_PHONENUMBER}

Operadora de prestadora de SIM secundário

- IDENTITY2_CARRIER_NETWORK_OPERATOR
- \${device.IDENTITY2_CARRIER_NETWORK_OPERATOR}

ICCID de SIM secundário

- IDENTITY2_ICCID
- \${device.IDENTITY2_ICCID}

Secundário IMEI SIM

- IDENTITY2_IMEI
- \${device.IDENTITY2_IMEI}

IMSI de SIM secundário

- IDENTITY2_IMSI
- \${device.IDENTITY2_IMSI}

SIM secundário Roaming

- IDENTITY2_ROAMING
- \${device.IDENTITY2_ROAMING}

Conformidade com roaming de SIM secundário

- IDENTITY2_ROAMING_COMPLIANCE
- \${device.IDENTITY2_ROAMING_COMPLIANCE}

Inicialização segura ativada?

- WINDOWS_HAS_SECURE_BOOT_ENABLED
- \${device.WINDOWS_HAS_SECURE_BOOT_ENABLED}

Status de inicialização segura

- SECURE_BOOT_STATE
- \${device.SECURE_BOOT_STATE}

SecureContainer ativado

- DLP_ACTIVE
- \${device.DLP_ACTIVE}

Nível de patch de segurança

- SYSTEM_SECURITY_PATCH_LEVEL

- `$(device.SYSTEM_SECURITY_PATCH_LEVEL)`

Número de série

- `SERIAL_NUMBER`
- `$(device.SERIAL_NUMBER)`

Com capacidade de SMS

- `IS_SMS_CAPABLE`
- `$(device.IS_SMS_CAPABLE)`

Supervisionado

- `SUPERVISED`
- `$(device.SUPERVISED)`

Motivo da suspensão

- `GOOGLE_AW_DIRECTORY_SUSPENSION_REASON`
- `$(device.GOOGLE_AW_DIRECTORY_SUSPENSION_REASON)`

Status alterado

- `TAMPERED_STATUS`
- `$(device.TAMPERED_STATUS)`

Termos e Condições

- `TERMS_AND_CONDITIONS`
- `$(device.TERMS_AND_CONDITIONS)`

Termos e contrato aceitos?

- `GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS`
- `$(device.GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS)`

Sinalização de teste ativada?

- `WINDOWS_HAS_TEST_SIGNING_ENABLED`
- `$(device.WINDOWS_HAS_TEST_SIGNING_ENABLED)`

Total de RAM

- `MEMORY`
- `$(device.MEMORY)`

Espaço de armazenamento total

- `TOTAL_DISK_SPACE`
- `$(device.TOTAL_DISK_SPACE)`

Versão de TPM

- TPM_VERSION
- \${device.TPM_VERSION}

UDID

- UDID
- \${device.UDID}

Status de controle de conta do usuário

- UAC_STATUS
- \${device.UAC_STATUS}

Agente de usuário

- USER_AGENT
- \${device.USER_AGENT}

Definida pelo usuário #1

- USER_DEFINED_1
- \${device.USER_DEFINED_1}

Definida pelo usuário #2

- USER_DEFINED_2
- \${device.USER_DEFINED_2}

Definida pelo usuário #3

- USER_DEFINED_3
- \${device.USER_DEFINED_3}

Idioma do usuário (local)

- USER_LANGUAGE
- \${device.USER_LANGUAGE}

Fornecedor

- VENDOR
- \${device.VENDOR}

Com capacidade de voz

- IS_VOICE_CAPABLE
- \${device.IS_VOICE_CAPABLE}

Roaming de voz permitido

- VOICE_ROAMING_ENABLED
- \${device.VOICE_ROAMING_ENABLED}

VSM ativado?

- WINDOWS_HAS_VSM_ENABLED
- \${device.WINDOWS_HAS_VSM_ENABLED}

Endereço MAC WiFi

- WIFI_MAC
- \${device.WIFI_MAC}

WINDOWS_ENROLLMENT_KEY

- WINDOWS_ENROLLMENT_KEY
- \${device.WINDOWS_ENROLLMENT_KEY}

WinPE ativado?

- WINDOWS_HAS_WINPE
- \${device.WINDOWS_HAS_WINPE}

Status de notificação WNS

- PROPERTY_WNS_PUSH_STATUS
- \${device.PROPERTY_WNS_PUSH_STATUS}

URL de notificação WNS

- PROPERTY_WNS_PUSH_URL
- \${device.PROPERTY_WNS_PUSH_URL}

Data de expiração da URL de notificação WNS

- PROPERTY_WNS_PUSH_URL_EXPIRY
- \${device.PROPERTY_WNS_PUSH_URL_EXPIRY}

ID de agente do XenMobile

- ENROLLMENT_AGENT_ID
- \${device.ENROLLMENT_AGENT_ID}

Revisão de agente do XenMobile

- EW_REVISION
- \${device.EW_REVISION}

Versão do agente XenMobile

- EW_VERSION
- \${device.EW_VERSION}

Zebra API disponível

- ZEBRA_MDM

- `${device.ZEBRA_MDM}`

Versão do MXMF Zebra

- ZEBRA_MDM_VERSION
- `${device.ZEBRA_MDM_VERSION}`

Versão do patch Zebra

- ZEBRA_PATCH_VERSION
- `${device.ZEBRA_PATCH_VERSION}`

Macros para obter as propriedades internas de usuário

Nome de exibição	Macros
domainname (nome de domínio; domínio padrão)	<code>\${ user.domainname }</code>
loginname (nome de usuário mais nome de domínio)	<code>\${ user.loginname }</code>
username (nome de login menos o domínio, se houver)	<code>\${ user.username }</code>

Macros para todas as propriedades de usuário

Nome de exibição	Elemento da Web	Macros
Tentativas de login do Active Directory com falha	badpwdcount	<code>\${ user.badpwdcount }</code>
Email de usuário do ActiveSync	asuseremail	<code>\${ user.asuseremail }</code>
Origem de dados ASM	asmpersonsource	<code>\${ user.asmpersonsource }</code>
Nome de conta DEP ASM	asmdepaccount	<code>\${ user.asmdepaccount }</code>
ID gerenciada da Apple ASM	asmpersonmanagedappleid	<code>\${ user.asmpersonmanagedappleid }</code>

Nome de exibição	Elemento da Web	Macros
Tipo de código de acesso ASM	asmpersonpasscodetype	<code>#{ user. asmpersonpasscodetype }</code>
ID pessoal ASM	asmpersonid	<code>#{ user.asmpersonid }</code>
Status pessoal ASM	asmpersonstatus	<code>#{ user. asmpersonstatus }</code>
Título pessoal ASM	asmpersontitle	<code>#{ user.asmpersontitle }</code>
ID exclusivo pessoal ASM	asmpersonuniqueid	<code>#{ user. asmpersonuniqueid }</code>
ID de sistema de origem ASM	asmpersonsourcesystemid	<code>#{ user. asmpersonsourcesystemid }</code>
Nível escolar de status ASM	asmpersongrade	<code>#{ user.asmpersongrade }</code>
Email de usuário de BES	besuseremail	<code>#{ user.besuseremail }</code>
Empresa	company	<code>#{ user.company }</code>
Nome da empresa	companyname	<code>#{ user.companyname }</code>
País	c	<code>#{ user.c }</code>
Departamento	department	<code>#{ user.department }</code>
Descrição	description	<code>#{ user.description }</code>
Usuário desativado	disableduser	<code>#{ user.disableduser }</code>
Nome de exibição	displayname	<code>#{ user.displayname }</code>
Nome distinto	distinguishedname	<code>#{ user. distinguishedname }</code>
Nome de domínio	domainname	<code>#{ user.domainname }</code>
E-mail	mail	<code>#{ user.mail }</code>
Nome	givenname	<code>#{ user.givenname }</code>
Endereço (residencial)	homestreetaddress	<code>#{ user. homestreetaddress }</code>
Cidade (residencial)	homecity	<code>#{ user.homecity }</code>
País (residencial)	homecountry	<code>#{ user.homecountry }</code>

Nome de exibição	Elemento da Web	Macros
Fax (residencial)	homefax	<code>\${ user.homefax }</code>
Telefone (residencial)	homephone	<code>\${ user.homephone }</code>
Estado/região (residencial)	homestate	<code>\${ user.homestate }</code>
CEP (residencial)	homezip	<code>\${ user.homezip }</code>
Telefone IP	iphone	<code>\${ user.ipphone }</code>
Inicial do meio	middleinitial	<code>\${ user.middleinitial }</code>
Segundo nome	middlename	<code>\${ user.middlename }</code>
Celular	mobile	<code>\${ user.mobile }</code>
Nome	cn	<code>\${ user.cn }</code>
Endereço (comercial)	physicaldeliveryofficename	<code>\${ user.physicaldeliveryofficename }</code>
Cidade (comercial)	l	<code>\${ user.l }</code>
Número de fax (comercial)	facsimiletelephonenumber	<code>\${ user.facsimiletelephonenumber }</code>
Estado/província (comercial)	st	<code>\${ user.st }</code>
Endereço (comercial)	officestreetaddress	<code>\${ user.officestreetaddress }</code>
Número de telefone (comercial)	telephonenumber	<code>\${ user.telephonenumber }</code>
Código postal (comercial)	postalcode	<code>\${ user.postalcode }</code>
Caixa postal	postofficebox	<code>\${ user.postofficebox }</code>
Pager	pager	<code>\${ user.pager }</code>
ID de grupo primário	primarygroupid	<code>\${ user.primarygroupid }</code>
Conta SAM	samaccountname	<code>\${ user.samaccountname }</code>
Endereço	streetaddress	<code>\${ user.streetaddress }</code>

Nome de exibição	Elemento da Web	Macros
Sobrenome	sn	<code>\${ user.sn }</code>
Título	title	<code>\${ user.title }</code>
Nome de login do usuário	userprincipalname	<code>\${ user. userprincipalname }</code>

Ações automatizadas

May 6, 2021

Você pode criar ações automatizadas no XenMobile para programar uma reação aos eventos, às propriedades do usuário ou dispositivo ou à existência de aplicativos em dispositivos de usuário. Quando você cria uma ação automatizada, os gatilhos definidos para a ação determinam o que acontece no dispositivo do usuário quando ele é conectado ao XenMobile. Quando um evento é disparado, você pode enviar uma notificação para o usuário corrigir um problema, antes que medidas mais sérias sejam necessárias.

Os efeitos que você define para acontecer automaticamente variam entre os seguintes:

- Limpar o dispositivo de forma total ou seletiva.
- Definir o dispositivo como fora de conformidade.
- Revogar o dispositivo.
- Enviar uma notificação para o usuário corrigir um problema, antes que medidas mais sérias sejam necessárias.

Você pode configurar ações de bloqueio de aplicativo e apagamento de aplicativos para o modo Somente MAM.

Nota:

Antes de poder notificar os usuários, você deve configurar os servidores de notificação nas configurações do XenMobile como SMTP e SMS para que o XenMobile possa enviar as mensagens. Para obter informações, consulte [Notificações](#). Além disso, configure todos os modelos de notificação que planeja usar antes de prosseguir. Para obter detalhes, consulte [Criar e atualizar modelos de notificação](#).

Exemplo de ações

Aqui estão alguns exemplos de uso de ações automatizadas:

Exemplo 1

- Você deseja detectar um aplicativo que bloqueou anteriormente (por exemplo, “Words with Friends”). Você pode especificar um gatilho que define o dispositivo do usuário como sem conformidade após detectar o aplicativo “Words with Friends”. A ação os notifica que eles devem remover o aplicativo para que o dispositivo esteja novamente em conformidade. Você também pode definir um limite de tempo para aguardar a conformidade dos usuários. Após esse limite de tempo, ocorre uma ação definida, como o apagamento seletivo do dispositivo.

Exemplo 2

- Você deseja verificar se os clientes estão usando o firmware mais recente e bloquear o acesso aos recursos se os usuários precisam atualizar seus dispositivos. Você pode especificar um gatilho que define o dispositivo do usuário como sem conformidade quando o dispositivo de um usuário não tem a versão mais recente. Você usa ações automatizadas para bloquear recursos e notificar os clientes.

Exemplo 3

- Um dispositivo de usuário é colocado como no estado sem conformidade e o usuário corrige o dispositivo. Você pode configurar uma política para implantar um pacote que redefina o dispositivo para um estado compatível.

Exemplo 4

- Você deseja marcar dispositivos de usuário que estiveram inativos por um determinado período de tempo como sem conformidade. Você pode criar uma ação automatizada para dispositivos inativos da seguinte forma:
 1. No console XenMobile, vá para **Configurações > Controle de acesso da rede** e selecione **Dispositivos inativos**. Para obter mais informações sobre a configuração **Dispositivos inativos**, consulte [Controle de Acesso da Rede](#).
 2. Siga as etapas para adicionar uma ação, conforme descrito em [Adicionar e gerenciar ações](#). A única diferença é que você define as configurações da seguinte forma na página **Detalhes da ação**:
 - **Gatilho**. Selecione **Propriedade de dispositivo, Sem conformidade e Verdadeiro**.
 - **Ação**. Selecione **Enviar notificação** e selecione o modelo que você criou usando **Modelo de notificação** em **Configurações**. Em seguida, defina o atraso em dias, horas ou minutos antes de executar a ação. Defina o intervalo durante o qual a ação se repete até que o usuário resolva o problema de gatilho.

Dica:

Para excluir dispositivos inativos em massa, use [Public API for REST Services](#). Primeiro, obtenha manualmente o ID de dispositivo dos dispositivos inativos que deseja excluir e, em seguida, execute a API de exclusão para excluí-los em massa.

Adicionar e gerenciar ações

Para adicionar, editar e filtrar ações automatizadas:

1. No console XenMobile, clique em **Configurar > Ações**. A página **Ações** é exibida.
2. Na página **Ações**, siga um destes procedimentos:
 - Clique em **Adicionar** para adicionar uma ação.
 - Selecione uma ação existente para editar ou excluir. Clique na opção desejada.
3. A página **Informações sobre a ação** é exibida.
4. Na página **Informações sobre a ação**, insira ou modifique as seguintes informações:
 - **Nome:** digite um nome para identificar a ação. Este campo é obrigatório.
 - **Descrição:** descreva a finalidade da ação.
5. Clique em **Avançar**. A página **Detalhes da ação** é exibida.

O exemplo a seguir mostra como definir um gatilho de **Evento**. Se você selecionar um gatilho diferente, as opções resultantes serão diferentes daquelas mostradas aqui.

The screenshot displays the 'Action details' configuration page in the XenMobile console. On the left, a sidebar lists navigation options: 'Actions', '1 Action Info', '2 Details' (highlighted), '3 Assignment (optional)', and '4 Summary'. The main content area is titled 'Action details' and includes a sub-header 'Choose a trigger event and the associated action for that event.' Below this, there are two dropdown menus: 'Trigger*' with 'Select a trigger' and 'Action*' with 'Select an action'. A 'Summary' section shows a conditional logic template: 'If **CONDITION IS FULFILLED**, then **DO ACTION**.' At the bottom, a list of deployment rules is shown with expandable arrows: 'Deployment Rules (iOS)', 'Deployment Rules (macOS)', 'Deployment Rules (Android)', 'Deployment Rules (Windows Mobile/CE)', 'Deployment Rules (Windows Desktop/Tablet)', and 'Deployment Rules (Windows Phone)'.

6. Na página **Detalhes da ação**, insira ou modifique as seguintes informações:

Na lista **Gatilho**, clique no tipo de gatilho de evento para esta ação. O significado de cada gatilho é o seguinte:

- **Evento:** reage a um evento predefinido.
- **Propriedade de dispositivo:** verifica se há um atributo de dispositivo em um dispositivo gerenciado por MDM e, em seguida, reage a ele. Para obter mais informações, consulte [Nomes de propriedade do dispositivo e os valores](#).
- **Propriedade do usuário:** reage a um atributo de usuário, geralmente do Active Directory.

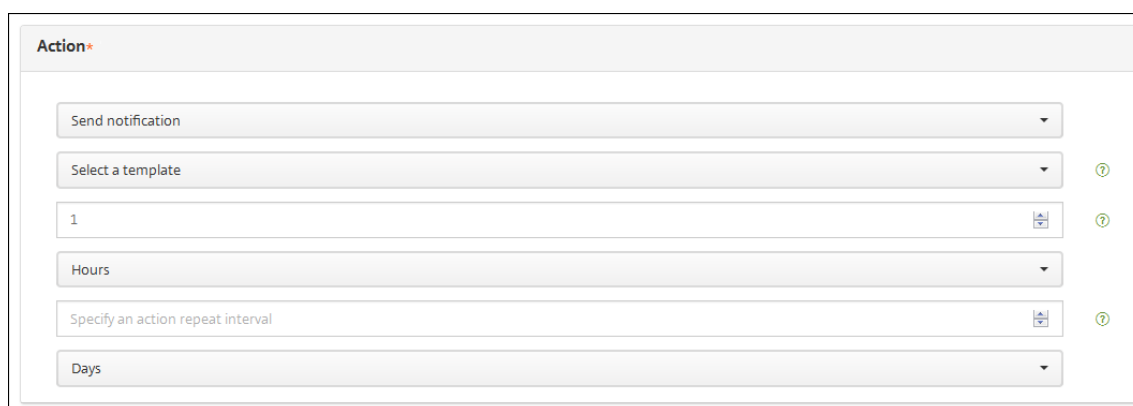
- **Nome do aplicativo instalado:** reage a um aplicativo que está sendo instalado. Não se aplica ao modo somente MAM. Requer que a política de inventário de aplicativos esteja ativada no dispositivo. A política de inventário de aplicativos está ativada em todas as plataformas por padrão. Para obter detalhes, consulte [Política de dispositivo de inventário de aplicativos](#).

7. Na próxima lista, clique na resposta para o gatilho.
8. Na lista **Ação**, clique na ação a ser executada quando o critério de gatilho é atendido. Com exceção da opção **Enviar notificação**, você escolhe um período durante o qual os usuários podem resolver o problema que causou o gatilho. Se o problema não for resolvido nesse período, a ação selecionada será tomada. Para obter uma definição das ações, consulte [Ações de segurança](#).

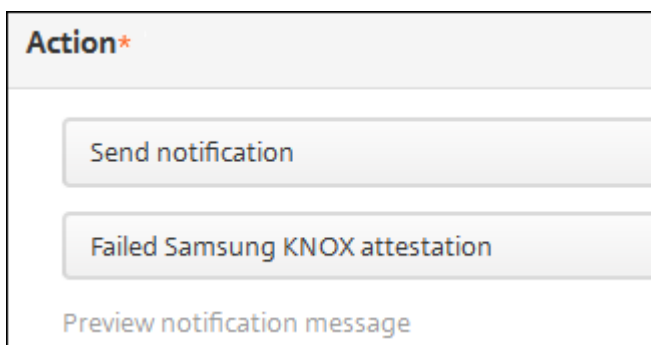
Se você selecionar **Enviar notificação**, use as etapas a seguir para enviar uma ação de notificação.

9. Na próxima lista, selecione o modelo a ser usado para a notificação. São exibidos modelos de notificação relevantes para o evento selecionado, a menos que ainda não exista um modelo para o tipo de notificação. Nesse caso, você receberá um aviso para configurar um modelo com a mensagem: Nenhum modelo para este tipo de evento. Crie o modelo usando **Modelo de Notificação** em **Configurações**.

Antes de poder notificar os usuários, você deve configurar os servidores de notificação em Configurações para SMTP e SMS para que o XenMobile possa enviar as mensagens, consulte [Notificações](#). Além disso, configure todos os modelos de notificação que planeja usar antes de prosseguir. Para obter detalhes sobre a configuração de modelos de notificação, consulte [Criar e atualizar modelos de notificação](#).



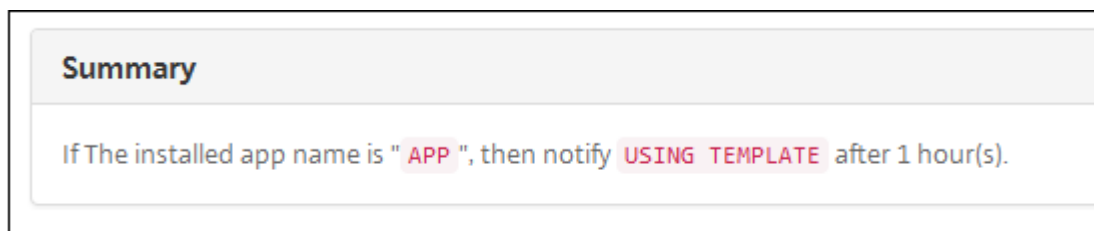
Depois de selecionar o modelo, você poderá visualizar a notificação clicando em **Visualizar mensagem de notificação**.



10. Nos campos a seguir, defina o atraso em dias, horas ou minutos antes de executar a ação. Defina o intervalo durante o qual a ação se repete até que o usuário resolva o problema de gatilho.



11. Em **Resumo**, verifique se você criou a ação automatizada como desejado.



12. Depois de configurar os detalhes da ação, você pode configurar as regras de implantação de cada plataforma individualmente. Para fazer isso, conclua a etapa 13 para cada plataforma desejada.
13. Configure as regras de implantação Para obter informações gerais sobre como configurar as regras de implantação, incluindo ilustrações, consulte [Implantar recursos](#).

Para este exemplo:

- A propriedade do dispositivo deve ser **BYOD**.
 - A criptografia local do dispositivo deve ser **True**.
 - O dispositivo deve ser compatível com código secreto.
 - O MCC do dispositivo não pode ser apenas Andorra.
14. Quando você terminar de definir as regras de implantação para a ação de plataforma, clique em **Avançar**. A página de **Atribuição de ações** é exibida, onde você pode atribuir a ação a um grupo ou grupos de entrega. Essa etapa é opcional.
15. Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega ou selecione

grupos na lista. Os grupos que você selecionar aparecerão na lista **Grupos de entrega que receberão a atribuição de aplicativos**.

16. Expanda Cronograma de implantação e defina estas configurações:
 - Ao lado de **Implantar**, clique em **I** para agendar a implantação ou em **O** para impedi-la. A opção padrão é **I**. Se você escolher **OFF**, nenhuma outra opção será necessária.
 - Ao lado do **Cronograma de implantação**, clique em **Agora** ou **Mais tarde**. A opção padrão é **Agora**.
 - Se você clicar em **Mais tarde**, clique no ícone de calendário e selecione a data e a hora da implantação.
 - Ao lado de **Condição de implantação**, clique em **Em cada conexão** ou em **Somente quando a implantação anterior tiver falhado**. A opção padrão é **Em cada conexão**.
 - Ao lado de **Implantar para conexões permanentes**, clique em **I** ou **O**. A opção padrão é **O**.

Essa opção será aplicável quando você tiver configurado a chave de implantação em segundo plano do cronograma em **Configurações > Propriedades do servidor**. A opção sempre conectada não está disponível para dispositivos iOS.

O cronograma de implantação que você configura é o mesmo para todas as plataformas. Todas as alterações feitas se aplicam a todas as plataformas, exceto **Implantar para conexões permanentes**, que não se aplica ao iOS.

17. Clique em **Avançar**. A página **Resumo** é exibida, onde você pode verificar a configuração da ação.
18. Clique em **Salvar** para salvar a ação.

Ações Bloqueio de aplicativo e Apagamento de aplicativos do modo somente MAM

Você pode apagar ou bloquear aplicativos em um dispositivo em resposta a todas as quatro categorias de gatilhos listadas no console XenMobile: evento, propriedade de dispositivo, propriedade do usuário e o nome do aplicativo instalado.

Para configurar o apagamento ou bloqueio de aplicativos automático

1. No console XenMobile, clique em **Configurar > Ações**.
2. Na página **Ações**, clique em **Adicionar**.
3. Na página **Informações sobre a ação**, insira um nome para a ação e uma descrição opcional.
4. Na página **Detalhes da Ação**, selecione o gatilho que você desejar.

5. Em **Ação**, selecione uma ação.

Para essa etapa, lembre-se as condições a seguir:

Quando o tipo de gatilho é **Evento** e o valor não é de **usuário desativado do Active Directory**, as ações de **Apagamento de aplicativo** e **Bloqueio de aplicativo** não são exibidas.

Quando o tipo de gatilho for **Propriedade do dispositivo** e o valor for **Modo MDM Perdido ativado**, não serão exibidas as seguintes ações:

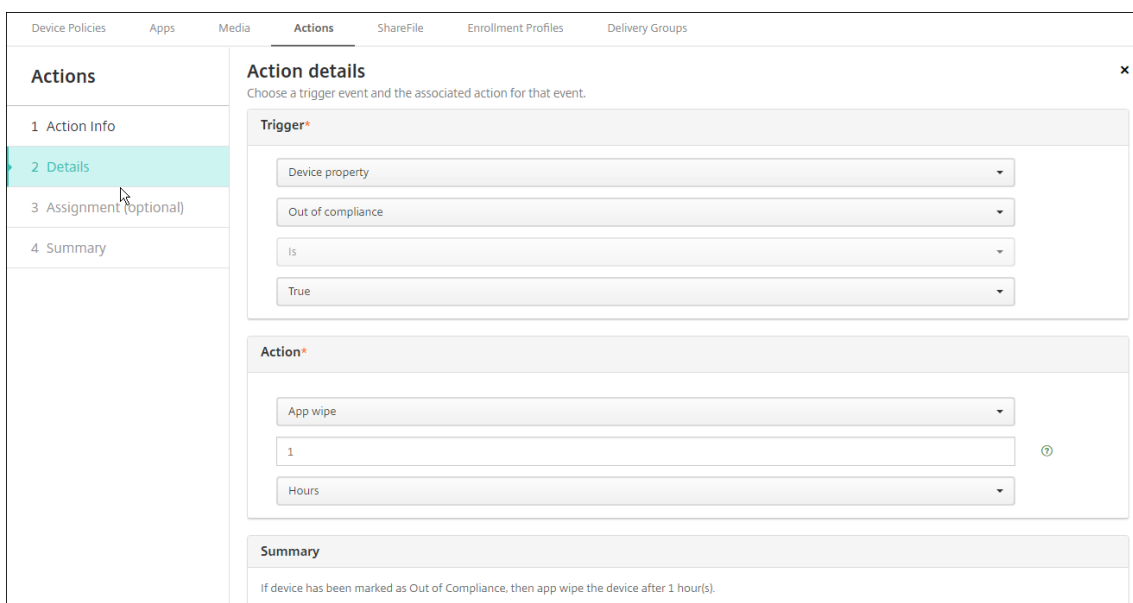
- Apagar seletivamente o dispositivo
- Apagar completamente o dispositivo
- Revogar o dispositivo

Para cada opção, um atraso de uma hora é definido automaticamente, mas você pode selecionar o período de atraso em minutos, horas ou dias. A intenção do atraso é dar aos usuários tempo para corrigir um problema antes que a ação ocorra. Para obter mais informações sobre as ações de apagamento de aplicativos e bloqueio de aplicativos, consulte [Ações de segurança](#).

Nota:

Se você definir o gatilho como **evento**, o intervalo de repetir automaticamente é um mínimo de 1 hora. O dispositivo deve executar uma atualização de políticas para sincronizar com o servidor de notificação para entrar. Normalmente, um dispositivo sincroniza com o servidor quando os usuários fazem logon no ou atualizam manualmente suas políticas através do Secure Hub.

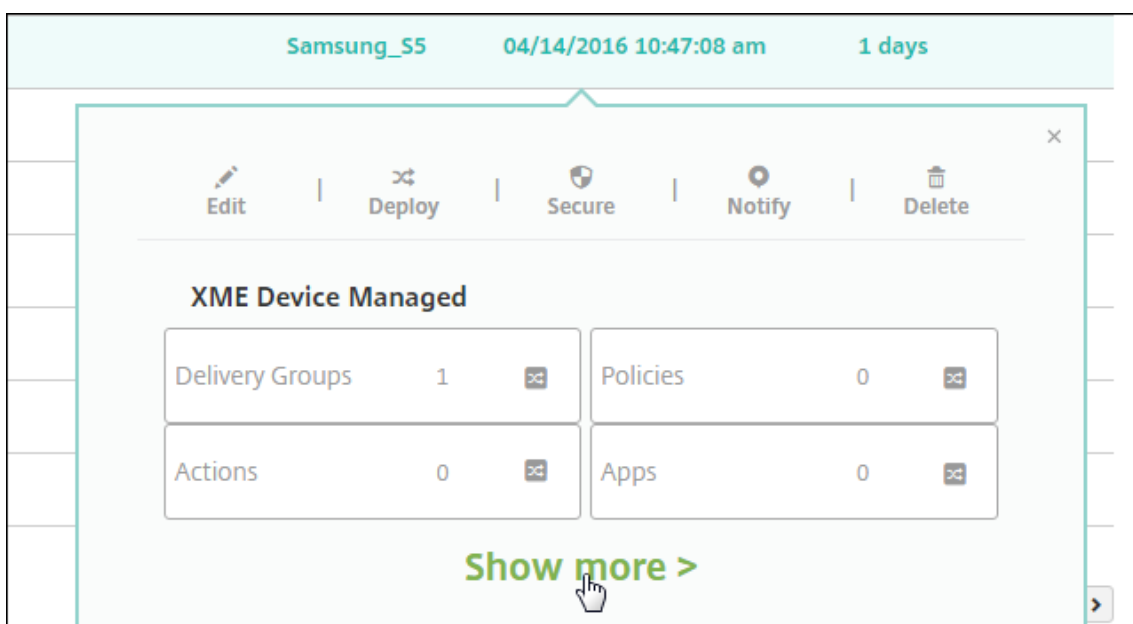
Um atraso extra de aproximadamente uma hora pode ocorrer antes que qualquer ação seja realizada para permitir que o banco de dados do Active Directory seja sincronizado com o XenMobile.



6. Configure as regras de implantação e clique em **Avançar**.
7. Configure as atribuições do grupo de entrega e um cronograma de implantação, e clique em **Avançar**.
8. Clique em **Salvar**.

Para verificar o status do apagamento de aplicativos ou do bloqueio de aplicativo

1. Acesse **Gerenciar > Dispositivos**, clique em um dispositivo e clique em **Mostrar mais**.



2. Role até **Apagamento de aplicativo do dispositivo** e **Bloqueio de aplicativo do dispositivo**.

Device details	
1 General	WiFi MAC Address NONE
2 Properties	Bluetooth MAC Address NONE
3 User Properties	Device Ownership <input type="radio"/> Corporate <input type="radio"/> BYOD
4 Assigned Policies	Security
5 Apps	Strong ID YEMXRMSG
6 Actions	Full Wipe of Device No device wipe.
7 Delivery Groups	Selective Wipe of Device No device selective wipe.
8 Certificates	Lock Device No device lock.
9 Connections	Device locate No device locate.
10 TouchDown	Device App Wipe No device App Wipe.
	Device App Lock App Lock was requested at 04/15/2016 01:59:47 pm.

Depois que um dispositivo for apagado, o usuário será solicitado a inserir um código PIN. Se o usuário esquecer o código, você pode procurá-lo nos Detalhes do dispositivo.

Monitoração e suporte

January 22, 2021

Você pode usar o painel do XenMobile e a página de suporte do XenMobile para monitorar e solucionar problemas do seu XenMobile Server. Use a página Suporte do XenMobile para acessar informações e ferramentas relacionadas a suporte.

Para um XenMobile Server no local, você também pode executar ações a partir da CLI do XenMobile. Para obter detalhes, consulte [Opções da interface de linha de comando](#).

No console XenMobile, clique no ícone de chave inglesa no canto superior direito.



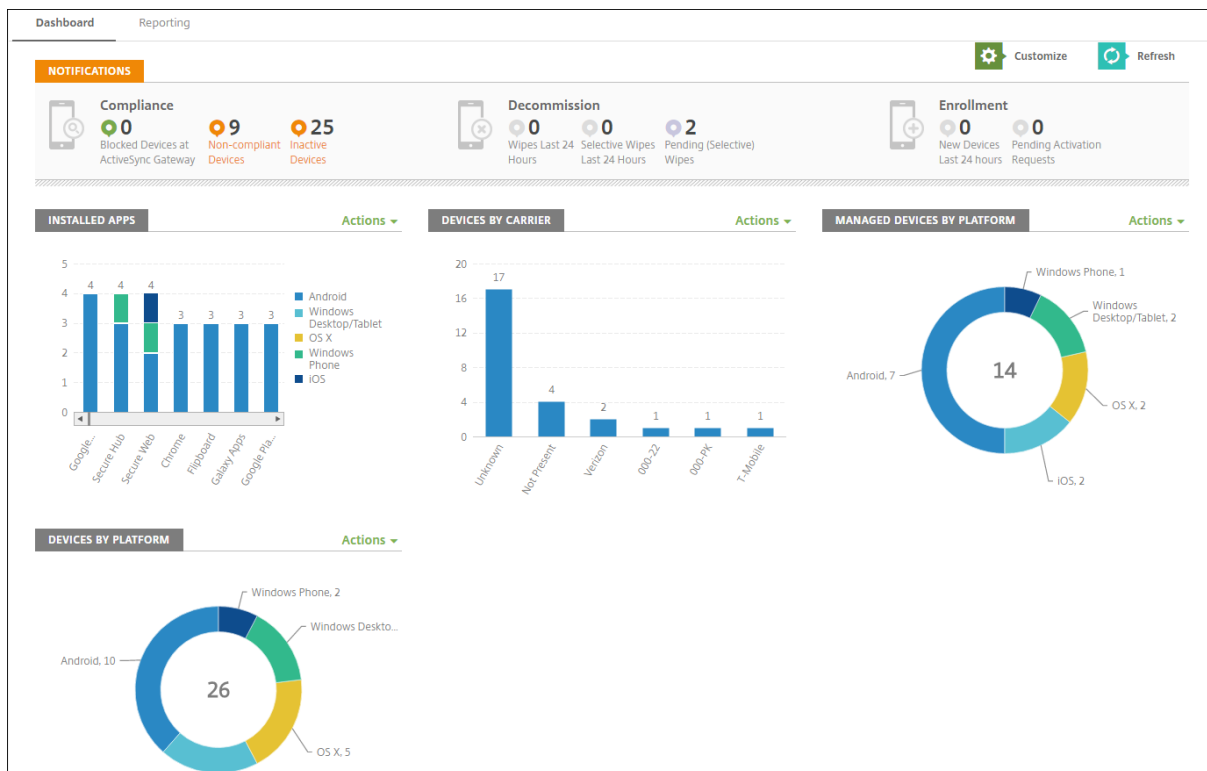
A página Solução de problemas e Suporte é exibida.

Use a página de **Suporte** do XenMobile para:

- Acessar diagnósticos.

- Criar pacotes de suporte (somente para instalações no local).
- Acessar links para a Documentação de produtos Citrix e o Knowledge Center.
- Acessar operações de log.
- Usar as opções de configuração avançada.
- Acessar um conjunto de ferramentas e utilitários.

Você também pode ver informações de resumo acessando o painel do console XenMobile. Com essas informações, você pode ver problemas e operações bem-sucedidas rapidamente usando widgets.



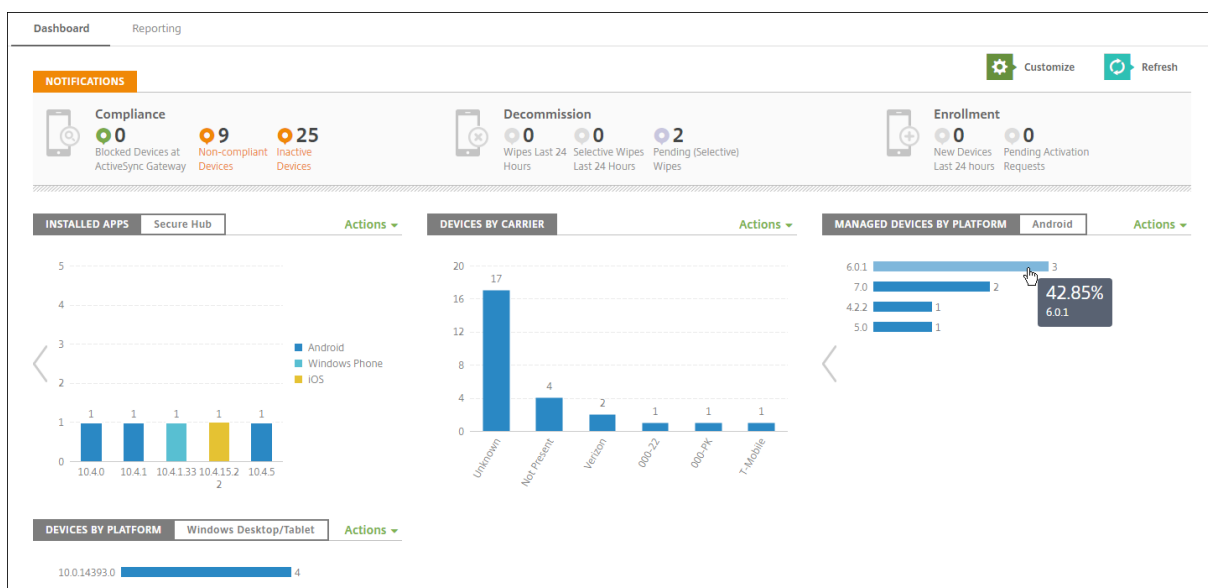
O painel é geralmente a tela que aparece quando você faz logon no console XenMobile. Para acessar o painel de qualquer outro lugar no console, clique em **Analisar**. Clique em **Personalizar** no painel para editar o layout da página e editar os widgets exibidos.

- **Meus painéis:** você pode salvar até quatro painéis. Você pode editar esses painéis separadamente e exibir cada um selecionando o painel salvo.
- **Estilo de layout:** nessa linha você pode selecionar quantos widgets são exibidos no painel e a sua disposição.
- **Seleção de widgets:** você pode escolher as informações que aparecem no painel.
 - **Notificações:** marque a caixa de seleção acima dos números à esquerda para adicionar uma barra de notificações acima dos seus widgets. Esta barra mostra o número de dispositivos compatíveis, dispositivos inativos e dispositivos apagados ou registrados nas últimas 24 horas.
 - **Dispositivos por plataforma:** exibe o número de dispositivos gerenciados e não gerenci-

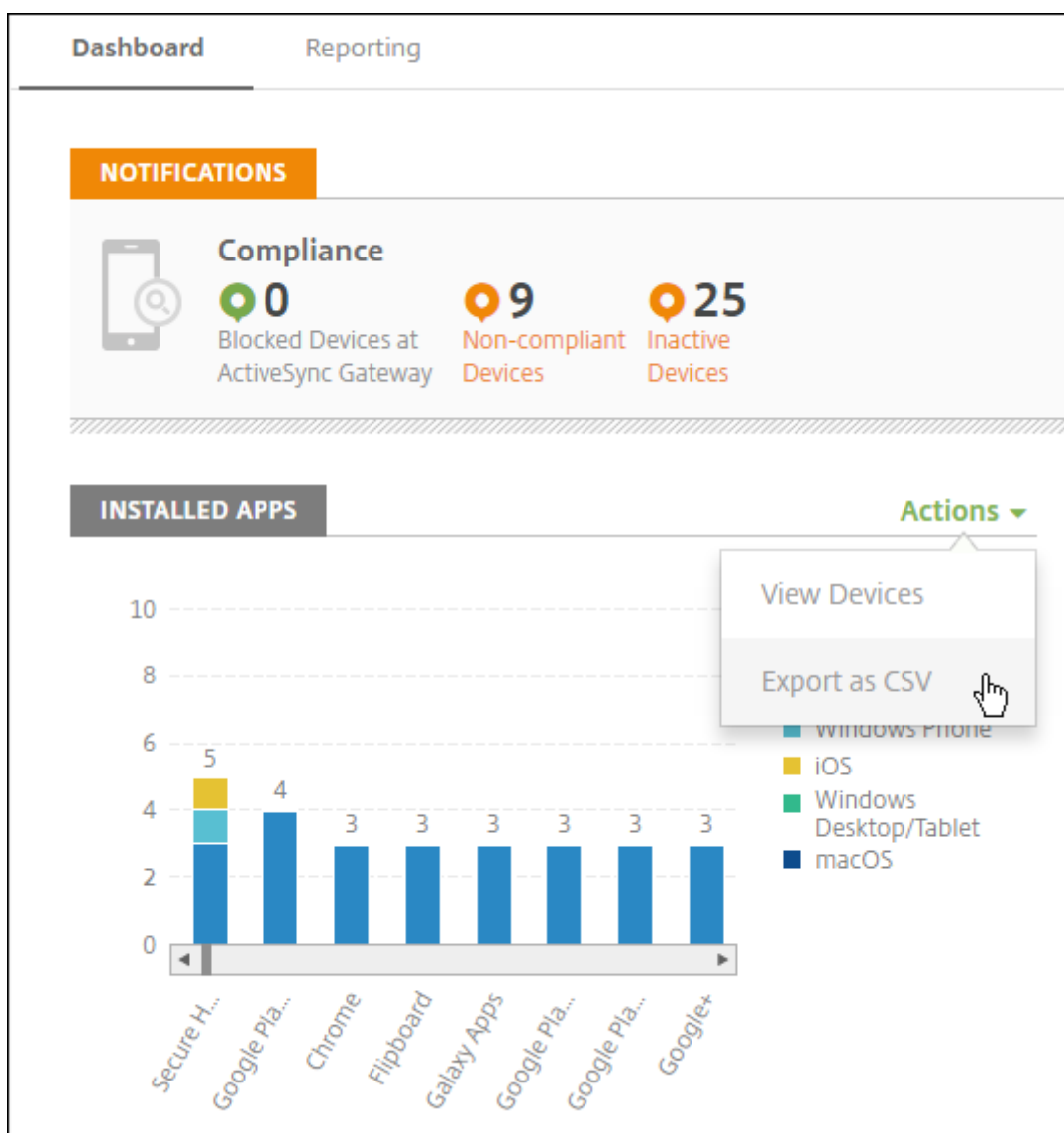
ados por plataforma.

- **Dispositivos por operadora:** exibe o número de dispositivos não gerenciados e gerenciados por operadora. Clique em cada barra para ver um demonstrativo por plataforma.
- **Dispositivos gerenciados por plataforma:** exibe o número de dispositivos gerenciados por plataforma.
- **Dispositivos não gerenciados por plataforma:** exibe o número de dispositivos não gerenciados por plataforma. Os dispositivos exibidos nesse gráfico podem ter um agente instalado, mas tiveram seus privilégios revogados ou foram apagados.
- **Dispositivos por Status do Gateway do ActiveSync:** exibe o número de dispositivos agrupados por status do ActiveSync Gateway. As informações mostram o status Desconhecido, Permitido ou Bloqueado. Você pode clicar em cada barra exibir os dados por plataforma.
- **Dispositivos por propriedade:** exibe o número de dispositivos agrupados por status de propriedade. As informações mostram o status de propriedade de propriedade da empresa, propriedade do funcionário ou desconhecido.
- **Implantações de grupo de entrega com falha:** exibe o número total de falhas de implantação por pacote. Apenas os pacotes que têm falhas de implementação.
- **Dispositivos por motivo de bloqueio:** exibe o número de dispositivos bloqueados pelo ActiveSync
- **Aplicativos instalados:** digite um nome de aplicativo para um gráfico de informações de aplicativos.
- **Uso da licença de aplicativos de compra por volume:** exibe as estatísticas de uso de aplicativos de compra por volume da Apple.

Em cada widget você pode clicar nas partes para analisar mais a fundo para obter mais informações.



Você também pode exportar as informações como um arquivo .csv clicando na lista suspensa **Ação**.



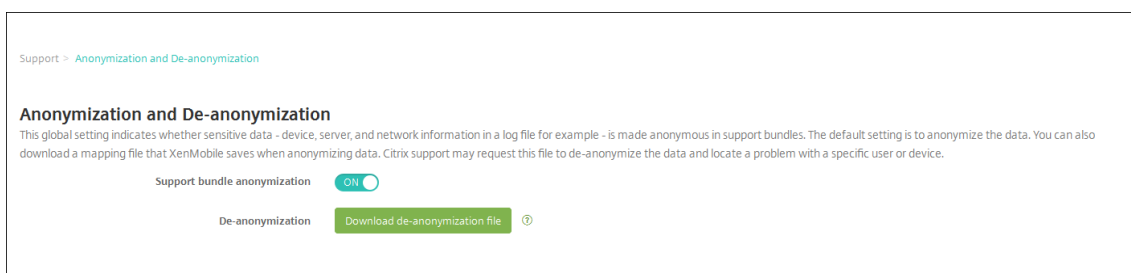
Anonimizar dados nos pacotes de suporte

August 24, 2018

Quando você cria pacotes de suporte no XenMobile, dados confidenciais do usuário, do servidor e da rede são anonimizados por padrão. Você pode alterar esse comportamento na página Anonimização e desanonimização. Você também pode baixar um arquivo de mapeamento que o XenMobile salva quando anonimiza dados. O suporte da Citrix pode solicitar esse arquivo para desanonimizar os dados e localizar um problema com um usuário ou um dispositivo específico.

1. No console XenMobile, clique no ícone de chave inglesa no canto superior direito. A página **Suporte** é exibida.

2. Na página **Suporte**, em **Avançado**, clique em **Anonimização e desanonimização**. A página **Anonimização e desanonimização** é exibida.



3. Em **Anonimização de pacote de suporte**, selecione se os dados serão anonimizados. O padrão é **I**.
4. Ao lado de **Desanonimização**, clique em **Baixar o arquivo de desanonimização** para baixar o arquivo de mapeamento a ser enviado para o suporte Citrix quando eles precisarem de informações específicas do dispositivo ou do usuário para diagnosticar um problema.

Verificações de conectividade

November 30, 2020

Na página **Suporte** do XenMobile, você pode verificar a conexão do XenMobile com o Citrix Gateway e outros servidores e localizações.

Conduzindo verificações de conectividade XenMobile

1. No console XenMobile, clique no ícone de chave de boca no canto superior direito do console. A página **Suporte** é exibida.
2. Em **Diagnósticos**, clique em **Verificações de Conectividade XenMobile**. A página **Verificações de conectividade XenMobile** é exibida. Se o seu ambiente do XenMobile contiver nós de cluster, todos os nós serão mostrados.

Support > XenMobile Connectivity Checks

XenMobile Connectivity Checks

Perform various connectivity checks for XenMobile. A complete check might take several minutes to run before results appear. If you are not using selected features within the console, clear the selections to speed the process.

Perform connectivity checks for [redacted]

<input type="checkbox"/>	Connectivity to	IP address or FQDN	
<input type="checkbox"/>	Windows Phone Store	windowsphone.com	
<input type="checkbox"/>	Database	[redacted].net	
<input type="checkbox"/>	Apple Feedback Push Notification Server	feedback.push.apple.com	
<input type="checkbox"/>	LDAP	[redacted].net	
<input type="checkbox"/>	Domain Name System (DNS)	[redacted]	
<input type="checkbox"/>	Nexmo Gateway	-	
<input type="checkbox"/>	Apple Push Notification Server	gateway.push.apple.com	
<input type="checkbox"/>	iTunes Store/Volume Purchase Program (VPP)	ax.itunes.apple.com	
<input type="checkbox"/>	Google Play	play.google.com	
<input type="checkbox"/>	Windows Security Token Service	login.live.com	

3. Selecione os servidores que você deseja incluir no teste de conectividade e clique em **Testar conectividade**. A página de resultados de teste é exibida.

XenMobile Connectivity Checks

Perform various connectivity checks for XenMobile. A complete check might take several minutes to run before results appear. If you are not using selected features within the console, clear the selections to speed the process.

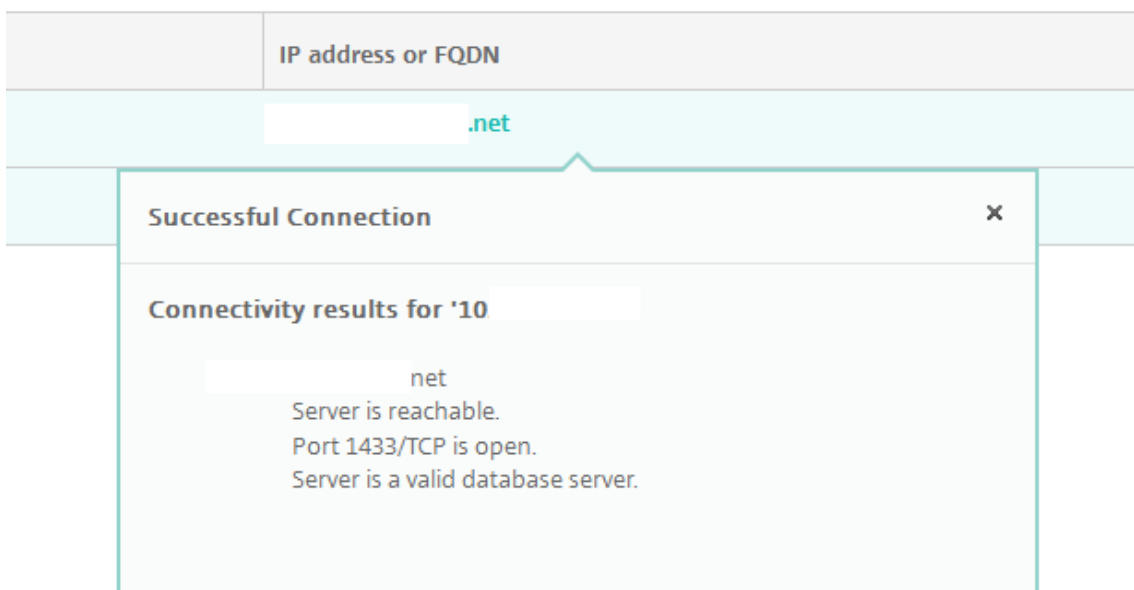
Perform connectivity checks for 10.

<input type="checkbox"/>	Connectivity to	IP address or FQDN	
<input type="checkbox"/>	Database	net	✓
<input type="checkbox"/>	Windows Phone Store	windowsphone.com	✓

Showing 1 - 2 of 2 items

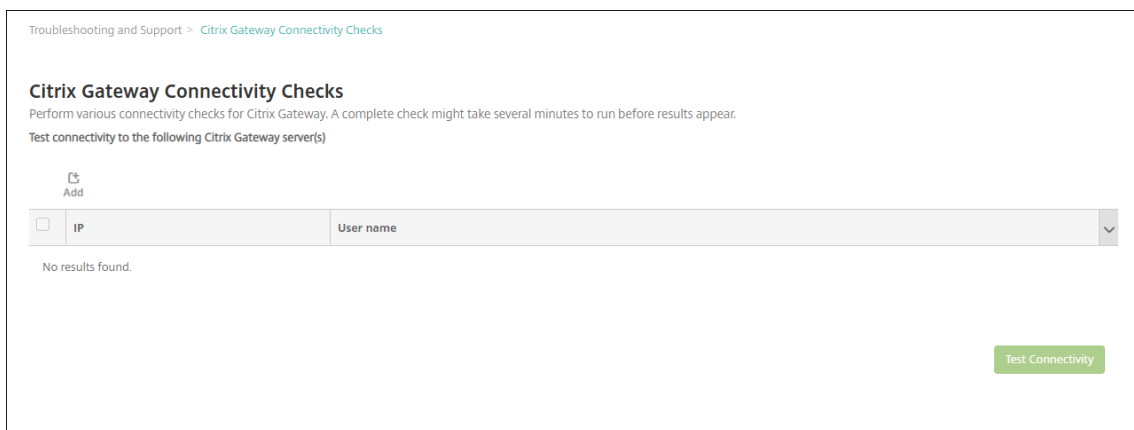
Clear Results Test Connectivity

4. Selecione um servidor na tabela dos resultados do teste para ver os resultados detalhados desse servidor.

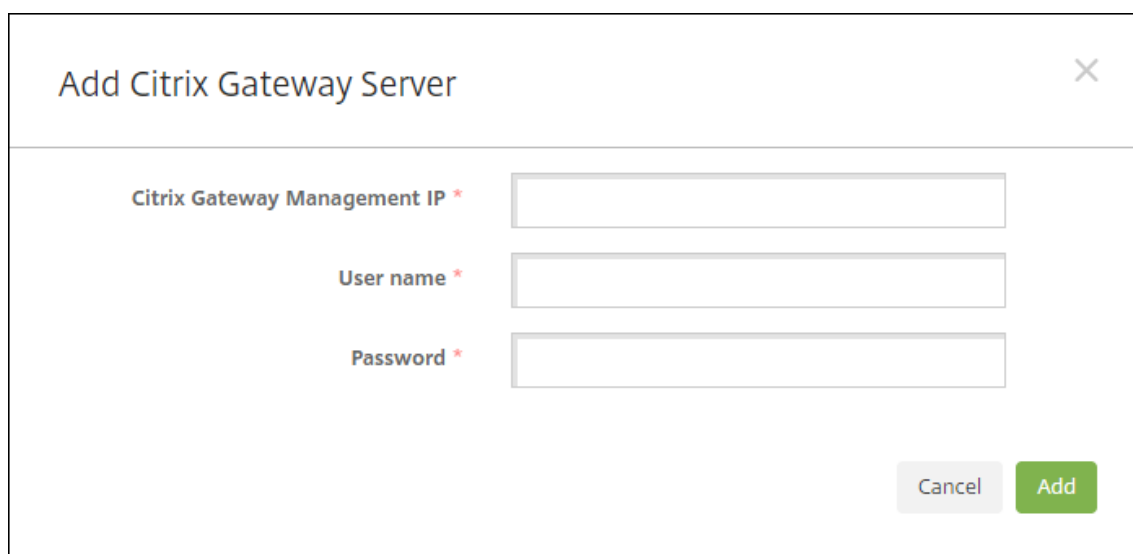


Conduzindo verificações de conectividade do Citrix Gateway

1. Na página **Suporte**, em **Diagnósticos**, clique em **Verificações de conectividade do Citrix Gateway**. A página **Verificações de conectividade do Citrix Gateway** é exibida. A tabela estará vazia se você ainda não tiver adicionado nenhum servidor do Citrix Gateway.



2. Clique em **Adicionar**. A caixa de diálogo **Adicionar Citrix Gateway Server** é exibida.



The screenshot shows a dialog box titled "Add Citrix Gateway Server" with a close button (X) in the top right corner. The dialog contains three input fields, each with a label and an asterisk indicating it is required: "Citrix Gateway Management IP *", "User name *", and "Password *". At the bottom right of the dialog, there are two buttons: "Cancel" and "Add".

3. Em **IP de gerenciamento do Citrix Gateway**, digite o endereço IP do servidor que executa o Citrix Gateway que você deseja testar.

Nota:

Se você estiver conduzindo uma verificação de conectividade para um servidor do Citrix Gateway que já foi adicionado antes, o endereço IP será fornecido.

4. Digite as suas credenciais de administrador para esse Citrix Gateway.

Nota:

Se você estiver conduzindo uma verificação de conectividade para um servidor do Citrix Gateway que já foi adicionado antes, o nome do usuário será fornecido.

5. Clique em **Adicionar**. O Citrix Gateway é adicionado à tabela na página **Verificações de conectividade do Citrix Gateway**.
6. Selecione o servidor do Citrix Gateway e, em seguida, clique em **Testar conectividade**. Os resultados são exibidos em uma tabela de resultados de teste.
7. Selecione um servidor na tabela dos resultados do teste para ver os resultados detalhados desse servidor.

Programa de Melhoria de Experiência do Cliente

October 4, 2018

O Programa de Melhoria de Experiência do Cliente (CEIP) da Citrix reúne dados anônimos de configuração e uso do XenMobile e envia-os automaticamente para a Citrix. Esses dados ajudam a Citrix a

melhorar a qualidade, a confiabilidade e o desempenho do XenMobile. A participação no CEIP é completamente voluntária. Quando você instala o XenMobile ou uma atualização, tem a opção de participar do CEIP. Quando você opta por participar, os dados são geralmente coletados em uma base semanal, e os dados de desempenho e uso são coletados a cada hora. Os dados são armazenados em disco e transferidos com segurança usando HTTPS para a Citrix semanalmente. Você pode alterar se deseja participar do CEIP no console XenMobile. Para obter mais informações sobre o CEIP, consulte [Sobre o programa de melhoria de experiência do cliente \(CEIP\) da Citrix](#).

Como optar para participar do CEIP

Na primeira vez que instalar o XenMobile ou quando fizer uma atualização, você verá a caixa de diálogo a seguir, que pergunta se você deseja participar.

Customer Experience Improvement Program ×

Help improve the quality and performance of Citrix products by sending anonymous statistics and usage information.

How does it work?

- No information that identifies individuals is collected
- Collects only configuration, performance, and reliability data
- Data is stored on disk until it is transferred to Citrix
- Secure weekly transfers via HTTPS to Citrix servers
- Data is immediately deleted from disk after successful transfer

[Learn more](#)

Would you like to help make Citrix products better by joining the program?
(You can go to Configure -> Settings -> More -> Experience Improvement Program to change your answer at any time.)

Yes, send anonymous usage and statistics information.

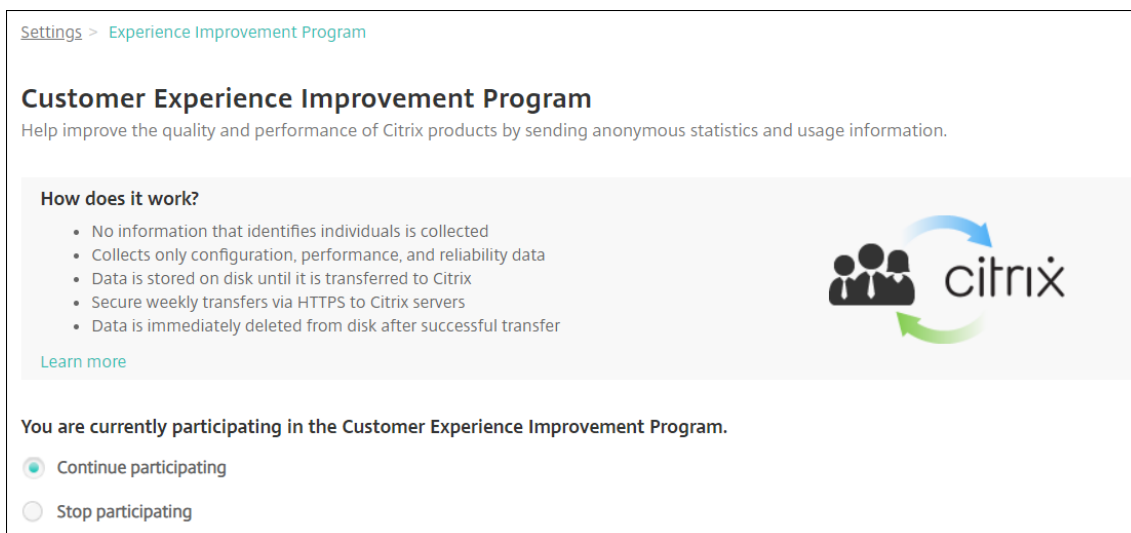
No

Cancel Save

Alterar sua configuração de participação no CEIP

1. Para alterar a sua configuração de participação no CEIP, no console XenMobile, clique no ícone de engrenagem no canto superior direito do console para abrir a página **Configurações**.

2. Em **Servidor**, clique em **Programa de melhoria de experiência**. A página **Programa de melhoria de experiência do cliente** é exibida. A página exata que você vê depende de você estar ou não participando do CEIP no momento.



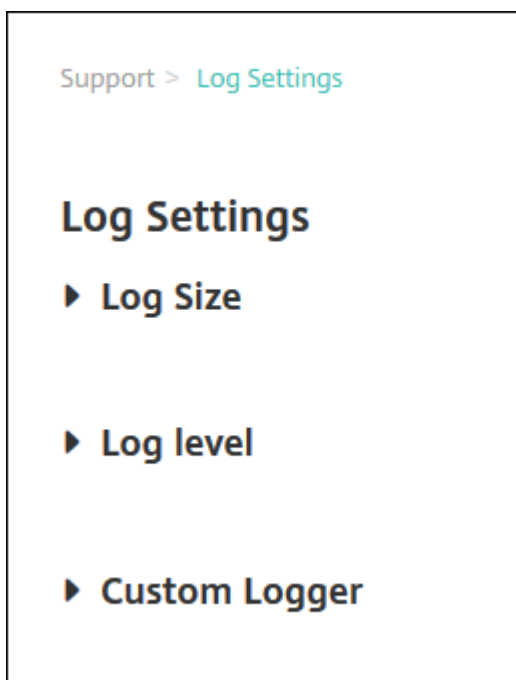
3. Se você participa do CEIP no momento e deseja parar, clique em **Parar participação**.
4. Se você não participa do CEIP no momento e deseja começar, clique em **Começar a participar**.
5. Clique em **Salvar**.

Logs

May 24, 2019

Você pode definir as configurações de log para personalizar a saída dos logs gerados pelo XenMobile. Se você tem servidores XenMobile em cluster, ao definir as configurações de log no console XenMobile, elas são compartilhadas com todos os outros servidores no cluster.

1. No console XenMobile, clique no ícone de chave de boca no canto superior direito do console. A página **Suporte** é exibida.
2. Em **Operações de log**, clique em **Configurações de log**. A página **Configurações de log** é exibida.



Na página **Configurações de log**, você pode acessar as seguintes opções:

- **Tamanho do log.** Use essa opção para controlar o tamanho do arquivo de log e o número máximo de arquivos de backup de log mantidos no banco de dados. O tamanho do log se aplica a cada um dos logs compatíveis com o XenMobile (log de depuração, log de atividades do administrador e log de atividades do usuário).
- **Nível de log.** Use essa opção para alterar o nível de log ou para manter as configurações.
- **Agente de log personalizado.** Use essa opção para criar um agente de log personalizado; os logs personalizados exigem um nome de classe e o nível de log.

Para configurar as opções de Tamanho do Log

1. Na página **Configurações de log**, expanda **Tamanho do log**.

Support > Log Settings

Log Settings

▼ Log Size

Debug log file size (MB)	10
Maximum number of debug backup files	50
Admin activity log file size (MB)	10
Maximum number of admin activity backup files	300
User activity log file size (MB)	10
Maximum number of user activity backup files	600

2. Defina estas configurações:

- **Tamanho de arquivo do log de depuração (MB):** na lista, clique em um tamanho entre 5 MB e 20 MB para alterar o tamanho máximo do arquivo de depuração. O tamanho do arquivo padrão é de **10 MB**.
- **Número máximo de arquivos de backup de depuração:** na lista, clique no número máximo de arquivos de depuração mantidos pelo servidor. Por padrão, o XenMobile mantém 50 arquivos de backup no servidor.
- **Tamanho de arquivo de log das atividades do administrador (MB):** na lista, clique em um tamanho entre 5 MB e 20 MB para alterar o tamanho máximo do arquivo de atividades do administrador. O tamanho do arquivo padrão é de **10 MB**.
- **Número máximo de arquivos de backup das atividades do administrador:** na lista, clique no número máximo de arquivos de atividades do administrador mantidos pelo servidor. Por padrão, o XenMobile mantém 300 arquivos de backup no servidor.
- **Tamanho do arquivo de log das atividades do usuário (MB):** na lista, clique em um tamanho entre 5 MB e 20 MB para alterar o tamanho máximo do arquivo de atividades do usuário. O tamanho do arquivo padrão é de **10 MB**.

- **Número máximo de arquivos de backup das atividades do usuário:** na lista, clique no número máximo de arquivos de atividades do usuário mantidos pelo servidor. Por padrão, o XenMobile mantém 300 arquivos de backup no servidor.

Para configurar as opções de Nível de Log

O nível de log permite especificar quais tipos de informações o XenMobile coleta no log. Você pode definir o mesmo nível para todas as classes ou definir classes individuais para níveis específicos.

1. Na página **Configurações de log**, expanda **Nível de log**. A tabela de todas as classes de log é exibida.

Support > Log Settings

Log Settings

▶ Log Size

▼ Log level

Edit all | Reset

<input type="checkbox"/>	Class	Sub-class	Log level	▼
<input type="checkbox"/>	Data Access	All	Info	
<input type="checkbox"/>	Data Access	XDM	Info	
<input type="checkbox"/>	Data Access	XAM	Info	
<input type="checkbox"/>	Data Access	Console	Info	
<input type="checkbox"/>	Data Access	OCA	Info	
<input type="checkbox"/>	IMI Services	All	Info	
<input type="checkbox"/>	IMI Services	Category Service	Info	
<input type="checkbox"/>	IMI Services	OPN Service	Info	

2. Você pode optar por um dos seguintes procedimentos:

- Clique na caixa de seleção ao lado de uma Classe e, em seguida, clique em **Definir Nível** para alterar apenas o nível de registro dessa classe.
- Clique em **Editar tudo** para aplicar a alteração no nível de log a todas as classes na tabela.

A caixa de diálogo **Definir nível de log** é exibida, na qual você pode definir o nível de log e selecionar se as configurações no nível de log devem persistir ao reinicializar o XenMobile Server.

Set Log Level

Class name Operation

Sub-class name Android Deployment

Log level Info

Included loggers

- com.sparus.nps.ServicesManager
- com.sparus.nps.RegistryPacketBuilder
- com.sparus.nps.engine.business.impl.EngineManager
- com.sparus.nps.SessionManager?

Persist settings

Cancel Set

- **Nome da classe:** esse campo exibirá Todas quando você estiver alterando o nível de log de todas as classes ou exibirá o nome da classe individual; ele não é editável.
- **Nome da subclasse:** esse campo exibirá Todas quando você estiver alterando o nível de log de todas as classes ou exibirá o nome da subclasse individual; ele não é editável.
- **Nível de log:** na lista, clique em um nível de log. Os níveis de log compatíveis incluem:
 - Fatal
 - Erro
 - Aviso
 - Informações
 - Depuração
 - Rastreamento

- Desativado

- **Agentes incluídos:** esse campo estará em branco quando você estiver alterando o nível de log de todas as classes ou exibirá os agentes de log configurados no momento para uma classe individual; ele não é editável.
- **Manter as configurações:** se você desejar que as configurações de nível de log sejam mantidas quando reiniciar o servidor, marque essa caixa de seleção. Não marcar essa caixa de seleção significa que as configurações de nível de log serão revertidas para o padrão quando você reiniciar o servidor.

3. Clique em **Definir** para confirmar as alterações.

Para adicionar um Agente de Log Personalizado

1. Na página **Configurações de log**, expanda **Agente de log personalizado**. A tabela **Agente de log personalizado** é exibida. Se você ainda não tiver adicionado nenhum agente de log personalizado, a tabela estará inicialmente vazia.

Support > Log Settings

Log Settings

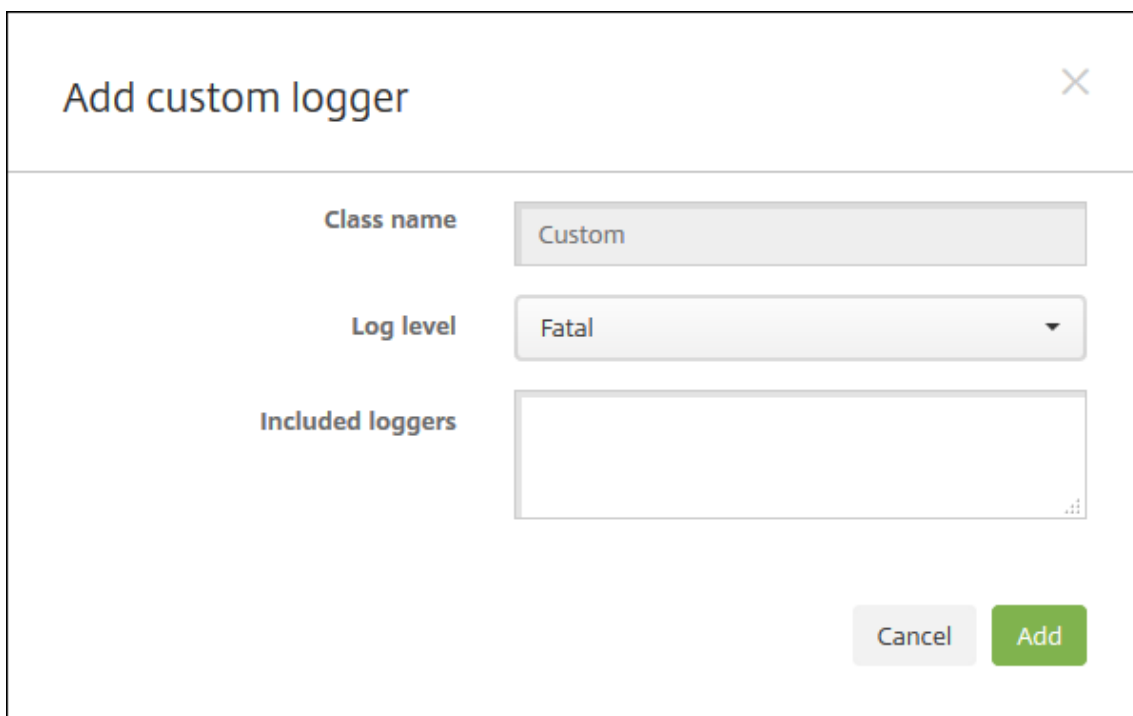
- ▶ Log Size
- ▶ Log level
- ▼ Custom Logger

Add | Set Level | Delete

<input type="checkbox"/>	Class	Logger	Log level	▼
<input type="checkbox"/>	Custom	All	Warning	
<input type="checkbox"/>	Custom	xms.oca.dao.hibernate	Trace	

Showing 1 - 2 of 2 items

2. Clique em **Adicionar**. A caixa de diálogo **Adicionar aplicativo** é exibida.



The screenshot shows a dialog box titled "Add custom logger" with a close button (X) in the top right corner. The dialog contains three main sections:

- Class name:** A text input field containing the word "Custom".
- Log level:** A dropdown menu with "Fatal" selected.
- Included loggers:** A large, empty text area for listing specific loggers.

At the bottom right of the dialog, there are two buttons: "Cancel" (grey) and "Add" (green).

3. Defina estas configurações:

- **Nome da classe:** esse campo exibe **Personalizado**; ele não é editável.
- **Nível de log:** na lista, clique em um nível de log. Os níveis de log compatíveis incluem:
 - Fatal
 - Erro
 - Aviso
 - Informações
 - Depuração
 - Rastreamento
 - Desativado
- **Agentes de log incluídos:** digite os agentes de log específicos que você deseja incluir no agente de log personalizado ou deixe o campo em branco para incluir todos os agentes de log.

4. Clique em **Adicionar**. O agente de log personalizado é adicionado à tabela **Agente de log personalizado**.

<input type="checkbox"/>	Class	Logger	Log level
<input type="checkbox"/>	Custom	All	Warning
<input type="checkbox"/>	Custom	xms.oca.dao.hibernate	Trace

Para excluir um Agente de Log Personalizado

1. Na página **Configurações de log**, expanda **Agente de log personalizado**.
2. Selecione o agente de log personalizado que você deseja excluir.
3. Clique em **Excluir**. Uma caixa de diálogo será exibida perguntando se você deseja excluir o agente de log personalizado. Clique em **OK**.

Importante:

Você não pode desfazer essa operação.

Provedor de serviços móveis

May 24, 2019

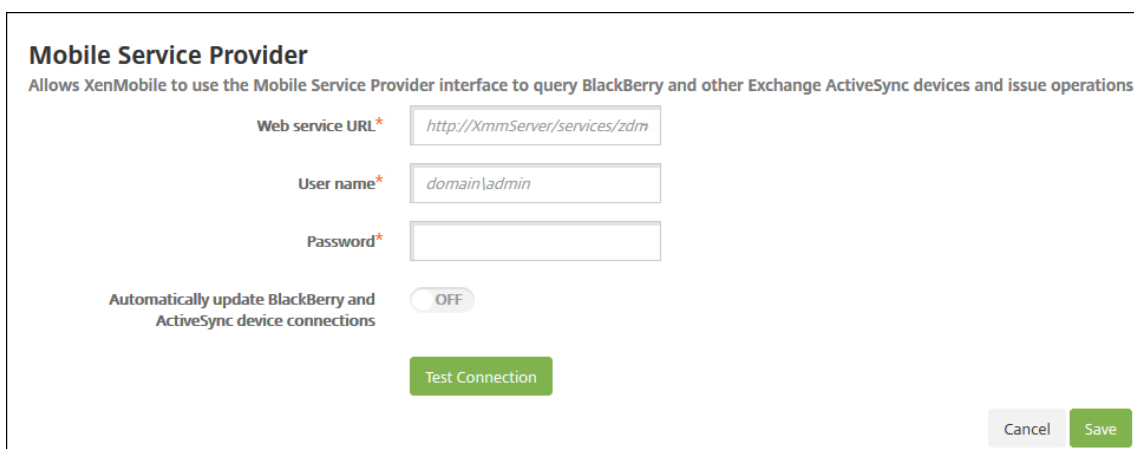
Você pode ativar o XenMobile para usar a interface do Provedor de Serviços Móveis para consultar o BlackBerry e dispositivos Exchange ActiveSync e emitir operações.

Por exemplo, sua empresa pode ter 1.000 usuários e cada usuário pode usar um ou mais dispositivos. Depois de comunicar com cada usuário que ele deve registrar seus dispositivos no XenMobile para gerenciamento, o console XenMobile indica o número de dispositivos que os usuários registram. Ao definir essa configuração, você pode determinar o número de dispositivos que se conectam ao Exchange Server. Desse modo, você pode fazer o seguinte:

- Verifique se algum usuário ainda precisaregistrar o dispositivo.
- Emita comandos para dispositivos de usuário que se conectam ao Exchange Server, como apagamentos de dados.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida.

2. Em **Servidor**, clique em **Provedor de serviços móveis**. A página **Provedor de serviços móveis** é exibida.



3. Defina estas configurações:

- **URL de serviço da Web:** digite a URL do serviço da Web; por exemplo, <https://<XmmServer>/services/xdm-service>
- **Nome de usuário:** digite o nome do usuário no formato domínio\administrador.
- **Senha:** digite a senha.
- **Atualizar automaticamente as conexões de dispositivo BlackBerry e ActiveSync:** selecione se as conexões do dispositivo são atualizadas automaticamente. O padrão é **O**.
- Clique em **Testar conexão** para verificar a conectividade.

4. Clique em **Salvar**.

Relatórios

August 10, 2020

O XenMobile fornece os seguintes relatórios predefinidos que permitem analisar as implantações de aplicativo e dispositivo. Cada relatório é exibido como uma tabela e um gráfico. Você pode classificar e filtrar as tabelas por coluna. Você pode selecionar elementos em gráficos de informações mais detalhadas.

- **Total de tentativas de implantação de aplicativos:** lista aplicativos implantados que os usuários tentaram instalar em seus dispositivos.
- **Aplicativos por Plataforma:** lista os aplicativos e as versões de aplicativo por plataforma e versão do dispositivo.
- **Aplicativos por Tipo:** lista os aplicativos por categoria, tipo e versão.
- **Registro do dispositivo:** lista todos os dispositivos registrados.

- **Dispositivos e aplicativos:** lista os dispositivos que executam os aplicativos gerenciados.
- **Dispositivos inativos:** uma lista de dispositivos que não tiveram atividades durante o número de dias especificado pela propriedade `device.inactivity.days.threshold` do XenMobile Server.
- **Dispositivos com jailbreak/root:** lista dispositivos iOS com jailbreak e dispositivos Android com root.
- **Termos e condições:** lista os usuários que aceitaram e recusaram os acordos de Termos e condições. Você pode selecionar áreas do gráfico para exibir mais detalhes.
- **Os 10 aplicativos mais usados:** falha na implantação: lista até 10 aplicativos cuja implantação falhou.
- **Aplicativos em lista negra por dispositivos e usuário:** lista de aplicativos bloqueados que os usuários têm em seus dispositivos.

Nota:

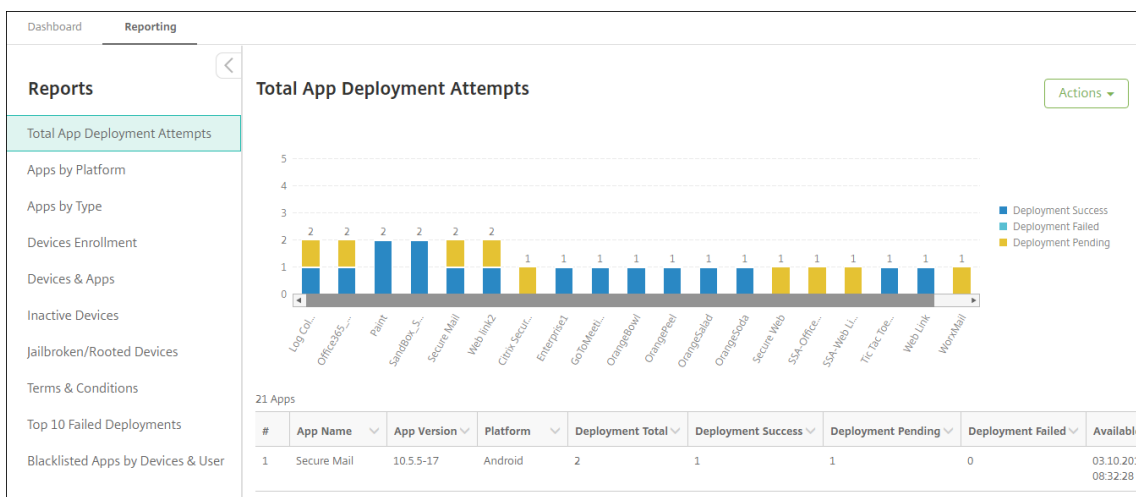
O console XenMobile Server inclui os termos “lista negra” e “lista branca”. Estamos alterando esses termos em uma próxima versão para “lista de bloqueio” e “lista de permissão”.

- **Dispositivos não compatíveis:** lista os dispositivos que não atendem aos critérios de conformidade, como, por exemplo, se o dispositivo está ou não em jailbreak, a versão do SO em execução e se o dispositivo tem um código de acesso.

Você pode exportar os dados de cada tabela para o formato .csv, que pode ser aberto por meio de programas como o Microsoft Excel. Você pode exportar o gráfico de cada relatório para o formato PDF.

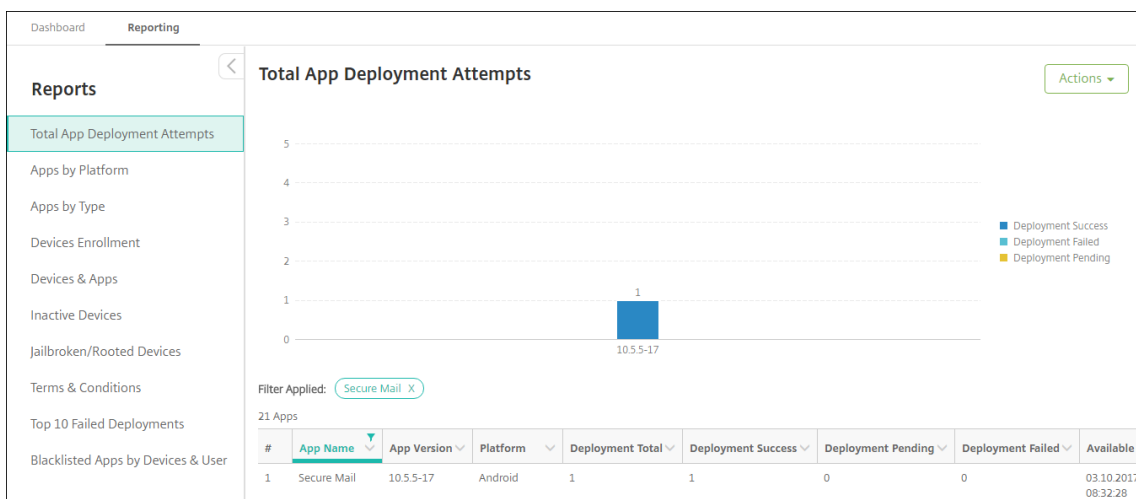
Para gerar um relatório

1. No console XenMobile, clique em **Analisar > Relatórios**. A página **Relatórios** é exibida.
2. Clique no relatório que você deseja gerar.



Para exibir mais detalhes de um relatório

1. Clique em áreas do gráfico para fazer uma busca detalhada e obter mais informações sobre detalhes.



Para classificar, filtrar ou pesquisar uma coluna da tabela, clique no cabeçalho da coluna

Dashboard Reporting

Reports

- Total App Deployment Attempts
- Apps by Platform
- Apps by Type
- Devices Enrollment
- Devices & Apps
- Inactive Devices
- Jailbroken/Rooted Devices
- Terms & Conditions
- Top 10 Failed Deployments
- Blacklisted Apps by Devices & User

22 Apps

#	App Name	App Version	Platform	Deployment Total	Deployment Success	Deployment Pending	Deployment Failed	Available
1	Enterprise1			1	1	0	0	03.10.2017 09:10:10
2	SandBox_S			1	1	0	0	03.10.2017 08:38:40
3	Fonts			1	0	1	0	03.10.2017 09:45:07
4	SandBox_S			1	1	0	0	03.10.2017 08:38:40
5	GoToMeeti			1	1	0	0	03.10.2017 12:34:35
6	Secure Mail	10.5.5-17	Android	1	1	0	0	03.10.2017 08:32:28
7	GreedyPenguins		Windows Mobile	1	1	0	0	03.10.2017 13:01:50

Para filtrar o relatório por data

1. Clique em um cabeçalho de coluna para exibir as configurações de filtro.

Dashboard Reporting

Reports

- Total App Deployment Attempts
- Apps by Platform
- Apps by Type
- Devices Enrollment
- Devices & Apps
- Inactive Devices
- Jailbroken/Rooted Devices
- Terms & Conditions
- Top 10 Failed Deployments
- Blacklisted Apps by Devices & User

Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29:27			03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_SP
Compliance	03.27.2017 09:29:27			03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Editor
Compliance	03.27.2017 09:29:27			03.27.2017 07:33:27	Unknown		SUCCESS	Tic Tac Toe Fre
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Web Link
Compliance	03.27.2017 09:55:27	03.27.2017 09:55:27	Enrolled	09.27.2016 04:48:39	Unknown		SUCCESS	Globoforce_SP

2. Em **Condição do filtro**, escolha como você deseja restringir as datas informadas.

The screenshot shows the 'Reporting' dashboard with a table of device data. A dropdown menu is open over the 'Last authentication' column, showing filter conditions: 'is on', 'is on or before', 'is on or after', and 'between'. The table has columns: Status, Last authentication, Last access, Enrollment state, Enrollment date, Device ownership, Location, Deployment status, and App name.

Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29:40	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_S...
Compliance	03.27.2017 09:29:40	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Edito...
Compliance	03.27.2017 09:29:40	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Tic Tac Toe Fre...
Compliance	03.27.2017 09:29:08	03.27.2017 09:44:07	Enrolled	03.27.2017 07:33:27	Unknown		SUCCESS	Web Link
Compliance	03.27.2017 09:55:27	03.27.2017 09:55:27	Enrolled	09.27.2016 04:48:39	Unknown		SUCCESS	Globoforce_S...

3. Use o seletor de data para especificar as datas.

The screenshot shows the same table as above, but with a date picker calendar open over the 'Last authentication' column. The calendar is for April 2017, showing days from 1 to 30. The 'Value' field above the calendar contains the text 'MM/DD/YYYY'.

4. Uma coluna com um filtro de data é exibida conforme o exemplo a seguir.

The screenshot shows the table with the 'Enrollment date' column highlighted with a purple box. A small downward arrow icon is visible next to the column header, indicating a filter is applied.

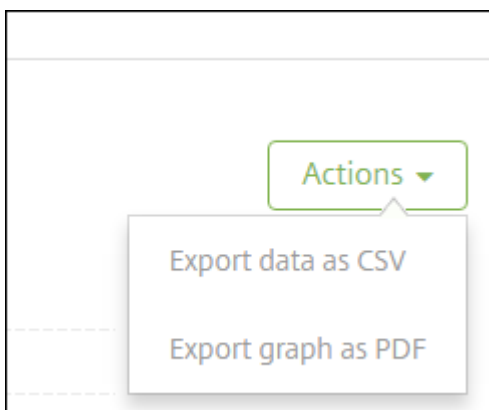
5. Para remover um filtro, clique no cabeçalho da coluna e depois em **Remover filtro**.

The screenshot shows the 'Reporting' section of the XenMobile dashboard. A table displays device compliance data. The 'Last authentication' column is filtered with a 'between' condition, showing dates from 12.31.2016 to 03.27.2017. The table includes columns for Status, Last authentication, Last access, Enrollment state, Enrollment date, Device ownership, Location, Deployment status, and App name.

Status	Last authentication	Last access	Enrollment state	Enrollment date	Device ownership	Location	Deployment status	App name
Compliance	03.27.2017 09:29:00			03.27.2017 07:33:27	Unknown		SUCCESS	Globoforce_S
Compliance	03.27.2017 09:29:00			03.27.2017 07:33:27	Unknown		SUCCESS	Jota Text Edito
Compliance	03.27.2017 09:29:00			03.27.2017 07:33:27	Unknown		SUCCESS	Tic Tac Toe Fre
Compliance	03.27.2017 09:29:00			03.27.2017 07:33:27	Unknown		SUCCESS	Web Link

Para exportar um gráfico ou uma tabela

- Para exportar o plano no formato PDF, clique em **Ações** e em **Exportar gráfico como PDF**.
- Para exportar os dados da tabela no formato CSV, clique em **Ações** e em **Exportar dados como CSV**.



Importante:

Embora seja possível usar o SQL Server para criar relatórios personalizados, Citrix não recomenda esse método. A Citrix não publica o esquema e pode alterar o esquema sem notificação. Se você decidir tomar esse método de emissão de relatórios, certifique-se de que as consultas do SQL são executadas usando uma conta de somente leitura. Esteja ciente de que uma consulta com várias associações JOIN que leva algum tempo para executar prejudica o desempenho do XenMobile Server durante esse período.

SNMP monitoring

April 23, 2020

Você pode ativar o SNMP Monitoring no XenMobile Server para permitir que os sistemas de monitoramento consultem e obtenham informações nos nós do XenMobile. As consultas usam parâmetros, como Carga do processador, Média da carga, Uso da memória e Conectividade. Para obter mais informações sobre o SNMP v3, como especificações de autenticação e criptografia, consulte a documentação oficial do SNMP para [RFC 3414](#).

Nota:

SNMP v3 Monitoring é compatível com o XenMobile Server 10.8 e versões posteriores.

Você pode usar vários aplicativos de monitoramento que suportam o monitoramento de SNMP, como o SCOM. Para obter detalhes sobre como configurar o SCOM, consulte este [artigo do Citrix Support Knowledge Center](#).

Pré-requisitos

Configure as seguintes portas TCP:

- **Porta 161 (UDP):** usada para tráfego SNMP usando o protocolo UDP. A origem é SNMP Manager e o destino é XenMobile.
- **Porta 162 (UDP):** usada para enviar alertas de interceptação SNMP ao SNMP Manager do XenMobile. A origem é XenMobile e o destino é SNMP Manager.

Para obter mais informações sobre a configuração das portas do XenMobile, consulte [Requisitos de porta](#).

Para ver um diagrama de arquitetura de uma implantação local do XenMobile que inclui o SNMP, consulte a [Arquitetura de referência para implantações locais](#).

As etapas gerais para configurar o SNMP são as seguintes.

1. **Adicionar usuários:** Os usuários herdam a permissão para receber interceptações e monitorar o XenMobile Server.
2. **Adicionar um SNMP Manager para receber interceptações:** Interceptações são alertas gerados pelo XenMobile quando o nó do XenMobile ultrapassa o limite de máximo definido pelo usuário.
3. **Configurar o SNMP Manager para interagir com o XenMobile:** O XenMobile Server usa certas bases de informações de gerenciamento (MIBs) para executar operações. Você faz o download de MIBs na página **Configurações > Configuração SNMP** no console XenMobile. Em seguida, você importa as MIBs para o SNMP Manager usando um MIB Importer.

Nota:

Cada SNMP Manager possui seu próprio MIB Importer.

4. **Ativar interceptações:** Você ativa interceptações no console XenMobile e define os intervalos e limites com base em seu ambiente.
5. **Exibir interceptações no SNMP Manager de terceiros:** Para exibir interceptações, verifique o SNMP Manager. Em alguns gerenciadores, no entanto, você pode definir configurações para ativar notificações fora do Manager. Você pode configurar as notificações para aparecer, por exemplo, no email.

Você pode gerar as seguintes interceptações no XenMobile.

Nome da interceptação: Carga do processador

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.2.1.25.3.3.1.2
- **Descrição:** Monitora a carga da CPU do sistema no intervalo definido pelo usuário. Se a carga exceder o valor de limite personalizado, o XenMobile gera a interceptação SNMP.

Nome da interceptação: Média de carga em um minuto

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.2021.10.1.5.1
- **Descrição:** Monitora a carga média do sistema durante um período de um minuto no intervalo definido pelo usuário. Se a média de carga exceder o valor de limite personalizado, o XenMobile gera a interceptação SNMP.

Nome da interceptação: Média de carga em cinco minutos

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.2021.10.1.5.2
- **Descrição:** Monitora a carga média do sistema durante um período de cinco minutos no intervalo definido pelo usuário. Se a média de carga exceder o valor de limite personalizado, o XenMobile gera a interceptação SNMP.

Nome da interceptação: Média de carga em 15 minutos

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.2021.10.1.5.3
- **Descrição:** Monitora a carga média do sistema durante um período de 15 minutos a cada intervalo definido pelo usuário. Se a média de carga exceder o valor de limite personalizado, o XenMobile gera a interceptação SNMP.

Nome da interceptação: Memória disponível total

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.2021.4.11
- **Descrição:** Monitora a memória disponível para cada intervalo definido pelo usuário. Se a memória disponível cair abaixo do valor de limite personalizado, o XenMobile gera a interceptação SNMP. Nota: A memória total disponível inclui RAM e memória swap (memória virtual). Para recuperar a memória swap total, você pode realizar uma consulta usando SNMP OID .1.3.6.1.4.1.2021.4.3 Para recuperar a memória swap disponível, você pode realizar uma consulta usando SNMP OID .1.3.6.1.4.1.2021.4.4

Nome de interceptação: Armazenamento em disco total usado

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.2021.9.1.9.1
- **Descrição:** Monitora o armazenamento em disco do sistema para cada intervalo definido pelo usuário. Se o armazenamento em disco exceder o valor de limite personalizado, o XenMobile gera a interceptação SNMP.

Nome da interceptação: Utilização da memória heap de Java

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.2.4.0
- **Descrição:** Monitora o uso de memória heap JVM (Java virtual machine) do XenMobile para cada intervalo definido pelo usuário. Se o uso exceder o valor de limite personalizado, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Uso de metaspço de Java

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.2.5.0
- **Descrição:** Monitora o uso de metaspço Java do XenMobile para cada intervalo definido pelo usuário. Se o uso exceder o valor de limite, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade LDAP

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.1.0
- **Descrição:** Monitora a conectividade entre o servidor LDAP e o nó do XenMobile para cada intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade DNS

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.2.0
- **Descrição:** Monitora a conectividade entre o servidor DNS e o nó do XenMobile para cada intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do servidor do Google Store

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.3.0
- **Descrição:** Monitora a conectividade entre o servidor do Google Store e o nó do XenMobile para cada intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do Windows Phone Store

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.4.0
- **Descrição:** Monitora a conectividade entre o servidor do Windows Phone Store e o nó do XenMobile para cada intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do Windows Tab Store

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.5.0

- **Descrição:** Monitora a conectividade entre o servidor do Windows Tab Store e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do servidor do Windows Security Token

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.6.0
- **Descrição:** Monitora a conectividade entre o servidor do Windows Security Token e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do servidor do Windows Notification

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.7.0
- **Descrição:** Monitora a conectividade entre o servidor do Windows Notification e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do servidor do APNs (Apple Push Notification Service)

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.8.0
- **Descrição:** Monitora a conectividade entre o servidor do APNs e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do servidor Apple Feedback

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.9.0
- **Descrição:** Monitora a conectividade entre o servidor do Apple Feedback e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do servidor do Apple Store

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.10.0
- **Descrição:** Monitora a conectividade entre o servidor do Apple Store e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome da interceptação: Conectividade do banco de dados do XenMobile

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.11.0
- **Descrição:** Monitora a conectividade entre o banco de dados do XenMobile e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do servidor do Firebase Cloud Messaging

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.12.0

- **Descrição:** Monitora a conectividade entre o servidor do Firebase Cloud Messaging e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do servidor de licenças Citrix

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.13.0
- **Descrição:** Monitora a conectividade entre o servidor de licença Citrix e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do Citrix Gateway

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.15.0
- **Descrição:** Monitora a conectividade entre o Citrix Gateway e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: conectividade entre nós do XenMobile

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.16.0
- **Descrição:** Monitora a conectividade entre nós em cluster do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

Nome de interceptação: Conectividade do serviço de nó do XenMobile Tomcat

- **Identificador de objeto (OID) de monitoramento:** .1.3.6.1.4.1.3845.5.1.1.18.17.0
- **Descrição:** Monitora a conectividade entre o serviço de nó do XenMobile Tomcat e os nós do XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.

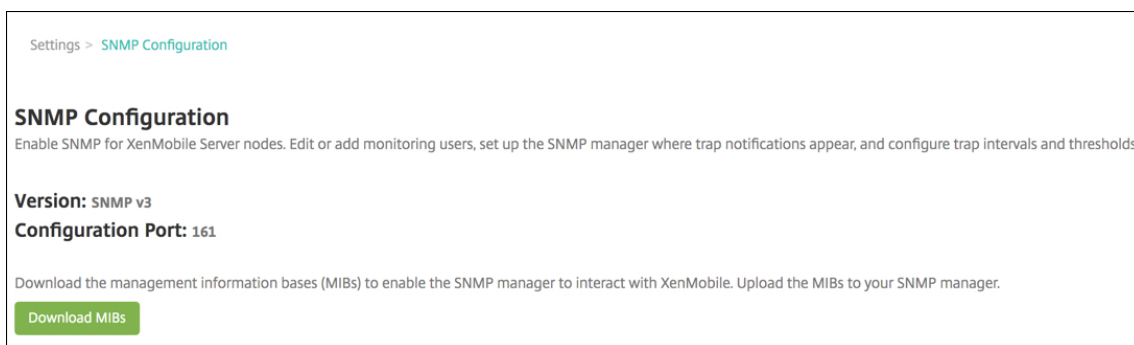
Para obter o melhor desempenho do servidor ao configurar os limites de SNMP, lembre-se dos seguintes fatores:

- Frequência de chamadas
- Dados de interceptação a serem coletados e as verificações de limite
- O mecanismo de comunicação entre nós
- Frequência de verificações de conectividade
- Tempos limite de falhas durante as verificações

Para adicionar usuários SNMP

Os usuários SNMP interagem com gerenciadores SNMP e recebem interceptações.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida.
2. Em **Monitoramento**, clique em **Configuração SNMP**. A página **Configuração SNMP** é exibida.



3. Em **Usuários de SNMP Monitoring**, clique em **Adicionar**.
4. Na caixa de diálogo **Adicionar usuário de SNMP Monitoring**, defina as seguintes configurações:

Add SNMP Monitoring User

User Name *

Authentication Protocol * SHA MD5

Authentication Password *

Privacy Protocol *

Privacy Password *

Nome de usuário: o nome do usuário usado para efetuar login no SNMP Manager. Embora você possa usar caracteres alfanuméricos, sublinhados e hifens, não é possível usar espaços e outros caracteres especiais no seu nome de usuário.

Nota:

Você não pode adicionar o nome de usuário “xmsmonitor” porque o XenMobile reserva o nome para uso interno.

Protocolo de autenticação:

- **SHA** (recomendado)
- **MD5**

Senha de autenticação: digite uma senha de 8 a 18 caracteres. Você pode incluir caracteres alfanuméricos e especiais.

Protocolo de privacidade:

- **DES**
- **AES 128** (recomendado)

Senha de privacidade: digite uma senha de 8 a 18 caracteres. Você pode incluir caracteres alfanuméricos e especiais.

Para adicionar um SNMP Manager

1. Em **SNMP Managers**, clique em **Adicionar**.
2. Na caixa de diálogo **Adicionar SNMP Manager**, defina as seguintes configurações:

The screenshot shows a dialog box titled "Add SNMP Manager" with a close button (X) in the top right corner. The dialog contains three input fields, each with a red asterisk indicating it is required:

- Server IP Address ***: An empty text input field.
- Port ***: A text input field containing the value "162".
- SNMP User Name ***: A dropdown menu with "xenmobile_monitor" selected.

At the bottom right of the dialog, there are two buttons: a grey "Cancel" button and a green "Add" button.

Endereço IP de servidor: digite o endereço IP do SNMP Manager.

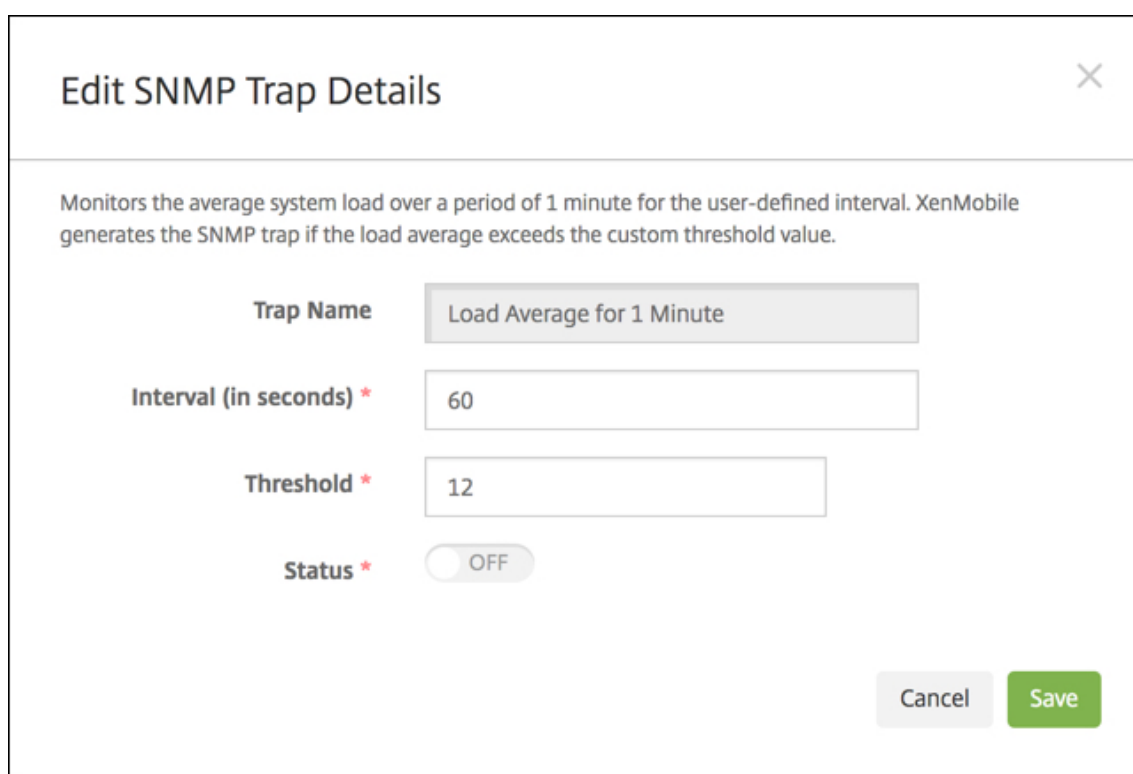
Porta: altere o número da porta, se necessário. O padrão é 162.

Nome de usuário SNMP: selecione o nome de um usuário com acesso ao Manager.

Para ativar e configurar intercepções SNMP

Para ajudar a determinar as configurações de intercepção adequadas para o seu ambiente, consulte [Escalabilidade e desempenho](#). Por exemplo, para monitorar a média de carga do XenMobile por um minuto, você pode ativar a Média de Carga em 1 minuto e fornecer um valor de limite. Se a média de carga do XenMobile Server por 1 minuto exceder o limite especificado, você receberá uma intercepção nos SNMP Managers configurados.

1. Para ativar intercepções individuais, siga um dos destes procedimentos:
 - Marque a caixa de seleção ao lado do parâmetro e, em seguida, clique em **Ativar**.
 - Para ativar todas as intercepções da lista, marque a caixa de seleção na parte superior e clique em **Ativar**.
2. Para editar uma intercepção, selecione o parâmetro e, em seguida, clique em **Editar**.
3. Na caixa de diálogo **Editar detalhes da intercepção SNMP**, você pode editar os valores de limite para intercepções individuais.



Edit SNMP Trap Details

Monitors the average system load over a period of 1 minute for the user-defined interval. XenMobile generates the SNMP trap if the load average exceeds the custom threshold value.

Trap Name Load Average for 1 Minute

Interval (in seconds) * 60

Threshold * 12

Status * OFF

Cancel Save

Nome da intercepção: o nome da intercepção. Você não pode editar esse campo.

Intervalo (em segundos): o intervalo permitido é de 60 a 86400 (24 horas).

Limite: você pode alterar o limite somente para as seguintes intercepções:

- Carga do processador
- Média de carga em 1 minuto

- Média de carga em 5 minutos
- Média de carga em 15 minutos
- Memória disponível total
- Armazenamento total de disco usado
- Utilização da memória heap de Java
- Uso de metaespaço de Java

Status: selecione **I** para ativar o SNMP Monitoring para a interceptação. Selecione **O** para desativar o Monitoring.

Para obter mais informações úteis sobre o monitoramento do XenMobile usando o SNMP, consulte esta [postagem no blog](#).

Pacotes de suporte

December 22, 2020

Para notificar um problema para a Citrix ou solucionar um problema, crie um pacote de suporte. Depois, carregue o pacote de suporte para o Citrix Insight Services (CIS).

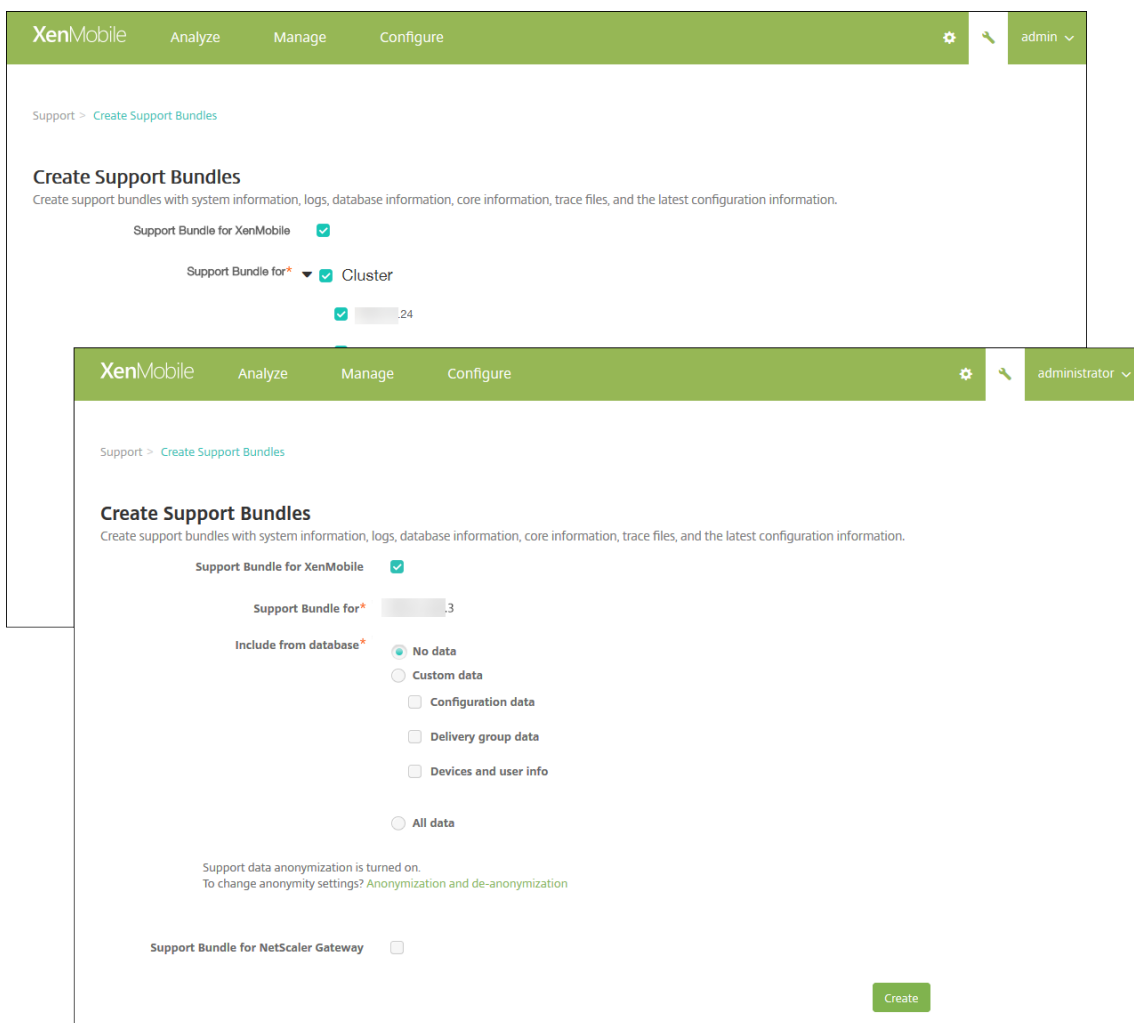
Por padrão, um pacote de suporte inclui um máximo de 100 arquivos de backup dos seguintes arquivos. O tamanho padrão desses arquivos é 10 MB.

- DebugLogFile.log
- AdminAuditLogFile.log
- UserAuditLogFile.log
- HibernateStats.log

Quando o pacote de suporte inclui 100 arquivos de log para cada uma dessas categorias, o arquivo de log é transferido. Se você configurar um número máximo mais baixo de arquivos de log, o XenMobile excluirá imediatamente os arquivos de log externos desse nó. Para configurar o número de arquivos de log, vá para **Solução de problemas e suporte > Configurações de log**.

Para criar um pacote de suporte:

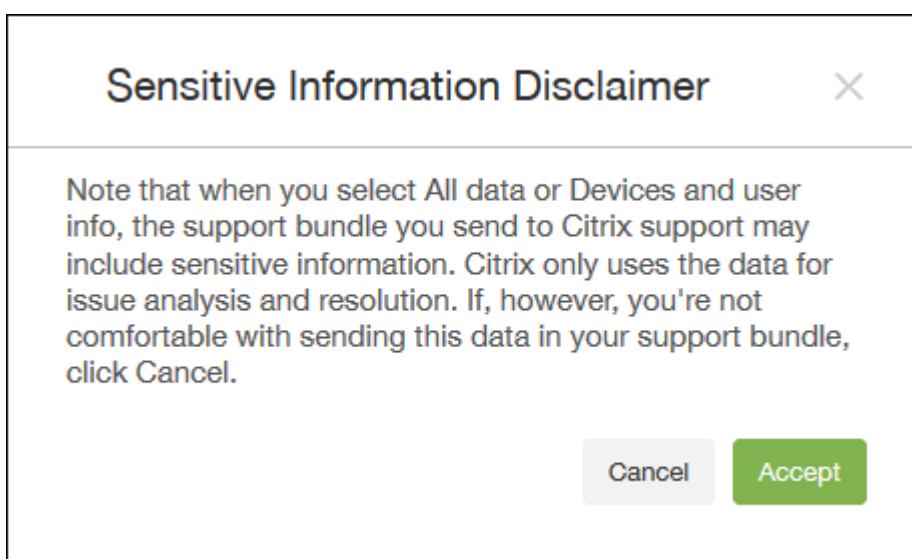
1. No console XenMobile, clique no ícone de chave inglesa no canto superior direito. A página **Suporte** é exibida.
2. Na página **Suporte**, clique em **Criar pacotes de suporte**. A página **Criar pacotes de suporte** é exibida. Se o seu ambiente do XenMobile contiver nós de cluster, todos os nós serão mostrados.



3. Verifique se a caixa de seleção **Pacote de suporte para XenMobile** está marcada.
4. Se o seu ambiente do XenMobile contiver nós de cluster, em **Pacote de suporte para**, você poderá selecionar todos os nós ou qualquer combinação de nós dos quais extrair dados.
5. Em **Incluir do banco de dados**, você pode optar por um dos seguintes procedimentos:
 - Clique em **Não há dados**.
 - Clique em **Dados personalizados**. Por padrão, todas essas opções estão selecionadas.
 - **Dados de configuração**: inclui configurações de certificado e políticas do gerenciador de dispositivo.
 - **Dados de grupo de entrega**: inclui informações de grupo de entrega de aplicativo que contêm detalhes de tipos de aplicativo e de política de entrega de aplicativo.
 - **Dispositivos e informações do usuário**: inclui políticas de dispositivo, aplicativos, ações e grupos de entrega.
 - Clique em **Todos os dados**.

Nota:

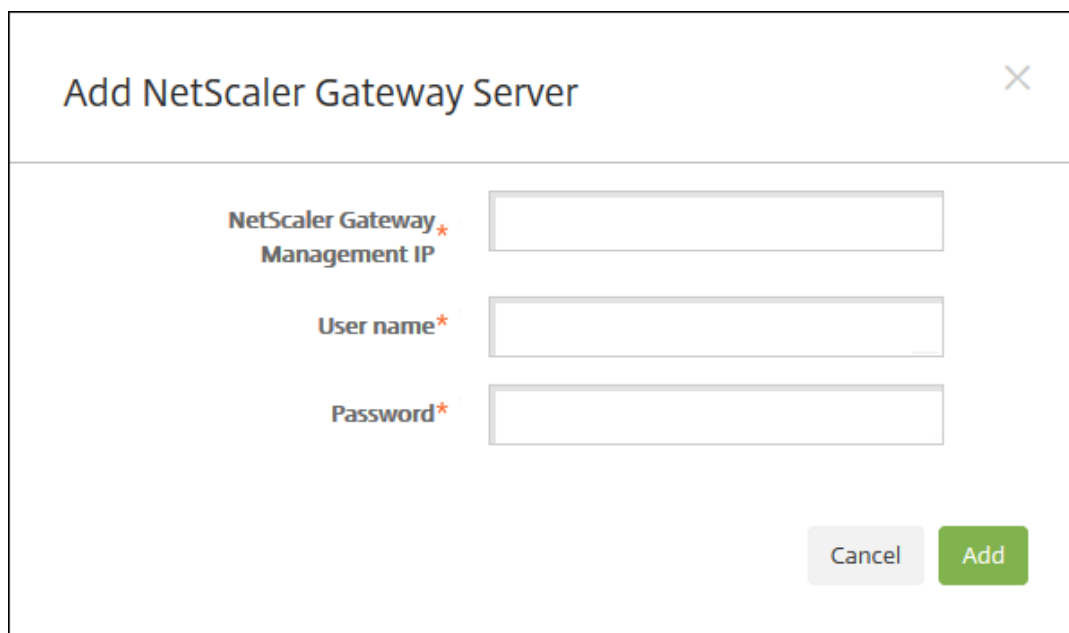
Se você escolher **Dispositivos e informações do usuário** ou **Todos os dados**, e esse for o primeiro pacote de suporte que você criou, a caixa de diálogo **Isenção de responsabilidade de informações confidenciais** será exibida. Leia o aviso de isenção de responsabilidade e clique em **Aceitar** ou **Cancelar**. Se você clicar em **Cancelar**, o pacote de suporte não poderá ser carregado para a Citrix. Se você clicar em **Aceitar**, poderá carregar o pacote de suporte para a Citrix e não verá o aviso de isenção de responsabilidade na próxima vez que criar um pacote de suporte que inclui dados de usuário ou dispositivo.



6. A opção **Anonimização de dados de suporte está ativada** indica que a configuração padrão é anonimizar os dados. A anonimização de dados significa que dados confidenciais do usuário, do servidor e da rede são feitos anônimos nos pacotes de suporte.

Para alterar essa configuração, clique em **Anonimização e desanonimização**. Para obter mais informações sobre a anonimização de dados, consulte [Anonimizando dados nos pacotes de suporte](#).

7. Para incluir pacotes de suporte do Citrix Gateway: marque a caixa de seleção **Pacote de suporte para o Citrix Gateway** e faça o seguinte:
 - a) Clique em **Adicionar**. A caixa de diálogo **Adicionar Citrix Gateway Server** é exibida.



Add NetScaler Gateway Server

NetScaler Gateway Management IP*

User name*

Password*

Cancel **Add**

- b) Em **IP de Gerenciamento do Citrix Gateway**, digite o endereço IP de gerenciamento do Citrix ADC do Citrix Gateway do qual você deseja extrair os dados de pacote de suporte.

Nota:

Se você estiver criando um pacote de um servidor Citrix Gateway que já foi adicionado, o endereço IP será fornecido.

- c) Em **Nome de usuário** e **Senha**, digite as credenciais de usuário necessárias para acessar o servidor que executa o Citrix Gateway.

Nota:

Se você estiver criando um pacote de um servidor Citrix Gateway que já foi adicionado, o nome do usuário será fornecido.

8. Clique em **Adicionar**. O novo pacote de suporte do Citrix Gateway é adicionado à tabela.
9. Repita a Etapa 7 para adicionar mais pacotes de suporte do Citrix Gateway.
10. Clique em **Criar**. O pacote de suporte é criado, e dois novos botões, **Carregar em CIS** e **Baixar para o cliente** são exibidos.

Carregando pacotes de suporte para o Citrix Insight Services

Depois de criar um pacote de suporte, você poderá carregá-lo para o Citrix Insight Services (CIS) ou baixá-lo para o seu computador.

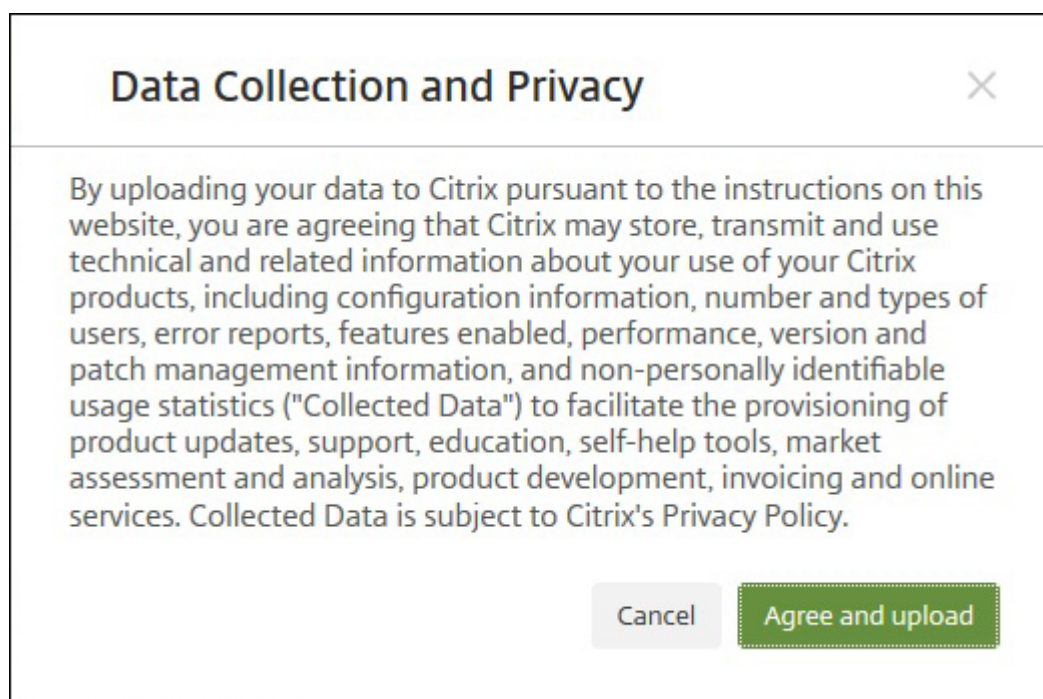
O carregamento do XenMobile para o CIS é realizado por meio de uma conexão de saída SSL. Abra a porta 443 para o endereço IP do servidor CIS (52.88.24.76, 52.88.118.220, 52.11.72.119). Se você tiver

um proxy para o tráfego HTTPS, verifique se o proxy pode alcançar o endereço IP do servidor CIS.

Essas etapas mostram como carregar o pacote para o CIS. Você precisa de um ID e senha do My Citrix para carregar para o CIS.

1. Na página **Criar pacotes de suporte**, clique em **Carregar em CIS**. A caixa de diálogo **Carregar para o Citrix Insight Services (CIS)** é exibida.
2. Em **Nome de usuário**, digite o seu ID do My Citrix.
3. Em **Senha**, digite a sua senha do My Citrix.
4. Se quiser conectar esse pacote a um número de solicitação de serviço existente, marque a caixa de seleção **Associar com nº de SR** e, nos dois novos campos que são exibidos, faça o seguinte:
 - Em **Nº de SR**, digite o número de solicitação de serviço de oito dígitos que você deseja associar a esse pacote.
 - Em **Descrição de SR**, digite uma descrição para o SR.
5. Clique em **Carregar**.

Se essa tiver sido a primeira vez que carregou um pacote de suporte para o CIS e você não tiver criado uma conta no CIS por meio de outro produto e aceitado o acordo de Privacidade e Coleta de Dados, a seguinte caixa de diálogo é exibida. Você deve aceitar o acordo antes de começar o carregamento. Se você tiver uma conta no CEI e tiver aceitado o acordo, o pacote de suporte será carregado imediatamente.



6. Leia o acordo e depois clique em **Concordar e carregar**. O pacote de suporte é carregado.

Baixando pacotes de suporte para o seu computador

Depois de criar um pacote de suporte, você poderá carregá-lo para o CIS ou baixá-lo para o seu computador. Se você desejar solucionar o problema por si mesmo, baixe o pacote de suporte para o seu computador.

Na página Criar pacotes de suporte, clique em Baixar para o cliente. O pacote é baixado para o seu computador.

O pacote de suporte contém arquivos de valor analítico variável. Consulte a tabela a seguir para obter uma lista de arquivos e seus valores analíticos.

Nome do arquivo	Tipo	Descrição	Valor
DbDump.json	Despejo de banco de dados JSON	Informações de usuários/dispositivos/aplicativos	Alta
Garbage.html	Arquivo HTML	Coletor de lixo Java	Baixo
MemoryInfo.html	Arquivo HTML	Uso de memória - uso de memória relacionada a java	Alta
MultiNodeClusterInfo.html	Arquivo HTML	Configuração do cluster	Alta
Patches.html	Arquivo HTML	Informação do patch. Melhor para xmspatches.txt	Alta
pg_dump0.sql	PG Dump	Despejo de instância padrão do Postgress	Média
rt_db/*	DB Copy (redundente, esta é uma representação binária de pg_dump0.sql)		N/D
sas_config/c3p0.properties	Arquivo de propriedades	Propriedades de C3P0 DB Config	Média
sas_config/catalina.policy	arquivo de política	Políticas do Web Server Catalina - Arquivos não mudam	Baixo
sas_config/catalina.properties	Arquivo de propriedades	Propriedades do Web Server Catalina - Arquivos não mudam	Baixo

Nome do arquivo	Tipo	Descrição	Valor
sas_config/ew-config.properties	Arquivo de propriedades	Informações sobre a configuração do servidor XM	Alta
sas_config/ew-config-reloadable.properties	Arquivo de propriedades	Informações sobre o modelo de segurança	Alta
sas_config/hazelcast.xr	Arquivo XML	Logs de Hazelcast - Não acho que seria muito útil.	Baixo
sas_config/pki.xml	Arquivo XML	Poderia ser usado para determinar se há servidor PKI de terceiros em uso.	Alta
sas_config/push_servic	Arquivo XML	Serviços Push - Arquivos não mudam	Baixo
sas_config/server.xml	Arquivo XML	Informações de codificação aqui - Relacionada à segurança	Alta
sas_config/sftu_config/	Arquivo de propriedades	Propriedades do AppC - Arquivos não mudam	Baixo
sas_config/sftu_config/catalina.properties	Arquivo de propriedades	Políticas do Catalina - Arquivos não mudam	Baixo
sas_config/sftu_config/	Arquivo de propriedades	Propriedades do Catalina - Arquivos não mudam	Baixo
sas_config/sftu_config/logging.properties	Arquivo de propriedades	Propriedades de registro em log - Arquivos não mudam	Baixo
sas_config/sftu_config/	Arquivo XML	Informações de codificação aqui - Relacionada à segurança	Alta
sas_config/sftu_config/server.xml	Arquivo XML	Informações sobre migração	Alta

Nome do arquivo	Tipo	Descrição	Valor
sas_config/sftu_config/	Arquivo XML	Configurações do usuário pela primeira vez	Alta
sas_config/sftu_config/tomcat-users.xml	Arquivo XML	Usuários do TomCat - Arquivos não mudam	Baixo
sas_config/sftu_config/	Arquivo XML	Web - Arquivos não mudam	Baixo
sas_config/sftu.properties	Arquivo de propriedades	Propriedades de SFTU config	Alta
sas_config/variables.xml	Arquivo XML	Variáveis - Arquivos não mudam	Baixo
sas_config/web.xml	Arquivo XML	Informações relacionadas ao Webserver	Média
sas_log/AdminAuditLog	Arquivo de log do Linux	Quaisquer alterações de configuração	Alta
sas_log/create_sb_output	Arquivo de log do Linux	Saída de comando de geração de suporte	Baixo
sas_log/DebugLogFile.log	Arquivo de log do Linux	Log de todos os recursos	Alta
sas_log/HibernateStats.log	Arquivo de log do Linux	Log de Hibernatestats	Baixo
sas_log/kafka-consumer.log	Arquivo de log do Linux	Log do Kafka	Baixo
sas_log/kafka-server.log	Arquivo de log do Linux	Log do Kafka	Baixo
sas_log/kafka-topics.log	Arquivo de log do Linux	Log do Kafka	Baixo
sas_log/LPE.log	Arquivo de log do Linux	Log do LPE	Baixo
sas_log/migration.log	Arquivo de log do Linux	Saída do processo de migração	Média

Nome do arquivo	Tipo	Descrição	Valor
sas_log/PlatformAuditLogFile.log	Arquivo de log do Linux	Informações de nível de auditoria de backend	Alta
sas_log/PlatformDebug.log	Arquivo de texto	Logs relacionados ao servidor de backend	Alta
sas_log/postgres.log	Arquivo de log do Linux	Logs do PostGres	Média
sas_log/SFTU.log	Arquivo de log do Linux	Log do SFTU	Média
sas_log/tc1/catalina.log	Arquivo de log do Linux	Log do Catalina	Baixo
sas_log/tc1/console	Arquivo de log do Linux	Console	Baixo
sas_log/tc1/host-manager.log	Arquivo de log do Linux	Gerenciador de host	Baixo
sas_log/tc1/localhost.log	Arquivo de log do Linux	LocalHost	Baixo
sas_log/updates.log	Arquivo de log do Linux	Saída do processo de patch	Média
sas_log/UserAuditLogFile.log	Arquivo de log do Linux	Ações do usuário	Alta
sas_log/zookeeper.txt	Arquivo de texto	Log do Zookeeper	Baixo
snmp/snmpd_etc_nets	Arquivo de propriedades	Propriedades de SNMP config	Baixo
snmp/snmpd_privileges.conf	Arquivo de propriedades	Propriedades de SNMP config	Baixo
sys_info/arp_entries.txt	Arquivo de texto	Entradas ARP no servidor XMS	Média
sys_info/chrony.txt	Arquivo de texto	Log do Chrony	Baixo
sys_info/diskspace_usage.txt	Arquivo de texto	Uso do espaço em disco	Alta
sys_info/firewall_rules.txt	Arquivo de texto	Regras de firewall definidas no XMS	Média

Nome do arquivo	Tipo	Descrição	Valor
sys_info/interface_conf	Arquivo de texto	Saída do comando do sistema	Média
sys_info/net_connections	Arquivo de texto	Saída do comando do sistema	Média
sys_info/root_account_	Arquivo de texto	Saída do comando do sistema	Média
sys_info/routing_table.txt	Arquivo de texto	Alto valor	Alta
sys_info/running_procs	Arquivo de texto	Alto valor	Alta
sys_info/top.txt	Arquivo de texto	Saída do comando do sistema	Média
ThreadDump.html	Arquivo HTML	Não é mais usado.	Baixo
ThreadDumpV2.html	Arquivo HTML	Rastreamento de pilhas de thread etc.	Média
var_log/auth.log	Arquivo de log do Linux	Log de nível de SO	Média
var_log/boot.log	Arquivo de log do Linux	Log de nível de SO	Média
var_log/btmp	Arquivo de log do Linux	Log de nível de SO	Média
var_log/daemon.log	Arquivo de log do Linux	Log de nível de SO	Média
var_log/kern.log	Arquivo de log do Linux	Log de nível de SO	Média
var_log/lastlog	Arquivo de log do Linux	Log de nível de SO	Média
var_log/mail.log	Arquivo de log do Linux	Log de nível de SO	Média
var_log/sys.log	Arquivo de log do Linux	Log de nível de SO	Média
var_log/user.log	Arquivo de log do Linux	Log de nível de SO	Média
var_log/wtmp	Arquivo de log do Linux	Log de nível de SO	Média

Nome do arquivo	Tipo	Descrição	Valor
version.txt	arquivo de texto	Versão do servidor XM	Média
XENMOBILE-<IP Address>-ConnectivityCheckResults.xml	Arquivo XML	Resultados da Verificação de Conectividade no servidor XMS	Média
xmspatches.txt	Arquivo de texto	Informação do patch.	Alta

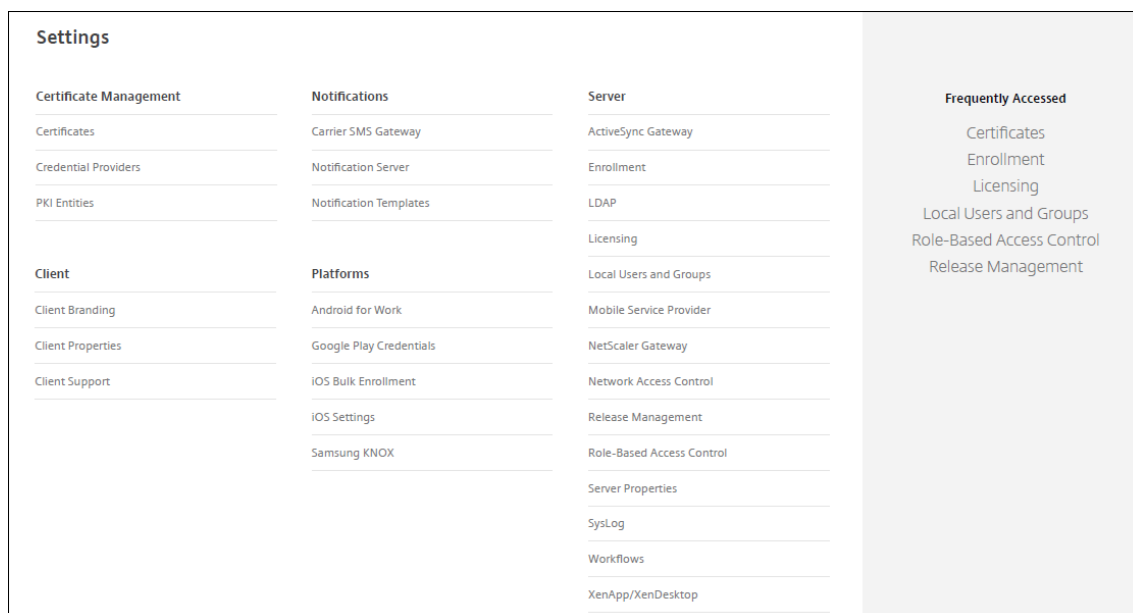
Opções de suporte e suporte remoto

April 23, 2020

Você pode fornecer um endereço de email para que os usuários entrem em contato com a equipe de suporte. Quando os usuários solicitarem assistência dos dispositivos deles, eles veem o endereço de email.

Você também pode configurar como os usuários enviam logs para o suporte técnico usando seus dispositivos. Você pode configurar os logs para que sejam enviados diretamente ou por email.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida.



2. Em **Cliente**, clique em **Suporte ao cliente**. A página **Suporte ao cliente** é exibida.

3. Faça as seguintes configurações:

- **Email de suporte (suporte técnico de TI):** digite o endereço de email do seu contato de suporte técnico de TI.
- **Enviar logs do dispositivo para o suporte técnico de TI:** selecione se os logs do dispositivo são enviados **diretamente** ou **por email**. O padrão é **por email**.
 - Quando você ativa **diretamente**, as configurações de Armazenar logs no ShareFile (agora chamado Citrix Content Collaboration) são exibidas. Se você habilitar os logs de armazenamento no Citrix Content Collaboration, os logs serão enviados diretamente para o Citrix Files. Caso contrário, os logs serão enviados ao XenMobile e, em seguida, enviados por email para o suporte técnico. Além disso, a opção **Se o envio direto falhar, use o email**, que é ativada por padrão, aparece. Você pode desativar essa opção quando não desejar usar o email do cliente para enviar os logs se houver um problema com o servidor. Porém, quando essa opção for desativada e ocorrer um problema com o servidor, os logs não serão enviados.
 - Quando você ativa a opção **por email**, o email do cliente sempre é usado para enviar os logs.

4. Clique em **Salvar**.

Suporte remoto

Nota:

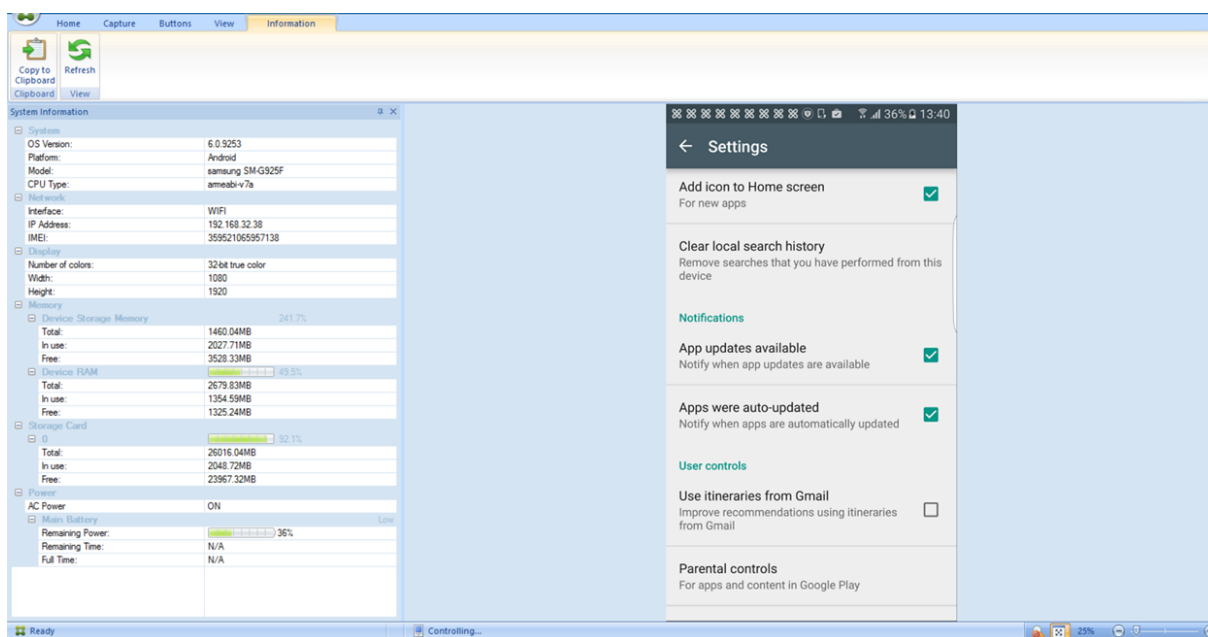
O Remote Support não está mais disponível para novos clientes desde 1º de janeiro de 2019. Os clientes existentes podem continuar a usar o produto, no entanto, a Citrix não fornecerá melhorias ou correções.

Para implantações do XenMobile Server no local: o suporte remoto permite que o pessoal da central de ajuda assuma o controle remotamente de dispositivos móveis gerenciados Windows CE e Android. Conversão de tela é compatível somente com dispositivos Samsung Knox.

O suporte remoto não está disponível para implantações do XenMobile Server em cluster no local.

Durante uma sessão de controle remoto:

- Os usuários veem no dispositivo móvel um ícone que indica uma sessão de controle remoto está ativa.
- Os usuários do Remote Support veem a janela de aplicativo de suporte remoto e uma janela de controle remoto que mostra uma representação do dispositivo controlado.



Usando o Remote Support, você pode fazer o seguinte:

- Fazer login remotamente em um dispositivo móvel e controlar a tela. Os usuários podem assistir você navegar pela tela deles, o que também pode ser útil para fins de treinamento.
- Navegar e reparar um dispositivo remoto em tempo real. Você pode alterar as configurações, solucionar problemas de sistema operacional e desabilitar ou parar aplicativos ou processos problemáticos.
- Isolar e conter ameaças antes que se espalhem para outros dispositivos móveis desabilitando o acesso a rede, interrompendo processos danosos e removendo aplicativos ou malware.
- Habilitar remotamente o toque do dispositivo e telefonas para o telefone para ajudar o usuário a localizar o dispositivo. Quando um usuário não consegue encontrar o dispositivo, você pode apagá-lo para garantir que os dados confidenciais não sejam comprometidos.

O Suporte Remoto também permite ao pessoal de suporte:

- Exibir uma lista de todos os dispositivos conectados dentro de uma ou mais instâncias do XenMobile.
- Exibir informações do sistema do modelo de dispositivo, inclusive nível do sistema operacional, International Mobile Station Equipment Identity (IMEI), o número de série, memória e status da bateria e conectividade.
- Exibir os usuários e grupos para o XenMobile.
- Executar o gerenciador de tarefas do dispositivo, no qual você pode exibir e terminar processos ativos e reiniciar o dispositivo móvel.
- Executar transferência de arquivos remotos que inclui transferência bidirecional entre os dispositivos móveis e um servidor de arquivos.
- Baixar e instalar programas de software em lote para um ou mais dispositivos móveis.

- Definir as configurações de chave de registro remotas no dispositivo.
- Otimizar o tempo de resposta por redes de celular de largura de banda estreita usando o controle remoto de tela de dispositivo em tempo real.
- Exibir a capa de dispositivo da maioria das marcas de modos de dispositivos móveis. Exibir um editor de capa para adicionar novos modelos de dispositivo e mapear chaves físicas.
- Ativar a captura, registro e reprodução de tela de dispositivo com a capacidade de capturar uma sequência de interações no dispositivo que cria um arquivo de vídeo AVI.
- Comandar reuniões compartilhadas ao vivo usando quadro de comunicações compartilhadas, comunicações de voz baseadas em VoIP e bate-papo entre usuários de dispositivos móveis e a equipe de suporte.

Requisitos de sistema do Remote Support

O software do Remote Support é instalado em computadores com base em Windows que atendem aos seguintes requisitos. Para conhecer os requisitos de porta, consulte [Requisitos de porta](#).

Plataformas com suporte:

- Intel Xeon/Pentium 4 - 1 GHz no mínimo workstation class
- 512 MB de RAM no mínimo
- 100 MB de espaço livre em disco no mínimo

Sistemas operacionais compatíveis:

- Microsoft Windows 2003 Server Standard Edition ou Enterprise Edition SP1 ou posterior
- Microsoft Windows 2000 Professional SP4
- Microsoft Windows XP SP2 ou posterior
- Microsoft Windows Vista SP1 ou posterior
- Microsoft Windows 10
- Microsoft Windows 8
- Microsoft Windows 7

Para instalar o Suporte a partir da linha de comando

Digite o seguinte comando:

```
1 \*RemoteSupport\*.exe /S
```

RemoteSupport é o nome do programa de instalação. Por exemplo:

```
1 XenMobileRemoteSupport-9.0.0.35265.exe /S
```

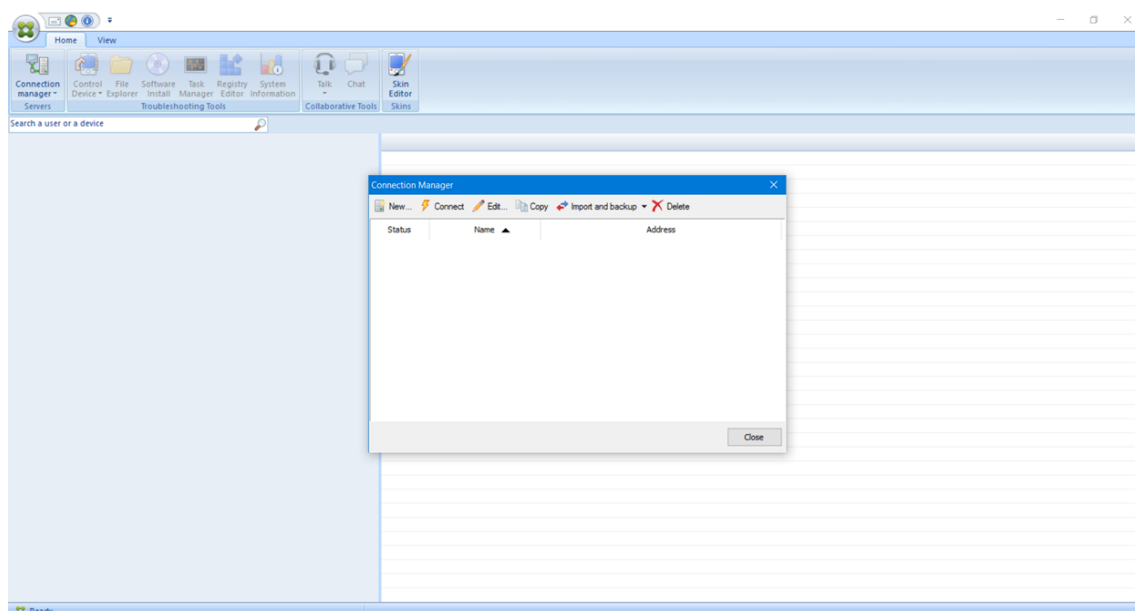
Você pode usar as variáveis a seguir ao instalar o Remote Support software:

- /S: para instalar o software do Remote Support com os parâmetros padrão.
- /D=dir: para especificar um diretório de instalação personalizado.

Para conectar-se ao Remote Support para XenMobile

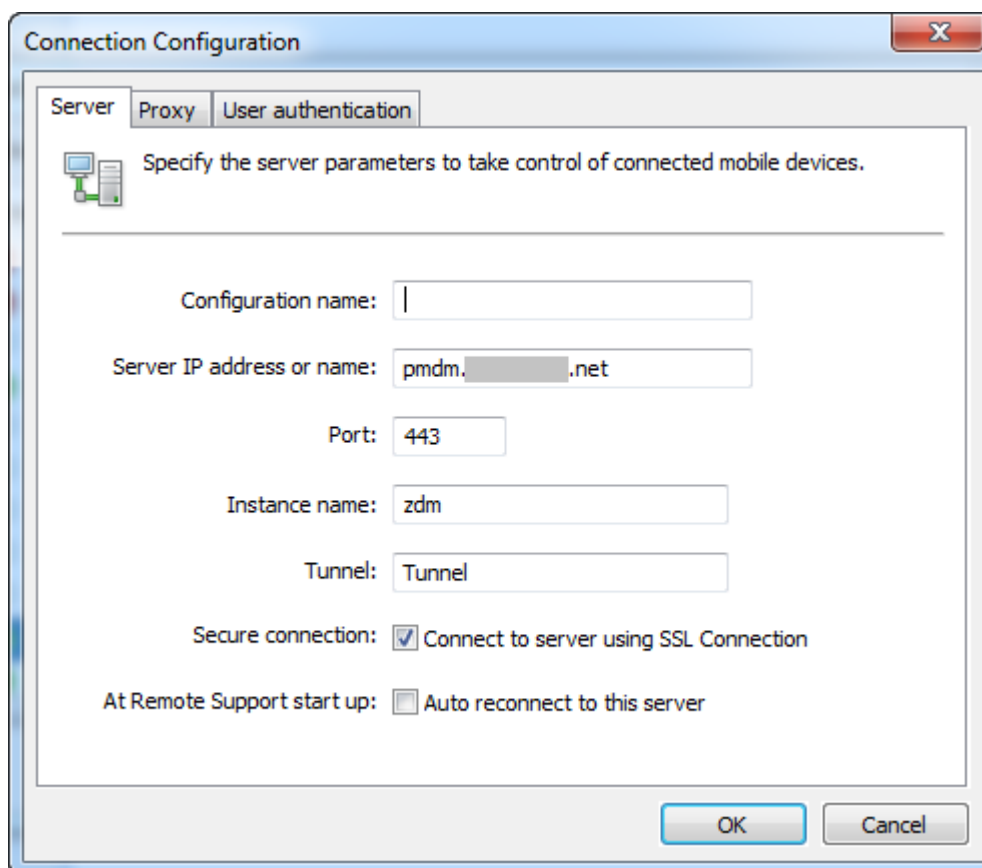
Para estabelecer conexões de suporte remoto para dispositivos gerenciados, você deve adicionar uma conexão de Remote Support para um ou mais XenMobile Servers que gerenciam os dispositivos. Esta conexão é executada através de um túnel de aplicativo definido na Política de Túnel MDM, uma política para dispositivos Android e Windows Mobile/CE. Defina o túnel de aplicativo para poder conectar o Remote Support ao XenMobile. Para obter detalhes, consulte [Política de dispositivo de encapsulamento de aplicativo](#).

1. Inicie o software do Remote Support e use suas credenciais do XenMobile para fazer login.
2. No **Connection Manager**, clique em **New**.

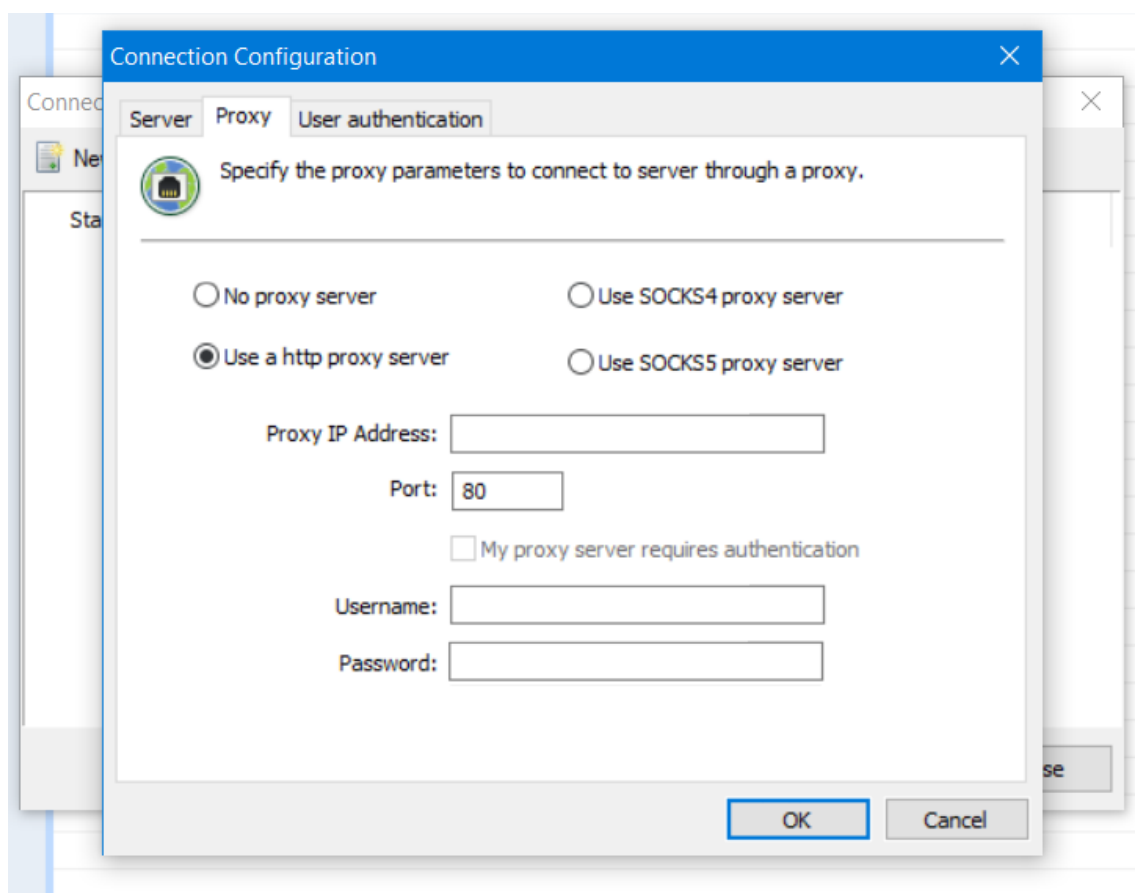


3. Na caixa de diálogo **Connection Configuration**, na guia **Server**, digite os seguintes valores:
 - a) Em **Configuration name**, digite um nome para a entrada de configuração.
 - b) Em **Server IP address or name**, digite o endereço IP ou o nome DNS do XenMobile Server.
 - c) Em **Port**, digite um número de porta TCP, conforme definido na configuração de XenMobile Server.
 - d) Em **Instance name**, se o XenMobile for parte de uma implantação multilocatário, digite um nome de instância.
 - e) Em **Tunnel**, digite o nome da Política de Túnel.
 - f) Marque a caixa de seleção **Connect to server using SSL Connection**.

- g) Marque a caixa de seleção **Auto reconnect to this server** para se conectar com o XenMobile Server configurado toda vez que o aplicativo Remote Support for iniciado.



4. Na guia **Proxy**, selecione **Use an http proxy server** e, em seguida, insira as seguintes informações:
- a) Em **Proxy IP Address**, digite o endereço IP do servidor proxy.
 - b) Em **Port**, digite um número de porta TCP usada pelo proxy.
 - c) Marque a caixa de seleção **My proxy server requires authentication** se o servidor proxy exigir autenticação para permitir tráfego.
 - d) Em **Username**, digite o nome do usuário a ser autenticado no servidor proxy.
 - e) Em **Password**, digite a senha a ser autenticada no servidor proxy.



5. Na guia **User Authentication**, marque a caixa de seleção **Remember my login and password** e insira as credenciais.
6. Clique em **OK**.

Para se conectar ao XenMobile, clique duas vezes na conexão que você criou e, em seguida, digite o nome do usuário e a senha que você configurou para a conexão.

Para habilitar o suporte remoto para dispositivos Samsung Knox

Crie uma política de Suporte Remoto no XenMobile para conceder a você acesso remoto aos dispositivos Samsung Knox. Você pode configurar dois tipos de suporte:

- **Básico:** permite que você exiba informações de diagnóstico sobre o dispositivo. Por exemplo, informações do sistema, os processos em execução, o gerenciador de tarefas (uso de memória e da CPU) e o conteúdo da pasta do software instalado.
- **Premium:** permite que você controle remotamente a tela de dispositivo. Por exemplo, controle de cores da janela, estabelecer uma sessão de VoIP entre o suporte técnico e o usuário e estabelecer uma sessão de bate-papo entre o suporte técnico e o usuário.

O suporte com Premium exige que você configure a política de dispositivo de chave de licença

MDM Samsung no console XenMobile. Quando você configurar essa política, selecione somente a plataforma **Samsung KNOX**. No caso da plataforma Samsung SAFE, a chave ELM é implantada automaticamente nos dispositivos Samsung quando eles se registram no XenMobile. Portanto, não selecione a plataforma Samsung SAFE no caso dessa política. Para obter detalhes, consulte [Chave de licença MDM Samsung](#).

Para obter informações sobre como configurar a Política de Suporte Remoto, consulte [Suporte remoto à política de dispositivo](#).

Para usar uma sessão de Remote Support

Após iniciar o Remote Support, o lado esquerdo da janela do aplicativo Remote Support apresenta grupos de usuários do XenMobile, conforme definido no console do XenMobile. Por padrão, aparecem apenas grupos que contêm usuários que estão conectados no momento. Você pode ver o dispositivo para cada usuário ao lado da entrada respectiva.

1. Para ver todos os usuários, expanda cada grupo na coluna à esquerda. Esses usuários conectados no momento ao XenMobile Server são indicadas por um ícone verde.
2. Para exibir todos os usuários, incluindo aqueles que não estão conectados no momento, clique em **View** e selecione **Non-connected devices**. Os usuários não conectados são exibidos sem o pequeno ícone verde.

Os dispositivos conectados ao XenMobile Server, mas que não foram atribuídos a um usuário, aparecem em modo anônimo. (A sequência **Anonymous** aparece na lista.) Você pode controlar esses dispositivos como o dispositivo de um usuário conectado.

Para controlar um dispositivo, selecione o dispositivo clicando na linha e, em seguida, em **Control Device**. Uma representação do dispositivo é exibida na janela do Remote Control. Você pode interagir com um dispositivo controlado das seguintes maneiras:

- Controlar a tela do dispositivo, incluindo controle com cores, na janela principal ou em janela flutuante separada.
- Criar uma sessão de Voice-over-IP (VoIP) entre o suporte técnico e o usuário. Definir as configurações do VoIP.
- Estabelecer uma sessão de bate-papo com o usuário.
- Acessar o dispositivo gerenciador de tarefas, para gerenciar itens como o uso da memória, o uso da CPU e aplicativos em execução.
- Explorar os diretórios locais do dispositivo móvel. Transferir arquivos.
- Editar o registro de dispositivo em dispositivos móveis do Windows.
- Exibir informações de sistema do dispositivo e todos os softwares instalados.
- Atualizar o status de conexão do dispositivo móvel com o XenMobile Server.

Syslog

November 30, 2020

Você pode configurar o XenMobile para enviar arquivos de log para um servidor de logs do sistema (syslog). Você precisa do nome do host ou do endereço IP do servidor.

Syslog é um protocolo padrão de log com dois componentes: um módulo de auditoria (que é executado no dispositivo) e um servidor, que pode ser executado em um sistema remoto. O protocolo Syslog usa o protocolo de dados de usuário (UDP) para transferência de dados. Os eventos de Administrador e os eventos de Usuário são gravados.

Você pode configurar o servidor para coletar os seguintes tipos de informações:

- Logs do sistema, que contêm um registro das ações realizadas pelo XenMobile.
- Logs de auditoria, que contêm um registro cronológico das atividades do sistema relativo ao XenMobile.

As informações de log que um servidor syslog coleta de um dispositivo são armazenadas em um arquivo de log na forma de mensagens. Essas mensagens geralmente contêm as seguintes informações:

- O endereço IP do dispositivo que gerou a mensagem de log
- Um carimbo de data/hora
- O tipo da mensagem
- O nível de log associado a um evento (Crítico, Erro, Notificação, Aviso, Informativo, Depuração, Alerta ou Emergência)
- As informações da mensagem

O XenMobile usa o log4j syslog appender para enviar mensagens de syslog formatadas RFC5424. Os dados da mensagem syslog estão em texto simples, sem formato específico.

Você pode usar essas informações para analisar a origem do alerta e executar a ação corretiva, se necessário.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida.
2. Clique em **Syslog**. A página **Syslog** é exibida.
3. Defina estas configurações:
 - **Servidor:** digite o endereço IP ou o nome de domínio totalmente qualificado (FQDN) do seu servidor syslog.
 - **Porta:** digite o número da porta. Por padrão, a porta é definida como 514.
 - **Informações para log:** marque ou desmarque **Logs do sistema** e **Auditoria**.
 - Logs do sistema contêm as ações realizadas pelo XenMobile.

- Logs de auditoria contêm um registro cronológico das atividades do sistema relativo ao XenMobile.
- Logs de depuração para o XenMobile.

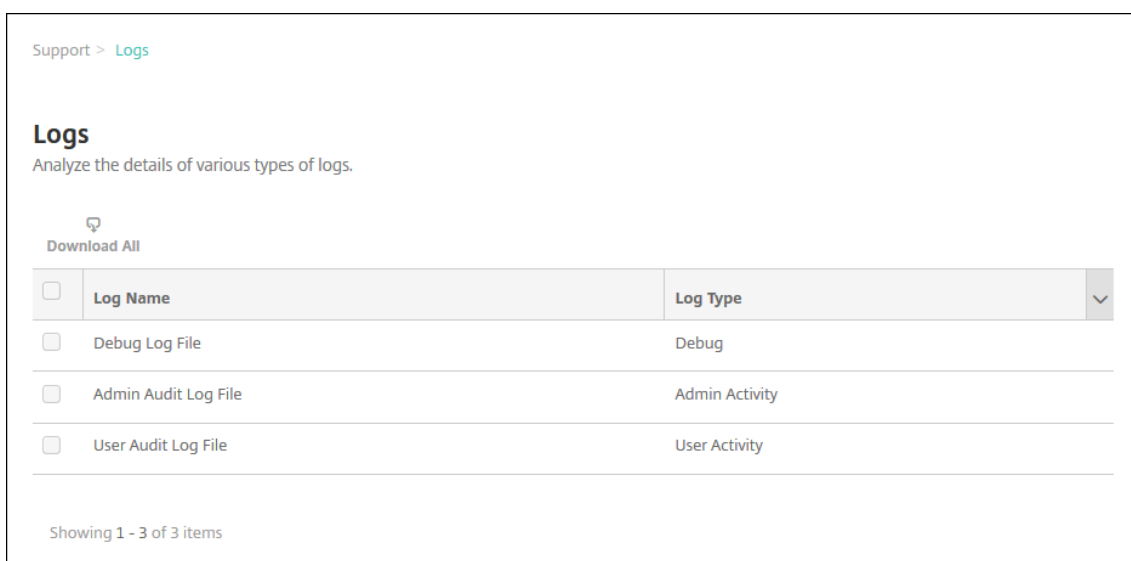
4. Clique em **Salvar**.

Exibir arquivos de log no XenMobile

January 8, 2020

Visualize, manipule e baixe logs para ajudar a gerenciar com o XenMobile.

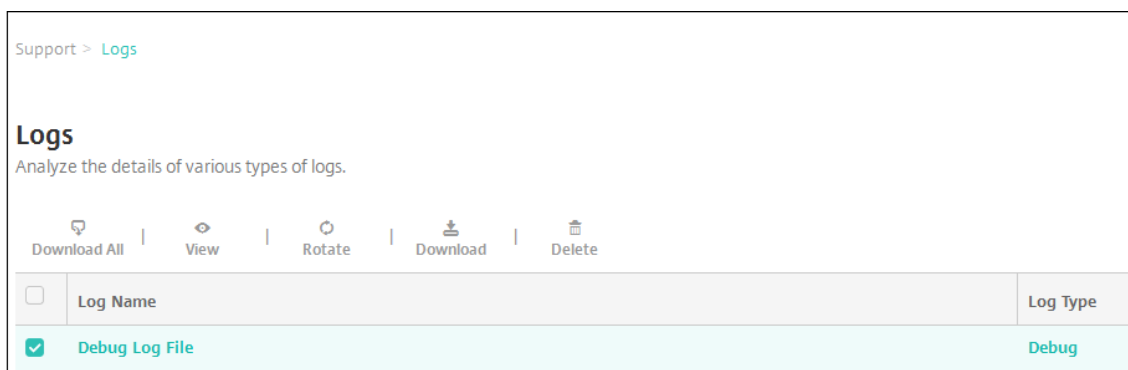
1. No console XenMobile, clique no ícone de chave de boca no canto superior direito do console. A página **Suporte** é aberta.
2. Em **Operações de log**, clique em **Logs**. A página **Logs** é exibida. Logs individuais são exibidos em uma tabela.



<input type="checkbox"/>	Log Name	Log Type	
<input type="checkbox"/>	Debug Log File	Debug	
<input type="checkbox"/>	Admin Audit Log File	Admin Activity	
<input type="checkbox"/>	User Audit Log File	User Activity	

Showing 1 - 3 of 3 items

3. Selecione o log que você deseja exibir:
 - Os Arquivos de Log de Depuração contêm informações úteis para o suporte da Citrix, como mensagens de erro e ações relacionadas.
 - Os Arquivos de Log de Auditoria do Administrador contêm informações de auditoria sobre as atividades no console XenMobile.
 - Os Arquivos de Log de Auditoria do Usuário contêm informações relacionadas aos usuários configurados.
4. Use as ações na parte superior da tabela para baixar tudo, exibir, girar, baixar um único log ou excluir o log selecionado.



Nota:

- Se você selecionar mais de um arquivo de log, somente as opções **Baixar todos** e **Girar** estarão disponíveis.
- Se você tiver servidores XenMobile em cluster, poderá exibir somente os logs do servidor ao qual está conectado. Para ver os logs de outros servidores, use uma das opções de download.

5. Você pode optar por um dos seguintes procedimentos:

- **Baixar todos:** o console baixa todos os logs presentes no sistema (incluindo de depuração, auditoria de administração, auditoria de usuário, logs do servidor e assim por diante).
- **Exibir:** mostra o conteúdo do log selecionado abaixo da tabela.
- **Girar:** Arquiva o arquivo de log atual e cria um novo arquivo para capturar entradas de log. Uma caixa de diálogo aparece quando um arquivo de log é arquivado; clique em Girar para continuar.
- **Baixar:** O console baixa somente o único tipo de arquivo de log selecionado; ele também baixa todos os logs arquivados desse mesmo tipo.
- **Excluir:** Remove permanentemente os arquivos de log selecionados.

Logs
Analyze the details of various types of logs.

Download All | View | Rotate | Download | Delete

<input type="checkbox"/>	Log Name	Log Type
<input checked="" type="checkbox"/>	Debug Log File	Debug
<input type="checkbox"/>	Admin Audit Log File	Admin Activity
<input type="checkbox"/>	User Audit Log File	User Activity

Showing 1 - 3 of 3 items

Log contents for Debug Log File

```

2016-11-06T06:28:38.908-0800 | INFO | node.scheduled.executor-8 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:29:38.926-0800 | INFO | node.scheduled.executor-10 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:30:38.762-0800 | INFO | node.pooled.executor2 | com.citrix.cg.task.handlers.NonPrvsnTask | Begin method executeNonPrvsnTask/job: Sun Nov 06 06:45:38 PST 2016
2016-11-06T06:30:38.766-0800 | INFO | node.pooled.executor2 | com.citrix.cg.task.handlers.NonPrvsnTask | The number of non provision tasks Picked 2.
2016-11-06T06:30:38.945-0800 | INFO | node.scheduled.executor-2 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:31:38.965-0800 | INFO | node.scheduled.executor-9 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:32:38.985-0800 | INFO | node.scheduled.executor-4 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:33:39.3-0800 | INFO | node.scheduled.executor-2 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:34:39.24-0800 | INFO | node.scheduled.executor-8 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:35:39.42-0800 | INFO | node.scheduled.executor-5 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
2016-11-06T06:36:39.502-0800 | INFO | Local 7: thread 11 | com.citrix.feature.FeatureManagerFactory | Enabling local feature management
    
```

Ferramenta XenMobile Analyzer

January 22, 2021

O XenMobile Analyzer é uma ferramenta baseada em nuvem que você pode usar para diagnosticar e resolver problemas relacionados do XenMobile relacionados à configuração e outros recursos. A ferramenta verifica se há registro do dispositivo ou de usuário e problemas de autenticação no seu ambiente do XenMobile.

Configure a ferramenta para apontar para o XenMobile Server e forneça informações, como tipo de implantação de servidor, plataforma móvel, tipo de autenticação e as credenciais do usuário. Em seguida, a ferramenta se conecta ao servidor e examina o ambiente quanto a problemas de configuração. Se o XenMobile Analyzer descobrir problemas, a ferramenta fornece recomendações para corrigir os problemas.

Características principais

- Microsserviço seguro e baseado em nuvem para resolver todos os problemas relativos ao XenMobile.
- Fornece recomendações precisas para resolver problemas de configuração do XenMobile.
- Menos chamadas ao suporte e solução de problemas acelerada de ambientes do XenMobile.
- Suporte de dia zero para versões para XenMobile Server.
- Agendamento de verificação de integridade com frequência diária ou semanal.
- Verificações de configuração do Citrix ADC.
- O Secure Web testa a acessibilidade a sites da intranet.

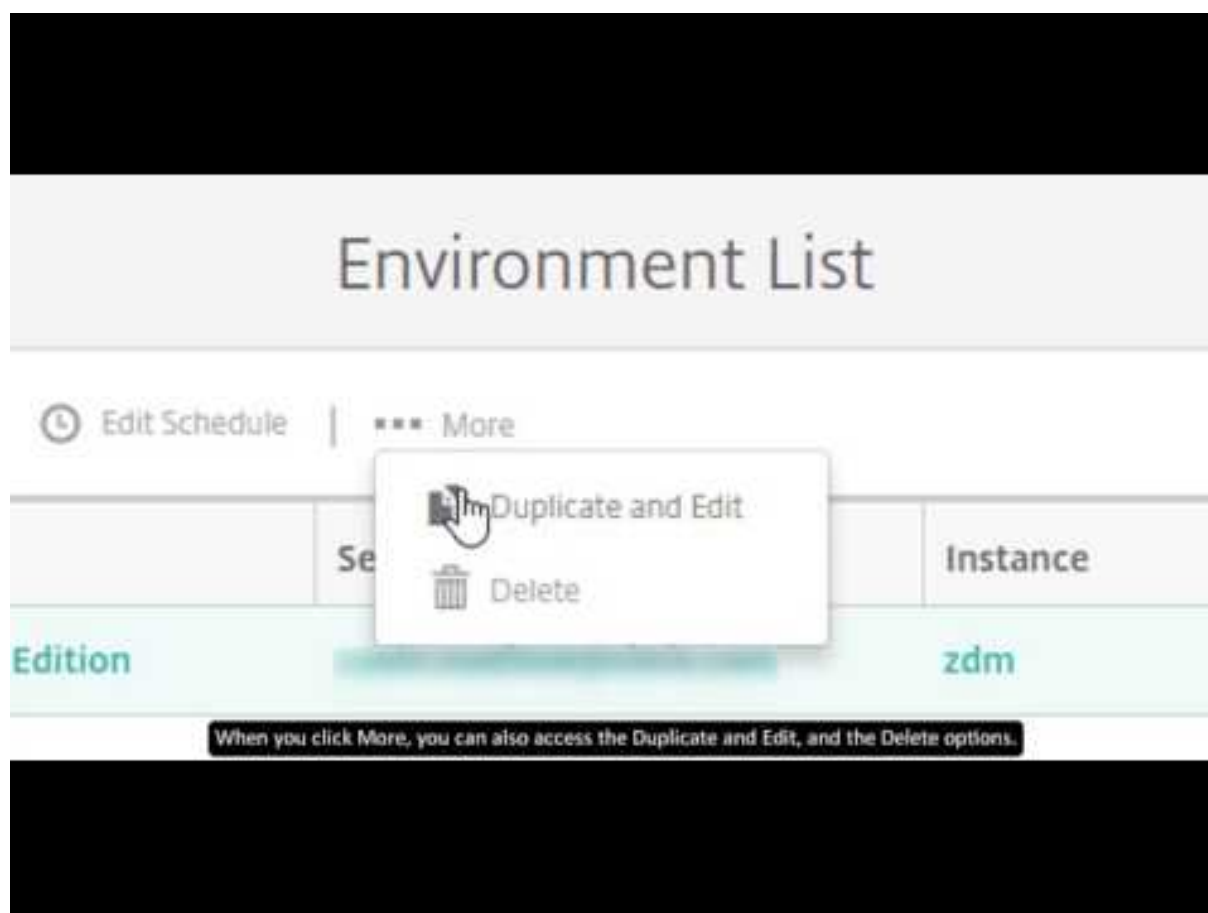
- Verificações de serviço de descoberta automática do Secure Mail.
- Verificações de logon único (SSO) do Citrix Files.

Novidades

- O Relatório de configuração do Citrix ADC exibe uma notificação de selo indicando o número de recomendações. As recomendações baseiam-se nas verificações de Configuração essencial em um Citrix Gateway específico.
- Os ícones na barra de navegação global da página Lista do ambiente de teste foram reordenadas para uma melhor experiência do usuário.

O vídeo a seguir destaca as alterações de navegação na interface do usuário.

Citrix XenMobile Analyzer: nova interface do usuário da lista de ambientes



Nota:

Esse vídeo não contém som de áudio. Ele é melhor visualizado no modo de tela inteira.

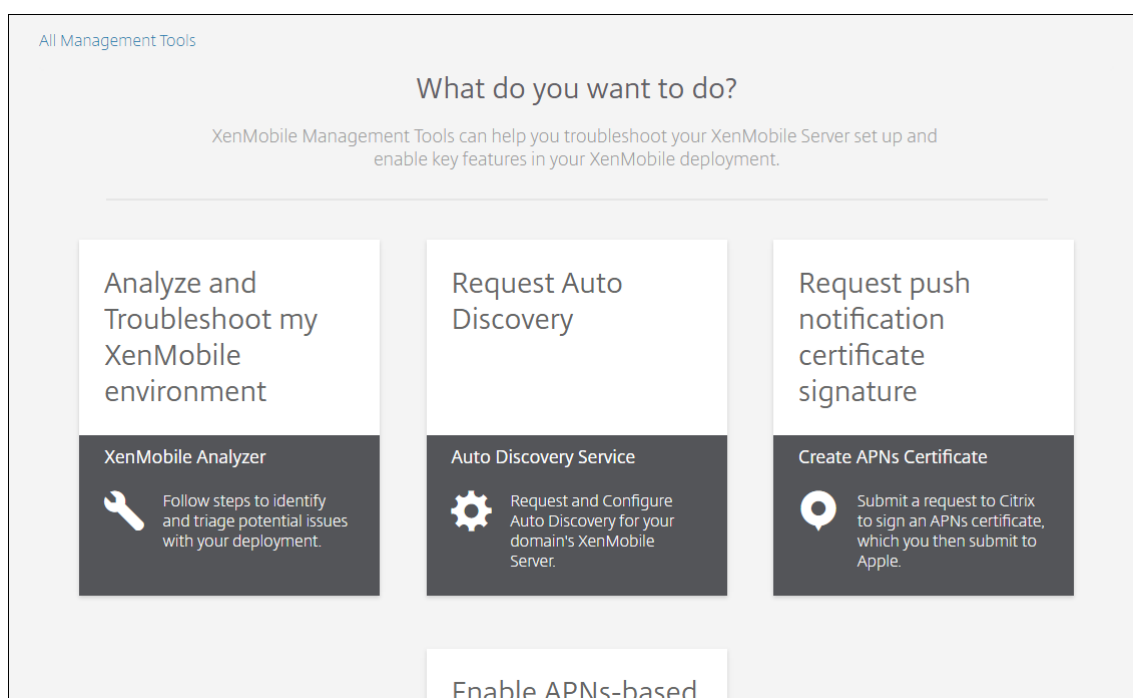
Acessar e iniciar o XenMobile Analyzer

Pré-requisitos

Produto	Versão com suporte
Servidor XenMobile	10.1.0 e posterior
Citrix Gateway	10.5 e versões posteriores
Simulação de registro de cliente	iOS e Android

Acesse o XenMobile Analyzer usando um destes métodos:

- No console XenMobile, clique no ícone de engrenagem no canto superior direito para abrir a página **Solução de problemas e suporte**.
- Use suas credenciais My Citrix para acessar a ferramenta em <https://tools.xm.cloud.com/>. Na página XenMobile Management Tools exibida, para iniciar o XenMobile Analyzer, clique em **Analyze and Troubleshoot my XenMobile Environment**.



O XenMobile Analyzer contém cinco opções criadas para guiar você durante o processo de separação e para reduzir o número de tíquete de suporte. As opções podem reduzir os custos para todos.

As opções são as seguintes:

- **Environment Check:** Esta etapa o orienta na configuração de testes para verificar a configuração em caso de problemas. A etapa também fornece recomendações e soluções para proble-

mas no dispositivo, registro de usuário e autenticação.

- **Citrix ADC Check:** Esta etapa o orienta na verificação das suas configurações do Citrix ADC para preparação de implantação do XenMobile.
- **Advanced Diagnostics:** Esta etapa fornece informações sobre como usar o Citrix Insight Services para encontrar mais problemas que a verificação de ambiente possa ter deixado de detectar.
- **Server Connectivity Checks:** Esta etapa instrui você a testar a conectividade dos seus servidores.
- **Contact Citrix Support:** Esta etapa conecta você ao site onde você poderá criar um caso de suporte da Citrix.

As seções a seguir descrevem cada opção com mais detalhes.

Execução de uma verificação de ambiente

1. Faça login no XenMobile Analyzer e clique em **XenMobile Environment**.



2. Clique em **Add Test Environment**.
3. Na caixa de diálogo **Add Test Environment**, faça o seguinte:

- a) Forneça um nome exclusivo para o teste que o ajude a identificar o teste no futuro.
 - b) Em **FQDN, UPN login, Email or URL Invitation**, digite as informações usadas para acessar o servidor.
 - c) Em **Instance Name**, se você usar uma instância personalizada, poderá fornecer esse valor.
 - d) Em **Choose Platform**, selecione **iOS** ou **Android** como a plataforma para teste.
 - e) Se você expandir **Advanced Deployment Options**, na lista **Deployment Mode**, você pode selecionar o modo de implantação do XenMobile 1. As opções disponíveis são **Enterprise (MDM + MAM)**, **App Management (MAM)** ou **Device Management (MDM)**.
 - f) Clique em **Continue**.
4. Na guia **Test Options**, escolha um ou mais dos seguintes testes e clique em **Continue**.
 - a) **Conectividade do Secure Web**. Forneça uma URL de intranet. A ferramenta testa a acessibilidade da URL. Isso detecta se há problemas de conectividade que possam ocorrer no aplicativo Secure Web ao tentar acessar URLs de intranet.

- b) **ADS do Secure Mail.** Forneça um ID de email de usuário. Essa ID é usada para testar a detecção automática do Microsoft Exchange Server em seu ambiente XenMobile. Ele detecta se há problemas relacionados à detecção automática do Secure Mail.
- c) **ShareFile SSO.** Se selecionado, o XenMobile Analyzer testará se a resolução DNS do Citrix Files tem êxito. A ferramenta também verifica se o logon único (SSO) do Citrix Files é compatível com as credenciais de usuário fornecidas.

The screenshot shows the 'Add Test Environment' dialog box. The environment name is 'testdev02'. The 'Test Options' tab is active, showing three optional connectivity tests: 'Secure Web connectivity', 'ShareFile SSO', and 'Secure Mail ADS', all of which are checked. There are input fields for the URL and email address for the checked options. 'Back' and 'Continue' buttons are at the bottom right.

5. Na guia **User Credentials**, dependendo da configuração do servidor, você verá campos diferentes. Os campos possíveis são **Username, Username e Password** ou **Username, Password e Enrollment PIN**.

testdev02

Environment Details Test Options **User Credentials**

Secure Hub User Credentials ⓘ

Note: XenMobile Analyzer tool does not store credentials.

Username ⓘ

Enter user account to test

Password

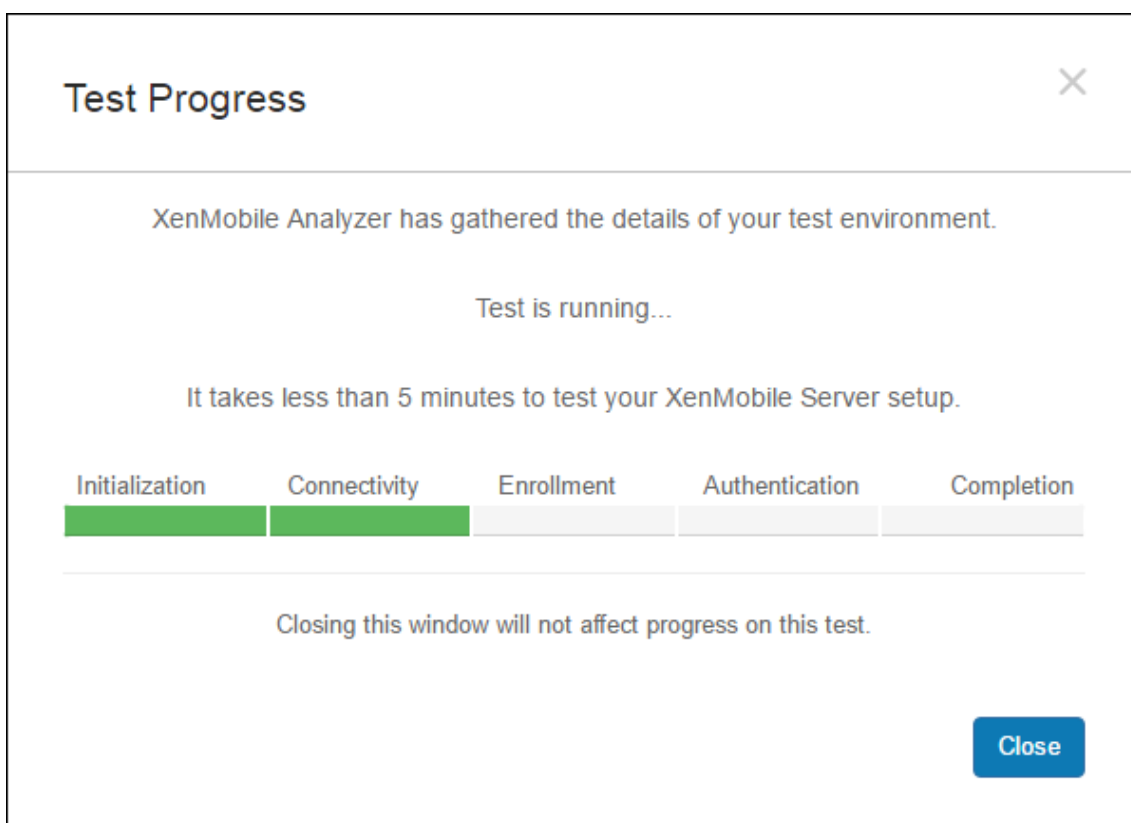
Enter password for user account

Back **Save & Run**

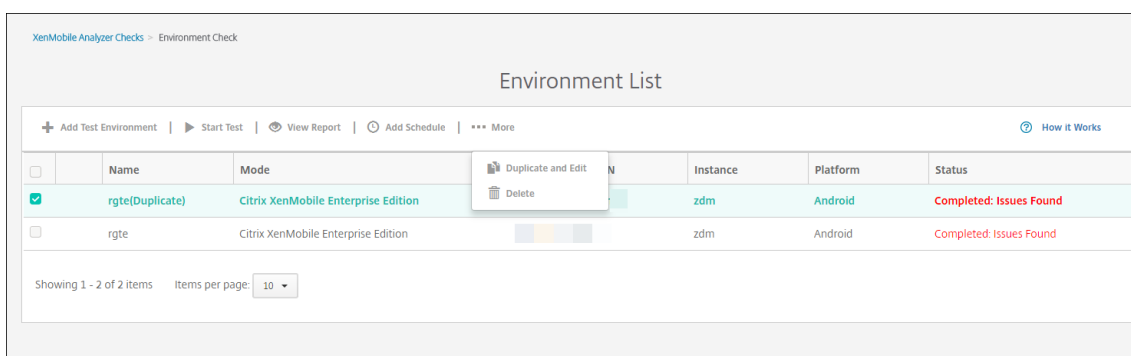
6. Clique em **Save & Run** para iniciar os testes.

Uma notificação de progresso é exibida. Você pode deixar a caixa de diálogo de progresso aberta ou fechar a caixa de diálogo a execução dos testes continua.

Os testes com aprovação aparecem em verde. Testes sem aprovação aparecem em vermelho.



Depois de fechar a caixa de diálogo de progresso, você poderá retornar à página **Environments List**.



A página **Results** mostra resultados do teste, recomendações e resultados.

7. Clique no ícone **View Report** para ver resultados do teste.

Se as recomendações tiverem um artigo da Base de Conhecimento da Citrix associado, esse artigo aparecerá nesta página.

8. Clique na guia **Results** para exibir a categoria e os testes que a ferramenta executou, com seus resultados.

a) Para baixar o relatório, clique em **Download Report**.

b) Para retornar à lista de ambientes de teste, clique em **Environment Check**.

- c) Para executar novamente o mesmo teste, clique em **Run Again**.
- d) Se você deseja executar novamente outro teste, volte para **Test Environments**, selecione o teste e clique em **Start Test**.
- e) Para selecionar outra opção do XenMobile Analyzer, clique em **Go To XenMobile Analyzer Checks**.

XenMobile Analyzer Checks > Environment Check > Report

Check Report

Check Complete: No Issues Found

Check Summary

Test Environment: testdoc
 Start Time: 2017-Jun-07 12:26 PM UTC
 Deployment Mode: Citrix XenMobile Enterprise Edition
 Server FQDN: navin.mathew@citrix.com
 Platform: iOS

[Edit Schedule](#) [Run Again](#)

Do you need assistance?

[Citrix Support is here to help!](#)

For additional information, please refer to the [Support Knowledge Center](#)

Download and share this report with your Citrix Support contact.

[Download Report](#)

Next, continue troubleshooting the XenMobile Environment using additional recommended checks:

[Troubleshoot the ActiveSync server using Secure Mail Test Tool.](#)

[Test connectivity of XenMobile Server and NetScaler Gateway.](#)

[Analyze logs and scan for known issues using Citrix Insight Services.](#)

[Go to XenMobile Analyzer Checks](#)

Detailed Results ✔

View all details of your test ^

	Category	Checks	Results
✔	Initialization and Connectivity	XenMobile Server FQDN DNS Resolution	Pass
		XenMobile Server FQDN Connectivity	Pass
		XenMobile Server Certificate Validation	Pass
		XenMobile Server instance name validation	Pass
✔	Enrollment	Enrollment Authentication	Pass
		XenMobile Enrollment	Pass
✔	Authentication	Is NetScaler Gateway configured?	Yes
		NetScaler Gateway Cert Auth Enabled?	No
		NetScaler Gateway DNS Resolution	Pass
		NetScaler Gateway Connectivity	Pass
		NetScaler Gateway Certificate Validation	Pass
		NetScaler Gateway Login	Pass
		XenMobile Server connectivity through NetScaler Gateway	Pass
		XenMobile Server Authentication	Pass
✔	App Enumeration	Store Connectivity	Pass
		Device Registration	Pass
		Store App Listing	Pass
⚠	Secure Web Connectivity	NetScaler Gateway DNS Resolution	Not Tested
		NetScaler Gateway server connectivity	Not Tested
⚠	ShareFile	ShareFile Subdomain Discovery	Not Tested
		ShareFile SAML SSO	Not Tested
⚠	Secure Mail ADS	Secure Mail Auto Discovery	Not Tested
✔	Logout	XenMobile Server Logout	Pass
		NetScaler Gateway Logout	Pass

9. Na página ambientes de teste, você pode copiar e editar testes. Para fazer isso, selecione um teste e, em seguida, clique em **More** e selecione **Duplicate and Edit**.

Uma cópia do teste selecionada é criada e a caixa de diálogo Adicionar ambiente de teste é aberta, permitindo que você modifique o novo teste.

Versão atual do XenMobile Server

XenMobile Analyzer Checks > Environment Check

Environment List

+ Add Test Environment | ▶ Start Test | 👁 View Report | ⌚ Add Schedule | ⋮ More 🔗 How it Works

<input type="checkbox"/>	Name	Mode	Instance	Platform	Status
<input checked="" type="checkbox"/>	rgte(Duplicate)	Citrix XenMobile Enterprise Edition	zdm	Android	Completed: Issues Found
<input type="checkbox"/>	rgte	Citrix XenMobile Enterprise Edition	zdm	Android	Completed: Issues Found

Showing 1 - 2 of 2 items Items per page: 10

Note: A context menu is open over the first row, showing 'Duplicate and Edit' and 'Delete' options.

XenMobile Analyzer Checks > Environment Check

Environment List

+ Add Test Environment | 🔄 Refresh 🔗 How it Works

<input type="checkbox"/>	Name	Mode	Server/Email/UPN	Instance	Platform	Status
<input type="checkbox"/>	rgte(Duplicate)	Citrix XenMobile Enterprise Edition		zdm	Android	Completed: Issues Found
<input type="checkbox"/>	rgte	Citrix XenMobile Enterprise Edition				Completed: Issues Found

Showing 1 - 2 of 2 items Items per page: 10

Note: A context menu is open over the second row, showing 'Start Test', 'View Report', 'Add Schedule', 'Duplicate and Edit', and 'Delete' options.

Add Test Environment ✕

Environment Details
Test Options
User Credentials

FQDN, UPN login, Email or Invitation URL ?

Click to enter

Instance Name ?

zdm

Choose Platform

iOS
 Android

Advanced Deployment Options ∨

Cancel

Continue

Adicionar um agendamento para verificações de ambiente

Você pode configurar testes para executar em um agendamento automático com resultados enviados para uma lista de usuários que você configura.

1. Na página **Environment List**, selecione o ambiente para a qual você deseja agendar e clique em **Add Schedule**.

XenMobile Analyzer Checks > Environment Check

Environment List

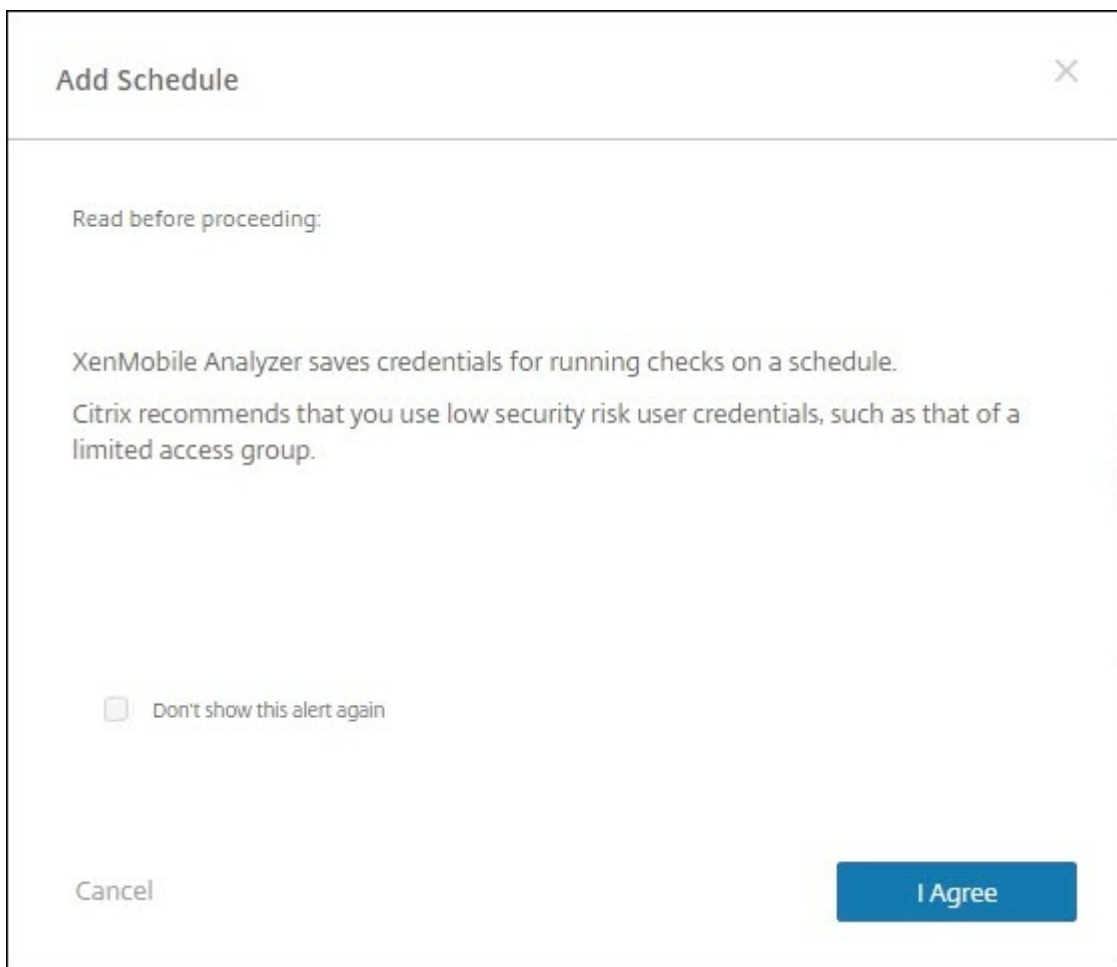
+ Add Test Environment | Refresh
How it Works

	Name	Mode	Server/Email/UPN	Instance	Platform	Status
<input type="checkbox"/>	rgte(Duplicate)	Citrix XenMobile Enterprise Edition		zdm	Android	Completed: Issues Found
<input type="checkbox"/>	rgte	Citrix XenMobile E				Completed: Issues Found

▶ Start Test
👁 View Report
🕒 Add Schedule
📄 Duplicate and Edit
🗑 Delete

Showing 1 - 2 of 2 items Items per page: 10

2. A janela **Add Schedule** exibe uma mensagem para avisar você que o XenMobile Analyzer salva as credenciais para executar testes em um agendamento. A Citrix recomenda que você use uma conta com acesso limitado para executar testes programados. Clique em **I Agree**.



3. Digite um **Nome de usuário** e **Senha** para executar o teste.

Add Schedule [X]

Enter credentials for the check

Test Name: testdoc

Environment Information

FQDN, UPN Login, Email

Instance Name
zdm

Platform
iOS

Secure Hub User Credentials

Username
Enter user account to test

Password
Enter password for user account

Note: Citrix stores this password securely

Cancel [Back] [Continue]

4. Configure um agendamento para execução do teste. Selecione **Daily** ou **Weekly** no menu suspenso. Selecione uma hora do dia para executar o teste e um fuso horário. Use o botão para selecionar uma data para que o teste agendado pare de ser executado ou deixe em branco para que o teste seja executado indefinidamente. Forneça uma lista de endereços de email para receber relatórios, separados por vírgulas. Clique em **Salvar**.

Add Schedule

When should it run?
Daily 6:15 PM

When should it end?
Never

Recipients
Enter email addresses to receive reports, separated by commas.

Cancel Back Save

- Um símbolo de relógio à esquerda do seu teste indica que está configurado um agendamento. Se você selecionar o seu teste, você pode clicar em **Edit Schedule** para alterar quando o teste for executado.

XenMobile Analyzer Checks - Environment Check

Environment List

	Name	Mode	Server/Email/UPN	Instance	Platform	Status
<input checked="" type="checkbox"/>	testdoc	Citrix XenMobile Enterprise Edition	@citrix.com	zdm	iOS	Completed: No Issues Found

Showing 1 - 1 of 1 items Items per page: 10

Start Test View Report Delete Duplicate and Edit Edit Schedule

- Nessa janela, você pode alterar quando o teste deve ser executado. Você também pode desativá-lo, clicando no botão na parte superior. Clique em **Salvar** quando terminar.

Edit Schedule

Run checks automatically during this schedule ON
You can turn on/off schedule at any time.

When should it run?

Daily 6:15 PM (UTC-11:00) Midway Island, Samoa

When should it end?

06/08/2017

Recipients

@citrix.com

Cancel Edit Credentials Save

Realizar outras verificações informativas

Você interage com a etapa Environment Check do XenMobile Analyzer diretamente para executar testes, enquanto as outras opções são informativas. Cada uma dessas opções fornece informações relativas às outras ferramentas de suporte que você pode usar para garantir que o seu ambiente do XenMobile seja configurado corretamente.

- **Advanced Diagnostics:** essa etapa instrui você a coletar informações sobre o seu ambiente e depois carregar as informações em Citrix Insight Services. A ferramenta analisa os dados e fornece um relatório personalizado com resoluções recomendadas.
- **Secure Mail Readiness:** essa etapa direciona você a baixar e executar o aplicativo XenMobile Exchange ActiveSync Test. O aplicativo resolve os problemas de servidores ActiveSync que a sua prontidão seja implantada com ambientes do XenMobile. Depois que o aplicativo for executado, você poderá exibir relatórios ou compartilhá-los com outras pessoas.
- **Server Connectivity Checks:** fornece instruções para verificar suas conexões com servidores XenMobile, Authentication e Content Collaboration.
- **Contact Citrix Support:** se nada mais funcionar, você poderá criar um tíquete de suporte com o suporte da Citrix.

Problemas conhecidos

Os seguintes problemas são conhecidos no XenMobile Analyzer:

- Ao realizar as verificações de conectividade do Secure Web, não é possível digitar várias URLs no caixa de texto.
- O recurso de autenticação de dispositivos compartilhados Secure Hub não tem suporte.
- O Secure Web testa somente verificar a conectividade com as URLs inserido e não a autenticação para sites correspondentes.

Problemas resolvidos

Os seguintes problemas com o XenMobile Analyzer foram corrigidos:

- Ao realizar uma verificação usando o convite para registro, passa o teste, mas o convite de registro não é trocado.

APIs REST

April 23, 2020

Nota:

Este artigo aborda as APIs REST para o XenMobile Server. Para as APIs REST para Endpoint Management, consulte [APIs REST](#).

Com a API REST do XenMobile, você pode chamar os serviços que são expostos por meio do console XenMobile. Você pode chamar os serviços REST usando um cliente REST. A API não exige que você faça logon no console XenMobile para chamar os serviços.

Para obter o conjunto completo e atual de APIs disponíveis, baixe o PDF [Public API for REST Services](#).

Permissões necessárias para acessar a API REST

Você precisa de uma das seguintes permissões para acessar a API REST:

- Permissão de acesso à API pública definida como parte da configuração de acesso com base em função. Para obter informações, consulte [Configuração de funções com RBAC](#).
- Permissão de superusuário

Para invocar os serviços da API REST

Você pode chamar os serviços da API REST usando o cliente REST ou comandos CURL. Os exemplos a seguir usam o cliente Advanced REST para Chrome.

Nota:

Nos exemplos a seguir, altere o nome de host e o número de porta para corresponder ao seu ambiente.

Login

URL: `https://<host-name>:<port-number>/xenmobile/api/v1/authentication/login`

Solicitação: { `"login": "administrator", "password": "password"`}

Tipo de método: POST

Tipo de conteúdo: application/json

The screenshot shows a REST client interface with the following details:

- URL:** `https://localhost:4443/xenmobile/api/v1/publicapi/login`
- Method:** POST (selected)
- Headers:** (Empty)
- Payload:**

```
{
  "login": "administrator",
  "password": "password"
}
```
- Content-Type:** application/json
- Status:** 200 OK (Loading time: 265 ms)
- Request headers:** User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/41.0.2272.101 Safari/537.36; Origin: chrome-extension://hgml0oofddffnphfgceilkdfbfjelo; Content-Type: application/json; Accept: */*; Accept-Encoding: gzip, deflate; Accept-Language: en-US,en;q=0.8; Cookie: JSESSIONID=6D607670BBCD51DE59CBFD6D91F9B163
- Response headers:** Server: Apache-Coyote/1.1; Content-Type: text/plain; Content-Length: 53; Date: Sun, 22 Mar 2015 22:43:48 GMT
- Response:**

```
{
  "auth_token": ""
}
```

Informações correlatas

- [API REST do XenMobile](#)

Conector de Endpoint Management para Exchange ActiveSync

January 22, 2021

O XenMobile Mail Manager é agora o conector de Endpoint Management para Exchange ActiveSync. Para obter mais detalhes sobre o portfólio unificado da Citrix, consulte o [Guia do produto Citrix](#).

O conector amplia os recursos do XenMobile das seguintes maneiras:

- Controle de Acesso Dinâmico para os dispositivos Exchange Active Sync (EAS). Os dispositivos EAS podem receber automaticamente permissão ou bloqueio de acesso aos serviços do Exchange.
- A capacidade para que o XenMobile acesse as informações de parceria do dispositivo EAS fornecidas pelo Exchange.
- A capacidade para que o XenMobile apague um dispositivo móvel com base no status do EAS.
- A capacidade para que o XenMobile acesse informações sobre dispositivos BlackBerry e execute operações de controle, como Wipe e ResetPassword.

Para apagar um dispositivo com base no status do EAS, configure uma ação automatizada com um gatilho do ActiveSync. Veja [Ações automatizadas](#).

Para baixar o conector de Endpoint Management para Exchange ActiveSync:

1. Acesse <https://www.citrix.com/downloads>.
2. Navegue para **Citrix Endpoint Management (e Citrix XenMobile Server) > XenMobile Server (no local) > Product Software > XenMobile Server 10 > Server Components**.
3. No bloco **Citrix Endpoint Management connector for Exchange ActiveSync**, clique em **Download File**.

Novidades

As seções a seguir listam o que há de novo no conector de Endpoint Management para Exchange ActiveSync, anteriormente XenMobile Mail Manager.

O que há de novo na versão 10.1.10

Os seguintes problemas foram resolvidos na versão 10.1.10:

- Os clientes que enfrentam problemas de rede frequentes podem não conseguir concluir um instantâneo nas três tentativas oferecidas previamente. Com essa versão, um administrador pode configurar o número máximo de tentativas (1-10). Essa correção permite que um instantâneo incorra em várias interrupções na comunicação sem abandonar completamente o

processo de captura de instantâneo. [CXM-70837]

The screenshot shows a 'Configuration' dialog box with the following settings:

- Type: On Premise
- Exchange Server: [Empty]
- User: [Empty]
- Password: [Empty]
- Major snapshot: Every 4 Hours
- Minor snapshot: Every 5 Minutes
- Snapshot Type: Shallow
- Default Access: Unchanged
- Command Mode: Powershell
- Connection Expiration: Every 00 Hours 30 Minutes
- Enable Diagnostics:
- Days to Keep Snapshot Data: 00
- Snapshot Maximum Attempts: 03
- View Entire Forest:
- Authentication: Kerberos
- Allow Redirection:

Buttons: Test Connectivity, Save, Cancel

- Nas versões anteriores, o tipo de Instantâneo não aparecia na lista de Configurações do Exchange. Agora, o tipo de instantâneo é exibido. [CXM-70846]
- A exceção PSRemotingTransport notificada pelo PowerShell indica que a sessão para o Exchange não é mais viável. O status é adicionado à lista de Erros Críticos no arquivo de configuração por padrão. Com isso, quando o PSRemotingTransportException é detectado, a conexão é marcada como em Erro para eliminação posterior. A próxima comunicação usa uma conexão válida ou cria uma nova conexão. [XMHELP-2184, CXM-70836]
- Quando uma alteração de configuração é salva, é possível que nem todos os componentes internos configurados anteriormente tenham sido descartados corretamente antes de carregar a nova configuração. Esse problema pode levar a um comportamento imprevisível. O comportamento depende da alteração específica e se a alteração entrou em conflito com a configuração anterior. Nesta versão, todos os componentes internos são descartados antes de carregar a nova configuração. [XMHELP-2259, CXM-71388]

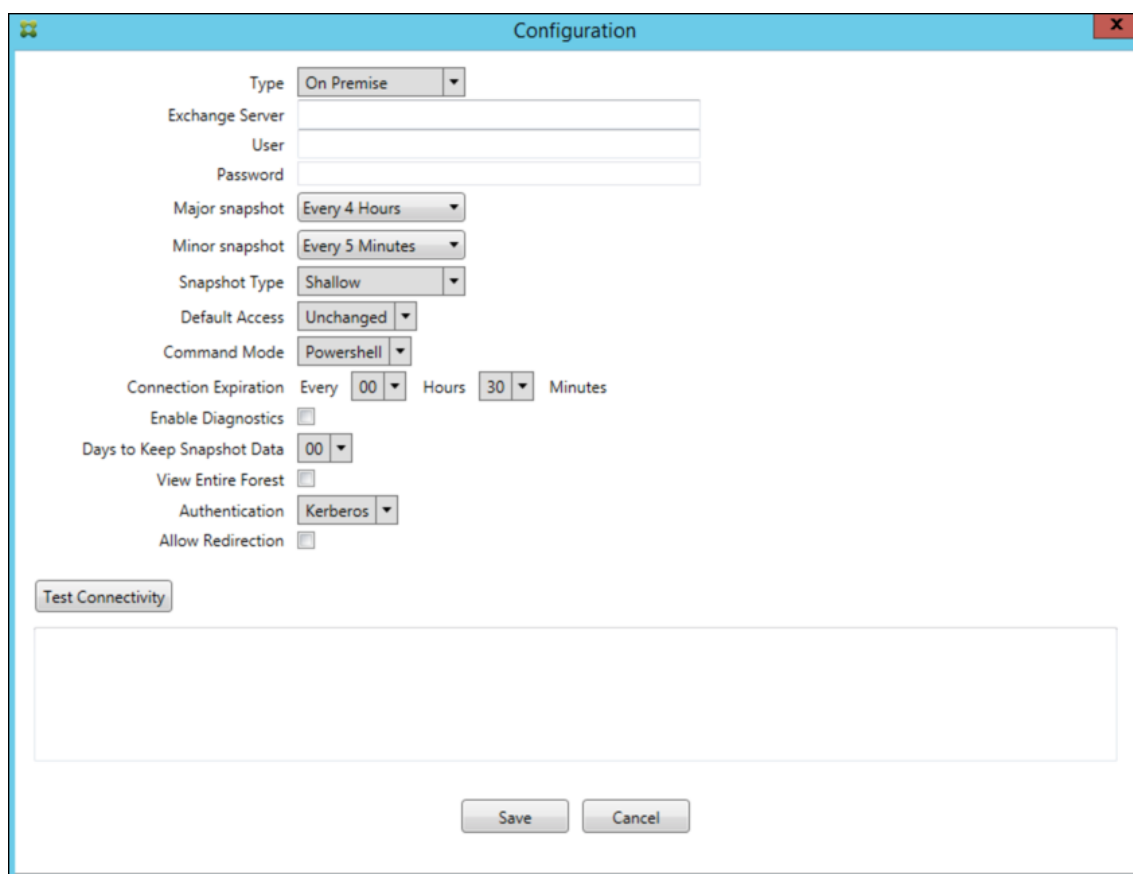
O que há de novo em versões anteriores

A seção a seguir lista os recursos e os problemas corrigidos em versões anteriores do conector de Endpoint Management para Exchange ActiveSync.

O que há de novo na versão 10.1.9

Os seguintes problemas foram resolvidos na versão 10.1.9:

- As alterações de configuração agora são tratadas de forma mais consistente. Quando o serviço detecta uma alteração na configuração, cada subsistema interno é interrompido, o que significa que qualquer processamento ativo ou agendado é interrompido. Em seguida, a nova configuração é carregada e os subsistemas são iniciados novamente, o que significa que todas as programações e outras infraestruturas internas são restabelecidas com novas configurações. Esse problema corrige um problema conhecido na versão 10.1.8. [CXM-47709, CXM-61330]
- Durante uma atualização, a configuração de banco de dados existente não foi mesclada com o novo arquivo de configuração. A configuração do banco de dados é agora agrupada ao arquivo de configuração atualizado. [CXM-49326]
- Nos arquivos de diagnóstico relacionados a instantâneos, os cabeçalhos de coluna estavam ausentes. Os cabeçalhos são restaurados. [CXM-62680]
- Ao atualizar a partir de uma versão anterior, a seção padrão do arquivo de configuração era substituída pela seção análoga do arquivo de configuração em uso. Esse problema impedia que adições ou melhorias na seção padrão fossem carregadas pelo serviço após a atualização. A partir desta versão, a seção padrão sempre reflete a configuração mais recente. [CXM-62681]
- Os administradores não podem mais acessar determinadas opções pressionando Shift com o aplicativo em execução. Essas opções estavam disponíveis anteriormente com permissão Citrix. Algumas opções agora estão totalmente disponíveis, como Permitir Redirecionamento, e outras, como Detecção de travamento e Correção de contagem, estão obsoletas. [CXM-62767]



O que há de novo na versão 10.1.8

Os seguintes problemas foram resolvidos na versão 10.1.8:

- É possível que o Exchange faça com que o conector Citrix Endpoint Management limite a emissão de comandos para o serviço Exchange ActiveSync com muita frequência. Isso é comum em conexões com o Office 365. O efeito da limitação requer que o serviço pause por um período de tempo especificado antes de enviar o próximo comando. O console Configure agora mostra o tempo restante em pausa. [CXM-48044]
- Quando são feitas modificações nas seções “Watchdog” ou “SpecialistsDefaults” do arquivo de configuração (config.xml), as alterações não são refletidas no arquivo de configuração após uma atualização. Nesta versão, as modificações são mescladas corretamente no novo arquivo de configuração. [CXM-52523]
- Mais detalhes foram adicionados às análises enviadas ao Google Analytics, especialmente no que diz respeito aos instantâneos. [CXM-56691]
- O recurso de conectividade de teste do Exchange tentava inicializar a conexão apenas uma vez. Uma vez que as conexões do Office 365 podem ser limitadas, era possível que uma conectividade de teste parecesse falhar quando ficava limitada. O conector Citrix Endpoint Management para Exchange ActiveSync agora tenta iniciar uma conexão até três vezes. [CXM-58180]

- Para efetivar políticas no Exchange, o conector Citrix Endpoint Management para Exchange ActiveSync deve compilar um comando **Set-CASMailbox** que inclua todos os dispositivos pertinentes para cada caixa de correio, em duas listas: permitir e bloquear. Se um dispositivo não estiver incluído em nenhuma das listas, o Exchange volta ao seu estado de acesso padrão. Se esse estado de acesso padrão for diferente do estado desejado para um dispositivo, o dispositivo ficará fora de conformidade. Consequentemente, um usuário pode perder o acesso ao email se o estado de acesso padrão do Exchange estiver bloqueado quando deveria ser permitido. Ou, um usuário cujo acesso ao email deveria ser bloqueado pode ter o acesso permitido. O conector Citrix Endpoint Management para Exchange ActiveSync agora garante que todos os dispositivos com um estado desejado válido sejam incluídos em cada comando **Set-CasMailbox**. [CXM-61251]

O seguinte problema é conhecido na versão 10.1.8:

Se um administrador fizer uma alteração no aplicativo Configure que modifique os dados de configuração, enquanto o serviço estiver executando operações de longa duração, como uma avaliação de política ou um instantâneo, o serviço pode entrar em um estado indeterminado. Um possível sintoma seria as alterações na política não serem processadas ou os instantâneos não serem iniciados. Para retornar o serviço a um estado de funcionamento, o serviço deve ser reiniciado. Talvez seja necessário usar o gerenciador de Serviços do Windows para encerrar o processo de serviço antes de iniciar o serviço. [CXM-61330]

O que há de novo na versão 10.1.7

- O XenMobile Mail Manager é agora o conector de Endpoint Management para Exchange ActiveSync.
- Nós substituímos a opção **Desativar Pipelining** na caixa de diálogo de configuração do Exchange. Você pode obter a mesma funcionalidade configurando várias etapas para cada comando no arquivo config.xml. [CXM-54593]

Os seguintes problemas foram resolvidos na versão 10.1.7:

- Na janela Histórico da Captura Instantânea, as mensagens de erro eram exibidas com pouco contexto. Agora, as mensagens de erro são prefixadas com o contexto de onde ocorreram. [CXM-49157]
- O arquivo .dll do XmmGoogleAnalytics não tinha a versão do arquivo correspondente para o lançamento. [CXM-52518]
- Para melhorar o diagnóstico, recentemente alteramos o formato da cadeia de caracteres para uma lista de IDs de dispositivos usados para definir um estado Permitido/Bloqueado da caixa de correio. Uma especificação de muitos dispositivos, no entanto, excedeu o tamanho máximo da cadeia de caracteres. Agora, usamos uma estrutura de dados de matriz interna. Essa estrutura não tem limite de tamanho e também formata os dados adequadamente para fins de

diagnóstico. [CXM-52610]

- Quando detectadas políticas de dispositivo que não estão em sincronia com o Exchange, seus comandos podem incluir dispositivos que não pertencem à caixa de correio relevante. O conector do Endpoint Management para Exchange ActiveSync agora garante que os comandos para o Exchange representem apenas os dispositivos que pertencem a suas respectivas caixas de correio. [CXM-54842]
- Em alguns ambientes, um assembly da Microsoft não está disponível. O assembly necessário agora é explicitamente instalado com o aplicativo. [CXM-55439]
- Se Nomes diferenciados para dispositivos ou caixas de correio tiverem espaços entre o nome do atributo e os iguais e/ou espaços após os iguais e antes do valor, o conector do Endpoint Management do Exchange ActiveSync podia não corresponder corretamente um dispositivo com a sua caixa de correio e vice-versa. O resultado era que alguns dispositivos e/ou caixas de correio podiam ser rejeitados durante a reconciliação de instantâneos. [CXM-56088]

Nota:

As seções a seguir se referem ao conector do Endpoint Management para Exchange ActiveSync por seu nome anterior, XenMobile Mail Manager. O nome foi alterado a partir da versão 10.1.7.

Atualização na versão 10.1.6.20

Uma atualização para 10.1.6 contém a seguinte correção na versão 10.1.6.20:

- Quando detectadas políticas de dispositivo que não estão em sincronia com o Exchange, seus comandos podem incluir dispositivos que não pertencem à caixa de correio relevante. O XenMobile Mail Manager agora garante que os comandos para o Exchange representem apenas os dispositivos que pertencem a suas respectivas caixas de correio. [CXM-54842]

O que há de novo na versão 10.1.6

O XenMobile Mail Manager versão 10.1.6 apresenta os seguintes problemas corrigidos e aprimoramentos:

- A janela de histórico do instantâneo (Snapshot History), às vezes, entrava em um estado em que sua atualização não era mais realizada. O mecanismo de atualização de janelas foi aprimorado para oferecer uma atualização mais confiável. [CXM-47983]
- Dois modos e caminhos de código separados eram usados para instantâneos particionados e não particionados. Como os instantâneos não particionados são equivalentes aos instantâneos particionados com uma configuração usando uma única partição “*”, o modo de instantâneo não particionado foi eliminado. O modo de instantâneo padrão é agora formado de instantâneos particionados com 36 partições (0–9, A – Z). [CXM-49093]

- Na janela Snapshot History de histórico do instantâneo, as mensagens de erro eram substituídas por mensagens de status. Agora, o XenMobile Mail Manager fornece dois campos separados para que os usuários possam visualizar status e erros simultaneamente. [CXM-51942]
- Ao se conectar ao Exchange Online (Office 365), as consultas relacionadas à captura instantânea podiam resultar em um conjunto de dados truncado. Esse problema ocorria quando o XenMobile Mail Manager executava um script com pipelines de vários comandos. O comando upstream não pode passar os dados com rapidez suficiente para o comando downstream, que conclui o trabalho prematuramente; o resultado são dados incompletos. O XenMobile Mail Manager agora pode imitar o próprio pipeline e aguardar até que o comando upstream seja realizado antes de chamar o comando downstream. Essa alteração resulta em todos os dados processados e capturados. [CXM-52280]
- Se ocorre um erro não resolvível em um comando de atualização de política para o Exchange, o mesmo comando é retornado à fila de trabalho repetidamente por um longo período. Essa situação resultava no envio do comando ao Exchange várias vezes. Nesta versão do XenMobile Mail Manager, um comando que resulta em um erro só é retornado para a fila de trabalho um pequeno número de vezes. [CXM-52633]
- Se a atualização de uma política de uma caixa de correio específica envolvesse a permissão ou o bloqueio de todos os dispositivos, o comando **Set-CASMailbox** emitido falhava devido à conversão da lista vazia em uma cadeia de caracteres vazia em vez de **NULL**. Os dados apropriados são enviados agora. [CXM-53759]
- Ao processar um novo dispositivo, o Exchange pode retornar o estado como “DeviceDiscovery” por um período (geralmente 15 minutos). O XenMobile Mail Manager não estava manipulando especificamente esse estado. O XenMobile Mail Manager agora manipula o estado. Na guia Monitor da interface do usuário, os usuários podem filtrar dispositivos nesse estado. [CXM-53840]
- O XenMobile Mail Manager não verificava a capacidade de gravar no banco de dados do XenMobile Mail Manager. Consequentemente, se as permissões fossem restritas, o comportamento não podia ser previsto. O XenMobile Mail Manager agora captura e valida as permissões necessárias do banco de dados. O XenMobile Mail Manager indica permissões reduzidas ao testar a conexão (mensagem mostrada) ou no indicador de banco de dados (passando o cursor sobre a mensagem) na parte inferior da janela principal de configuração. [CXM-54219]
- Dependendo da carga de trabalho atual, quando direcionado, o serviço XenMobile Mail Manager nem sempre parava imediatamente. Portanto, o serviço parecia estar em um estado letárgico. Com as melhorias, as tarefas contínuas são interrompidas, resultando em um desligamento mais fácil. [CXM-54282]

O que há de novo na versão 10.1.5

O XenMobile Mail Manager versão 10.1.5 apresenta os seguintes problemas corrigidos:

- Quando o Exchange está aplicando a limitação à atividade do XenMobile Mail Manager, não há

nenhuma indicação (fora dos logs) de que a limitação está ocorrendo. Com esta versão, um usuário pode passar o mouse sobre o instantâneo ativo e um estado de “limitação” aparece. Além disso, enquanto o XenMobile Mail Manager está sendo limitado, o início de um instantâneo principal é proibido até que o Exchange elimine o embargo de limitação. [CXM-49617]

- Se o XenMobile Mail Manager estiver sendo limitado pelo Exchange durante um instantâneo principal, é possível que uma quantidade insuficiente de tempo passe antes da execução da próxima tentativa de criar um instantâneo. Esse problema resulta em mais limitação e em um instantâneo com falha. Agora, o XenMobile Mail Manager aguarda o tempo mínimo especificado pelo Exchange entre as tentativas de captura instantânea. [CXM-49618]
- Quando o diagnóstico está ativado, o arquivo de comandos mostra comandos **Set-CasMailbox** com hifens ausentes antes do nome de cada propriedade. Esse problema ocorre apenas na formatação do arquivo de diagnóstico e não no comando para o Exchange. O hífen ausente impede que um usuário corte o comando e cole-o diretamente em um prompt do PowerShell para teste ou validação. Os hifens foram adicionados. [CXM-52520]
- Se a identidade de uma caixa de correio estiver no formato “sobrenome, nome”, o Exchange adicionará uma barra invertida antes da vírgula ao retornar dados de uma consulta. Essa barra invertida deve ser removida quando o XenMobile Mail Manager usa a identidade para consultar mais dados. [CXM-52635]

Limitação conhecida

Nota:

A limitação a seguir está resolvida na versão 10.1.6.

O XenMobile Mail Manager possui uma limitação conhecida que pode fazer com que os comandos do Exchange falhem. Para aplicar alterações de política ao Exchange, um comando **Set_CASMailbox** é emitido pelo XenMobile Mail Manager. Esse comando pode ter duas listas de dispositivos: uma para Permitir e outra para Bloquear. O comando é aplicado aos dispositivos associados a uma caixa de correio.

Essas listas são limitadas a 256 caracteres cada pela API da Microsoft. Se uma dessas listas exceder a limitação, o comando falhará na sua totalidade, impedindo que as políticas de caixa de correio desses dispositivos sejam configuradas. O erro relatado, que aparecerá nos logs do XenMobile Mail Manager, será semelhante ao seguinte. Este exemplo é de uma lista bloqueada.

“Message:’Não é possível vincular o parâmetro ‘ActiveSyncBlockedDeviceIDs’ ao destino. Exception setting ‘ActiveSyncBlockedDeviceIDs’: ‘O comprimento da propriedade é muito longo. O comprimento máximo é 256 e o comprimento do valor fornecido é...’”

Os tamanhos de ID dos dispositivos podem variar, mas, via de regra, cerca de 10 dispositivos ou mais simultaneamente Permitidos ou Bloqueados poderão exceder o limite. Embora ter muitos dispositivos associados a uma caixa de correio específica seja raro, essa é uma possibilidade. Até que o Xen-

Mobile Mail Manager seja aprimorado para lidar com esse cenário, recomendamos limitar o número de dispositivos associados a um usuário e a uma caixa de correio a 10 ou menos. [CXM-52633]

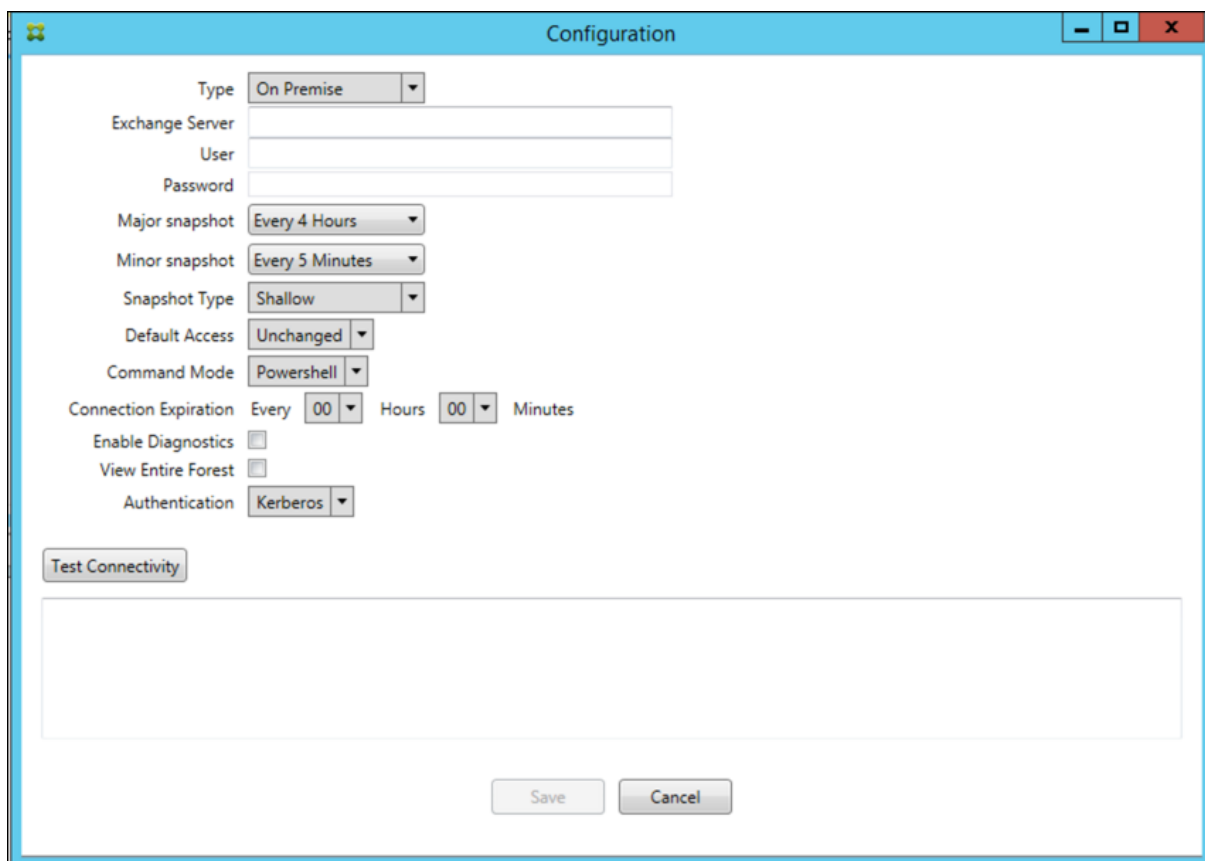
O que há de novo na versão 10.1.4

O XenMobile Mail Manager versão 10.1.4 apresenta os seguintes problemas corrigidos:

- Devido ao enfraquecimento da segurança, o TLS 1.0 está sendo suspenso pelo PCI Council. O suporte para o TLS 1.1 e 1.2 é adicionado ao XenMobile Mail Manager. [CXM-38573, CXM-32560]
- O XenMobile Mail Manager inclui um novo arquivo de diagnóstico. Quando a opção **Ativar diagnóstico** está selecionada na especificação do Exchange, um novo arquivo de Histórico de Captura Instantânea é gerado. Com cada tentativa de instantâneo, uma linha é adicionada ao arquivo com os resultados do instantâneo. [CXM-49631]
- No arquivo de diagnóstico Comandos, a lista de dispositivos permitidos ou bloqueados não foi exibida para o comando **Set-CASMailbox**. Em vez disso, o nome da classe interna foi mostrado no arquivo para os argumentos relacionados. O XenMobile Mail Manager agora mostra a lista de deviceIDs como uma lista delimitada por vírgulas. [CXM-50693]
- Quando uma tentativa de adquirir uma conexão com o Exchange falha devido a uma especificação incorreta: a mensagem de erro é substituída por uma mensagem incorreta: “Todas as conexões em uso”. Mais mensagens descritivas aparecem agora, como “Todas as conexões estão inoperantes”, “O pool de conexões está vazio”, “Todas as conexões são limitadas” e “Nenhuma conexão disponível”. [CXM-50783]
- Em alguns casos, os comandos Permitir/Bloquear/Apagar são enfileirados várias vezes no cache interno do XenMobile Mail Manager. Esse problema causa um atraso no comando que está sendo enviado para o Exchange. O XenMobile Mail Manager agora só enfileira uma instância de cada comando. [CXM-51524]

O que há de novo na versão 10.1.3

- **Suporte ao Google Analytics:** queremos saber como você usa o XenMobile Mail Manager para nos concentrarmos em como podemos melhorar o produto.
- **Configuração para ativar o diagnóstico:** uma caixa de seleção **Ativar diagnóstico** é exibida no console Configurar na caixa de diálogo **Configuração**.



Problemas resolvidos na versão 10.1.3

- Na janela **Histórico da Captura Instantânea**, as dicas de ferramentas que mostram o estado atual da captura instantânea não refletem o estado real. [CXM-5570]
Ocasionalmente, o XenMobile Mail Manager não pode gravar no arquivo de diagnósticos de Comandos. Quando isso ocorre, o histórico de comandos não é registrado em sua totalidade. [CXM-49217]
- Quando ocorre um erro com uma conexão, a conexão não é marcada como “com erro”. Como resultado, um comando subsequente pode tentar usar a conexão e causar outro erro. [CXM-49495]
- Quando a limitação do Exchange Server ocorre, uma exceção pode ser lançada na rotina de Verificação de Integridade. Como resultado, as conexões que sofreram um erro ou expiraram podem não ser limpas. Além disso, o XenMobile Mail Manager não cria conexões até que o tempo de limitação expire. [CXM-49794].
- Quando a contagem máxima de sessões do Exchange é excedida, o XenMobile Mail Manager relata o erro “Falha na Captura do Dispositivo”, que não é uma mensagem precisa. Em vez disso, a mensagem deve indicar que as duas sessões que o XenMobile Mail Manager normalmente usa para a comunicação do Exchange estão em uso. [CXM-49994]

O que há de novo na versão 10.1.2

- **Melhor conexão com o Exchange:** o XenMobile Mail Manager usa as sessões do PowerShell para se comunicar com o Exchange. Uma sessão do PowerShell, especialmente ao lidar com o Office 365, pode se tornar instável depois de algum tempo, impedindo o êxito dos comandos subsequentes. O XenMobile Mail Manager agora pode definir um período de expiração para conexões. Quando a conexão atinge seu tempo de expiração, o XenMobile Mail Manager encerra a sessão do PowerShell e cria uma sessão. Ao fazer isso, é menos provável que a sessão do PowerShell se torne instável, reduzindo significativamente a chance de uma falha de instantâneo.
- **Fluxo de trabalho de instantâneo aprimorado:** os principais instantâneos são uma operação demorada e de processo intenso. Se ocorrer um erro durante um instantâneo, agora o XenMobile Mail Manager tentará várias vezes (até três) concluir um instantâneo. Tentativas subsequentes não começam do início. O XenMobile Mail Manager continua de onde parou. Esse aprimoramento melhora a taxa de sucesso de instantâneos em geral, permitindo que erros transitórios passem enquanto um instantâneo ainda está em andamento.
- **Diagnóstico aprimorado:** a solução de problemas de operações de instantâneos agora ficou mais fácil, com três novos arquivos de diagnóstico gerados opcionalmente durante um instantâneo. Esses arquivos ajudam a identificar problemas de comando do PowerShell, caixas de correio com informações ausentes e dispositivos que não podem ser relacionados a uma caixa de correio. Um administrador pode usar esses arquivos para identificar dados que podem não estar corretos no Exchange.
- **Melhor uso de memória:** agora, o XenMobile Mail Manager é mais eficiente no uso de memória. Os administradores podem agendar o XenMobile Mail Manager para reiniciar automaticamente para fornecer uma barreira limpa ao sistema.
- **Pré-requisito do Microsoft .NET Framework 4.6:** o pré-requisito para o Microsoft .NET Framework agora é a versão 4.6.

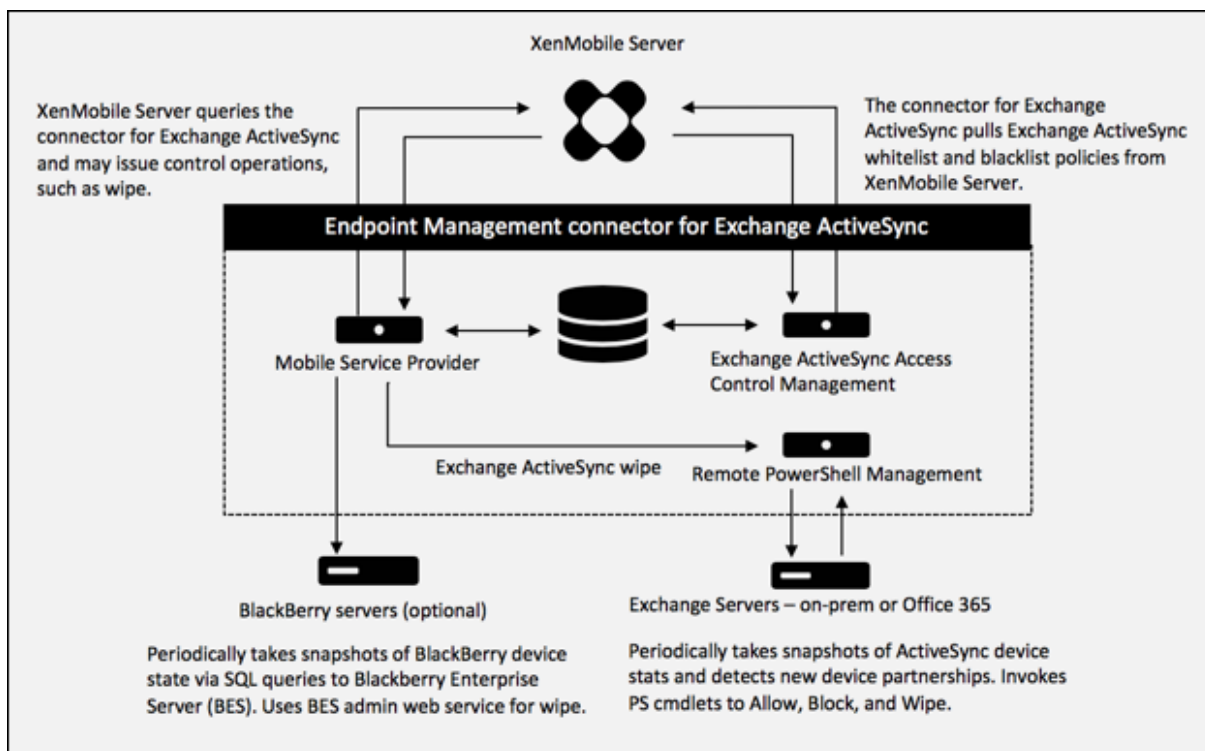
Problemas resolvidos

- Aviso de erro de credenciais: a instabilidade da sessão do Office 365 muitas vezes causou esse erro. O melhoria Conexão Aprimorado ao Exchange resolve esse problema. (XMHELP-293, XMHELP-311, XMHELP-801)
- Imprecisões na contagem de caixas de correio e dispositivos: o XenMobile Mail Manager possui um algoritmo aprimorado de associação de Caixa de Correio com Dispositivo. O recurso Diagnóstico Aprimorado ajuda na identificação de caixas de correio e dispositivos que o XenMobile Mail Manager considera que não estão dentro de seu domínio de responsabilidade. (XMHELP-623)
- Comandos Permitir/Bloquear/Apagar não são reconhecidos: um bug foi corrigido onde, às vezes, os comandos de permissão/bloqueio/apagamento do XenMobile Mail Manager não são reconhecidos. (XMHELP-489)

- Gerenciamento de memória: melhor gerenciamento de memória e mitigação. (XMHELP-419)

Arquitetura

A figura a seguir mostra os principais componentes do conector do Endpoint Management para Exchange ActiveSync. Para um diagrama da arquitetura de referência detalhada, consulte [Arquitetura](#).



Os três componentes principais são:

- **Exchange ActiveSync Access Control Management:** comunica-se com o XenMobile para recuperar uma política do Exchange ActiveSync do XenMobile e mesclá-la com qualquer política definida localmente para determinar os dispositivos do Exchange ActiveSync que devem ter o acesso ao Exchange permitido ou negado. A política local permite a extensão das regras da política para possibilitar o controle de acesso pelo Grupo do Active Directory, Usuário, Tipo de Dispositivo ou Agente de Usuário do Dispositivo (geralmente o número de versão de plataforma).
- **Remote PowerShell Management:** responsável pelo cronograma e invocação de comandos PowerShell remotos para impor a política compilada pelo Exchange ActiveSync Access Control Management. Tira periodicamente um instantâneo do banco de dados do Exchange ActiveSync para detectar dispositivos do Exchange ActiveSync novos ou alterados.
- **Mobile Service Provider:** fornece uma interface de serviços da Web para que o XenMobile possa consultar o Exchange ActiveSync, consultar dispositivos Blackberry e emitir operações de controle, como o Wipe nos dispositivos Blackberry e no ActiveSync.

Requisitos do sistema e pré-requisito

Os seguintes requisitos mínimos do sistema são necessários para usar o conector de Endpoint Management para Exchange ActiveSync:

- Windows Server 2016, Windows Server 2012 R2 ou Windows Server 2008 R2 Service Pack 1. Deve ser um servidor com base no inglês. O suporte para Windows Server 2008 R2 Service Pack 1 termina em 14 de janeiro de 2020.
- Microsoft SQL Server 2016 Service Pack 2 ou SQL Server 2014 Service Pack 3.
- Microsoft .NET Framework 4.6.
- BlackBerry Enterprise Service versão 5 (opcional)

Versões mínimas compatíveis do Microsoft Exchange Server:

- Microsoft Office 365
- Exchange Server 2016
- Exchange Server 2013
- Exchange Server 2010 Service Pack 3 (o suporte termina em 14 de janeiro de 2020)

Pré-requisitos

- O Windows Management Framework deve estar instalado.
 - PowerShell V5, V4 e V3
- A política de execução do PowerShell deve ser definida como RemoteSigned via Set-ExecutionPolicy RemoteSigned.
- A porta TCP 80 deve estar aberta entre o computador que está executando o conector de Endpoint Management para Exchange ActiveSync e o Exchange Server remoto.
- **Clientes de email de dispositivos:** nem todos os clientes de email sempre retornam o mesmo ActiveSync ID para um dispositivo. Como o conector de Endpoint Management para Exchange ActiveSync espera uma ID exclusiva do ActiveSync para cada dispositivo, apenas os clientes de email que consistentemente geram a mesma ID exclusiva do ActiveSync para cada dispositivo são suportados. Esses clientes de email foram testados pela Citrix e executados sem erros:
 - Cliente de email nativo Samsung
 - Cliente de email nativo iOS
- **Exchange:** os requisitos para o computador local executando o Exchange são os seguintes:

As credenciais especificadas na interface do usuário da Configuração do Exchange devem conseguir realizar a conexão com o Exchange Server e ter acesso total para executar os seguintes cmdlets do PowerShell específicos do Exchange.

- **Para o Exchange Server 2010 SP2:**

- * Get-CASMailbox
 - * Set-CASMailbox
 - * Get-Mailbox
 - * Get-ActiveSyncDevice
 - * Get-ActiveSyncDeviceStatistics
 - * Limpar ActiveSyncDevice
 - * Get-ExchangeServer
 - * Get-ManagementRole
 - * Get-ManagementRoleAssignment
- **Para o Exchange Server 2013 e Exchange Server 2016:**
- * Get-CASMailbox
 - * Set-CASMailbox
 - * Get-Mailbox
 - * Get-MobileDevice
 - * Get-MobileDeviceStatistics
 - * Clear-MobileDevice
 - * Get-ExchangeServer
 - * Get-ManagementRole
 - * Get-ManagementRoleAssignment
- Se o conector de Endpoint Management para Exchange ActiveSync estiver configurado para exibir a floresta inteira, a permissão deve ter sido concedida para execução de: **Set-AdServerSettings -ViewEntireForest \$true**
- As credenciais fornecidas devem ter o direito de conexão com o Exchange Server por meio do Shell remoto. Por padrão, o usuário que instalou o Exchange tem esse direito.
- Para estabelecer uma conexão remota e executar comandos remotos, as credenciais devem corresponder a um usuário que seja um administrador no computador remoto. Você pode usar Set-PSSessionConfiguration para eliminar o requisito administrativo, mas a discussão desse comando está além do escopo deste documento. Para obter mais informações, consulte o artigo da Microsoft [About Session Configurations](#).
- O Exchange Server deve ser configurado para oferecer suporte a solicitações remotas do PowerShell por meio de HTTP. Normalmente, um administrador que executa o seguinte comando do PowerShell no Exchange Server é só o que é necessário: WinRM QuickConfig.
- O Exchange apresenta muitas políticas de limitação. Uma das políticas controla quantas conexões simultâneas do PowerShell são permitidas por usuário. O número padrão de conexões simultâneas permitidas para um usuário é 18 no Exchange 2010. Quando o limite de conexão é atingido, o conector de Endpoint Management para Exchange ActiveSync não consegue se conectar ao Exchange Server. Existem maneiras de alterar o número máximo permitido de conexões simultâneas por meio do PowerShell que estão além do escopo desta documentação. Se você tiver interesse, investigue as políticas de limitação do

Exchange relacionadas ao gerenciamento remoto com o PowerShell.

Requisitos do Office 365 Exchange

- **Permissões:** as credenciais especificadas na interface do usuário da Configuração do Exchange devem conseguir realizar a conexão com o Office 365 e ter acesso total para executar os seguintes cmdlets do PowerShell específicos do Exchange:
 - Get-CASMailbox
 - Set-CASMailbox
 - Get-Mailbox
 - Get-MobileDevice
 - Get-MobileDeviceStatistics
 - Clear-MobileDevice
 - Get-ExchangeServer
 - Get-ManagementRole
 - Get-ManagementRoleAssignment
- **Privilégios:** as credenciais fornecidas devem ter o direito de conexão com o servidor do Office 365 por meio do Shell remoto. Por padrão, o administrador online do Office 365 tem os privilégios necessários.
- **Throttling policies:** Exchange has many throttling policies. Uma das políticas controla quantas conexões simultâneas do PowerShell são permitidas por usuário. O número padrão de conexões simultâneas permitidas para um usuário é três no Office 365. Quando o limite de conexão é atingido, o conector de Endpoint Management para Exchange ActiveSync não consegue se conectar ao Exchange Server. Existem maneiras de alterar o número máximo permitido de conexões simultâneas por meio do PowerShell que estão além do escopo desta documentação. Se você tiver interesse, investigue as políticas de limitação do Exchange relacionadas ao gerenciamento remoto com o PowerShell.

Instalar e configurar

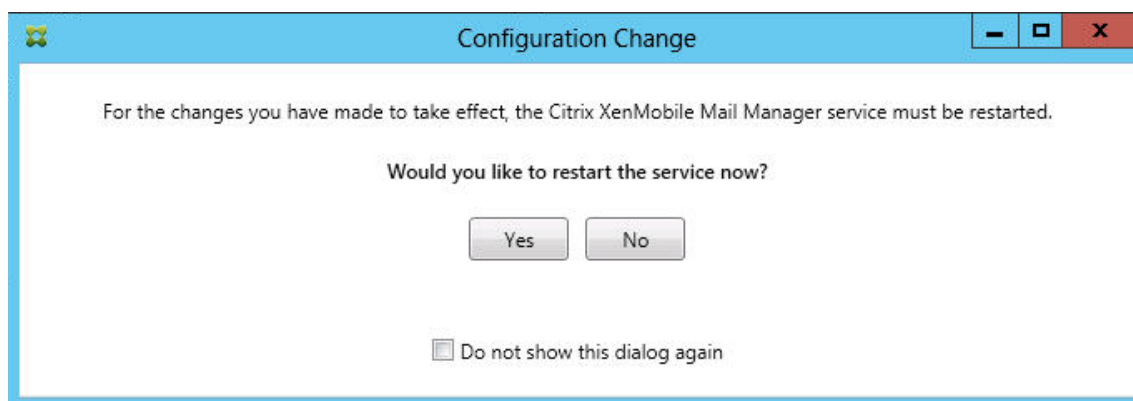
1. Clique no arquivo XmmSetup.msi e siga os prompts no instalador para instalar o conector de Endpoint Management para Exchange ActiveSync.
2. Deixe a opção **Launch the Configure utility** selecionada na última tela do assistente de configuração. Ou, no menu **Iniciar**, abra o conector de Endpoint Management para Exchange ActiveSync.
3. Configure as seguintes propriedades de banco de dados:
 - Selecione a guia **Configure > Database**.
 - Digite o nome do SQL Server (o padrão é localhost).
 - Mantenha o banco de dados como o padrão **CitrixXmm**.

4. Selecione um dos seguintes modos de autenticação usados para SQL:

- **SQL:** digite o nome do usuário e a senha de um usuário válido do SQL.
- **Windows Integrated:** se você selecionar essa opção, as credenciais de login do serviço conector de Endpoint Management para Exchange ActiveSync deverão ser alteradas para uma conta do Windows que tenha permissões para acessar o SQL Server. Para fazer isso, abra o **Painel de Controle > Ferramentas Administrativas > Serviços**, clique com o botão direito do mouse no serviço conector de Endpoint Management para Exchange ActiveSync e clique na guia **Logon**.

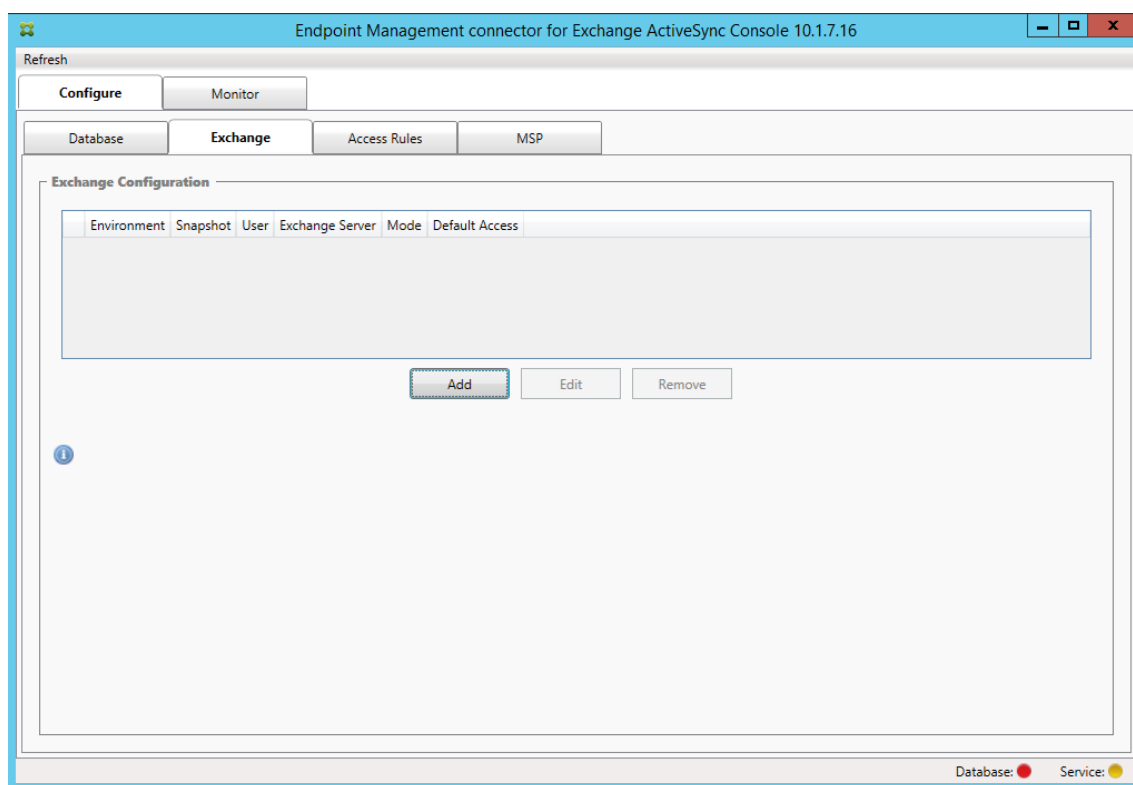
Se a opção Windows Integrated também for escolhida para a conexão de banco de dados do BlackBerry, a conta do Windows especificada aqui também deverá ter acesso ao banco de dados do BlackBerry.

5. Clique em **Test Connectivity** para verificar se uma conexão com o SQL Server pode ser realizada e clique em **Save**.
6. Uma mensagem solicita que você reinicie o serviço. Clique em **Yes**.



7. Configure um ou mais Exchange Servers:

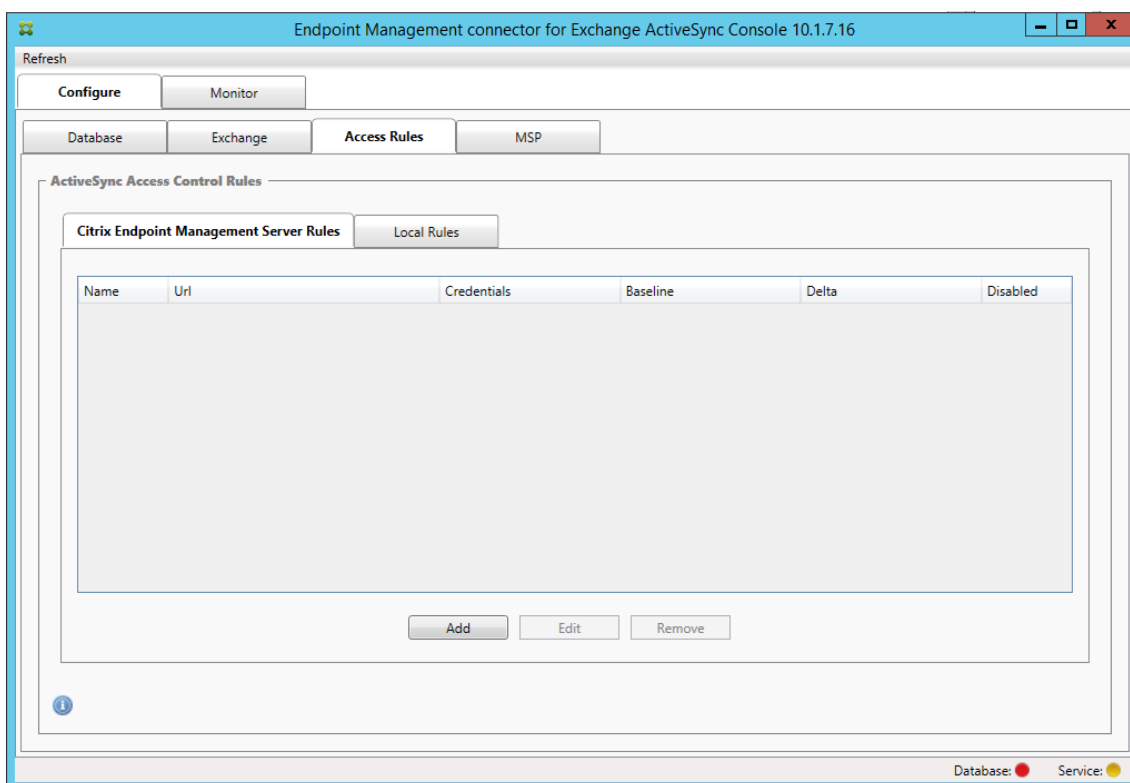
- Se estiver gerenciando um único ambiente do Exchange, especifique apenas um único servidor. Se estiver gerenciando vários ambientes do Exchange, especifique um único Exchange Server para cada ambiente do Exchange.
- Clique na guia **Configure > Exchange** e, em seguida, clique em **Add**.



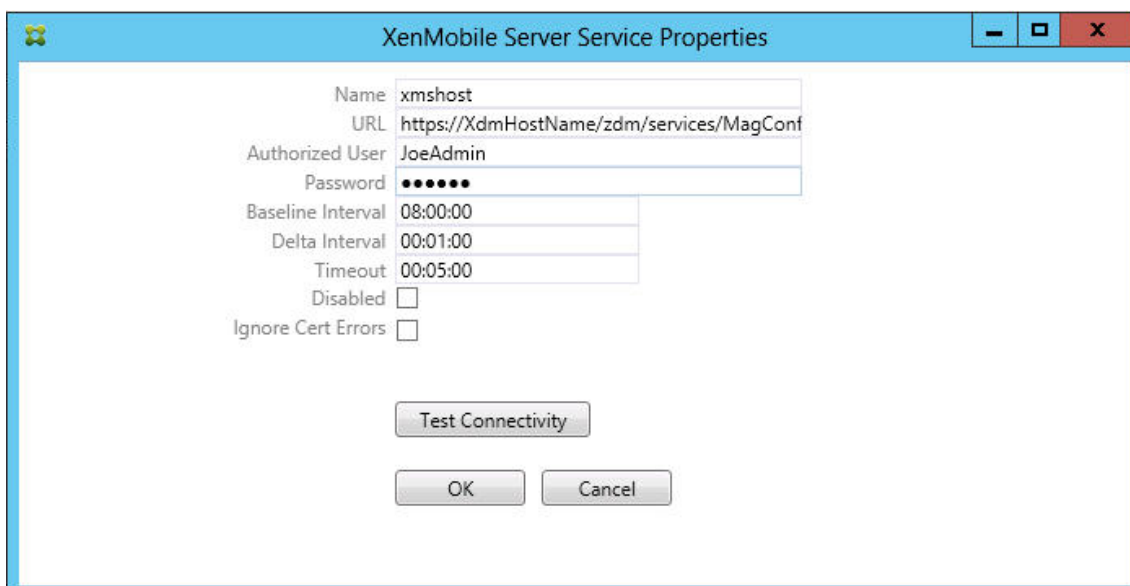
8. Selecione o tipo de ambiente do Exchange Server: **On Premise** ou **Office 365**.

- Se você selecionar **On Premise**, digite o nome do Exchange Server que será usado para os comandos do Remote PowerShell.
- Digite o **nome do usuário** de uma identidade do Windows que tenha os direitos adequados no Exchange Server, conforme especificado na seção Requisitos, e insira a **senha** do usuário.
- Selecione o cronograma da execução de instantâneos principais. Um instantâneo principal detecta cada parceria do Exchange ActiveSync.
- Selecione o cronograma da execução de instantâneos secundários. Um instantâneo secundário detecta parcerias do Exchange ActiveSync recém-criadas.
- Selecione o Snapshot Type: **Deep** ou **Shallow**. Os instantâneos superficiais (Snapshot Shallow) são tipicamente muito mais rápidos e são suficientes para executar todas as funções de Controle de Acesso do Exchange ActiveSync do conector de Endpoint Management para Exchange ActiveSync. Os instantâneos profundos (Snapshot Deep) podem demorar mais tempo e serão necessários somente se o Provedor de Serviços Móveis estiver ativado para o ActiveSync. Essa opção permite que o XenMobile consulte dispositivos não gerenciados.
- Selecione o Default Access: **Allow**, **Block** ou **Unchanged**. Essa configuração controla como todos os dispositivos diferentes dos identificados por regras explícitas do XenMobile ou Locais são tratados. Se você selecionar **Allow**, o acesso do ActiveSync a todos esses dispositivos será permitido. Se você selecionar **Block**, o acesso será negado. Se

- você selecionar **Unchanged**, nenhuma alteração será feita.
- Selecione o ActiveSync Command Mode: **PowerShell** ou **Simulation**.
 - No modo **PowerShell**, o conector de Endpoint Management para Exchange ActiveSync emite comandos do PowerShell para efetuar o controle de acesso desejado. No modo **Simulation**, o conector de Endpoint Management para Exchange ActiveSync não emite comandos do PowerShell, mas registra o comando e os resultados pretendidos no banco de dados. No modo **Simulation**, o usuário pode usar a guia **Monitor** para ver o que teria acontecido se o modo **PowerShell** estivesse ativado.
 - Em **Connection Expiration**, defina as horas e minutos para a duração de uma conexão. Quando uma conexão atinge a duração especificada, a conexão é marcada como expirada, de modo que a conexão nunca seja usada novamente. Quando a conexão expirada não é mais usada, o conector de Endpoint Management para Exchange ActiveSync encerra a conexão normalmente. Quando uma conexão é necessária novamente, uma nova conexão é inicializada se nenhuma estiver disponível. Se nenhuma for especificada, o padrão de 30 minutos será usado.
 - Selecione **View Entire Forest** para configurar o conector de Endpoint Management para Exchange ActiveSync para exibir toda a floresta do Active Directory no ambiente do Exchange.
 - Selecione o protocolo de autenticação: **Kerberos** ou **Basic**. O conector de Endpoint Management para Exchange ActiveSync oferece suporte à autenticação **Basic** para implantações locais. Isso permite que o conector de Endpoint Management para Exchange ActiveSync seja usado quando o conector de servidor Endpoint Management para Exchange ActiveSync não é membro do domínio no qual o Exchange Server reside.
 - Clique em **Test Connectivity** para verificar se uma conexão com o Exchange Server pode ser realizada e clique em **Save**.
 - Uma mensagem solicita que você reinicie o serviço. Clique em **Yes**.
9. Configure as regras de acesso: selecione a guia **Configure > Access Rules**, clique na guia **XMS Rules** e, em seguida, clique em **Add**.



- Na página de **Propriedades do servidor XenMobile Service**, modifique a sequência de URL para apontar para o XenMobile Server. Por exemplo, se o nome da instância for **zdm**, insira <https://<XdmHostName>/zdm/services/MagConfigService>. No exemplo, substitua **XdmHostName** pelo endereço IP ou DNS do XenMobile Server.

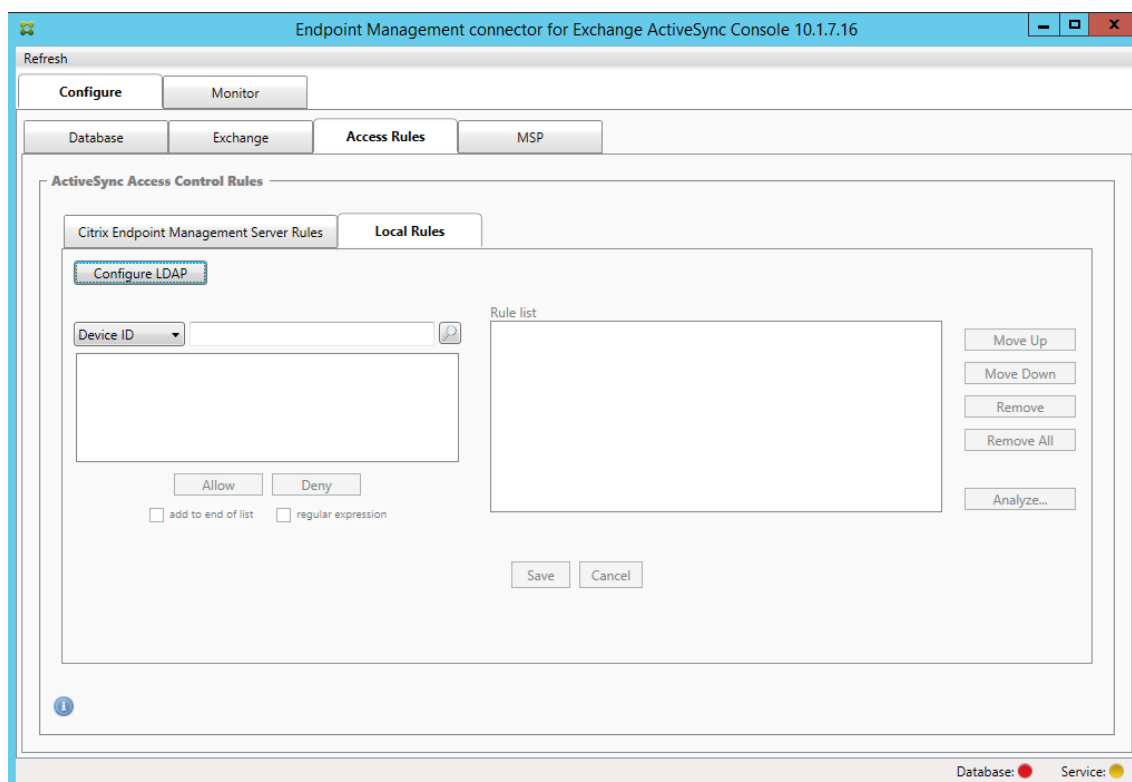


- Insira um usuário autorizado do servidor.
- Insira a senha de usuário.
- Mantenha os valores padrão de **Baseline Interval**, **Delta Interval** e **Timeout**.

- Clique em **Test Connectivity** para verificar a conexão com o servidor e depois clique em **OK**.

Se a caixa de seleção **Disabled** estiver marcada, o XenMobile Mail Service não coletará políticas do XenMobile.

11. Clique na guia **Local Rules**.



- Você pode adicionar regras locais com base em ActiveSync Device ID, Device Type, AD Group, User ou UserAgent de dispositivo. Na lista, selecione o tipo adequado.
- Insira texto ou fragmentos de texto na caixa de texto. Opcionalmente, clique no botão de consulta para exibir as entidades que correspondem ao fragmento.

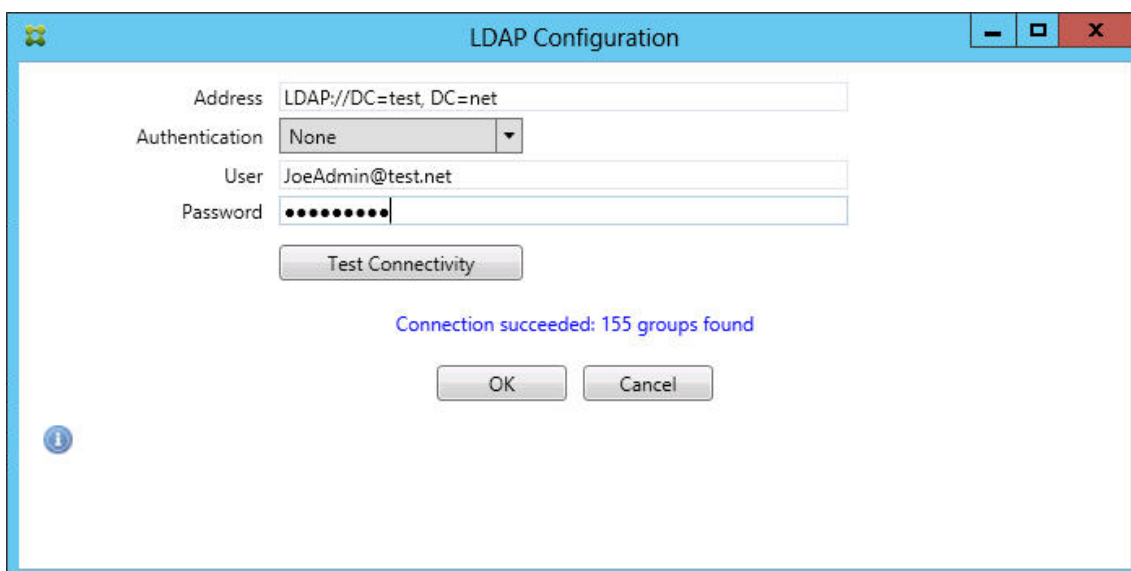
Para todos os tipos diferentes de Group, o sistema se baseia nos dispositivos que foram encontrados em um instantâneo. Portanto, se você estiver apenas começando e ainda não tiver concluído um instantâneo, nenhuma entidade estará disponível.

- Selecione um valor de texto e clique em **Allow** ou **Deny** para adicioná-lo ao painel **Rule List** à direita. Você pode alterar a ordem das regras ou removê-las usando os botões à direita do painel **Rule List**. A ordem é importante pois, para um determinado usuário e dispositivo, as regras são avaliadas na ordem mostrada e uma correspondência em uma regra superior (mais perto do topo) faz com que as regras subsequentes não tenham nenhum efeito. Por exemplo, se houver uma regra que permite todos os dispositivos iPad e uma regra subsequente que bloqueia o usuário Matt, o iPad de Matt ainda será permitido,

pois a regra iPad tem uma prioridade efetiva mais alta do que a regra Matt.

- Para executar uma análise das regras na lista de regras para localizar possíveis substituições, conflitos ou construções complementares, clique em **Analyze** e depois clique em **Save**.

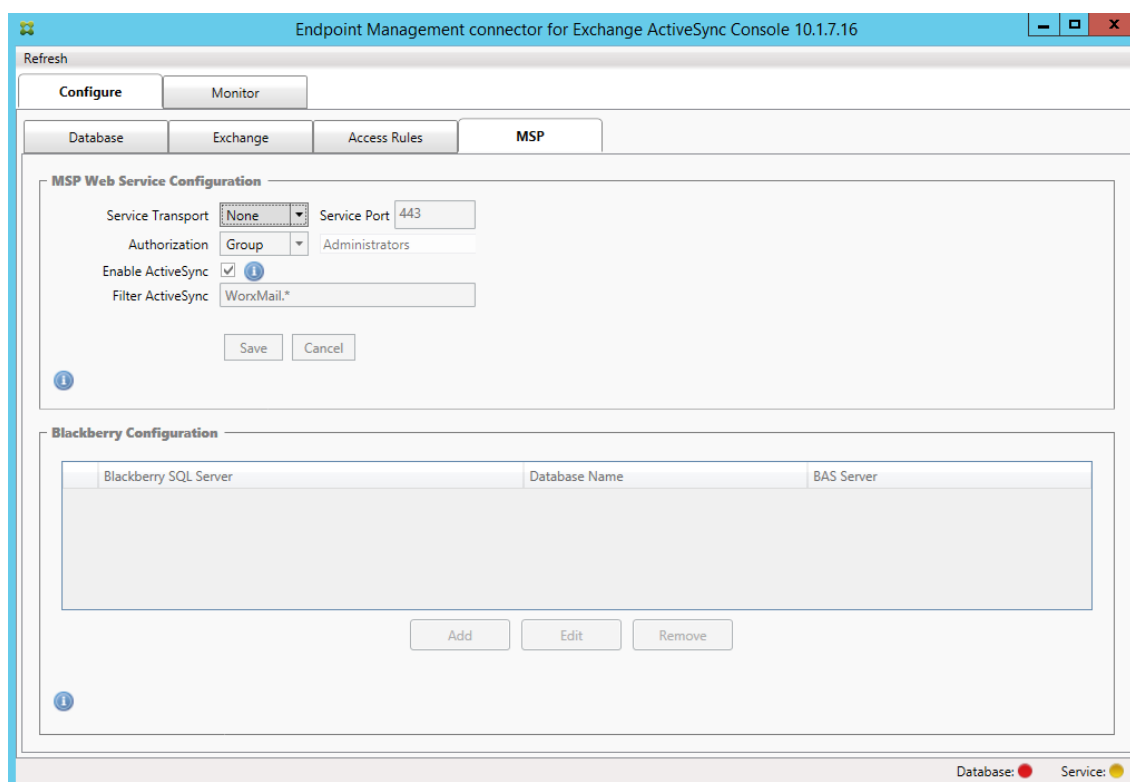
12. Se você deseja criar regras locais que operam em Grupos do Active Directory, clique em **Configure LDAP** e, em seguida, configure as propriedades de conexão LDAP.



13. Configure o Provedor de Serviços Móveis.

O provedor de serviços móveis é opcional. Essa configuração é necessária apenas se o XenMobile também estiver configurado para usar a interface do Provedor de serviços móveis para consultar dispositivos não gerenciados.

- Clique na guia **Configure > MSP**.



- Defina o tipo de Service Transport, como **HTTP** ou **HTTPS**, do serviço do Provedor de Serviços Móveis.
- Defina a **Service Port** (normalmente 80 ou 443) do serviço do Provedor de Serviços Móveis. Se você usar a porta 443, ela exigirá um certificado SSL associado a ela no IIS.
- Defina o **Authorization Group** ou **User**. Isso define o usuário ou o conjunto de usuários que poderá se conectar ao serviço do Provedor de Serviços Móveis do XenMobile.
- Defina se as consultas do ActiveSync estão ativadas ou não. Se as consultas do ActiveSync estiverem ativadas para o XenMobile Server, o tipo de instantâneo para um ou mais Exchange Servers deverá ser definido como **Deep**. Essa configuração pode ter custos de desempenho significativos para tirar instantâneos.
- Por padrão, os dispositivos ActiveSync que correspondam à expressão regular WorxMail.* não serão enviados para o XenMobile. Para alterar esse comportamento, altere o campo **Filter ActiveSync** conforme necessário.
Em branco significa que todos os dispositivos são encaminhados ao XenMobile.
- Clique em **Salvar**.

14. Opcionalmente, configure uma ou mais instâncias do BlackBerry Enterprise Server (BES): clique em **Add** e digite o nome do servidor do BES SQL Server.

- Insira o nome do banco de dados de gerenciamento do BES.
- Selecione o modo **Authentication**. Se você selecionar a autenticação Integrated do Windows, a conta de usuário do serviço conector de Endpoint Management para Exchange ActiveSync é a conta usada para conectar-se ao SQL Server do BES. Se você também escolher a conexão Integrated do Windows para a conexão do banco de dados do conector de Endpoint Management para Exchange ActiveSync, a conta do Windows especificada aqui também deverá receber acesso ao banco de dados do conector de Endpoint Management para Exchange ActiveSync.
- Se você selecionar **SQL authentication**, digite o nome do usuário e a senha.
- Defina o **Sync Schedule**. Esse é o calendário usado para conexão com o SQL Server do BES e verifica se há alguma atualização de dispositivo.
- Clique em **Test Connectivity** para verificar a conectividade com o SQL Server. Se você selecionar Windows Integrated, esse teste usará o usuário atualmente conectado e não o serviço conector do Endpoint Management para Exchange ActiveSync e, portanto, não testará com precisão a autenticação do SQL.
- Para dar suporte a Wipe ou ResetPassword de dispositivos BlackBerry a partir do XenMo-

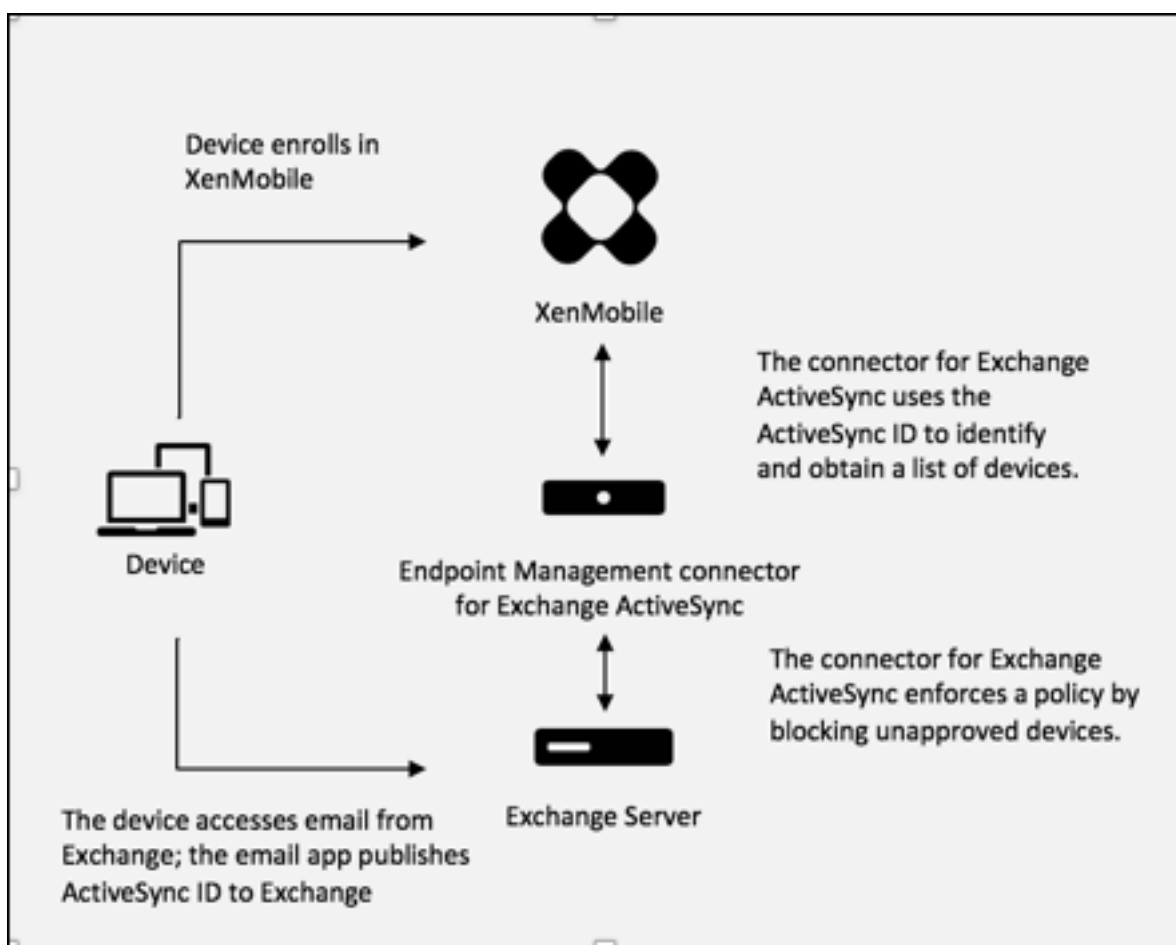
bile, marque a caixa de seleção **Enabled**.

- Insira o nome de domínio totalmente qualificado (FQDN) do BES.
- Insira a porta do BES usada para o serviço da Web de administração.
- Insira o usuário totalmente qualificado e a senha exigidos pelo serviço do BES.
- Clique em **Test Connectivity** para testar a conexão com o BES.
- Clique em **Salvar**.

Impor políticas de email com IDs do ActiveSync

Sua política de email corporativo pode ditar que determinados dispositivos não sejam aprovados para o uso de email corporativo. Para cumprir essa política, você deseja garantir que os funcionários não consigam acessar o email corporativo desses dispositivos. O conector de Endpoint Management para Exchange ActiveSync e o XenMobile trabalham em conjunto para impor essa política de email. O XenMobile define a política de acesso a email corporativo e, quando um dispositivo não aprovado se registra no XenMobile, o conector de Endpoint Management para Exchange ActiveSync impõe a política.

O cliente de email em um dispositivo se apresenta para o Exchange Server (ou o Office 365) usando o ID de dispositivo, também conhecido como o ActiveSync ID, que é usado para identificar o dispositivo. O Secure Hub obtém um identificador semelhante e o envia para o XenMobile quando o dispositivo se registra. Ao comparar os dois IDs de dispositivo, o conector de Endpoint Management para Exchange ActiveSync pode determinar se um dispositivo específico deve ter acesso a email corporativo. A figura a seguir ilustra esse conceito:



Se o XenMobile enviar ao conector de Endpoint Management para Exchange ActiveSync um ID do ActiveSync diferente do ID que o dispositivo publica no Exchange, o conector de Endpoint Management para Exchange ActiveSync não poderá indicar ao Exchange o que fazer com o dispositivo.

A correspondência de IDs do ActiveSync funciona de forma confiável na maioria das plataformas. No entanto, a Citrix descobriu que, em algumas implementações do Android, o ID do ActiveSync do dispositivo é diferente do ID que o cliente de email apresenta ao Exchange. Para atenuar esse problema, você pode fazer o seguinte:

- Na plataforma Samsung SAFE, envie por push a configuração do ActiveSync do dispositivo do XenMobile.

Para garantir que a sua política de acesso ao email corporativo seja aplicada corretamente, você poderá adotar uma postura de segurança defensiva e configurar o conector de Endpoint Management para Exchange ActiveSync para bloquear emails definindo a política estática como Deny by default. Isso significa que se um funcionário configura um cliente de email em um dispositivo Android, e se a detecção do ID do ActiveSync não funcionar corretamente, o funcionário terá o acesso ao email corporativo negado.

Regras de controle de acesso

O conector de Endpoint Management para Exchange ActiveSync fornece uma abordagem baseada em regras para configurar dinamicamente o controle de acesso a dispositivos Exchange ActiveSync. Um conector de Endpoint Management para Exchange ActiveSync consiste em duas partes: uma expressão correspondente e um estado de acesso desejado (Permitir ou Bloquear). Uma regra pode ser avaliada em relação um determinado dispositivo Exchange ActiveSync para determinar se ela é aplicável ou corresponde ao dispositivo. Existem vários tipos de expressões correspondentes; por exemplo, uma regra pode corresponder a todos os dispositivos de um determinado Tipo de Dispositivo ou a um ID de dispositivo Exchange ActiveSync específico, ou a todos os dispositivos de um usuário específico e assim por diante.

Em qualquer momento durante a adição, remoção e reorganização das regras na lista de regras, clicar no botão **Cancel** reverterá a lista de regras para o estado em que estava quando ela foi aberta pela primeira vez. A menos que você clique em **Save**, todas as alterações feitas nessa janela serão perdidas se você fechar a ferramenta Configure.

O conector do Endpoint Management for Exchange ActiveSync tem três tipos de regras: regras locais, regras do XenMobile Server (também conhecidas como regras XDM) e a regra de acesso padrão.

Regras locais: as regras locais têm a prioridade mais alta: se um dispositivo corresponde a uma regra local, a avaliação da regra é interrompida. Nem as regras do XenMobile Server nem a regra de acesso padrão serão consultadas. As regras locais são configuradas localmente para o conector de Endpoint Management para Exchange ActiveSync na guia **Configure > Access Rules > Local Rules**. A correspondência de suporte é baseada na associação de um usuário em um determinado grupo do Active Directory. A correspondência de suporte é baseada em expressões regulares para os seguintes campos:

- Active Sync Device ID
- Tipo de dispositivo ActiveSync
- Nome UPN
- ActiveSync User Agent (normalmente a plataforma do dispositivo ou o cliente de email)

Desde que um instantâneo principal tenha sido concluído e localizado dispositivos, você deverá conseguir adicionar uma regra normal ou de expressão regular. Se um instantâneo principal não tiver sido concluído, você poderá adicionar somente regras de expressão regular.

Regras do servidor XenMobile: as regras do XenMobile Server são referências a um XenMobile Server externo que fornece regras sobre dispositivos gerenciados. O XenMobile Server pode ser configurado com suas próprias regras de alto nível que identificam os dispositivos que devem ser permitidos ou bloqueados com base nas propriedades conhecidas do XenMobile, como se o dispositivo tem jail-break ou se o dispositivo contém aplicativos proibidos. O XenMobile avalia as regras de alto nível e produz um conjunto de IDs de dispositivos ActiveSync permitidos ou bloqueados, que são entregues ao conector de Endpoint Management para Exchange ActiveSync.

Regra de acesso padrão: a regra de acesso padrão é exclusiva, no sentido que ela potencialmente pode corresponder a cada dispositivo e sempre é avaliada por último. Essa regra é a regra genérica, o que significa que se um determinado dispositivo não corresponder a uma regra local ou do XenMobile Server, o estado de acesso desejado do dispositivo será determinado pelo estado de acesso desejado da regra de acesso padrão.

- **Default Access – Allow:** qualquer dispositivo que não for correspondido por uma regra local ou do XenMobile Server será permitido.
- **Default Access – Block:** qualquer dispositivo que não for correspondido por uma regra local ou do XenMobile Server será bloqueado.
- **Default Access - Unchanged:** qualquer dispositivo que não for correspondido por uma regra local ou do XenMobile Server não terá seu estado de acesso modificado de nenhuma forma pelo conector de Endpoint Management para Exchange ActiveSync. Se um dispositivo tiver sido colocado no modo Quarantine pelo Exchange, nenhuma ação será tomada; por exemplo, a única maneira de remover um dispositivo do modo Quarantine é ter uma regra Local ou o XDM explicitamente substituir a quarentena.

Sobre as avaliações de regra

Para cada dispositivo que o Exchange relata para o conector de Endpoint Management para Exchange ActiveSync, as regras são avaliadas em sequência, da prioridade mais alta para a mais baixa, desta forma:

- Regras locais
- Regras do XenMobile Server
- Regra de acesso padrão

Quando uma correspondência é encontrada, a avaliação é interrompida. Por exemplo, se uma regra local corresponder a um determinado dispositivo, ele não será avaliado em relação a qualquer das regras do XenMobile Server ou à regra de acesso padrão. Isso é verdadeiro também em um determinado tipo de regra. Por exemplo, se houver mais de uma única correspondência para um determinado dispositivo na lista de regras locais, assim que a primeira correspondência seja encontrada, a avaliação é interrompida.

O conector de Endpoint Management para Exchange ActiveSync reavalia o conjunto de regras atualmente definido quando as propriedades do dispositivo são alteradas ou quando os dispositivos são adicionados ou removidos ou quando as próprias regras são alteradas. Os instantâneos principais detectam as alterações na propriedade de dispositivo e as remoções em intervalos configuráveis. Os instantâneos secundários detectam novos dispositivos em intervalos configuráveis.

O Exchange ActiveSync também apresenta regras que regem o acesso. É importante entender como essas regras funcionam no contexto do conector de Endpoint Management para Exchange ActiveSync. O Exchange pode ser configurado com três níveis de regras: isenções pessoais, regras de dispositivo

e configurações de organização. O conector de Endpoint Management para Exchange ActiveSync automatiza o controle de acesso emitindo programaticamente as solicitações remotas do PowerShell para afetar as listas de isenções pessoais. Elas são listas de IDs de dispositivo Exchange ActiveSync permitidos ou bloqueados associados a uma determinada caixa de correio. Quando implantado, o conector de Endpoint Management para Exchange ActiveSync efetivamente assume o gerenciamento do recurso de listas de isenção no Exchange. Para obter detalhes, consulte o artigo da Microsoft [Controlando acesso a dispositivo](#).

Analisar é especialmente útil em situações nas quais várias regras foram definidas para o mesmo campo. Você pode solucionar problemas das relações entre as regras. Execute a análise da perspectiva dos campos de regra; por exemplo, as regras são analisadas em grupos com base no campo que está sendo correspondido, como ID de dispositivo ActiveSync, tipo de dispositivo ActiveSync, Usuário, Agente do Usuário e assim por diante.

Terminologia de regra

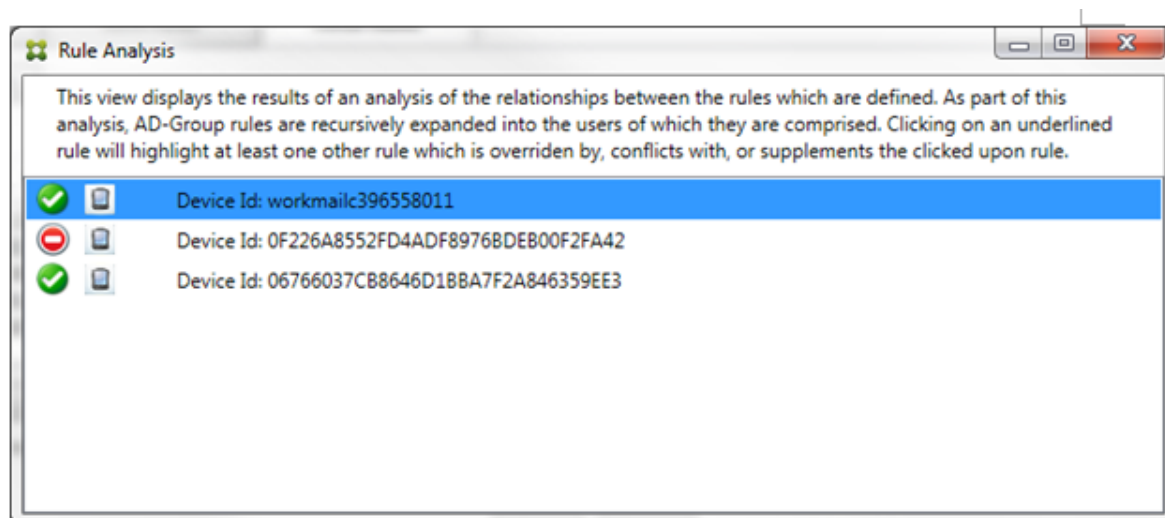
- **Regra predominante:** uma predominância ocorre quando mais de uma única regra poderia ser aplicada ao mesmo dispositivo. Como as regras são avaliadas por prioridade na lista, as instâncias de regra de menor prioridade que podem ser aplicadas podem nunca ser avaliadas.
- **Regra conflitante:** um conflito ocorre quando mais de uma única regra poderia ser aplicada ao mesmo dispositivo, mas o acesso (Permitir/Bloquear) não é correspondente. Se as regras conflitantes não forem regras de expressão regular, um conflito sempre conotará implicitamente uma substituição
- **Regra suplementar:** um suplemento ocorre quando mais de uma regra é uma regra de expressão regular e, portanto, pode haver a necessidade de garantir que as duas (ou mais) expressões regulares também possam ser combinadas em uma única regra de expressão regular ou que não estejam duplicando a funcionalidade. Uma regra suplementar também pode entrar em conflito no respectivo acesso (Permitir/Bloquear).
- **Regra principal:** a regra principal é a regra que foi clicada na caixa de diálogo. A regra é indicada visualmente por uma borda sólida que a contorna. A regra também terá uma ou duas setas verdes, apontando para cima ou para baixo. Se uma seta apontar para cima, ela indicará que existem regras auxiliares que precedem a regra principal. Se uma seta apontar para baixo, ela indicará que existem regras auxiliares que se seguem a regra principal. Somente uma única regra principal pode estar ativa em determinado momento.
- **Regra auxiliar:** uma regra auxiliar está relacionada de alguma forma à regra principal por meio de substituição, conflito ou uma relação suplementar. As regras são indicadas visualmente por uma borda tracejada que as contorna. Pode haver uma a muitas regras auxiliares para cada regra principal. Quando você clica em qualquer entrada sublinhada, a regra auxiliar ou as regras que são realçadas são sempre da perspectiva da regra principal. Por exemplo, a regra auxiliar é substituída pela regra principal e/ou a regra auxiliar entrará em conflito no respectivo acesso

com a regra principal, e/ou a regra auxiliar suplementará a regra principal.

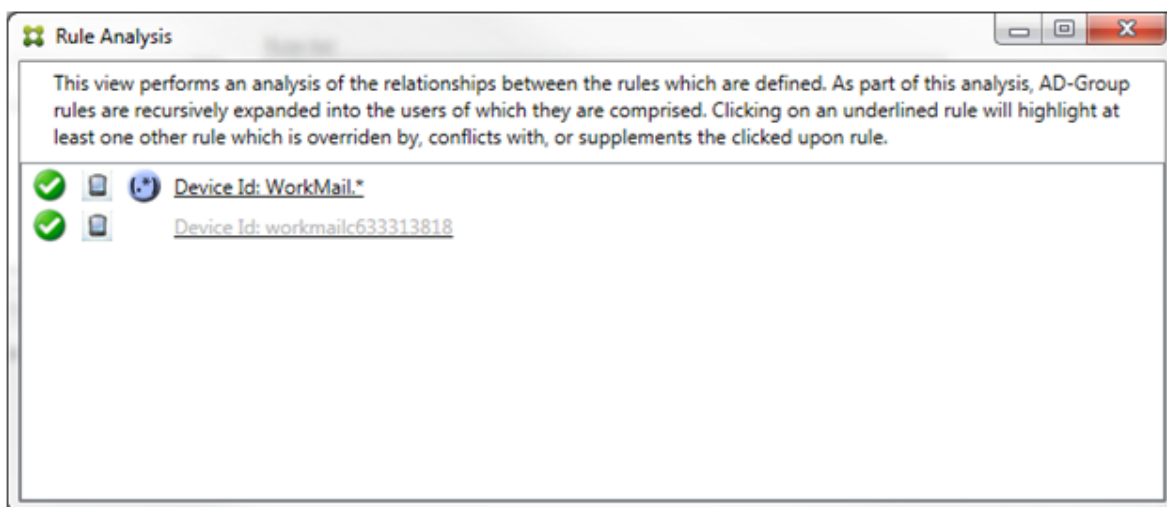
Como os tipos de regras aparecem na caixa de diálogo Rule Analysis

Quando não existirem conflitos, substituições ou suplementos, a caixa de diálogo Rule Analysis não apresentará entradas sublinhadas. Clicar em qualquer um dos itens não terá impacto; por exemplo, os visuais normais de item selecionado ocorrem.

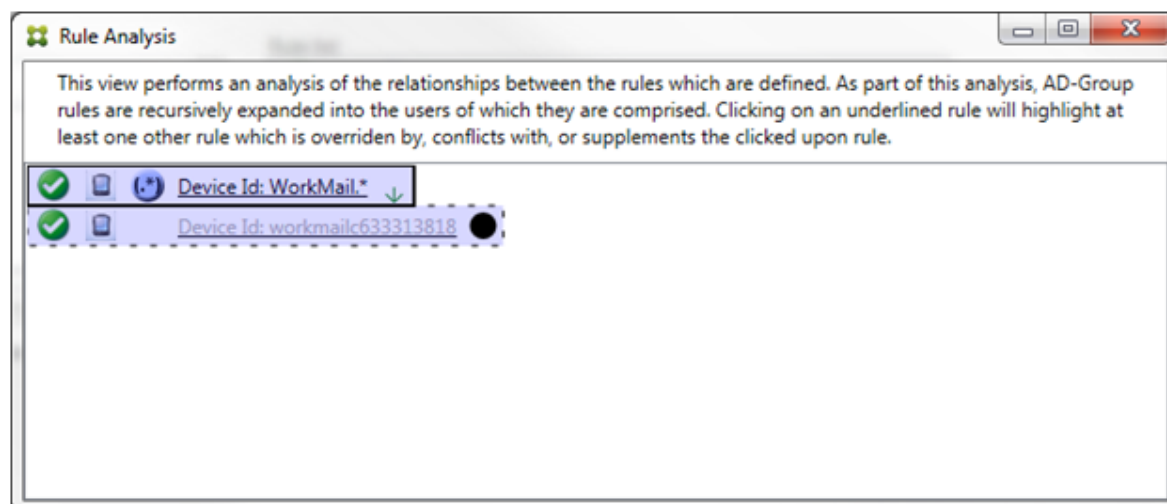
A janela Análise de regras tem uma caixa de seleção que, quando selecionada, exibe somente as regras que são conflitos, substituições, redundâncias ou suplementos.



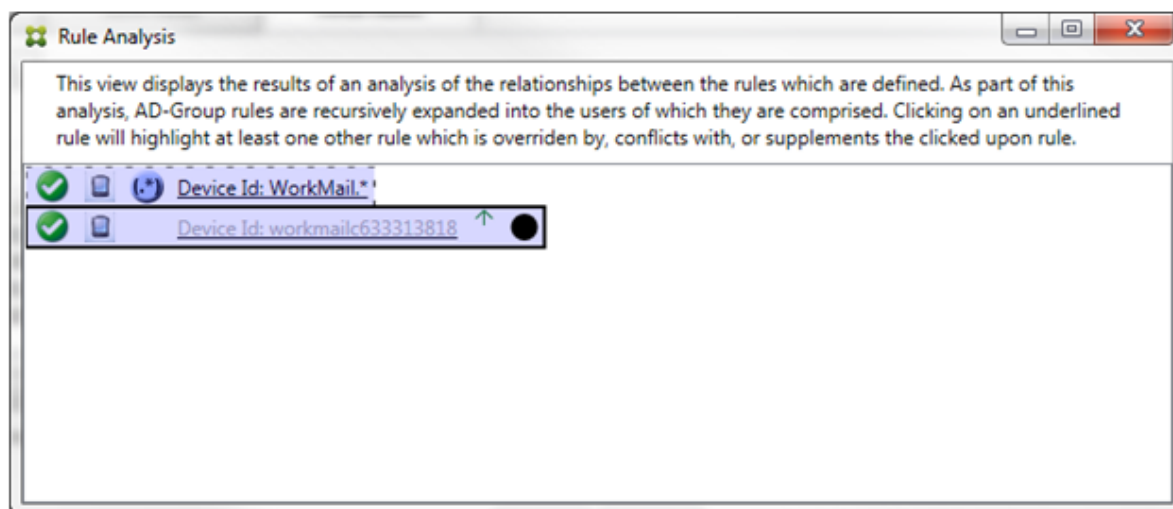
Quando ocorrer uma substituição, pelo menos duas regras serão sublinhadas: a regra principal e a regra ou as regras auxiliares. Pelo menos uma regra auxiliar é exibida em uma fonte mais fina para indicar que a regra foi substituída por uma regra de prioridade mais alta. Você pode clicar na regra predominante para descobrir qual regra ou regras a substituíram. Sempre que uma regra predominante for realçada como resultado de a regra ser a regra principal ou auxiliar, um círculo preto é exibido ao lado dela como uma indicação visual adicional de que a regra está inativa. Por exemplo, antes de clicar na regra, a caixa de diálogo é exibida da seguinte forma:



Quando você clica na regra de prioridade mais alta, a caixa de diálogo é exibida da seguinte forma:

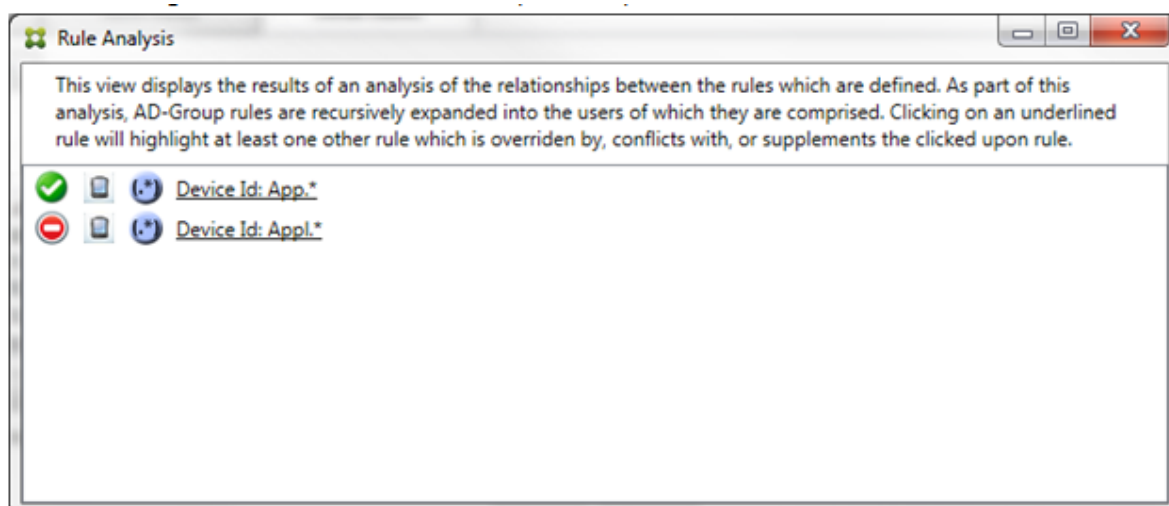


Nesse exemplo, a regra de expressão regular `WorkMail.*` é a regra principal (indicada pela borda sólida) e a regra normal `workmailc633313818` é uma regra auxiliar (indicada pela borda tracejada). O ponto preto ao lado da regra auxiliar é uma indicação visual adicional de que a regra está inativa (nunca será avaliada) devido à regra de expressão regular de prioridade mais alta que a precede. Depois de clicar na regra predominante, a caixa de diálogo é exibida da seguinte forma:



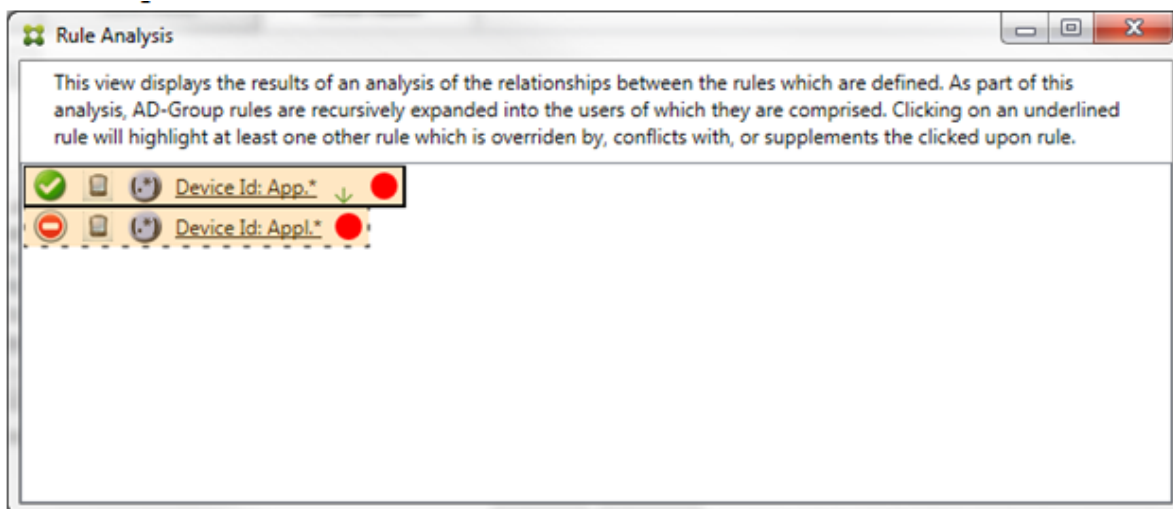
No exemplo anterior, a regra de expressão regular `WorkMail.*` é a regra auxiliar (indicada pela borda tracejada) e a regra normal `workmailc633313818` é uma regra principal (indicada pela borda sólida). Nesse exemplo simples, não há muita diferença. Para um exemplo mais complicado, consulte o exemplo de expressão complexa mais adiante neste tópico. Em um cenário com muitas regras definidas, clicar na regra substituída rapidamente identifica qual regra ou regras a substituíram.

Quando ocorrer um conflito, pelo menos duas regras serão sublinhadas: a regra principal e a regra ou as regras auxiliares. As regras em conflito são indicadas por um ponto vermelho. Regras que só entram em conflito uma com a outra são possíveis somente com duas ou mais regras de expressão regular definidas. Em todos os outros cenários de conflito, não haverá somente um conflito, mas uma substituição envolvida. Antes de clicar em qualquer uma das regras em um exemplo simples, a caixa de diálogo é exibida da seguinte forma:



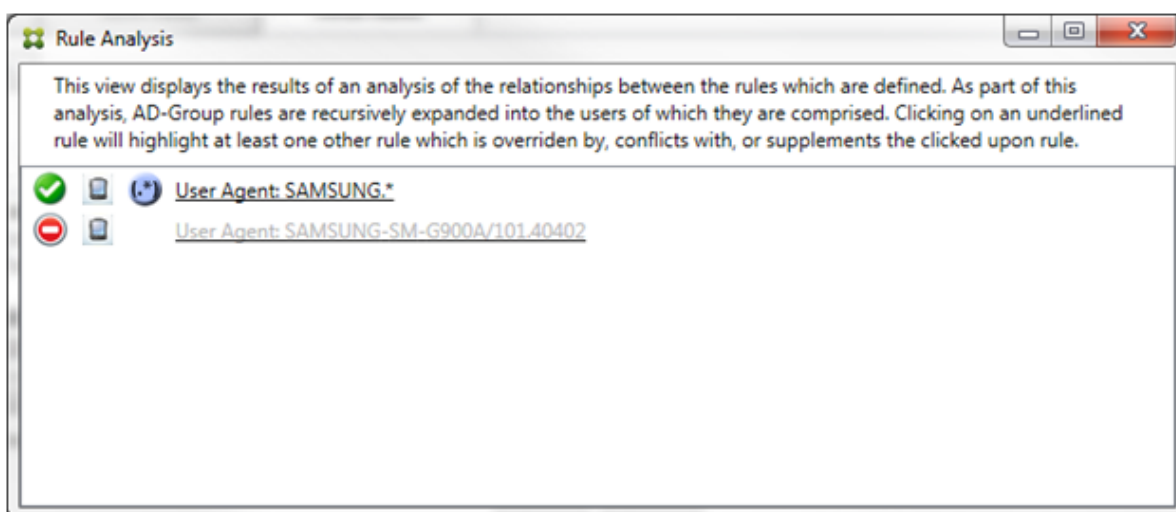
Quando se inspeciona as duas regras de expressão regular, fica evidente que a primeira regra permite todos os dispositivos com um ID de dispositivo que contém "App" e que a segunda regra nega todos os dispositivos com um ID de dispositivo que contém "Appl". Além disso, mesmo que a segunda re-

gra negue todos os dispositivos com um ID de dispositivo que contém “Appl”, nenhum dispositivo com esses critérios de correspondência jamais será negado, devido à precedência mais alta da regra permitir. Depois de clicar na primeira regra, a caixa de diálogo é exibida da seguinte forma:



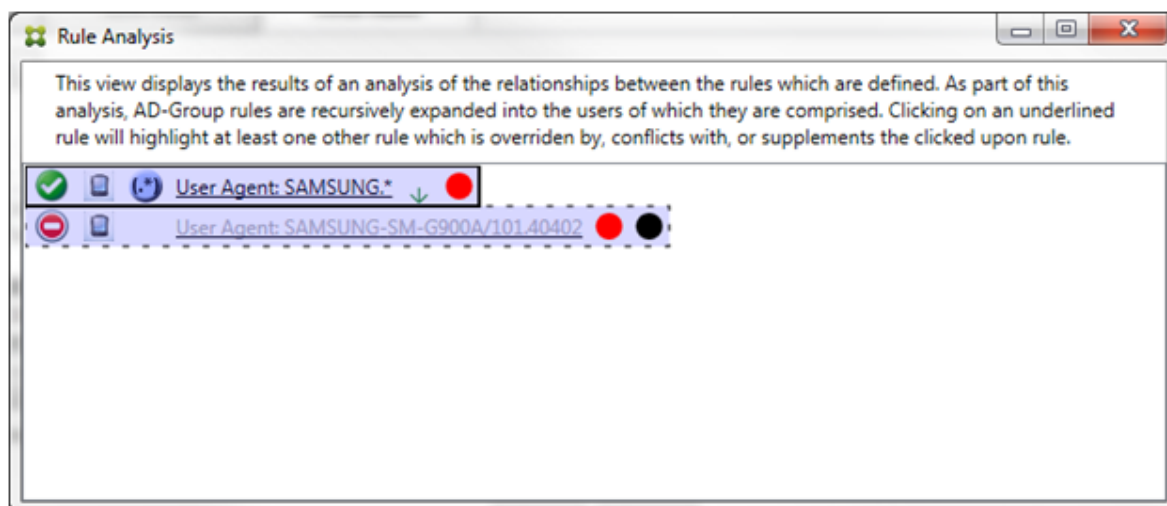
No cenário anterior, tanto a regra principal (a regra de expressão regular `App.*`) quanto a regra auxiliar (a regra de expressão regular `Appl.*`) são realçadas em amarelo. Trata-se simplesmente de um aviso visual para alertar para o fato de que você aplicou mais de uma única regra de expressão regular a um único campo passível de correspondência, o que pode significar um problema de redundância ou algo mais sério.

Em um cenário com um conflito e uma predominância, tanto a regra principal (a regra de expressão regular `App.*`) quanto a regra auxiliar (a regra de expressão regular `Appl.*`) são realçadas em amarelo. Trata-se simplesmente de um aviso visual para alertar para o fato de que você aplicou mais de uma única regra de expressão regular a um único campo passível de correspondência, o que pode significar um problema de redundância ou algo mais sério.



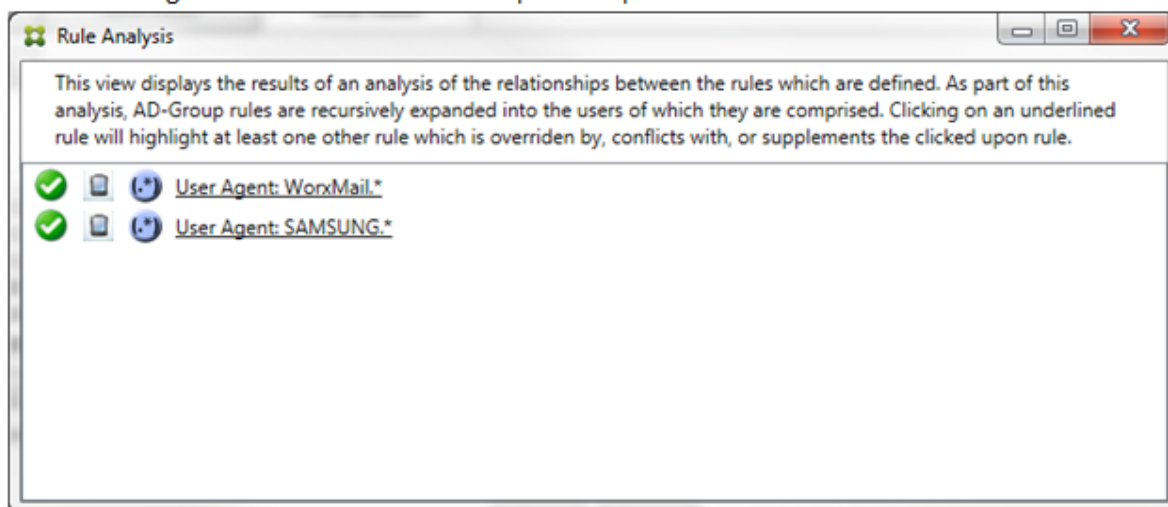
É fácil ver, no exemplo anterior, que a primeira regra (a regra de expressão regular `SAMSUNG.*`) não somente substitui a regra seguinte (a regra normal `SAMSUNG-SM-G900A/101.40402`), mas as duas regras diferem no respectivo acesso (a principal especifica Permitir, a auxiliar especifica Bloquear). A segunda regra (a regra normal `SAMSUNG-SM-G900A/101.40402`) é exibida em um texto mais fino para indicar que ela foi substituída e, portanto, está inativa.

Depois de clicar na regra de expressão regular, a caixa de diálogo é exibida da seguinte forma:

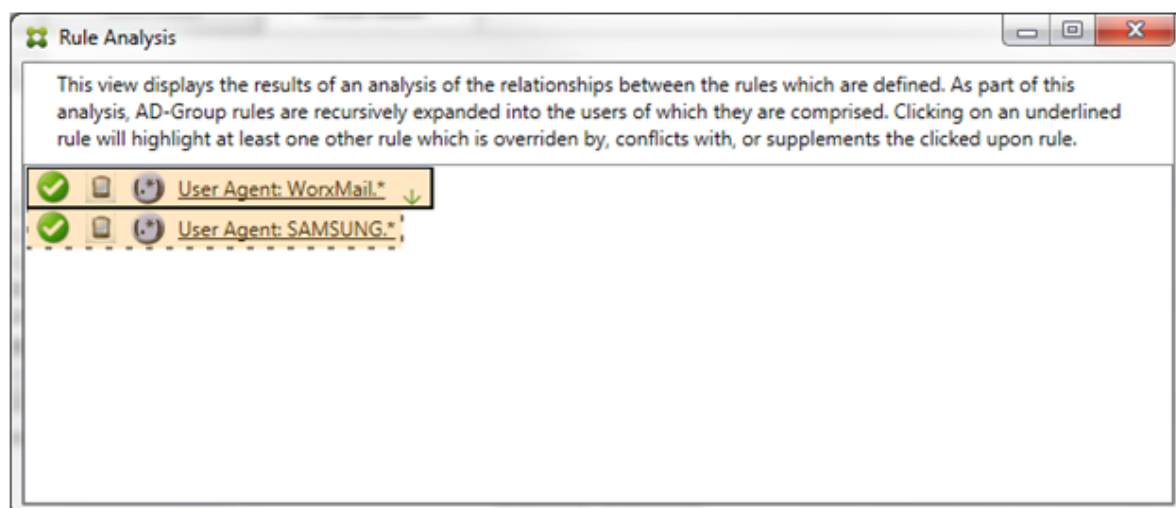


A regra principal (a regra de expressão regular `SAMSUNG.*`) é seguida por um ponto vermelho para indicar que o estado de acesso dela entra em conflito com uma ou mais regras auxiliares. A regra auxiliar (regra normal `SAMSUNG-SM-G900A/101.40402`) é seguida por um ponto vermelho para indicar que seu estado de acesso está em conflito com a regra primária. Essa regra também é seguida por um ponto preto para indicar que foi substituída e, portanto, está inativa.

Pelo menos duas regras serão sublinhadas: a regra principal e a regra ou as regras auxiliares. As regras que somente suplementam uma à outra envolverão apenas regras de expressão regular. Quando regras suplementam uma à outra, elas são indicadas por uma sobreposição amarela. Antes de clicar em qualquer uma das regras em um exemplo simples, a caixa de diálogo é exibida da seguinte forma:



A inspeção visual facilmente revela que ambas as regras são regras de expressão regular que foram aplicadas ao campo de ID de dispositivo ActiveSync no conector de Endpoint Management para Exchange ActiveSync. Depois de clicar na primeira regra, a caixa de diálogo tem a seguinte aparência:

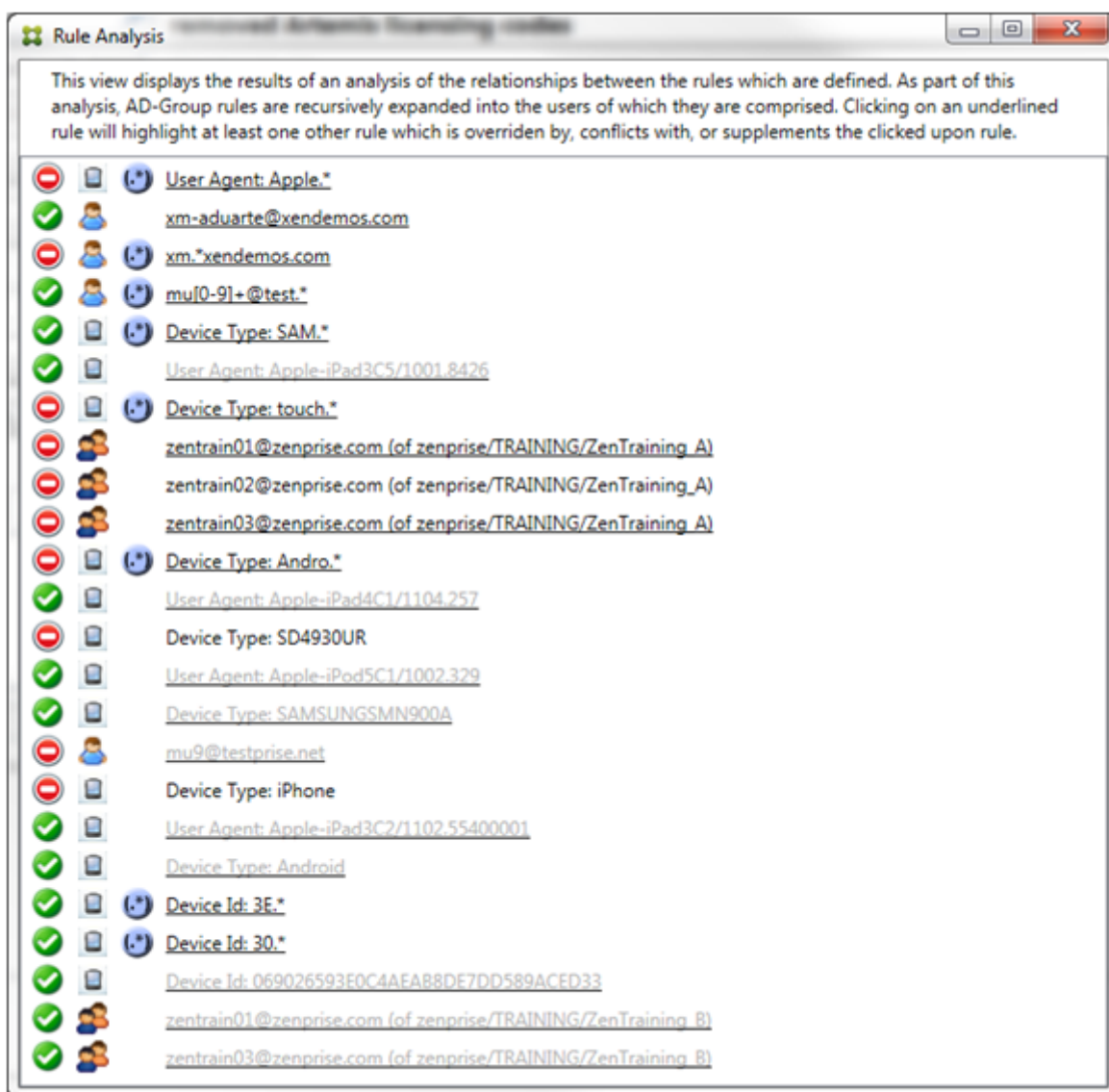


A regra principal (a regra de expressão regular `WorkMail.*`) é realçada com uma sobreposição amarela para indicar que existe pelo menos uma regra auxiliar a mais que é uma expressão regular. A regra auxiliar (a regra de expressão regular `SAMSUNG.*`) é realçada com uma sobreposição amarela para indicar que ela e a regra principal são regras de expressão regular aplicadas ao mesmo campo no conector de Endpoint Management para Exchange ActiveSync. Nesse caso, esse campo é o ID do dispositivo do ActiveSync. As expressões regulares podem ou não se sobrepor. Cabe a você decidir se as expressões regulares foram devidamente trabalhadas.

Exemplo de uma expressão complexa

Muitas substituições, conflitos ou suplementos possíveis podem ocorrer, tornando impossível oferecer um exemplo de todos os cenários possíveis. O exemplo a seguir discute o que não fazer, servindo também para ilustrar todo o poder da construção visual de análise de regra. A maioria dos itens estão sublinhados na figura a seguir. Muitos dos itens são exibidos em uma fonte mais fina, o que indica que a regra em questão foi substituída por uma regra de prioridade mais alta de alguma maneira. Muitas

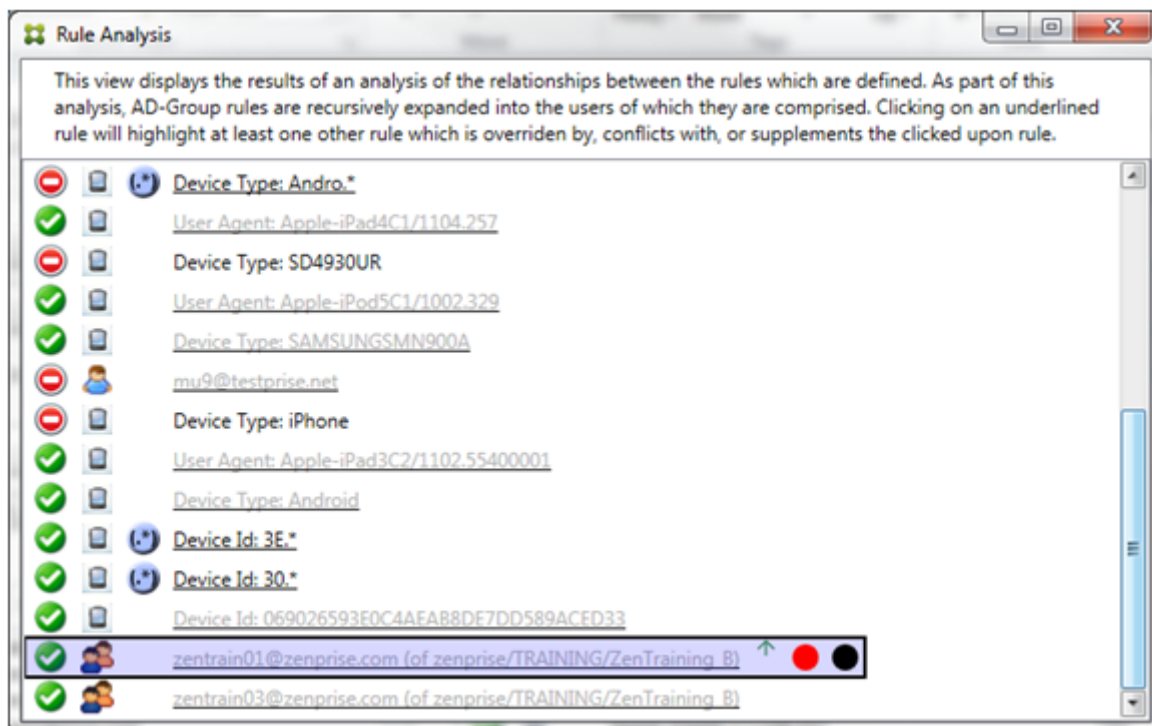
regras de expressão regular também estão incluídas na lista, conforme indicado pelo ícone



Como analisar uma substituição

Para ver qual regra ou regras substituíram uma regra específica, clique nela.

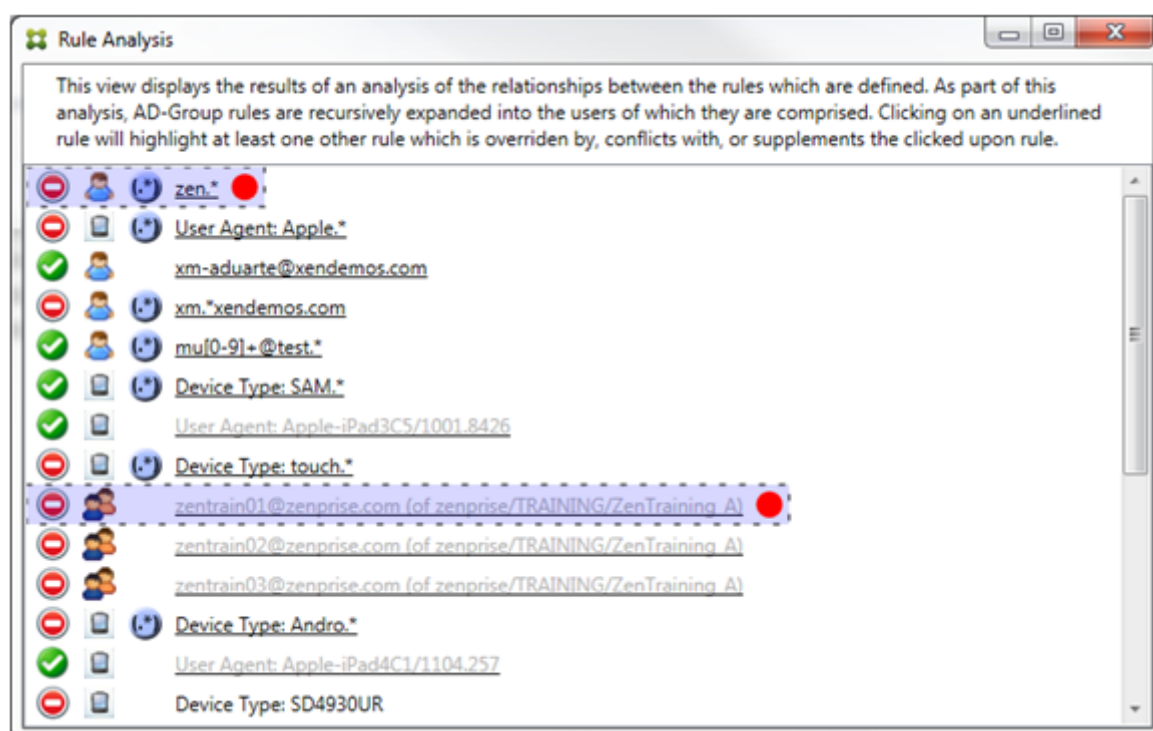
Exemplo 1: Esse exemplo examina por que `zentrain01@zenprise.com` foi substituída.



A regra principal (regra `zenprise/TRAINING/ZenTraining_B`, da qual `zentrain01@zenprise.com` é um membro) apresenta as seguintes características:

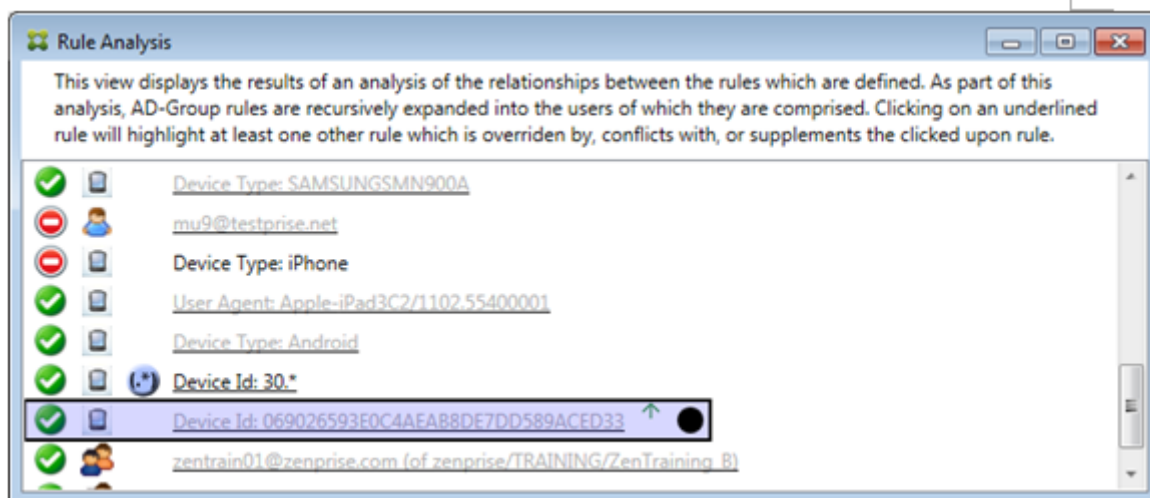
- Está realçada em azul e tem uma borda sólida.
- Tem uma seta verde apontando para cima (para indicar que a regra ou as regras auxiliares todas se encontram acima dela).
- É seguida por um círculo vermelho e um círculo preto para indicar, respectivamente, que um ou mais regras auxiliares entram em conflito com o respectivo acesso e que a regra principal foi substituída e, portanto, está inativa.

Quando você rola para cima, vê o seguinte:



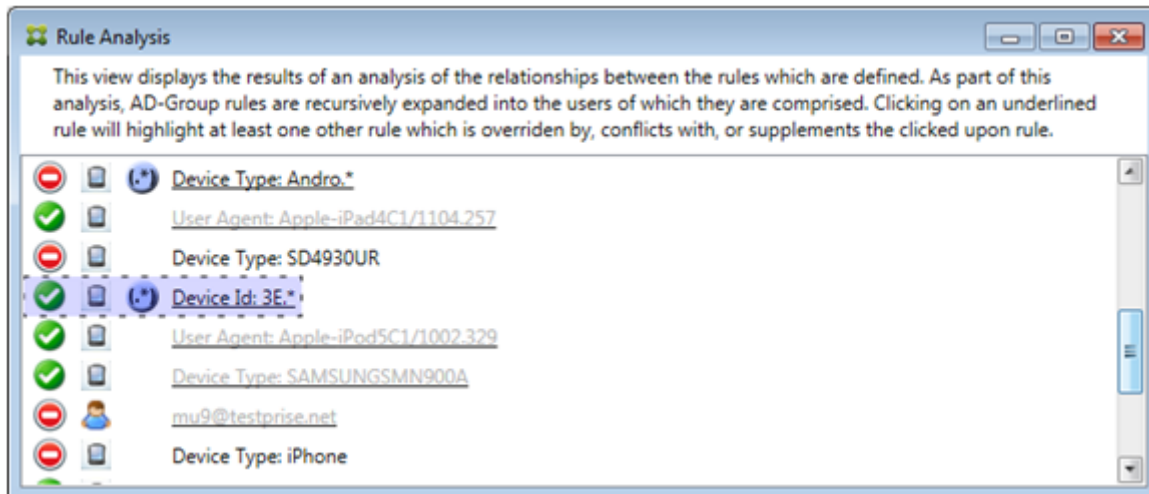
Nesse caso, há duas regras auxiliares que substituem a regra principal: a regra de expressão regular `zen.*` e a regra normal `zentrain01@zenprise.com` (de `zenprise/TRAINING/ZenTraining A`). No caso da última regra auxiliar, o que ocorreu é que a regra de Grupo do Active Directory `ZenTraining A` contém o usuário `zentrain01@zenprise.com` e a regra de Grupo do Active Directory `ZenTraining B` também contém o usuário `zentrain01@zenprise.com`. No entanto, como a regra auxiliar tem uma precedência mais alta do que a regra principal, a regra principal foi substituída. O acesso da regra principal é Permitir e, como o acesso da regra auxiliar é Bloquear, todas são seguidas por um círculo vermelho como indicação adicional de um conflito de acesso.

Exemplo 2: Esse exemplo mostra por que o dispositivo com um ID de dispositivo ActiveSync `069026593E0C4AEAB8DE7DD589ACED33` foi substituído:



A regra principal (regra de ID de dispositivo normal 069026593E0C4AEAB8DE7DD589ACED33) apresenta as seguintes características:

- Está realçada em azul e tem uma borda sólida.
- Tem uma seta verde apontando para cima (para indicar que a regra auxiliar se encontra acima dela).
- É seguida por um círculo preto para indicar que uma regra auxiliar substituiu a regra principal e, portanto, está inativa.

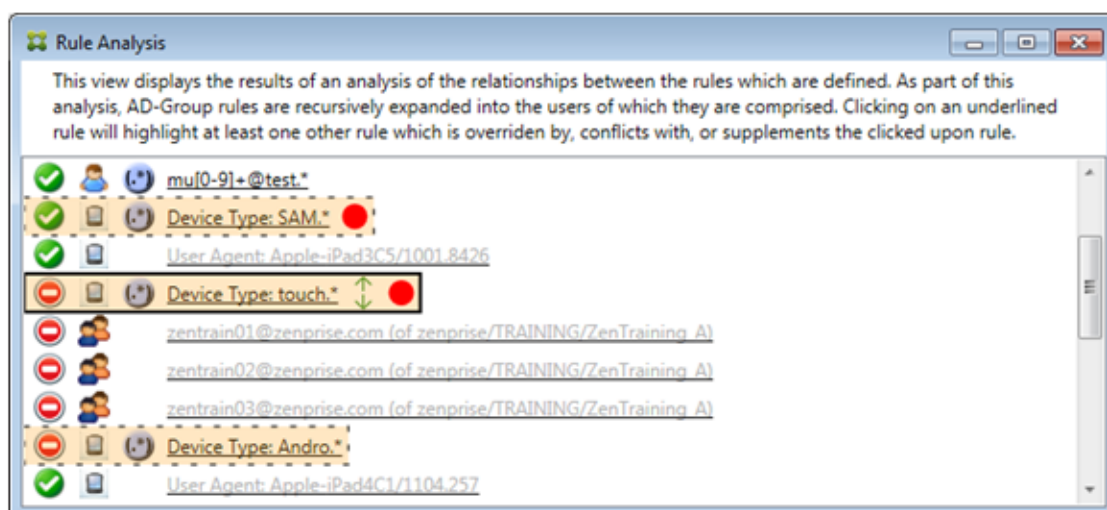


Nesse caso, uma única regra auxiliar substituiu a regra principal: a regra de ID de dispositivo ActiveSync de expressão regular é 3E.*. Como a expressão regular 3E.* corresponderia a 069026593E0C4AEAB8DE7DD589ACED33, a regra principal nunca será avaliada.

Como analisar um suplemento e um conflito

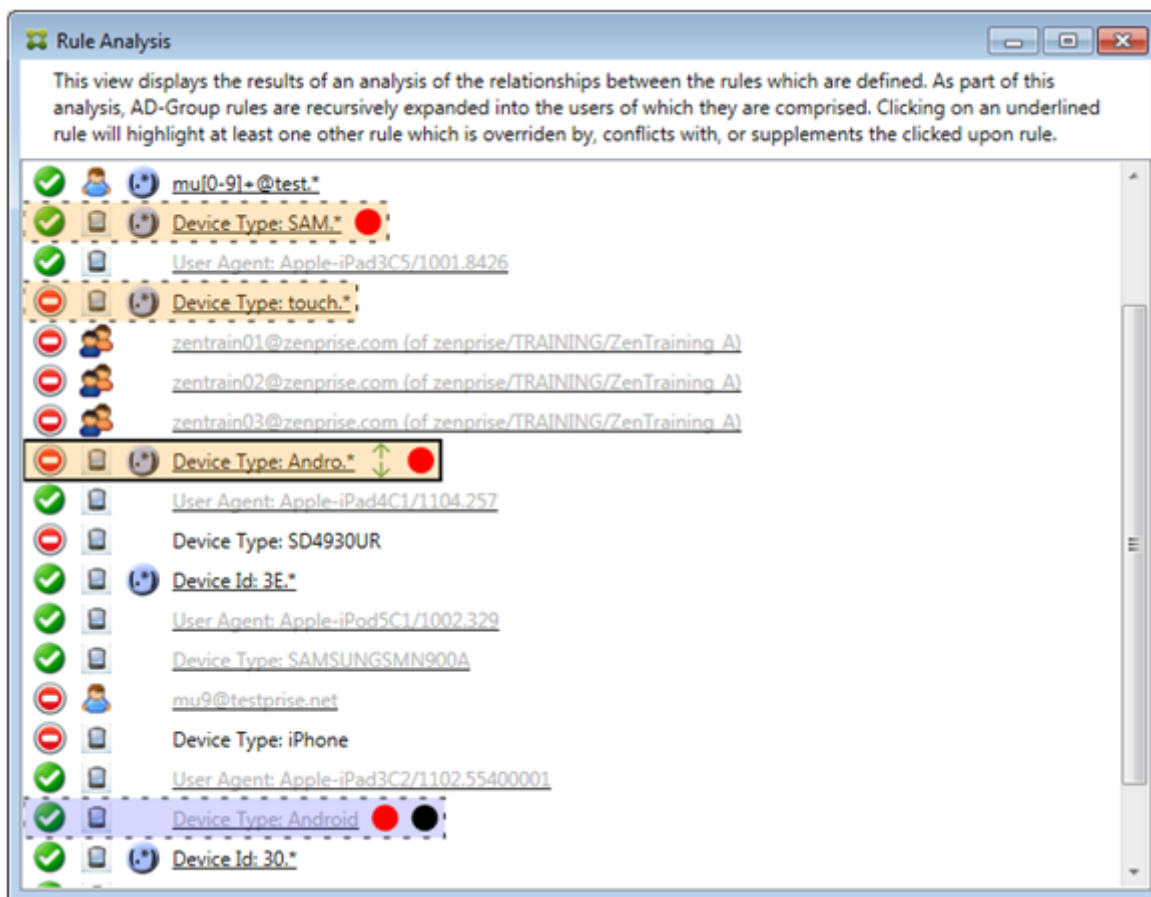
Neste caso, a regra principal é a regra de tipo de dispositivo ActiveSync de expressão regular `touch.*`. As características são as seguintes:

- É indicada por uma borda sólida com uma sobreposição amarela, como um aviso de que há mais de uma única regra de expressão regular em funcionamento em relação a um campo de regra específico; nesse caso, o tipo de dispositivo ActiveSync.
- Duas setas apontam respectivamente para cima e para baixo, indicando que há pelo menos uma regra auxiliar com prioridade mais alta e pelo menos uma regra auxiliar com prioridade mais baixa.
- O círculo vermelho ao lado dela indica que pelo menos uma regra auxiliar tem o respectivo acesso definido como Permitir, o que entra em conflito com o acesso Bloquear da regra principal
- Existem duas regras auxiliares: a regra de tipo de dispositivo ActiveSync de expressão regular `SAM.*` e a regra de tipo de dispositivo ActiveSync de expressão regular `Andro.*`.
- Ambas as regras auxiliares têm bordas tracejadas para indicar que são auxiliares.
- Ambas as regras auxiliares têm uma sobreposição amarela para indicar que também são aplicadas ao campo de regra do tipo de dispositivo ActiveSync.
- Em tais cenários, você deve garantir que as respectivas regras de expressão regular não sejam redundantes.



Como analisar ainda mais as regras

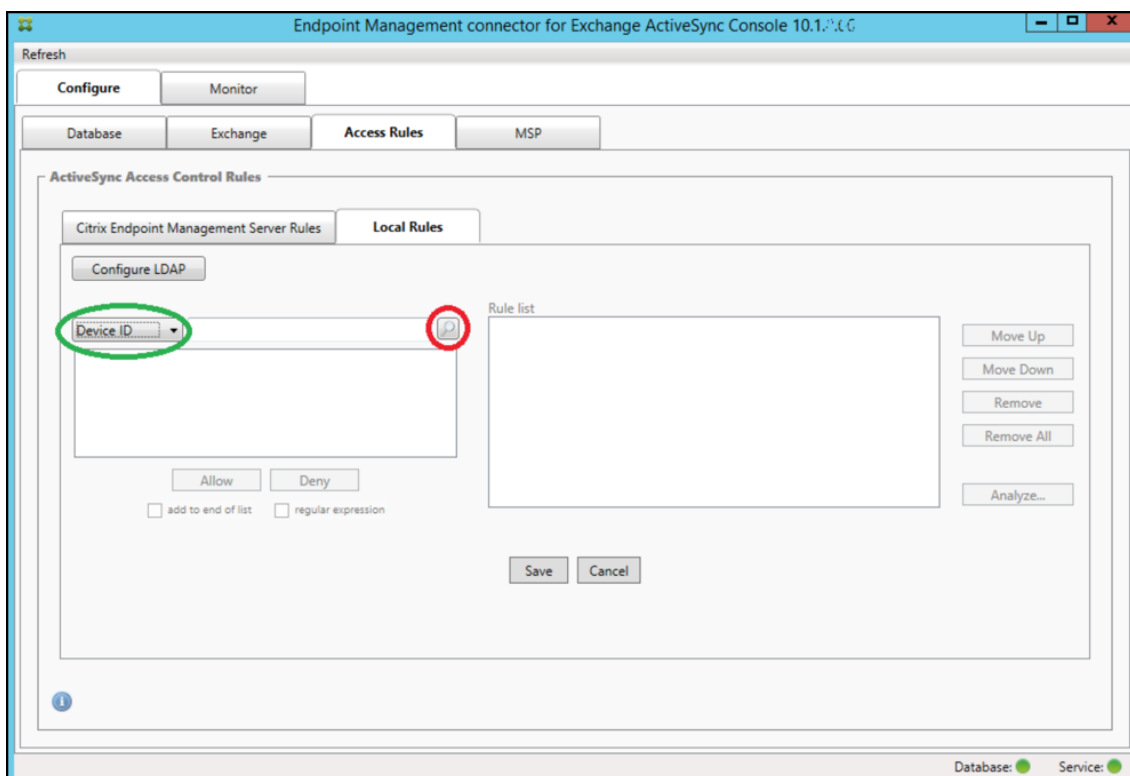
Este exemplo explora como as relações entre regras sempre existem na perspectiva da regra principal. O exemplo anterior mostrou como clicar na regra de expressão regular aplicada ao campo de regra do tipo de dispositivo com um valor de `touch.*`. Clicar na regra auxiliar `Andro.*` mostra um conjunto diferente de regras auxiliares destacadas.



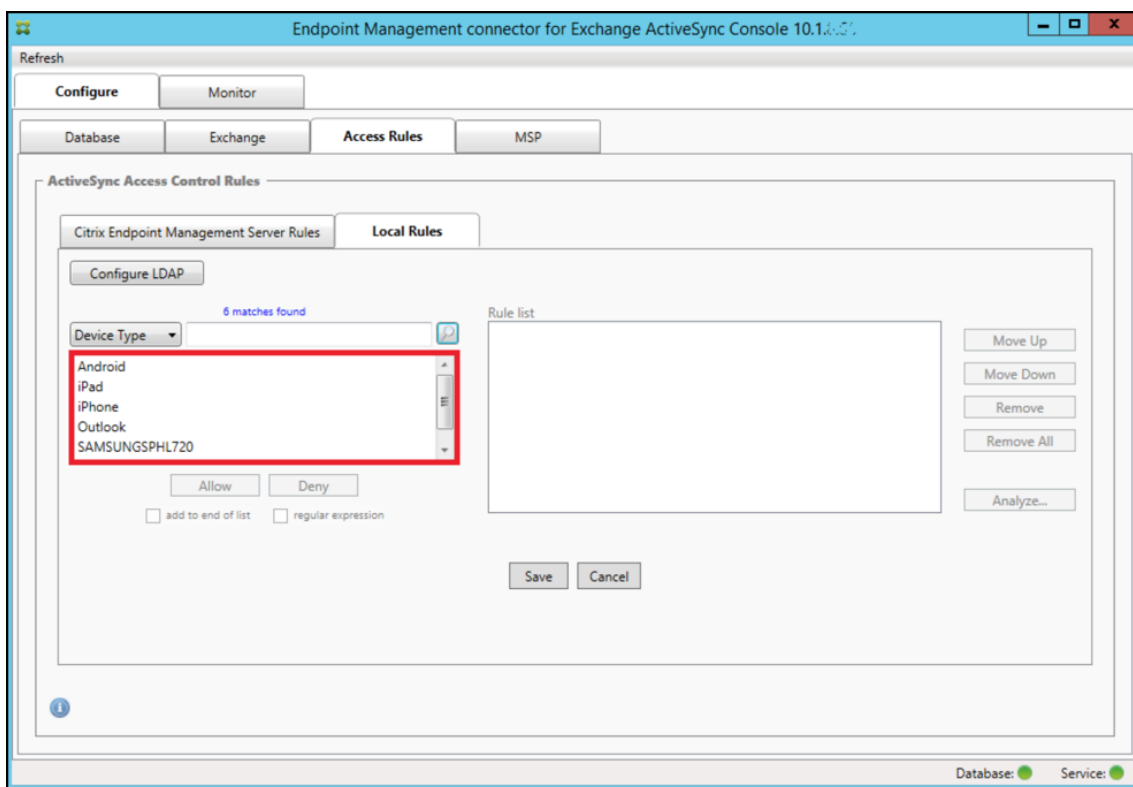
O exemplo mostra uma regra substituída que está incluída na relação de regra. Essa regra é a regra normal de tipo de dispositivo ActiveSync *Android*, que é substituída (indicada pela fonte fina e o círculo preto ao lado dela) e também entra em conflito no respectivo acesso com a regra de tipo de dispositivo ActiveSync de expressão regular da regra principal *Andro.**. Essa regra era anteriormente uma regra auxiliar antes de ser clicada. No exemplo anterior, a regra normal de tipo de dispositivo ActiveSync *Android* não era exibida como uma regra auxiliar pois, na perspectiva da regra principal naquele momento (a regra de tipo de dispositivo ActiveSync de expressão regular *touch.**), a regra não era relacionada a ela.

Para configurar uma regra local de expressão normal

1. Clique na guia **Access Rules**.



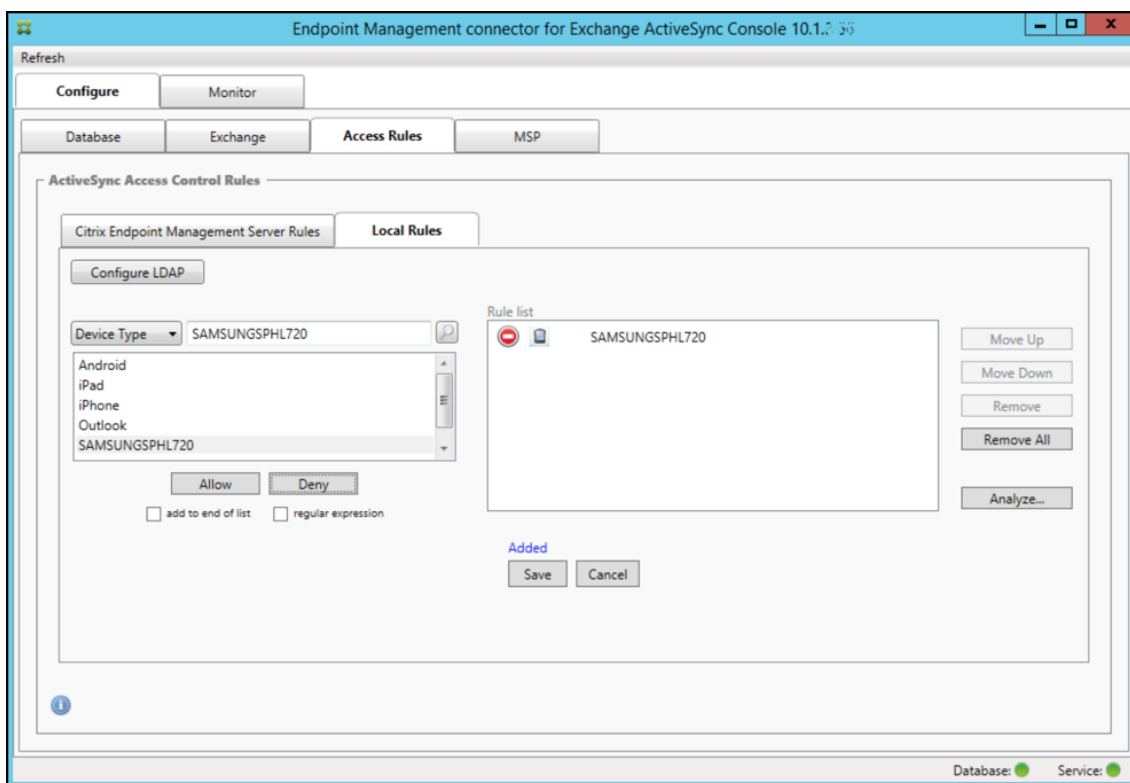
2. Na lista **Device ID**, selecione o campo para o qual você deseja criar uma Regra Local.
3. Clique no ícone de lupa para exibir todas as correspondências exclusivas do campo escolhido. Neste exemplo, o campo **Device Type** foi escolhido e as opções são mostradas abaixo, na caixa de lista.



4. Clique em um dos itens na caixa de lista de resultados e, em seguida, clique em uma das seguintes opções:

- **Allow** significa que o Exchange será configurado para permitir o tráfego do ActiveSync para todos os dispositivos correspondentes.
- **Deny** significa que o Exchange será configurado para negar o tráfego do ActiveSync para todos os dispositivos correspondentes.

Neste exemplo, todos os dispositivos que têm um tipo de dispositivo SamsungSPHL720 têm acesso negado.



Para adicionar uma expressão regular

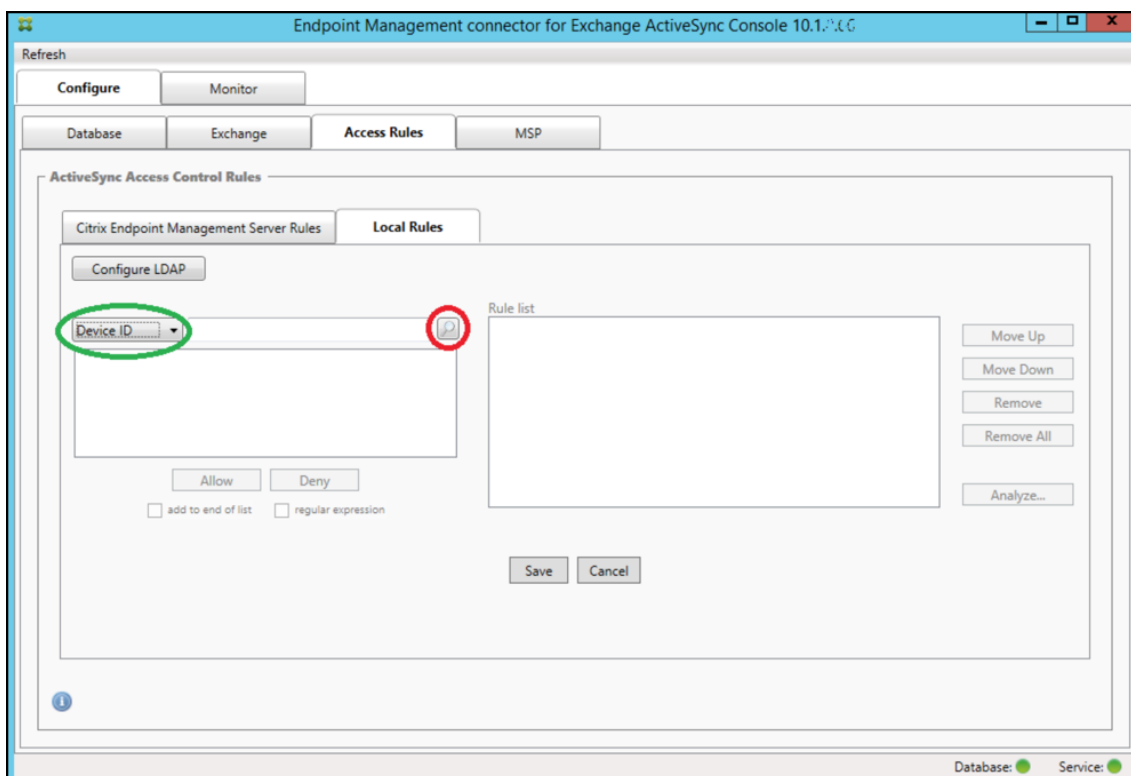


As regras locais de expressão regular podem ser distinguidas pelo ícone exibido ao lado delas -

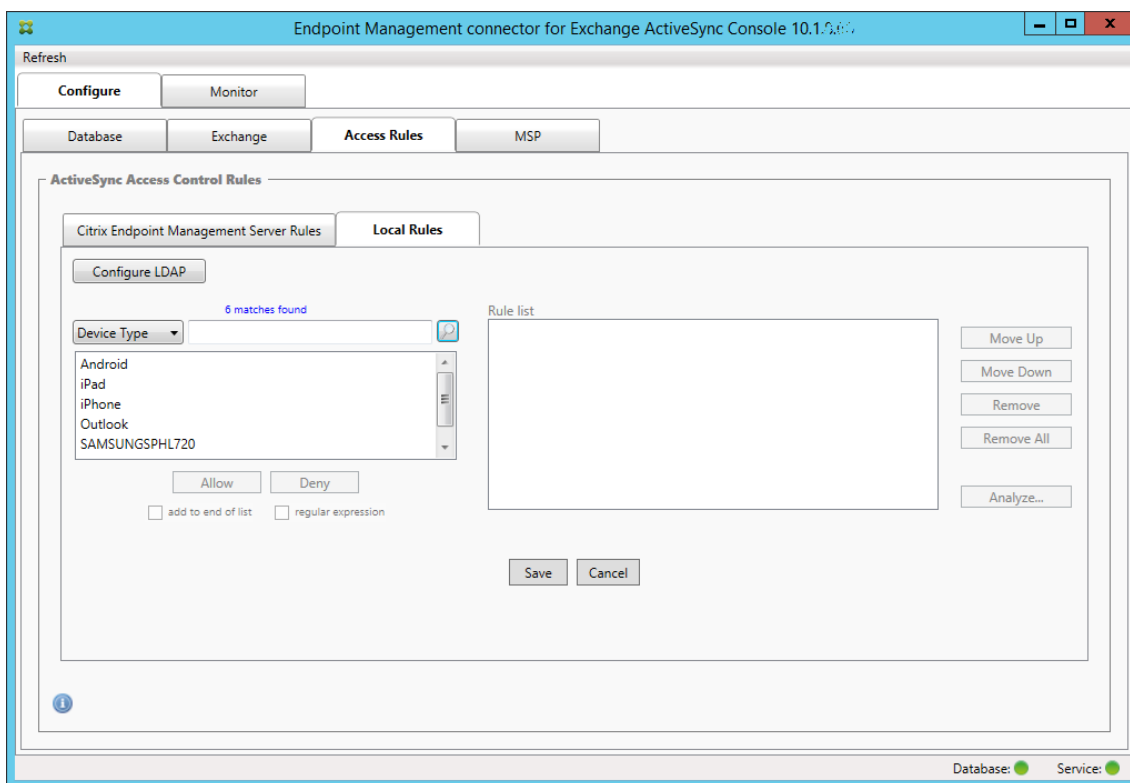
Para adicionar uma regra de expressão regular, você pode criar uma regra de expressão regular com base em um valor existente na lista de resultados de um determinado campo (desde que um instante principal tenha sido concluído) ou pode simplesmente digitar a expressão regular que desejar.

Para criar uma expressão regular com base em um valor de campo existente

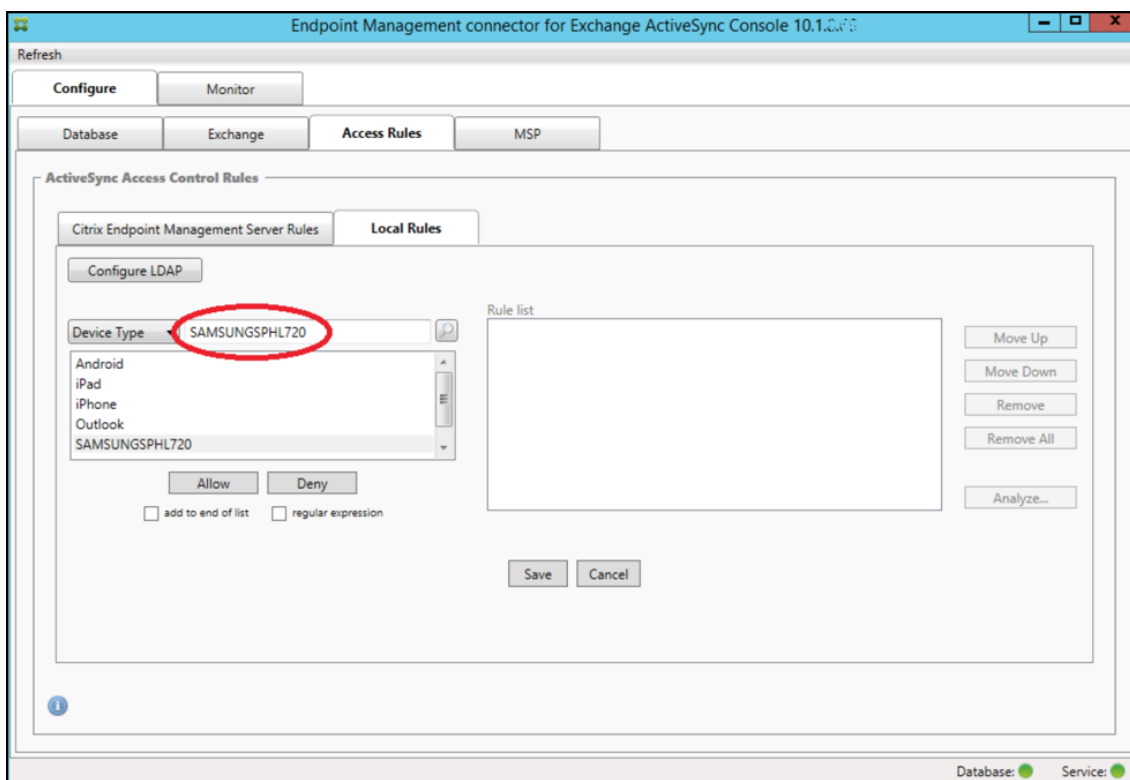
1. Clique na guia **Access Rules**.



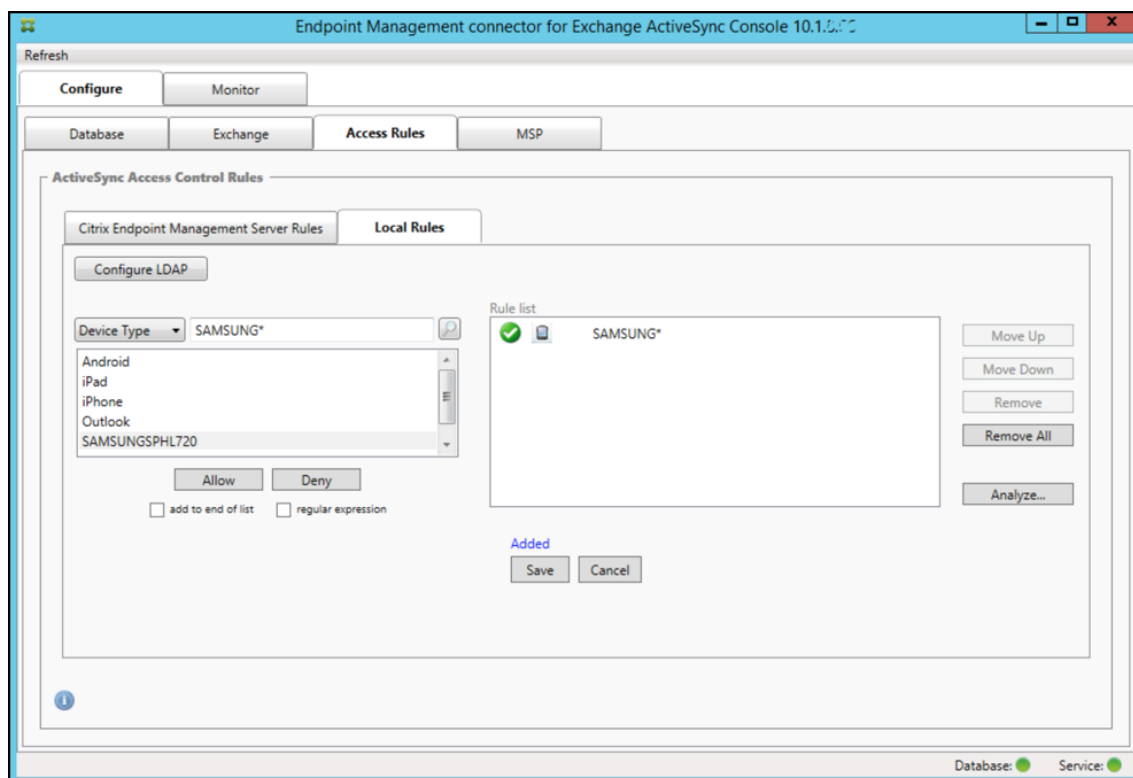
2. Na lista **Device ID**, selecione o campo para o qual você deseja criar uma Regra Local de expressão regular.
3. Clique no ícone de lupa para exibir todas as correspondências exclusivas do campo escolhido. Neste exemplo, o campo **Device Type** foi escolhido e as opções são mostradas abaixo, na caixa de lista.



4. Clique em um dos itens na lista de resultados. Nesse exemplo, **SAMSUNGSPHL720** foi selecionado e é exibido na caixa de texto adjacente a **Device Type**.

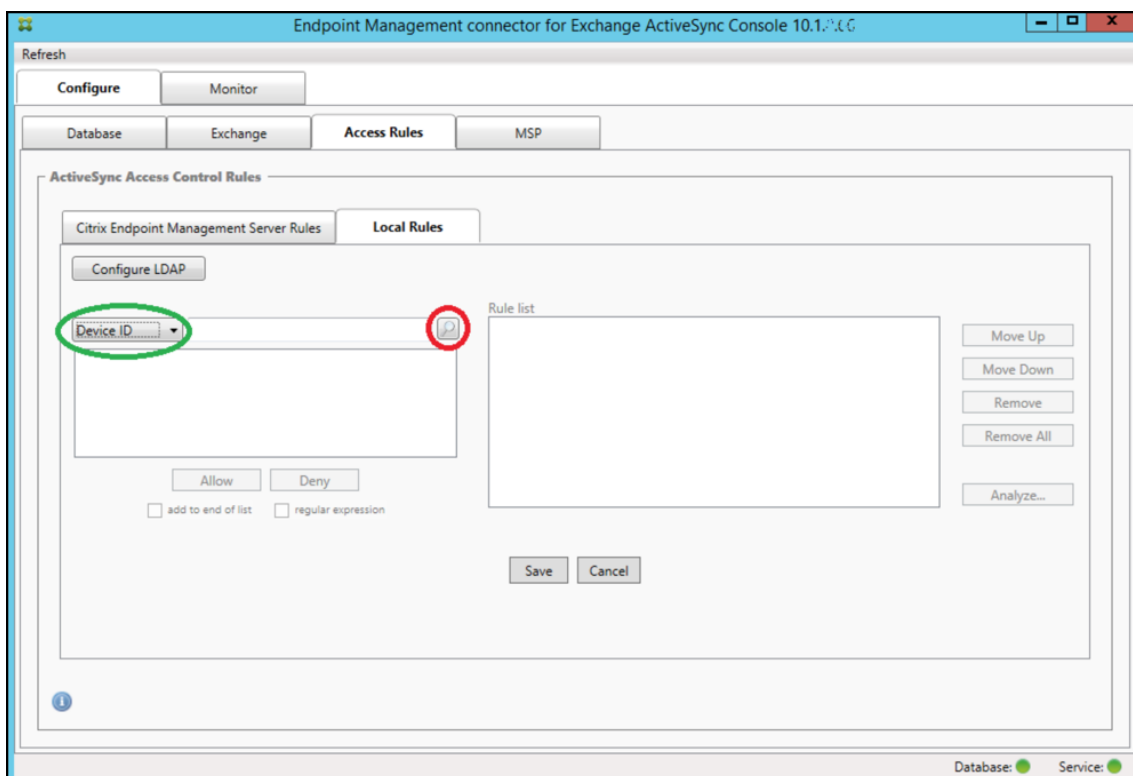


5. Para permitir todos os tipos de dispositivo que têm “Samsung” no respectivo valor de tipo de dispositivo, adicione uma regra de expressão regular seguindo estas etapas:
 - a) Clique na caixa de texto do item selecionado.
 - b) Altere o texto de **SAMSUNGSPHL720** para **SAMSUNG.***.
 - c) Verifique se a caixa de seleção regular expression está marcada.
 - d) Clique em **Allow**.

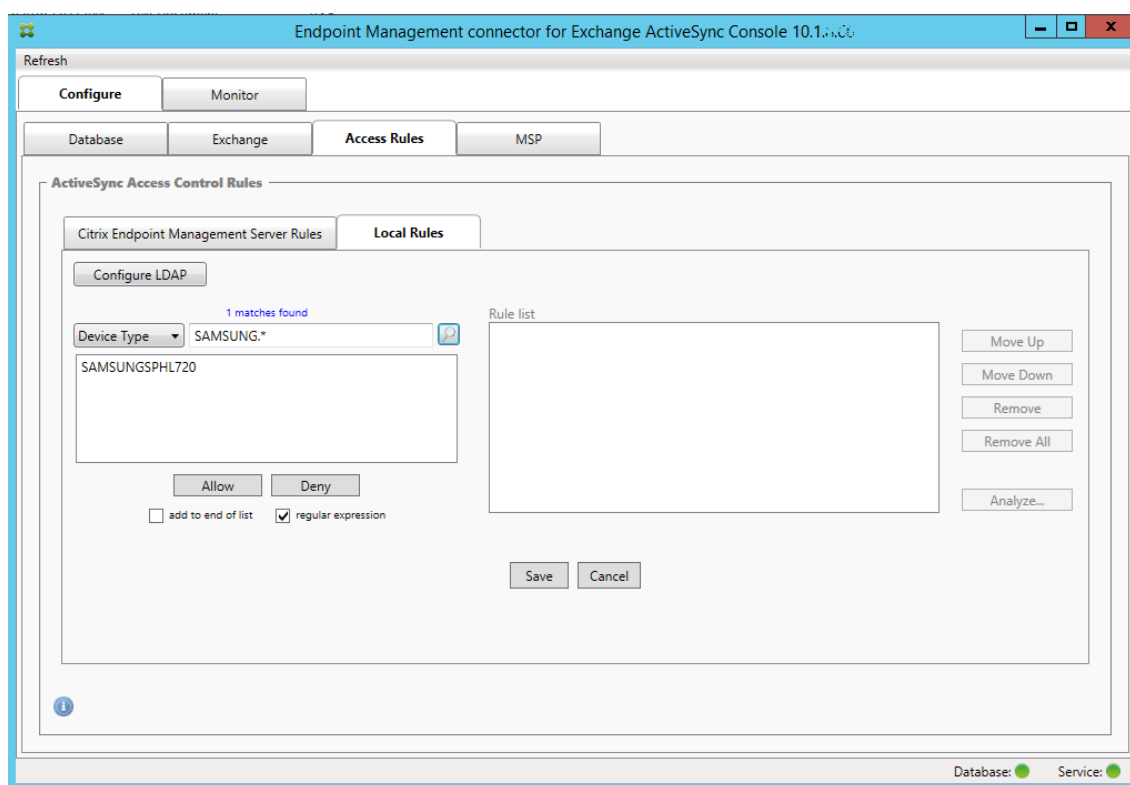


Para criar uma regra de acesso

1. Clique na guia **Local Rules**.
2. Para inserir a expressão regular, você precisa usar a lista Device ID e a caixa de texto do item selecionado.



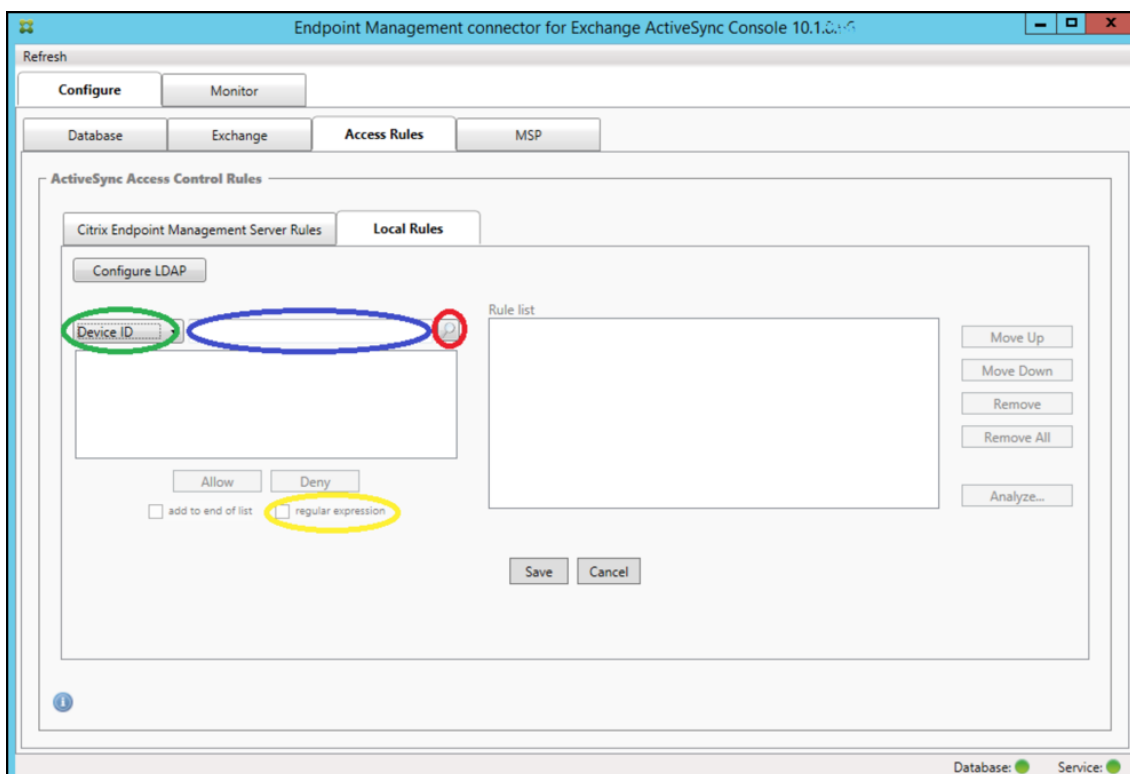
3. Selecione o campo em relação ao qual você deseja corresponder. Esse exemplo usa Device Type.
4. Digite a expressão regular. Esse exemplo usa `samsung.*`
5. Verifique se a caixa de seleção regular expression está marcada e clique em **Allow** ou em **Deny**. Neste exemplo, a escolha é **Permitir**. O resultado final é o seguinte:



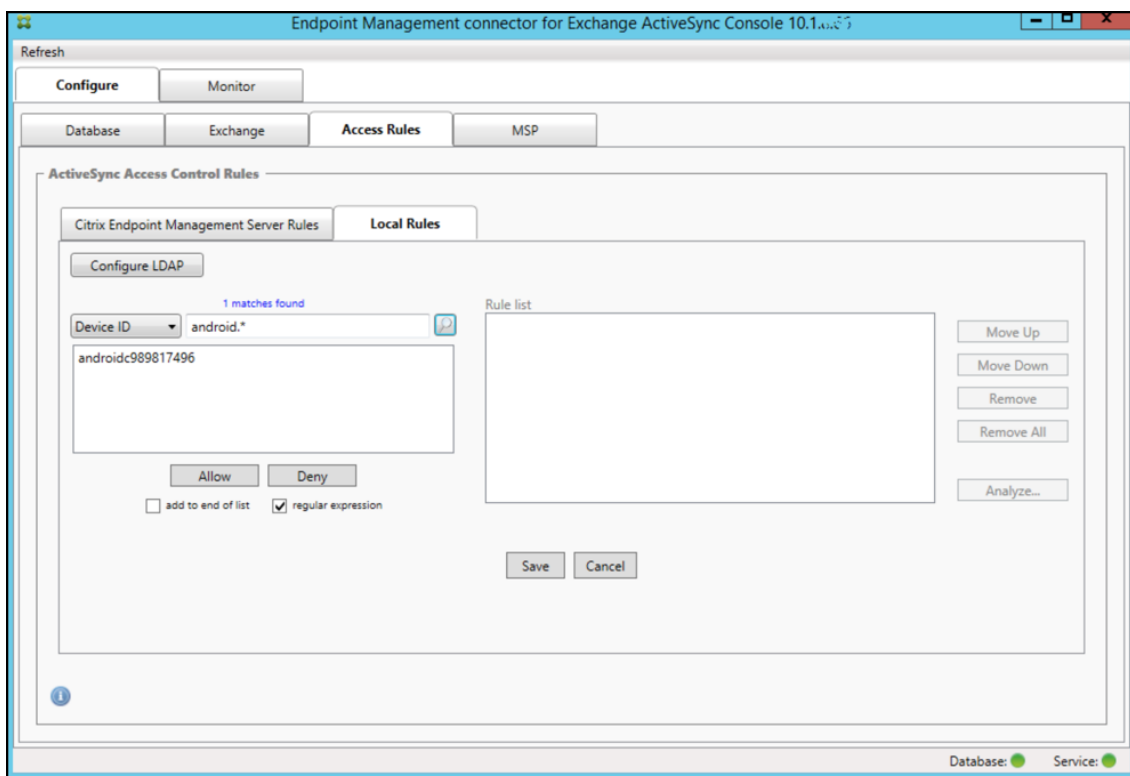
Para encontrar dispositivos

Ao marcar a caixa de seleção de expressão regular, você pode executar pesquisas para dispositivos específicos que correspondem à expressão específica. Esse recurso estará disponível somente se um instantâneo principal tiver sido concluído com êxito. Você pode usar esse recurso mesmo que não haja nenhum planejamento para usar regras de expressão regular. Por exemplo, suponha que você deseja encontrar todos os dispositivos que tenham o texto “workmail” no respectivo ID de dispositivo ActiveSync. Para fazê-lo, siga este procedimento.

1. Clique na guia **Access Rules**.
2. Verifique se o seletor do campo de correspondência do dispositivo está definido como Device ID (o padrão).



3. Clique na caixa de texto do item selecionado (conforme mostrado em azul na figura anterior) e digite **workmail.***.
4. Confirme que a caixa de seleção regular expression esteja marcada e, em seguida, clique no ícone de lupa para exibir as correspondências, conforme mostrado na figura a seguir.

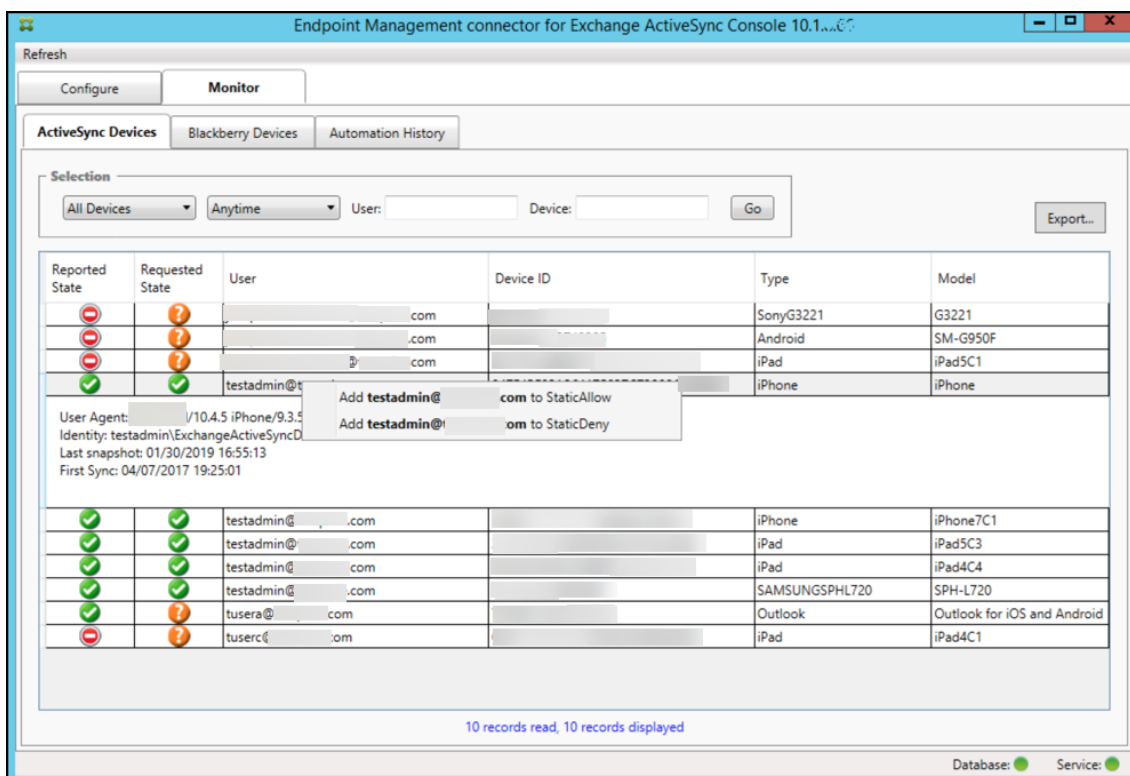


Para adicionar um usuário, um dispositivo ou um tipo de dispositivo individual a uma regra estática

Você pode adicionar regras estáticas com base no usuário, no ID de dispositivo ou no tipo de dispositivo na guia ActiveSync Devices.

1. Clique na guia **ActiveSync Devices**.
2. Na lista, clique com o botão direito em um usuário, um dispositivo ou um tipo de dispositivo e selecione se você deseja permitir ou negar a sua seleção.

A imagem a seguir mostra a opção Allow/Deny quando user1 está selecionado.



Monitoramento de dispositivo

A guia **Monitor** no conector de Endpoint Management para Exchange ActiveSync permite navegar nos dispositivos do Exchange ActiveSync e do BlackBerry que foram detectados e no histórico de comandos automatizados do PowerShell que foram emitidos. A guia **Monitor** tem as seguintes três guias:

- **ActiveSync Devices:**
 - Você pode exportar as parcerias de dispositivo do ActiveSync exibidas clicando no botão **Export**.
 - Você pode adicionar regras locais (estáticas) clicando nas colunas **User**, **Device ID** ou **Type** e selecionando o tipo de regra de permissão ou bloqueio apropriado.
 - Para recolher uma linha expandida, clique com o Ctrl pressionado na linha expandida.
- **Dispositivos BlackBerry**
- **Histórico de automação**

A guia **Configure** mostra o histórico de todos os instantâneos. O histórico de instantâneos mostra quando o instantâneo ocorreu, o tempo que levou, quantos aparelhos foram detectados e todos os erros que ocorreram:

- Na guia **Exchange**, clique no ícone de informações do Exchange Server desejado.
- Na guia **MSP**, clique no ícone de informações do BlackBerry Server desejado.

Resolução de problemas e diagnósticos

O conector de Endpoint Management para Exchange ActiveSync registra erros e outras informações operacionais no respectivo arquivo de log: *pasta de instalação\log\XmmWindowsService.log*. O conector de Endpoint Management para Exchange ActiveSync também registra eventos significativos no Log de Eventos do Windows.

Para alterar o nível de log

O conector de gerenciamento de ponto de extremidade para o Exchange ActiveSync inclui os seguintes níveis de log: Erro, Informações, Aviso, Depuração e Rastreamento.

Nota:

Cada nível sucessivo gera mais detalhes (mais dados). Por exemplo, o nível Erro fornece o mínimo de detalhes, enquanto o nível de Rastreamento fornece o máximo de detalhes.

Para alterar o nível de log, faça o seguinte:

1. Em C:\Program Files\Citrix\Citrix Endpoint Management connector, abra o arquivo `nlog.config`.
2. Na seção `<rules>`, altere o parâmetro `minilevel` para o nível de log que você preferir. Por exemplo:

```
1 <rules>
2
3 <logger name="*" writeTo="file" minlevel="Debug" />
4
5 </rules>
6 <!--NeedCopy-->
```

3. Salve o arquivo.

As alterações entram em vigor imediatamente. Não é necessário reiniciar o conector do Exchange ActiveSync.

Erros comuns

A seguinte lista inclui os erros comuns:

- O serviço conector de Endpoint Management para Exchange ActiveSync não inicia
Verifique o arquivo de log e o Log de Eventos do Windows em busca de erros. As causas típicas são as seguintes:
 - O serviço conector de Endpoint Management para Exchange ActiveSync não consegue acessar o SQL Server. Isso pode ser devido a estes problemas:

- * O serviço do SQL Server não está em execução.
- * Falha na autenticação.

Se a autenticação Integrated do Windows estiver configurada, a conta de usuário do serviço conector de Endpoint Management para Exchange ActiveSync deve ser um login permitido do SQL. A conta do serviço conector de Endpoint Management para Exchange ActiveSync tem como padrão o Sistema Local, mas pode ser alterada para qualquer conta que tenha privilégios de administrador local. Se a autenticação de SQL estiver configurada, o login do SQL deverá ser configurado corretamente no SQL.

- A porta configurada para o Provedor de Serviços Móveis (MSP) não está disponível. Deve haver uma porta de escuta selecionada que não seja usada por outro processo no sistema.

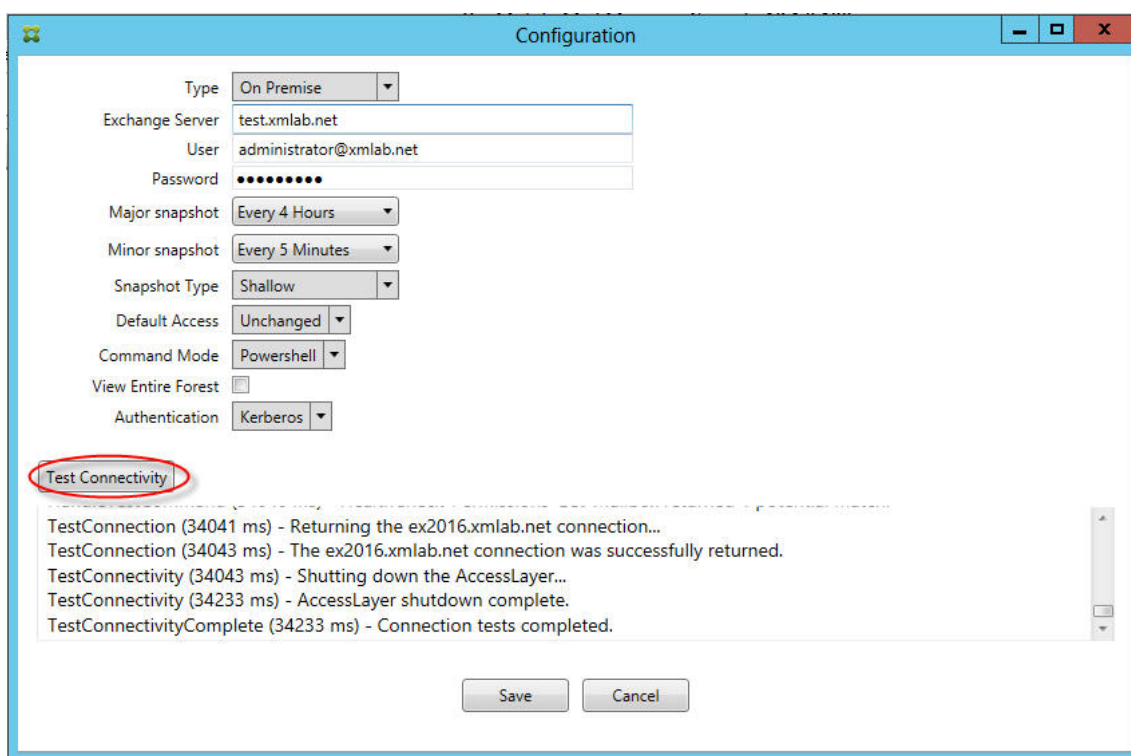
- O XenMobile não consegue se conectar ao MSP

Verifique se a porta de serviço e o transporte do MSP estão configurados corretamente na guia **Configure > MSP** do console conector de Endpoint Management para Exchange ActiveSync. Verifique se o Authorization Group ou o User está configurado corretamente.

Se HTTPS estiver configurado, um certificado de servidor SSL válido deverá ser instalado. Se IIS estiver instalado, o Gerenciador do IIS poderá ser usado para instalar o certificado. Se o IIS não estiver instalado, consulte [Como configurar uma porta com um certificado SSL](#) para obter detalhes sobre como instalar os certificados.

O conector de Endpoint Management para Exchange ActiveSync contém um programa utilitário para testar a conectividade com o serviço MSP. Execute o programa *PastadeInstalaçãoMspTestServiceClient.exe* e defina a URL e as credenciais para uma URL e credenciais que serão configuradas no XenMobile e, em seguida, clique em **Test Connectivity**. Isso simula as solicitações de serviço da Web que o XenMobile Server emite. Observe que, se HTTPS estiver configurado, você deverá especificar o nome de host real do servidor (o nome especificado no certificado SSL).

Quando você estiver usando **Test Connectivity**, verifique se há pelo menos um registro do ActiveSyncDevice ou o teste poderá falhar.



Ferramentas de solução de problemas

Um conjunto de utilitários do PowerShell para solução de problemas está disponível na pasta Support\PowerShell.

Uma ferramenta de solução de problemas executa uma análise profunda das caixas de correio e dispositivos do usuário, detectando condições de erro e possíveis áreas de falha e análise detalhada RBAC de usuários. Pode salvar a saída bruta de todos os cmdlets para um arquivo de texto.

Conector Citrix Gateway para Exchange ActiveSync

January 22, 2021

O XenMobile Citrix ADC Conector é agora o conector Citrix Gateway para Exchange ActiveSync. Para obter mais detalhes sobre o portfólio unificado da Citrix, consulte o [Guia do produto Citrix](#).

O conector para Exchange ActiveSync oferece um serviço de autorização de nível de dispositivo dos clientes ActiveSync para o Citrix ADC agindo como um proxy reverso para o protocolo do Exchange ActiveSync. A autorização é controlada por uma combinação de políticas que você define no XenMobile e por regras definidas localmente pelo conector Citrix Gateway para Exchange ActiveSync.

Para obter mais informações, consulte [ActiveSync Gateway](#).

Para um diagrama da arquitetura de referência detalhada, consulte [Arquitetura](#).

A versão atual do conector do Citrix Gateway para Exchange ActiveSync é a versão 8.5.2.

Novidades

As seções a seguir listam o que há de novo nas versões atuais e anteriores do conector Citrix Gateway para Exchange ActiveSync, anteriormente XenMobile Citrix ADC Connector.

O que há de novo na versão 8.5.3

- Esta versão adiciona suporte aos protocolos ActiveSync 16.0 e 16.1.
- Mais detalhes foram adicionados às análises enviadas ao Google Analytics, especialmente no que diz respeito aos instantâneos. [CXM-52261]

O que há de novo na versão 8.5.2

- O XenMobile Citrix ADC Connector é agora o conector Citrix Gateway para Exchange ActiveSync.

Os seguintes problemas foram corrigidos nesta versão:

- Se mais de um critério for usado na definição de uma regra de política e se um dos critérios envolver o ID do usuário, poderá ocorrer o seguinte problema: se um usuário tiver mais aliases, os aliases também não serão verificados ao aplicar a regra. [CXM-55355]

Nota:

A seção de novidades a seguir se refere ao conector Citrix Gateway para Exchange ActiveSync por seu nome anterior, XenMobile Citrix ADC Connector. O nome foi alterado a partir da versão 8.5.2.

O que há de novo na versão 8.5.1.11

- **Alteração do requisito do sistema:** a versão atual do Citrix ADC Connector requer o Microsoft .NET Framework 4.5.
- **Suporte ao Google Analytics:** queremos saber como você usa o XenMobile Citrix ADC Connector para nos concentrarmos em como podemos melhorar o produto.
- **Suporte para TLS 1.1 e 1.2:** devido ao enfraquecimento da segurança, o TLS 1.0 está sendo substituído pelo PCI Council. O suporte para TLS 1.1 e 1.2 é adicionado ao XenMobile Citrix ADC Connector.

Monitoramento do conector Citrix Gateway para Exchange ActiveSync

O utilitário de configuração do conector Citrix Gateway para Exchange ActiveSync fornece registro detalhado que você pode usar para visualizar todo o tráfego que passa pelo seu Exchange Server que é permitido ou bloqueado pelo Secure Mobile Gateway.

Use a guia **Log** para visualizar o histórico das solicitações do ActiveSync encaminhadas para o conector para Exchange ActiveSync pelo Citrix ADC para autorização.

Além disso, para garantir que o serviço web do conector Citrix Gateway para Exchange ActiveSync esteja em execução, carregue a seguinte URL em um navegador no servidor do conector `https://<host:port>/services/ActiveSync/Version`. Se a URL retornar a versão do produto como uma string, o serviço da Web está responsivo.

Para simular o tráfego do ActiveSync com o conector Citrix Gateway para Exchange ActiveSync

Você pode usar o conector Citrix Gateway para Exchange ActiveSync para simular como o tráfego do ActiveSync se parecerá em conjunto com suas políticas. No utilitário de configuração do conector, selecione a guia **Simulador**. Os resultados mostram como suas políticas serão aplicadas de acordo com as regras que você configurou.

Escolha de filtros para o conector Citrix Gateway para Exchange ActiveSync

Os filtros do conector Citrix Gateway para Exchange ActiveSync funcionam analisando um dispositivo para uma determinada violação de política ou configuração de propriedade. Se o dispositivo atender aos critérios, o dispositivo será colocado em uma Lista de dispositivos. Essa lista de dispositivos não é uma lista permitir ou uma lista de bloqueio. É uma lista de dispositivos que atendem aos critérios definidos. Os filtros a seguir estão disponíveis para o conector no XenMobile. As duas opções para cada filtro são **Permitir** ou **Negar**.

- **Dispositivos anônimos:** permite ou nega dispositivos que estão registrados no XenMobile, mas a identidade do usuário é desconhecida. Por exemplo, poderia ser um usuário que foi registrado, mas de quem a senha do usuário do Active Directory expirou, ou um usuário que foi registrado com credenciais desconhecidas.
- **Falha no atestado Samsung KNOX:** os dispositivos Samsung possuem funcionalidade para segurança e diagnóstico. Este filtro fornece confirmação de que o dispositivo está configurado para o KNOX. Para obter detalhes, consulte [Samsung Knox](#).
- **Aplicativos proibidos:** permite ou nega dispositivos com base na Lista de dispositivos definida pelas políticas de lista de bloqueio e presença de aplicativos bloqueados.
- **Permissão/Negação implícita:** cria uma Lista de dispositivos de todos os dispositivos que não atendem a qualquer um dos outros critérios de regra do filtro e permite ou nega com base nessa

lista. A opção Permissão/negação implícita garante que o status do conector Citrix Gateway para Exchange ActiveSync na guia Dispositivos esteja ativado e mostre o status do conector para seus dispositivos. A opção Permissão/negação implícita também controla todos os outros filtros do conector que não foram selecionados. Por exemplo, o conector nega aplicativos bloqueados e permite todos os outros filtros porque a opção Permitir/Negar implícita está definida como **Permitir**.

- **Dispositivos inativos:** cria uma Lista de dispositivos que não se comunicaram com o XenMobile dentro de um período especificado. Esses dispositivos são considerados inativos. O filtro permite ou nega os dispositivos de acordo.
- **Aplicativos obrigatórios ausentes:** quando um usuário se registra, o usuário recebe uma lista de aplicativos obrigatórios que devem ser instalados. O filtro de aplicativos obrigatórios ausentes indica que um ou mais dos aplicativos não estão mais presentes: por exemplo, o usuário excluiu um ou mais aplicativos.
- **Aplicativos não sugeridos:** quando um usuário se registra, ele recebe uma lista dos aplicativos que deve instalar. O filtro de aplicativos não sugeridos verifica o dispositivo em busca de aplicativos que não estão nessa lista.
- **Senha não compatível:** cria uma lista de todos os dispositivos que não têm um código secreto no dispositivo.
- **Dispositivos sem conformidade:** permite negar ou permitir dispositivos que atendam aos seus próprios critérios internos de conformidade com TI. A conformidade é uma configuração arbitrária definida pela propriedade do dispositivo chamada Sem conformidade, que é um sinalizador booleano que pode ser **True** ou **False**. (Você pode criar esta propriedade manualmente e definir o valor, ou pode usar Ações automatizadas para criar esta propriedade em um dispositivo, se o dispositivo atender ou não atender a critérios específicos.)
 - **Sem conformidade = True.** Se um dispositivo não atende aos padrões de conformidade e definições de políticas definidos pelo seu departamento de TI, o dispositivo está sem conformidade.
 - **Sem conformidade = False.** Se um dispositivo atende aos padrões de conformidade e definições de políticas definidos pelo seu departamento de TI, o dispositivo está em conformidade.
- **Status revogado:** cria uma Lista de todos os dispositivos revogados e permite ou nega com base no status de revogado.
- **Dispositivos Android com root/iOS com jailbreak.** Cria uma Lista de Dispositivos de todos os dispositivos sinalizados como com root e permite ou nega com base no status com root.
- **Dispositivos não gerenciados.** Cria uma lista de dispositivos de todos os dispositivos no banco de dados do XenMobile. O Gateway de aplicativo móvel deve ser implantado em um modo de bloqueio.

Para configurar uma conexão ao conector Citrix Gateway para Exchange ActiveSync

O conector Citrix Gateway para Exchange ActiveSync se comunica com o XenMobile e outros provedores de configuração remota através de serviços do Web Secure.

1. No utilitário de configuração do conector, clique na guia **Provedores de configuração** e, em seguida, clique em **Adicionar**.
2. Na caixa de diálogo **Provedores de configuração**, em **Nome**, digite um nome de usuário que tenha privilégios administrativos e seja usado para autorização HTTP básica com o XenMobile Server.
3. Em **Url**, digite o endereço da Web do XenMobile GCS, geralmente no formato `https://<FQDN>/<instanceName>/services/<MagConfigService>`. O nome *MagConfigService* diferencia maiúsculas de minúsculas.
4. Em **Senha**, digite a senha que será usada para a autorização básica de HTTP com o XenMobile Server.
5. Em **Gerenciamento de host**, insira o nome do servidor do conector.
6. Em **Intervalo de linha de base**, especifique um período de tempo para quando um novo conjunto de regras dinâmicas atualizado é recebido do Device Manager.
7. Em **Intervalo delta**, especifique um período de tempo para quando uma atualização de regras dinâmicas é recebida.
8. Em **Tempo limite de solicitação**, especifique o intervalo de tempo limite de solicitação do servidor.
9. Em **Provedor de configuração**, selecione se a instância do servidor do provedor de configuração fornece a configuração da política.
10. Em **Eventos ativados**, ative esta opção se desejar que o conector notifique o XenMobile quando um dispositivo estiver bloqueado. Essa opção é necessária se você estiver usando as regras do conector em qualquer uma das suas ações automatizadas do XenMobile.
11. Clique em **Salvar** e, em seguida, clique em **Testar a conectividade** para testar a conectividade do provedor de gateway para configuração. Se a conexão falhar, verifique se as configurações do firewall local permitem a conexão, ou entre em contato com o administrador.
12. Quando a conexão for bem-sucedida, desmarque a caixa de seleção **Desativado** e clique em **Salvar**.

Quando você adiciona um novo provedor de configuração, o conector Citrix Gateway para Exchange ActiveSync cria automaticamente uma ou mais políticas associadas ao provedor. Essas políticas são definidas por uma definição de modelo contida em `config\policyTemplates.xml` na seção `NewPolicyTemplate`. Para cada elemento de Política definido nesta seção, uma nova política é criada.

O operador pode adicionar, remover ou modificar elementos da política, se ocorrer o seguinte: o elemento da política está em conformidade com a definição de esquema e as cadeias de caracteres de substituição padrão (colocadas entre chaves) não são modificadas. Em seguida, adicione novos grupos para o provedor e atualize a política para que inclua os novos grupos.

Para importar uma política do XenMobile

1. No utilitário de configuração do conector Citrix Gateway para Exchange ActiveSync, clique na guia **Provedores de configuração** e, em seguida, clique em **Adicionar**.
2. Na caixa de diálogo **Provedores de configuração**, em **Nome**, digite um nome de usuário que será usado para autorização HTTP básica com o XenMobile Server e que tenha privilégios administrativos.
3. Em **URL**, digite o endereço da Web do XenMobile Gateway Configuration Service (GCS), geralmente no formato `https://<xdmHost>/xdm/services/<MagConfigService>`. O nome MagConfigService diferencia maiúsculas de minúsculas.
4. Em **Senha**, digite a senha que será usada para a autorização de HTTP básico com o XenMobile Server.
5. Clique em **Testar a conectividade** para testar a conectividade do provedor de gateway para configuração. Se a conexão falhar, verifique se as configurações do firewall local permitem a conexão, ou entre em contato com o administrador.
6. Quando a conexão for bem-sucedida, desmarque a caixa de seleção **Desativado** e clique em **Salvar**.
7. Em **Gerenciamento de host**, deixe o nome DNS padrão do computador host local. Essa configuração costumava coordenar a comunicação com o XenMobile quando vários servidores do Forefront Threat Management Gateway (TMG) estavam configurados em uma matriz.

Depois de salvar as configurações, abra o GCS.

Configuração do modo de política do conector Citrix Gateway para Exchange ActiveSync

O conector Citrix Gateway para Exchange ActiveSync pode ser executado nos seis modos a seguir:

- **Permitir todos.** Este modo de política concede acesso para todo o tráfego que passa pelo conector. Não são utilizadas outras regras de filtragem.
- **Negar todos.** Este modo de política bloqueia o acesso para todo o tráfego que passa pelo conector. Não são utilizadas outras regras de filtragem.
- **Regras estáticas: modo de Bloqueio.** Esse modo de política executa regras estáticas com uma instrução de negação ou bloqueio implícita no final. O conector bloqueia dispositivos que não são permitidos através de outras regras de filtro.
- **Regras estáticas: modo de Permissão.** Esse modo de política executa regras estáticas com uma instrução de permissão implícita no final. Os dispositivos que não são bloqueados ou negados por outras regras de filtro são permitidos por meio do conector.

- **Regras estáticas + ZDM:** modo de Bloqueio. Esse modo de política executa regras estáticas primeiro, seguido por regras dinâmicas do XenMobile com uma instrução de negação ou bloqueio implícita no final. Os dispositivos são permitidos ou negados com base nos filtros definidos e regras do Device Manager. Os dispositivos que não correspondem a regras e filtros definidos são bloqueados.
- **Regras estáticas + ZDM:** modo de Permissão. Esse modo de política executa regras estáticas primeiro, seguido por regras dinâmicas do XenMobile com uma instrução de permissão implícita no final. Os dispositivos são permitidos ou negados com base nos filtros definidos e regras do XenMobile. Os dispositivos que não correspondem a regras e filtros definidos são permitidos.

O processo do conector Citrix Gateway para Exchange ActiveSync permite ou bloqueia regras dinâmicas com base em IDs ActiveSync exclusivos para dispositivos móveis com iOS e Windows recebidos do XenMobile. Os dispositivos Android diferem no seu comportamento com base no fabricante e alguns não expõem prontamente um ID exclusivo do ActiveSync. Para compensar, o XenMobile envia informações de ID de usuário para dispositivos Android para emitir uma autorização de permissão ou bloqueio. Como resultado, se um usuário tiver apenas um dispositivo Android, as permissões e os bloqueios funcionam normalmente. Se o usuário tiver vários dispositivos Android, todos os dispositivos são permitidos porque os dispositivos Android não podem ser diferenciados. Você pode configurar o gateway para bloquear estaticamente estes dispositivos pelo ActiveSyncID, se eles forem conhecidos. Você também pode configurar o gateway para bloquear com base no tipo de dispositivo ou agente de usuário.

Para especificar o modo de política, no utilitário SMG Controller Configuration, faça o seguinte:

1. Clique na guia **Filtros do caminho** e, em seguida, clique em **Adicionar**.
2. Na caixa de diálogo **Propriedades do caminho**, selecione um modo de política na lista de **Políticas** e clique em **Salvar**.

Você pode revisar as regras na guia **Políticas** do utilitário de configuração. As regras são processadas no conector Citrix Gateway para Exchange ActiveSync de cima para baixo. As políticas Permitir são exibidas com marca de seleção verde. As políticas Negar são exibidas como um círculo vermelho com uma linha através dele. Para atualizar a tela e ver as regras mais atualizadas, clique em **Atualizar**. Você também pode modificar a ordem das regras no arquivo config.xml.

Para testar as regras, clique na guia **Simulador**. Especifique os valores nos campos. Estes também podem ser obtidos a partir dos logs. Uma mensagem de resultado aparecerá especificando Permitir ou Bloquear.

Para configurar regras estáticas

Insira regras estáticas com valores que o filtro ISAPI da solicitação da conexão do ActiveSync HTTP lê. As regras estáticas habilitam o conector Citrix Gateway para Exchange ActiveSync a permitir ou

bloquear o tráfego pelos seguintes critérios:

- **Usuário.** O conector Citrix Gateway para Exchange ActiveSync usa a estrutura de valor e nome de usuário autorizada que foi capturada durante o registro do dispositivo. Isso é comumente encontrado como domínio\nome de usuário como referenciado pelo servidor que executa o XenMobile conectado ao Active Directory via LDAP. A guia **Log** no utilitário de configuração do conector mostra os valores que são passados através do conector. Os valores são passados se a estrutura do valor precisar ser determinada ou se for diferente.
- **Deviceid (ActiveSyncID).** Também conhecido como o ActiveSyncID do dispositivo conectado. Esse valor é comumente encontrado na página Propriedades do dispositivo específico no console XenMobile. Esse valor também pode ser rastreado a partir da guia Log no utilitário de configuração do conector.
- **DeviceType.** O conector pode determinar se um dispositivo é um iPhone, iPad ou outro tipo de dispositivo e pode permitir ou bloquear com base nesse critério. Tal como acontece com outros valores, o utilitário de configuração do conector pode revelar todos os tipos de dispositivos conectados que estão sendo processados para a conexão ActiveSync.
- **UserAgent.** Contém informações sobre o cliente ActiveSync que é usado. Na maioria dos casos, o valor especificado corresponde a uma compilação e versão do sistema operacional específicas para a plataforma do dispositivo móvel.

O utilitário de configuração do conector executado no servidor sempre gerencia as regras estáticas.

1. No utilitário SMG Controller Configuration, clique na guia **Regras estáticas** e clique em **Adicionar**.
2. Na caixa de diálogo **Propriedades da regra estática**, especifique os valores que você deseja usar como critérios. Por exemplo, você pode inserir um usuário para permitir o acesso inserindo o nome do usuário (por exemplo, AllowedUser) e, em seguida, desmarcando a caixa de seleção **Desativado**.
3. Clique em **Salvar**.

A regra estática agora está em vigor. Além disso, você pode usar expressões regulares para definir valores, mas você deve habilitar o modo de processamento de regras no arquivo config.xml.

Para configurar regras dinâmicas

Políticas e propriedades de dispositivo no XenMobile definem regras dinâmicas e podem disparar um filtro dinâmico do conector Citrix Gateway para Exchange ActiveSync. Os disparadores são baseados na presença de uma violação de política ou configuração de propriedade. Os filtros do conector funcionam analisando um dispositivo para uma determinada violação de política ou configuração de propriedade. Se o dispositivo atender aos critérios, o dispositivo será colocado em uma Lista de dispositivos. Essa lista de dispositivos não é uma lista de permissão ou uma lista de bloqueio. Ela é uma

lista de dispositivos que atende aos critérios definidos. As opções de configuração a seguir permitem que você defina se deseja permitir ou negar dispositivos na Lista de dispositivos usando o conector.

Nota:

Você deve usar o console XenMobile para configurar regras dinâmicas.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Settings** é exibida.
2. Em **Servidor**, clique em **ActiveSync Gateway**. A página ActiveSync Gateway é exibida.
3. Em **Ativar as regras a seguir**, selecione uma ou mais regras que você deseja ativar.
4. Em Somente Android, em **Enviar usuários de domínio do Android para o ActiveSync Gateway**, clique em **SIM** para garantir que o XenMobile envie as informações do dispositivo Android para o Secure Mobile Gateway.

Quando essa opção está ativada, o XenMobile envia as informações do dispositivo Android para o conector Citrix Gateway para Exchange ActiveSync caso o XenMobile não tenha o identificador do ActiveSync do usuário do dispositivo Android.

Para configurar políticas personalizadas editando o arquivo XML do conector Citrix Gateway para Exchange ActiveSync

Você pode visualizar as políticas básicas na configuração padrão na guia **Políticas** do utilitário de configuração do conector Citrix Gateway para Exchange ActiveSync. Se você quiser criar políticas personalizadas, você pode editar o arquivo de configuração XML do conector (config\config.xml).

1. Encontre a seção **PolicyList** no arquivo e, em seguida, adicione um novo elemento **Policy**.
2. Se um novo grupo também for necessário, como outro grupo estático ou um grupo para suportar outro GCP, adicione o novo elemento **Group** à seção **GroupList**.
3. Opcionalmente, você pode alterar a ordem dos grupos dentro de uma política existente reorganizando os elementos **GroupRef**.

Configuração do arquivo XML do conector Citrix Gateway para Exchange ActiveSync

O conector Citrix Gateway para Exchange ActiveSync usa um arquivo de configuração XML para ditar as ações do conector. Entre outras entradas, o arquivo especifica os arquivos de grupo e as ações associadas que o filtro leva em consideração ao avaliar solicitações HTTP. Por padrão, o arquivo é chamado config.xml e pode ser encontrado no seguinte local: ..\Program Files\Citrix\XenMobile Citrix ADC Connector\config.

Nós GroupRef

Os nós GroupRef definem os nomes dos grupos lógicos. Os padrões são AllowGroup e DenyGroup.

Nota:

A ordem dos nós GroupRef tal como aparecem no nó GroupRefList é importante.

O valor do ID de um nó GroupRef identifica um contêiner lógico ou uma coleção de membros que são usados para combinar contas ou dispositivos específicos de usuários. Os atributos de ação especificam como o filtro trata um membro que corresponde a uma regra na coleção. Por exemplo, uma conta de usuário ou dispositivo que corresponda a uma regra no conjunto AllowGroup “passará”. Passar significa ter permissão para acessar as autoridades de certificação do Exchange, Exchange CAS. Uma conta de usuário ou dispositivo que corresponde a uma regra no conjunto DenyGroup é “rejeitado”. Rejeitado significa não ter permissão para acessar as autoridades de certificação do Exchange, Exchange CAS.

Quando uma conta de usuário/dispositivo específico ou uma combinação de regras atende a ambos os grupos, uma convenção de precedência é usada para direcionar o resultado da solicitação. A precedência é incorporada na ordem dos nós GroupRef no arquivo config.xml de cima para baixo. Os nós GroupRef são classificados em ordem de prioridade. As regras para uma determinada condição no grupo Allow sempre terão precedência sobre as regras para a mesma condição no grupo Deny.

Nós Group

Além disso, o config.xml define os nós do grupo Group. Esses nós vinculam os contêineres lógicos AllowGroup e DenyGroup aos arquivos XML externos. As entradas armazenadas nos arquivos externos são a base das regras do filtro.

Nota:

Nesta versão, apenas arquivos XML externos são suportados.

A instalação padrão implementa dois arquivos XML na configuração: allow.xml e deny.xml.

Configuração do conector Citrix Gateway para Exchange ActiveSync

Você pode configurar o conector Citrix Gateway para Exchange ActiveSync para seletivamente bloquear ou permitir solicitações do ActiveSync com base nas propriedades a seguir: **ID de serviço do Active Sync**, **Tipo de dispositivo**, **Agente de usuário** (sistema operacional do dispositivo), **Usuário autorizado** e **Comando ActiveSync**.

A configuração padrão suporta uma combinação de grupos estáticos e dinâmicos. Você mantém grupos estáticos usando o utilitário do SMG Controller Configuration. Os grupos estáticos podem consistir em categorias conhecidas de dispositivos, como todos os dispositivos que usam um determinado agente de usuário.

Uma fonte externa chamada Gateway Configuration Provider mantém grupos dinâmicos. O conector Citrix Gateway para Exchange ActiveSync conecta os grupos periodicamente. O XenMobile pode exportar grupos de usuários e dispositivos permitidos e bloqueados para o conector.

Os grupos dinâmicos são mantidos por uma fonte externa chamada Gateway Configuration Provider e coletados pelo conector Citrix Gateway para Exchange ActiveSync periodicamente. O XenMobile pode exportar grupos de usuários e dispositivos permitidos e bloqueados para o conector.

Uma Política é uma lista ordenada de grupos na qual cada grupo tem uma ação associada (permitir ou bloquear) e uma lista de membros do grupo. Uma política pode ter qualquer número de grupos. A ordem do grupo dentro de uma política é importante porque, quando uma correspondência é encontrada, a ação do grupo é realizada e os grupos subsequentes não são avaliados.

Um membro define uma maneira de combinar as propriedades de uma solicitação. Ele pode corresponder a uma única propriedade, como ID de dispositivo, ou a várias propriedades, como o agente de usuário e o tipo de dispositivo.

Escolha de um modelo de segurança para o conector Citrix Gateway para Exchange ActiveSync

Estabelecer um modelo de segurança é essencial para uma implantação bem-sucedida de dispositivos móveis para organizações de qualquer tamanho. É comum usar o controle de rede protegido ou em quarentena para permitir o acesso a um usuário, computador ou dispositivo por padrão. Essa prática nem sempre é ideal. Toda organização que gerencia a segurança de TI pode ter uma abordagem ligeiramente diferente ou adaptada da segurança para dispositivos móveis.

A mesma lógica aplica-se à segurança do dispositivo móvel. O uso de um modelo permissivo é uma escolha fraca devido à infinidade de tipos e dispositivos móveis, dispositivos móveis por usuário e plataformas e aplicativos do sistema operacional disponíveis. Na maioria das organizações, o modelo restritivo será a escolha mais lógica.

Os cenários de configuração que a Citrix permite para integrar o conector Citrix Gateway para Exchange ActiveSync ao XenMobile são os seguintes:

Modelo Permissivo (Modo de Permissão)

O modelo de segurança permissivo opera na premissa de que a tudo é permitido ou concedido acesso por padrão. Apenas por meio de regras e filtragem algo é bloqueado e é aplicada uma restrição. O modelo permissivo de segurança é bom para organizações que têm uma preocupação com a segurança relativamente fraca sobre dispositivos móveis. O modelo só se aplica a controles restritivos para negar o acesso quando apropriado (quando uma regra de política é falha).

Modelo Restritivo (Modo de Bloqueio)

O modelo de segurança restritivo se baseia na premissa de que a nada é permitido ou concedido acesso por padrão. Tudo que passa pelo ponto de verificação de segurança é filtrado e inspecionado, e o acesso é negado a menos que as regras que permitem o acesso sejam aprovadas. O modelo restritivo de segurança é bom para organizações que têm um critério de segurança relativamente rígido sobre dispositivos móveis. O modo somente concede acesso para uso e funcionalidade com os serviços de rede quando todas as regras para permitir o acesso forem aprovadas.

Gerenciamento do conector Citrix Gateway para Exchange ActiveSync

Você pode usar o conector Citrix Gateway para Exchange ActiveSync para criar regras de controle de acesso. As regras permitem ou bloqueiam o acesso a solicitações de conexão do ActiveSync de dispositivos gerenciados. O acesso é baseado no status do dispositivo, listas de permissão ou bloqueio de aplicativos e outras condições de conformidade.

Ao usar o utilitário de configuração do conector Citrix Gateway para Exchange ActiveSync, você pode criar regras dinâmicas e estáticas que impõem as políticas corporativas de e-mail, permitindo que você bloqueie os usuários que estão em violação dos padrões de conformidade. Você também pode configurar criptografia de anexos de e-mail, de modo que todos os anexos que passam pelo seu Exchange Server para dispositivos gerenciados sejam criptografados e apenas visíveis em dispositivos gerenciados por usuários autorizados.

Para desinstalar o conector Citrix Gateway para Exchange ActiveSync

1. Execute XnclnInstaller.exe com uma conta de administrador.
2. Siga as instruções na tela para concluir a desinstalação.

Para instalar, atualizar ou desinstalar o conector Citrix Gateway para Exchange ActiveSync

1. Execute o XnclnInstaller.exe com uma conta de administrador para instalar o conector ou permitir a atualização ou remoção de um conector existente.
2. Siga as instruções na tela para concluir a instalação, atualização ou desinstalação.

Depois de instalar o conector, manualmente reinicie o serviço de configuração do XenMobile e o serviço de notificação.

Instalação do conector Citrix Gateway para Exchange ActiveSync

Você instala o conector Citrix Gateway para Exchange ActiveSync em seu próprio Windows Server.

A carga de CPU que o conector coloca em um servidor depende da quantidade de dispositivos gerenciados. Para um grande número de dispositivos (mais de 50.000), talvez seja necessário fornecer mais

de um núcleo se você não tiver um ambiente em cluster. A espaço de memória do connector não é suficientemente significativo para garantir mais memória.

Requisitos de sistema do conector Citrix Gateway para Exchange ActiveSync

O conector Citrix Gateway para Exchange ActiveSync se comunica com o Citrix ADC sobre uma ponte SSL configurada no dispositivo Citrix ADC. A ponte permite que o dispositivo transmita todo o tráfego seguro diretamente para o XenMobile. O conector requer a seguinte configuração mínima do sistema:

Componente	Requisito
Computador e processador	Processador 733 MHz Pentium III de 733 MHz ou superior. Processador Pentium III de 2.0 GHz ou superior (recomendado)
Citrix ADC	Dispositivo Citrix ADC com software versão 10
Memória	1 GB
Disco rígido	Partição local formatada em NTFS com 150 MB de espaço disponível no disco rígido
Sistema operacional	Windows Server 2016, Windows Server 2012 R2 ou Windows Server 2008 R2 Service Pack 1. Deve ser um servidor com base no inglês. O suporte para Windows Server 2008 R2 Service Pack 1 termina em 14 de janeiro de 2020.
Outros dispositivos	Adaptador de rede compatível com o sistema operacional host para comunicação com a rede interna
Microsoft .NET Framework	A versão 8.5.1.11 requer o Microsoft .NET Framework 4.5.
Tela	Monitor VGA ou resolução superior

O computador host para o conector Citrix Gateway para Exchange ActiveSync requer o espaço em disco mínimo disponível seguinte:

- **Aplicativo:** 10–15 MB (recomendado 100 MB)
- **Registro em log:** 1 GB (recomendado 20 GB)

Para obter informações sobre o suporte de plataforma para o conector Citrix Gateway para Exchange ActiveSync, consulte [Sistemas operacionais compatíveis de dispositivos](#).

Os clientes de email do dispositivo

Nem todos os clientes de email sempre retornam a mesma ID do ActiveSync para um dispositivo. Como o conector Citrix Gateway para Exchange ActiveSync espera uma ID exclusiva do ActiveSync para cada dispositivo, aplica-se o seguinte: apenas os clientes de email que consistentemente geram a mesma ID exclusiva do ActiveSync para cada dispositivo são suportados. A Citrix testou esses clientes de email e os clientes foram executados sem erros:

- Cliente de email nativo Samsung
- Cliente de email nativo iOS

Implantação do conector Citrix Gateway para Exchange ActiveSync

O conector Citrix Gateway para Exchange ActiveSync permite que você use Citrix ADC para proxy e balanceamento de carga de comunicação do XenMobile Server com dispositivos gerenciados XenMobile. O conector se comunica periodicamente com o XenMobile para sincronizar as políticas. O conector e o XenMobile podem ser agrupados, em conjunto ou independentemente, e podem ter a carga balanceada pelo Citrix ADC.

Componentes do conector Citrix Gateway para Exchange ActiveSync

- **Serviço do conector Citrix Gateway para Exchange ActiveSync:** este serviço fornece uma interface de serviço web REST que pode ser invocada pelo Citrix ADC para determinar se uma solicitação do ActiveSync de um dispositivo está autorizada.
- **Serviço de configuração do XenMobile:** este serviço se comunica com o XenMobile para sincronizar as alterações de política do XenMobile com o conector.
- **Serviço de notificação do XenMobile:** este serviço envia notificações de acesso a dispositivo não autorizado para o XenMobile. Desta forma, o XenMobile pode tomar as medidas apropriadas, como notificar o usuário por que o dispositivo foi bloqueado.
- **Utilitário de configuração do conector Citrix Gateway para Exchange ActiveSync:** este aplicativo permite ao administrador configurar e monitorar o conector.

Para configurar endereços de escuta para o conector Citrix Gateway para Exchange ActiveSync

Para o conector Citrix Gateway para Exchange ActiveSync receber solicitações do Citrix ADC para autorizar o tráfego do ActiveSync, faça como a seguir. Especifique a porta em que o conector Citrix Gateway para Exchange ActiveSync escuta as chamadas de serviço da web do Citrix ADC.

1. No menu **Iniciar**, selecione o utilitário de configuração do conector Citrix Gateway para Exchange ActiveSync.
2. Clique na guia **Serviços da Web** e, em seguida, digite os endereços de escuta para o serviço da web do conector Citrix Gateway para Exchange ActiveSync. Você pode selecionar **HTTP** ou

HTTPS ou ambos. Se o conector for co-residente com o XenMobile (instalado no mesmo servidor), selecione valores de porta que não entrem em conflito com o XenMobile.

3. Depois que os valores forem configurados, clique em **Salvar** e, em seguida, clique em **Iniciar serviço** para iniciar o serviço da web.

Para configurar políticas de controle de acesso para dispositivos no conector Citrix Gateway para Exchange ActiveSync

Para configurar a política de controle de acesso que deseja aplicar aos seus dispositivos gerenciados, faça o seguinte:

1. No utilitário de configuração do conector Citrix Gateway para Exchange ActiveSync, clique na guia **Filtros do caminho**.
2. Selecione a primeira linha, **Microsoft-Server-ActiveSync é para o ActiveSync** e, em seguida, clique em **Editar**.
3. Na lista **Política**, selecione a política desejada. Para uma política que inclua as políticas do XenMobile, selecione **Estática + ZDM: modo de Permissão ou Estática + ZDM: modo de Bloqueio**. Essas políticas combinam regras locais (ou estáticas) com as regras do XenMobile. Modo de permissão significa que todos os dispositivos que não são explicitamente identificados pelas regras têm acesso autorizado ao ActiveSync. Modo de bloqueio significa que esses dispositivos são bloqueados.
4. Depois de configurar as políticas, clique em **Salvar**.

Para configurar a comunicação com o XenMobile

Especifique o nome e as propriedades do XenMobile Server (também conhecido como Config Provider) que você deseja usar com o conector Citrix Gateway para Exchange ActiveSync e o Citrix ADC.

Nota:

Essa tarefa pressupõe que você já instalou e configurou o XenMobile.

1. No utilitário de configuração do conector Citrix Gateway para Exchange ActiveSync, clique na guia **Provedores de configuração** e, em seguida, clique em **Adicionar**.
2. Digite o nome e a URL do XenMobile Server que você está usando nessa implantação. Se você tiver vários XenMobile Servers implantados em uma implantação multilocatário, esse nome deve ser exclusivo para cada instância do servidor. Por exemplo, para **Nome**, você pode digitar **XMS**.
3. Em **Url**, digite o endereço da Web do XenMobile GlobalConfig Provider (GCP), geralmente no formato `https://<FQDN>/<instanceName>/services/<MagConfigService>`. O nome *MagConfigService* diferencia maiúsculas de minúsculas.

4. Em **Senha**, digite a senha que será usada para a autorização básica de HTTP com o XenMobile Server.
5. Em **Gerenciamento de host**, digite o nome do servidor em que você instalou o conector do Citrix Gateway para Exchange ActiveSync.
6. Em **Intervalo de linha de base**, especifique um período de tempo para quando um novo conjunto de regras dinâmicas atualizado é recebido do XenMobile.
7. Em **Tempo limite de solicitação**, especifique o intervalo de tempo limite de solicitação do servidor.
8. Em **Provedor de configuração**, selecione se a instância do servidor do provedor de configuração fornece a configuração da política.
9. Em **Eventos ativados**, ative esta opção se desejar que o Secure Mobile Gateway notifique o XenMobile quando um dispositivo estiver bloqueado. Esta opção é necessária se você estiver usando as regras do Secure Mobile Gateway em qualquer uma das Ações Automatizadas do Device Manager.
10. Depois de configurar o servidor, clique em **Testar Conectividade** para testar a conexão com o XenMobile.
11. Quando a conectividade for estabelecida, clique em **Salvar**.

Implantação do conector Citrix Gateway para Exchange ActiveSync para redundância e escalabilidade

Se deseja dimensionar sua implantação do conector Citrix Gateway para Exchange ActiveSync e do XenMobile, você pode instalar instâncias do conector em vários Windows Servers, todas apontando para a mesma instância XenMobile e, em seguida, usar o Citrix ADC para balancear a carga dos servidores.

Existem dois modos de configuração do conector Citrix Gateway para Exchange ActiveSync:

- No modo não compartilhado, cada instância do conector Citrix Gateway para Exchange ActiveSync se comunica com um XenMobile Server e mantém sua própria cópia privada da política resultante. Por exemplo, se você tiver um cluster de XenMobile Servers, poderá executar uma instância do conector em cada XenMobile Server e o conector obterá as políticas da instância do XenMobile local.
- No modo compartilhado, um nó do conector é designado como o nó primário e ele se comunica com o XenMobile. A configuração resultante é compartilhada entre os outros nós, seja por um compartilhamento de rede do Windows ou pela replicação do Windows (ou de terceiros).

Toda a configuração do conector está em uma única pasta (que consiste em alguns arquivos XML). O processo do conector detecta as alterações aos arquivos nesta pasta e recarrega automaticamente a configuração. Não há failover para o nó primário no modo compartilhado. Mas o sistema pode tolerar que o servidor primário fique desativado por alguns minutos (por exemplo, para reiniciar) porque a última configuração boa conhecida é armazenada em cache no processo do conector.

Conceitos avançados

May 24, 2019

Nota:

Este artigo aborda conceitos avançados para o XenMobile Server. Para obter informações avançadas sobre o Endpoint Management, consulte [Conceitos avançados](#).

Os artigos XenMobile Advanced Concepts oferecem um mergulho mais profundo na documentação do produto XenMobile. O objetivo é ajudar a reduzir o tempo de implantação por meio de técnicas especializadas. Os artigos podem citar o especialista técnico ou especialistas que criaram o conteúdo.

Para recomendações, perguntas comuns e casos de uso para o seu ambiente XenMobile de ponta a ponta, consulte o Manual de implantação do XenMobile nesta seção.

Para fóruns de suporte de comunidade no XenMobile, consulte [Citrix Discussions](#).

Interação do XenMobile no local com o Active Directory

April 23, 2020

Contribuição de Siddartha Vuppala

Este artigo explica a interação entre o servidor XenMobile e do Active Directory. O XenMobile Server interage com o Active Directory em linha e em segundo plano. As seções a seguir fornecem mais informações sobre operações em linha e em segundo plano que envolvem a interação do Active Directory.

Nota:

Este artigo é uma visão geral da interação e não abrange os detalhes. Para obter mais informações sobre como configurar o Active Directory e LDAP no console XenMobile, consulte [Configure autenticação de domínio ou de domínio de segurança](#).

Interações em linha

O XenMobile Server se comunica com o Active Directory usando as configurações de LDAP que um administrador configura. As configurações recuperam informações sobre os usuários e grupos. A seguir estão as operações que resultam em interação entre o XenMobile Server e o Active Directory.

1. **Configuração de LDAP.** A configuração do Active Directory em si resulta em uma interação com o Active Directory. XenMobile Server attempts to validate the information by authenticating the

information with Active Directory. O servidor faz isso por meio do protocolo internet, porta e credenciais de conta de serviço fornecidas. Uma associação bem-sucedida indica que a conexão está configurada corretamente.

2. Interações baseadas em grupo.

- a) Pesquisar um ou mais grupos durante o Controle de Acesso Baseado em Função (RBAC) e criação de definição de grupo de entrega. O administrador do servidor XenMobile insere uma cadeia de caracteres de texto de pesquisa no console XenMobile. O XenMobile Server pesquisa no domínio selecionado todos os grupos que contêm a subcadeia de caracteres que é fornecida. Em seguida, do servidor XenMobile recupera o objectGUID, sAMAccountName e atributos de nome distinto dos grupos identificados na pesquisa.

Nota:

Essas informações não são armazenadas no banco de dados do XenMobile Server.

- b) Adição ou atualização de RBAC ou de definição de grupo de implantação. O administrador do XenMobile Server seleciona grupos de interesse do Active Directory com base na pesquisa anterior e os inclui na definição de grupo de implantação. XenMobile Server searches for the specific group, one at a time, in Active Directory. XenMobile Server searches for the objectGUID attribute and retrieves selected attributes, including membership information. As informações de associação de grupo ajudam a determinar a associação entre o grupo recuperado e usuários ou grupos existentes no banco de dados do XenMobile Server. Alterações de associação de grupo resultam em RBAC e derivação de grupo de implantação para os membros de usuário afetados, o que resulta em direitos de usuário.

Nota:

As alterações na definição de grupo de implantação podem levar a alteração em direitos de aplicativos e política para usuários atingidos.

- c) **Convites de PIN de uso único (OTP).** O administrador do XenMobile Server seleciona um grupo da lista de grupos do Active Directory presentes no banco de dados do XenMobile Server. Para este grupo, todos os usuários, diretos e indiretos, são recuperados do Active Directory. Convites de OTP são enviadas para os usuários que foram identificados na etapa anterior.

Nota:

As três interações anteriores implicam que interações baseadas em grupo devem ser acionadas com base nas alterações de configuração do XenMobile Server. Quando não há nenhuma alteração de configuração, as interações implicam que não há nenhuma interações com o Active Directory. Elas também implicam que não há nenhum

requisito para os trabalhos de segundo plano para capturar do lado do grupo de alterações periodicamente.

3. Interação com base no usuário.

- a) Autenticação do usuário. O fluxo de trabalho de autenticação de usuário resulta em duas interações com o Active Directory:
- Usado para autenticar o usuário com as credenciais fornecidas.
 - Adicionar ou atualizar atributos de usuário selecionados no banco de dados do XenMobile Server, incluindo objectGUID, nome diferenciado, sAMAccountName e direta filiação a grupos. Alterações à filiação ao grupo resultam na nova avaliação do aplicativo, políticas e direitos de acesso.

O usuário pode autenticar com o dispositivo ou no console do XenMobile Server. Em ambos os cenários a interação com o Active Directory segue o mesmo comportamento.

- b) Acesso e atualização do App Store. Uma atualização da loja resulta em uma atualização de atributos do usuário, incluindo associações de grupo diretas. Esta ação permite uma nova avaliação de direitos de usuário.
- c) Check-ins do dispositivo. Os administradores podem configurar no console XenMobile check-ins do dispositivo periodicamente. Toda vez que um dispositivo faz check-in, os atributos de usuário correspondentes são atualizados, incluindo associações de grupo diretas. Esses check-ins permitem uma nova avaliação dos direitos de usuário.
- d) Convites de OTP por grupo. O administrador do XenMobile Server seleciona um grupo da lista de grupos do Active Directory presentes no banco de dados do XenMobile Server. Membros de usuário, diretos e indiretos (por causa de aninhamento), são recuperados do Active Directory e salvos no banco de dados do XenMobile Server. Convites de OTP são enviados para os membros do usuário que foram identificados na etapa anterior.
- e) Convites de OTP por usuário. O administrador do XenMobile Server insere uma cadeia de caracteres de texto de pesquisa dentro do console XenMobile. O XenMobile Server consulta o Active Directory e retorna os registros de usuário que correspondem à cadeia de caracteres de texto de entrada. O administrador seleciona, em seguida, o usuário para enviar o convite OTP. O XenMobile Server recupera os detalhes do usuário do Active Directory e atualiza os mesmos detalhes no banco de dados antes de enviar o convite para o usuário.

Interações de segundo plano

Uma conclusão da comunicação em linha com o Active Directory é que interações baseadas em grupo são acionadas depois de alterações de seleção para a configuração do XenMobile Server. Quando não

há nenhuma alteração de configuração, isso implica que não há interações com o Active Directory para grupos.

Essa interação requer trabalhos em segundo plano que periodicamente sincronizam com o Active Directory e as alterações relevantes de atualização para os grupos interessados.

A seguir estão os trabalhos de plano de fundo que interagem com o Active Directory.

1. **Trabalho de sincronização de grupo.** O objetivo deste trabalho é consultar o Active Directory, um grupo por vez, em grupos interessados quanto a alterações do nome distinto ou atributos sAMAccountName. A solicitação de pesquisa para o Active Directory usa o objectGUID do grupo de interessados para obter os valores atuais do nome diferenciado e atributos sAMAccountName. As alterações no nome distinto ou valores de sAMAccountName para grupos interessados são atualizadas para o banco de dados.

Nota:

Esta tarefa não atualiza o usuário às informações de associação ao grupo.

2. **Trabalho de sincronização de grupo aninhado.** Esse trabalho atualiza as alterações na hierarquia de aninhamento de grupos interessados. O XenMobile Server permite diretos e indiretos membros de um grupo interessado para obter direitos. A associação direta dos usuários é atualizada durante interações de usuário incorporadas. Sendo executado em segundo plano, esse trabalho controla associações indiretas. Associações indiretas ocorrem quando um usuário é um membro de um grupo que é um membro de um grupo interessado.

Este trabalho reúne a lista de grupos do Active Directory do banco de dados do XenMobile Server. Esses grupos fazem parte do grupo de implantação ou a definição de RBAC. Para cada grupo na lista, o XenMobile Server obtém os membros do grupo. Membros de um grupo são uma lista de nomes distintos que representam os usuários e grupos. O XenMobile Server faz outra consulta ao Active Directory para obter somente os membros de usuário do grupo interessado. A diferença entre as duas listas oferece somente os membros do grupo para o grupo interessado. As alterações em grupos membros são atualizadas no banco de dados. O mesmo processo é repetido para todos os grupos na hierarquia.

As alterações de aninhamento resulta no processamento de usuários afetados quanto a alterações de direito.

3. **Verificação de usuário desativado.** Esta tarefa é executada somente quando o administrador do XenMobile cria uma ação de verificação de usuários desativados. O trabalho é executado dentro do escopo de um trabalho de sincronização de grupo. O trabalho consulta o Active Directory para verificar o status de desativado de usuários interessados, um usuário por vez.

Perguntas frequentes

O que é a frequência padrão da execução de tarefas em segundo plano?

- Trabalhos de sincronização de grupo executado a cada cinco horas, começando às 02:00h no horário local.
- Os trabalhos de sincronização de grupo aninhado são executados uma vez por dia às meia-noite, horário local.

Por que é necessário um trabalho de sincronização de grupo?

- O atributo `memberOf` de um registro de usuário no Active Directory fornece a lista de grupos, da qual o usuário é um membro direto. Se um grupo se move de uma unidade Organizacional para outra, o atributo `memberOf` reflete o valor mais recente do nome distinto. O banco de dados do XenMobile Server também tem o valor mais recente atualizado. Qualquer discrepância entre os nomes distintos do grupo pode resultar na perda de acesso ao grupo de implantação por parte do usuário. O usuário também pode perder os aplicativos e políticas associadas a esse grupo de implantação.
- O trabalho em segundo plano mantém o atributo de nome distinto grupo atualizado no banco de dados do XenMobile Server para garantir que os usuários tenham acesso a seus direitos.
- Os trabalhos de sincronização estão programados para cada cinco horas porque se presume que as alterações de grupo do Active Directory são incomuns.

Um trabalho de sincronização de grupo pode ser desativado?

- Você pode desativar trabalhos quando sabe que grupos interessados não mudam de uma unidade Organizacional para outra.

Por que é necessário um trabalho de segundo plano de processamento de grupo aninhado?

- As alterações de aninhamento de grupos do Active Directory não são uma ocorrência diária. Alterações à hierarquia de aninhamento de grupos interessados resultam em alterações direitos dos usuários afetados. Quando um grupo é adicionado à hierarquia, seus usuários membros passam a ter o direito às respectivas funções. Quando um grupo sai do aninhamento, os usuários membros do grupo podem perder o acesso aos direitos baseados em função.
- As alterações de aninhamento não são capturadas durante a atualização do usuário. Como as alterações de aninhamento não podem ser sob demanda, as alterações são capturadas por meio de um trabalho em segundo plano.
- As alterações de aninhamento são consideradas incomuns e, portanto, o trabalho em segundo plano executa uma vez por dia para verificar se existem alterações.

Um trabalho de processamento de grupo aninhado pode ser desativado?

- Você pode desativar trabalhos quando sabe alterações de aninhamento não ocorrem em grupos interessados.

Implantação do XenMobile

November 30, 2020

Há muito a considerar quando você está planejando uma implantação do XenMobile.

- Quais dispositivos escolher?
- Como gerenciar os dispositivos?
- Como garantir que sua rede permaneça segura e ainda ofereça uma ótima experiência ao usuário?
- Qual hardware você precisa e como solucionar possíveis problemas?

Os artigos desta seção visam ajudar a responder a tais perguntas. Ele incluem casos de uso e recomendações sobre tópicos que abrangem considerações de implantação.

Tenha em mente que uma diretriz ou recomendação pode não se aplicar a todos os ambientes ou casos de uso. Certifique-se de configurar um ambiente de teste antes de iniciar a implantação do XenMobile.

Os artigos desta seção abrangem estas áreas:

- **Avaliar:** Casos de uso comuns e perguntas a serem consideradas ao planejar sua implantação.
- **Projetar e configurar:** Recomendações para projetar e configurar seu ambiente
- **Operar e monitorar:** Garantia do bom funcionamento do ambiente de execução.

Avaliar

Como em qualquer implantação, avaliar suas necessidades é a principal prioridade. Qual é a sua principal necessidade para o XenMobile? Você precisa gerenciar todos os dispositivos em seu ambiente ou apenas os aplicativos? Talvez você precise gerenciar os dois. Qual o nível de segurança que você precisa que seu ambiente XenMobile tenha? Vejamos alguns casos de uso comuns e perguntas a serem consideradas ao planejar sua implantação.

- [Modos de gerenciamento](#)
- [Requisitos de dispositivo](#)
- [Segurança e experiência do usuário](#)
- [Aplicativos](#)
- [Comunidades do usuário](#)
- [Estratégia de email](#)
- [Integração do XenMobile](#)
- [Requisitos para vários locais](#)

Projetar e configurar

Depois de concluir a avaliação de suas necessidades de implantação, você pode determinar o projeto e a configuração de seu ambiente. Algumas coisas que você precisa planejar:

- Escolher o hardware para o servidor
- Configurar políticas para aplicativos e dispositivos
- Ter os usuários cadastrados

Esta seção inclui casos de uso e recomendações para cada um desses cenários e muito mais.

- [Integração com Citrix ADC e Citrix Gateway](#)
- [Considerações sobre SSO e proxy para aplicativos MDX](#)
- [Autenticação](#)
- [Arquitetura de referência para implantações locais](#)
- [Propriedades do servidor](#)
- [Políticas de dispositivos e aplicativos](#)
- [Opções de registro do usuário](#)
- [Ajuste das operações do XenMobile](#)

Operar e monitorar

Depois que o ambiente do XenMobile estiver em funcionamento, você deverá monitorá-lo para garantir uma operação contínua. A seção de monitoramento discute onde você pode encontrar os vários logs e mensagens que o XenMobile e seus componentes geram, e como ler esses logs. Esta seção também inclui várias etapas comuns de solução de problemas que você pode seguir para reduzir o tempo de feedback do atendimento ao cliente.

- [Provisionamento e desprovisionamento de aplicativos](#)
- [Operações baseadas em painel](#)
- [Controle de Acesso baseado em função e suporte ao XenMobile](#)
- [Monitoramento de sistemas](#)
- [Recuperação de desastres](#)
- [Processo de suporte Citrix](#)

Modos de gerenciamento

April 8, 2021

Para cada instância do XenMobile (um único servidor ou um cluster de nós), você pode escolher se deseja gerenciar dispositivos, aplicativos ou ambos. O XenMobile usa os seguintes termos para os modos de gerenciamento de dispositivos e aplicativos:

- Modo de gerenciamento de dispositivo móvel (modo MDM)
- Modo de gerenciamento de aplicativo móvel (modo MAM)
- Modo MDM+MAM (modo Empresarial)

Gerenciamento de dispositivo móvel (modo MDM)

Importante:

Se você configurar o modo MDM e depois mudar para o modo ENT, certifique-se de usar a mesma autenticação (Active Directory). O XenMobile não dá suporte à alteração para o modo de autenticação após o registro de usuário. Para obter mais informações, consulte [Atualização](#).

Com o MDM, você pode configurar, proteger e dar suporte a dispositivos móveis. O MDM permite proteger dispositivos e dados em dispositivos no nível do sistema. Você pode configurar políticas, ações e funções de segurança. Por exemplo, você pode apagar um dispositivo seletivamente se o dispositivo for perdido, roubado ou estiver fora de conformidade. Embora o gerenciamento de aplicativos não esteja disponível no modo MDM, você pode entregar aplicativos móveis, como da loja de aplicativos pública e aplicativos corporativos, nesse modo. A seguir se encontram casos de uso comuns do modo MDM:

- O MDM é uma consideração para dispositivos de propriedade corporativa em que são necessárias políticas ou restrições de gerenciamento no nível do dispositivo, como apagamento completo, apagamento seletivo ou localização geográfica.
- Quando os clientes exigem o gerenciamento de um dispositivo real, mas não exigem políticas MDX, como containerização de aplicativos, controles no compartilhamento de dados de aplicativos ou micro VPN.
- Quando os usuários só precisam de e-mails entregues a seus clientes de email nativos em seus dispositivos móveis, e o Exchange ActiveSync ou o Servidor de Acesso para Cliente já é acessível externamente. Nesse caso de uso, você pode usar o MDM para configurar a entrega de emails.
- Quando você implanta aplicativos corporativos nativos (não MDX), aplicativos de loja de aplicativos pública ou aplicativos MDX entregues de lojas públicas. Considere que uma solução MDM sozinha não pode impedir o vazamento de dados de informações confidenciais entre aplicativos no dispositivo. O vazamento de dados pode ocorrer com operações de copiar e colar ou Salvar Como nos aplicativos do Office 365.

Gerenciamento de aplicativo móvel (modo MAM)

O MAM protege os dados do aplicativo e permite controlar o compartilhamento de dados de aplicativo. O MAM também permite o gerenciamento de dados e recursos corporativos, separadamente dos dados pessoais. Com o XenMobile configurado para o modo MAM, você pode usar aplicativos móveis habilitados para MDX para fornecer containerização e controle por aplicativo. O termo modo

MAM também é chamado de modo somente MAM. Este termo distingue este modo de um modo MAM legado.

Aproveitando as políticas MDX, o XenMobile fornece controle em nível de aplicativo sobre o acesso à rede (como micro VPN), interação com aplicativos e dispositivos, criptografia de dados e acesso a aplicativos.

O MAM geralmente é adequado para dispositivos BYO (traga o seu próprio) porque, embora o dispositivo não seja gerenciado, os dados corporativos permanecem protegidos. O MDX tem muitas políticas somente MAM que não exigem um controle MDM.

O MAM também suporta os aplicativos móveis de produtividade. Esse suporte inclui entrega segura de e-mails para o Citrix Secure Mail, compartilhamento de dados entre aplicativos móveis de produtividade protegidos e armazenamento seguro de dados no Citrix Files. Para obter detalhes, consulte [aplicativos móveis de produtividade](#).

O MAM é geralmente adequado para os exemplos a seguir:

- Você entrega aplicativos móveis, como aplicativos MDX, gerenciados no nível do aplicativo.
- Você não é obrigado a gerenciar dispositivos no nível do sistema.

MDM+MAM (modo Empresarial)

O MDM+MAM é um modo híbrido, também chamado de Modo Empresarial, que habilita todos os conjuntos de recursos disponíveis na solução XenMobile Enterprise Mobility Management (EMM). A configuração do XenMobile com o modo MDM+MAM habilita os recursos do MDM e do MAM.

O XenMobile permite especificar se os usuários podem optar por desativar o gerenciamento de dispositivos ou se você precisa do gerenciamento de dispositivos. Essa flexibilidade é útil para ambientes que incluem uma mistura de casos de uso. Esses ambientes podem ou não exigir o gerenciamento de um dispositivo por meio de políticas do MDM para acessar seus recursos do MAM.

O MDM+MAM é adequado para os exemplos a seguir:

- Você tem um único caso de uso no qual o MDM e o MAM são necessários. O MDM é necessário para acessar seus recursos do MAM.
- Alguns casos de uso exigem MDM, enquanto outros não.
- Alguns casos de uso exigem o MAM, enquanto outros não.

Você especifica o modo de gerenciamento do XenMobile Server por meio da propriedade Modo do Servidor. Você define a configuração no console XenMobile. O modo pode ser MDM, MAM ou ENT (para MDM+MAM).

A edição XenMobile para a qual você possui uma licença determina os modos de gerenciamento e outros recursos disponíveis, conforme mostrado na tabela a seguir.

XenMobile MDM Edition	XenMobile Advanced Edition	XenMobile Enterprise Edition
Recursos do MDM	Recursos do MDM	Recursos do MDM
-	Recursos do MAM	Recursos do MAM
-	MDX Toolkit	MDX Toolkit
Secure Hub	Secure Hub	Secure Hub
-	Secure Mail	Secure Mail
-	Secure Web	Secure Web
QuickEdit	QuickEdit	QuickEdit
-	-	ShareConnect
-	-	Citrix Files

Modos de gerenciamento e perfis de registro

Os modos de gerenciamento e os perfis de registro funcionam juntos. Você usa um perfil de registro para configurar as opções de registro de gerenciamento de aplicativo e gerenciamento de dispositivo para dispositivos Android e iOS. Para Android, as opções de registro disponíveis para o modo de servidor MDM+MAM diferem das opções para o modo MDM. Para obter mais informações, consulte [Perfis de registro](#).

Gerenciamento de dispositivos e registro do MDM

Um ambiente XenMobile Enterprise pode incluir uma mistura de casos de uso, alguns dos quais exigem gerenciamento de dispositivos por meio de políticas do MDM para permitir acesso a recursos do MAM. Antes de implantar aplicativos móveis de produtividade para os usuários, avalie completamente os casos de uso e decida se exigem o registro no MDM. Se posteriormente você decidir alterar o requisito de registro no MDM, é provável que os usuários tenham que registrar seus dispositivos novamente.

Nota:

Para especificar se é preciso ou não que os usuários se registrem no MDM, use a propriedade do XenMobile Server **Inscrição obrigatória** no console XenMobile (**Configurações > Propriedades do servidor**). Essa propriedade de servidor global se aplica a todos os usuários e dispositivos da instância do XenMobile. A propriedade se aplica somente quando o Modo do XenMobile Server

é ENT.

A seguir, você encontra um resumo das vantagens e desvantagens (juntamente com as atenuações) de exigir o registro do MDM em uma implantação do modo XenMobile Enterprise.

Quando o registro no MDM é opcional

Vantagens:

- Os usuários podem acessar os recursos do MAM sem colocar seus dispositivos sob o gerenciamento do MDM. Esta opção pode aumentar a adoção do usuário.
- Capacidade acessar os recursos do MAM com segurança para proteger dados corporativos.
- Políticas de MDX, como **Código secreto de aplicativo**, podem controlar o acesso a aplicativos para cada aplicativo MDX.
- Configurar o tempo de espera do Citrix ADC, do XenMobile Server e por aplicativo, juntamente com o Citrix PIN, fornece uma camada extra de proteção.
- Embora as ações do MDM não se apliquem ao dispositivo, algumas políticas de MDX estão disponíveis para negar o acesso ao MAM. A negação seria baseada nas configurações do sistema, como dispositivos com jailbreak ou root.
- Os usuários podem optar por registrar seus dispositivos no MDM durante o primeiro uso.

Desvantagens:

- Os recursos do MAM estão disponíveis para dispositivos não registrados no MDM.
- As políticas e ações do MDM estão disponíveis apenas para dispositivos registrados no MDM.

Opções de atenuação:

- Solicite que os usuários concordem com os termos e condições da empresa e se responsabilizem caso decidam não atender à conformidade. Solicite que os administradores monitorem dispositivos não gerenciados.
- Gerencie o acesso e a segurança do aplicativo usando timers de aplicativos. Valores de tempo limite reduzidos aumentam a segurança, mas podem afetar a experiência do usuário.
- Um segundo ambiente XenMobile com registro no MDM é uma opção. Ao considerar essa opção, tenha em mente a sobrecarga de gerenciar dois ambientes e os recursos adicionais necessários.

Quando o registro no MDM é necessário

Vantagens:

- Capacidade de restringir o acesso a recursos do MAM apenas de dispositivos gerenciados pelo MDM.
- As políticas e ações do MDM podem ser aplicadas a todos os dispositivos no ambiente, conforme desejado.

- Os usuários não podem desativar o registro do dispositivo.

Desvantagens:

- Requer que todos os usuários se registrem no MDM.
- Pode diminuir a adoção por usuários que se opõem ao gerenciamento corporativo de seus dispositivos pessoais.

Opções de atenuação:

- Informe os usuários sobre o que o XenMobile realmente gerencia em seus dispositivos e quais informações os administradores podem acessar.
- Você pode usar um segundo ambiente XenMobile, com um modo de servidor de MAM (também chamado de modo somente MAM), para dispositivos que não precisam de gerenciamento do MDM. Ao considerar essa opção, tenha em mente a sobrecarga de gerenciar dois ambientes e os recursos adicionais necessários.

Sobre os modos MAM e MAM Legado

O XenMobile 10.3.5 introduziu um novo modo de servidor Somente MAM. Para distinguir os modos MAM anterior e novo, a documentação usa estes termos. O novo modo é chamado Somente MAM ou MA, o modo MAM anterior é chamado de modo MAM Legado.

O modo somente MAM estará em vigor quando a propriedade Modo de Servidor do XenMobile for MAM. Os dispositivos se registram no modo MAM.

A funcionalidade do MAM legado estará em vigor quando a propriedade Modo de Servidor do XenMobile for ENT e os usuários recusarem o gerenciamento de dispositivo. Nesse caso, os dispositivos se registram no modo MAM. Os usuários que optam pelo gerenciamento do MDM continuam recebendo a funcionalidade do MAM Legado.

Nota:

Anteriormente, definir a propriedade Modo de Servidor como MAM tinha o mesmo efeito que defini-la como ENT: os usuários que recusavam o gerenciamento MDM recebiam a funcionalidade do MAM legado.

A seguinte tabela resume a configuração do Modo de Servidor a ser usada para um tipo específico de licença e o modo de dispositivo desejado:

Suas licenças são desta edição	Você deseja que os dispositivos se registrem neste modo	Defina a propriedade Modo de Servidor como
---------------------------------------	--	---

Enterprise/Advanced/MDM	Modo MDM	MDM
Enterprise/Advanced	Modo MAM (também chamado de modo somente MAM)	MAM
Enterprise/Advanced	Modo MDM+MAM	ENT (Os usuários que recusam o gerenciamento de dispositivo operam sob o modo MAM legado.)

O modo somente MAM suporta os seguintes recursos anteriormente disponíveis apenas para ENT. Esses recursos não estão disponíveis para o Windows Phone.

- **Autenticação baseada em certificado:** o modo somente MAM oferece suporte à autenticação baseada em certificado. Os usuários terão acesso contínuo aos aplicativos mesmo quando a senha do Active Directory expirar. Se você usa autenticação baseada em certificado para dispositivos MAM, você deve configurar seu Citrix Gateway. Por padrão, nas **Configurações do XenMobile > Citrix Gateway**, Entregar certificado de usuário para autenticação está **Desativado**, o que significa que a autenticação de nome e senha de usuário é usada. Altere essa configuração para **Ativado** para ativar a autenticação de certificado.
- **Portal de Autoajuda:** para permitir que os usuários executem suas próprias operações de bloqueio de aplicativo e apagamento de aplicativo. Essas ações se aplicam a todos os aplicativos no dispositivo. Você pode configurar as ações Bloqueio de aplicativo e Apagamento de aplicativos em **Configurar > Ações**.
- **Todos os modos de segurança de registro:** incluindo Alta Segurança, URL de Convite e Dois Fatores, configurados por meio de **Gerenciar > Convites para registro**.
- **Limite de registro do dispositivo para dispositivos Android e iOS:** a propriedade do servidor **Número de dispositivos por usuário** foi movida para **Configurar > Perfis de registro** e agora se aplica a todos os modos do servidor.
- **APIs somente MAM:** para dispositivos somente MAM, você pode chamar os serviços REST usando qualquer cliente REST e a API REST do XenMobile para chamar os serviços que o console XenMobile expõe.
- As APIs somente MAM permitem:
 - Enviar uma URL de convite e um PIN de uso único.
 - Emitir ações de bloqueio e apagamento de aplicativos em dispositivos.

A tabela a seguir resume as diferenças entre a funcionalidade MAM legado e somente MAM.

Cenários de registro e outros recursos	MAM legado (o modo de servidor é ENT)	Modo somente MAM (o modo de servidor é MAM)
Autenticação de certificado	Não compatível.	Compatível. Para a autenticação de certificado, o Citrix Gateway é necessário.
Requisito de implantação	O Servidor XenMobile não precisa ser diretamente acessível dos dispositivos.	O Servidor XenMobile não precisa ser diretamente acessível dos dispositivos.
Opção de registro	Use o FQDN do Citrix Gateway ou, ao usar o FQDN do MDM, opte por não se registrar.	Use o FQDN do Servidor XenMobile.
Métodos de registro*	Nome de usuário + Senha	Nome de usuário + Senha, Alta Segurança, URL de Convite, URL de Convite + PIN, URL de Convite + Senha, Dois Fatores, Nome de usuário + PIN
Bloqueio e apagamento de aplicativos	Compatível.	Compatível.
Opções do Portal de Autoajuda para bloqueio e apagamento de aplicativos	Não compatível.	Compatível.
Comportamento do apagamento de aplicativos	Os aplicativos permanecem no dispositivo, mas não são utilizáveis. O XenMobile exclui a conta apenas no cliente.	Os aplicativos permanecem no dispositivo, mas não são utilizáveis. O XenMobile exclui a conta apenas no cliente.
Ações automatizadas para os usuários somente MAM.	As ações de evento, propriedade de dispositivo e propriedade de usuário são compatíveis. Não suporta ações automatizadas baseadas em aplicativos instaladas.	Suporta evento, propriedade de dispositivo, propriedade de usuário e algumas ações baseadas em aplicativo, incluindo apagamento de aplicativo e bloqueio de aplicativo.

Ação interna quando um usuário do Active Directory é excluído	Suporta apagamento de aplicativos.	Suporta apagamento de aplicativos.
Limite de registro	Compatível; configurado por meio de um perfil de registro.	Compatível; configurado por meio de um perfil de registro.
Inventário de software	Compatível. O XenMobile lista aplicativos instalados em um dispositivo	Não compatível.

***Em relação às notificações:** o SMTP é o único método suportado para enviar convites de registro.

Importante:

Para o modo somente MAM, os usuários registrados anteriormente devem registrar seus dispositivos novamente. Forneça aos usuários o FQDN do XenMobile Server que eles precisam para o registro. No modo somente MAM, como no modo ENT, os dispositivos se registram usando o FQDN do XenMobile Server. (No modo MAM legado, os dispositivos se registram usando o FQDN do Citrix Gateway.)

Requisitos de dispositivo

April 1, 2021

Um ponto importante a ser considerado em qualquer implantação é o dispositivo que você planeja lançar. Nas plataformas iOS, Android e Windows, as opções são numerosas. Para obter uma lista de dispositivos compatíveis com o XenMobile, consulte [Plataformas de dispositivo com suporte](#).

Em um ambiente “traga seu próprio dispositivo” (BYOD), é possível uma mistura de plataformas suportadas. No entanto, considere as limitações no artigo sobre a plataforma de dispositivos com suporte ao informar os usuários sobre os dispositivos que podem ser registrados. Mesmo se você permitir apenas um ou dois dispositivos em seu ambiente, o XenMobile funciona de maneira um pouco diferente em dispositivos iOS, Android e Windows. Conjuntos de recursos diferentes estão disponíveis em cada plataforma.

Além disso, nem todos os designs de aplicativos segmentam os fatores de formato de tablets e de telefones. Antes de fazer alterações generalizadas, teste os aplicativos para garantir que eles se encaixem na tela do dispositivo que você deseja implantar.

Você também pode considerar fatores de registro. Apple e Google oferecem programas de registro corporativa. Por meio do [Programa de implantação da Apple](#) e do [Google Android Enterprise](#) você pode comprar dispositivos pré-configurados e prontos para serem usados pelos funcionários.

Para obter mais informações sobre registro, consulte [Opções de registro do usuário](#).

Segurança e experiência do usuário

April 8, 2021

A segurança é importante para qualquer organização, mas você precisa encontrar um equilíbrio entre segurança e experiência do usuário. Por exemplo, você pode ter um ambiente altamente seguro que é difícil para os usuários usarem. Ou o seu ambiente pode ser tão fácil de usar que o seu controle de acesso não se mostra tão rigoroso. As outras seções deste manual virtual cobrem os recursos de segurança em detalhes. O objetivo deste artigo é oferecer uma visão geral das considerações comuns de segurança e das opções de segurança disponíveis no XenMobile.

Aqui estão algumas considerações importantes a serem analisadas para cada caso de uso:

- Você quer proteger determinados aplicativos, o dispositivo inteiro ou ambos?
- Como você deseja que seus usuários autentiquem a identidade deles? Você planeja usar LDAP, autenticação baseada em certificado ou uma combinação dos dois?
- Como você deseja lidar com os tempos limite de sessão do usuário? Tenha em mente que existem diferentes valores de tempo limite para serviços em segundo plano, Citrix ADC e para poder acessar aplicativos enquanto estiver off-line.
- Deseja que os usuários definam um código secreto no nível do dispositivo, um código secreto no nível do aplicativo ou ambos? Quantas tentativas de login você deseja conceder aos usuários? Tenha em mente que os requisitos extras de autenticação por aplicativo implementados com o MAM podem afetar a experiência do usuário.
- Quais outras restrições você deseja impor aos usuários? Deseja que os usuários acessem serviços de nuvem como a Siri? O que eles podem e não podem fazer com cada aplicativo que você disponibiliza a eles? Deseja implantar políticas de Wi-Fi corporativas para impedir que os planos de dados da rede celular sejam consumidos enquanto estiver dentro da área do escritório?

Aplicativo versus Dispositivo

Uma das primeiras coisas a considerar é se deve-se proteger apenas determinados aplicativos usando o gerenciamento de aplicativos móveis (MAM). Ou se você também quer gerenciar todo o dispositivo usando o gerenciamento de dispositivos móveis (MDM). Normalmente, se você não precisar de cont-

role no nível do dispositivo, e apenas gerenciar aplicativos móveis, especialmente se a sua organização trabalhar com dispositivos BYOD (Traga seu próprio dispositivo).

Usuários com dispositivos que o XenMobile não gerencia podem instalar aplicativos através da App Store. Em vez de controles no nível do dispositivo, como apagamento seletivo ou completo, você controla o acesso aos aplicativos por meio de políticas de aplicativos. As políticas, dependendo dos valores definidos, exigem que o dispositivo verifique o XenMobile rotineiramente para confirmar que os aplicativos ainda têm permissão para serem executados.

O MDM permite proteger um dispositivo inteiro, incluindo a capacidade de fazer o inventário de todo o software em um dispositivo. Você pode impedir o registro se o dispositivo estiver com jailbreak, root ou tiver um software inseguro instalado. No entanto, esse nível de controle deixa os usuários desconfiados de dar tanto poder sobre seus dispositivos pessoais e poderá reduzir as taxas de registro.

Autenticação

Autenticação é onde ocorre grande parte da experiência do usuário. Se sua organização já estiver executando o Active Directory, o uso do Active Directory é a maneira mais simples de fazer com que seus usuários acessem o sistema.

Outra parte significativa da experiência do usuário em relação à autenticação é o tempo limite. Um ambiente de alta segurança pode exigir que os usuários façam logon toda vez que acessarem o sistema, mas essa opção não é ideal para todas as organizações. Por exemplo, fazer com que os usuários insiram suas credenciais toda vez que quiserem acessar seus e-mails pode afetar significativamente a experiência do usuário.

Entropia de usuário

Para maior segurança, você pode ativar um recurso chamado *entropia de usuário*. O Citrix Secure Hub e alguns outros aplicativos geralmente compartilham dados comuns, como senhas, PINs e certificados, para garantir que tudo funcione corretamente. Essas informações são armazenadas em um cofre genérico no Secure Hub. Se você habilitar a entropia de usuário através da opção **Criptografar segredos**, o XenMobile cria um novo cofre chamado UserEntropy. O XenMobile move as informações do cofre genérico para o novo cofre. Para que o Secure Hub ou outro aplicativo acesse os dados, os usuários devem inserir uma senha ou PIN.

A ativação da entropia de usuário adiciona outra camada de autenticação a vários lugares. Como resultado, os usuários devem inserir uma senha ou PIN sempre que um aplicativo exigir acesso a dados compartilhados, incluindo certificados, no cofre UserEntropy.

Você pode saber mais sobre a entropia de usuário lendo [Sobre o MDX Toolkit](#) na documentação do XenMobile. Para ativar a entropia de usuário, você pode encontrar as configurações relacionadas nas [Propriedades do cliente](#).

Políticas

As políticas MDX e MDM oferecem bastante flexibilidade às organizações, mas também podem restringir os usuários. Por exemplo, convém bloquear o acesso a aplicativos na nuvem, como a Siri ou o iCloud, que podem enviar dados confidenciais para vários locais. Você pode configurar uma política para bloquear o acesso a esses serviços, mas lembre-se de que tal política pode ter consequências indesejadas. O microfone para teclado do iOS também depende do acesso à nuvem, e você irá bloquear o acesso a esse recurso também.

Aplicativos

Gerenciamento de Mobilidade Empresarial (EMM) em Gerenciamento de Dispositivos Móveis (MDM) e Gerenciamento de Aplicativos Móveis (MAM). Enquanto o MDM permite que as organizações protejam e controlem dispositivos móveis, o MAM facilita a entrega e o gerenciamento de aplicativos. Com a crescente adoção do BYOD, você pode implementar uma solução MAM, para ajudar na entrega de aplicativos, no licenciamento de software, na configuração e no gerenciamento do ciclo de vida do aplicativo.

Com o XenMobile, você pode proteger esses aplicativos ainda mais, configurando políticas específicas de MAM e configurações de VPN para evitar o vazamento de dados e outras ameaças de segurança. O XenMobile oferece às organizações a flexibilidade de implantar qualquer uma das seguintes soluções:

- Ambiente somente MAM
- Ambiente somente MDM
- Ambiente unificado XenMobile Enterprise que fornece funcionalidade MDM e MAM na mesma plataforma

Além da capacidade de fornecer aplicativos para dispositivos móveis, o XenMobile oferece contêiner de aplicativos por meio da tecnologia MDX. O MDX protege aplicativos por meio de criptografia separada da criptografia no nível do dispositivo fornecida pela plataforma. Você pode apagar ou bloquear o aplicativo, e os aplicativos estão sujeitos a controles granulares baseados em políticas. Os fornecedores independentes de software (ISVs) podem aplicar esses controles usando o Mobile Apps SDK.

Em um ambiente corporativo, os usuários usam diferentes aplicativos móveis para ajudar em suas funções. Os aplicativos podem incluir aplicativos da loja de aplicativos pública, aplicativos desenvolvidos internamente e aplicativos nativos. O XenMobile categoriza esses aplicativos da seguinte maneira:

Aplicativos públicos: estes aplicativos incluem os aplicativos gratuitos ou pagos em uma loja de aplicativos pública, como o Apple App Store ou o Google Play. Fornecedores fora da organização geralmente disponibilizam seus aplicativos em lojas de aplicativos públicas. Esta opção permite que seus clientes baixem os aplicativos diretamente da Internet. Você pode usar vários aplicativos públicos em sua organização, dependendo das necessidades dos usuários. Exemplos de tais aplicativos incluem os aplicativos GoToMeeting, Salesforce e EpicCare.

A Citrix não suporta o download de binários de aplicativos diretamente de lojas de aplicativos públicas para posterior preparação com o MDX Toolkit para distribuição corporativa. Para habilitar com MDX aplicativos de terceiros, fale com o fornecedor do aplicativo para obter os binários do aplicativo. Você pode preparar os binários usando o MDX Toolkit ou integrar o MAM SDK com os binários.

Aplicativos internos: muitas organizações possuem desenvolvedores internos que criam aplicativos que fornecem funcionalidade específica e são desenvolvidos e distribuídos de maneira independente dentro da organização. Em certos casos, algumas organizações também podem ter aplicativos que os ISVs fornecem. Você pode implantar esses aplicativos como aplicativos nativos ou pode agrupar os aplicativos em contêineres usando uma solução MAM, como o XenMobile. Por exemplo, uma organização de medicina e saúde pode criar um aplicativo interno que permita que os médicos visualizem informações do paciente em dispositivos móveis. A organização pode então habilitar o aplicativo com MAM SDK ou preparar o aplicativo com MDX para proteger as informações do paciente e permitir o acesso VPN ao servidor de banco de dados de pacientes de back-end.

Aplicativos Web e SaaS: esses aplicativos incluem os aplicativos acessados em uma rede interna (aplicativos Web) ou em uma rede pública (SaaS). O XenMobile também permite que você crie aplicativos da Web e SaaS personalizados usando uma lista de conectores de aplicativos. Esses conectores de aplicativos podem facilitar o logon único (SSO) em aplicativos da Web existentes. Para obter detalhes, consulte [Tipos de conector de aplicativo](#). Por exemplo, você pode usar o SAML do Google Apps para SSO com base no SAML (Security Assertion Markup Language) para o Google Apps.

Aplicativos móveis de produtividade: aplicativos desenvolvidos pela Citrix e incluídos na licença do XenMobile. Para obter detalhes, consulte [Sobre aplicativos móveis de produtividade](#). A Citrix também oferece outros [aplicativos prontos para negócios](#) que os ISVs desenvolvem usando o Mobile Apps SDK.

Aplicativos HDX: aplicativos hospedados no Windows que você publica com o StoreFront. Se você tiver um ambiente Citrix Virtual Apps and Desktops, poderá integrar os aplicativos ao XenMobile para disponibilizá-los para os usuários registrados.

Dependendo do tipo de aplicativos móveis que você planeja implantar e gerenciar com o XenMobile, a configuração e a arquitetura subjacentes serão diferentes. Por exemplo, se vários grupos de usuários com diferentes níveis de permissões consumirem um único aplicativo, talvez você precise separar os grupos de entrega para implantar duas versões do aplicativo. Além disso, você deve garantir que a associação do grupo de usuários seja mutuamente exclusiva para evitar incompatibilidades de política nos dispositivos do usuário.

Também é possível gerenciar o licenciamento de aplicativos iOS usando a compra por volume da Apple. Essa opção exigirá que você se registre na compra por volume da Apple e configure os parâmetros de compra por volume do XenMobile no console XenMobile para distribuir os aplicativos com as licenças de compra por volume. Uma variedade de tais casos de uso torna importante avaliar e planejar sua estratégia MAM antes de implementar o ambiente XenMobile. Você pode começar a planejar sua estratégia MAM definindo o seguinte:

Tipos de aplicativos: liste os diferentes tipos de aplicativos aos quais planeja oferecer suporte e categorize-os. Por exemplo: aplicativos móveis de produtividade, públicos, nativos, aplicativos ISV, Web, internos e assim por diante. Além disso, categorize os aplicativos para diferentes plataformas de dispositivos, como iOS e Android. Essa categorização ajuda você a alinhar as configurações do XenMobile necessárias para cada tipo de aplicativo. Por exemplo, alguns aplicativos podem não se qualificar para preparação, ou podem exigir o Mobile Apps SDK para habilitar APIs especiais para interação com outros aplicativos.

Requisitos de rede: configure aplicativos com requisitos específicos de acesso à rede com as configurações apropriadas. Por exemplo, alguns aplicativos podem precisar de acesso à sua rede interna por meio de VPN. Alguns aplicativos podem exigir acesso à Internet para rotear o acesso via DMZ. Para permitir que esses aplicativos se conectem à rede necessária, você precisa definir várias configurações de acordo. A definição de requisitos de rede por aplicativo ajuda a finalizar suas decisões de arquitetura desde o início, o que simplifica o processo geral de implementação.

Requisitos de segurança: é fundamental definir os requisitos de segurança que se aplicam a aplicativos individuais ou a todos os aplicativos. Esse planejamento garante que você crie as configurações certas ao instalar o XenMobile Server. Embora as configurações, como as políticas de MDX, se apliquem a aplicativos individuais, as configurações de sessão e autenticação se aplicam a todos os aplicativos. Alguns aplicativos podem ter requisitos específicos de criptografia, containerização, preparação, criptografia, autenticação, cerca geográfica, código secreto ou compartilhamento de dados que você pode descrever antecipadamente para simplificar a implementação.

Requisitos de implantação: convém usar uma implantação baseada em políticas para permitir que apenas usuários em conformidade baixem os aplicativos publicados. Por exemplo, você pode querer que determinados aplicativos exijam que:

- a criptografia baseada em plataforma de dispositivo está habilitada
- o dispositivo é gerenciado
- o dispositivo atende a uma versão mínima do sistema operacional
- determinados aplicativos estão disponíveis apenas para usuários corporativos

Você também pode querer que determinados aplicativos estejam disponíveis apenas para usuários corporativos. Descreva esses requisitos com antecedência para poder configurar as regras ou ações de implantação apropriadas.

Requisitos de licenciamento: mantenha um registro dos requisitos de licenciamento relacionados a aplicativo. Essas notas ajudam a gerenciar o uso de licenças de forma eficaz e a decidir se você deseja configurar recursos específicos no XenMobile para facilitar o licenciamento. Por exemplo, se você implantar um aplicativo iOS gratuito ou pago, a Apple irá aplicar os requisitos de licenciamento no aplicativo exigindo que os usuários façam login em suas contas do iTunes. Você pode se registrar na compra por volume da Apple para distribuir e gerenciar esses aplicativos usando o XenMobile. A compra por volume permite que os usuários baixem os aplicativos sem precisar entrar em suas contas

do iTunes. Além disso, as ferramentas, como o Samsung SAFE e o Samsung Knox, têm requisitos especiais de licenciamento, que você precisa concluir antes de implantar esses recursos.

Requisitos de lista de permissão e lista de bloqueio: você provavelmente vai querer impedir que os usuários instalem ou usem alguns aplicativos. Crie uma lista de permissão de aplicativos que tornam um dispositivo fora de conformidade. Em seguida, configure as políticas para disparar quando um dispositivo se tornar não compatível. Por outro lado, um aplicativo pode ser aceitável para uso, mas pode cair na lista de bloqueio por algum motivo. Nesse caso, você pode adicionar o aplicativo a uma lista de permissão e indicar que o aplicativo é aceitável para uso, mas não é necessário. Além disso, lembre-se de que os aplicativos pré-instalados em novos dispositivos podem incluir alguns aplicativos comumente usados que não fazem parte do sistema operacional. Esses aplicativos podem entrar em conflito com sua estratégia de lista de bloqueio.

Caso de uso de aplicativos

Uma organização de saúde planeja implantar o XenMobile para servir como uma solução MAM para seus aplicativos móveis. Aplicativos móveis são entregues a usuários corporativos e BYOD. A TI decide entregar e gerenciar os seguintes aplicativos:

- **Aplicativos móveis de produtividade:** Aplicativos para iOS e Android fornecidos pela Citrix.
- **Secure Mail:** email, calendário e aplicativo de contato.
- **Secure Web:** navegador seguro que fornece acesso aos sites da Internet e da intranet.
- **Citrix Files:** aplicativo para acessar dados compartilhados e para compartilhar, sincronizar e editar arquivos.

Loja de aplicativos pública

- **Secure Hub:** cliente usado por todos os dispositivos móveis para se comunicar com o XenMobile. A TI envia parâmetros de segurança, configurações e aplicativos móveis para dispositivos móveis via cliente do Secure Hub. Dispositivos Android e iOS se registram no XenMobile através do Secure Hub.
- **Citrix Receiver:** aplicativo móvel que permite aos usuários abrir aplicativos hospedados por aplicativos e áreas de trabalho virtuais em dispositivos móveis.
- **GoToMeeting:** um cliente de reunião on-line, compartilhamento de área de trabalho e videoconferência que permite que os usuários se encontrem com outros usuários de computador, clientes, consumidores ou colegas pela Internet em tempo real.
- **SalesForce1:** o Salesforce1 permite que os usuários acessem o Salesforce a partir de dispositivos móveis e reúnam todos os aplicativos Chatter, CRM, personalizados e de negócios em uma experiência unificada para qualquer usuário do Salesforce.
- **RSA SecurID:** token baseado em software para autenticação de dois fatores.

- **Aplicativos EpicCare:** esses aplicativos fornecem aos profissionais de saúde acesso seguro e portátil a prontuários, listas de pacientes, agendamentos e mensagens.
 - **Haiku:** aplicativo móvel para telefones iPhone e Android.
 - **Canto:** aplicativo móvel para o iPad
 - **Rover:** aplicativos móveis para iPhone e iPad.

HDX: estes aplicativos são fornecidos via Citrix Virtual Apps and Desktops.

- **Epic Hyperspace:** aplicativo cliente Epic para gerenciamento eletrônico de prontuários médicos.

ISV

- **Vocera:** aplicativo móvel de mensagens e IP de voz compatível com HIPAA que amplia os benefícios da tecnologia de voz Vocera a qualquer hora, em qualquer lugar, através de smartphones iPhone e Android.

Aplicativos internos

- **HCMail:** aplicativo que ajuda a compor mensagens criptografadas, pesquisar catálogos de endereços em servidores de e-mail internos e enviar as mensagens criptografadas para os contatos usando um cliente de e-mail.

Aplicativos da web internos

- **PatientRounding:** aplicativo da Web usado para registrar informações médicas do paciente por diferentes departamentos.
- **Outlook Web Access:** permite o acesso de email por meio de um navegador da web.
- **SharePoint:** usado para compartilhamento de arquivos e dados em toda a organização.

A tabela a seguir lista as informações básicas necessárias para a configuração do MAM.

Nome do aplicativo	Tipo de aplicativo	Preparação de MDX	iOS	Android
Secure Mail	XenMobile App	Não para a versão 10.4.1 e posterior	Sim	Sim
Secure Web	XenMobile App	Não para a versão 10.4.1 e posterior	Sim	Sim

Citrix Files	XenMobile App	Não para a versão 10.4.1 e posterior	Sim	Sim
Secure Hub	Aplicativo público	N/D	Sim	Sim
Citrix Receiver	Aplicativo público	N/D	Sim	Sim
GoToMeeting	Aplicativo público	N/D	Sim	Sim
SalesForce1	Aplicativo público	N/D	Sim	Sim
RSA SecurID	Aplicativo público	N/D	Sim	Sim
Epic Haiku	Aplicativo público	N/D	Sim	Sim
Epic Canto	Aplicativo público	N/D	Sim	Não
Epic Rover	Aplicativo público	N/D	Sim	Não
Epic Hyperspace	Aplicativo HDX	N/D	Sim	Sim
Vocera	Aplicativo ISV	Sim	Sim	Sim
HCMail	Aplicativo interno	Sim	Sim	Sim
PatientRounding	Aplicativo Web	N/D	Sim	Sim
Outlook Web Access	Aplicativo Web	N/D	Sim	Sim
SharePoint	Aplicativo Web	N/D	Sim	Sim

As tabelas a seguir listam os requisitos específicos que você pode consultar ao configurar as políticas do MAM no XenMobile.

| Nome do aplicativo | VPN necessária | Interação | Interação | Criptografia baseada em plataforma de dispositivo |
|| (com aplicativos fora do contêiner) | (de aplicativos fora do contêiner) ||

-----		-----	-----	-----
Secure Mail	S	Permitido seletivamente	Permitido	Desnecessário
Secure Web	S	Permitido	Permitido	Desnecessário
Citrix Files	S	Permitido	Permitido	Desnecessário
Secure Hub	S	N/D	N/D	N/D
Citrix Receiver	S	N/D	N/D	N/D
GoToMeeting	N	N/D	N/D	N/D
Salesforce1	N	N/D	N/D	N/D
RSA SecurID	N	N/D	N/D	N/D
Epic Haiku	S	N/D	N/D	N/D
Epic Canto	S	N/D	N/D	N/D
Epic Rover	S	N/D	N/D	N/D
Epic Hyperspace	S	N/D	N/D	N/D
Vocera	S	Bloqueado	Bloqueado	Desnecessário
HCMail	S	Bloqueado	Bloqueado	Obrigatório
PatientRounding	S	N/D	N/D	Obrigatório
Outlook Web Access	S	N/D	N/D	Desnecessário
SharePoint	S	N/D	N/D	Desnecessário

Nome do aplicativo	Filtragem Proxy	Cerca Licenciamento	Cerca geográfica	Mobile Apps SDK	Versão mínima do sistema operacional
Secure Mail	Obrigatório	N/D	Seletivamente Obrigatório	N/D	Imposto
Secure Web	Obrigatório	N/D	Desnecessário	N/D	Imposto
Citrix Files	Obrigatório	N/D	Desnecessário	N/D	Imposto
Secure Hub	Desnecessário	Compra por volume	Desnecessário	N/D	Não aplicado
Citrix Receiver	Desnecessário	Compra por volume	Desnecessário	N/D	Não aplicado
GoToMeeting	Desnecessário	Compra por volume	Desnecessário	N/D	Não aplicado
SalesForce1	Desnecessário	Compra por volume	Desnecessário	N/D	Não aplicado
RSA SecurID	Desnecessário	Compra por volume	Desnecessário	N/D	Não aplicado

Nome do aplicativo	Filtragem Proxy	Licenciamento	Cerca geográfica	Mobile Apps SDK	Versão mínima do sistema operacional
Epic Haiku	Desnecessário	Compra por volume	Desnecessário	N/D	Não aplicado
Epic Canto	Desnecessário	Compra por volume	Desnecessário	N/D	Não aplicado
Epic Rover	Desnecessário	Compra por volume	Desnecessário	N/D	Não aplicado
Epic Hyperspace	Desnecessário	N/D	Desnecessário	N/D	Não aplicado
Vocera	Obrigatório	N/D	Obrigatório	Obrigatório	Imposto
HCMail	Obrigatório	N/D	Obrigatório	Obrigatório	Imposto
PatientRound- ing	Obrigatório	N/D	Desnecessário	N/D	Não aplicado
Outlook Web Access	Obrigatório	N/D	Desnecessário	N/D	Não aplicado
SharePoint	Obrigatório	N/D	Desnecessário	N/D	Não aplicado

Comunidades do usuário

Cada organização consiste em diversas comunidades de usuários que operam em diferentes funções. Essas comunidades de usuários executam tarefas e funções de escritório diferentes usando vários recursos fornecidos por meio dos dispositivos móveis dos usuários. Os usuários podem trabalhar em casa ou em escritórios remotos usando dispositivos móveis fornecidos por você. Ou os usuários podem usar seus dispositivos móveis pessoais, o que permite que eles acessem ferramentas que estão sujeitas a determinadas regras de conformidade de segurança.

Com mais comunidades de usuários usando dispositivos móveis, o gerenciamento de mobilidade empresarial (EMM) se torna crítico para evitar vazamentos de dados e impor restrições de segurança. Para um gerenciamento eficiente e sofisticado de dispositivos móveis, você pode categorizar suas comunidades de usuários. Isso simplifica o mapeamento de usuários para recursos e garante que as políticas de segurança corretas sejam aplicadas aos usuários certos.

O exemplo a seguir ilustra como as comunidades de usuários de uma organização de assistência médica são classificadas para o EMM.

Cado de uso de comunidades de usuários

Neste exemplo, esta organização de assistência médica fornece recursos de tecnologia e acesso a vários usuários, incluindo funcionários e voluntários da rede e afiliados. A organização optou por implantar a solução EMM apenas para usuários não executivos.

Os cargos e funções dos usuários dessa organização podem ser divididos em subgrupos, incluindo: clínico, não clínico e contratados. Um grupo selecionado de usuários recebe dispositivos móveis corporativos, enquanto outros podem acessar recursos limitados da empresa a partir de seus dispositivos pessoais. Para impor o nível certo de restrições de segurança e impedir vazamentos de dados, a organização decidiu que a TI corporativa gerencia cada dispositivo registrado, seja corporativo ou BYOD (traga seu próprio dispositivo). Além disso, os usuários só podem registrar um único dispositivo.

A seção a seguir fornece uma visão geral dos cargos e funções de cada subgrupo:

Clínico

- Enfermeiros
- Médicos (doutores, cirurgiões e outros)
- Especialistas (nutricionistas, anestesistas, radiologistas, cardiologistas, oncologistas e outros)
- Médicos externos (médicos não empregados e trabalhadores de escritório que trabalham em escritórios remotos)
- Serviços de Saúde Domiciliar (trabalhadores de escritório e móveis realizando serviços médicos em visitas domiciliares ao paciente)
- Especialista em pesquisa (trabalhadores do conhecimento e usuários avançados em seis institutos de pesquisa que realizam pesquisas clínicas para encontrar respostas para problemas clínicos)
- Educação e Formação (enfermeiros, médicos e especialistas em educação e formação)

Não clínico

- Serviços compartilhados (funcionários de escritório executando várias funções de back-office, incluindo: RH, folha de pagamento, contas a pagar, serviço de cadeia de fornecimento e outros)
- Serviços Médicos (funcionários do escritório realizando várias soluções de gestão de saúde, serviços administrativos e processos de negócios para fornecedores, incluindo: Serviços Administrativos, Analytics e Business Intelligence, Sistemas de Negócios, Serviços ao Cliente, Finanças, Administração de Cuidados Gerenciados, Soluções de Acesso ao Paciente, Soluções de Ciclo de Receita e outros)
- Serviços de Suporte (trabalhadores de escritório realizando várias funções não clínicas, incluindo Administração de Benefícios, Integração Clínica, Comunicações, Gerenciamento de

Compensação e Desempenho, Serviços de Instalações e Propriedade, Sistemas de Tecnologia de RH, Serviços de Informação, Auditoria Interna e Melhoria de Processos e outros)

- Programas filantrópicos (funcionários de escritório e móveis que realizam várias funções de apoio a programas filantrópicos)

Contratados

- Parceiros fabricantes e fornecedores (conectados no local e remotamente via VPN site-to-site, fornecendo várias funções de suporte não clínicas)

Com base nas informações anteriores, a organização criou as seguintes entidades. Para obter mais informações sobre grupos de entrega no XenMobile, consulte [Implantar recursos](#).

Grupos e Unidades Organizacionais (OUs) do Active Directory

Para OU = Recursos do XenMobile:

- OU = Clínico; Grupos =
 - XM-Enfermeiros
 - XM-Médicos
 - XM-Especialistas
 - XM-Médicos Externos
 - XM-Serviços de Saúde Domiciliar
 - XM-Especialista em Pesquisa
 - XM-Educação e Formação
- OU = Não clínico; Grupos =
 - XM-Serviços Compartilhados
 - XM-Serviços Médicos
 - XM-Serviços de Suporte
 - XM-Programas Filantrópicos

Usuários locais e grupos do XenMobile

ForGroup= Contratados, Usuários =

- Vendor1
- Vendor2
- Vendor3
- ... Vendor10

Grupos de entrega do XenMobile

- Clínico-Enfermeiros

- Clínico-Médicos
- Clínico-Especialistas
- Clínico-Médicos Externos
- Clínico-Serviços de Saúde Domiciliar
- Clínico-Especialista em Pesquisa
- Clínico-Educação e Formação
- Não clínicos-Serviços Compartilhados
- Não clínicos-Serviços Médicos
- Não clínicos-Serviços de Suporte
- Não clínicos-Programas Filantrópicos

Mapeamento de Grupo de entrega e Grupo de usuários

Grupos do Active Directory	Grupos de entrega do XenMobile
XM-Enfermeiros	Clínico-Enfermeiros
XM-Médicos	Clínico-Médicos
XM-Especialistas	Clínico-Especialistas
XM-Médicos Externos	Clínico-Médicos Externos
XM-Serviços de Saúde Domiciliar	Clínico-Serviços de Saúde Domiciliar
XM-Especialista em Pesquisa	Clínico-Especialista em Pesquisa
XM-Educação e Formação	Clínico-Educação e Formação
XM-Serviços Compartilhados	Não clínicos-Serviços Compartilhados
XM-Serviços Médicos	Não clínicos-Serviços Médicos
XM-Serviços de Suporte	Não clínicos-Serviços de Suporte
XM-Programas Filantrópicos	Não clínicos-Programas Filantrópicos

Mapeamento de Grupo de entrega e Recursos

As tabelas a seguir ilustram os recursos atribuídos a cada grupo de entrega neste caso de uso. A primeira tabela mostra as atribuições do aplicativo móvel. A segunda tabela mostra o aplicativo público, os aplicativos HDX e os recursos de gerenciamento de dispositivos.

Grupos de entrega do XenMobile	Aplicativos móveis Citrix	Aplicativos móveis públicos	Aplicativos móveis HDX
Clínico-Enfermeiros	X		
Clínico-Médicos			
Clínico-Especialistas			
Clínico-Médicos Externos	X		
Clínico-Serviços de Saúde Domiciliar	X		
Clínico-Especialista em Pesquisa	X		
Clínico-Educação e Formação		X	X
Não clínicos-Serviços Compartilhados		X	X
Não clínicos-Serviços Médicos		X	X
Não clínicos-Serviços de Suporte	X	X	X
Não clínicos-Programas Filantrópicos	X	X	X
Contratados	X	X	X

Grupos de entrega do XenMobile	Aplicativo público: RSA SecurID	Aplicativo público: EpicCare Haiku	Aplicativo HDX: Epic Hy-perspace	Política de código secreto	Restrições de dispositivos	Ações automatizadas	Política de WiFi
Clínico-Enfermeiros							X

Clínico- Médicos			X
Clínico- Especialistas			
Clínico- Médicos Externos			
Clínico- Serviços de Saúde Domicil- iar			
Clínico- Especialista em Pesquisa			
Clínico- Educação e For- mação	X		X
Não clínicos- Serviços Compar- tilhados	X		X
Não clínicos- Serviços Médicos	X		X
Não clínicos- Serviços de Suporte	X		X

Notas e considerações

- O XenMobile cria um grupo de entrega padrão chamado Todos os Usuários durante a configuração inicial. Se você não desabilitar esse grupo de entrega, todos os usuários do Active Directory terão direitos para se registrar no XenMobile.
- O XenMobile sincroniza usuários e grupos do Active Directory sob demanda usando uma conexão dinâmica com o servidor LDAP.
- Se um usuário fizer parte de um grupo que não esteja mapeado no XenMobile, esse usuário não poderá se registrar. Da mesma forma, se um usuário for membro de vários grupos, o XenMobile categoriza o usuário como apenas nos grupos mapeados para o XenMobile.
- Para tornar o registro no MDM obrigatório, defina a opção de Registro Obrigatório como True em Propriedades do Servidor no console XenMobile. Para obter detalhes, consulte [Propriedades do servidor](#).
- Você pode excluir um grupo de usuários de um grupo de entrega do XenMobile excluindo a entrada no banco de dados do SQL Server, em `dbo.userlistgrps`.

Cuidado: antes de executar esta ação, crie um backup do XenMobile e do banco de dados.

Sobre a Propriedade de dispositivo no XenMobile

Você pode agrupar usuários de acordo com o proprietário do dispositivo de um usuário. A propriedade do dispositivo inclui dispositivos de propriedade da empresa e dispositivos de propriedade do usuário, também conhecidos como BYOD (traga o seu próprio dispositivo). Você pode controlar como os dispositivos BYOD se conectam à sua rede em dois locais no console XenMobile: nas regras de implantação para cada tipo de recurso e nas propriedades do servidor na página **Configurações**. Para obter detalhes sobre regras de implantação, consulte [Configuração de regras de implantação](#) na documentação do XenMobile. Para obter detalhes sobre as propriedades do servidor, consulte [Propriedades do servidor](#).

Você pode exigir que todos os usuários de BYOD aceitem o gerenciamento corporativo de seus dispositivos antes que eles possam acessar os aplicativos. Ou você pode conceder aos usuários acesso a aplicativos corporativos sem precisar gerenciar seus dispositivos.

Quando você define a configuração do servidor **wsapi.mdm.required.flag** como **true**, o XenMobile gerencia todos os dispositivos BYOD, e qualquer usuário que recusar o registro não terá acesso aos aplicativos. Sugerimos configurar **wsapi.mdm.required.flag** como **true** em ambientes nos quais as equipes de TI corporativas precisam de alta segurança em conjunto com uma experiência de usuário positiva ao registrar dispositivos de usuários no XenMobile.

Se você deixar o **wsapi.mdm.required.flag** como **false**, que é a configuração padrão, os usuários poderão recusar o registro, mas ainda poderão acessar os aplicativos em seus dispositivos através da XenMobile Store. Considere configurar **wsapi.mdm.required.flag** como **false** em ambientes nos quais as restrições de privacidade, legais ou regulamentares não exigem gerenciamento de dispositi-

tivos, apenas gerenciamento de aplicativos corporativos.

Usuários com dispositivos que o XenMobile não gerencia podem instalar aplicativos através da XenMobile Store. Em vez de controles no nível do dispositivo, como apagamento seletivo ou completo, você controla o acesso aos aplicativos por meio de políticas de aplicativos. As políticas, dependendo dos valores definidos, exigem que o dispositivo verifique o XenMobile Server rotineiramente para confirmar que os aplicativos ainda têm permissão para serem executados.

Requisitos de segurança

A quantidade de considerações de segurança ao implantar um ambiente XenMobile pode se acumular rapidamente. Há muitas definições e configurações interligadas. Para ajudá-lo a começar e escolher um nível aceitável de proteção, a Citrix fornece recomendações para alta, maior e altíssima segurança, descritas na tabela a seguir.

Sua opção de modo de implantação envolve mais do que apenas considerações de segurança. É importante também revisar os requisitos do caso de uso e decidir se você pode atenuar as considerações com a segurança antes de escolher seu modo de implantação.

Alta: o uso dessas configurações proporciona uma experiência de usuário ideal, mantendo um nível básico de segurança aceitável para a maioria das organizações.

Maior: essas configurações criam um equilíbrio mais acirrado entre segurança e usabilidade.

Altíssima: seguir essas recomendações fornece um nível alto de segurança em troca de usabilidade e adoção do usuário.

Considerações sobre segurança no modo de implantação

A tabela a seguir especifica os modos de implantação para cada nível de segurança.

Alta Segurança	Maior segurança	Altíssima segurança
MAM ou MDM	MDM+MAM	MDM+MAM; mais FIPS

Notas:

- Dependendo do caso de uso, uma implantação somente MDM ou somente MAM pode atender aos requisitos de segurança e fornecer uma boa experiência ao usuário.
- Se você não precisar de containerização de aplicativo, micro VPN ou políticas específicas de aplicativo, o MDM é suficiente para gerenciar e proteger dispositivos.
- Para casos de uso como BYOD em quais a containerização de aplicativos por si só pode satisfazer

todos os requisitos comerciais e de segurança, a Citrix recomenda o modo somente MAM.

- Para ambientes de alta segurança (e dispositivos corporativos), a Citrix recomenda o MDM+MAM para aproveitar todos os recursos de segurança disponíveis. Certifique-se de impor o registro no MDM.
- Opções FIPS para ambientes com as mais altas necessidades de segurança, como o governo federal.

Se você habilitar o modo FIPS, deverá configurar o SQL Server para criptografar o tráfego do SQL.

Considerações de segurança do Citrix ADC e Citrix Gateway

A tabela a seguir especifica as recomendações do Citrix ADC e do Citrix Gateway para cada nível de segurança.

Alta Segurança	Maior segurança	Altíssima segurança
O Citrix ADC é recomendado. O Citrix Gateway é necessário para MAM e ENT; recomendado para MDM	Configuração padrão do assistente do Citrix ADC for XenMobile com ponte de SSL se o XenMobile estiver na DMZ. Ou descarga de SSL, se for necessário para atender aos padrões de segurança quando o XenMobile Server estiver na rede interna.	Descarga de SSL com criptografia de ponta a ponta

Notas:

- Expor o XenMobile Server à Internet por meio de NAT ou proxies de terceiros existentes e balanceadores de carga pode ser uma opção para MDM. No entanto, essa configuração requer que o tráfego SSL seja terminado no XenMobile Server, o que representa um risco potencial de segurança.
- Para ambientes de alta segurança, o Citrix ADC com a configuração padrão do XenMobile normalmente atende ou excede os requisitos de segurança.
- Para ambientes de MDM com as mais altas necessidades de segurança, a terminação SSL no Citrix ADC permite a inspeção de tráfego no perímetro e mantém a criptografia SSL de ponta a ponta.
- Opções para definir criptografias SSL/TLS.
- O hardware SSL FIPS Citrix ADC também está disponível.
- Para obter mais informações, consulte [Integração com Citrix Gateway e Citrix ADC](#).

Considerações sobre segurança de registro

A tabela a seguir especifica as recomendações do Citrix ADC e do Citrix Gateway para cada nível de segurança.

Alta Segurança	Maior segurança	Altíssima segurança
Somente membros do Grupo Active Directory. Grupo de entrega Todos os Usuários desativado.	Modo de segurança de registro apenas por convite. Somente membros do Grupo Active Directory. Grupo de entrega Todos os Usuários desativado	Modo de segurança de registro vinculado ao ID do dispositivo. Somente membros do Grupo Active Directory. Grupo de entrega Todos os Usuários desativado

Notas:

- A Citrix geralmente recomenda que você restrinja o registro somente aos usuários em grupos predefinidos do Active Directory. Essa configuração requer a desativação do grupo de entrega interno Todos os Usuários.
- Você pode usar convites de registro para restringir o registro para os usuários com apenas um convite. Os convites para registro não estão disponíveis para dispositivos Android Enterprise e Windows.
- Você pode usar os convites de registro de PIN de uso único (OTP) como uma solução de autenticação de dois fatores e para controlar o número de dispositivos que um usuário pode registrar.
- Para ambientes com requisitos de segurança, você pode associar convites de registro a um dispositivo por UDID/SN/EMEI. Uma opção de autenticação de dois fatores também está disponível para exigir uma senha do Active Directory e OTP. OTP não é uma opção suportada por dispositivos Windows.

Considerações sobre segurança do código secreto do dispositivo

A tabela a seguir especifica as recomendações de código secreto do dispositivo para cada nível de segurança.

Alta Segurança	Maior segurança	Altíssima segurança
-----------------------	------------------------	----------------------------

Recomendado Alta segurança é necessária para criptografia no nível do dispositivo. Imposta usando MDM. Você pode definir alta segurança conforme necessário para Somente MAM usando a política MDX, Comportamento do dispositivo não compatível.	Imposta usando MDM, uma política MDX ou ambos.	Aplicado usando a política MDM e MDX. Política de código secreto Complexo do MDM.
--	--	---

Notas:

- A Citrix recomenda o uso de um código secreto de dispositivo.
- Você pode impor um código secreto de dispositivo por meio de uma política de MDM.
- Você pode usar uma política de MDX para tornar um código secreto de dispositivo um requisito para o uso de aplicativos gerenciados. Por exemplo, para casos de uso BYOD.
- A Citrix recomenda combinar as opções de política MDM e MDX para aumentar a segurança em ambientes MDM+MAM.
- Para ambientes com os mais altos requisitos de segurança, você pode configurar políticas complexas de código secreto e aplicá-las com o MDM. Você pode configurar ações automáticas para notificar os administradores ou iniciar o apagamento seletivo/completo de dispositivos quando um dispositivo não obedecer a uma política de código secreto.

Aplicativos

April 8, 2021

Gerenciamento de Mobilidade Empresarial (EMM) em Gerenciamento de Dispositivos Móveis (MDM) e Gerenciamento de Aplicativos Móveis (MAM). Enquanto o MDM permite que as organizações protejam e controlem dispositivos móveis, o MAM facilita a entrega e o gerenciamento de aplicativos. Para dar suporte à adoção de BYOD, geralmente é possível implementar uma solução MAM, como o XenMobile, para auxiliar com:

- entrega de aplicativos
- licenciamento de software
- configuração

- gerenciamento do ciclo de vida dos aplicativos

Você pode exigir ou permitir que os usuários também optem pelo gerenciamento MDM

Com o XenMobile, você pode proteger esses aplicativos ainda mais, configurando políticas específicas de MAM e configurações de VPN para evitar o vazamento de dados e outras ameaças de segurança. O XenMobile oferece às organizações a flexibilidade de implantar suas soluções, como:

- Ambiente somente MAM
- Ambiente somente MDM
- Ambiente unificado XenMobile Enterprise que fornece funcionalidade MDM e MAM

Além da capacidade de fornecer aplicativos para dispositivos móveis, o XenMobile oferece contêiner de aplicativos por meio da tecnologia MDX. Os aplicativos estão sujeitos a controles granulares baseados em políticas. Os fornecedores independentes de software (ISVs) podem aplicar esses controles usando o Mobile Apps SDK.

Em um ambiente corporativo, os usuários usam diferentes aplicativos móveis para ajudar em suas funções. Os aplicativos podem incluir aplicativos da loja de aplicativos pública, aplicativos desenvolvidos internamente ou aplicativos nativos. O XenMobile categoriza esses aplicativos da seguinte maneira:

- **Aplicativos públicos:** estes aplicativos incluem os aplicativos gratuitos ou pagos em uma loja de aplicativos pública, como o Apple App Store ou o Google Play. Fornecedores fora da organização geralmente disponibilizam seus aplicativos em lojas de aplicativos públicas. Esta opção permite que seus clientes baixem os aplicativos diretamente da Internet. Você pode usar vários aplicativos públicos em sua organização, dependendo das necessidades dos usuários. Exemplos de tais aplicativos incluem os aplicativos GoToMeeting, Salesforce e EpicCare.
 - **Se você usar o SDK MAM:** obtenha os binários do aplicativo com o fornecedor do aplicativo. Em seguida, integre o MAM SDK no aplicativo.
 - **Se você usa o MDX Service ou Toolkit:** a Citrix não suporta o download de binários de aplicativos diretamente de lojas de aplicativos públicas para posterior preparação com o MDX Toolkit para distribuição corporativa. Para preparar aplicativos de terceiros, fale com o fornecedor do aplicativo para obter os binários do aplicativo. Assim você pode preparar os binários usando o MDX Toolkit.
- **Aplicativos internos:** muitas organizações possuem desenvolvedores internos que criam aplicativos que fornecem funcionalidade específica e são desenvolvidos e distribuídos de maneira independente dentro da organização. Em certos casos, algumas organizações também podem ter aplicativos que os ISVs fornecem. Você pode implantar esses aplicativos como aplicativos nativos ou pode agrupar os aplicativos em contêineres usando uma solução MAM, como o XenMobile.

Por exemplo, uma organização de medicina e saúde pode criar um aplicativo interno que per-

mita que os médicos visualizem informações do paciente em dispositivos móveis. Uma organização poderá então proteger as informações do paciente e habilitar o acesso VPN ao banco de dados do paciente usando um destes:

- SDK MAM
 - MDX Service ou MDX Toolkit
- **Aplicativos Web e SaaS:** esses aplicativos incluem os aplicativos acessados em uma rede interna (aplicativos Web) ou em uma rede pública (SaaS). O XenMobile também permite que você crie aplicativos da Web e SaaS personalizados usando uma lista de conectores de aplicativos. Esses conectores de aplicativos podem facilitar o logon único (SSO) em aplicativos da Web existentes. Para obter detalhes, consulte [Tipos de conector de aplicativo](#). Por exemplo, você pode usar o SAML do Google Apps para SSO com base no SAML (Security Assertion Markup Language) para o Google Apps.
 - **Aplicativos móveis de produtividade:** aplicativos móveis de produtividade são aplicativos desenvolvidos pela Citrix e incluídos na licença do XenMobile. Para obter detalhes, consulte [Sobre aplicativos móveis de produtividade](#). A Citrix também oferece outros [aplicativos prontos para negócios](#) que os ISVs desenvolvem usando o Mobile Apps SDK.
 - **Aplicativos HDX:** aplicativos HDX são aplicativos hospedados no Windows que você publica com o StoreFront. Se você usa o Citrix Virtual Apps and Desktops e o Citrix Workspace, os aplicativos HDX estarão disponíveis para usuários cadastrados.

Dependendo do tipo de aplicativos móveis que você planeja implantar e gerenciar com o XenMobile, a configuração subjacente poderá ser diferente. Por exemplo, vários grupos de usuários com diferentes níveis de permissões podem consumir um único aplicativo. Nesse caso, você pode criar grupos de entrega separados para implantar duas versões separadas do mesmo aplicativo. Além disso, você deve garantir que a associação do grupo de usuários seja mutuamente exclusiva para evitar incompatibilidades de política nos dispositivos dos usuários.

Você também pode gerenciar o licenciamento de aplicativos iOS usando a compra por volume da Apple. Essa opção requer que você se registre no programa de compra por volume e configure os parâmetros de compra por volume no console XenMobile. Essa configuração permite distribuir os aplicativos com as licenças de compra por volume. Vários casos de uso tornam importante avaliar e planejar sua estratégia MAM antes de implementar o ambiente XenMobile. Você pode começar a planejar sua estratégia MAM definindo o seguinte:

- **Tipos de aplicativos:** Liste os diferentes tipos de aplicativos aos quais você planeja oferecer suporte e categorizar, como aplicativos públicos, nativos, Web, internos ou ISV. Além disso, categorize os aplicativos para diferentes plataformas de dispositivos, como iOS e Android. Essa categorização ajuda a alinhar as várias configurações do XenMobile necessárias para cada tipo de aplicativo. Por exemplo, alguns aplicativos podem exigir o uso do Mobile Apps SDK para habilitar APIs especiais para interação com outros aplicativos.

- **Requisitos de rede:** defina as configurações de aplicativos que têm requisitos específicos de acesso à rede. Por exemplo, alguns aplicativos podem precisar de acesso à sua rede interna por meio de VPN. Alguns aplicativos podem exigir acesso à Internet para rotear o acesso via DMZ. Para permitir que esses aplicativos se conectem à rede necessária, você precisa definir várias configurações de acordo. A definição de requisitos de rede por aplicativo ajuda a finalizar suas decisões de arquitetura desde o início, o que simplifica o processo geral de implementação.
- **Requisitos de segurança:** você pode definir os requisitos de segurança para aplicar a aplicativos individuais ou a todos os aplicativos.
 - Configurações, como as políticas MDX, se aplicam a aplicativos individuais
 - Configurações de sessão e autenticação se aplicam a todos os aplicativos
 - Alguns aplicativos podem ter requisitos específicos de containerização, MDX, autenticação, cerca geográfica, código secreto ou compartilhamento de dados

Descreva esses requisitos com antecedência para simplificar sua implantação. Para obter detalhes sobre segurança no Endpoint Management, consulte [Segurança e experiência do usuário](#).

- **Requisitos de implantação** - convém usar uma implantação baseada em políticas para permitir que apenas usuários em conformidade baixem os aplicativos publicados. Por exemplo, alguns aplicativos podem exigir que o dispositivo seja gerenciado ou que o dispositivo atenda a uma versão mínima do sistema operacional. Você também pode querer que determinados aplicativos estejam disponíveis apenas para usuários corporativos. Descreva esses requisitos com antecedência para poder configurar as regras ou ações de implantação apropriadas.
- **Requisitos de licenciamento:** mantenha um registro dos requisitos de licenciamento relacionados ao aplicativo. Suas notas podem ajudá-lo a gerenciar o uso de licenças de forma eficaz e decidir se deseja configurar recursos específicos no XenMobile para facilitar o licenciamento. Por exemplo, se você implantar um aplicativo iOS gratuito ou pago, a Apple irá aplicar os requisitos de licenciamento no aplicativo. Como resultado, os usuários deverão fazer login na conta da Apple App Store.

No entanto, você pode se registrar na compra por volume da Apple para distribuir e gerenciar esses aplicativos usando o XenMobile. A compra por volume permite que os usuários baixem os aplicativos sem precisar entrar na conta da Apple App Store.

Algumas plataformas, como o Samsung SAFE e o Samsung Knox, têm requisitos especiais de licenciamento a atender antes de implantar esses recursos.

- **Requisitos de lista de permissão e lista de bloqueio:** você pode identificar aplicativos que não deseja que os usuários instalem ou usem. Criar uma lista de bloqueio define um evento de falta de conformidade. Depois, você pode configurar políticas para disparar quando o evento ocorrer. Por outro lado, um aplicativo pode ser aceitável para uso, mas pode cair na lista de bloqueio por algum motivo. Nesse caso, você pode adicionar o aplicativo a uma lista de permissão e indicar que o aplicativo é aceitável para uso, mas não é necessário. Além disso, lembre-se de

que os aplicativos pré-instalados em novos dispositivos podem incluir alguns aplicativos comumente usados que não fazem parte do sistema operacional. Esses aplicativos podem entrar em conflito com sua estratégia de lista de bloqueio.

Caso de uso

Uma organização de saúde planeja implantar o XenMobile para servir como uma solução MAM para seus aplicativos móveis. Aplicativos móveis são entregues a usuários corporativos e BYOD. A TI decide entregar e gerenciar os seguintes aplicativos:

Aplicativos móveis de produtividade: Aplicativos para iOS e Android fornecidos pela Citrix. Para obter detalhes, consulte [aplicativos móveis de produtividade](#).

Citrix Secure Hub: cliente usado por todos os dispositivos móveis para se comunicar com o XenMobile. Você envia por push parâmetros de segurança, configurações e aplicativos móveis para dispositivos móveis via Secure Hub. Dispositivos Android e iOS se registram no XenMobile através do Secure Hub.

Citrix Receiver: aplicativo móvel que permite que usuários de dispositivos móveis abram aplicativos hospedados pelo Citrix Virtual Apps.

GoToMeeting: um cliente de reunião on-line, compartilhamento de área de trabalho e videoconferência que permite que os usuários se encontrem com outros usuários de computador, clientes, consumidores ou colegas pela Internet em tempo real.

SalesForce1: o Salesforce1 permite que os usuários acessem o Salesforce a partir de dispositivos móveis e reúnam todos os aplicativos Chatter, CRM, personalizados e de negócios em uma experiência unificada para qualquer usuário do Salesforce.

RSA SecurID: token baseado em software para autenticação de dois fatores.

Aplicativos EpicCare: esses aplicativos fornecem aos profissionais de saúde acesso seguro e portátil a prontuários, listas de pacientes, agendamentos e mensagens.

Haiku: aplicativo móvel para telefones iPhone e Android.

Canto: aplicativo móvel para o iPad

Rover: aplicativos móveis para iPhone e iPad.

HDX: o Citrix Virtual Apps oferece aplicativos HDX.

- **Epic Hyperspace:** aplicativo cliente Epic para gerenciamento eletrônico de prontuários médicos.

ISV:

- **Vocera:** aplicativo móvel de mensagens e IP de voz compatível com HIPAA que amplia os benefícios da tecnologia de voz Vocera a qualquer hora, em qualquer lugar, através de smartphones iPhone e Android.

Apps internos:

- **HCMail:** aplicativo que ajuda a compor mensagens criptografadas, pesquisar catálogos de endereços em servidores de e-mail internos e enviar as mensagens criptografadas para os contatos usando um cliente de e-mail.

Aplicativos da web internos:

- **PatientRounding:** aplicativo da Web usado para registrar informações médicas do paciente por diferentes departamentos.
- **Outlook Web Access:** permite o acesso de email por meio de um navegador da web.
- **SharePoint:** usado para compartilhamento de arquivos e dados em toda a organização.

A tabela a seguir lista as informações básicas necessárias para a configuração do MAM.

Nome do aplicativo	Tipo de aplicativo	Integração do MAM SDK ou preparação do MDX	iOS	Android
Secure Mail	XenMobile App	Não para a versão 10.4.1 e posterior	Sim	Sim
Secure Web	XenMobile App	Não para a versão 10.4.1 e posterior	Sim	Sim
Citrix Files	XenMobile App	Não para a versão 10.4.1 e posterior	Sim	Sim
Secure Hub	Aplicativo público	N/D	Sim	Sim
Citrix Receiver	Aplicativo público	N/D	Sim	Sim
GoToMeeting	Aplicativo público	N/D	Sim	Sim
SalesForce1	Aplicativo público	N/D	Sim	Sim

RSA SecurID	Aplicativo público	N/D	Sim	Sim
Epic Haiku	Aplicativo público	N/D	Sim	Sim
Epic Canto	Aplicativo público	N/D	Sim	Não
Epic Rover	Aplicativo público	N/D	Sim	Não
Epic Hyperspace	Aplicativo HDX	N/D	Sim	Sim
Vocera	Aplicativo ISV	Sim	Sim	Sim
HCMail	Aplicativo interno	Sim	Sim	Sim
PatientRounding	Aplicativo Web	N/D	Sim	Sim
Outlook Web Access	Aplicativo Web	N/D	Sim	Sim
SharePoint	Aplicativo Web	N/D	Sim	Sim

A tabela a seguir lista os requisitos específicos que você pode consultar para configurar as políticas do MAM no XenMobile.

Nome do aplicativo	VPN necessária	Interação		Filtragem Proxy	Cerca geográfica	Mobile Apps SDK	Versão mínima do sistema operacional	
		(com aplicativos fora do con- têiner)	(de aplicativos fora do con- têiner)					
Secure Mail	S	Permitido seletivamente	Permitido	Obrigatório	N/D	Seletivar Obrigatório	N/D	Imposto
Secure Web	S	Permitido	Permitido	Obrigatório	N/D	Desnecessário	N/D	Imposto

Nome do aplicativo	VPN necessária	Interação (com aplicativos fora do contêiner)	Interação (de aplicativos fora do contêiner)	Filtragem Proxy	Licenciamento	Cerca	Mobile Apps SDK	Versão mínima do sistema operacional
						ge-ográ-fico		
Citrix Files	S	Permitido	Permitido	Obrigatório	N/D	Desnecessário	N/D	Imposto
Secure Hub	S	N/D	N/D	Desnecessário	Compra por volume	Desnecessário	N/D	Não aplicado
Citrix Receiver	S	N/D	N/D	Desnecessário	Compra por volume	Desnecessário	N/D	Não aplicado
GoToMeeting	N	N/D	N/D	Desnecessário	Compra por volume	Desnecessário	N/D	Não aplicado
SalesForce	N	N/D	N/D	Desnecessário	Compra por volume	Desnecessário	N/D	Não aplicado
RSA SecurID	N	N/D	N/D	Desnecessário	Compra por volume	Desnecessário	N/D	Não aplicado
Epic Haiku	S	N/D	N/D	Desnecessário	Compra por volume	Desnecessário	N/D	Não aplicado
Epic Canto	S	N/D	N/D	Desnecessário	Compra por volume	Desnecessário	N/D	Não aplicado
Epic Rover	S	N/D	N/D	Desnecessário	Compra por volume	Desnecessário	N/D	Não aplicado
Epic Hyper-space	S	N/D	N/D	Desnecessário	N/D	Desnecessário	N/D	Não aplicado
Vocera	S	Bloqueado	Bloqueado	Obrigatório	N/D	Obrigatório	Obrigatório	Imposto

Nome do aplicativo	VPN necessária	Interação		Filtragem Proxy	Cerca geográfica	Mobile Apps SDK	Versão mínima do sistema operacional
		(com aplicativos fora do con- tainer)	(de aplicativos fora do con- tainer)				
HCMail	S	Bloqueado	Bloqueado	Obrigatório	N/D	Obrigatório	Obrigatório
PatientRc ing	S	N/D	N/D	Obrigatório	N/D	Desneces	N/D
Outlook Web Access	S	N/D	N/D	Obrigatório	N/D	Desneces	N/D
SharePoi	S	N/D	N/D	Obrigatório	N/D	Desneces	N/D

Comunidades do usuário

November 30, 2020

Cada organização consiste em diversas comunidades de usuários que operam em diferentes funções. Essas comunidades de usuários executam tarefas e funções de escritório diferentes usando vários recursos fornecidos por meio dos dispositivos móveis dos usuários. Os usuários podem trabalhar em casa ou em escritórios remotos usando dispositivos móveis fornecidos por você. Ou, os usuários podem usar dispositivos móveis pessoais, o que permite que eles acessem ferramentas que estão sujeitas a determinadas regras de conformidade de segurança.

Com mais comunidades de usuários usando dispositivos móveis, o gerenciamento de mobilidade empresarial (EMM) se torna crítico para evitar o vazamento de dados e impor restrições de segurança organizacional. Para um gerenciamento eficiente e sofisticado de dispositivos móveis, você pode categorizar suas comunidades de usuários. Isso simplifica o mapeamento de usuários para recursos e garante que as políticas de segurança corretas sejam aplicadas aos usuários certos.

A categorização de comunidades de usuários pode incluir o uso dos seguintes componentes:

- Grupos e Unidades Organizacionais (OUs) do Active Directory

Os usuários adicionados a grupos de segurança específicos do Active Directory podem receber políticas e recursos, como aplicativos. A remoção de usuários dos grupos de segurança do Active Directory remove o acesso a recursos do XenMobile permitidos anteriormente.

- Usuários locais e grupos do XenMobile

Para usuários que não possuem uma conta no Active Directory, você pode criá-los como usuários locais do XenMobile. Você pode adicionar usuários locais a grupos de entrega e provisionar recursos a eles da mesma maneira que aos usuários do Active Directory.

- Grupos de entrega do XenMobile

Se vários grupos de usuários com diferentes níveis de permissão consumirem um único aplicativo, seria indicado criar grupos de entrega separados. Com grupos de entrega separados, você pode implantar duas versões separadas do mesmo aplicativo.

- Mapeamento de grupo de entrega e grupo de usuários

O grupo de entrega para mapeamentos de grupos do Active Directory pode ser um para um ou um para muitos. Atribuir políticas e aplicativos de base a um mapeamento de grupo de entrega de um para muitos. Atribuir políticas e aplicativos específicos a função a mapeamentos de grupo de entrega um para um.

- Mapeamento de Grupo de entrega e Recursos dos aplicativos

Atribuir aplicativos específicos a cada grupo de entrega.

- Mapeamento de Grupo de entrega e Recursos do MDM

Atribua aplicativos e recursos de gerenciamento de dispositivos específicos a cada grupo de entrega. Por exemplo, configure um grupo de entrega com qualquer destas combinações: tipos de aplicativos (públicos, HDX e assim por diante), aplicativos específicos por tipo de aplicativo, e recursos, como políticas de dispositivos e ações automatizadas.

O exemplo a seguir ilustra como as comunidades de usuários de uma organização de assistência médica são classificadas para o EMM.

Caso de uso

Neste exemplo, esta organização de assistência médica fornece recursos de tecnologia e acesso a vários usuários, incluindo funcionários e voluntários da rede e afiliados. A organização optou por implantar a solução EMM apenas para usuários não executivos.

Você pode dividir os cargos e funções dos usuários dessa organização em subgrupos, incluindo: clínico, não clínico e contratados. Um grupo selecionado de usuários recebe dispositivos móveis corporativos, enquanto outros podem acessar recursos limitados da empresa a partir de seus dispositivos pessoais (BYOD, traga seu próprio dispositivo). Para impor o nível apropriado de restrições

de segurança e impedir o vazamento de dados, a organização decidiu que a TI corporativa gerencia cada dispositivo registrado. Além disso, os usuários só podem registrar um único dispositivo.

Aa seções a seguir fornecem uma visão geral dos cargos e funções de cada subgrupo:

Clínico

- Enfermeiros
- Médicos (doutores, cirurgiões e outros)
- Especialistas (nutricionistas, flebotomistas, anestesistas, radiologistas, cardiologistas, oncologistas e outros)
- Médicos externos (médicos não empregados e trabalhadores de escritório que trabalham em escritórios remotos)
- Serviços de Saúde Domiciliar (trabalhadores de escritório e móveis realizando serviços médicos em visitas domiciliares ao paciente)
- Especialista em pesquisa (trabalhadores do conhecimento e usuários avançados em seis institutos de pesquisa que realizam pesquisas clínicas para encontrar respostas para problemas clínicos)
- Educação e Formação (enfermeiros, médicos e especialistas em educação e formação)

Não clínico

- Serviços compartilhados (funcionários de escritório executando várias funções de back-office, incluindo: RH, folha de pagamento, contas a pagar, serviço de cadeia de fornecimento e outros)
- Serviços Médicos (funcionários do escritório realizando várias soluções de gestão de saúde, serviços administrativos e processos de negócios para fornecedores, incluindo: Serviços Administrativos, Analytics e Business Intelligence, Sistemas de Negócios, Serviços ao Cliente, Finanças, Administração de Cuidados Gerenciados, Soluções de Acesso ao Paciente, Soluções de Ciclo de Receita e outros)
- Serviços de Suporte (trabalhadores de escritório realizando várias funções não clínicas, incluindo Administração de Benefícios, Integração Clínica, Comunicações, Gerenciamento de Compensação e Desempenho, Serviços de Instalações e Propriedade, Sistemas de Tecnologia de RH, Serviços de Informação, Auditoria Interna e Melhoria de Processos e outros)
- Programas filantrópicos (funcionários de escritório e móveis que realizam várias funções de apoio a programas filantrópicos)

Contratados

- Parceiros fabricantes e fornecedores (conectados no local e remotamente via VPN site-to-site, fornecendo várias funções de suporte não clínicas)

Com base nas informações anteriores, a organização criou as seguintes entidades. Para obter mais informações sobre grupos de entrega no XenMobile, consulte [Implantar recursos](#) na documentação do produto XenMobile.

Grupos e Unidades Organizacionais (OUs) do Active Directory

Para OU = Recursos do XenMobile

- OU = Clínico; Grupos =
 - XM-Enfermeiros
 - XM-Médicos
 - XM-Especialistas
 - XM-Médicos Externos
 - XM-Serviços de Saúde Domiciliar
 - XM-Especialista em Pesquisa
 - XM-Educação e Formação
- OU = Não clínico; Grupos =
 - XM-Serviços Compartilhados
 - XM-Serviços Médicos
 - XM-Serviços de Suporte
 - XM-Programas Filantrópicos

Usuários locais e grupos do XenMobile

ForGroup= Contratados, Usuários =

- Vendor1
- Vendor2
- Vendor3
- ... Vendor10

Grupos de entrega do XenMobile

- Clínico-Enfermeiros
- Clínico-Médicos
- Clínico-Especialistas
- Clínico-Médicos Externos
- Clínico-Serviços de Saúde Domiciliar
- Clínico-Especialista em Pesquisa
- Clínico-Educação e Formação
- Não clínicos-Serviços Compartilhados

- Não clínicos-Serviços Médicos
- Não clínicos-Serviços de Suporte
- Não clínicos-Programas Filantrópicos

Mapeamento de Grupo de entrega e Grupo de usuários

Grupos do Active Directory	Grupos de entrega do XenMobile
XM-Enfermeiros	Clínico-Enfermeiros
XM-Médicos	Clínico-Médicos
XM-Especialistas	Clínico-Especialistas
XM-Médicos Externos	Clínico-Médicos Externos
XM-Serviços de Saúde Domiciliar	Clínico-Serviços de Saúde Domiciliar
XM-Especialista em Pesquisa	Clínico-Especialista em Pesquisa
XM-Educação e Formação	Clínico-Educação e Formação
XM-Serviços Compartilhados	Não clínicos-Serviços Compartilhados
XM-Serviços Médicos	Não clínicos-Serviços Médicos
XM-Serviços de Suporte	Não clínicos-Serviços de Suporte
XM-Programas Filantrópicos	Não clínicos-Programas Filantrópicos

Mapeamento de Grupo de entrega e Recursos dos aplicativos

	Secure Mail	Secure Web	ShareFile	Citrix Receiver	SalesFor	RSA SecurID	EpicCare Haiku	Epic Hyper-space
Clínico-Enfermeiros	X	X	X					
Clínico-Médicos								
Clínico-Especialistas								

Clínico- Médicos Exter- nos	X	X		
Clínico- Serviços de Saúde Domi- ciliar	X	X		
Clínico- Especiali- em Pesquisa	X	X		
Clínico- Educação e For- mação			X	X
Não clínicos- Serviços Com- partil- hados			X	X
Não clínicos- Serviços Médi- cos			X	X
Não clínicos- Serviços de Su- porte	X	X	X	X

Não clínicos-Programas Fi-lantrópicos	X	X			X	X
Contrata	X	X	X	X	X	X

Mapeamento de Grupo de entrega e Recursos do MDM

	MDM: Política de código secreto	MDM: Restrições de dispositivos	MDM: Ações automatizadas	MDM: Política de WiFi
Clínico-Enfermeiros				X
Clínico-Médicos		X		
Clínico-Especialistas				
Clínico-Médicos Externos				
Clínico-Serviços de Saúde Domiciliar				
Clínico-Especialista em Pesquisa				
Clínico-Educação e Formação				
Não clínicos-Serviços Compartilhados				

Não
clínicos-Serviços
Médicos

Não
clínicos-Serviços
de Suporte

Não clínicos-
Programas
Filantrópicos

Contratados

X

Notas e considerações

- O XenMobile cria um grupo de entrega padrão chamado Todos os Usuários durante a configuração inicial. Se você não desabilitar esse grupo de entrega, todos os usuários do Active Directory terão direitos para se registrar no XenMobile.
- O XenMobile sincroniza usuários e grupos do Active Directory sob demanda usando uma conexão dinâmica com o servidor LDAP.
- Se um usuário fizer parte de um grupo que não esteja mapeado no XenMobile, esse usuário não poderá se registrar. Da mesma forma, se um usuário for membro de vários grupos, o XenMobile categoriza o usuário apenas como estando nos grupos mapeados para o XenMobile.
- Para tornar o registro no MDM obrigatório, defina a opção de **Registro Obrigatório** como **True** em **Propriedades do Servidor** no console XenMobile. Para obter detalhes, consulte [Propriedades do servidor](#).
- Para excluir um grupo de usuários de um grupo de entrega do XenMobile, exclua a entrada no banco de dados do SQL Server, em dbo.userlistgrps.

Cuidado:

Antes de executar esta ação, crie um backup do XenMobile e do banco de dados.

Sobre a Propriedade de dispositivo no XenMobile

Você pode agrupar usuários de acordo com o proprietário do dispositivo de um usuário. A propriedade do dispositivo inclui dispositivos de propriedade da empresa e dispositivos de propriedade do usuário, também conhecidos como BYOD (traga o seu próprio dispositivo). Você pode controlar

como os dispositivos BYOD se conectam à sua rede em dois locais no console XenMobile: nas Regras de implantação e nas propriedades do XenMobile Server na página **Configurações**. Para obter detalhes sobre regras de implantação, consulte [Implantar recursos](#) na documentação do XenMobile. Para obter detalhes sobre as propriedades do servidor, consulte [Propriedades do servidor](#) neste manual.

Ao definir as propriedades do servidor, você pode exigir que todos os usuários de BYOD aceitem o gerenciamento corporativo de seus dispositivos antes que eles possam acessar os aplicativos. Ou você pode conceder aos usuários acesso a aplicativos corporativos sem precisar gerenciar seus dispositivos.

Quando você define a propriedade do servidor **wsapi.mdm.required.flag** como **true**, o XenMobile gerencia todos os dispositivos BYOD, e qualquer usuário que recusar o registro não terá acesso aos aplicativos. Considere configurar o **wsapi.mdm.required.flag** como **true** em ambientes nos quais as equipes de TI corporativas precisam de alta segurança, além de uma experiência de usuário positiva durante o registro.

Se você deixar o **wsapi.mdm.required.flag** como **false**, que é a configuração padrão, os usuários poderão recusar o registro. No entanto, eles podem acessar aplicativos em seus dispositivos através da XenMobile Store. Considere configurar **wsapi.mdm.required.flag** como **false** em ambientes nos quais as restrições de privacidade, legais ou regulamentares não exigem gerenciamento de dispositivos, apenas gerenciamento de aplicativos corporativos.

Usuários com dispositivos que o XenMobile não gerencia podem instalar aplicativos através da XenMobile Store. Em vez de controles no nível do dispositivo, como apagamento seletivo ou completo, você controla o acesso aos aplicativos por meio de políticas de aplicativos. Algumas configurações de políticas exigem que o dispositivo verifique o XenMobile Server rotineiramente para confirmar que os aplicativos ainda têm permissão para serem executados.

Estratégia de email

January 22, 2021

O acesso seguro ao email de dispositivos móveis é um dos principais impulsionadores da iniciativa de gerenciamento de mobilidade de qualquer organização. Decidir sobre a estratégia de e-mail adequada é muitas vezes um componente-chave de qualquer design do XenMobile. O XenMobile oferece várias opções para acomodar diferentes casos de uso, com base na segurança, na experiência do usuário e nos requisitos de integração. Este artigo aborda o processo típico de decisão de design e as considerações para escolher a solução certa, desde a seleção do cliente até o fluxo de tráfego de correio.

Escolhendo seus clientes de e-mail

A seleção de clientes geralmente está no topo da lista do design geral da estratégia de email. Você pode escolher entre vários clientes: o Citrix Secure Mail, o correio nativo incluído em um determinado sistema operacional de plataforma móvel ou outros clientes de terceiros disponíveis nas lojas de aplicativos públicas. Dependendo de suas necessidades, você pode possivelmente oferecer suporte às comunidades de usuários com um único cliente (padrão) ou talvez seja necessário usar uma combinação de clientes.

A tabela a seguir descreve algumas considerações de design para as diferentes opções de cliente disponíveis:

Tópico	Secure Mail	Nativo (por exemplo, o iOS Mail)	Email de terceiros
XenMobile Edition mínimo	Avançado	MDM	MDM
Configuração	Perfis de conta do Exchange configurados por meio de uma política do MDX.	Perfis de conta do Exchange configurados por meio de uma política do MDM. O suporte para Android está limitado a: SAFE/KNOX e Android Enterprise. Todos os outros clientes são considerados clientes de terceiros.	Geralmente requer configuração manual pelo usuário.

Segurança	Seguro por design, proporcionando a mais alta segurança. Usa políticas de MDX com níveis de criptografia de dados adicionais. O Secure Mail é um aplicativo totalmente gerenciado por meio de uma política de MDX. Camada adicional de autenticação com o Citrix PIN.	Com base no conjunto de recursos do fornecedor/aplicativo. Fornece maior segurança. Usa configurações de criptografia de dispositivo (sem segurança por meio de políticas de MDX). Depende da autenticação no nível do dispositivo para acesso ao aplicativo.	Com base no conjunto de recursos do fornecedor/aplicativo. Fornece alta segurança.
Integração	Permite a interação com aplicativos gerenciados (MDX) por padrão. Abra URLs da Web com o Citrix Secure Web. Salve arquivos e anexe arquivos do Citrix Files. Entrar e digitar diretamente no GoToMeeting.	Só é possível interagir com outros aplicativos não gerenciados (não MDX) por padrão.	Só é possível interagir com outros aplicativos não gerenciados (não MDX) por padrão.
Implantação/licenciamento	Você pode enviar o Secure Mail pelo MDM diretamente de lojas de aplicativos públicas. Incluído no licenciamento XenMobile Advanced e Enterprise.	Aplicativo cliente incluído no sistema operacional da plataforma. Nenhum requisito de licenciamento adicional.	Pode enviar por meio do MDM, como um aplicativo corporativo ou diretamente de lojas de aplicativos públicas. Modelo de licenciamento associado/custos com base no fornecedor do aplicativo.

Suporte	Único suporte de fornecedor para o cliente e solução de EMM (Citrix). Informações de contato do suporte incorporado nos recursos de registro de depuração do Secure Hub/aplicativo. Um cliente para suporte.	Suporte definido pelo fornecedor (Apple/Google). Pode ser necessário oferecer suporte a diferentes clientes com base na plataforma do dispositivo.	Suporte definido pelo fornecedor. Um cliente para suportar, pressupondo-se que o cliente de terceiros é suportado em todas as plataformas de dispositivos gerenciados.
---------	--	--	--

Fluxo de tráfego de email e considerações de filtragem

Esta seção discute os três principais cenários e considerações de design relacionadas ao fluxo de tráfego de email (ActiveSync) no contexto do XenMobile.

Cenário 1: Exchange exposto

Ambientes que suportam clientes externos geralmente possuem serviços do Exchange ActiveSync expostos à Internet. Os clientes do Mobile ActiveSync se conectam por meio desse caminho externo por meio de um proxy reverso (por exemplo, Citrix ADC) ou por meio de um servidor de borda. Essa opção é necessária para o uso de clientes de email nativos ou de terceiros, tornando esses clientes a escolha popular para esse cenário. Embora não seja uma prática comum, você também pode usar o cliente do Secure Mail nesse cenário. Ao fazer isso, você se beneficia dos recursos de segurança oferecidos pelo uso de políticas de MDX e pelo gerenciamento do aplicativo.

Cenário 2: Encapsulado via Citrix ADC (micro VPN e STA)

Esse cenário é o padrão ao usar o cliente do Secure Mail, devido aos seus recursos de micro VPN. Nesse caso, o cliente do Secure Mail estabelece uma conexão segura com o ActiveSync via Citrix Gateway. Em essência, você pode considerar o Secure Mail como o cliente que se conecta diretamente ao ActiveSync pela rede interna. Os clientes da Citrix costumam padronizar o Secure Mail como o cliente móvel do ActiveSync preferido. Essa decisão é parte de uma iniciativa para evitar a exposição dos serviços do ActiveSync à Internet em um Exchange Server exposto, conforme descrito no primeiro cenário.

Somente os aplicativos com o MAM SDK habilitado ou preparados com MDX podem usar a função micro VPN. Esse cenário não se aplica a clientes nativos se você preparar com MDX. Mesmo que seja possível preparar clientes de terceiros com o MDX Toolkit, essa prática não é comum. O uso de clientes VPN em nível de dispositivo para permitir acesso com túnel para clientes nativos ou de terceiros provou ser uma solução incômoda e não viável.

Cenário 3: Serviços do Hosted Exchange na nuvem

Serviços do Hosted Exchange na nuvem, como o Microsoft Office 365, estão se tornando mais populares. No contexto do XenMobile, esse cenário pode ser tratado da mesma maneira que o primeiro cenário, porque o serviço ActiveSync também é exposto à Internet. Nesse caso, os requisitos do provedor de serviços de nuvem determinam as escolhas do cliente. As opções geralmente incluem suporte para a maioria dos clientes do ActiveSync, como o Secure Mail e outros clientes nativos ou de terceiros.

O XenMobile pode agregar valor em três áreas neste cenário:

- Clientes com políticas de MDX e gerenciamento de aplicativos com o Secure Mail
- Configuração do cliente com o uso de uma política de MDM em clientes de email nativos com suporte
- Opções de filtragem do ActiveSync com o uso do conector de Endpoint Management para Exchange ActiveSync

Considerações sobre filtragem de tráfego de email

Como na maioria dos serviços expostos à Internet, você deve proteger o caminho e fornecer filtragem para acesso autorizado. A solução XenMobile inclui dois componentes projetados especificamente para fornecer recursos de filtragem do ActiveSync para clientes nativos e de terceiros: conector Citrix Gateway para Exchange ActiveSync e conector de Endpoint Management para Exchange ActiveSync.

Conector Citrix Gateway para Exchange ActiveSync

O Citrix Gateway para Exchange ActiveSync fornece filtragem do ActiveSync no perímetro, usando o Citrix ADC como um proxy para o tráfego do ActiveSync. Como resultado, o componente de filtragem fica no caminho do fluxo de tráfego de mensagens, interceptando mensagens à medida que elas entram ou saem do ambiente. O conector Citrix Gateway para Exchange ActiveSync atua como intermediário entre o Citrix ADC e o XenMobile Server. Quando um dispositivo se comunica com o Exchange através do servidor virtual ActiveSync no Citrix ADC, o Citrix ADC executa uma chamada HTTP para o serviço do conector para Exchange ActiveSync. Esse serviço verifica o status do dispositivo com o XenMobile. Com base no status do dispositivo, o conector para Exchange ActiveSync responde ao Citrix ADC para permitir ou negar a conexão. Você também pode configurar regras estáticas para filtrar o acesso com base no usuário, agente e tipo de dispositivo ou ID.

Essa configuração permite que os serviços do Exchange ActiveSync sejam expostos à Internet com uma camada adicional de segurança para impedir o acesso não autorizado. Considerações de design incluem o seguinte:

- **Windows Server:** o componente conector para Exchange ActiveSync requer um Windows Server.
- **Conjunto de regras de filtragem:** o conector do Exchange ActiveSync foi projetado para filtragem com base no estado e nas informações do dispositivo, em vez de se basear nas informações do usuário. Embora você possa configurar regras estáticas para filtrar por ID do usuário, não há opções para filtragem com base na associação do grupo do Active Directory, por exemplo. Se houver um requisito para a filtragem de grupos do Active Directory, você poderá usar o conector Endpoint Management para Exchange ActiveSync.
- **Escalabilidade do Citrix ADC:** dado o requisito de fazer o proxy do tráfego do ActiveSync via Citrix ADC, a escalabilidade adequada da instância do Citrix ADC é crítica para suportar a carga de trabalho adicional de todas as conexões SSL do ActiveSync.
- **Cache Integrado do Citrix ADC:** a configuração do conector para Exchange ActiveSync no Citrix ADC usa a função Cache Integrado para armazenar em cache as respostas do conector para Exchange ActiveSync. Como resultado dessa configuração, o Citrix ADC não precisa emitir uma solicitação ao conector Citrix Gateway para Exchange ActiveSync para cada transação do ActiveSync em uma determinada sessão. Essa configuração também é crítica para um desempenho e escala adequados. O Cache Integrado está disponível com o Citrix ADC Platinum Edition, ou você pode licenciar o recurso separadamente para Enterprise Editions.
- **Políticas de filtragem personalizadas:** pode ser necessário criar políticas personalizadas do Citrix ADC para restringir determinados clientes do ActiveSync fora dos clientes móveis nativos padrão. Essa configuração requer conhecimento sobre solicitações HTTP do ActiveSync e criação de políticas de resposta do Citrix ADC.
- **Clientes Secure Mail:** o Secure Mail possui recursos de micro VPN que eliminam a necessidade de filtragem no perímetro. O cliente Secure Mail geralmente seria tratado como um cliente ActiveSync interno (confiável) quando conectado através do Citrix Gateway. Se for necessário suporte para clientes nativos e de terceiros (com o conector para Exchange ActiveSync) e Secure Mail, a Citrix recomenda que o tráfego do Secure Mail não flua pelo servidor virtual Citrix ADC usado para o conector para Exchange ActiveSync. Você pode realizar esse fluxo de tráfego via DNS e evitar que a política do Exchange ActiveSync afete os clientes Secure Mail.

Para obter um diagrama do conector Citrix Gateway para Exchange ActiveSync em uma implantação do XenMobile, consulte [Arquitetura de referência para implantações locais](#).

Conector de Endpoint Management para Exchange ActiveSync

O conector de Endpoint Management para Exchange ActiveSync é um componente do XenMobile que fornece filtragem do ActiveSync no nível de serviço do Exchange. Como resultado, a filtragem só

ocorre quando o email chega ao serviço do Exchange, e não quando entra no ambiente do XenMobile. O Mail Manager usa o PowerShell para consultar o Exchange ActiveSync em busca de informações sobre parceria de dispositivos e controle de acesso por meio de ações de quarentena de dispositivos. Essas ações colocam e retiram os dispositivos da quarentena com base nos critérios de regra do conector de Endpoint Management para Exchange ActiveSync. Semelhante ao conector Citrix Gateway para Exchange ActiveSync, o conector de Endpoint Management para Exchange ActiveSync verifica o status do dispositivo no XenMobile para filtrar o acesso com base na conformidade do dispositivo. Você também pode configurar regras estáticas para filtrar o acesso com base no tipo ou ID do dispositivo, na versão do agente e na associação do grupo do Active Directory.

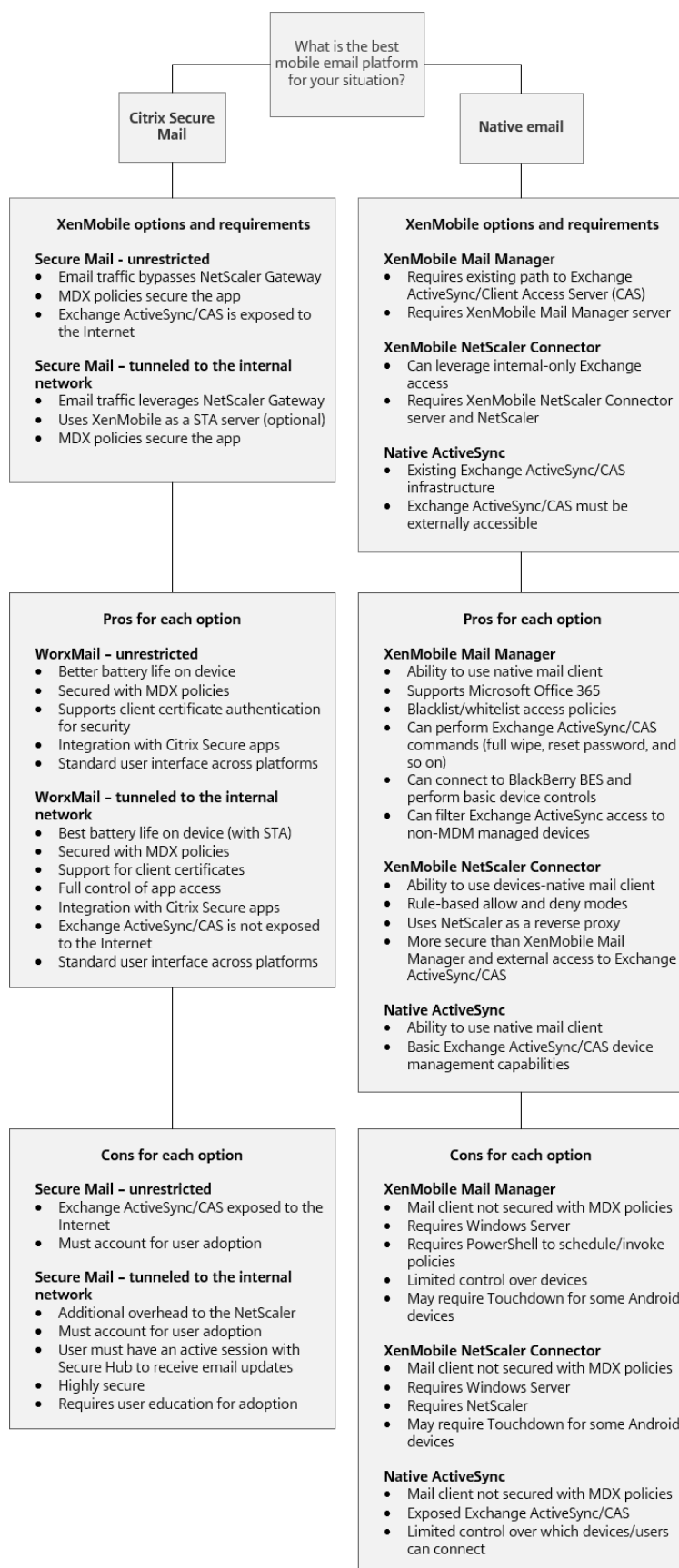
Esta solução não requer o uso do Citrix ADC. Você pode implantar o conector de Endpoint Management para Exchange ActiveSync sem alterar o roteamento do tráfego do ActiveSync existente. Considerações de design incluem:

- Windows Server: o componente conector de Endpoint Management para Exchange ActiveSync requer a implantação do Windows Server.
- Conjunto de regras de filtragem: assim como o conector Citrix Gateway para Exchange ActiveSync, o conector de Endpoint Management para Exchange ActiveSync inclui regras de filtragem para avaliar o estado do dispositivo. Além disso, o conector de Endpoint Management para Exchange ActiveSync também oferece suporte a regras estáticas para filtrar com base na associação do grupo do Active Directory.
- Integração com o Exchange: o conector de Endpoint Management para Exchange ActiveSync requer acesso direto ao servidor de acesso para cliente (CAS) do Exchange que hospeda a função do ActiveSync e controla as ações de quarentena do dispositivo. Esse requisito pode representar um desafio, dependendo da arquitetura do ambiente e da postura de segurança. É fundamental que você avalie essa exigência técnica antecipadamente.
- Outros clientes do ActiveSync: como o conector de Endpoint Management para Exchange ActiveSync está sendo filtrado no nível de serviço do ActiveSync, considere outros clientes do ActiveSync fora do ambiente do XenMobile. Você pode configurar as regras estáticas do conector de Endpoint Management para Exchange ActiveSync para evitar impacto não intencional em outros clientes do ActiveSync.
- Funções estendidas do Exchange: por meio da integração direta com o Exchange ActiveSync, o conector de Endpoint Management para Exchange ActiveSync permite que o XenMobile execute um apagamento do Exchange ActiveSync em um dispositivo móvel. O conector de Endpoint Management para Exchange ActiveSync também permite que o XenMobile acesse informações sobre dispositivos Blackberry e realize outras operações de controle.

Para obter um diagrama do conector de Endpoint Management para Exchange ActiveSync em uma implantação do XenMobile, consulte [Arquitetura de referência para implantações locais](#).

Árvore de decisão da plataforma de e-mail

A figura a seguir ajuda a distinguir os prós e contras entre o uso de soluções de email nativo ou Secure Mail na sua implantação do XenMobile. Cada escolha permite opções e requisitos associados ao XenMobile para habilitar o acesso ao servidor, rede e banco de dados. Os prós e contras incluem detalhes sobre considerações de segurança, política e interface do usuário.



Integração do XenMobile

July 10, 2020

Este artigo aborda o que considerar ao planejar como o XenMobile deve se integrar à sua rede e soluções existentes. Por exemplo, se você já estiver usando o Citrix ADC para Virtual Apps and Desktops:

- Você deve usar a instância existente do Citrix ADC ou uma nova instância dedicada?
- Você deseja integrar com o XenMobile os aplicativos HDX que são publicados usando o StoreFront?
- Você planeja usar o Citrix Files com o XenMobile?
- Você tem uma solução de controle de acesso da rede que deseja integrar ao XenMobile?
- Você implementa proxies da web para todo o tráfego de saída da sua rede?

Citrix ADC e Citrix Gateway

O Citrix Gateway é obrigatório nos modos XenMobile ENT e MAM. O Citrix Gateway oferece um caminho de micro VPN para acesso a todos os recursos corporativos e fornece um forte suporte de autenticação multifator. O balanceamento de carga do Citrix ADC é necessário para todos os modos de dispositivo do XenMobile Server:

- Se você tiver vários XenMobile Servers
- Ou, se o XenMobile Server estiver dentro da sua rede DMZ ou interna (e, portanto, o tráfego flui dos dispositivos para o Citrix ADC para o XenMobile)

Você pode usar instâncias existentes do Citrix ADC ou configurar instâncias novas para o XenMobile. As seções a seguir observam as vantagens e desvantagens de usar instâncias Citrix ADC dedicadas novas ou existentes.

O MPX compartilhado do Citrix ADC com um VIP Citrix Gateway criado para XenMobile

Vantagens:

- Usa uma instância comum do Citrix ADC para todas as conexões remotas Citrix: Citrix Virtual Apps and Desktops, VPN completa e VPN sem cliente.
- Usa as configurações existentes do Citrix ADC, como para autenticação de certificado e para acessar serviços como DNS, LDAP e NTP.
- Usa uma única licença de plataforma Citrix ADC.

Desvantagens:

- É mais difícil planejar a escala quando você lida com dois casos de uso diferentes no mesmo Citrix ADC.

- Às vezes, você precisa de uma versão específica do Citrix ADC para um caso de uso do Citrix Virtual Apps and Desktops. Essa mesma versão pode ter problemas conhecidos no XenMobile. Ou o XenMobile pode ter problemas conhecidos na versão do Citrix ADC.
- Se existir um Citrix Gateway, não será possível executar o assistente Citrix ADC for XenMobile uma segunda vez para criar a configuração do Citrix ADC para o XenMobile.
- Exceto quando licenças Platinum são usadas para o Citrix Gateway 11.1 ou posterior: as licenças de acesso de usuário instaladas no Citrix ADC e necessárias para conectividade VPN são agrupadas. Como essas licenças estão disponíveis para todos os servidores virtuais Citrix ADC, outros serviços além do XenMobile podem potencialmente consumi-las.

Instância dedicada do Citrix ADC VPX/MPX

Vantagens:

A Citrix recomenda o uso de uma instância dedicada do Citrix ADC.

- Mais fácil de planejar a escala e separa o tráfego do XenMobile de uma instância do Citrix ADC que pode já estar com restrição de recursos.
- Evita problemas quando o Citrix Virtual Apps and Desktops precisa de versões diferentes do software Citrix ADC. A recomendação geralmente é usar a última versão e compilação compatíveis do Citrix ADC para XenMobile.
- Permite a configuração do XenMobile do Citrix ADC através do assistente interno Citrix ADC for XenMobile.
- Separação virtual e física de serviços.
- Exceto quando as licenças Platinum são usadas para o Citrix Gateway 11.1 ou posterior: as licenças de acesso de usuário necessárias para o XenMobile só estão disponíveis para os serviços do XenMobile no Citrix ADC.

Desvantagens:

- Requer configuração de serviços extras no Citrix ADC para suportar a configuração do XenMobile.
- Requer outra licença da plataforma Citrix ADC. Licencie cada instância do Citrix ADC para Citrix Gateway.

Para obter informações sobre o que considerar ao integrar o Citrix ADC e o Citrix Gateway com cada modo de XenMobile Server, consulte [Integração com Citrix ADC e Citrix Gateway](#).

StoreFront

Se você tiver um ambiente Citrix Virtual Apps and Desktops, poderá integrar aplicativos HDX ao XenMobile usando o StoreFront. Quando você integra aplicativos HDX ao XenMobile:

- Os aplicativos ficam disponíveis para usuários registrados no XenMobile.

- Os aplicativos são exibidos na XenMobile Store juntamente com outros aplicativos móveis.
- O XenMobile usa o site legado PNAgent (serviços) no StoreFront.
- Quando o Citrix Receiver é instalado em um dispositivo, os aplicativos HDX começam a usar o Receiver.

StoreFront tem uma limitação de um site de serviços por instância de StoreFront. Suponha que você tenha várias lojas de aplicativos e queira segmentá-las de outro uso de produção. Nesse caso, a Citrix geralmente recomenda que você considere usar uma nova instância do StoreFront e site de serviço para o XenMobile.

As considerações incluem:

- Existem requisitos de autenticação diferentes para o StoreFront? O site de serviços StoreFront requer credenciais do Active Directory para logon. Os clientes que usam somente a autenticação baseada em certificado não podem enumerar aplicativos por meio do XenMobile usando o mesmo Citrix Gateway.
- Usar a mesma loja ou criar uma nova?
- Usar o mesmo servidor StoreFront ou um diferente?

As seções a seguir observam as vantagens e desvantagens de usar StoreFront separado ou combinado para Citrix Receiver e aplicativos móveis de produtividade.

Integrar sua instância StoreFront existente com o XenMobile Server

Vantagens:

- Mesma loja de aplicativos: nenhuma configuração adicional do StoreFront é necessária para o XenMobile, supondo que você use o mesmo VIP Citrix ADC para acesso HDX. Suponha que você decida usar a mesma loja e queira direcionar o acesso do Citrix Receiver a um novo VIP Citrix ADC. Nesse caso, adicione a configuração apropriada do Citrix Gateway ao StoreFront.
- Mesmo servidor StoreFront: usa a instalação e configuração do StoreFront existente.

Desvantagens:

- Mesma loja de aplicativos: qualquer reconfiguração do StoreFront para suportar cargas de trabalho de aplicativos e áreas de trabalho virtuais pode afetar adversamente o XenMobile também.
- Mesmo servidor StoreFront: em ambientes grandes, considere a carga adicional do uso do XenMobile do PNAgent para enumeração e inicialização do aplicativo.

Use uma nova instância dedicada do StoreFront para integração com o XenMobile Server

Vantagens:

- Nova loja de aplicativos: as alterações na configuração da loja StoreFront para o XenMobile não devem afetar as cargas de trabalho dos aplicativos e áreas de trabalho virtuais existentes.
- Novo servidor StoreFront: as alterações na configuração do servidor não devem afetar o fluxo de trabalho dos aplicativos e áreas de trabalho virtuais. Além disso, a carga fora do uso do XenMobile do PNAgent para enumeração e inicialização de aplicativos não deve afetar a escalabilidade.

Desvantagens:

- Nova loja de aplicativos: configuração da loja StoreFront.
- Novo servidor StoreFront: requer nova instalação e configuração do StoreFront.

Para obter mais informações, consulte [Aplicativos e áreas de trabalho virtuais através do Citrix Secure Hub](#) na documentação do XenMobile.

Citrix Content Collaboration e Citrix Files

O Citrix Files permite que os usuários acessem e sincronizem todos os seus dados de qualquer dispositivo. Com o Citrix Files, os usuários podem compartilhar dados com segurança com pessoas dentro e fora da organização. Se você integrar o Citrix Content Collaboration ao XenMobile Advanced Edition ou Enterprise Edition, o XenMobile poderá fornecer ao Citrix Files:

- Autenticação de logon único para usuários do XenMobile App.
- Provisionamento de conta de usuário baseado no Active Directory.
- Políticas abrangentes de controle de acesso.

Os usuários móveis podem se beneficiar do conjunto completo de recursos da conta Enterprise.

Como alternativa, você pode configurar o XenMobile para integração apenas com os conectores de zona de armazenamento. Através dos conectores de zona de armazenamento, o Citrix Files fornece acesso a:

- Documentos e pastas
- Compartilhamentos de arquivos de rede
- Nos sites do SharePoint: conjuntos de sites e bibliotecas de documentos.

Os compartilhamentos de arquivos conectados podem incluir as mesmas unidades iniciais de rede usadas nos ambientes Citrix Virtual Apps and Desktops. Você usa o console XenMobile para configurar a integração com Citrix Files ou conectores de zonas de armazenamento. Para obter mais informações, consulte [Uso do Citrix Files com XenMobile](#).

As seções a seguir observam as perguntas a serem feitas ao tomar decisões de design para o Citrix Files.

Integrar com arquivos Citrix ou apenas conectores de zona de armazenamento

Perguntas a serem feitas:

- Você precisa armazenar dados em zonas de armazenamento gerenciadas pela Citrix?
- Você deseja fornecer aos usuários recursos de compartilhamento e sincronização de arquivos?
- Deseja permitir que os usuários acessem arquivos no site do Citrix Files? Ou acessar conteúdo do Office 365 e conectores de nuvem pessoal de dispositivos móveis?

Decisão de design:

- Se a resposta a qualquer uma dessas perguntas for “sim”, integre com Citrix Files.
- Uma integração apenas com os conectores de zona de armazenamento fornece aos usuários do iOS acesso móvel seguro a repositórios de armazenamento locais existentes, como sites do SharePoint e compartilhamentos de arquivos em rede. Nessa configuração, você não define um subdomínio de Content Collaboration, provisiona usuários para o Citrix Files ou hospeda dados do Citrix Files. O uso de conectores de zonas de armazenamento com XenMobile está em conformidade com as restrições de segurança contra o vazamento de informações do usuário fora da rede corporativa.

Localização do servidor do controlador de zonas de armazenamento

Perguntas a serem feitas:

- Você precisa de armazenamento ou recursos locais, como conectores de zona de armazenamento?
- Se estiver usando recursos locais do Citrix Files, onde os controladores de zonas de armazenamento ficarão na rede?

Decisão de design:

- Determine se deseja localizar os servidores do controlador de zonas de armazenamento na nuvem do ShareFile, em seu sistema de armazenamento de locatário único no local ou no armazenamento na nuvem de terceiros suportados.
- Os controladores de zonas de armazenamento exigem certo acesso à Internet para se comunicar com o plano de controle do Citrix Files. Você pode se conectar de várias maneiras, incluindo acesso direto, configurações NAT/PAT ou configurações de proxy.

Conectores de zona de armazenamento

Perguntas a serem feitas:

- Quais são os caminhos de compartilhamento CIFS?
- Quais são os URLs do SharePoint?

Decisão de design:

- Determine se os controladores de zonas de armazenamento locais precisam acessar essas localizações.
- Devido à comunicação do conector de zona de armazenamento com recursos internos, como repositórios de arquivos, compartilhamentos CIFS e SharePoint, a Citrix recomenda que os controladores de zonas de armazenamento residam na rede interna por trás dos firewalls DMZ e protegidos pelo Citrix ADC.

Integração SAML com XenMobile Enterprise

Perguntas a serem feitas:

- A autenticação do Active Directory é necessária para o Citrix Files?
- O primeiro uso do aplicativo Citrix Files for XenMobile requer SSO?
- Existe um IdP padrão no seu ambiente atual?
- Quantos domínios são necessários para usar SAML?
- Existem vários aliases de email para usuários do Active Directory?
- Há alguma migração de domínio do Active Directory em andamento ou agendada para breve?

Decisão de design:

Os ambientes do XenMobile Enterprise podem optar por usar SAML como o mecanismo de autenticação do Citrix Files. As opções de autenticação são:

- Usar o XenMobile Server como o provedor de identidade (IdP) para SAML

Essa opção pode fornecer excelente experiência do usuário e automatizar a criação de conta do Citrix Files, bem como habilitar recursos SSO do aplicativo móvel.

- O servidor XenMobile é aprimorado para este processo: ele não exige a sincronização do Active Directory.
- Use a Ferramenta de gerenciamento de usuário do Citrix Files para provisionamento de usuários.
- Use um fornecedor de terceiros suportado como o IdP para SAML

Se você tiver um IdP existente e compatível e não precisar de recursos de SSO de aplicativos móveis, essa é a melhor opção para você. Essa opção também requer o uso da Ferramenta de gerenciamento de usuário do Citrix Files para provisionamento de contas.

O uso de soluções de IdP de terceiros, como ADFS, também pode fornecer recursos de SSO no lado do cliente do Windows. Não deixe de avaliar casos de uso antes de escolher seu IdP SAML do Citrix Files.

Além disso, para satisfazer ambos os casos de uso, você pode [configurar o ADFS e o XenMobile como um IdP duplo](#).

Aplicativos móveis

Perguntas a serem feitas:

- Qual aplicativo móvel Citrix Files você planeja usar (público, MDM, MDX)?

Decisão de design:

- Você distribui aplicativos móveis de produtividade a partir da Apple App Store e da Google Play Store. Com essa distribuição de lojas de aplicativos públicas, você obtém aplicativos preparados da página de downloads da Citrix.
- Se a segurança estiver baixa e você não precisar de containerização, o aplicativo Citrix Files público pode não ser adequado. Em um ambiente somente MDM, você pode entregar a versão MDM do aplicativo Citrix Files usando o XenMobile no modo MDM.
- Para obter mais informações, consulte [Aplicativos](#) e [Citrix Files para XenMobile](#).

Segurança, políticas e controle de acesso

Perguntas a serem feitas:

- Quais restrições você precisa para usuários de computadores, web e dispositivos móveis?
- Quais configurações de controle de acesso padrão você deseja para os usuários?
- Qual política de retenção de arquivo você planeja usar?

Decisão de design:

- O Citrix Files permite gerenciar permissões de funcionários e segurança de dispositivos. Para obter informações, consulte [Permissões de funcionários](#) e [Gerenciamento de dispositivos e aplicativos](#).
- Algumas configurações de segurança do dispositivo Citrix Files e políticas MDX controlam os mesmos recursos. Nesses casos, as políticas do XenMobile têm precedência, seguidas pelas configurações de segurança do dispositivo Citrix Files. Exemplos: se você desativar aplicativos externos no Citrix Files, mas ativá-los no XenMobile, os aplicativos externos serão desativados no Citrix Files. Você pode configurar os aplicativos para que o XenMobile não exija um PIN/código secreto, mas o aplicativo Citrix Files exija um PIN/código secreto.

Zonas de armazenamento padrões e restritas

Perguntas a serem feitas:

- Você precisa de zonas de armazenamento restritas?

Decisão de design:

- Uma zona de armazenamento padrão é destinada a dados não confidenciais e permite que os funcionários compartilhem dados com não funcionários. Esta opção suporta fluxos de trabalho que envolvem o compartilhamento de dados fora do seu domínio.

- Uma zona de armazenamento restrita protege os dados confidenciais: somente os usuários do domínio autenticados podem acessar os dados armazenados na zona.

Proxies da Web

O cenário mais provável para rotear o tráfego do XenMobile por meio de um proxy HTTP(S)/SOCKS é o seguinte: quando a sub-rede em que o XenMobile Server reside não tiver acesso à Internet para endereços IP da Apple, Google ou Microsoft. Você pode especificar as configurações do servidor proxy no XenMobile para rotear todo o tráfego da Internet para o servidor proxy. Para obter mais informações, consulte [Ativar servidores proxy](#).

A tabela a seguir descreve as vantagens e desvantagens do proxy mais comum usado com o XenMobile.

Opção	Vantagens	Desvantagens
Usar um proxy HTTP(S)/SOCKS com o XenMobile Server.	Nos casos em que as políticas não permitem conexões de saída da Internet da sub-rede do XenMobile Server: você pode configurar um proxy HTTP(S) ou SOCKS para fornecer conectividade com a Internet.	Se o servidor proxy falhar, a conectividade do APNs (iOS) ou do Firebase Cloud Messaging (Android) será interrompida. Como resultado, as notificações do dispositivo falham em todos os dispositivos iOS e Android.
Use um Proxy HTTP(S) com Secure Web.	Você pode monitorar o tráfego HTTP/HTTPS para garantir que a atividade da Internet esteja em conformidade com os padrões da sua organização.	Essa configuração exige que todo o tráfego da Secure Web Internet retorne para a rede corporativa antes de ser enviado de volta à Internet. Se a sua conexão com a Internet restringir a navegação: essa configuração pode afetar o desempenho da navegação na Internet.

Sua configuração de perfil da sessão do Citrix ADC para túnel dividido afeta o tráfego da seguinte maneira.

Quando o Túnel dividido do Citrix ADC está **desativado**:

- Se a política de **acesso à rede** MDX for **Com túnel para a rede interna**: todo o tráfego é forçado a usar o túnel micro VPN ou VPN sem cliente (cVPN) de volta ao Citrix Gateway.
- Configure os perfis/políticas de tráfego do Citrix ADC para o servidor proxy e associe-os ao VIP Citrix Gateway.

Importante:

Certifique-se de excluir o tráfego cVPN Secure Hub do proxy.

- Para obter mais informações, consulte [Tráfego do XenMobile Secure Hub através do servidor proxy no modo Secure Browse](#).

Quando o **Túnel dividido do Citrix ADC** está **ativado**:

- Quando os aplicativos são configurados com a política de **acesso à rede** MDX configurada como **Com túnel para a rede interna**: primeiro, os aplicativos tentam obter o recurso da Web diretamente. Se o recurso da Web não estiver publicamente disponível, esses aplicativos retornarão ao Citrix Gateway.
- Configure políticas e perfis de tráfego do Citrix ADC para o servidor proxy. Em seguida, associe essas políticas e perfis ao VIP Citrix Gateway.

Importante:

Certifique-se de excluir o tráfego cVPN Secure Hub do proxy.

Sua configuração do perfil de sessão do Citrix ADC para o **DNS Dividido** (em **Experiência do Cliente**) funciona de forma semelhante ao Túnel Dividido.

Com o **DNS Dividido** ativado e definido como **Ambos**:

- Primeiro, o cliente tenta resolver o FQDN localmente e, em seguida, retorna para o Citrix ADC para a resolução de DNS durante a falha.

Com o **DNS Dividido** definido como **Remoto**:

- A resolução de DNS ocorre apenas no Citrix ADC.

Com o **DNS Dividido** definido como **Local**:

- O cliente tenta resolver o FQDN localmente. O Citrix ADC não é usado para resolução de DNS.

Controle de acesso

As empresas podem gerenciar dispositivos móveis dentro e fora das redes. As soluções de Gerenciamento de Mobilidade Empresarial, como o XenMobile, são ótimas para fornecer segurança e controles para dispositivos móveis, independentemente da localização. No entanto, quando as combina com uma solução NAC (Network Access Control), você pode adicionar QoS e um controle mais refinado aos dispositivos internos da sua rede. Essa combinação permite estender a avaliação de segurança

do dispositivo XenMobile através da sua solução NAC. Sua solução NAC pode então usar a avaliação de segurança do XenMobile para facilitar e manipular decisões de autenticação.

Você pode usar qualquer uma dessas soluções para impor políticas NAC:

- Citrix Gateway
- Cisco Identity Services Engine (ISE)
- ForeScout

A Citrix não garante integração para outras soluções NAC.

As vantagens de uma integração de solução NAC com o XenMobile incluem o seguinte:

- Melhor segurança, conformidade e controle para todos os endpoints em uma rede corporativa.
- Uma solução NAC pode:
 - Detectar dispositivos no instante em que eles tentarem se conectar à sua rede.
 - Consultar o XenMobile para atributos do dispositivo.
 - Usar essas informações do dispositivo para determinar se deve permitir, bloquear, limitar ou redirecionar esses dispositivos. Essas decisões dependem das políticas de segurança que você decide impor.
- Uma solução NAC fornece aos administradores de TI uma visão de dispositivos não gerenciados e não compatíveis.

Para obter uma descrição dos filtros de conformidade com NAC suportados pelo XenMobile e uma visão geral da configuração, consulte [Controle de Acesso da Rede](#).

Requisitos para vários locais

April 23, 2020

Você pode desenvolver e configurar implantações do XenMobile que incluem vários locais para alta disponibilidade e recuperação de desastres. Este artigo fornece uma visão geral dos modelos de alta disponibilidade e recuperação de desastres usados nas implantações do XenMobile.

Alta disponibilidade

- Para nós de cluster do XenMobile, o Citrix ADC manipula o balanceamento de carga. Para obter mais informações, consulte [Configurar o clustering](#)
- Nós do XenMobile Server operam em uma configuração ativa/ativa.
- Nós adicionais do XenMobile Server são adicionados a um cluster de alta disponibilidade, pois a capacidade é necessária. Um nó pode manipular até aproximadamente 8.500 dispositivos de usuário (consulte [Escalabilidade e desempenho](#) para obter detalhes adicionais).

- A Citrix recomenda a configuração de “n+1” XenMobile Servers: um servidor para cada 8.500 dispositivos de usuários e um servidor extra para redundância.
- A Citrix recomenda alta disponibilidade para todas as instâncias do Citrix ADC, sempre que possível, para permitir que as configurações sejam sincronizadas com um segundo Citrix ADC.
- O par padrão de alta disponibilidade do Citrix ADC opera em uma configuração ativa/passiva.

Uma implantação típica do XenMobile de alta disponibilidade geralmente inclui:

- Duas instâncias Citrix ADC (VPX ou MPX). Se a plataforma Citrix ADC SDX for usada, a alta disponibilidade também deve ser considerada.
- Dois ou mais XenMobile Servers configurados com as mesmas configurações de banco de dados.

Recuperação de desastres

Você pode configurar o XenMobile para recuperação de desastre em dois datacenters com um datacenter ativo e um datacenter passivo. O Citrix ADC e o balanceamento de carga global do servidor (GSLB) são usados para criar um caminho de dados ativo/ativo para que a experiência do usuário seja a de uma configuração ativa/ativa.

Para recuperação de desastres, uma implantação do XenMobile inclui:

- Dois datacenters: cada um contém uma ou mais instâncias do Citrix ADC, servidores do XenMobile e bancos de dados do SQL Server.
- Um servidor GSLB para direcionar o tráfego para os datacenters. O servidor GSLB é configurado para a URL de registro do XenMobile e para a URL do Citrix Gateway que manipulam o tráfego para o site.
- Quando você usa o assistente Citrix ADC for XenMobile para configurar o Citrix Gateway, por padrão, o GSLB não está habilitado para resolver o tráfego para o servidor de registro do XenMobile e o tráfego para o Citrix Gateway, na rota para o servidor de balanceamento de carga do MAM; como resultado, etapas adicionais são necessárias. Para obter mais informações sobre como preparar e implementar essas etapas, consulte [Recuperação de desastres](#).
- SQL Servers em cluster de grupos de disponibilidade Always On.
- A latência entre os XenMobile Servers e o SQL Server deve ser menor que 5 ms.

Nota:

Os métodos de recuperação de desastres descritos neste manual fornecem apenas recuperação automatizada de desastres para a camada de acesso. Você deve iniciar manualmente todos os nós do XenMobile Server e o banco de dados do SQL Server no failover do site antes que os dispositivos possam se conectar ao XenMobile Server.

Integração com Citrix Gateway e Citrix ADC

December 22, 2020

Quando integrado ao XenMobile, o Citrix Gateway fornece um mecanismo de autenticação para o acesso de dispositivos remotos à rede interna para dispositivos MAM. A integração permite que os aplicativos móveis de produtividade se conectem a servidores corporativos na intranet através de uma micro VPN. A micro VPN é criada a partir dos aplicativos no dispositivo móvel para o Citrix Gateway. O Citrix Gateway oferece um caminho de micro VPN para acesso a todos os recursos corporativos e fornece um forte suporte de autenticação multifator.

O balanceamento de carga do Citrix ADC é necessário para todos os modos de dispositivo do XenMobile Server nestes casos:

- Se você tiver vários XenMobile Servers
- Ou se o XenMobile Server estiver dentro da sua rede DMZ ou interna (e, portanto, o tráfego flui dos dispositivos para o Citrix ADC para o XenMobile)

Requisitos de integração para os modos do XenMobile Server

Os requisitos de integração para o Citrix Gateway e Citrix ADC diferem com base nos modos do XenMobile Server: MAM, MDM e ENT.

MAM

Com o XenMobile Server no modo MAM:

- O **Citrix Gateway** é necessário. O Citrix Gateway oferece um caminho de micro VPN para acesso a todos os recursos corporativos e fornece um forte suporte de autenticação multifator.
- O **Citrix ADC** é recomendado para balanceamento de carga.

A Citrix recomenda implantar o XenMobile em uma configuração de alta disponibilidade, que requer um balanceador de carga na frente do XenMobile. Para obter detalhes, consulte [Sobre os modos MAM e MAM Legado](#).

MDM

Com o XenMobile Server no modo MDM:

- O Citrix Gateway não é necessário. Para implantações de MDM, a Citrix recomenda o Citrix Gateway para VPN de dispositivo móvel.

- O Citrix ADC é recomendado para segurança e balanceamento de carga.

A Citrix recomenda que você implemente um dispositivo Citrix ADC na frente do XenMobile Server, para segurança e balanceamento de carga. Para implantações padrão com o XenMobile na DMZ, a Citrix recomenda o assistente do Citrix ADC for XenMobile juntamente com o balanceamento de carga do XenMobile no modo Ponte de SSL. Você também pode considerar a descarga de SSL para implantações nas quais:

- O XenMobile Server reside na rede interna em vez de na DMZ
- Ou sua equipe de segurança requer uma configuração de Ponte de SSL

A Citrix não recomenda expor o XenMobile Server à Internet por meio de NAT ou proxies de terceiros existentes ou balanceadores de carga para MDM. Essas configurações representam um risco potencial de segurança, mesmo que o tráfego SSL seja terminado no XenMobile Server (Ponte de SSL).

Para ambientes de alta segurança, o Citrix ADC com a configuração padrão do XenMobile atende ou excede os requisitos de segurança.

Para ambientes de MDM com as mais altas necessidades de segurança, a terminação SSL no Citrix ADC permite a você inspecionar o tráfego no perímetro, enquanto mantém a criptografia SSL de ponta a ponta. Para obter mais informações, consulte [Requisitos de segurança](#). O Citrix ADC oferece opções para definir criptografias SSL/TLS e hardware SSL FIPS Citrix ADC.

ENT (MAM+MDM)

Com o XenMobile Server no modo ENT:

- O Citrix Gateway é necessário. O Citrix Gateway oferece um caminho de micro VPN para acesso a todos os recursos corporativos e fornece um forte suporte de autenticação multifator.

Quando o modo do XenMobile Server é ENT e um usuário opta pelo registro no MDM, o dispositivo opera no modo MAM Legado. No modo MAM legado, os dispositivos se registram usando o FQDN do Citrix Gateway. Para obter detalhes, consulte [Sobre os modos MAM e MAM Legado](#).

- O Citrix ADC é recomendado para balanceamento de carga. Para obter mais informações, consulte o ponto Citrix ADC anteriormente neste artigo em “MDM”.

Importante:

Para o registro inicial, o tráfego dos dispositivos do usuário é autenticado no XenMobile Server, independentemente de você configurar servidores virtuais de balanceamento de carga para Descarga de SSL ou Ponte de SSL.

Decisões de design

As seções a seguir resumem as várias decisões de design a serem consideradas ao planejar uma integração do Citrix Gateway com o XenMobile.

Licenciamento e edição

Detalhe da decisão:

- Qual edição do Citrix ADC você planeja usar?
- Você já aplicou licenças de plataforma ao Citrix ADC?
- Caso precise da funcionalidade MAM, você aplicou as licenças de acesso universal do Citrix ADC?

Orientação de design:

Certifique-se de aplicar as licenças apropriadas ao Citrix Gateway. Se você estiver usando o conector Citrix Gateway para Exchange ActiveSync, o armazenamento em cache integrado pode ser necessário. Portanto, você deve garantir que o Citrix ADC Edition apropriado esteja em uso.

Os requisitos de licença para ativar os recursos do Citrix ADC são os seguintes.

- O balanceamento de carga do XenMobile MDM requer uma licença de plataforma padrão do Citrix ADC no mínimo.
- O balanceamento de carga do Citrix Content Collaboration com o controlador de zonas de armazenamento requer uma licença de plataforma padrão do Citrix ADC no mínimo.
- A edição XenMobile Enterprise inclui as licenças universais necessárias do Citrix Gateway para o MAM.
- O balanceamento de carga do Exchange requer uma licença de plataforma Citrix ADC Platinum ou uma licença de plataforma Citrix ADC Enterprise com a adição de uma licença de Cache Integrado.

Versão do Citrix ADC para XenMobile

Detalhe da decisão:

- Qual versão o Citrix ADC está executando no ambiente XenMobile?
- Você precisa de uma instância separada?

Orientação de design:

A Citrix recomenda o uso de uma instância dedicada do Citrix ADC para o seu servidor virtual Citrix Gateway. Certifique-se de que a versão e a compilação mínimas do Citrix ADC estejam em uso no ambiente XenMobile. Geralmente, o melhor é usar a última versão e compilação compatíveis do Citrix ADC for XenMobile. Se a atualização do Citrix Gateway afetar seus ambientes existentes, uma segunda instância dedicada para o XenMobile poderá ser apropriada.

Se você planeja compartilhar uma instância do Citrix ADC com XenMobile e outros aplicativos que usam conexões VPN, certifique-se de ter licenças de VPN suficientes para todos. Tenha em mente que os ambientes de teste e produção do XenMobile não podem compartilhar uma instância do Citrix ADC.

Certificados

Detalhe da decisão:

- Você exige um maior grau de segurança para registros e acesso ao ambiente XenMobile?
- O LDAP não é uma opção?

Orientação de design:

A configuração padrão para o XenMobile é autenticação de nome de usuário e senha. Para adicionar outra camada de segurança para registro e acesso ao ambiente do XenMobile, considere usar a autenticação baseada em certificado. Você pode usar certificados com LDAP para autenticação de dois fatores, fornecendo um maior grau de segurança sem precisar de um servidor RSA.

Se você não permitir LDAP e usar cartões inteligentes ou similar métodos, a configuração de certificados permite a você representar um cartão inteligente para o XenMobile. Em seguida, os usuários se registram usando um PIN exclusivo que o XenMobile gera para eles. Depois que o usuário puder acessar, o XenMobile cria e implanta o certificado usado para autenticar no ambiente XenMobile.

O XenMobile dá suporte a Lista de revogação de certificados (CRL) somente para uma Autoridade de Certificação terceira. Se você tiver configurado uma AC da Microsoft, o XenMobile usa o Citrix ADC para gerenciar a revogação. Quando você configura a autenticação baseada em certificado de cliente, decida se você precisa configurar a opção Lista de revogação de certificados (CRL) do Citrix ADC, **Ativar atualização automática da CRL**. Esta etapa garante que o usuário de um dispositivo registrado no MAM apenas não possa autenticar usando um certificado existente no dispositivo. O XenMobile emite novamente um novo certificado porque ele não impede que um usuário gere um certificado de usuário se um tiver sido revogado. Essa opção aumenta a segurança de entidades PKI quando a CRL verifica entidades PKI expiradas.

Topologia de rede

Detalhe da decisão:

- Qual topologia Citrix ADC é necessária?

Orientação de design:

A Citrix recomenda o uso de uma instância do Citrix ADC para XenMobile. No entanto, você pode não querer tráfego indo de dentro da rede interna para a DMZ. Nesse caso, considere a configuração de uma instância extra do Citrix ADC. Use uma instância do Citrix ADC para usuários internos e uma para

usuários externos. Quando os usuários alternam entre as redes interna e externa, o cache de registros DNS pode resultar em um aumento nas solicitações de logon do Secure Hub.

O XenMobile não suporta o salto duplo do Citrix Gateway.

VIPs Citrix Gateway dedicados ou compartilhados

Detalhe da decisão:

- No momento, você usa o Citrix Gateway para Virtual Apps and Desktops?
- Você planeja que o XenMobile use o mesmo Citrix Gateway que o Virtual Apps and Desktops?
- Quais são os requisitos de autenticação para ambos os fluxos de tráfego?

Orientação de design:

Quando seu ambiente Citrix inclui o XenMobile, além do Virtual Apps and Desktops, você pode usar a mesma instância do Citrix ADC e o servidor virtual Citrix Gateway para ambos. Devido a possíveis conflitos de versão e isolamento do ambiente, instâncias dedicadas do Citrix ADC e do Citrix Gateway são recomendadas para cada ambiente XenMobile. No entanto, se uma instância dedicada do Citrix ADC não for uma opção, a Citrix recomenda o uso de um servidor virtual Citrix Gateway dedicado para separar os fluxos de tráfego do Secure Hub. Essa configuração é no lugar da de um servidor virtual compartilhado entre o XenMobile e o Virtual Apps and Desktops.

Se você usar a autenticação LDAP, o Citrix Receiver e o Secure Hub poderão se autenticar no mesmo Citrix Gateway sem problemas. Se você usar a autenticação baseada em certificado, o XenMobile enviará um certificado no contêiner MDX e o Secure Hub usará o certificado para se autenticar no Citrix Gateway. O Citrix Receiver é separado do Secure Hub e não pode usar o mesmo certificado do Secure Hub para se autenticar no mesmo Citrix Gateway.

Considere a seguinte solução alternativa, a qual permite que você use o mesmo FQDN para dois VIPs Citrix Gateway.

- Crie dois VIPs Citrix Gateway com o mesmo endereço IP. O VIP para Secure Hub usa a porta 443 padrão e o VIP para Virtual Apps and Desktops (que implanta o Receiver) usa a porta 444.
- Como resultado, um FQDN resolve para o mesmo endereço IP.
- Para essa alternativa, você pode configurar o StoreFront para retornar um arquivo ICA para a porta 444, em vez da porta padrão 443. Esta solução alternativa não requer que os usuários insiram um número de porta.

Tempos limite do Citrix Gateway

Detalhe da decisão:

- Como você deseja configurar os tempos limite do Citrix Gateway para o tráfego do XenMobile?

Orientação de design:

O Citrix Gateway inclui as configurações de Tempo limite da sessão e Tempo limite forçado. Para obter detalhes, consulte [Configurações recomendadas](#). Tenha em mente que existem diferentes valores de tempo limite para serviços em segundo plano, Citrix ADC e para acessar aplicativos enquanto estiver off-line.

Endereço IP do balanceador de carga XenMobile para MAM

Detalhe da decisão:

- Você está usando endereços IP internos ou externos para VIPs?

Orientação de design:

Em ambientes onde você pode usar endereços IP públicos para VIPs Citrix Gateway, atribuir o VIP e o endereço de balanceamento de carga do XenMobile dessa maneira causa falhas no registro.

Verifique se o VIP de balanceamento de carga usa um IP interno para evitar falhas de registro nesse cenário. Esse endereço IP virtual deve seguir o padrão RFC 1918 de endereços IP privados. Se você usar um endereço IP não privado para esse servidor virtual, o Citrix ADC não pode contatar o XenMobile Server com êxito durante o processo de autenticação. Para obter detalhes, consulte <https://support.citrix.com/article/CTX200430>.

Mecanismo de balanceamento de carga do MDM

Detalhe da decisão:

- Como o Citrix Gateway balanceará a carga de XenMobile Servers?

Orientação de design:

Use a Ponte SSL se o XenMobile estiver na DMZ. Use descarga de SSL, se for necessário para atender aos padrões de segurança, quando o XenMobile estiver na rede interna.

- Quando você faz o balanceamento de carga do XenMobile Server com VIPs Citrix ADC no modo Ponte de SSL, o tráfego da Internet flui diretamente para o XenMobile Server, onde as conexões terminam. O modo Ponte de SSL é o modo mais simples de configurar e solucionar problemas.
- Quando você faz o balanceamento de carga do XenMobile Server com VIPs Citrix ADC no modo Descarga de SSL, o tráfego da Internet flui diretamente para o Citrix ADC, onde as conexões terminam. Assim, o Citrix ADC estabelece novas sessões do Citrix ADC ao XenMobile Server. O modo de descarga SSL envolve complexidade extra durante a configuração e a solução de problemas.

Porta de serviço para balanceamento de carga do MDM com a descarga de SSL

Detalhe da decisão:

- Se você planeja usar o modo de descarga de SSL para o balanceamento de carga, qual porta o serviço de back-end usará?

Orientação de design:

Para Descarga de SSL, escolha a porta 80 ou 8443 da seguinte maneira:

- Use a porta 80 de volta ao XenMobile Server, para uma verdadeira descarga.
- A criptografia de ponta a ponta, ou seja, a uma nova criptografia do tráfego, não é suportada. Para obter detalhes, consulte o artigo do Suporte Citrix, [Arquiteturas suportadas entre o NetScaler e o XenMobile Server](#).

FQDN de registro

Detalhe da decisão:

- O que você planeja usar como o FQDN para registro e o VIP para instância/balanceamento de carga do XenMobile?

Orientação de design:

A configuração inicial do primeiro XenMobile Server em um cluster requer que você forneça o FQDN do XenMobile Server. Esse FQDN deve corresponder ao URL do VIP de MDM e ao URL do VIP do balanceador de carga de MAM interno. (Um registro de endereço interno do Citrix ADC resolve o VIP do balanceador de carga do MAM.) Para obter detalhes, consulte “FQDN de registro para cada modo de gerenciamento”, posteriormente neste artigo.

Além disso, você deve usar o mesmo certificado como a seguir:

- Certificado de ouvinte SSL do XenMobile
- Certificado VIP LB MAM interno
- Certificado VIP MDM (se estiver usando Descarga de SSL para VIP MDM)

Importante:

Depois de configurar o FQDN de registro, você não poderá alterá-lo. Um novo FQDN de registro exige uma nova compilação do banco de dados do SQL Server e do XenMobile Server.

Tráfego do Secure Web

Detalhe da decisão:

- Você planeja restringir o Secure Web à navegação na Web interna apenas?
- Você planeja habilitar o Secure Web para a navegação na Web interna e externa?

Orientação de design:

Se você planeja usar o Secure Web somente para navegação interna na Web, a configuração do Citrix Gateway será direta. O Secure Web deve acessar todos os sites internos por padrão. Talvez seja necessário configurar firewalls e servidores proxy.

Se você planeja usar o Secure Web para a navegação interna e externa, deverá ativar o SNIP para ter acesso de saída à Internet. A TI geralmente vê os dispositivos registrados (usando o contêiner MDX) como uma extensão da rede corporativa. Assim, a TI normalmente deseja que as conexões do Secure Web voltem ao Citrix ADC, passem por um servidor proxy e saiam para a Internet. Por padrão, o Secure Web usa um túnel VPN por aplicativo de volta à rede interna para todo o acesso à rede. O Citrix ADC usa configurações de túnel dividido.

Para ver uma discussão sobre conexões do Secure Web, consulte [Configurando conexões de usuário](#).

Notificações por Push para o Secure Mail

Detalhe da decisão:

- Você planeja usar notificações por push?

Orientação de design para iOS:

Sua configuração do Citrix Gateway pode incluir Secure Ticket Authority (STA), com túnel dividido desligado. O Citrix Gateway deve permitir o tráfego do Secure Mail para os URLs do serviço de ouvinte Citrix especificados em Notificações por Push para Secure Mail para iOS.

Orientação de design para o Android:

Use o Firebase Cloud Messaging (FCM) para controlar como e quando os dispositivos Android precisam se conectar ao XenMobile. Com o FCM configurado, qualquer ação de segurança ou comando de implantação dispara uma notificação por push para o Secure Hub para solicitar ao usuário que se reconecte ao XenMobile Server.

STAs HDX

Detalhe da decisão:

- Quais STAs usar se você planeja integrar o acesso ao aplicativo HDX?

Orientação de design:

As STAs HDX devem corresponder às STAs no StoreFront e devem ser válidas para o farm do Virtual Apps and Desktops.

Citrix Files e Citrix Content Collaboration

Detalhe da decisão:

- Você planeja usar controladores de zona de armazenamento no ambiente?
- Qual URL de VIP do Citrix Files você planeja usar?

Orientação de design:

Se você incluir controladores de zona de armazenamento em seu ambiente, certifique-se de configurar corretamente o seguinte:

- VPI do comutador do Citrix Files (usado pelo plano de controle do Citrix Files para se comunicar com os servidores do controlador de zona de armazenamento)
- VIPs de balanceamento de carga do Citrix Files
- Todas as políticas e perfis necessários

Para obter informações, consulte [a documentação do controlador de zonas de armazenamento](#).

IdP SAML

Detalhe da decisão:

- Se o SAML for necessário para o Citrix Files, você deseja usar o XenMobile como o IdP SAML?

Orientação de design:

A prática recomendada é integrar o Citrix Files ao XenMobile Advanced Edition ou ao XenMobile Enterprise Edition, uma alternativa mais simples para configurar a federação baseada em SAML. Quando você usa o Citrix Files com essas edições do XenMobile, o XenMobile fornece ao Citrix Files:

- Autenticação de logon único (SSO) de usuários de aplicativos móveis de produtividade
- Provisionamento de conta de usuário baseado no Active Directory
- Políticas abrangentes de controle de acesso

O console XenMobile permite que você execute a configuração do Citrix Files e monitore os níveis de serviço e o uso da licença.

Existem dois tipos de clientes Citrix Files: clientes do Citrix Files para XenMobile (também conhecidos como Citrix Files preparados) e clientes móveis do Citrix Files (também conhecidos como Citrix Files não preparados). Para entender as diferenças, consulte [Como os clientes do Citrix Files para XenMobile diferem dos clientes móveis do Citrix Files](#).

Você pode configurar o XenMobile e o Citrix Content Collaboration para usar o SAML para fornecer acesso SSO a:

- Aplicativos móveis Citrix Files
- Clientes do Citrix Files não preparados, como site, plug-in do Outlook ou clientes de sincronização

Para usar o XenMobile como o IdP SAML para o Citrix Files, verifique se as configurações adequadas foram definidas. Para obter detalhes, consulte [SAML para SSO com Citrix Files](#).

Conexões diretas do ShareConnect

Detalhe da decisão:

- Os usuários deverão acessar um computador host a partir de um computador ou dispositivo móvel que esteja executando o ShareConnect usando conexões diretas?

Orientação de design:

O ShareConnect permite que os usuários se conectem com segurança com seus computadores através iPads, tablets Android e telefones Android para acessar seus arquivos e aplicativos. Para ligações diretas, o XenMobile usa o Citrix Gateway para fornecer o acesso seguro a recursos de dados fora da rede local. Para ver detalhes de configuração, consulte [ShareConnect](#).

FQDN de registro para cada modo de gerenciamento

Modo de gerenciamento	FQDN de registro
Enterprise (MDM+MAM) com registro obrigatório no MDM	FQDN do XenMobile Server
Enterprise (MDM+MAM) com registro opcional no MDM	FQDN do XenMobile Server ou FQDN do Citrix Gateway
Apenas MDM	FQDN do XenMobile Server
Somente MAM (legado)	FQDN do Citrix Gateway
Somente MAM	FQDN do XenMobile Server

Resumo de Implantação

A Citrix recomenda que você use o assistente Citrix ADC for XenMobile para garantir a configuração adequada. Você pode usar o assistente apenas uma vez. Se você tiver várias instâncias do XenMobile, como ambientes de teste, desenvolvimento e produção, deverá configurar o Citrix ADC para os ambientes adicionais manualmente. Quando você tiver um ambiente de trabalho, anote as configurações antes de tentar configurar o Citrix ADC manualmente para o XenMobile.

A sua principal decisão quando usa o assistente é se usará HTTPS ou HTTP para comunicação com o XenMobile Server. O HTTPS fornece comunicação de back-end segura, já que o tráfego entre o Citrix ADC e o XenMobile é criptografado. A nova criptografia afeta o desempenho do XenMobile Server. O

HTTP oferece melhor desempenho do XenMobile Server. O tráfego entre o Citrix ADC e o XenMobile não é criptografado. As tabelas a seguir mostram os requisitos de porta HTTP e HTTPS para o Citrix ADC e XenMobile Server.

HTTPS

A Citrix normalmente recomenda a Ponte SSL para configurações do servidor virtual MDM do Citrix ADC. Para o uso da descarga de SSL do Citrix ADC com servidores virtuais MDM, o XenMobile suporta apenas a porta 80 como o serviço de backend.

Modo de gerenciamento	Método de balanceamento de carga Citrix ADC	Nova criptografia SSL	Porta do XenMobile Server
MDM	Ponte SSL	N/D	443, 8443
MAM	Descarga de SSL	Ativado	8443
Empresarial	MDM: Ponte SSL	N/D	443, 8443
Empresarial	MAM: Descarga de SSL	Ativado	8443

HTTP

Modo de gerenciamento	Método de balanceamento de carga Citrix ADC	Nova criptografia SSL	Porta do XenMobile Server
MDM	Descarga de SSL	Sem suporte	80
MAM	Descarga de SSL	Ativado	8443
Empresarial	MAM: Descarga de SSL	Sem suporte	80
Empresarial	MAM: Descarga de SSL	Ativado	8443

Para obter diagramas do Citrix Gateway em implantações XenMobile, consulte [Arquitetura de referência para implantações locais](#).

Considerações sobre SSO e proxy para aplicativos MDX

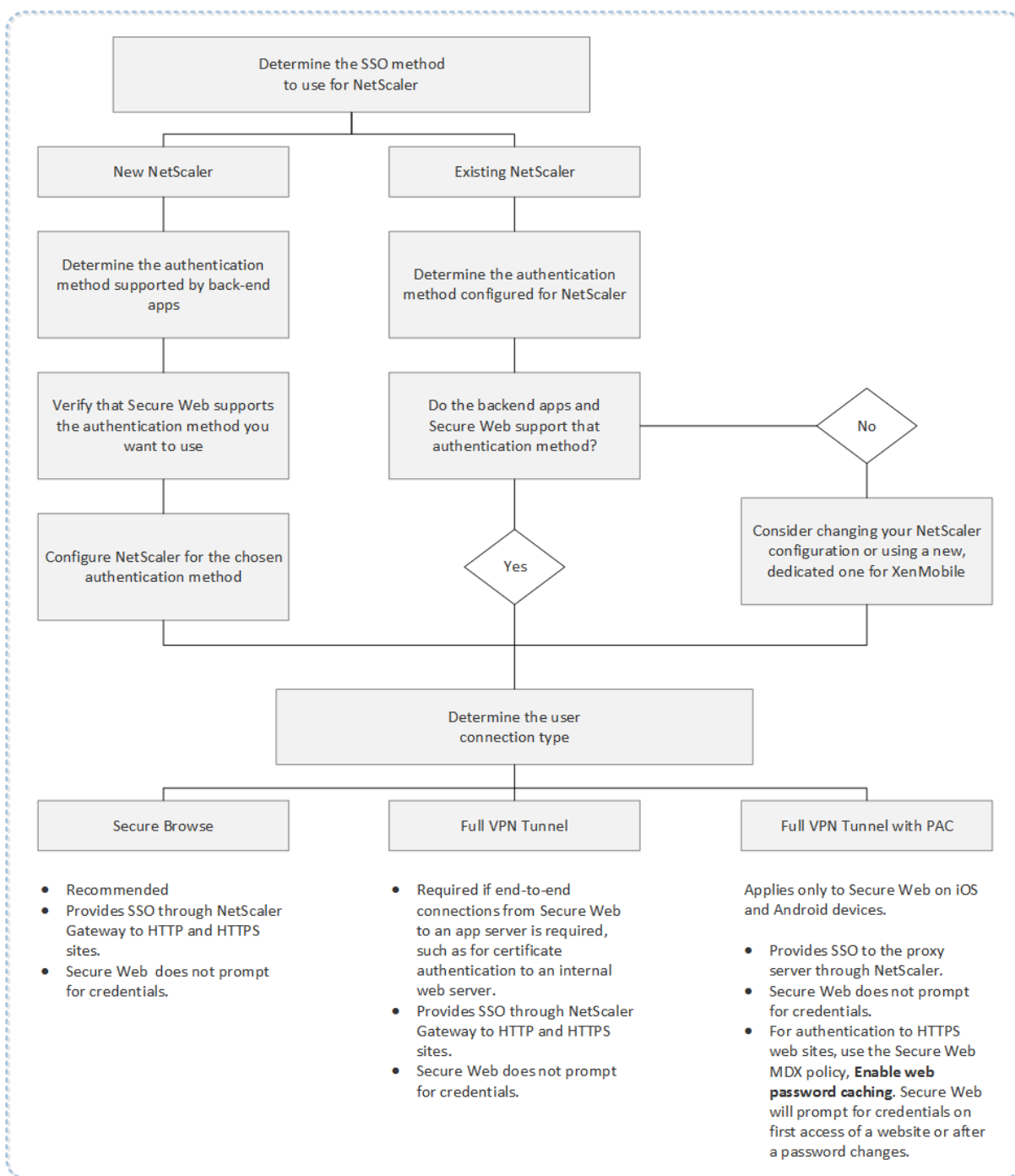
December 22, 2020

A integração do XenMobile com o Citrix ADC permite que você forneça aos usuários logon único (SSO) para todos os recursos HTTP/HTTPS de back-end. Dependendo dos seus requisitos de autenticação de SSO, você pode configurar conexões de usuário para um aplicativo MDX para usar uma das seguintes opções:

- Secure Browse, que é um tipo de VPN sem cliente
- Túnel Full VPN

Se o Citrix ADC não for a melhor maneira de fornecer o SSO em seu ambiente, você poderá configurar um aplicativo MDX com senhas locais em cache com base em políticas. Este artigo explora as diversas opções de SSO e proxy, com foco no Secure Web. Os conceitos se aplicam a outros aplicativos MDX.

O fluxograma a seguir resume o fluxo de decisão para conexões do usuário e SSO.



Métodos de Autenticação do Citrix ADC

Esta seção fornece informações gerais sobre os métodos de autenticação suportados pelo Citrix ADC.

Autenticação SAML

Quando você configura o Citrix ADC para SAML (Security Assertion Markup Language), os usuários podem se conectar a aplicativos da Web que suportam o protocolo SAML para conexões de logon único. O Citrix Gateway suporta o logon único do provedor de identidade (IdP) para aplicativos da Web SAML.

Configuração necessária:

- Configure o SAML SSO no perfil Citrix ADC Traffic.
- Configure o SAML IdP para o serviço solicitado.

Autenticação NTLM

Se o SSO para aplicativos da Web estiver ativado no perfil da sessão, o Citrix ADC executará a autenticação NTLM automaticamente.

Configuração necessária:

- Ative o SSO no perfil Citrix ADC Session ou no Citrix ADC Traffic.

Representação de Kerberos

O XenMobile oferece suporte apenas ao Kerberos for Secure Web. Quando você configura o Citrix ADC for Kerberos SSO, o Citrix ADC usa a representação quando uma senha de usuário está disponível para o Citrix ADC. Representação significa que o Citrix ADC usa credenciais de usuário para obter o tíquete necessário para obter acesso a serviços, como o Secure Web.

Configuração necessária:

- Configure a política de sessão “Worx” do Citrix ADC para permitir que identifique o realm Kerberos de sua conexão.
- Configure uma conta Kerberos Constrained Delegation (KCD) no Citrix ADC. Configure essa conta sem senha e vincule-a a uma política de tráfego no seu gateway XenMobile.
- Para esses e outros detalhes de configuração, consulte o blog da Citrix: [WorxWeb and Kerberos Impersonation SSO](#).

Kerberos Constrained Delegation

O XenMobile oferece suporte apenas ao Kerberos for Secure Web. Quando você configura o Citrix ADC for Kerberos SSO, o Citrix ADC usa a delegação restrita quando uma senha de usuário não está disponível para o Citrix ADC.

Com a delegação restrita, o Citrix ADC usa uma conta de administrador especificada para obter tíquetes em nome de usuários e serviços.

Configuração necessária:

- Configure uma conta KCD no Active Directory com as permissões necessárias e uma conta KCD no Citrix ADC.
- Ative o SSO no perfil Citrix ADC Traffic.
- Configure o site de backend para autenticação Kerberos.

Autenticação de preenchimento de formulário

Quando você configura o Citrix ADC para o logon único baseado em formulário, os usuários podem efetuar login uma única vez para acessar todos os aplicativos protegidos em sua rede. Este método de autenticação aplica-se a aplicativos que usam os modos Secure Browse ou Full VPN.

Configuração necessária:

- Configure o SSO baseado em formulário no perfil Citrix ADC Traffic.

Autenticação HTTP Digest

Se você habilitar o SSO para aplicativos da Web no perfil da sessão, o Citrix ADC executará a autenticação HTTP resumida automaticamente. Este método de autenticação aplica-se a aplicativos que usam os modos Secure Browse ou Full VPN.

Configuração necessária:

- Ative o SSO no perfil Citrix ADC Session ou no Citrix ADC Traffic.

Autenticação HTTP Basic

Se você habilitar o SSO para aplicativos da Web no perfil da sessão, o Citrix ADC executará a autenticação HTTP básica automaticamente. Este método de autenticação aplica-se a aplicativos que usam os modos Secure Browse ou Full VPN.

Configuração necessária:

- Ative o SSO no perfil Citrix ADC Session ou no Citrix ADC Traffic.

Secure Browse, Túnel Full VPN ou Túnel Full VPN com PAC

As seções a seguir descrevem os tipos de conexão do usuário para o Secure Web. Para obter mais informações, consulte este artigo da Secure Web na documentação do Citrix, [Configurando conexões de usuário](#).

Túnel Full VPN

Conexões que fazem túnel para a rede interna podem usar um túnel VPN completo. Use a política de modo Preferred VPN do Secure Web para configurara o túnel Full VPN. A Citrix recomenda o Túnel Full VPN para conexões que usam certificados de cliente ou SSL de ponta a ponta a um recurso na rede interna. O túnel Full VPN lida com qualquer protocolo sobre TCP. Você pode usar o túnel Full VPN com dispositivos Windows, Mac, iOS e Android.

No modo Túnel Full VPN, o Citrix ADC não tem visibilidade dentro de uma sessão HTTPS.

Navegação segura

Conexões que fazem túnel para a rede interna podem usar uma variação de uma VPN sem cliente, chamado de Secure Browse. O Secure Browse é a configuração padrão especificada para a política do Secure Web **Modo VPN preferencial**. A Citrix recomenda o Secure Browse para conexões que exigem um logon único (SSO).

No modo Secure Browse, o Citrix ADC divide a sessão HTTPS em duas partes:

- Do cliente para o Citrix ADC
- Do Citrix ADC para o servidor de recursos de back-end.

Dessa maneira, o Citrix ADC tem total visibilidade de todas as transações entre o cliente e o servidor, permitindo que ele forneça o SSO.

Você também pode configurar servidores proxy para o WorxWeb quando usado no modo navegação segura. Para obter detalhes, consulte o blog [XenMobile WorxWeb Traffic Through Proxy Server in Secure Browse Mode](#).

Túnel Full VPN com PAC

Você pode usar um arquivo PAC (Proxy Automatic Configuration) com uma implantação de túnel Full VPN para o Secure Web em dispositivos iOS e Android. O XenMobile é compatível com a autenticação de proxy fornecida pelo Citrix ADC. Um arquivo PAC contém regras que definem como os navegadores selecionam um proxy para acessar uma URL especificada. O arquivo de regras PAC pode especificar a manipulação tanto para sites internos quanto externos. O WorxWeb analisa o arquivo de regras PAC e envia as informações do servidor proxy para o Citrix Gateway. O Citrix Gateway não reconhece o arquivo PAC nem o servidor proxy.

Para autenticação de sites HTTPS, a política MDX do Secure Web, **Ativar armazenamento em cache de senha da web**, permite ao Secure Web autenticar e fornecer SSO para o servidor proxy por meio de MDX.

Túnel dividido do Citrix ADC

Ao planejar sua configuração de SSO e proxy, você também deve decidir se deseja usar o túnel dividido do Citrix ADC. A Citrix recomenda que você use o túnel dividido do Citrix ADC somente se necessário. Esta seção fornece uma visão de alto nível de como funciona o túnel dividido: o Citrix ADC determina o caminho de tráfego com base em sua tabela de roteamento. Quando o túnel dividido do Citrix ADC está ativado, o Secure Hub distingue o tráfego de rede interno (protegido) do tráfego da Internet. O Secure Hub faz essa determinação com base nos aplicativos de sufixo DNS e intranet. O Secure Hub então encapsula apenas o tráfego da rede interna através do túnel VPN. Quando o túnel dividido do Citrix ADC está desativado, todo o tráfego passa pelo túnel VPN.

- Se você preferir monitorar todo o tráfego devido a considerações de segurança, desative o túnel dividido do Citrix ADC. Como resultado, todo o tráfego passa pelo túnel VPN.
- Se você usar o túnel VPN completo com PAC, deve desativar o túnel dividido do Citrix Gateway. Se o túnel dividido estiver ativado e você tiver configurado um arquivo PAC, as regras do arquivo PAC substituem as regras de túnel dividido Citrix ADC. Um servidor proxy configurado em uma política de tráfego não substitui as regras de túnel dividido do Citrix ADC.

O padrão da política **Acesso à rede** no Secure Web é ser configurada como **Com túnel para a rede interna**. Com essa configuração, os aplicativos MDX usam as configurações do túnel dividido do Citrix ADC. O padrão da política **Acesso à rede** é diferente para alguns outros aplicativos móveis de produtividade.

O Citrix Gateway também possui um modo de túnel dividido Micro VPN reverse. Essa configuração suporta uma lista de exclusão de endereços IP que não são encapsulados no Citrix ADC. Em vez disso, esses endereços são enviados usando a conexão de internet do dispositivo. Para obter mais informações sobre o túnel dividido reverse, consulte a documentação do Citrix Gateway.

O XenMobile inclui a **Lista de exclusão de reverse split tunnel**. Para impedir que determinados sites se encapsulem em um túnel por meio do Citrix Gateway, adicione uma lista separada por vírgulas de nomes de domínio totalmente qualificados (FQDN) ou de sufixos DNS que se conectam usando a rede local. Esta lista se aplica apenas ao modo Secure Browse com o Citrix Gateway configurado para o túnel dividido reverse.

Autenticação

November 30, 2020

Em uma implantação do XenMobile, várias considerações entram em ação ao decidir como configurar a autenticação. Esta seção ajudará você a entender os vários fatores que afetam a autenticação e falará sobre:

- As principais políticas de MDX, as propriedades do cliente XenMobile e as configurações do Citrix Gateway envolvidas na autenticação.
- As formas como essas políticas, propriedades do cliente e configurações interagem.
- As compensações de cada escolha.

Este artigo também inclui três exemplos de configurações recomendadas para aumentar o grau de segurança.

Em termos gerais, uma segurança mais forte resulta em uma experiência de usuário não tão ideal, porque os usuários precisam se autenticar com mais frequência. Como você equilibra essas preocupações depende das necessidades e prioridades de sua organização. Após examinar as três configurações recomendadas, você entenderá melhor a interação das medidas de autenticação disponíveis para você e como melhor implantar seu próprio ambiente XenMobile.

Modos de Autenticação

Autenticação on-line: permite que os usuários entrem na rede do XenMobile. Requer uma conexão com a Internet.

Autenticação offline: acontece no dispositivo. Os usuários desbloqueiam o cofre seguro e têm acesso offline a itens, como emails baixados, sites em cache e anotações.

Métodos de Autenticação

Fator Único

LDAP: você pode configurar uma conexão no XenMobile a um ou mais diretórios, como o Active Directory, que sejam compatíveis com o protocolo LDAP. Esse é um método comumente usado para fornecer logon único (SSO) para ambientes da empresa. Você pode optar pelo Citrix PIN com senha em cache do Active Directory para melhorar a experiência do usuário com o LDAP e, ao mesmo tempo, fornecer a segurança de senhas complexas no registro, expiração de senha e bloqueio de conta.

Para obter mais detalhes, consulte [Domínio ou domínio mais autenticação de ticket de segurança](#).

Certificado de cliente: o XenMobile pode integrar-se a autoridades de certificação padrão do setor para usar certificados como o único método de autenticação on-line. O XenMobile fornece esse certificado após o registro do usuário, o que requer uma senha de uso único, URL de convite ou credenciais LDAP. Ao usar um certificado de cliente como o principal método de autenticação, um Citrix PIN é necessário em ambientes cliente somente certificado para proteger o certificado no dispositivo.

O XenMobile dá suporte à Lista de revogação de certificados (CRL) somente para uma Autoridade de Certificação terceira. Se você tiver configurado uma AC da Microsoft, o XenMobile usa o Citrix ADC para gerenciar a revogação. Quando você configura a autenticação baseada em certificado de cliente, decida se você precisa configurar a opção Lista de revogação de certificados (CRL) do Citrix ADC, Ativar

atualização automática da CRL. Esta etapa garante que o usuário de um dispositivo no modo somente MAM não possa autenticar usando um certificado existente no dispositivo; o XenMobile emite um novo certificado porque não impede que um usuário gere um certificado de usuário de um tiver sido revogado. Essa opção aumenta a segurança de entidades PKI quando a CRL verifica entidades PKI expiradas.

Para obter um diagrama que mostre a implantação necessária, se você planeja usar a autenticação baseada em certificado para os usuários ou se precisar usar sua autoridade de certificação corporativa para emitir certificados de dispositivo, consulte [Arquitetura de referência para implantações locais](#).

Dois Fatores

LDAP + Certificado cliente: No ambiente do XenMobile, essa configuração é a melhor combinação para a segurança e experiência do usuário, com as melhores possibilidades de SSO combinadas com a segurança fornecida pela autenticação de dois fatores no Citrix ADC. O uso de LDAP e certificado cliente fornece segurança com algo que os usuários sabem (suas senhas do Active Directory) e algo que eles têm (certificados cliente em seus dispositivos). O Secure Mail (e alguns outros aplicativos móveis de produtividade) pode configurar automaticamente e fornecer uma experiência aos usuários iniciais sem interrupções com autenticação de certificado cliente, com um ambiente de servidor de acesso cliente Exchange corretamente configurado. Para melhor usabilidade, você pode combinar essa opção com o Citrix PIN e armazenamento em cache de senha do Active Directory.

LDAP + token: essa configuração permite a configuração clássica de credenciais LDAP, além de uma senha de uso único, usando o protocolo RADIUS. Para melhor usabilidade, você pode combinar essa opção com o Citrix PIN e armazenamento em cache de senha do Active Directory.

Políticas Importantes, Configurações e Propriedades do Cliente Envolvidas na Autenticação

As seguintes políticas, configurações e propriedades do cliente entram em ação com as três configurações recomendadas a seguir:

Políticas de MDX

Código secreto de aplicativo: se o valor for **Ativado**, será necessário um Citrix PIN ou código secreto para desbloquear o aplicativo quando ele for iniciado ou reiniciado após um período de inatividade. O padrão é **Ativado**.

Para configurar o timer de inatividade de todos os aplicativos, defina o valor de INACTIVITY_TIMER em minutos no console XenMobile nas **Propriedades do cliente** da guia **Configurações**. O padrão é 15 minutos. Para desativar o timer de inatividade de forma que um aviso de PIN ou código secreto seja exibido somente quando o aplicativo for iniciado, defina o valor como zero.

Nota:

Se você selecionar Seguro offline para a política Chaves de criptografia, a política será ativada automaticamente.

Sessão online obrigatória de o valor for **Ativado**, o usuário deverá ter uma conexão com a rede corporativa e uma sessão ativa para poder acessar o aplicativo no dispositivo. Se **Desativado**, não será necessária uma sessão ativa para acessar o aplicativo no dispositivo. O padrão é **Desativado**.

Período máximo offline (horas): define o período máximo durante o qual um aplicativo pode ser executado sem reconfirmar o direito de aplicativo e atualizar as políticas do XenMobile. Quando você define o Período máximo offline, se o Secure Hub para iOS tiver um token válido do Citrix Gateway, o aplicativo recuperará novas políticas para aplicativos MDX do XenMobile sem interrupção para os usuários. Se o Secure Hub não tiver um token válido do Citrix ADC, os usuários deverão se autenticar por meio do Secure Hub para que as políticas de aplicativo sejam atualizadas. O token do Citrix ADC pode se tornar inválido devido a uma inatividade de sessão do Citrix Gateway ou a uma política de tempo limite de sessão forçada. Quando os usuários fazem logon no Secure Hub novamente, eles podem continuar a executar o aplicativo.

Os usuários são lembrados para fazer logon em 30, 15 e 5 minutos antes da expiração do período. Após a expiração, o aplicativo será bloqueado até que usuários façam logon. O valor padrão é **72 horas (3 dias)**. O período mínimo é de 1 hora.

Nota:

Tenha em mente que, em um cenário em que os usuários viajam com frequência e podem usar roaming internacional, o padrão de 72 horas (3 dias) pode ser muito curto.

Expiração de tíquete de serviços em segundo plano: O período de tempo que um serviço de rede em segundo plano continua válido. Quando o Secure Mail se conecta por meio do Citrix Gateway a um Exchange Server com ActiveSync, XenMobile emite um token que o Secure Mail usa para se conectar ao Exchange Server interno. Essa definição de configuração determina a duração que o Secure Mail pode usar o token sem exigir um novo token de autenticação e a conexão ao Exchange Server. Quando o limite de tempo expirar, os usuários devem fazer logon novamente para gerar um novo token. O padrão é **168 horas (7 dias)**. Quando esse tempo limite expirar, as notificações por email serão interrompidas.

Período de tolerância para sessão online obrigatória: determina por quantos minutos um usuário pode usar o aplicativo offline antes de a política Sessão online obrigatória impedir o uso do aplicativo (até que a sessão online seja validada). O padrão é 0 (sem período de tolerância).

Para obter informações sobre políticas de autenticação, consulte:

- Se você usar o SDK do MAM: [Visão geral do SDK MAM](#)
- Se você usar o MDX Service ou MDX Toolkit: [Políticas do MDX para iOS](#) e [Políticas do MDX para Android](#)

Propriedades do cliente XenMobile

Nota:

Propriedades do cliente são uma configuração global que se aplica a todos os dispositivos que se conectam ao XenMobile.

Citrix PIN: para uma experiência de login simplificada, você pode optar por ativar o Citrix PIN. Com o PIN, os usuários não precisam inserir outras credenciais repetidamente, como o nome de usuário e senha do Active Directory. Você pode configurar o PIN Citrix somente como uma autenticação offline autônoma ou combinar o PIN com o armazenamento de senha em cache do Active Directory para agilizar a autenticação e otimizar a usabilidade. Você configura o Citrix PIN em **Configurações > Cliente > Propriedades do Cliente** no console XenMobile.

Veja a seguir um resumo de algumas propriedades importantes. Para obter mais informações, consulte [Propriedades do cliente](#).

ENABLE_PASSCODE_AUTH

Nome de exibição: Ativar autenticação com PIN da Citrix

Essa chave permite que você ative a funcionalidade do PIN da Citrix. Com o PIN ou código secreto da Citrix, os usuários são solicitados a definir um PIN a ser usado em vez da senha do Active Directory. Você deve ativar essa configuração se **ENABLE_PASSWORD_CACHING** estiver ativado ou se o XenMobile estiver usando a autenticação de certificado.

Valores possíveis: true ou false

Valor padrão: false

ENABLE_PASSWORD_CACHING

Nome de exibição: Ativar armazenamento em cache de senha de usuário

Essa chave permite que a senha do Active Directory de usuários seja armazenada em cache localmente no dispositivo móvel. Quando você define essa chave como true, os usuários são solicitados a definir um PIN ou código secreto da Citrix. A chave ENABLE_PASSCODE_AUTH deve ser definida como true quando você define essa chave como **true**.

Valores possíveis: true ou false

Valor padrão: false

PASSCODE_STRENGTH

Nome de exibição: requisito de Força do PIN

Essa chave define a força do Citrix PIN ou do código secreto. Quando você alterar essa configuração, os usuários serão solicitados a definir um novo PIN ou código secreto da Citrix na próxima vez em que eles forem solicitados a autenticar.

Valores possíveis: Baixa, Média ou Forte

Valor padrão: Média

INACTIVITY_TIMER

Nome de exibição: Timer de Inatividade

Essa chave define o tempo, em minutos, durante o qual os usuários podem deixar seus dispositivos inativos para depois poder acessar um aplicativo sem que lhes seja solicitado um Citrix PIN ou código secreto. Para ativar essa configuração em um aplicativo MDX, você deve definir a configuração Código Secreto do Aplicativo como **Ativado**. Se a configuração de código secreto de aplicativo estiver definida como **Desativado**, os usuários serão redirecionados para o Secure Hub para efetuar uma autenticação completa. Quando você altera essa configuração, o valor entra em vigor na próxima vez em que houver solicitação para que os usuários se autentiquem. O padrão é 15 minutos.

ENABLE_TOUCH_ID_AUTH

Nome de exibição: Ativar Autenticação de Touch ID

Permite o uso do leitor de impressão digital (somente no iOS) para autenticação offline. A autenticação online ainda exigirá o método de autenticação principal.

ENCRYPT_SECRETS_USING_PASSCODE

Nome de exibição: Criptografar segredos usando o Código Secreto

Essa chave permite que dados confidenciais sejam armazenados no dispositivo móvel em um cofre secreto em vez de em um armazenamento nativo baseada na plataforma, como as chaves do iOS. Essa chave de configuração ativa a criptografia forte de artefatos de chave, mas também adiciona entropia do usuário (um código PIN aleatório, gerado pelo usuário, que somente o usuário conhece).

Valores possíveis: true ou false

Valor padrão: false

Configurações do Citrix ADC

Tempo limite da sessão: se você habilitar essa configuração, o Citrix Gateway desconectará a sessão se o Citrix ADC não detectar atividade de rede para o intervalo especificado. Essa configuração é imposta aos usuários que se conectam com o plug-in do Citrix Gateway, Citrix Receiver, Secure Hub ou por meio de um navegador da Web. O padrão é **1440** minutos. Se você definir esse valor como zero, a configuração será desativada.

Tempo limite forçado: se você habilitar essa configuração, o Citrix Gateway desconectará a sessão após o intervalo de tempo limite, independentemente de o que o usuário esteja fazendo. Quando o intervalo de tempo limite termina, não há nada que o usuário possa fazer para evitar a desconexão. Essa configuração é imposta aos usuários que se conectam com o plug-in do Citrix Gateway, Citrix Receiver, Secure Hub ou por meio de um navegador da Web. Se o Secure Mail estiver usando STA,

um modo especial do Citrix ADC, a configuração Tempo Limite Forçado não se aplicará às sessões do Secure Mail. O padrão é **1440** minutos. Se você deixar esse valor em branco, a configuração será desativada.

Para obter mais informações sobre configurações de tempo limite no Citrix Gateway, consulte a documentação do Citrix ADC.

Para obter mais informações sobre os cenários que solicitam que os usuários se autentiquem no XenMobile inserindo as credenciais em seus dispositivos, consulte [Aviso de autenticação de cenários](#).

Definições da configuração padrão

Essas configurações são os padrões fornecidos pelo:

- Assistente do NetScaler para XenMobile
- MAM SDK, MDX Service ou MDX Toolkit
- Console XenMobile

Configuração	Onde encontrar a configuração	Configuração padrão
Session time-out	Citrix Gateway	1440 minutos
Forçar tempo limite	Citrix Gateway	1440 minutos
Período máximo offline	Políticas de MDX	72 horas
Expiração de tíquete de serviços em segundo plano	Políticas de MDX	168 horas (7 dias)
Sessão online obrigatória	Políticas de MDX	Desativado
Período de tolerância para sessão online obrigatória	Políticas de MDX	0
Código secreto do aplicativo	Políticas de MDX	Ativado
Criptografar segredos usando código secreto	Propriedades do cliente XenMobile	false
Ativar autenticação do PIN do Citrix	Propriedades do cliente XenMobile	false
Requisito de força do PIN	Propriedades do cliente XenMobile	Média
Tipo de PIN	Propriedades do cliente XenMobile	Numérico
Ativar armazenamento em cache de senha	Propriedades do cliente XenMobile	false

Configuração	Onde encontrar a configuração	Configuração padrão
Timer de inatividade	Propriedades do cliente XenMobile	15
Ativar Autenticação de Touch ID	Propriedades do cliente XenMobile	false

Configurações recomendadas

Esta seção fornece exemplos de três configurações do XenMobile que abrangem desde a mais baixa segurança, com a experiência ideal do usuário, até a mais alta segurança, com a experiência do usuário mais intrusiva. Esses exemplos fornecem pontos de referência úteis para determinar onde, na escala, você deseja colocar sua própria configuração. Esteja ciente de que modificar essas configurações pode exigir que você altere outras configurações também. Por exemplo, o período máximo offline deve ser sempre menor que o tempo limite da sessão.

Altíssima segurança

Essa configuração oferece o mais alto nível de segurança, mas contém desvantagens de usabilidade significativas.

Configuração	Onde encontrar a configuração	Configuração recomendada	Impacto no comportamento
Session time-out	Citrix Gateway	1440	Os usuários inserem suas credenciais do Secure Hub apenas quando a autenticação on-line é necessária: a cada 24 horas.
Forçar tempo limite	Citrix Gateway	1440	A autenticação on-line será estritamente necessária a cada 24 horas. A atividade não prolonga a vida da sessão.

Período máximo offline	Políticas de MDX	23	Requer atualização da política todos os dias.
Expiração de tíquete de serviços em segundo plano	Políticas de MDX	72 horas	Tempo limite para STA, que permite sessões de longa duração sem um token de sessão do Citrix Gateway. No caso do Secure Mail, fazer com que o tempo limite da STA seja maior do que o tempo limite da sessão evita que as notificações de email parem sem avisar o usuário se ele não abra o aplicativo antes que a sessão expire.
Sessão online obrigatória	Políticas de MDX	Desativado	Garante uma conexão de rede válida e uma sessão do Citrix Gateway para usar aplicativos.
Período de tolerância para sessão online obrigatória	Políticas de MDX	0	Nenhum período de tolerância (se você ativou a Sessão on-line necessária).
Código secreto do aplicativo	Políticas de MDX	Ativado	Requer código secreto para aplicação.

Criptografar segredos usando código secreto	Propriedades do cliente XenMobile	true	Uma chave derivada da entropia do usuário protege o cofre.
Ativar autenticação do PIN do Citrix	Propriedades do cliente XenMobile	true	Ative o Citrix PIN para uma experiência de autenticação simplificada.
Requisito de força do PIN	Propriedades do cliente XenMobile	Forte	Requisitos de senha de alta complexidade.
Tipo de PIN	Propriedades do cliente XenMobile	Alfanumérico	O PIN é uma sequência alfanumérica.
Ativar armazenamento de senha em cache	Propriedades do cliente XenMobile	false	A senha do Active Directory não é armazenada em cache e o Citrix PIN será usado para autenticações offline.
Timer de inatividade	Propriedades do cliente XenMobile	15	Se o usuário não usar aplicativos MDX ou Secure Hub durante esse período, solicite a autenticação offline.
Ativar Autenticação de Touch ID	Propriedades do cliente XenMobile	false	Desativa o Touch ID para casos de uso de autenticação off-line no iOS.

Maior segurança

Uma abordagem mais intermediária, essa configuração exige que os usuários se autentiquem com mais frequência: a cada três dias, no máximo, em vez de sete, e reforcem a segurança. O aumento do número de autenticações bloqueia o contêiner com mais frequência, garantindo a segurança dos dados quando os dispositivos não estão em uso.

Configuração	Onde encontrar a configuração	Configuração recomendada	Impacto no comportamento
Session time-out	Citrix Gateway	4320	Os usuários inserem suas credenciais do Secure Hub apenas quando a autenticação on-line é necessária: a cada 3 dias.
Forçar tempo limite	Citrix Gateway	Sem valor	As sessões serão estendidas se houver alguma atividade.
Período máximo offline	Políticas de MDX	71	Requer atualização da política a cada 3 dias. A diferença de horário serve para permitir a atualização antes do tempo limite da sessão.

Expiração de tíquete de serviços em segundo plano	Políticas de MDX	168 horas	Tempo limite para STA, que permite sessões de longa duração sem um token de sessão do Citrix Gateway. No caso do Secure Mail, fazer com que o tempo limite da STA seja maior do que o tempo limite da sessão evita que as notificações de email parem sem avisar o usuário se ele não abra o aplicativo antes que a sessão expire.
Sessão online obrigatória	Políticas de MDX	Desativado	Garante uma conexão de rede válida e uma sessão do Citrix Gateway para usar aplicativos.
Período de tolerância para sessão online obrigatória	Políticas de MDX	0	Nenhum período de tolerância (se você ativou a Sessão on-line necessária).
Código secreto do aplicativo	Políticas de MDX	Ativado	Requer código secreto para aplicação.
Criptografar segredos usando código secreto	Propriedades do cliente XenMobile	false	Não exija entropia de usuário para criptografar o cofre.

Ativar autenticação do PIN do Citrix	Propriedades do cliente XenMobile	true	Ative o Citrix PIN para uma experiência de autenticação simplificada.
Requisito de força do PIN	Propriedades do cliente XenMobile	Média	Aplica regras de complexidade de senha média.
Tipo de PIN	Propriedades do cliente XenMobile	Numérico	PIN é uma sequência numérica.
Ativar armazenamento de senha em cache	Propriedades do cliente XenMobile	true	O PIN do usuário armazena em cache e protege a senha do Active Directory.
Timer de inatividade	Propriedades do cliente XenMobile	30	Se o usuário não usar aplicativos MDX ou Secure Hub durante esse período, solicite a autenticação offline.
Ativar Autenticação de Touch ID	Propriedades do cliente XenMobile	true	Ativa o Touch ID para casos de uso de autenticação off-line no iOS.

Alta Segurança

Essa configuração, a mais conveniente para os usuários, oferece segurança básica.

Configuração	Onde encontrar a configuração	Configuração recomendada	Impacto no comportamento
--------------	-------------------------------	--------------------------	--------------------------

Session time-out	Citrix Gateway	10080	Os usuários inserem suas credenciais do Secure Hub apenas quando a autenticação on-line é necessária: a cada 7 dias
Forçar tempo limite	Citrix Gateway	Sem valor	As sessões serão estendidas se houver alguma atividade.
Período máximo offline	Políticas de MDX	167	Requer atualização da política toda semana (a cada 7 dias). A diferença de horário serve para permitir a atualização antes do tempo limite da sessão.
Expiração de tíquete de serviços em segundo plano	Políticas de MDX	240	Tempo limite para STA, que permite sessões de longa duração sem um token de sessão do Citrix Gateway. No caso do Secure Mail, fazer com que o tempo limite da STA seja maior do que o tempo limite da sessão evita que as notificações de email parem sem avisar o usuário se ele não abra o aplicativo antes que a sessão expire.

Sessão online obrigatória	Políticas de MDX	Desativado	Garante uma conexão de rede válida e uma sessão do Citrix Gateway para usar aplicativos.
Período de tolerância para sessão online obrigatória	Políticas de MDX	0	Nenhum período de tolerância (se você ativou a Sessão on-line necessária).
Código secreto do aplicativo	Políticas de MDX	Ativado	Requer código secreto para aplicação.
Criptografar segredos usando código secreto	Propriedades do cliente XenMobile	false	Não exija entropia de usuário para criptografar o cofre.
Ativar autenticação do PIN do Citrix	Propriedades do cliente XenMobile	true	Ative o Citrix PIN para uma experiência de autenticação simplificada.
Requisito de força do PIN	Propriedades do cliente XenMobile	Baixo	Nenhum requisito de complexidade de senha
Tipo de PIN	Propriedades do cliente XenMobile	Numérico	PIN é uma sequência numérica.
Ativar armazenamento de senha em cache	Propriedades do cliente XenMobile	true	O PIN do usuário armazena em cache e protege a senha do Active Directory.
Timer de inatividade	Propriedades do cliente XenMobile	90	Se o usuário não usar aplicativos MDX ou Secure Hub durante esse período, solicite a autenticação offline.

Ativar Autenticação de Touch ID	Propriedades do cliente XenMobile	true	Ativa o Touch ID para casos de uso de autenticação off-line no iOS.
---------------------------------	-----------------------------------	------	---

Usando a autenticação aumentada

Alguns aplicativos podem exigir autenticação avançada (por exemplo, um fator de autenticação secundário, como um token ou tempos limites de sessão rígidos). Você controla esse método de autenticação por meio de uma política MDX. O método também requer um servidor virtual separado para controlar os métodos de autenticação (no mesmo ou em dispositivos Citrix ADC separados).

Configuração	Onde encontrar a configuração	Configuração recomendada	Impacto no comportamento
Citrix Gateway alternativo	Políticas de MDX	Requer o FQDN e a porta do dispositivo Citrix ADC secundário.	Permite a autenticação avançada controlada pelas políticas de sessão e autenticação do dispositivo do Citrix ADC secundário.

Se um usuário abrir um aplicativo que efetua logon na instância alternativa do Citrix Gateway, todos os outros aplicativos usarão essa instância do Citrix Gateway para se comunicar com a rede interna. A sessão só voltará para a instância do Citrix Gateway de segurança inferior quando a sessão expirar na instância do Citrix Gateway com segurança avançada.

Usando a sessão online obrigatória

Para determinados aplicativos, como o Secure Web, uma sugestão seria você garantir que os usuários executem um aplicativo somente quando tiverem uma sessão autenticada e enquanto o dispositivo estiver conectado a uma rede. Essa política aplica essa opção e permite um período de tolerância para que os usuários possam concluir seu trabalho.

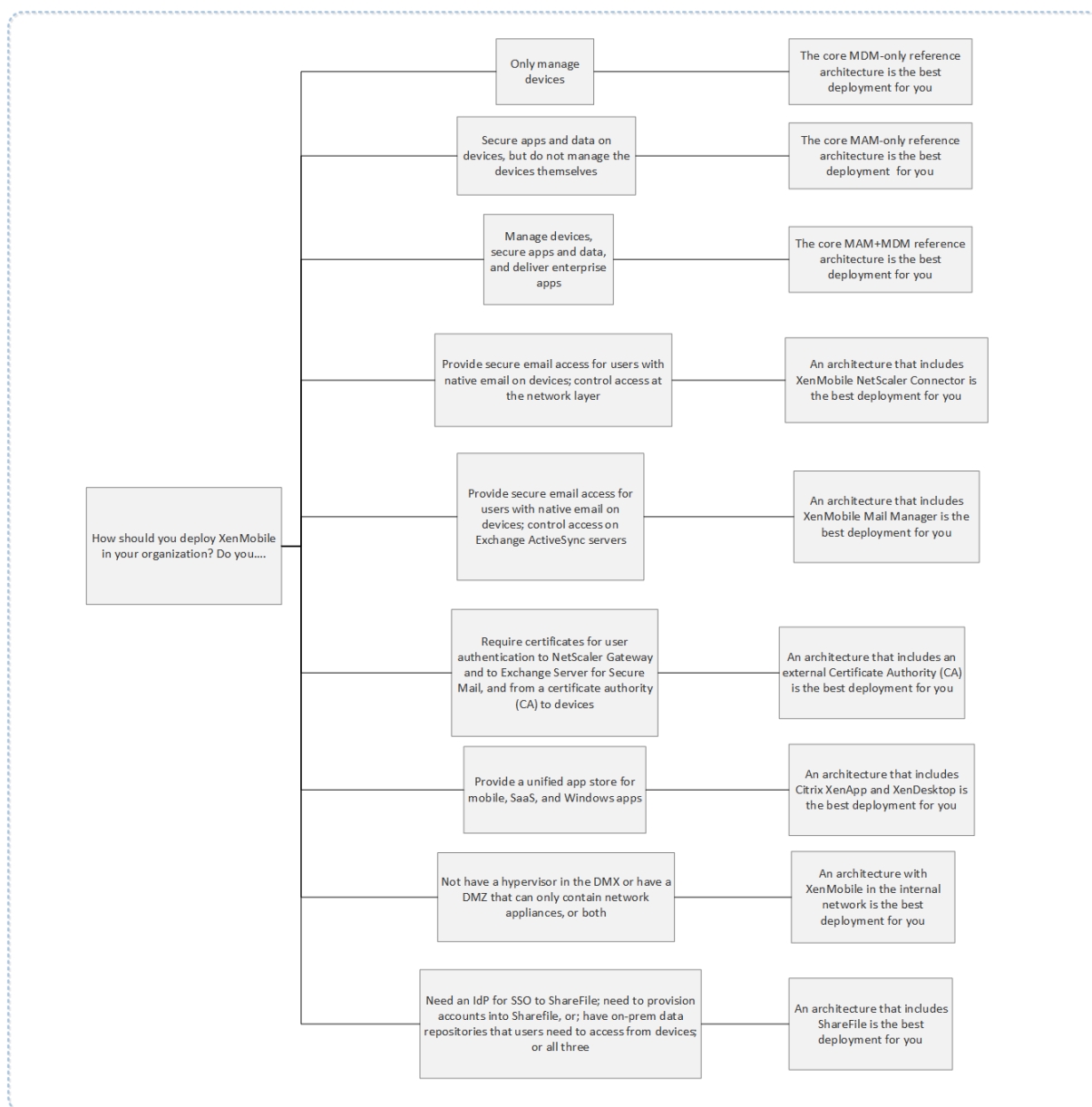
Configuração	Onde encontrar a configuração	Configuração recomendada	Impacto no comportamento
Sessão online obrigatória	Políticas de MDX	Ativado	Garante que o dispositivo esteja on-line e tenha um token de autenticação válido.
Período de tolerância para sessão online obrigatória	Políticas de MDX	15	Permite um período de tolerância de 15 minutos antes que o usuário não possa mais usar aplicativos

Arquitetura de referência para implantações locais

April 23, 2020

As figuras neste artigo ilustram as arquiteturas de referência para a implantação do XenMobile nas instalações locais. Os cenários de implantação incluem somente MDM, somente MAM e MDM+MAM como as principais arquiteturas, bem como aquelas que incluem componentes, como o SNMP Manager, conector Citrix Gateway para Exchange ActiveSync, conector de Endpoint Management para Exchange ActiveSync e aplicativos e áreas de trabalho virtuais. As figuras mostram os componentes mínimos necessários para o XenMobile.

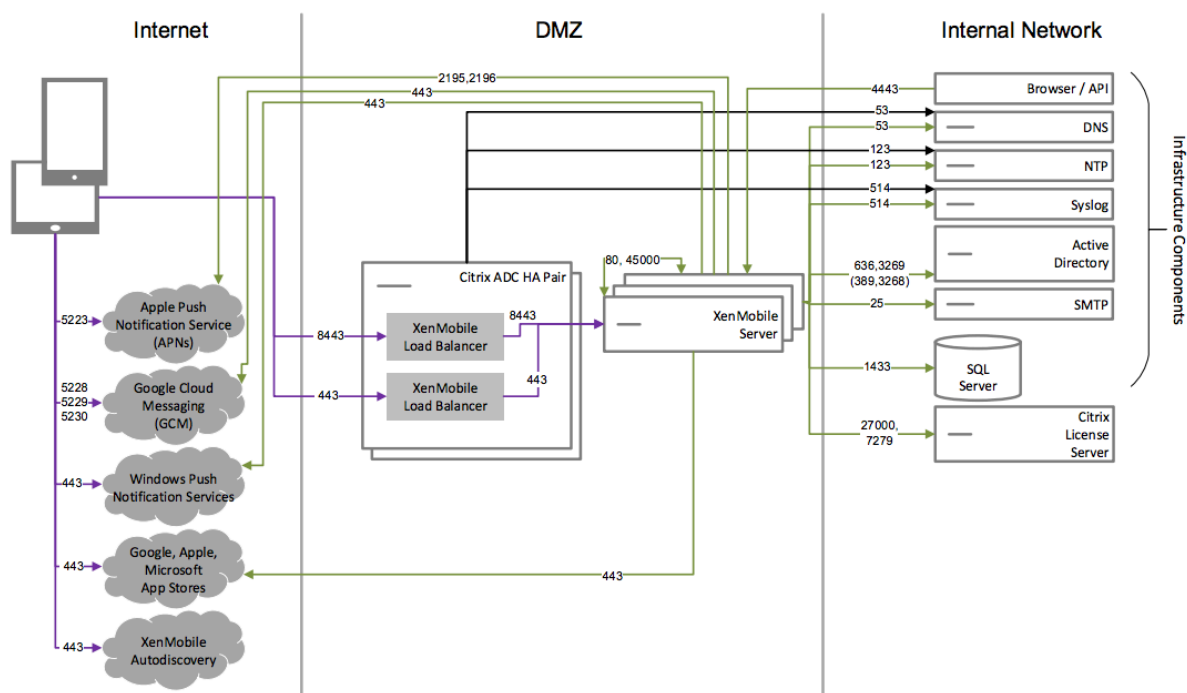
Use este gráfico como um guia geral para suas decisões de implantação.



Nas figuras, os números dos conectores representam portas que você deve abrir para permitir as conexões entre os componentes. Para obter uma lista completa de portas, consulte [Requisitos de porta](#) na documentação do XenMobile.

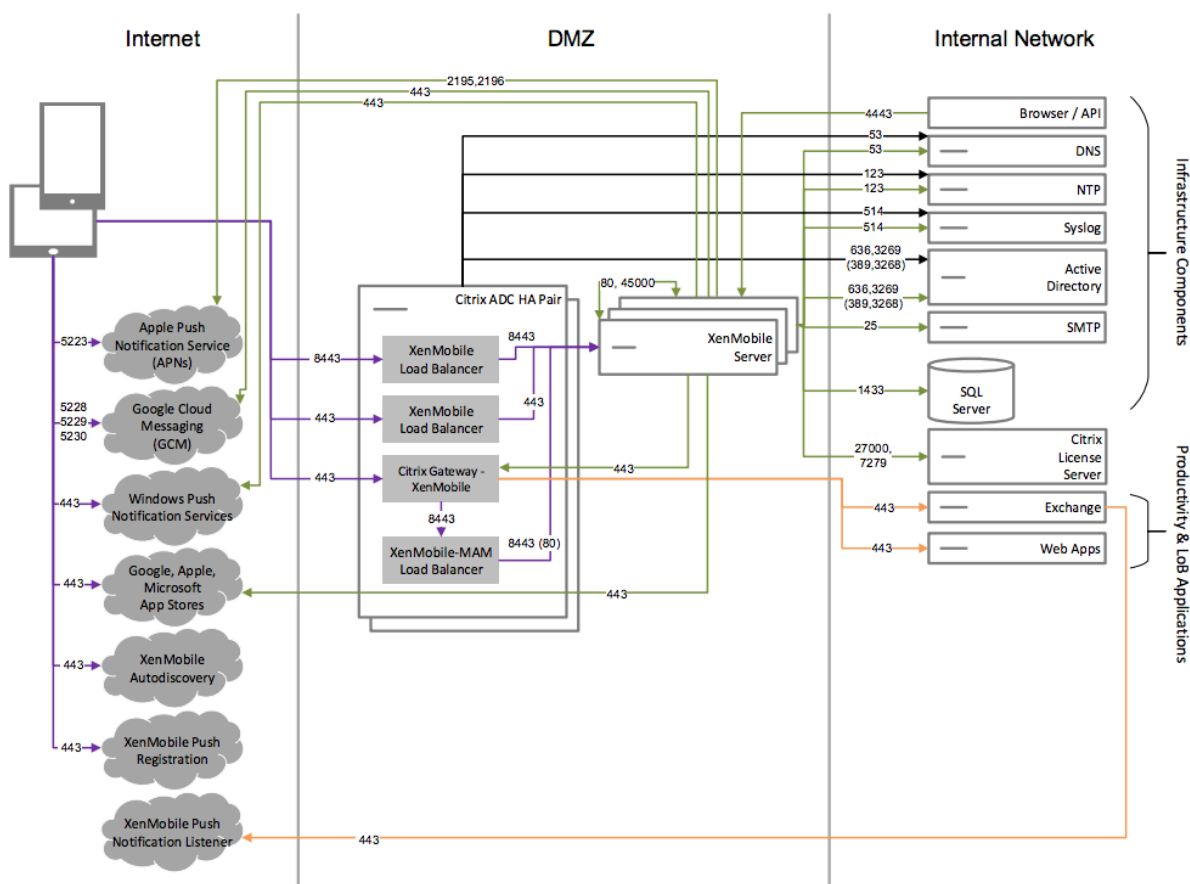
Arquitetura de referência somente MDM principal

Implante essa arquitetura se você planeja usar somente os recursos MDM do XenMobile. Por exemplo, você precisa gerenciar um dispositivo emitido pela empresa por meio do MDM para implantar políticas de dispositivo e aplicativos, além de recuperar os inventários de ativos e ser capaz de realizar ações em dispositivos, como um apagamento de dispositivo.



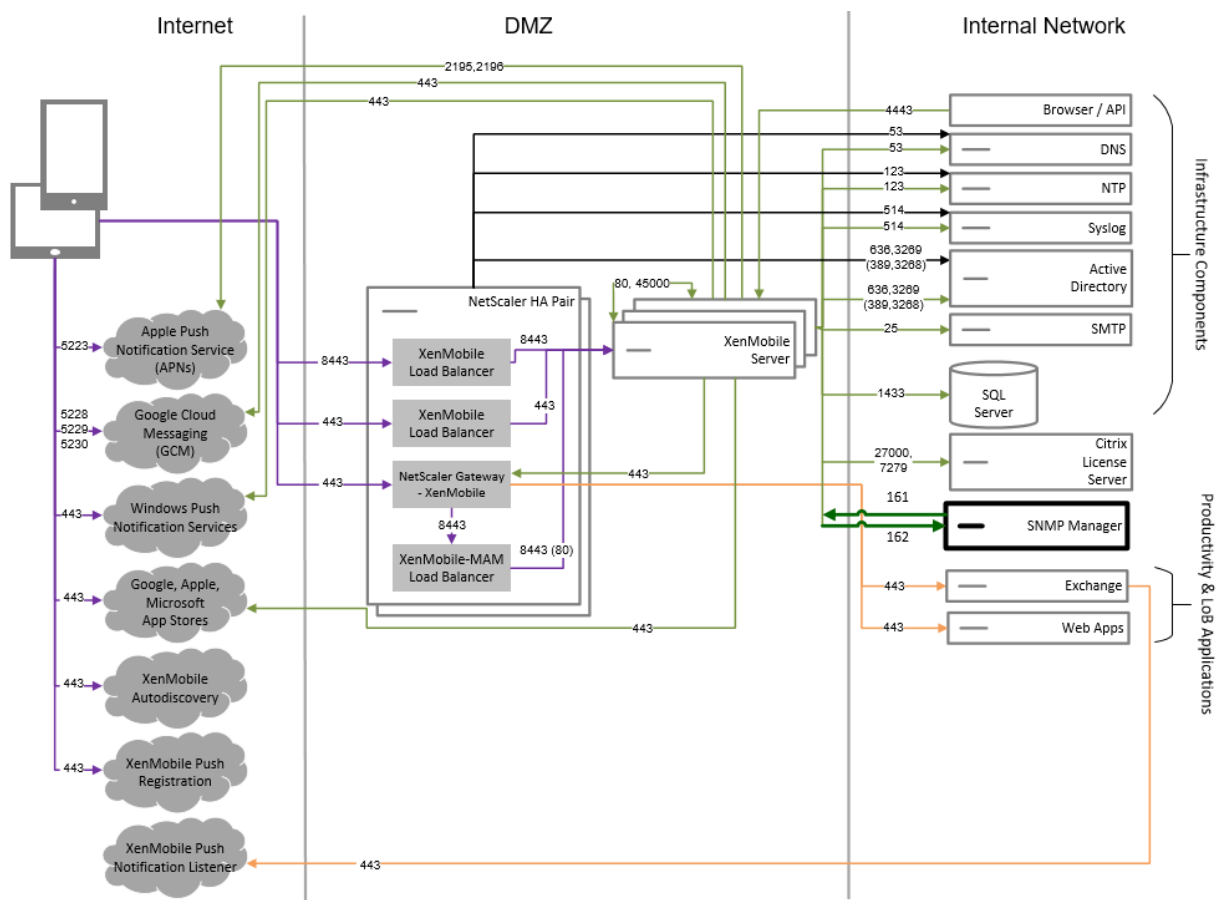
Arquitetura de referência somente MAM principal

Implante essa arquitetura se você planeja usar somente os recursos MAM do XenMobile sem precisar registrar dispositivos para MDM. Por exemplo, você deseja proteger aplicativos e dados em dispositivos móveis BYO; você deseja entregar aplicativos móveis empresariais e ser capaz de bloquear aplicativos e apagar os respectivos dados. Os dispositivos não podem registrados no MDM.



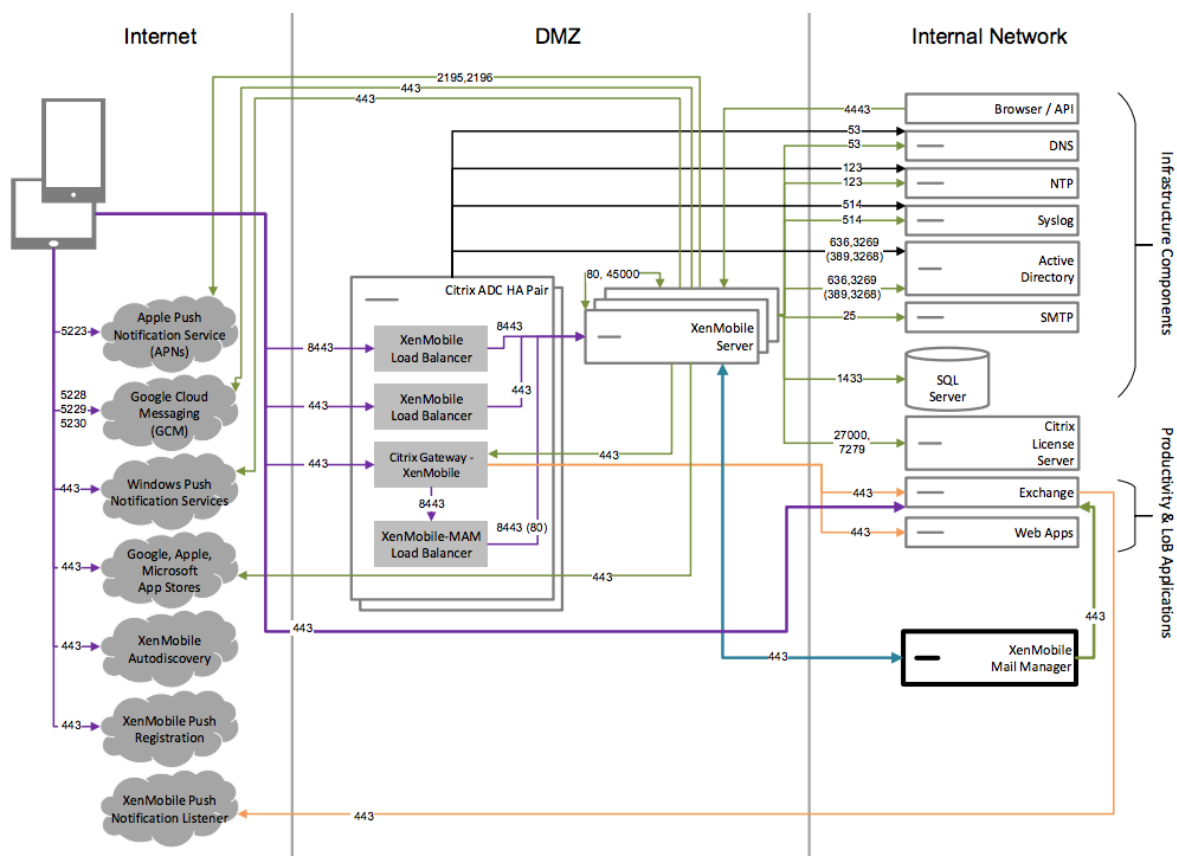
Arquitetura de referência com SNMP

Implemente esta arquitetura se você planeja ativar o monitoramento SNMP com o XenMobile. Por exemplo, se você quiser permitir que os sistemas de monitoramento consultem e obtenham informações nos nós do XenMobile. Para obter detalhes, consulte [SNMP monitoring](#).



Arquitetura de referência com o conector Citrix Gateway para Exchange ActiveSync

Implemente esta arquitetura se você planeja usar o conector Citrix Gateway para Exchange ActiveSync com o XenMobile. Por exemplo, se você precisar fornecer acesso seguro a e-mail aos usuários que usam aplicativos de e-mail móveis nativos. Esses usuários continuarão acessando o e-mail por meio de um aplicativo nativo, ou, se quiser, você poderá fazer a transição gradual deles para o Citrix Secure Mail. O controle de acesso precisa ocorrer na camada de rede antes que o tráfego atinja os servidores do Exchange Active Sync. Embora o diagrama mostre o conector do Exchange ActiveSync implantado em uma arquitetura MDM e MAM, você também pode implantar o conector de Exchange ActiveSync da mesma maneira como parte de uma arquitetura somente MDM.

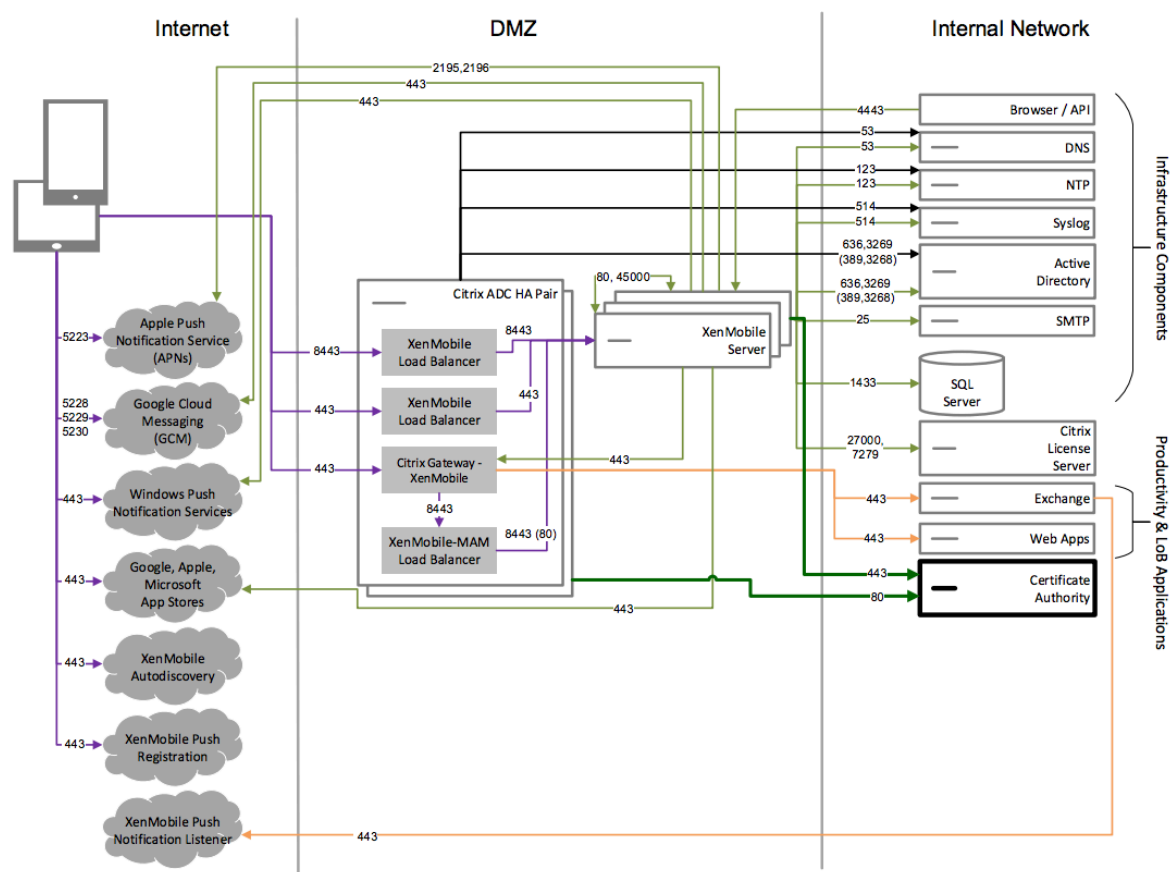


Arquitetura de referência com autoridade de certificação externa

Recomenda-se uma implantação que inclua uma autoridade de certificação externa para atender a um ou mais dos seguintes requisitos:

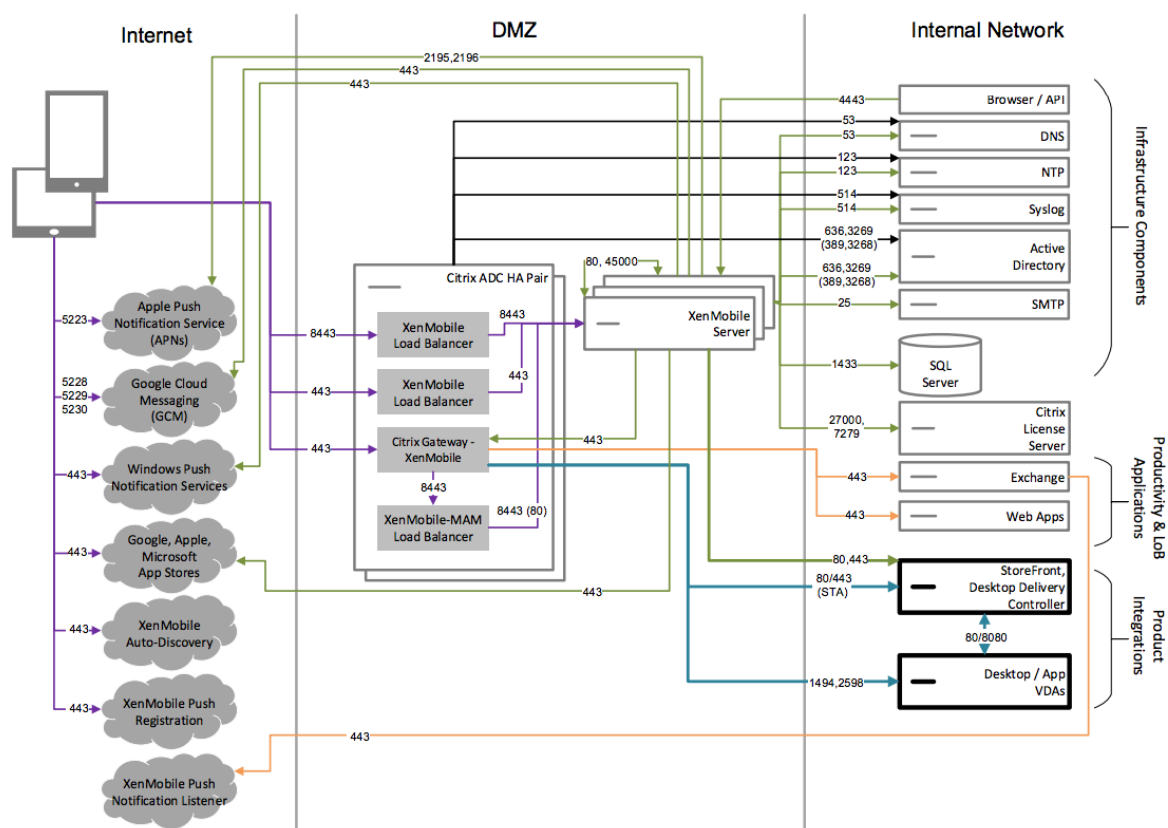
- Você precisa de certificados de usuário para autenticação do usuário no Citrix Gateway (para acesso à intranet).
- Você precisa que os usuários do Secure Mail sejam autenticados no Exchange Server usando um certificado de usuário.
- Você precisa enviar certificados emitidos pela Autoridade de Certificação corporativa para dispositivos móveis para acesso Wi-Fi, por exemplo.

Embora o diagrama mostre uma autoridade de certificação externa implantada em uma arquitetura MDM+MAM, você também pode implantar uma Autoridade de Certificação externa da mesma maneira como parte de uma arquitetura somente MDM ou somente MAM.



Arquitetura de referência com aplicativos e áreas de trabalho virtuais

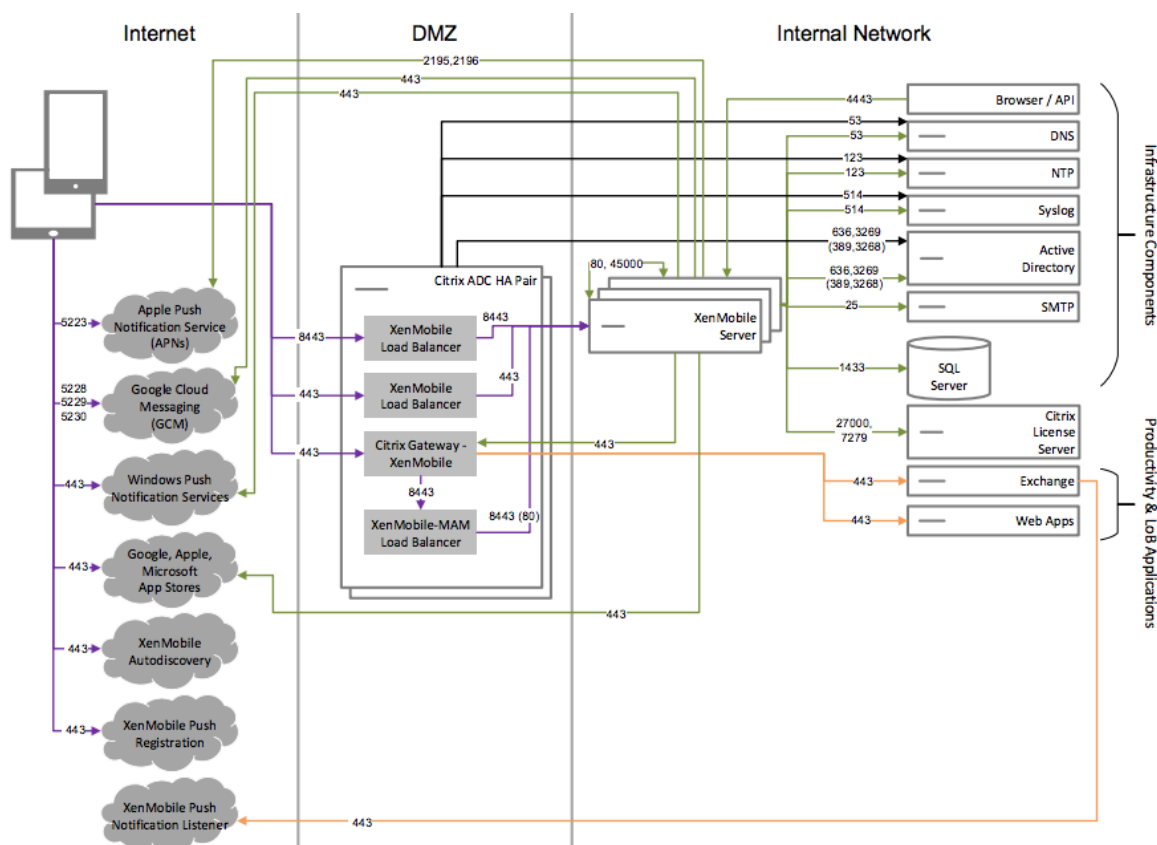
Implemente esta arquitetura se você planeja integrar aplicativos e áreas de trabalho virtuais com o XenMobile. Por exemplo, você precisa fornecer uma loja de aplicativos unificada para usuários móveis para todos os tipos de aplicativos (móveis, SaaS e Windows). Embora o diagrama mostre áreas de trabalho virtuais implementadas em uma arquitetura MDM e MAM, você também pode implantar essas áreas de trabalho da mesma maneira como parte de uma arquitetura somente MAM.



Arquitetura de referência com o XenMobile na rede interna

Você pode implantar uma arquitetura com o XenMobile na rede interna para atender a um ou mais dos seguintes requisitos:

- Você não tem ou não tem permissão para ter um hipervisor na DMZ.
- Sua DMZ pode conter apenas dispositivos de rede.
- Seus requisitos de segurança requerem o uso do SSL Offload.



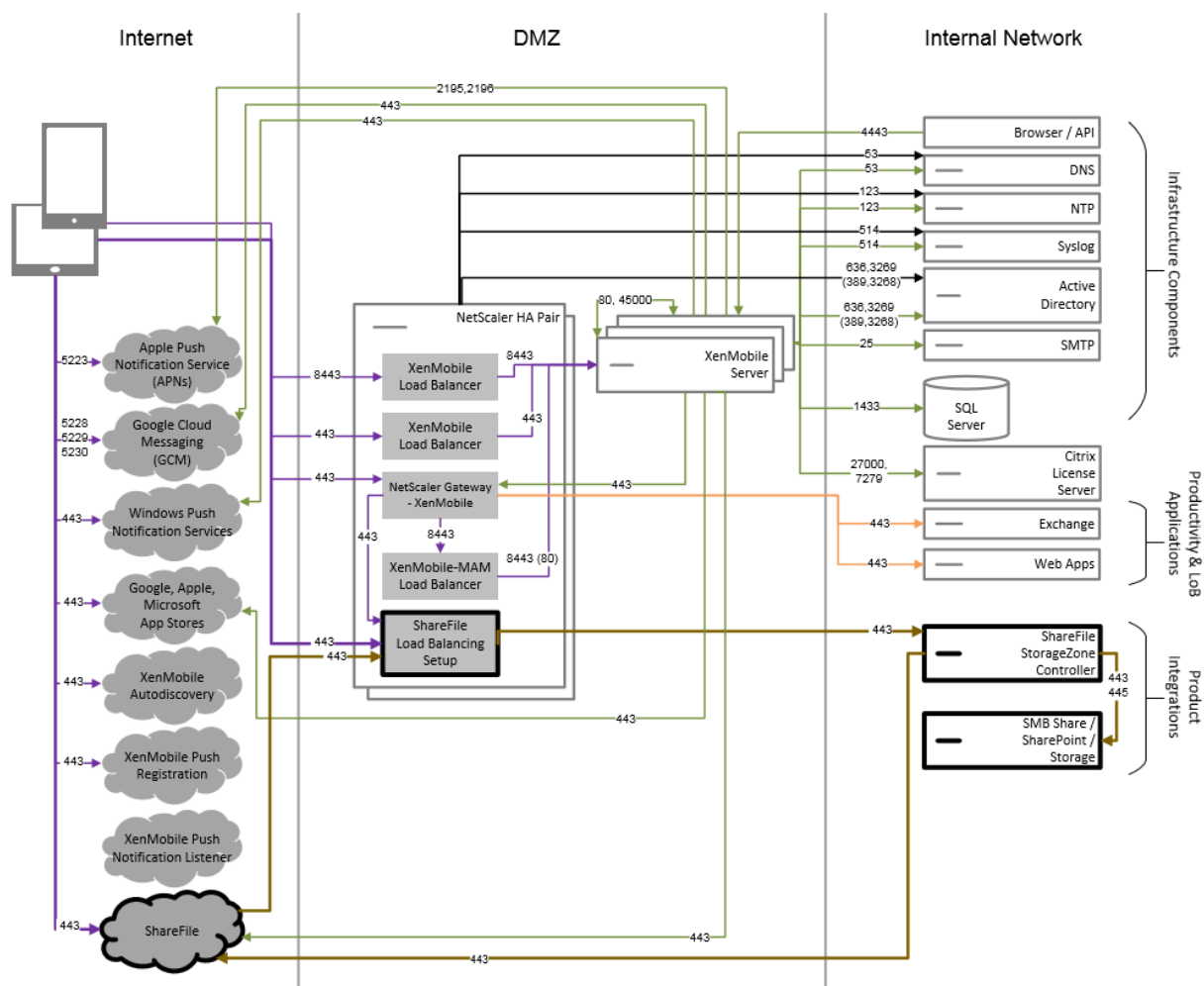
Arquitetura de referência com Citrix Content Collaboration

Implemente esta arquitetura se você quiser integrar o Citrix Files ou apenas os conectores de zona de armazenamento com o XenMobile. A integração do Citrix Files permite atender a um ou mais dos seguintes requisitos:

- Você precisa de um IDP para fornecer aos usuários login único (SSO) para o ShareFile.com.
- Você precisa de uma maneira de provisionar contas no ShareFile.com.
- Você tem repositórios de dados no local que precisam ser acessados a partir de dispositivos móveis.

Uma integração apenas com os conectores de zona de armazenamento fornece aos usuários acesso móvel seguro a repositórios de armazenamento locais existentes, como sites do SharePoint e compartilhamentos de arquivos em rede. Nessa configuração, você não precisa definir um subdomínio do Citrix Content Collaboration, provisionar usuários para o Citrix Files ou hospedar dados do Citrix Files.

Embora o diagrama mostre o Citrix Files implementado em uma arquitetura MDM+MAM, você também pode implantar o Citrix Files da mesma maneira como parte de uma arquitetura somente MAM.



Propriedades do servidor

November 30, 2020

Propriedades do servidor são propriedades globais que se aplicam a operações, usuários e dispositivos em uma instância inteira do XenMobile. A Citrix recomenda que você avalie para o seu ambiente as propriedades do servidor abordadas neste artigo. Não deixe de consultar a Citrix antes de alterar outras propriedades do servidor.

A alteração em algumas propriedades do servidor requer uma reinicialização de cada nó do XenMobile Sever. O XenMobile avisa quando uma reinicialização é necessária.

Algumas propriedades do servidor ajudam a melhorar o desempenho e a estabilidade. Para obter detalhes, consulte [Ajuste das operações do XenMobile](#).

Acessar todos os aplicativos na loja gerenciada do Google Play. Se **true**, o XenMobile torna todos os aplicativos da loja pública do Google Play acessíveis a partir da loja gerenciada do Google Play.

Definir esta propriedade como **true** acrescentará os aplicativos da loja pública do Google Play a uma lista de permissão para todos os usuários do Android Enterprise. Os administradores podem usar a [Política de dispositivo de restrições](#) para controlar o acesso a esses aplicativos. O padrão é **false**.

Permitir nomes de host para links da iOS App Store: a propriedade `ios.app.store.allowed.hostnames` é uma lista de nomes de host permitidos usados ao carregar aplicativos da loja de aplicativos pública para o servidor usando as APIs públicas. Se você planeja fazer upload de aplicativos da loja de aplicativos pública usando as APIs públicas em vez de fazer o upload dos aplicativos pelo servidor, configure essa propriedade. O valor padrão é `itunes.apple.com,vpp.itunes.apple.com,apps.apple.com`.

Bloquear registro de dispositivos Android com root e iOS com jailbreak: quando essa propriedade é **true**, o XenMobile bloqueia o registro de dispositivos Android com root e dispositivos iOS com jailbreak. O padrão é **true**. A configuração recomendada é **true** para todos os níveis de segurança.

Registro obrigatório: `wsapi.mdm.required.flag`, que se aplica somente quando o Modo do XenMobile Server é ENT, especifica se você exige que os usuários se registrem no MDM. A propriedade se aplica a todos os usuários e dispositivos da instância do XenMobile. Exigir registro oferece um nível mais alto de segurança. No entanto, essa decisão depende se você deseja exigir o MDM. Por padrão, o registro não é obrigatório.

Quando essa propriedade é **false**, os usuários podem recusar o registro, mas ainda podem acessar os aplicativos em seus dispositivos através da XenMobile Store. Quando essa propriedade for **true**, qualquer usuário que recusar o registro terá acesso negado aos aplicativos.

Se você alterar essa propriedade depois que os usuários se registrarem, os usuários deverão se registrar novamente.

Para ver um debate sobre a necessidade de exigir o registro no MDM, consulte [Gerenciamento de dispositivos e registro do MDM](#).

Ativar registro multimodo: a propriedade `enable.multimode.xmls` permite criar perfis de registro em um XenMobile Server que controla as configurações de registro para o gerenciamento de dispositivos e aplicativos para dispositivos Android e iOS. Além disso, o novo recurso de perfis de registro aprimorado permite o registro de dispositivos dedicados para Android e o registro somente MAM para dispositivos Android e iOS. Quando a propriedade é **false**, essas opções de registro não estão disponíveis ao configurar os perfis de registro. O valor padrão é **true**. Dispositivos que se registram quando a propriedade é **true** continuam a funcionar se você alterar a propriedade para **false**.

Ativar o Portal de Autoajuda: se `shp.console.enable` for **false**, isso impedirá o acesso ao Portal de Autoajuda. Os usuários que navegam para o Portal de Autoajuda na porta 443 recebem um erro 404. Os usuários que navegam para o portal na porta 4443 recebem uma mensagem “Acesso negado”. Se **true**, fornece acesso ao Portal de Autoajuda através da porta 443. O padrão é **false**.

Limite de bloqueio de conta de usuário local: utilizando a política de restrição, você pode definir um limite para tentativas de logon para usuários do Active Directory. Use a chave `local.user.account`

`.lockout.limit` para fazer o mesmo para contas de usuário locais. Depois que os usuários tentarem fazer logon no número de vezes que você especificar, eles não poderão tentar novamente até que um período de tempo passe. Configure esse período de tempo com a propriedade de **Tempo de bloqueio de conta de usuário local**. O valor padrão é 6.

Tempo de bloqueio de conta de usuário local: a propriedade `local.user.account.lockout.time` permite que você defina o número de minutos que devem passar antes que uma conta de usuário local bloqueada possa tentar fazer logon novamente. O valor padrão é 30 minutos.

Tamanho máximo da restrição de carregamento de arquivo ativado: ative a configuração de restrição de tamanho máximo do arquivo para carregamento `max.file.size.upload.restriction` como **true**. Se você habilitar essa restrição, configure o tamanho máximo do arquivo usando `max.file.size.upload.allowed`. O valor padrão para essa propriedade é **true**.

Tamanho máximo de carregamento de arquivo permitido: com `max.file.size.upload.allowed`, você pode especificar um tamanho máximo de arquivo para qualquer carregamento. Os valores de exemplo incluem 500 B, 1 KB, 1 MB, 1 MiB, 1 G ou 1 GiB. O valor padrão é 5 MB.

Tempo limite de inatividade em minutos: o número de minutos após os quais o XenMobile faz o logout de um usuário inativo que usou a API pública do XenMobile Server para acessar o console XenMobile ou algum aplicativo de terceiros. Um tempo limite de 0 significa que um usuário inativo permanece conectado. Para aplicativos de terceiros que acessam a API, normalmente é necessário permanecer conectado. O padrão é 5.

Registro no gerenciamento de dispositivo iOS: instalar CA raiz se necessário: o fluxo de trabalho de registro mais recente da Apple requer que os usuários instalem manualmente os perfis MDM. Esse fluxo de trabalho não se aplica ao registro do MDM em servidores atribuídos no Apple Business Manager ou Apple School Manager. No entanto, durante o registro manual no MDM, os usuários de dispositivos iOS recebem somente a solicitação do certificado de dispositivo MDM durante o registro.

Para proporcionar uma melhor experiência de usuário durante o registro manual, a Citrix recomenda alterar a propriedade do servidor de `ios.mdm.enrollment.installRootCaIfRequired` para **false**. O valor padrão é **true**. Com essa alteração, uma janela do Safari é aberta durante o registro no MDM para simplificar a instalação do perfil para os usuários.

Intervalo de linha de base do VPP: a propriedade `vpp.baseline` define o intervalo mínimo em que o XenMobile reimporta as licenças de compra por volume da Apple. A atualização de informações de licença garante que o XenMobile reflita todas as alterações, como quando você exclui manualmente um aplicativo importado da compra por volume. Por padrão, o XenMobile atualiza a linha de base da licença de compra por volume no mínimo a cada 1440 minutos.

Se você tem muitas licenças de compra por volume instaladas (por exemplo, mais de 50.000), a Citrix recomenda que você aumente o intervalo da linha de base para reduzir a sobrecarga de importação de licenças. Se você espera mudanças frequentes de licenças de compra por volume da Apple, a Citrix recomenda reduzir o valor para manter o XenMobile atualizado com essas mudanças. O intervalo

mínimo entre duas linhas de base é de 60 minutos. Como o trabalho cron é executado a cada 60 minutos, se o intervalo de linha de base de compra por volume for de 60 minutos, o intervalo entre linhas de base pode ser adiado até 119 minutos.

Intervalo máximo de inatividade para o console do portal de autoatendimento do XenMobile MDM (em minutos): esse nome de propriedade reflete as versões antigas do XenMobile. A propriedade controla o intervalo máximo de inatividade do console XenMobile. Esse intervalo é o número de minutos após os quais o XenMobile faz logoff de um usuário inativo do console XenMobile. Um tempo limite de 0 significa que um usuário inativo permanece conectado. O padrão é 30.

Políticas de dispositivos e aplicativos

April 8, 2021

As políticas de dispositivos e aplicativos do XenMobile permitem otimizar o equilíbrio entre fatores, como:

- Segurança da empresa
- Dados corporativos e proteção de ativos
- Privacidade do usuário
- Experiências de usuário produtivas e positivas

O equilíbrio ideal entre esses fatores pode variar. Por exemplo, organizações altamente regulamentadas, como as financeiras, exigem controles de segurança mais rigorosos do que outros setores, como educação e varejo, nos quais a produtividade do usuário é uma consideração primordial.

Você pode controlar e configurar as políticas de modo centralizado com base na identidade, no dispositivo, no local e no tipo de conectividade dos usuários para restringir o uso mal-intencionado de conteúdo corporativo. No caso de um dispositivo ser perdido ou roubado, você poderá desabilitar, bloquear ou apagar remotamente aplicativos e dados comerciais. O resultado geral é uma solução que aumenta a satisfação e a produtividade dos funcionários, garantindo segurança e controle administrativo.

O foco principal deste artigo são as várias políticas de dispositivos e aplicativos relacionadas à segurança.

Políticas que abordam riscos de segurança

As políticas de dispositivos e aplicativos do XenMobile abordam muitas situações que podem representar um risco de segurança, como:

- Quando os usuários tentam acessar aplicativos e dados de dispositivos não confiáveis e locais imprevisíveis.

- Quando os usuários passam dados de um dispositivo para outro.
- Quando um usuário não autorizado tenta acessar dados.
- Quando um usuário que saiu da empresa usou seu próprio dispositivo (BYOD).
- Quando um usuário perde um dispositivo.
- Quando os usuários precisam acessar a rede com segurança todo o tempo.
- Quando os usuários têm seu próprio dispositivo gerenciado e você precisa separar os dados de trabalho dos dados pessoais.
- Quando um dispositivo está inativo e requer verificação de credenciais do usuário novamente.
- Quando os usuários copiam e colam conteúdo confidencial em sistemas de e-mail desprotegidos.
- Quando os usuários recebem anexos de e-mail ou links da Web com dados confidenciais em um dispositivo que contém contas pessoais e corporativas.

Essas situações referem-se a duas áreas principais de preocupação ao proteger os dados da empresa, que ocorrem quando os dados estão:

- Em repouso
- Em trânsito

Como o XenMobile protege os dados em repouso

Dados armazenados em dispositivos móveis são vistos como dados em repouso. O XenMobile usa a criptografia de dispositivo fornecida pelas plataformas iOS e Android. O XenMobile complementa a criptografia baseada na plataforma com recursos como verificação de conformidade, disponíveis por meio do Citrix MAM SDK.

Os recursos de gerenciamento de aplicativos móveis (MAM) do XenMobile permitem gerenciamento, proteção e controle total de aplicativos móveis de produtividade, aplicativos habilitados para MDX e seus dados associados.

O SDK de aplicativos móveis habilita os aplicativos para implantação do XenMobile usando a tecnologia de contêiner do aplicativo Citrix MDX. A tecnologia de contêiner separa aplicativos e dados corporativos de aplicativos e dados pessoais no dispositivo de um usuário. A separação de dados permite que você proteja qualquer aplicativo móvel personalizado desenvolvido, de terceiros ou BYO com controles abrangentes baseados em políticas.

O XenMobile também inclui criptografia em nível de aplicativo. O XenMobile criptografa separadamente os dados armazenados em qualquer aplicativo habilitado para MDX sem exigir o código secreto do dispositivo e sem exigir que você gerencie o dispositivo para impor a política.

Políticas e o Mobile Apps SDK permitem que você:

- Separe aplicativos e dados comerciais e pessoais em um contêiner móvel seguro.

- Proteja aplicativos com criptografia e outras tecnologias móveis de prevenção contra perda de dados (DLP).

As políticas de MDX fornecem muitos controles operacionais. Você pode habilitar a integração entre aplicativos habilitados para MAM SDK ou preparados com MDX sem interrupções, além de controlar toda a comunicação. Dessa forma, você pode impor políticas, de modo a garantir que os dados sejam acessíveis somente por aplicativos habilitados para MAM SDK ou preparados com MDX.

Além do controle de políticas de dispositivos e aplicativos, a melhor maneira de proteger os dados em repouso é a criptografia. O XenMobile adiciona uma camada de criptografia a todos os dados armazenados em um aplicativo habilitado para MDX, oferecendo a você controle de políticas de recursos como criptografia de arquivos públicos, criptografia de arquivos privados e exclusões de criptografia. O Mobile Apps SDK usa criptografia FIPS 140-2 de compatibilidade AES 256 bits com chaves armazenadas em um Citrix Secret Vault protegido.

Como o XenMobile protege os dados em trânsito

Os dados que se movem entre os dispositivos móveis de seus usuários e sua rede interna são chamados de dados em trânsito. A tecnologia de contêiner de aplicativo MDX fornece acesso VPN específico ao aplicativo para sua rede interna por meio do Citrix Gateway.

Considere uma situação em que um funcionário deseja acessar os seguintes recursos que residem na rede empresarial segura a partir de um dispositivo móvel:

- O servidor de e-mail corporativo
- Um aplicativo web habilitado para SSL hospedado na intranet corporativa
- Documentos armazenados em um servidor de arquivos ou no Microsoft SharePoint

O MDX permite o acesso a todos esses recursos corporativos a partir de dispositivos móveis por meio de uma micro VPN específica ao aplicativo. Cada dispositivo tem seu próprio túnel micro VPN dedicado.

A funcionalidade Micro VPN não requer uma VPN de dispositivo, o que pode comprometer a segurança em dispositivos móveis não confiáveis. Como resultado, a rede interna não fica exposta a malwares ou ataques que possam infectar todo o sistema corporativo. Aplicativos móveis corporativos e aplicativos móveis pessoais podem coexistir em um único dispositivo.

Para oferecer níveis ainda mais fortes de segurança, você pode configurar aplicativos habilitados para MDX com uma política de Citrix Gateway alternativo, usada para autenticação e para sessões de micro VPN com um aplicativo. Você pode usar um Citrix Gateway alternativo com a política necessária para a sessão On-line para forçar os aplicativos a se autenticarem novamente no gateway específico. Esses gateways normalmente têm requisitos de autenticação (maior garantia) e políticas de gerenciamento de tráfego diferentes.

Além dos recursos de segurança, o recurso micro VPN também oferece técnicas de otimização de dados, incluindo algoritmos de compactação. Algoritmos de compactação garantem que:

- Apenas o mínimo de dados seja transferido
- A transferência é feita no menor tempo possível. A velocidade melhora a experiência do usuário, que é um fator chave para o sucesso da adoção de dispositivos móveis.

Reavalie suas políticas de dispositivo periodicamente, como nessas situações:

- Quando uma nova versão do XenMobile inclui políticas novas ou atualizadas devido ao lançamento de atualizações do sistema operacional do dispositivo

- Quando você adiciona um tipo de dispositivo:

Apesar de muitas políticas serem comuns a todos os dispositivos, cada dispositivo tem um conjunto de políticas específicas ao seu sistema operacional. Como resultado, você pode encontrar diferenças entre dispositivos iOS, Android e Windows, e até mesmo entre dispositivos com Android de diferentes fabricantes.

- Manter a operação do XenMobile em sincronia com as mudanças na empresa ou do setor, como novas políticas de segurança corporativa ou regulamentos de conformidade
- Quando uma nova versão do MDX Service inclui políticas novas ou atualizadas
- Quando você adiciona ou atualiza um aplicativo
- Integrar novos fluxos de trabalho para seus usuários como resultado de novos aplicativos ou novos requisitos

Políticas de aplicativos e cenários de casos de uso

Embora você possa escolher quais aplicativos estão disponíveis por meio do Secure Hub, convém também definir como esses aplicativos interagem com o XenMobile. Usar políticas de aplicativos:

- Se você quiser que os usuários se autentiquem após um determinado período de tempo passar.
- Se você quiser fornecer aos usuários acesso offline às suas informações.

As seções a seguir incluem algumas das políticas e exemplo de uso.

- Para obter uma lista das políticas de terceiros que você pode integrar em seu aplicativo iOS e Android usando o SDK do MAM, consulte [Visão geral do SDK MAM](#).
- Para obter uma lista de todas as políticas de MDX por plataforma, consulte [Resumo das políticas do MDX](#).

Políticas de autenticação

- **Código secreto do dispositivo**

Por que usar esta política: ative a política de código secreto do dispositivo para garantir que um usuário possa acessar um aplicativo MDX somente se o dispositivo tiver um código secreto de dispositivo ativado. Esse recurso garante o uso da criptografia iOS no nível do dispositivo.

Exemplo de usuário: ativar essa política significa que o usuário deve definir um código secreto no dispositivo iOS antes de poder acessar o aplicativo MDX.

- **Código secreto do aplicativo**

Por que usar esta política: ative a política de senha do aplicativo para que o Secure Hub solicite que um usuário se autentique no aplicativo gerenciado antes que ele possa abrir o aplicativo e acessar os dados. O usuário pode se autenticar com sua senha do Active Directory, PIN da Citrix ou TouchID do iOS, dependendo do que você configurar em Propriedades do Cliente nas Configurações do XenMobile Server. Você pode definir um temporizador de inatividade nas Propriedades do Cliente para que, com o uso continuado, o Secure Hub não solicite que o usuário se autentique no aplicativo gerenciado novamente até que o timer expire.

O código secreto do aplicativo difere de um código secreto de dispositivo no sentido que, com uma política de código secreto de dispositivo enviada para um dispositivo, o Secure Hub solicita aos usuários que configurem um código secreto ou PIN, que eles devem desbloquear antes que possam acessar o dispositivo quando ligarem o dispositivo ou quando o timer de inatividade expirar. Para obter mais informações, consulte [Autenticação no XenMobile](#).

Exemplo de usuário: ao abrir o aplicativo Citrix Secure Web no dispositivo, o usuário deve inserir seu Citrix PIN antes de poder navegar nos sites se o período de inatividade expirar.

- **Sessão online obrigatória**

Por que usar esta política: se um aplicativo exigir acesso a um aplicativo da web (serviço da web), ative essa política para que o XenMobile solicite que o usuário se conecte à rede da empresa ou tenha uma sessão ativa antes de usar o aplicativo.

Exemplo de usuário: quando um usuário tenta abrir um aplicativo MDX com a política necessária para sessão online ativada, ele não pode usar o aplicativo até que se conecte à rede usando um serviço de celular ou Wi-Fi.

- **Período máximo offline**

Por que usar esta política: use esta política como uma opção de segurança adicional para garantir que os usuários não possam executar um aplicativo offline por longos períodos sem reconfirmar as políticas de direito e atualização de aplicativos do XenMobile.

Exemplo de usuário: se você configurar um aplicativo MDX com um período offline Máximo, o usuário poderá abrir e usar o aplicativo offline até que o período do timer offline expire. Nesse ponto, o usuário deve se conectar novamente à rede por meio do serviço de celular ou Wi-Fi e se autenticar novamente, se solicitado.

Outras Políticas de Acesso

- **Período de tolerância de atualização de aplicativo (horas)**

Por que usar esta política: o período de tolerância da atualização do aplicativo é o tempo disponível para o usuário antes que ele precise atualizar um aplicativo que tenha uma versão mais recente liberada na XenMobile Store. No momento da expiração, o usuário deve atualizar o aplicativo antes que possa obter acesso aos dados no aplicativo. Ao definir esse valor, lembre-se das necessidades de sua força de trabalho móvel, especialmente daqueles que podem passar longos períodos offline quando viajando internacionalmente.

Exemplo de usuário: você carrega uma nova versão do Secure Mail na XenMobile Store e, em seguida, define um período de tolerância de atualização do aplicativo de 6 horas. Todos os usuários do Secure Mail verão uma mensagem solicitando a atualização do aplicativo Secure Mail, até que as 6 horas expirem. Quando as 6 horas expirarem, o Secure Hub encaminhará os usuários para a XenMobile Store.

- **Intervalo ativo de sondagem (minutos)**

Por que usar esta política: o intervalo ativo de sondagem é o período no qual o XenMobile verifica aplicativos para executar ações de segurança, como o Bloqueio de aplicativos e o Apagamento de aplicativos.

Exemplo de usuário: se você definir a política Intervalo ativo de sondagem para 60 minutos, quando você enviar o comando de bloqueio de aplicativo do XenMobile para o dispositivo, o bloqueio ocorrerá dentro de 60 minutos a contar de quando a última pesquisa foi realizada.

Políticas de comportamento de dispositivos não compatíveis

Quando um dispositivo fica abaixo dos requisitos mínimos de conformidade, a política de Comportamento do dispositivo não compatível permite que você selecione a ação a ser executada. Para obter informações, consulte [Comportamento do dispositivo não compatível](#).

Políticas de interação de aplicativos

Por que usar essas políticas: use políticas de interação de aplicativos para controlar o fluxo de documentos e dados de aplicativos MDX para outros aplicativos no dispositivo. Por exemplo, você pode impedir que um usuário mova dados para seus aplicativos pessoais fora do contêiner ou cole dados de fora do contêiner nos aplicativos em contêineres.

Exemplo de usuário: você define uma política de interação de aplicativos como Restrito, o que significa que um usuário pode copiar texto do Secure Mail para o Secure Web, mas não pode copiar esses dados para o navegador pessoal Safari ou Chrome que está fora do contêiner. Além disso, um usuário pode abrir um documento anexado do Secure Mail no Citrix Files ou no QuickEdit, mas não pode abrir

o documento anexado em seus próprios aplicativos de visualização de arquivo pessoal que estão fora do contêiner.

Políticas de restrições de aplicativos

Por que usar essas políticas: use as políticas de restrição de aplicativos para controlar quais recursos os usuários podem acessar a partir de um aplicativo MDX enquanto ele estiver aberto. Isso ajuda a garantir que nenhuma atividade maliciosa ocorra enquanto o aplicativo estiver em execução. As políticas de restrição de aplicativos variam ligeiramente entre o iOS e o Android. Por exemplo, no iOS, você pode bloquear o acesso ao iCloud enquanto o aplicativo MDX está em execução. No Android, você pode interromper o uso de NFC enquanto o aplicativo MDX estiver em execução.

Exemplo de usuário: se você ativar a política de restrição de aplicativos para bloquear o ditado no iOS em um aplicativo MDX, o usuário não poderá usar a função ditar no teclado do iOS enquanto o aplicativo MDX estiver em execução. Assim, o ditado dos usuários de dados não é passado para o serviço de ditado de nuvem de terceiros desprotegido. Quando o usuário abre seu aplicativo pessoal fora do contêiner, a opção de ditado permanece disponível para o usuário para suas comunicações pessoais.

Políticas de acesso à rede do aplicativo

Por que usar essas políticas: use as políticas de acesso à rede do aplicativo para fornecer acesso a partir de um aplicativo MDX no contêiner do dispositivo a dados localizados dentro de sua rede corporativa. Para a política de acesso à rede, defina a opção **Com túnel para a rede interna** para automatizar uma micro VPN a partir do aplicativo MDX por meio do Citrix ADC para um serviço da web de backend ou armazenamento de dados.

Exemplo de usuário: quando um usuário abre um aplicativo MDX, como o Secure Web, que tem o encapsulamento ativado, o navegador abre e inicia um site de intranet sem que o usuário precise iniciar uma VPN. O aplicativo Secure Web acessa automaticamente o site interno usando a tecnologia micro VPN.

Políticas de geolocalização e geocerca do aplicativo

Por que usar essas políticas: as políticas que controlam a geolocalização e a delimitação geográfica de aplicativos incluem a longitude do ponto central, a latitude do ponto central e o raio. Essas políticas contêm acesso aos dados nos aplicativos MDX para uma área geográfica específica. As políticas definem uma área geográfica por um raio de coordenadas de latitude e longitude. Se um usuário tentar usar um aplicativo fora do raio definido, o aplicativo permanecerá bloqueado e o usuário não poderá acessar os dados do aplicativo.

Exemplo de usuário: um usuário pode acessar dados de fusão e aquisição enquanto está na localidade do escritório. Quando sai a localidade do escritório, esses dados confidenciais ficam inacessíveis.

Políticas do Aplicativo Secure Mail

- **Serviços de rede em segundo plano**

Por que usar esta política: os serviços de rede em segundo plano no Secure Mail utilizam STA (Secure Ticket Authority), que é efetivamente um proxy SOCKS5 para conexão através do Citrix Gateway. O STA suporta conexões de longa duração e oferece melhor duração da bateria em comparação com a micro VPN. Assim, o STA é ideal para correios que se conectam constantemente. A Citrix recomenda que você defina essas configurações para o Secure Mail. O assistente Citrix ADC for XenMobile configura automaticamente o STA para Secure Mail.

Exemplo de usuário: quando a STA não está habilitada e um usuário do Android abre o Secure Mail, ele é solicitado a abrir uma VPN, que permanece aberta no dispositivo. Quando o STA está habilitado e o usuário do Android abre o Secure Mail, o Secure Mail conecta-se sem precisar de VPN.

- **Intervalo de sincronização padrão**

Por que usar esta política: essa configuração especifica os dias padrão de email que são sincronizados com o Secure Mail quando o usuário acessa o Secure Mail pela primeira vez. Esteja ciente de que duas semanas de e-mail demoram mais para sincronizar do que três dias e prolongam o processo de configuração do usuário.

Exemplo de usuário: se o intervalo de sincronização padrão for definido como 3 dias quando o usuário configurar pela primeira vez o Secure Mail, ele poderá ver todos os e-mails na Caixa de entrada que recebeu da data presente até três dias anteriores. Se um usuário quiser ver e-mails de mais de três dias atrás, ele poderá fazer uma busca. O Secure Mail mostra os e-mails mais antigos armazenados no servidor. Depois de instalar o Secure Mail, cada usuário pode alterar essa configuração para melhor atender às suas necessidades.

Políticas de dispositivo e comportamento do caso de uso

As políticas de dispositivo, às vezes chamadas de políticas de MDM, determinam como o XenMobile funciona com dispositivos. Apesar de muitas políticas serem comuns a todos os dispositivos, cada dispositivo tem um conjunto de políticas específicas ao seu sistema operacional. A lista a seguir inclui algumas das políticas do dispositivo e discute como você pode usá-las. Para obter uma lista de todas as políticas de dispositivos, consulte os artigos em [Políticas de dispositivo](#).

- **Política de inventário de aplicativos**

Por que usar esta política: implante a política de inventário de aplicativos em um dispositivo se você precisar ver os aplicativos instalados por um usuário. Se você não implantar a política de inventário de aplicativos, poderá ver apenas os aplicativos que um usuário instalou da XenMobile Store e não os aplicativos instalados pessoalmente. Você deve usar esta política se quiser bloquear a execução de determinados aplicativos em dispositivos corporativos.

Exemplo de usuário: um usuário com um dispositivo gerenciado pelo MDM não pode desativar essa funcionalidade. Os aplicativos instalados pelo usuário ficam visíveis para os administradores do XenMobile.

- **Política de bloqueio de aplicativo**

Por que usar esta política: a política de Bloqueio de Aplicativos, para Android, permite que você bloqueie ou permita aplicativos. Por exemplo, ao permitir aplicativos, você pode configurar um dispositivo de quiosque. Normalmente, você implanta a política de bloqueio de aplicativos somente em dispositivos de propriedade corporativa, pois limita os aplicativos que os usuários podem instalar. Você pode definir uma senha de substituição para fornecer acesso de usuário a aplicativos bloqueados.

Exemplo de usuário: suponha que você implemente uma política de bloqueio de aplicativo que bloqueie o aplicativo Angry Birds. O usuário pode instalar o aplicativo Angry Birds no Google Play, mas quando ele abre o aplicativo, uma mensagem avisa que o administrador bloqueou o aplicativo.

- **Política de agendamento de conexão**

Por que usar esta política: você deve usar a política de agendamento de conexão para que dispositivos Windows Mobile possam se conectar de volta ao XenMobile Server para gerenciamento MDM, envio de aplicativo e implantação de políticas. Para dispositivos Android, Android Enterprise e Chrome OS, use o Google Firebase Cloud Messaging (FCM), em vez desta política, para controlar conexões com o XenMobile Server. As opções de agendamento são as seguintes:

- **Sempre:** mantém a conexão ativa de forma permanente. A Citrix recomenda esta opção para segurança otimizada. Quando você escolher **Sempre**, use também a política de timer de conexão para garantir que a conexão não esteja esgotando a bateria. Ao manter a conexão ativa, você pode enviar comandos de segurança por push, como apagar ou bloquear o dispositivo sob demanda. Você também deve selecionar a opção do Cronograma de implantação **Implantar para conexão permanente** em cada política implantada no dispositivo.
- **Nunca:** conecta-se manualmente. A Citrix não recomenda essa opção para implantações de produção, pois a opção **Nunca** impede que você implante políticas de segurança nos dispositivos; portanto, os usuários nunca recebem novos aplicativos ou políticas.
- **A cada:** conecta-se no intervalo designado. Quando essa opção está em vigor e você envia

uma política de segurança, como um bloqueio ou um apagamento, o XenMobile processa a política no dispositivo na próxima vez em que ele se conectar.

- **Definir programação:** quando ativada, o XenMobile tenta se reconectar o dispositivo do usuário ao XenMobile Server após uma perda de conexão de rede e monitora a conexão mediante a transmissão de pacotes de controle em intervalos regulares no período de tempo que você definir.

Exemplo de usuário: você deseja implantar uma política de código secreto para dispositivos registrados. A política de agendamento garante que os dispositivos se conectem novamente ao servidor em um intervalo regular para coletar a nova política.

- **Política de credenciais**

Por que usar esta política: geralmente usada em conjunto com uma política WiFi, a política de Credenciais permite que você implante certificados para autenticação em recursos internos que exigem autenticação de certificado.

Exemplo de usuário: você implanta uma política de Wi-Fi que configura uma rede sem fio no dispositivo. A rede Wi-Fi requer um certificado para autenticação. A política de Credenciais implementa um certificado que é armazenado no keystore do sistema operacional. O usuário pode então selecionar o certificado quando conectado ao recurso interno.

- **Política do Exchange**

Por que usar esta política: com o XenMobile, você tem duas opções para entregar e-mails do Microsoft Exchange ActiveSync.

- **Aplicativo Secure Mail:** entregue e-mails usando o aplicativo Secure Mail que você distribui da loja de aplicativos pública ou da XenMobile Store.
- **Aplicativo de e-mail nativo:** use a política do Exchange para habilitar e-mail do ActiveSync para o cliente de e-mail nativo no dispositivo. Com a política do Exchange para e-mail nativo, você pode usar macros para preencher os dados do usuário de seus atributos do Active Directory, como `${user.username}`, para preencher o nome de usuário, e `${user.domain}`, para preencher o domínio do usuário.

Exemplo de usuário: quando você envia a política do Exchange, envia detalhes do Exchange Server para o dispositivo. O Secure Hub, em seguida, solicita que o usuário se autentique e o e-mail começa a ser sincronizado.

- **Política de localização**

Por que usar esta política: a política de localização permite localizar geograficamente dispositivos em um mapa, se o dispositivo tiver o GPS ativado para o Secure Hub. Depois de implantar essa política e enviar um comando locate do XenMobile Server, o dispositivo responde com as coordenadas de localização.

Exemplo de usuário: quando você implanta a política de localização e o GPS está habilitado no dispositivo, se os usuários perderem o dispositivo, eles poderão fazer logon no Portal de Autoatendimento do XenMobile e escolher a opção locate para ver a localização do dispositivo em um mapa. Observe que o usuário opta por permitir que o Secure Hub use os serviços de localização. Você não pode impor o uso de serviços de localização quando os usuários registram um dispositivo. Outra consideração para usar esta política é o efeito na duração da bateria.

- **Política de código secreto**

Por que usar esta política: a política de código secreto permite que você imponha um código PIN ou senha em um dispositivo gerenciado. Essa política permite definir a complexidade e os tempos limite do código secreto no dispositivo.

Exemplo de usuário: quando você implementa uma política de código secreto para um dispositivo gerenciado, o Secure Hub solicita aos usuários que configurem um código secreto ou PIN, que eles devem desbloquear antes que possam acessar o dispositivo quando ligarem o dispositivo ou quando o timer de inatividade expirar.

- **Política de remoção de perfil**

Por que usar esta política: suponha que você implemente uma política para um grupo de usuários e, posteriormente, precise remover essa política de um subconjunto de usuários. Você pode remover a política dos usuários selecionados criando uma política de remoção de perfil e usando regras de implantação para implementar a política de remoção de perfil apenas a nomes de usuário especificados.

Exemplo de usuário: quando você implanta uma política de remoção de perfil em dispositivos de usuário, os usuários podem não notar a alteração. Por exemplo, se a política de remoção de perfil remover uma restrição que desativou a câmera do dispositivo, o usuário não saberá que o uso da câmera agora é permitido. Considere informar os usuários quando as alterações afetarem a experiência do usuário.

- **Política de restrições**

Por que usar esta política: a política de restrição dá a você muitas opções para bloquear e controlar os recursos e as funcionalidades no dispositivo gerenciado. Você pode habilitar centenas de opções de restrição para permitir que os dispositivos compatíveis desativem a câmera ou o microfone em um dispositivo para aplicar as regras de roaming e o acesso a serviços de terceiros, como lojas de aplicativos

Exemplo de usuário: se você implantar uma restrição em um dispositivo iOS, o usuário pode não conseguir acessar o iCloud ou a Apple App Store.

- **Política de termos e condições**

Por que usar esta política: você talvez precise informar os usuários sobre as implicações legais de terem seus dispositivos gerenciados. Além disso, convém garantir que os usuários estejam

cientes dos riscos de segurança quando os dados corporativos são enviados para o dispositivo. O documento Termos e Condições personalizado permite publicar regras e avisos antes de o usuário se registrar.

Exemplo de usuário: um usuário vê as informações dos Termos e Condições durante o processo de registro. Caso se recuse a aceitar as condições declaradas, o processo de registro terminará e o usuário não poderá acessar os dados corporativos. Você pode gerar um relatório para fornecer às equipes de RH/Jurídico/Conformidade para mostrar quem aceitou ou recusou os termos.

- **Política de VPN**

Por que usar esta política: use a política de VPN para fornecer acesso a sistemas de back-end usando a tecnologia de gateway de VPN mais antiga. A política suporta um número de provedores de VPN, incluindo Cisco AnyConnect, Juniper, bem como Citrix VPN. Também é possível vincular essa política a uma CA e à VPN ativada sob demanda (se o gateway VPN oferecer suporte a essa opção).

Exemplo de usuário: com a política de VPN ativada, o dispositivo de um usuário abre uma conexão VPN quando o usuário acessa um domínio interno.

- **Política de clip web**

Por que usar esta política: use a política de clip Web se você quiser enviar para os dispositivos um ícone que seja aberto diretamente para um site. Um clip web contém um link para um site e pode incluir um ícone personalizado. Em um dispositivo, um clip web parece um ícone de aplicativo.

Exemplo de usuário: um usuário pode clicar em um ícone de clip web para abrir um site da Internet que fornece serviços que precisa acessar. Usar um link da Web é mais conveniente do que precisar abrir um aplicativo de navegador e digitar um endereço de link.

- **Política de WiFi**

Por que usar esta política: a política de Wi-Fi permite implantar detalhes da rede Wi-Fi, como SSID, dados de autenticação e dados de configuração, em um dispositivo gerenciado.

Exemplo de usuário: quando você implanta a política de Wi-Fi, o dispositivo se conecta automaticamente à rede Wi-Fi e autentica o usuário para que ele possa obter acesso à rede.

- **Política de proteção de informações do Windows**

Por que usar esta política: use a política de Proteção de Informações do Windows (WIP) para se proteger contra o possível vazamento de dados corporativos. Você pode especificar os aplicativos que requerem Proteção de informações do Windows no nível de execução que você definir. Por exemplo, você pode bloquear compartilhamentos de dados inadequados ou avisar sobre um compartilhamento de dados adequado e permitir que os usuários substituam

a política. Você pode executar o WIP silenciosamente enquanto registra o log e permite o compartilhamento de dados inadequado.

Exemplo de usuário: suponha que você configure a política de WIP para bloquear o compartilhamento de dados inadequado. Se um usuário copiar ou salvar um arquivo protegido em um local não protegido, será exibida uma mensagem semelhante à seguinte: Não é possível colocar conteúdo protegido de trabalho neste local.

- **Política XenMobile Store**

Por que usar esta política: a XenMobile Store é uma loja de aplicativos unificada, na qual os administradores podem publicar todos os aplicativos corporativos e recursos de dados necessários para seus usuários. Um administrador pode adicionar:

- Aplicativos Web, aplicativos SaaS e aplicativos habilitados para MAM SDK ou aplicativos preparados com MDX
- Aplicativos móveis de produtividade Citrix
- Aplicativos móveis nativos, como arquivos .ipa ou .apk
- Aplicativos Apple App Store e Google Play
- Links de Web
- Citrix Virtual Apps publicados usando o Citrix StoreFront

Exemplo de usuário: depois que um usuário registra seu dispositivo no XenMobile, ele acessa a XenMobile Store por meio do aplicativo Citrix Secure Hub. O usuário pode ver todos os aplicativos e serviços corporativos disponíveis para ele. Os usuários podem clicar em um aplicativo para instalá-lo, acessar os dados, avaliar e revisar o aplicativo, além de baixar as atualizações de aplicativos da XenMobile Store.

Opções de registro do usuário

April 8, 2021

Você pode fazer com que os usuários registrem seus dispositivos no XenMobile de várias maneiras. Antes de considerar pontos específicos, decida quais dispositivos você deseja registrar no MDM+MAM, MDM ou MAM. Para obter mais informações sobre esses modos de gerenciamento, consulte [Modos de gerenciamento](#).

No nível mais alto, existem quatro opções de registro:

- **Convite para registro:** envie um convite para registro ou uma URL de convite aos usuários. Os URLs e convites para registro não estão disponíveis para dispositivos Android Enterprise ou Windows.

- **Portal de autoajuda:** configure um portal que os usuários possam visitar para fazer o download do Secure Hub e registrar seus dispositivos ou enviar um convite de registro a eles mesmos.
- **Registro manual:** envie um e-mail, manual ou alguma outra comunicação para informar aos usuários que o sistema está disponível para registro. Os usuários então baixam o Secure Hub e registram seus dispositivos manualmente.
- **Empresarial:** outra opção para o registro de dispositivos é por meio do Apple Deployment Program e do Google Android Enterprise. Por meio de cada um desses programas, você pode comprar dispositivos pré-configurados e prontos para o uso pelos funcionários. Para obter mais informações, consulte os artigos do Apple Deployment Program no [Suporte da Apple](#) e a documentação do Google Android Enterprise no [site do Android Enterprise](#).

Convite para registro

Você pode enviar um convite para registro por e-mail para usuários com dispositivos iOS, macOS ou Android legado. Os URLs e convites para registro não estão disponíveis para dispositivos Android Enterprise ou Windows.

Você também pode enviar um link de instalação por SMTP ou SMS aos usuários com dispositivos iOS, macOS, Android, ou Windows. Para obter mais informações, consulte [Registrar dispositivos](#).

Se você optar por usar o método de convite para registro, pode:

- Escolher entre até sete modos de segurança de registro, dependendo da plataforma.
- Usar qualquer combinação de modos.
- Ativar ou desativar os modos na página **Configurações**.
- Selecionar um padrão entre Nome de usuário + Senha, Dois fatores e Nome de usuário + PIN. Para obter informações sobre cada modo de segurança de registro, consulte [Para configurar modos de segurança de registro](#).

Se você escolher baseado em certificado, considere excluir a autenticação tradicional de Nome de usuário + Senha das opções permitidas. A autenticação de Nome de usuário + Senha pode expor um vetor de integração fraco em seu ambiente e potencialmente anular a qualidade da segurança exigida.

Convites servem a muitos propósitos. O uso mais comum de convites é notificar os usuários de que o sistema está disponível e que eles podem se registrar. Os URLs de convite são exclusivos. Depois que um usuário usa um URL de convite, o URL não está mais disponível. Você pode usar essa propriedade para limitar o registro de usuários ou dispositivos em seu sistema.

Ao configurar um perfil de registro, você pode controlar o número de dispositivos que usuários específicos podem registrar, com base em grupos do Active Directory. Por exemplo, você pode permitir à sua divisão Financeira apenas um dispositivo por usuário.

Esteja ciente dos custos extras e dos imprevistos de certas opções de registro. Por exemplo, enviar convites usando SMS requer infraestrutura extra. Para obter mais informações sobre essa opção, con-

sulte [Notificações](#).

Além disso, para enviar convites por e-mail, verifique se os usuários têm uma maneira de acessar e-mails fora do Secure Hub. Você pode usar um modo de segurança de registro de senha única (OTP) como uma alternativa às senhas do Active Directory para registro no MDM.

Portal de Autoajuda

Os usuários podem solicitar um convite de registro através do Portal de Autoajuda. O modo padrão é Nome de usuário + Senha, mas você também pode alterar esse requisito para Dois fatores ou Nome de usuário + PIN. Para obter informações sobre como configurar o Portal de Autoajuda, consulte [Para configurar modos de segurança de registro](#).

Registro manual

Com o registro manual, os usuários se conectam ao XenMobile por meio do AutoDiscovery ou inserindo as informações do servidor. Com o AutoDiscovery, os usuários fazem logon apenas com o endereço de email ou com as credenciais do Active Directory no formato Nome Principal do Usuário. Sem o AutoDiscovery, eles devem inserir o endereço do servidor e suas credenciais do Active Directory. Para obter mais informações sobre como configurar o AutoDiscovery, consulte [XenMobile AutoDiscovery Service](#).

Você pode facilitar o registro manual de várias maneiras. Você pode criar um guia, distribuí-lo aos usuários e fazer com que eles se registrem. O seu departamento de TI pode registrar os grupos de usuários manualmente em determinados intervalos de tempo. Você pode usar qualquer método semelhante em que os usuários devam inserir suas credenciais, informações do servidor ou todos esses dados.

Integração de usuários

Depois de configurar seu ambiente, você precisa decidir como colocar os usuários nesse ambiente. Uma seção anterior deste artigo discute as especificidades dos modos de segurança de registro do usuário. Esta seção discute como você chega aos usuários.

Registro aberto versus Convite seletivo

Durante a integração dos usuários, você pode permitir o registro por meio de dois métodos básicos:

- Registro aberto. Por padrão, qualquer usuário com credenciais LDAP e as informações do ambiente XenMobile pode se registrar.

- Registro limitado. Você pode limitar o número de usuários permitindo apenas que os usuários com convites se registrem. Você também pode limitar o registro aberto pelo grupo do Active Directory.

Com o método de convite, você também pode limitar o número de dispositivos que um usuário pode registrar. Na maioria das situações, o registro aberto é aceitável, mas há algumas coisas a serem consideradas:

- Para o registro MAM, você pode limitar facilmente o registro aberto por meio da associação ao grupo do Active Directory.
- Para o registro MDM, você pode limitar o número de dispositivos que podem se registrar com base na associação do grupo do Active Directory. Se você permitir apenas dispositivos corporativos em seu ambiente, essa limitação geralmente não é um problema. Contudo, você pode considerar esse método em um local de trabalho BYOD caso deseje limitar o número de dispositivos em seu ambiente.

Geralmente, o convite seletivo é realizado com menos frequência porque requer um pouco mais de trabalho do que o registro aberto. Para os usuários registrarem seus dispositivos em seu ambiente, você deve enviar um convite exclusivo para cada usuário. Para obter informações sobre como enviar um convite de registro, consulte [Envio de convite para registro](#).

Enquanto puder usar grupos do Active Directory para criar convites em lotes, você deve executar essa abordagem de forma incremental.

Primeiro contato com os usuários

Depois de decidir entre o registro aberto ou o convite seletivo e configurar esses ambientes, você deve informar os usuários sobre as opções de registro.

Se você usar o método de convite seletivo, as mensagens de e-mail e SMS farão parte do processo. Você também pode enviar e-mails através do console XenMobile para registro aberto. Para obter detalhes, consulte [Envio de convite para registro](#).

Em ambos os casos, lembre-se de que, para email, você precisa de um servidor SMTP. Para mensagens de texto, você precisa de um servidor SMS. Esses servidores podem incorrer em custos extras a serem considerados ao tomar sua decisão. Antes de selecionar um método, considere como você espera que novos usuários acessem informações, como email. Se você quiser que todos os usuários acessem seus emails através do XenMobile, enviar um convite por e-mail seria problemático.

Você também pode enviar comunicações por outros meios fora do XenMobile para um ambiente de registro aberto. Para essa opção, certifique-se de incluir todas as informações relevantes. Informe os usuários onde eles podem obter o aplicativo Secure Hub e qual método usar para se registrar. Se a descoberta estiver desativada, forneça também aos usuários o endereço do XenMobile Server. Para saber mais sobre o AutoDiscovery, consulte [XenMobile AutoDiscovery Service](#).

Ajuste das operações do XenMobile

May 24, 2021

O desempenho e a estabilidade das operações do XenMobile envolvem muitas configurações no XenMobile e dependem da configuração do banco de dados do Citrix ADC e do SQL Server. Este artigo foca nas configurações mais frequentemente definidas pelos administradores, relacionadas ao ajuste e à otimização do XenMobile. A Citrix recomenda que você avalie cada uma das configurações deste artigo antes de implantar o XenMobile.

Importante:

Essas diretrizes pressupõem que a CPU e a RAM do XenMobile Server são adequadas para o número de dispositivos. Para obter mais informações sobre escalabilidade, consulte [Escalabilidade e desempenho](#).

As seguintes propriedades do servidor se aplicam globalmente a operações, usuários e dispositivos a uma instância inteira do XenMobile. A alteração em algumas propriedades do servidor requer uma reinicialização de cada nó do XenMobile Sever. O XenMobile avisa quando uma reinicialização é necessária.

Essas diretrizes de ajuste se aplicam a ambientes em cluster e não-cluster.

hibernate.c3p0.idle_test_period

Essa propriedade do XenMobile Server, uma chave personalizada, determina o tempo ocioso em segundos antes de uma conexão ser validada automaticamente. Configure a chave da seguinte maneira. O padrão é **30**.

- Chave: **chave personalizada**
- Chave: **hibernate.c3p0.idle_test_period**
- Valor: **120**
- Nome de exibição: **hibernate.c3p0.idle_test_period**
- Descrição: **período de teste de inatividade de hibernação**

hibernate.c3p0.max_size

Essa chave personalizada determina o número máximo de conexões que o XenMobile pode abrir no banco de dados do SQL Server. O XenMobile usa o valor especificado para esta chave personalizada como um limite superior. As conexões abrem somente se você precisar delas. Baseie suas configurações na capacidade do seu servidor de banco de dados.

Observe a seguinte equação em uma configuração em cluster. Sua conexão c3p0 multiplicada pelo número de nós é igual ao número máximo real de conexões que o XenMobile pode abrir para o banco de dados do SQL Server.

Na configuração em cluster e não-cluster, definir um valor muito alto com um SQL Server subdimensionado pode causar problemas de recursos no lado do SQL durante o pico de carga. Configurar um valor muito baixo poderá afetar o bom-aproveitamento dos recursos SQL disponíveis.

Configure a chave da seguinte maneira. O padrão é **1000**.

- Chave: **hibernate.c3p0.max_size**
- Valor: **1000**
- Nome de exibição: **hibernate.c3p0.max_size**
- Descrição: conexões de banco de dados ao SQL

hibernate.c3p0.min_size

Essa chave personalizada determina o número mínimo de conexões que o XenMobile abre no banco de dados do SQL Server. Configure a chave da seguinte maneira. O padrão é **100**.

- Chave: **hibernate.c3p0.min_size**
- Valor: **100**
- Nome de exibição: **hibernate.c3p0.min_size**
- Descrição: conexões de banco de dados ao SQL

hibernate.c3p0.timeout

Essa chave personalizada determina o tempo limite de ociosidade. Se você usar o failover de cluster do banco de dados, a Citrix recomenda que você adicione essa chave personalizada e defina-a para reduzir o tempo limite de inatividade. O padrão é **120**.

- Chave: **chave personalizada**
- Chave: **hibernate.c3p0.timeout**
- Valor: **120**
- Nome de exibição: **hibernate.c3p0.timeout**
- Descrição: tempo limite de inatividade do banco de dados

Intervalo de pulsação de serviços push

Esta configuração determina com que frequência um dispositivo iOS verifica se uma notificação de APNs não foi entregue nesse ínterim. Aumentar a frequência de pulsação dos APNs pode otimizar as comunicações do banco de dados. Um valor muito grande pode adicionar carga desnecessária. Essa configuração se aplica apenas ao iOS. O padrão é **20** horas.

Se você tiver vários dispositivos iOS em seu ambiente, o intervalo de pulsação pode levar a uma carga maior do que a necessária. As ações de segurança, como apagamento seletivo, bloqueio e apagamento completo, não dependem dessa pulsação. O motivo é que uma notificação de APNs é enviada ao dispositivo quando essas ações são executadas. Esse valor determina a rapidez com que uma política é atualizada depois que a associação ao Grupo do Active Directory é alterada. Como tal, muitas vezes é adequado aumentar esse valor para algo entre 12 e 20 horas para reduzir a carga.

Tamanho do pool de conexões APNS de iOS MDM

Um pool de conexões APNs muito pequeno pode afetar negativamente o desempenho das atividades de APNs quando você tem mais de 100 dispositivos. Os problemas de desempenho incluem a implantação mais lenta de aplicativos e políticas em dispositivos e o registro mais lento de dispositivos. O padrão é **1**. Recomendamos que você aumente esse valor em 1 a cada cerca de 400 dispositivos.

auth.ldap.connect.timeout

Para compensar lentas respostas LDAP, a Citrix recomenda que você adicione as propriedades do servidor para as seguintes chaves personalizadas.

- Chave: **chave personalizada**
- Chave: **auth.ldap.connect.timeout**
- Valor: **60000**
- Nome de exibição: **auth.ldap.connect.timeout**
- Descrição: **tempo limite da conexão LDAP**

auth.ldap.read.timeout

Para compensar lentas respostas LDAP, a Citrix recomenda que você adicione as propriedades do servidor para as seguintes chaves personalizadas.

- Chave: **chave personalizada**
- Chave: **auth.ldap.read.timeout**
- Valor: **60000**
- Nome de exibição: **auth.ldap.read.timeout**
- Descrição: **tempo limite de leitura do LDAP**

Outras otimizações de servidores

Propriedade do servidor	Configuração padrão	Por que mudar essa configuração?
Implementação em segundo plano	1.440 minutos	A frequência de implantações de políticas em segundo plano, em minutos. Aplica-se apenas a conexões permanentes de dispositivos Android. Aumentar a frequência de implantações de políticas reduz a carga do servidor. A configuração recomendada é 1440 (24 horas).
Inventário de hardware em segundo plano	1.440 minutos	A frequência do inventário de hardware em segundo plano, em minutos. Aplica-se apenas a conexões permanentes de dispositivos Android. Aumentar a frequência do inventário de hardware reduz a carga do servidor. A configuração recomendada é 1440 (24 horas).
Intervalo para verificação de usuário do Active Directory excluído	15 minutos	O tempo de sincronização padrão do Active Directory é de 15 minutos. O valor 0 impede que o XenMobile verifique usuários do Active Directory excluídos. A configuração recomendada é de 15 minutos.

MaxNumberOfWorker	3	O número de threads utilizados ao importar várias licenças de compra por volume. O padrão é 3 . Se precisar de mais otimização, você pode aumentar o número de threads. No entanto, lembre-se de que com um número maior de threads, como 6, uma importação de compra por volume resulta em uso de CPU alto.
--------------------------	---	---

Como verificar deadlocks em um banco de dados SQL e excluir dados históricos

Quando você vir deadlocks, execute a consulta a seguir para ver os deadlocks. Depois, um administrador de banco de dados ou a equipe do Microsoft SQL pode confirmar as informações.

Consulta SQL

```
1 SELECT
2
3 db.name DB_Service,
4
5 tl.request_session_id,
6
7 wt.blocking_session_id,
8
9 OBJECT_NAME(p.OBJECT_ID) BlockedObjectName,
10
11 tl.resource_type,
12
13 h1.TEXT AS RequestingText,
14
15 h2.TEXT AS BlockingText,
16
17 tl.request_mode
18
```

```
19 FROM sys.dm_tran_locks AS tl
20
21 INNER JOIN sys.databases db ON db.database_id = tl.resource_database_id
22
23 INNER JOIN sys.dm_os_waiting_tasks AS wt ON tl.lock_owner_address = wt.
    resource_address
24
25 INNER JOIN sys.partitions AS p ON p.hobt_id = tl.
    resource_associated_entity_id
26
27 INNER JOIN sys.dm_exec_connections ec1 ON ec1.session_id = tl.
    request_session_id
28
29 INNER JOIN sys.dm_exec_connections ec2 ON ec2.session_id = wt.
    blocking_session_id
30
31 CROSS APPLY sys.dm_exec_sql_text(ec1.most_recent_sql_handle) AS h1
32
33 CROSS APPLY sys.dm_exec_sql_text(ec2.most_recent_sql_handle) AS h2
34
35 GO
36 <!--NeedCopy-->
```

Limpar o banco de dados

Importante:

Faça backup do banco de dados antes de fazer alterações nas tabelas.

1. Execute a consulta a seguir para verificar os dados históricos.

```
1 select COUNT(*) as total_record from dbo.EWDEPLOY_HISTO;
2 select COUNT(*) as total_record from dbo.EWSESS;
3 select COUNT(*) as total_record from dbo.EWAUDIT;
4 <!--NeedCopy-->
```

2. Exclua os dados das três tabelas anteriores.

Nota:

Você talvez não possa ver dados históricos em uma tabela. Em caso afirmativo, ignore a execução da consulta truncada dessa tabela específica.

```
1 truncate TABLE dbo.EWDEPLOY_HISTO;
2 truncate TABLE dbo.EWSESS;
3 truncate TABLE dbo.EWAUDIT;
```

```
4 <!--NeedCopy-->
```

3. Desbloquear as consultas SELECT que foram bloqueadas devido a deadlocks. Essa etapa cuida de mais deadlocks.

```
1 ALTER DATABASE <database_name> SET          READ_COMMITTED_SNAPSHOT
   ON WITH ROLLBACK IMMEDIATE
2 <!--NeedCopy-->
```

4. Por padrão, a limpeza do banco de dados é de sete dias para reter os dados de retenção de sessão e os dados de retenção de auditoria, o que é alto para muitos usuários. Altere o valor de limpeza para 1 ou 2 dias. Nas propriedades do servidor, faça a seguinte alteração:

```
1 zdm.dbcleanup.sessionRetentionTimeInDays = 1 day
2 zdm.dbcleanup.deployHistRetentionTimeInDays = 1 day
3 zdm.dbcleanup.auditRetentionTimeInDays=1 day
4 <!--NeedCopy-->
```

Limpar órfãos na tabela KEYSTORE

Se os nós XenMobile tiverem desempenho ruim, verifique se a tabela KEYSTORE é muito grande. O XenMobile armazena certificados de registro nas tabelas ENROLLMENT_CERTIFICATE e KEYSTORE. Quando você exclui ou registra novamente os dispositivos, os certificados na tabela ENROLLMENT_CERTIFICATE são excluídos. As entradas na tabela KEYSTORE permanecem, o que pode causar problemas de desempenho. Execute o procedimento a seguir para limpar os órfãos da tabela KEYSTORE.

Importante:

Faça backup do banco de dados antes de fazer alterações nas tabelas.

1. Execute a consulta a seguir para verificar os dados históricos.

```
1 select COUNT(*) from KEYSTORE
2 <!--NeedCopy-->
```

2. Verifique se há órfãos na tabela KEYSTORE com a seguinte consulta.

```
1 WITH cte(KEYSTORE_ID)
2 AS (SELECT KEYSTORE_ID
3     FROM ENROLLMENT_CERTIFICATE
4     UNION
5     SELECT CA_KEYSTORE_ID
6     FROM LDAP_CONFIG
7     UNION
```

```

8     SELECT CLIENT_KEYSTORE_ID
9     FROM LDAP_CONFIG
10    UNION
11    SELECT KEYSTORE_ID
12    FROM SAML_SERVICE_PROVIDER
13    UNION
14    SELECT KEYSTORE_ID
15    FROM SERVER_CERTIFICATE)
16 SELECT keystore.id
17 FROM keystore
18     LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
19 WHERE KEYSTORE_ID IS NULL;
20 <!--NeedCopy-->

```

3. Limpe os órfãos usando a seguinte consulta.

```

1  WITH cte(KEYSTORE_ID)
2    AS (SELECT KEYSTORE_ID
3         FROM ENROLLMENT_CERTIFICATE
4         UNION
5         SELECT CA_KEYSTORE_ID
6         FROM LDAP_CONFIG
7         UNION
8         SELECT CLIENT_KEYSTORE_ID
9         FROM LDAP_CONFIG
10        UNION
11        SELECT KEYSTORE_ID
12        FROM SAML_SERVICE_PROVIDER
13        UNION
14        SELECT KEYSTORE_ID
15        FROM SERVER_CERTIFICATE)
16 DELETE FROM keystore
17 WHERE id IN
18 (
19     SELECT keystore.id
20     FROM keystore
21         LEFT JOIN cte ON keystore.id = cte.KEYSTORE_ID
22     WHERE KEYSTORE_ID IS NULL AND keystore.TYPE = 'X_509'
23 );
24 <!--NeedCopy-->

```

4. Adicione um índice à tabela KEYSTORE para melhorar a eficiência da pesquisa.

```

1  DROP INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE";
2  ALTER TABLE "KEYSTORE" ALTER COLUMN "NAME" NVARCHAR(255) NULL;

```

```
3 CREATE INDEX "KEYSTORE_NAME_IDX" ON "KEYSTORE"("NAME") INCLUDE ("
  ID", "TYPE", "CONTENT", "PASSWORD", "PUBLICLY_TRUSTED", "
  DESCRIPTION", "ALIAS", "MODIFICATION_DATE");
4 <!--NeedCopy-->
```

Provisionamento e desprovisionamento de aplicativos

November 30, 2020

O provisionamento de aplicativos gira em torno do gerenciamento do ciclo de vida de aplicativos móveis: preparar, configurar, entregar e gerenciar aplicativos móveis em um ambiente XenMobile. Em alguns casos, desenvolver ou modificar o código do aplicativo também pode fazer parte do processo de provisionamento. O XenMobile está equipado com várias ferramentas e processos que você pode usar para provisionamento de aplicativos.

Antes de ler este artigo sobre o provisionamento de aplicativos, recomendamos ler os artigos a seguir:

- [Aplicativos - Comunidades do usuário](#)

Depois de finalizar o tipo de aplicativos que sua organização planeja fornecer aos usuários, você pode descrever o processo de gerenciamento dos aplicativos em todo o ciclo de vida.

Considere os seguintes pontos ao definir seu processo de provisionamento de aplicativo:

- **Perfil de aplicativos:** sua organização pode começar com um número limitado de aplicativos. No entanto, o número de aplicativos gerenciados pode aumentar rapidamente conforme as taxas de adoção dos usuários aumentam e o ambiente se expande. Defina perfis de aplicativos específicos desde o início para facilitar o gerenciamento do provisionamento de aplicativos. O perfil do aplicativo ajuda você a categorizar aplicativos em grupos lógicos de uma perspectiva não técnica. Por exemplo, você pode criar perfis de aplicativos com base nos seguintes fatores:
 - Versão: versão do aplicativo para acompanhamento
 - Instâncias: várias instâncias implantadas para diferentes conjuntos de usuários, por exemplo, com diferentes níveis de acesso
 - Plataforma: iOS, Android ou Windows
 - Público-alvo: usuários padrão, departamentos, executivos de nível C
 - Propriedade: departamento que possui o aplicativo
 - Tipo: MDX, Público, Web e SaaS ou links da Web
 - Ciclo de atualização: com que frequência o aplicativo é atualizado
 - Licenciamento: requisitos de licenciamento e propriedade
 - Políticas do MAM SDK ou MDX: para aplicar recursos MDX a seus aplicativos móveis
 - Acesso à rede: tipo de acesso, como Secure Browse ou VPN completa

Nota:

Com túnel - SSO de Web é o nome do Secure Browse nas configurações de MDX. O comportamento é o mesmo.

Exemplo:

Fator	Secure Mail	Email	In-House	Epic Rover
Versão	10.1	10.1	X.x	X.x
Instância	VIP	Médicos	Clínico	Clínico
Plataforma	iOS	iOS	iOS	iOS
Usuários-alvo	Usuários VIP	Médicos	Usuários Clínicos	Usuários Clínicos
Propriedade	IT	IT	IT	IT
Digite	MDX	MDX	Nativo	Público
Ciclo de Atualização	Trimestral	Trimestral	Anual	N/D
Licenciamento	N/D	N/D	N/D	Compra por volume
Políticas de MDX	Sim	Sim	Sim	Não
Acesso à rede	VPN	VPN	VPN	Público

- **Versão de aplicativos:** manter e acompanhar versões de aplicativos é uma parte crítica do processo de provisionamento. O controle de versão é transparente para os usuários. Eles só recebem notificações quando uma nova versão do aplicativo está disponível para download. Do seu ponto de vista, revisar e testar cada versão do aplicativo na condição de não produção também é fundamental para evitar o impacto na produção.

Também é importante avaliar se uma atualização específica é necessária. As atualizações de aplicativos geralmente são de dois tipos: o primeiro tipo é uma atualização secundária, como a correção de um bug específico. O segundo tipo é uma atualização principal, que introduz mudanças significativas e melhorias no aplicativo. Em ambos os casos, leia cuidadosamente as notas de versão do aplicativo para avaliar se a atualização é necessária.

- **Desenvolvimento de aplicativos:** ao integrar o MAM SDK nos aplicativos móveis que você desenvolveu, você aplica recursos MDX a esses aplicativos. Veja [Visão geral do SDK MAM](#).

O MAM SDK substitui o MDX Service e o MDX Toolkit, que está programado para ser preterido em setembro de 2021. Para obter informações sobre a preparação de aplicativos, consulte [Endpoint Management MDX Service](#). O processo de provisionamento de aplicativo para um

aplicativo preparado é diferente do processo de provisionamento de um aplicativo padrão não preparado.

- **Segurança do aplicativo:** você define os requisitos de segurança de aplicativos individuais ou perfis de aplicativos como parte do processo de provisionamento. Você pode mapear requisitos de segurança para políticas específicas de MDM ou MAM antes de implantar os aplicativos. Esse planejamento simplifica e agiliza a implantação de aplicativos. Por exemplo:
 - Você pode querer implantar determinados aplicativos de uma forma diferente.
 - Você pode precisar fazer alterações de arquitetura em seu ambiente XenMobile. As alterações dependem do tipo de conformidade de segurança que os aplicativos exigem. Por exemplo, você pode querer que o dispositivo seja criptografado para permitir o uso de um aplicativo crítico de business intelligence. Ou um determinado aplicativo pode exigir criptografia SSL de ponta a ponta ou geocerca.
- **Entrega de aplicativos:** o XenMobile permite entregar aplicativos como aplicativos MDM ou como aplicativos MAM. Os aplicativos MDM aparecem na XenMobile Store. Esta loja permite que você forneça convenientemente aplicativos públicos ou nativos aos usuários. O único controle de aplicativos MDM que você gerencia é o de imposição de restrições no nível do dispositivo. No entanto, a entrega de aplicativos usando o MAM permite o controle total da entrega do aplicativo e do próprio aplicativo. Normalmente, entregar os aplicativos através do MAM é mais adequado.
- **Manutenção de aplicativos:**
 - Realize uma auditoria inicial: acompanhe a versão do aplicativo em seu ambiente de produção e o último ciclo de atualização. Anote os recursos específicos ou as correções de bugs que exigiram a atualização.
 - Estabelecer linhas de base: mantenha uma lista da versão estável mais recente de cada aplicativo. Esta versão do aplicativo será a versão de fall-back caso ocorra um problema inesperado após a atualização. Desenvolva também um plano de reversão. Teste atualizações de aplicativos em um ambiente de teste antes de realizar a implantação de produção. Se possível, implante a atualização em um subconjunto de usuários de produção primeiro e, depois, em toda a base de usuários.
 - Inscreva-se para receber as notificações de atualização de software da Citrix e as notificações dos fornecedores de softwares de terceiros. Manter-se atualizado com a versão mais recente dos aplicativos é essencial. Uma compilação EAR (versão de acesso antecipado) pode estar disponível para teste.
 - Conceba uma estratégia para notificar usuários: defina uma estratégia para notificar os usuários quando as atualizações de aplicativos estiverem disponíveis. Prepare os usuários com treinamento antes da implantação. Você pode enviar várias notificações antes de atualizar os aplicativos. Dependendo do aplicativo, o melhor método de notificação será notificações por email ou sites.

O gerenciamento do ciclo de vida do aplicativo representa o ciclo de vida completo de um aplicativo desde sua implantação inicial até a desativação. O ciclo de vida de um aplicativo tem as seguintes fases:

1. Requisitos para especificações: comece com o caso de negócios e os requisitos do usuário.
2. Desenvolvimento: valide se o aplicativo atende às necessidades de negócios.
3. Teste: identifique usuários de teste, problemas e bugs.
4. Implantação: implante o aplicativo para usuários em produção.
5. Manutenção: atualize a versão do aplicativo. Implante o aplicativo em um ambiente de teste antes de atualizar o aplicativo em um ambiente de produção.

Exemplo de ciclo de vida do aplicativo usando o Secure Mail

1. Requisitos para especificações: como um requisito de segurança, você precisa de um aplicativo de email que esteja em contêiner e ofereça suporte às políticas de segurança de MDX.
2. Desenvolvimento: valide se o aplicativo atende às necessidades de negócios. Você deve poder aplicar controles de política de MDX ao aplicativo.
3. Teste: atribua o Secure Mail a um grupo de usuários de teste e implante o arquivo MDX correspondente do XenMobile Server. Os usuários de teste validam que eles podem enviar e receber emails com sucesso e têm acesso a calendário e contatos. Os usuários de teste também relatam problemas e identificam bugs. Com base no feedback dos usuários de teste, você otimiza a configuração do Secure Mail para uso em produção.
4. Implantação: quando a fase de teste é concluída, você atribui o Secure Mail aos usuários de produção e implanta o arquivo MDX correspondente do XenMobile.
5. Manutenção: uma nova atualização para o Secure Mail está disponível. Você baixa o novo arquivo MDX dos downloads do Citrix e substitui o arquivo MDX existente no XenMobile Server. Instrua os usuários a realizar a atualização. Nota: a Citrix recomenda que você conclua e teste esse processo em um ambiente de teste. Depois, carregue o aplicativo em um ambiente de produção XenMobile e implante o aplicativo para os usuários.

Para obter mais informações, consulte [Preparação de aplicativos móveis iOS](#) e [Preparação de aplicativos móveis Android](#).

Operações baseadas em painel

January 22, 2021

Você pode exibir informações de forma abrangente acessando o painel de controle do console XenMobile. Com essas informações, você pode ver problemas e operações bem-sucedidas rapidamente usando widgets.

O painel é geralmente a tela exibida primeiramente quando você faz logon no console XenMobile. Para acessar o painel de qualquer outro lugar no console, clique em **Analisar**. Clique em **Personalizar** no painel para editar o layout da página e editar os widgets exibidos.

- **Meus painéis:** você pode salvar até quatro painéis. Você pode editar esses painéis separadamente e exibir cada um selecionando o painel salvo.
- **Estilo de layout:** nessa linha você pode selecionar quantos widgets são exibidos no painel e a sua disposição.
- **Seleção de widgets:** você pode escolher as informações que aparecem no painel.
 - **Notificações:** marque a caixa de seleção acima dos números à esquerda para adicionar uma barra de notificações acima dos seus widgets. Esta barra mostra o número de dispositivos compatíveis, dispositivos inativos e dispositivos apagados ou registrados nas últimas 24 horas.
 - **Dispositivos por plataforma:** exibe o número de dispositivos gerenciados e não gerenciados por plataforma.
 - **Dispositivos por operadora:** exibe o número de dispositivos não gerenciados e gerenciados por operadora. Clique em cada barra para ver um demonstrativo por plataforma.
 - **Dispositivos gerenciados por plataforma:** exibe o número de dispositivos gerenciados por plataforma.
 - **Dispositivos não gerenciados por plataforma:** exibe o número de dispositivos não gerenciados por plataforma. Os dispositivos que são exibidos neste gráfico podem ter um agente instalado, mas tiveram seus privilégios revogados ou foram apagados.
 - **Dispositivos por Status do Gateway do ActiveSync:** exibe o número de dispositivos agrupados por status do ActiveSync Gateway. As informações mostram o status Desconhecido, Permitido ou Bloqueado. Você pode clicar em cada barra exibir os dados por plataforma.
 - **Dispositivos por propriedade:** exibe o número de dispositivos agrupados por status de propriedade. As informações de mostram o status de propriedade de propriedade da empresa, propriedade do funcionário ou desconhecido.
 - **Implantações de grupo de entrega com falha:** exibe o número total de falhas de implantação por pacote. Apenas os pacotes que têm falhas de implementação.
 - **Dispositivos por motivo de bloqueio:** exibe o número de dispositivos bloqueados pelo ActiveSync
 - **Aplicativos instalados:** usando este widget, você pode digitar um nome de aplicativo, e um gráfico exibe as informações sobre esse aplicativo.
 - **Uso da licença de aplicativos de compra por volume:** exibe as estatísticas de uso de aplicativos de compra por volume da Apple.

Casos de uso

Veja abaixo alguns exemplos de diferentes maneiras de usar widgets do painel para monitorar seu ambiente.

- Você implantou aplicativos móveis de produtividade e está recebendo tíquetes de suporte referentes à falha de instalação de aplicativos móveis de produtividade nos dispositivos. Use os widgets **Dispositivos Fora de Conformidade** e **Aplicativos Instalados** para ver os dispositivos que não têm aplicativos móveis de produtividade instalados.
- Você gostaria de monitorar dispositivos inativos para poder remover os dispositivos de seu ambiente e recuperar as licenças. Use o widget **Dispositivos Inativos** para acompanhar esta estatística.
- Você está recebendo tickets de suporte referentes a dados que não estão sendo sincronizados corretamente. Você pode querer usar os widgets **Dispositivos pelo Status do ActiveSync Gateway** e **Dispositivos pelo Motivo de bloqueio** para determinar se o problema está relacionado ao ActiveSync.

Criação de relatórios

Depois que seu ambiente for configurado e os usuários registrados, você poderá gerar relatórios para saber mais sobre sua implantação. O XenMobile vem com vários relatórios internos para ajudá-lo a ter uma melhor ideia sobre os dispositivos em execução no seu ambiente. Para obter detalhes, consulte [Relatórios](#).

Importante:

Embora seja possível usar o SQL Server para criar relatórios personalizados, Citrix não recomenda esse método. Usar o banco de dados do SQL Server dessa maneira pode ter consequências inesperadas na sua implantação do XenMobile. Se você decidir tomar esse método de emissão de relatórios, certifique-se de que as consultas do SQL são executadas usando uma conta de somente leitura.

Controle de Acesso Baseado em Função e Suporte XenMobile

April 1, 2021

O XenMobile usa o controle de acesso baseado em função (RBAC) para restringir o acesso de usuários e grupos às funções do sistema XenMobile, como o Console XenMobile, o Remote Support e a API pública. Este artigo descreve as funções incorporadas ao XenMobile e inclui considerações para decidir sobre o modelo de suporte para o XenMobile que se integre com o RBAC.

Nota:

O Remote Support não está mais disponível para novos clientes desde 1º de janeiro de 2019. Os clientes existentes podem continuar a usar o produto, no entanto, a Citrix não fornecerá melhorias ou correções.

Funções incorporadas

Você pode alterar o acesso concedido às seguintes funções internas e adicionar funções. Para obter o conjunto completo de permissões de acesso e recursos associados a cada função e suas configurações padrão, baixe os [Padrões de Controle de Acesso Baseado em Funções](#) da documentação do XenMobile. Para obter uma definição de cada recurso, consulte [Configurar funções com RBAC](#) na documentação do XenMobile.

Função de Administrador

Acesso padrão concedido:

- Acesso total ao sistema, exceto ao Remote Support.
- Por padrão, os administradores podem executar algumas tarefas de suporte, como verificar conectividade e criar pacotes de suporte.

Considerações:

- Alguns ou todos os administradores precisam de acesso ao Remote Support? Nesse caso, você pode editar a função de administrador ou adicionar funções de administrador.
- Para restringir ainda mais o acesso a alguns administradores ou grupos de administradores, adicione funções com base no modelo de administrador e edite as permissões.

Provisionamento de dispositivo

Acesso padrão concedido:

- Acesso ao console XenMobile para executar administração básica em dispositivos Windows CE: adicionar, alterar e remover dispositivos; usar a página Configurações.

Considerações:

- Aplica-se apenas a dispositivos Windows CE.

Suporte

Acesso padrão concedido:

- Acesso ao Remote Support.

Considerações:

- Para implantações do XenMobile Server no local: o suporte remoto permite que o pessoal da central de ajuda assuma o controle remotamente de dispositivos móveis gerenciados Windows CE e Android. Conversão de tela é compatível com somente dispositivos Samsung KNOX.
- O suporte remoto não está disponível para implantações do XenMobile Server em cluster no local.

Usuário

Acesso padrão concedido:

- Acesso restrito ao console XenMobile: recursos do dispositivo (como apagar, bloquear/desbloquear dispositivo; bloquear/desbloquear contêiner; ver local e definir restrições geográficas; tocar o dispositivo; redefinir senha do contêiner); adicionar, remover e enviar convites de registro.

Considerações:

- A função de usuário permite que você habilite os usuários a se ajudarem.
- Para suportar dispositivos compartilhados, crie uma função de usuário para o registro de dispositivos compartilhados.

Considerações para um modelo de suporte XenMobile

Os modelos de suporte que você pode adotar podem variar muito e podem envolver terceiros que lidam com suporte de nível 1 e 2, enquanto os funcionários lidam com suporte de nível 3 e 4. Independentemente de como você distribui a carga de suporte, tenha em mente as considerações nesta seção específicas à sua implantação e base de usuários do XenMobile.

Os usuários possuem dispositivos corporativos ou BYO?

A principal questão que influencia o suporte é quem possui os dispositivos do usuário em seu ambiente XenMobile. Se seus usuários tiverem dispositivos de propriedade da empresa, você poderá oferecer um nível de suporte mais baixo, como forma de bloquear os dispositivos. Nesse caso, você pode fornecer um suporte técnico que ajude os usuários com problemas de dispositivos e como usar os dispositivos. Dependendo dos tipos de dispositivos que você precisa dar suporte, pense em como você pode usar as funções de provisionamento e suporte de dispositivos RBAC para a sua central de ajuda.

Se seus usuários tiverem dispositivos BYO, sua organização provavelmente espera que os usuários encontrem suas próprias fontes para suporte ao dispositivo. Nesse caso, o suporte fornecido pela sua organização é mais uma função administrativa focada em problemas específicos do XenMobile.

Qual é o seu modelo de suporte para computadores desktop?

Considere se o seu modelo de suporte para desktops é apropriado para outros dispositivos de propriedade da empresa. Você pode usar a mesma organização de suporte? Que treinamento adicional eles precisam?

Deseja dar aos usuários acesso ao Portal de Autoajuda do XenMobile?

Use **Configurações > Registro** para ativar o Portal de Autoajuda para um modo de segurança de registro. No Portal de Autoajuda, os usuários podem gerar links de registro que permitem registrar seus dispositivos ou enviar a si mesmos um convite de registro. Consulte [Para configurar modos de segurança de registro](#).

Monitoramento de sistemas

August 10, 2020

Para garantir o tempo de atividade ideal para o acesso e a conectividade do aplicativo, você deve monitorar os seguintes componentes principais no ambiente do XenMobile.

XenMobile server

O XenMobile Server gera e armazena logs no repositório local que você também pode exportar para um servidor de log de sistemas (syslogs). Você pode definir configurações de log para especificar restrições de tamanho, nível de log ou criar agentes de log personalizados para filtrar eventos específicos. Você pode consultar os logs do XenMobile Server no console XenMobile a qualquer momento. Você também pode exportar informações nos logs por meio do servidor syslog para seus servidores de log de produção do Splunk.

A lista a seguir descreve os diferentes tipos de arquivos de log disponíveis no XenMobile:

Arquivo de log de depuração: contém informações sobre o nível de depuração dos principais serviços da Web do XenMobile, incluindo mensagens de erro e ações relacionadas ao servidor.

Formato da mensagem:

```
<date> <timestamp> <loglevel> <class name (including the package)> - <id> <log message>
```

- onde <id> é um identificador exclusivo como sessionId.
- onde <log message> é a mensagem fornecida pelo aplicativo.

Arquivo de log de auditoria do administrador: contém informações de auditoria sobre as atividades no console XenMobile.

Nota:

O mesmo formato é usado para os logs de auditoria do administrador e de auditoria do usuário.

Formato da mensagem:

Com exceção dos valores obrigatórios de Date e Timestamp, todos os outros atributos são opcionais. Campos opcionais são representados com “ ” na mensagem.

```
<date> <timestamp> "<username/id>"<sessionid>"<deviceid>"<clientip>"
"<action>"<status>"<application name>"<app user id>"<user agent>"<
details>"
```

A tabela a seguir lista os eventos de log de auditoria do administrador disponíveis:

Mensagens de log de auditoria do administrador para eventos	Status
Login	sucesso/falha
Logout	sucesso/falha
Get admin	sucesso/falha
Update admin	sucesso/falha
Get application	sucesso/falha
Add application	sucesso/falha
Update application	sucesso/falha
Delete application	sucesso/falha
Bind application	sucesso/falha
Unbind application	sucesso/falha
Disable application	sucesso/falha
Enable application	sucesso/falha
Get category	sucesso/falha
Add category	sucesso/falha
Update category	sucesso/falha
Delete category	sucesso/falha
Add certificate	sucesso/falha
Delete certificate	sucesso/falha
Active certificate	sucesso/falha
CSR certificate	sucesso/falha

Mensagens de log de auditoria do administrador para eventos	Status
Export certificate	sucesso/falha
Delete certificate chain	sucesso/falha
Add certificate chain	sucesso/falha
Get connector	sucesso/falha
Add connector	sucesso/falha
Delete connector	sucesso/falha
Update connector	sucesso/falha
Get device	sucesso/falha
Bloquear dispositivo	sucesso/falha
Desbloquear dispositivo	sucesso/falha
Wipe device	sucesso/falha
Unwipe device	sucesso/falha
Delete device	sucesso/falha
Get role	sucesso/falha
Add role	sucesso/falha
Update role	sucesso/falha
Delete role	sucesso/falha
Bind role	sucesso/falha
Unbind role	sucesso/falha
Update config settings	sucesso/falha
Update workflow email	sucesso/falha
Add workflow	sucesso/falha
Delete workflow	sucesso/falha
Add Active Directory	sucesso/falha
Update Active Directory	sucesso/falha
Add masteruserlist	sucesso/falha
Update masteruserlist	sucesso/falha
Update DNS	sucesso/falha

Mensagens de log de auditoria do administrador para eventos	Status
Update Network	sucesso/falha
Update log server	sucesso/falha
Transfer log from log server	sucesso/falha
Update syslog	sucesso/falha
Update receiver updates	sucesso/falha
Update time server	sucesso/falha
Update trust	sucesso/falha
Add service record	sucesso/falha
Update service record	sucesso/falha
Update receiver email	sucesso/falha
Upload patch	sucesso/falha
Import snapshot	sucesso/falha
Fetch app store app details	sucesso/falha
Update MDM	sucesso/falha
Delete MDM	sucesso/falha
Add HDX	sucesso/falha
Update HDX	sucesso/falha
Delete HDX	sucesso/falha
Add Branding	sucesso/falha
Delete Branding	sucesso/falha
Update SSL offload	sucesso/falha
Add account property	sucesso/falha
Delete account property	sucesso/falha
Update account property	sucesso/falha
Add beacon	sucesso/falha

Arquivo de log de auditoria do usuário: contém informações relacionadas à atividade do usuário de dispositivos registrados.

Nota:

O mesmo formato é usado para os logs de auditoria do usuário e de auditoria do administrador.

Formato da mensagem:

Com exceção dos valores obrigatórios de Date e Timestamp, todos os outros atributos são opcionais. Campos opcionais são representados com “ “ na mensagem. Por exemplo,

```
<date> <timestamp> "<username/id>""<sessionid>""<deviceid>""<clientip>"
"<action>""<status>""<application name>""<app user id>""<user agent>""<
details>"
```

A tabela a seguir lista os eventos do log de auditoria do usuário disponíveis:

Mensagens de log de auditoria do usuário para eventos	Status
Login	sucesso/falha
Session time-out	sucesso/falha
Subscribe	sucesso/falha
Unsubscribe	sucesso/falha
Pre-launch	sucesso/falha
AGEE SSO	sucesso/falha
Token SAML para Citrix Files	sucesso/falha
Device registration	sucesso/falha
Device check	lock/wipe
Device update	sucesso/falha
Token refresh	sucesso/falha
Secret saved	sucesso/falha
Secret retrieved	sucesso/falha
User initiated change password	sucesso/falha
Mobile client download	sucesso/falha
Logout	sucesso/falha
Discovery Service	sucesso/falha
Endpoint Service	sucesso/falha

Funções do MDM	Status
REGHIVE	sucesso/falha
Cab inventory	sucesso/falha
Cab	sucesso/falha
Cab auto install	sucesso/falha
Cab shell install	sucesso/falha
Cab create folder	sucesso/falha
Cab file get	sucesso/falha
File create folder	sucesso/falha
File get	sucesso/falha
File sent	sucesso/falha
Script create folder	sucesso/falha
Script get	sucesso/falha
Script sent	sucesso/falha
Script shell execution	sucesso/falha
Script auto execution	sucesso/falha
APK inventory	sucesso/falha
APK	sucesso/falha
APK shell install	sucesso/falha
APK auto install	sucesso/falha
APK create folder	sucesso/falha
APK file get	sucesso/falha
APK App	sucesso/falha
EXT App	sucesso/falha
List get	sucesso/falha
List sent	sucesso/falha
Locate device	sucesso/falha
CFG	sucesso/falha
Desbloquear	sucesso/falha
SharePoint wipe	sucesso/falha

Funções do MDM	Status
SharePoint Configuration	sucesso/falha
Remove profile	sucesso/falha
Remove application	sucesso/falha
Remove unmanaged application	sucesso/falha
Remove unmanaged profile	sucesso/falha
IPA App	sucesso/falha
EXT App	sucesso/falha
Apply redemption code	sucesso/falha
Apply settings	sucesso/falha
Enable tracking device	sucesso/falha
App management policy	sucesso/falha
SD card wipe	sucesso/falha
Encrypted email attachment	sucesso/falha
Branding	sucesso/falha
Secure browser	sucesso/falha
Container browser	sucesso/falha
Container unlock	sucesso/falha
Container password reset	sucesso/falha
AG client auth creds	sucesso/falha

O Citrix ADC também monitora o estado do serviço da Web do XenMobile, que é configurado com probes de monitoramento inteligente para simular solicitações HTTP para cada nó do cluster do servidor XenMobile. Os probes determinam se o serviço está online e, em seguida, respondem com base na resposta recebida. No caso de um nó não responder como esperado, o Citrix ADC marca o servidor como inativo. Além disso, o Citrix ADC retira o nó do pool de balanceamento de carga e faz o log do evento para uso na geração de alertas por meio da solução de monitoramento Citrix ADC.

Você também pode usar ferramentas padrão de monitoramento de hipervisor para monitorar as máquinas virtuais do XenMobile e fornecer alertas relevantes em relação às métricas de utilização de CPU, memória e armazenamento.

SQL Server e banco de dados

O desempenho do SQL Server e do banco de dados afeta diretamente os XenMobile Services. A instância do XenMobile requer acesso ao banco de dados em todos os momentos e fica offline (por exemplo, para de responder) no caso de uma interrupção na infraestrutura do SQL. O console XenMobile pode continuar a funcionar por um tempo após problemas de espaço em disco com o SQL Server. Para garantir o tempo de atividade máximo do banco de dados e o desempenho adequado da carga de trabalho do XenMobile, você deve monitorar proativamente o estado de seus SQL Servers. Para obter mais informações sobre como monitorar seus SQL Servers, consulte [Visão geral de monitoramento e ajuste de desempenho](#). Além disso, você deve ajustar a alocação de recursos para CPU, memória e armazenamento para garantir acordos de nível de serviço à medida que seu ambiente XenMobile continua a crescer.

Citrix ADC

O Citrix ADC fornece a capacidade de registrar métricas no armazenamento interno ou enviar logs para um servidor de registro externo. Você pode configurar o servidor syslog para exportar logs do Citrix ADC para seus servidores de log de produção do Splunk. Os seguintes níveis de registro estão disponíveis no Citrix ADC:

- Emergência
- Alerta
- Crítico
- Erro
- Aviso
- Informativo

Os arquivos de log também são armazenados no repositório do Citrix ADC no diretório `/var/log/ns.log` e nomeados `newslog`. O Citrix ADC reúne e comprime os arquivos usando o algoritmo GZIP. O nome dos arquivos de log é `newslog.xx.gz`, em que `xx` representa um número de execução.

O Citrix ADC também suporta interceptações e alertas de SNMP como opção de monitoramento. Para obter uma lista de interceptações de SNMP, consulte o [SNMP monitoring](#).

Recuperação de desastres

April 14, 2020

Você pode desenvolver e configurar implantações do XenMobile que incluem vários locais de recuperação de desastres usando uma estratégia de failover ativo-passivo.

A estratégia de recuperação de desastres recomendada discutida neste artigo consiste em:

- Um único site ativo do XenMobile no datacenter de uma localização geográfica atendendo a todos os usuários da empresa globalmente, conhecido como o site principal.
- Um segundo site XenMobile no datacenter de um segundo local geográfico, conhecido como site de recuperação de desastre. Este site de recuperação de desastre fornece failover de site ativo-passivo em caso de falha de um datacenter em todo o site principal. O site principal inclui o XenMobile, o banco de dados SQL, a infraestrutura do Citrix ADC para facilitar o failover e fornecer aos usuários acesso ao XenMobile por meio do evento de falha de conectividade no site principal.

Os servidores XenMobile no site de recuperação de desastre permanecem off-line durante as operações normais e são colocados on-line apenas em cenários de recuperação de desastre, onde é necessário um failover completo do site principal para o site de recuperação de desastre. Os SQL Servers no site de recuperação de desastre devem estar ativos e prontos para atender às conexões antes de iniciar os servidores XenMobile no site de recuperação de desastre.

Essa estratégia de recuperação de desastre depende do failover manual da camada de acesso do Citrix ADC por meio de alterações de DNS para rotear conexões do MDM e do MAM para o site de recuperação de desastre no caso de uma indisponibilidade.

Nota:

Para usar essa arquitetura, você deve ter um processo para backups assíncronos dos bancos de dados e alguma maneira de garantir alta disponibilidade para a infraestrutura SQL.

Processo de Failover de Recuperação de Desastres

1. Se você estiver testando seu processo de failover de recuperação de desastre, encerre os servidores XenMobile no site principal para simular a falha do site.
2. Altere os registros DNS públicos dos servidores XenMobile para apontar para os endereços IP externos do site de recuperação de desastre.
3. Altere o registro DNS interno do SQL Server para apontar para o endereço IP do SQL Server do site de recuperação de desastre.
4. Coloque os bancos de dados XenMobile SQL on-line no site de recuperação de desastre. Certifique-se de que o SQL Server e o banco de dados estejam ativos e prontos para atender às conexões dos servidores XenMobile locais ao site.
5. Ative os servidores XenMobile no site de recuperação de desastre.

Processo de atualização do servidor XenMobile

Siga estas etapas sempre que você atualizar o XenMobile com patches e novas versões, para manter o código dos servidores principal e de recuperação de desastres uniformes.

1. Certifique-se de que os servidores XenMobile no site principal foram corrigidos ou atualizados.

Como funciona o GSLB

O GSLB é, no seu núcleo, uma forma de DNS. Os dispositivos Citrix ADC participantes atuam como servidores DNS autoritativos e resolvem os registros DNS para o endereço IP correto (geralmente o VIP que deve receber tráfego). O dispositivo Citrix ADC verifica a integridade do sistema antes de responder a uma consulta DNS direcionando o tráfego para esse sistema.

Quando um registro é resolvido, a função do GSLB na resolução do tráfego é concluída. O cliente se comunica diretamente com o endereço de IP virtual (VIP) de destino. O comportamento do cliente DNS desempenha um papel importante no controle de como e quando um registro expira. Isso está em grande parte fora dos limites do sistema Citrix ADC. Como tal, o GSLB está sujeito às mesmas limitações que a resolução de nomes DNS. Respostas de clientes em cache; entretanto, o balanceamento de carga dessa maneira não é tão em tempo real quanto o balanceamento de carga tradicional.

A configuração do GSLB no Citrix ADC, incluindo sites, serviços e monitores, existe para fornecer a resolução de nomes DNS correta.

A configuração real dos servidores de publicação (nesse cenário, a configuração criada pelo assistente Citrix ADC for XenMobile) não é afetada pelo GSLB. O GSLB é um serviço separado no Citrix ADC.

Desafios com a delegação de domínio ao usar o GSLB com o XenMobile

O assistente Citrix ADC for XenMobile configura o Citrix Gateway para o XenMobile. Esse assistente gera três servidores virtuais de balanceamento de carga e um servidor virtual Citrix Gateway.

Dois dos servidores virtuais de balanceamento de carga lidam com o tráfego do MDM, nas portas 443 e 8443. O Citrix Gateway recebe o tráfego do MAM e o encaminha para o terceiro servidor, o servidor virtual de balanceamento de carga do MAM, na porta 8443. Todo o tráfego para o servidor virtual de balanceamento de carga do MAM passa pelo Citrix Gateway.

O servidor virtual de balanceamento de carga do MAM requer o mesmo certificado SSL dos servidores XenMobile e usa o mesmo FQDN usado para registrar dispositivos. O servidor de balanceamento de carga do MAM também usa a mesma porta (8443) que um dos servidores de balanceamento de carga do MDM. Para permitir que o tráfego seja resolvido, o assistente Citrix ADC for XenMobile cria um registro DNS local no Citrix Gateway. O registro DNS corresponde ao FQDN usado para registrar dispositivos.

Essa configuração é efetiva quando a URL do servidor XenMobile não é uma URL de domínio do GSLB. Se uma URL de domínio do GSLB for usada como a URL do XenMobile Server, conforme exigido para recuperação de desastre, o registro DNS local impedirá que o Citrix Gateway resolva o tráfego para os servidores de balanceamento de carga do MDM.

Usando o Método CNAME para Recuperação de Desastres GSLB

Para resolver os desafios apresentados pela configuração padrão criada pelo assistente Citrix ADC for XenMobile, você pode criar um registro CNAME para o FQDN do XenMobile Server no domínio pai (`company.com`) e apontar um registro na subzona delegada (`gslb.company.com`) para a qual o Citrix ADC é autoritativo. Isso permite a criação do registro DNS A estático para o endereço VIP de balanceamento de carga do MAM, necessário para resolver o tráfego.

1. No DNS externo, crie um CNAME para o FQDN do XenMobile Server que aponta para o FQDN do domínio GSLB no Citrix ADC GSLB. Você precisa de dois domínios GSLB: um para o tráfego do MDM e outro para o tráfego do MAM (Citrix Gateway).

Exemplo:

```
CNAME = xms.company.com IN CNAME xms.gslb.comany.com
```

2. Na instância do Citrix Gateway de cada site, crie um servidor virtual GSLB com um FQDN, para o qual o registro CNAME está apontando.

Exemplo:

```
bind gslb vserver xms-gslb -domainName xms.gslb.company.com
```

Ao usar o assistente Citrix ADC for XenMobile para implantar o Citrix Gateway, use a URL do servidor XenMobile ao configurar o servidor de balanceamento de carga MAM. Isso cria um registro DNS A estático para a URL do XenMobile Server.

3. Teste com clientes registrados no Secure Hub usando a URL do XenMobile Server (`xms.company.com`).

Este exemplo usa os seguintes FQDNs:

- `xms.company.com` é a URL usada pelo tráfego do MDM e é usada pelo registro de dispositivos, que é configurado neste exemplo usando o assistente Citrix ADC for XenMobile.
- `xms.gslb.company.com` é o FQDN do domínio GSLB para o XenMobile Server.

Processo de Suporte Citrix

January 22, 2021

Você pode ativar os Serviços de Suporte Técnico da Citrix para ajudar nos problemas relacionados aos produtos Citrix. O grupo oferece soluções alternativas e trabalha de mãos dadas com as equipes de desenvolvimento para oferecer soluções.

Citrix Consulting Services ou Citrix Education Services oferecem ajuda relacionada ao treinamento de produtos, conselhos sobre uso, configuração, instalação ou arquitetura e design do ambiente do produto.

A Citrix Consulting ajuda com os projetos relacionados ao produto Citrix, incluindo provas de conceitos, avaliação de impacto econômico, verificações de integridade de infraestrutura, análise de requisitos de projeto, verificação de projeto de arquitetura, integração e desenvolvimento de processos operacionais.

A Citrix Education oferece o melhor treinamento e certificação de TI da Citrix em virtualização, nuvem e tecnologias de rede.

A Citrix recomenda que você aproveite ao máximo os recursos e recomendações do Citrix Self-Help antes de criar um caso de suporte. Por exemplo, existem vários lugares onde você pode acessar artigos e boletins escritos por especialistas técnicos da Citrix, ver a documentação do produto para conhecer as soluções e tecnologias da Citrix ou ler materiais diretamente dos executivos da Citrix, equipes de produtos e especialistas técnicos. Consulte as páginas [Knowledge Center](#), [Documentação de produtos](#) e [Blogs](#), respectivamente.

Para obter assistência mais interativa, você pode participar de fóruns de discussão nos quais pode fazer perguntas e obter respostas reais de outros clientes, compartilhar ideias, opiniões, informações técnicas e práticas recomendadas em grupos de usuários e grupos de interesse ou interagir com engenheiros do Citrix Support. que monitoram sites de redes sociais do Citrix Support. Consulte as páginas [Fóruns de suporte](#) e [Comunidade Citrix](#), respectivamente.

Você também tem acesso a cursos de treinamento e certificação para desenvolver suas habilidades. Veja [Citrix Education](#).

O Citrix Insight Services fornece uma plataforma simples para solução de problemas on-line e um verificador de integridade para seu ambiente Citrix. Disponível para XenMobile, Citrix Virtual Apps and Desktops, Citrix Hypervisor e Citrix Gateway. Veja [Analysis Tool](#).

Para buscar suporte técnico, você pode criar um caso de suporte por telefone ou pela Web. Você pode usar a Web para resolver problemas de baixa e média gravidade e usar a opção de telefone para problemas de alta gravidade. Para obter informações sobre como entrar em contato com o suporte para solucionar problemas do XenMobile, consulte [Como entrar em contato com o suporte](#).

Se você procura um único ponto de contato altamente treinado com ampla experiência na entrega de soluções Citrix, a Citrix Services oferece um Gerente de Relacionamento Técnico. Para obter mais informações sobre ofertas e benefícios de serviços da Citrix, consulte [Citrix Worldwide Services](#).

Enviar convites para registro em grupo no XenMobile

April 1, 2021

Contribuição de John Bartel III

Você pode enviar convites para registro para grupos e grupos aninhados no XenMobile Server. Os convites para registro não estão disponíveis para dispositivos Android Enterprise e Windows.

Ao configurar o convite de grupo, você pode especificar uma ou várias plataformas de dispositivos. Você também pode marcar dispositivos para, por exemplo, distinguir dispositivos de propriedade da empresa dos dispositivos de propriedade dos funcionários. Em seguida, você define o tipo de autenticação para dispositivos do usuário.

Nota:

Se você planejar usar modelos de notificação personalizados, deverá configurar os modelos antes de você configurar os modos de segurança de registro. Para obter mais informações sobre modelos de notificação, consulte [Criar e atualizar modelos de notificação](#).

Para obter mais informações sobre configurações básicas em contas de usuário, funções e modos de segurança de registro e convites, consulte [Contas de usuário, funções e registro](#).

Etapas gerais

1. No console XenMobile, clique em **Gerenciar > Convites para registro**.
2. Clique em **Adicionar** no canto superior esquerdo da tela e clique em **Adicionar convite**.
3. Clique em **Grupo** no menu **Destinatário**.

Esta etapa permite escolher uma ou várias plataformas. Se você tiver um misto de diferentes plataformas de sistema operacional em sua empresa, escolha todas as plataformas. Limpe a seleção da plataforma apenas se você tiver certeza de que nenhum usuário está usando a plataforma específica.

4. Você pode marcar dispositivos durante o processo de convite. Escolha **Corporativo** ou **Funcionário**.

A marcação facilita a separação de dispositivos corporativos e dispositivos de propriedade dos funcionários.

5. Na lista **Domínio**, escolha o domínio no qual o grupo existe.
6. Na lista **Grupo**, selecione o grupo do Active Directory para o qual você deseja enviar os convites.
7. O **Modo de registro** permite que você defina o tipo de segurança de autenticação que preferir para os usuários.
 - Nome de usuário + Senha
 - Alta Segurança
 - URL de Convite
 - URL de Convite + PIN
 - URL de Convite + Senha

- Dois Fatores
 - Nome de usuário + PIN
8. Para os modelos **Download do Agente**, **URL de registro**, **PIN de registro** e **Confirmação de registro**, escolha o modelo de notificação personalizado que você criou no passado. Ou escolha o padrão listado.

Se você planejar usar modelos de notificação personalizados, deverá configurar os modelos antes de você configurar os modos de segurança de registro. Para obter mais informações sobre modelos de notificação, consulte [Notificações](#).

Para esses modelos de notificação, use a configuração do servidor SMTP configurado no XenMobile. Defina suas informações SMTP primeiro antes de prosseguir.

Nota:

As opções **Expira após** e **Máximo de tentativas** são alteradas com base na opção do **modo de registro** que você escolher. Você não pode alterar essas opções.

9. Selecione ON para **Enviar convite** e clique em **Salvar e Enviar** para concluir o processo.

Suporte a grupo aninhado

Você pode usar grupos aninhados para enviar convites. Normalmente, os grupos aninhados são usados em ambientes de grande porte, onde grupos com permissões semelhantes são vinculados uns aos outros.

Navegue para **Configurações > LDAP** e ative a opção **Proteger grupos aninhados**.

Resolução de problemas e limitações conhecidas

Problema: os convites estão sendo enviados aos usuários, mesmo que tenham sido removidos de um grupo do Active Directory.

Solução: dependendo do tamanho do seu ambiente do Active Directory, pode levar até seis horas para que as alterações se propaguem para todos os servidores. Se um usuário ou grupo aninhado foi removido recentemente, o XenMobile ainda poderá considerar esses usuários como parte do grupo.

Portanto, é melhor aguardar até seis horas antes de enviar outro convite em grupo para o seu grupo.

Configurar um servidor de atestado de integridade de dispositivo no local

April 23, 2020

Contribuição de Sanket Mishra

Você pode ativar o Atestado de Integridade de Dispositivo (DHA, Device Health Attestation) para dispositivos móveis Windows 10 por meio de um Windows Server no local. Para habilitar o DHA no local, você primeiro configura um servidor DHA.

Depois de configurar o servidor DHA, você cria uma política do XenMobile Server para habilitar o serviço DHA local. Para obter informações sobre como criar essa política, consulte [Política de dispositivo de Atestado de Integridade de Dispositivo](#).

Pré-requisitos para um servidor DHA

- Um servidor executando o Windows Server Technical Preview 5 ou posterior, instalado usando a opção de instalação do Desktop Experience.
- Um ou mais dispositivos clientes do Windows 10. Esses dispositivos devem ter o TPM 1.2 ou 2.0 executando a versão mais recente do Windows.
- Esses certificados:
 - **Certificado SSL DHA.** Um certificado SSL x.509 que é vinculado a uma raiz confiável corporativa com uma chave privada exportável. Este certificado protege as comunicações de dados DHA em trânsito, incluindo as comunicações servidor a servidor (serviço DHA e servidor MDM) e servidor a cliente (serviço DHA e dispositivo Windows 10).
 - **Certificado de assinatura do DHA.** Um certificado x.509 que é vinculado a uma raiz confiável corporativa com uma chave privada exportável. O serviço DHA usa esse certificado para assinatura digital.
 - **Certificado de criptografia DHA.** Um certificado x.509 que é vinculado a uma raiz confiável corporativa com uma chave privada exportável. O serviço DHA também usa esse certificado para criptografia.
- Escolha um destes modos de validação de certificado:
 - **EKCert.** O modo de validação EKCert é otimizado para dispositivos em organizações que não estão conectadas à Internet. Os dispositivos que se conectam a um serviço DHA em execução no modo de validação EKCert não têm acesso direto à Internet.
 - **AIKCert.** O modo de validação AIKCert é otimizado para ambientes operacionais que têm acesso à Internet. Os dispositivos que se conectam a um serviço DHA em execução no modo de validação AIKCert devem ter acesso direto à Internet e estar habilitados a obter um certificado AIK da Microsoft.

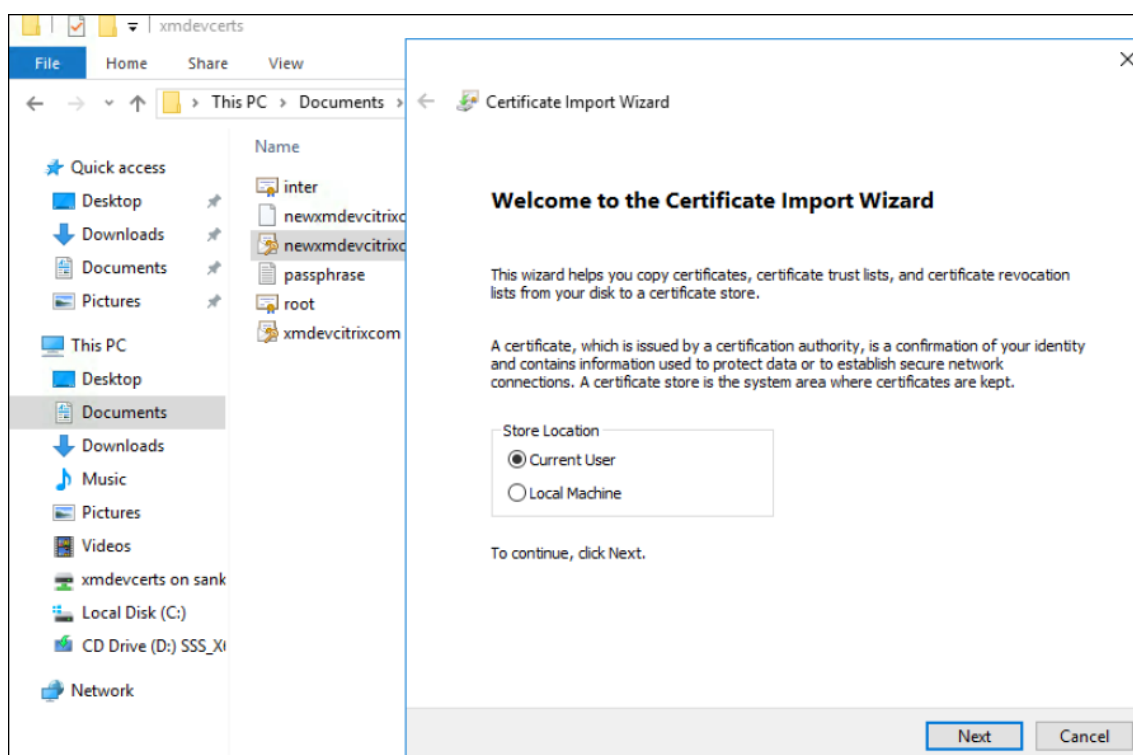
Adicione a função de servidor DHA ao Windows Server

1. No Windows Server, se o Gerenciador de Servidores ainda não estiver aberto, clique em **Iniciar** e, em seguida, clique em **Gerenciador de Servidores**.
2. Clique em **Adicionar funções e recursos**.

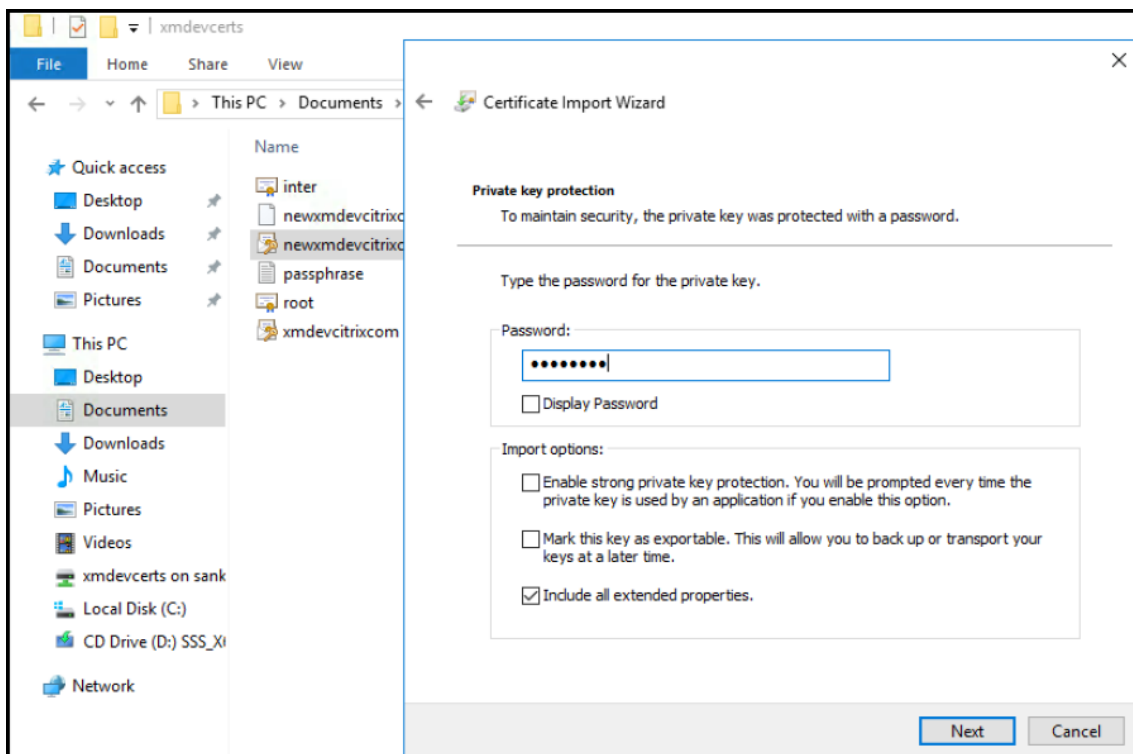
3. Na página **Antes de começar**, clique em **Avançar**.
4. Na página **Selecionar tipo de instalação**, clique em **Instalação baseada em função ou recurso** e clique em **Avançar**.
5. Na página **Selecionar servidor de destino**, clique em **Selecionar um servidor no pool de servidor**, selecione o servidor e clique em **Avançar**.
6. Na página **Selecionar funções de servidor**, marque a caixa de seleção **Atestado de Integridade de Dispositivo**.
7. Opcional: clique em **Adicionar recursos** para instalar outros serviços e recursos de função necessários.
8. Clique em **Avançar**.
9. Na página **Selecionar recursos**, clique em **Avançar**.
10. Na página **Função Servidor Web (IIS)**, clique em **Avançar**.
11. Na página **Selecionar serviços de função**, clique em **Avançar**.
12. Na página **Serviço de Atestado de Integridade do Dispositivo**, clique em **Avançar**.
13. Na página **Confirmar Seleções de Instalação**, clique em **Instalar**.
14. Quando a instalação estiver concluída, clique em **Fechar**.

Adicione o certificado SSL ao repositório de certificados do servidor

1. Vá até o arquivo de certificado SSL e selecione-o.
2. Selecione **Usuário atual** como o local do repositório e clique em **Avançar**.



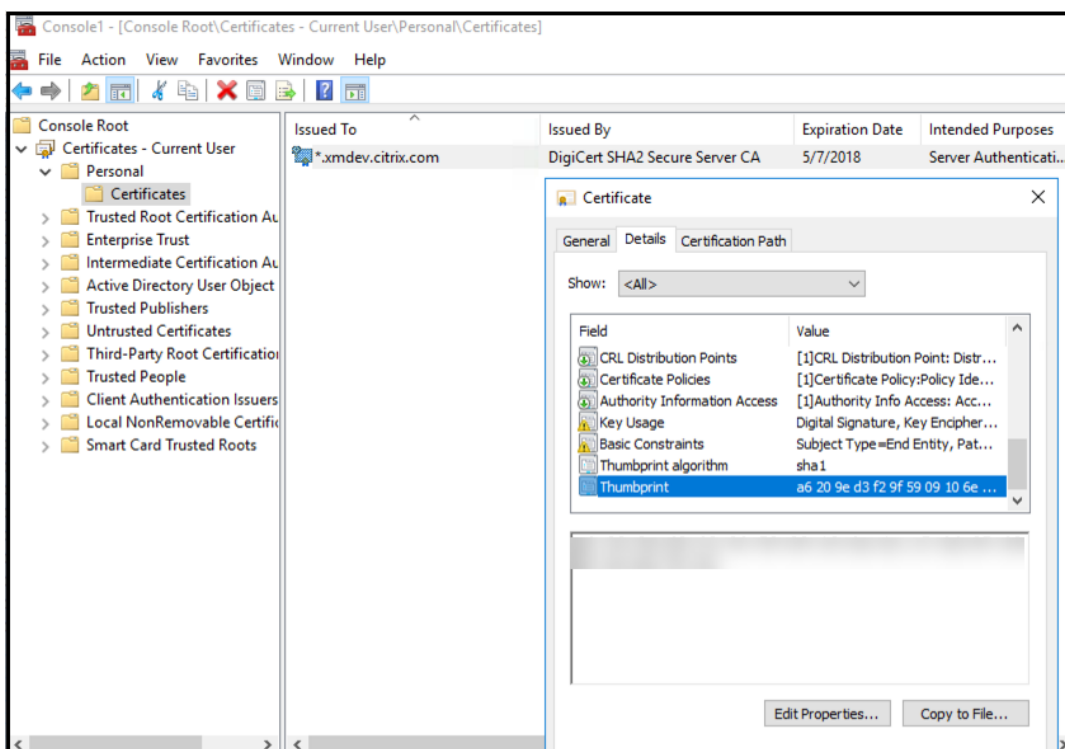
3. Digite a senha para a chave privada.
4. Assegure-se de que a opção de importação **Incluir todas as propriedades estendidas** esteja selecionada. Clique em **Avançar**.



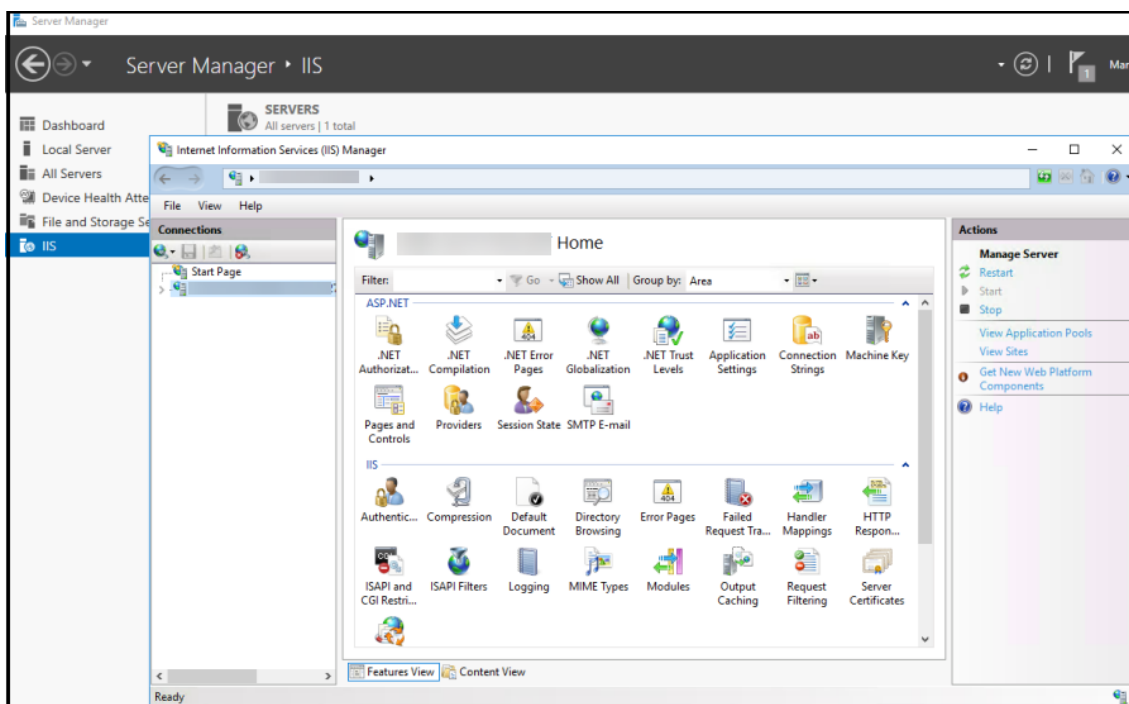
5. Quando esta janela aparecer, clique em **Sim**.



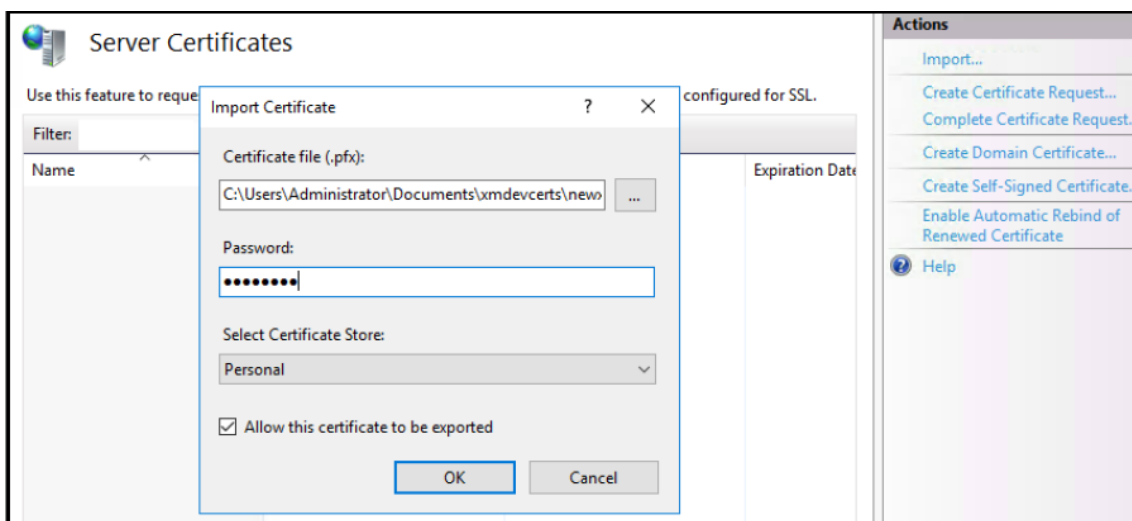
6. Confirme se o certificado está instalado:
 - a) Abra uma janela do prompt de comando.
 - b) Digite **mmc** e pressione a tecla Enter. Para exibir certificados no repositório do computador local, você deve estar na função Administrador.
 - c) No menu Arquivo, clique em **Adicionar/Remover Snap-In**.
 - d) Clique em **Adicionar**.
 - e) Na caixa de diálogo Adicionar snap-in autônomo, selecione **Certificados**.
 - f) Clique em **Adicionar**.
 - g) Na caixa de diálogo Snap-in de Certificados, selecione **Minha conta de usuário**. (Se você estiver conectado como titular da conta de serviço, selecione **Conta de serviço**.)
 - h) Na caixa de diálogo Selecionar Computador, clique em **Concluir**.



7. Vá para **Gerenciador do Servidor > IIS** e selecione **Certificados do Servidor** na lista de ícones.

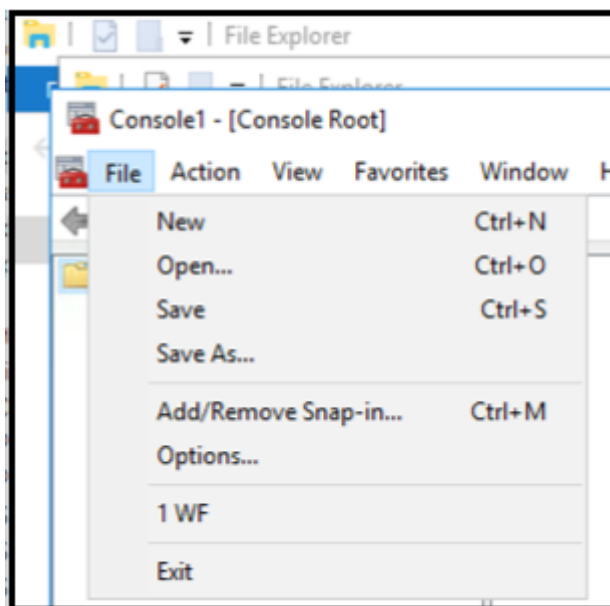


8. No menu Ação, selecione **Importar...** para importar o certificado SSL.

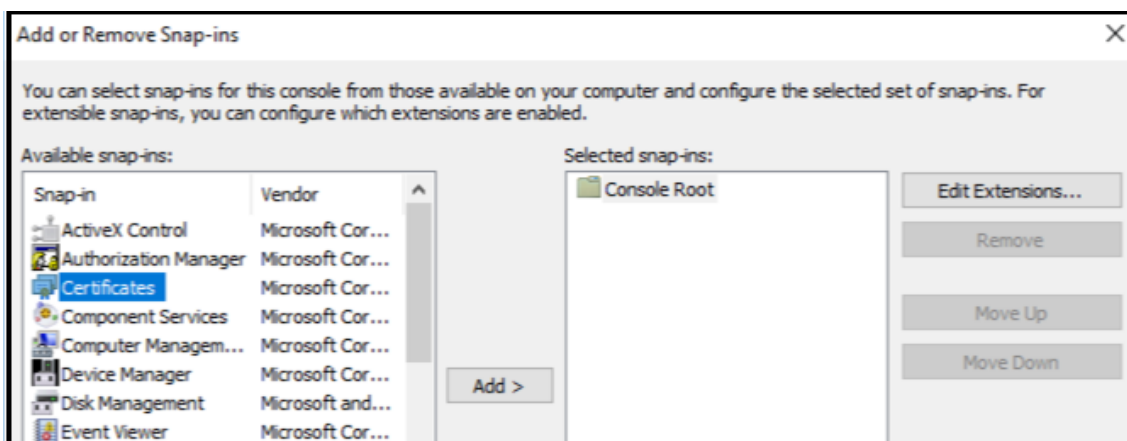


Recupere e salve a impressão digital do certificado

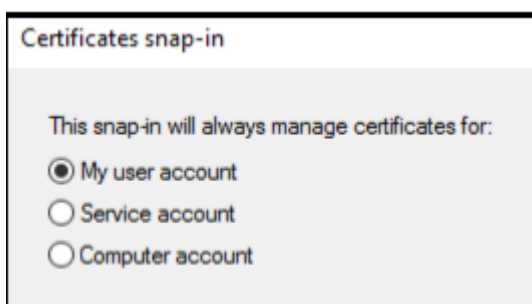
1. Na barra de pesquisa do Explorador de Arquivos, digite **mmc**.
2. Na janela Raiz do Console, clique em **Arquivo > Adicionar/Remover Snap-in...**



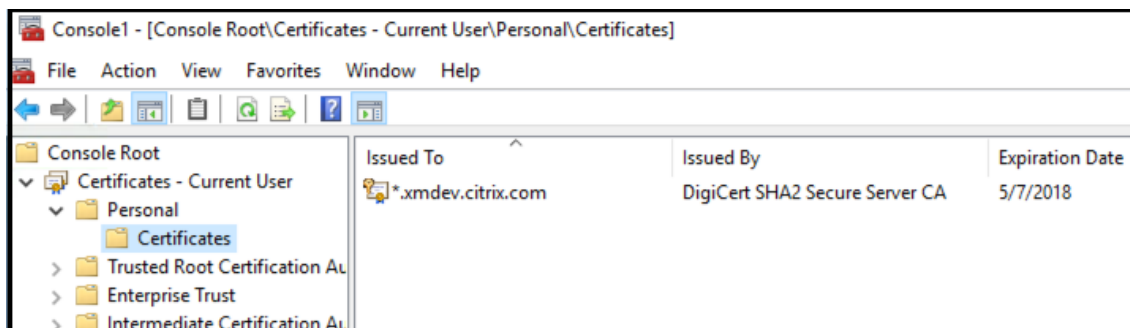
3. Selecione o certificado do snap-in disponível e adicione-o aos snap-ins selecionados.



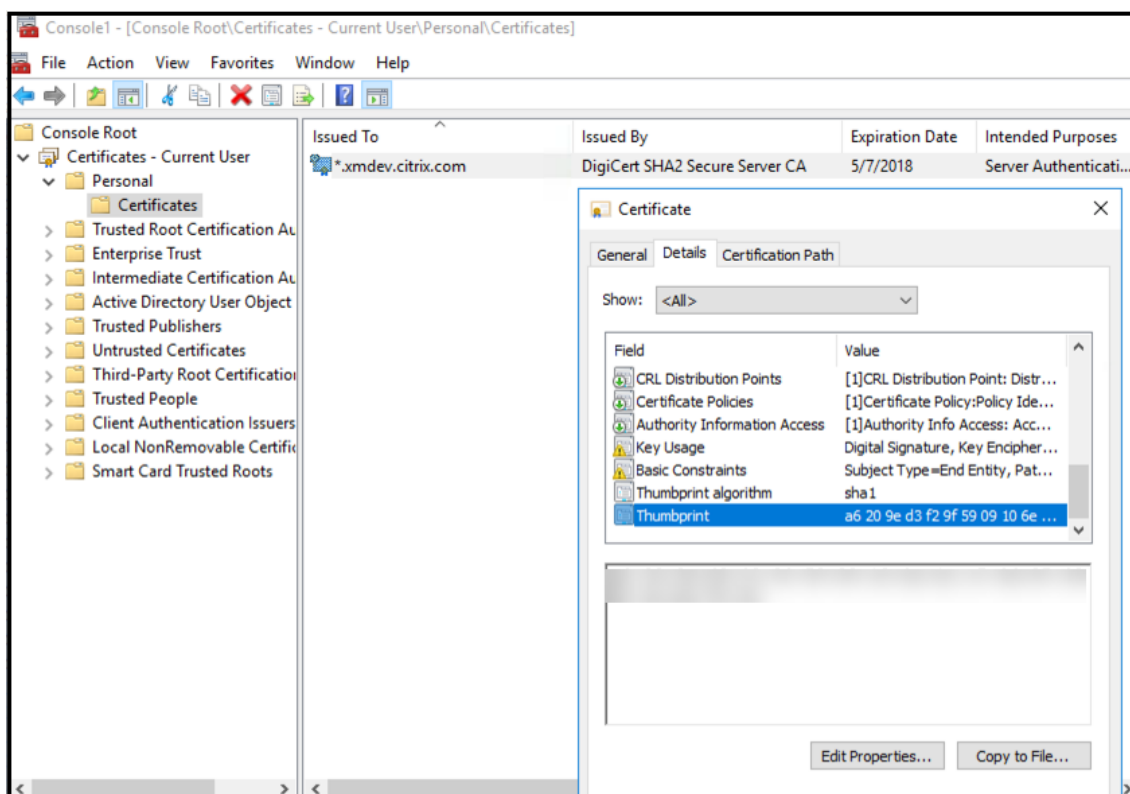
4. Selecione **Minha conta de usuário**.



5. Selecione o certificado e clique em **OK**.



6. Clique duas vezes no certificado e selecione a guia **Detalhes**. Role para baixo para ver a impressão digital do certificado.



7. Copie a impressão digital para um arquivo. Remova os espaços ao usar a impressão digital nos comandos do PowerShell.

Instalar os certificados de assinatura e criptografia

Execute esses comandos do PowerShell no Windows Server para instalar os certificados de assinatura e criptografia.

Substitua o espaço reservado ReplaceWithThumbprint e coloque-o entre aspas duplas, conforme mostrado.

```

1 $key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {
2   $_.Thumbprint -like "ReplaceWithThumbprint" }
3
4
5 $keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName
6
7 $keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys" +
8   $keyname iccls $keypath /grant IIS_IUSRS`:R
9 <!--NeedCopy-->

```

Extraia o certificado raiz do TPM e instale o pacote de certificado confiável

Execute estes comandos no Windows Server:

```
1 mkdir .\TrustedTpm
2
3 expand -F:* .\TrustedTpm.cab .\TrustedTpm
4
5 cd .\TrustedTpm
6
7 .\setup.cmd
8 <!--NeedCopy-->
```

Configurar o serviço DHA

Execute este comando no Windows Server para configurar o serviço DHA.

Substitua o espaço reservado ReplaceWithThumbprint.

```
1 Install-DeviceHealthAttestation -EncryptionCertificateThumbprint
   ReplaceWithThumbprint
2
3 -SigningCertificateThumbprint ReplaceWithThumbprint
4
5 -SslCertificateStoreName My -SslCertificateThumbprint
   ReplaceWithThumbprint
6
7 -SupportedAuthenticationSchema "AikCertificate"
8 <!--NeedCopy-->
```

Execute esses comandos no Windows Server para configurar a política de cadeia de certificados para o serviço DHA:

```
1 $policy = Get-DHASCertificateChainPolicy
2
3 $policy.RevocationMode = "NoCheck"
4
5 Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy
6 <!--NeedCopy-->
```

Responda a estes prompts da seguinte maneira:

```
1 Confirm
2
3 Are you sure you want to perform this action?
```

```
4
5     Performing the operation "Install-DeviceHealthAttestation" on
      target "WIN-N27D1FKCEBT".
6
7     [Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?]
      Help (default is "Y"): A
8
9     Adding SSL binding to website 'Default Web Site'.
10
11    Add SSL binding?
12
13    [Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
14
15    Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.
16
17    Add application pool?
18
19    [Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
20
21    Adding web application 'DeviceHealthAttestation' to website '
      Default Web Site'.
22
23    Add web application?
24
25    [Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
26
27    Adding firewall rule 'Device Health Attestation Service' to allow
      inbound connections on port(s) '443'.
28
29    Add firewall rule?
30
31    [Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
32
33    Setting initial configuration for Device Health Attestation Service
      .
34
35    Set initial configuration?
36
37    [Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
38
39    Registering User Access Logging.
40
41    Register User Access Logging?
42
43    [Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y
```

```
44 <!--NeedCopy-->
```

Verificar a configuração

Para verificar se o DHASActiveSigningCertificate está ativo, execute este comando no servidor:

```
Get-DHASActiveSigningCertificate
```

Se o certificado estiver ativo, o tipo de certificado (Assinatura) e a impressão digital serão exibidos.

Para verificar se o DHASActiveSigningCertificate está ativo, execute estes comandos no servidor

Substitua o espaço reservado ReplaceWithThumbprint e coloque-o entre aspas duplas, conforme mostrado.

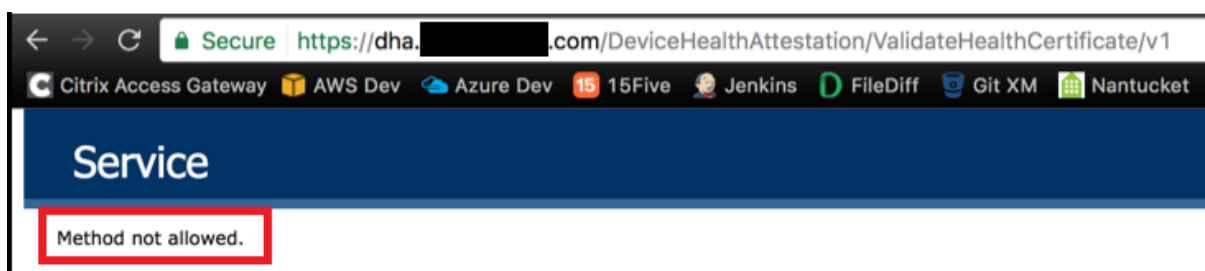
```
1 Set-DHASActiveEncryptionCertificate -Thumbprint "ReplaceWithThumbprint"
   -Force
2
3 Get-DHASActiveEncryptionCertificate
4 <!--NeedCopy-->
```

Se o certificado estiver ativo, a impressão digital será exibida.

Para realizar uma verificação final, acesse esta URL:

```
https://<dha.myserver.com>/DeviceHealthAttestation/ValidateHealthCertificate/v1
```

Se o serviço DHA estiver sendo executado, será exibido “Método não permitido”.



Configurar a autenticação baseada em certificado com o EWS para notificações por push do Secure Mail

April 23, 2020

Contribuição de Vijay Kumar Kunchakuri

Para garantir que as notificações por push do Secure Mail funcionem, você deve configurar o Exchange Server para autenticação baseada em certificado. Esse requisito é especialmente necessário quando o Secure Hub é registrado no XenMobile com autenticação baseada em certificado.

Você precisa configurar o diretório virtual do Active Sync e do Exchange Web Services (EWS) no Exchange Mail Server com autenticação baseada em certificado.

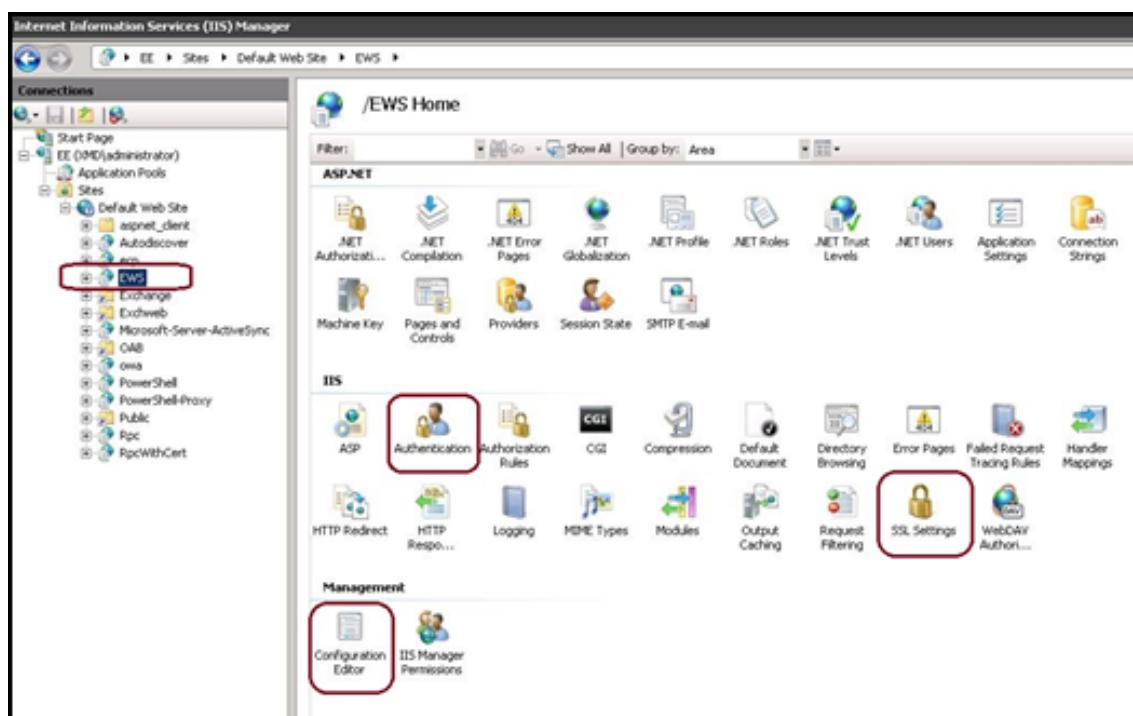
A menos que você conclua essas configurações, a assinatura das notificações por push do Secure Mail falhará e nenhuma atualização de selo ocorrerá no Secure Mail.

Este artigo descreve as etapas para configurar a autenticação baseada em certificado. As configurações são especificamente contra o diretório virtual do EWS no Exchange Server.

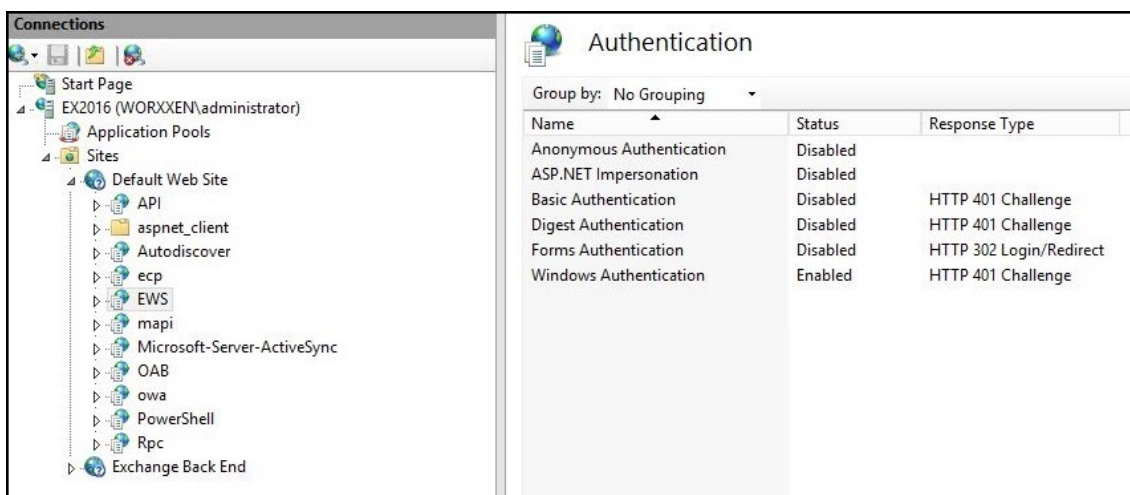
Para começar a usar a configuração, faça o seguinte:

1. Faça login no servidor ou servidores em que o diretório virtual do EWS está instalado.
2. Abra o console do gerenciador do IIS.
3. No **Site padrão**, clique no diretório virtual do EWS.

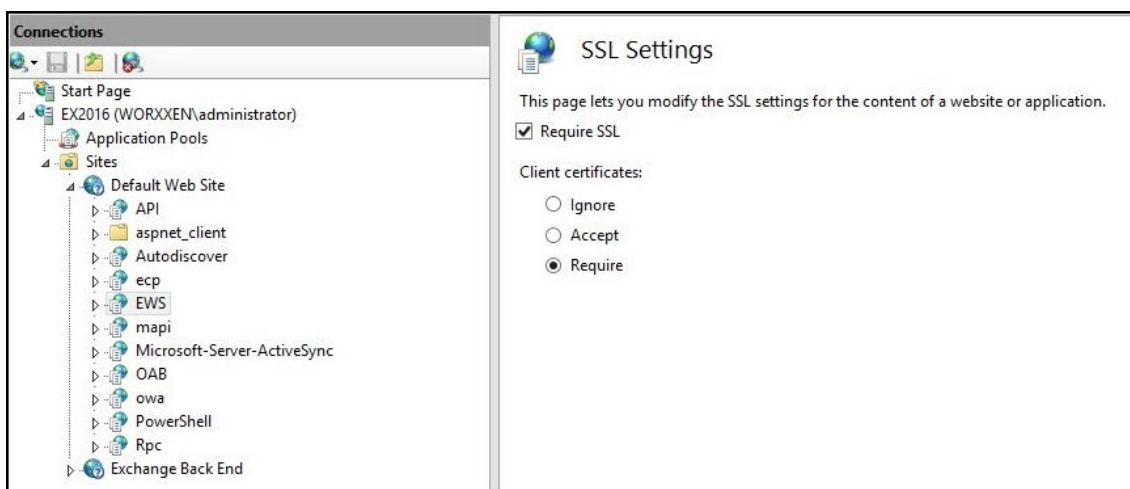
Os snap-ins de Autenticação, SSL, Editor de configuração estão no lado direito do console do gerenciador do IIS



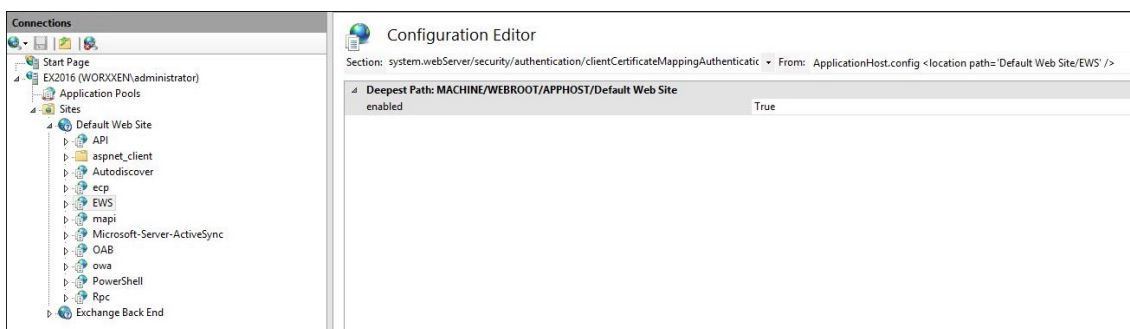
4. Certifique-se de que as configurações de **Autenticação** para o EWS estejam configuradas conforme mostrado na figura a seguir.



5. Defina as **Configurações de SSL** para o diretório virtual do EWS.
 - a) Marque a caixa de seleção **Exigir SSL**.
 - b) Em **Certificados do Cliente**, clique em **Exigir**. Você pode definir essa opção como **Aceitar** se outros clientes de e-mail do EWS se conectarem com nome de usuário e senha como credenciais para autenticar e se conectar ao Exchange Server.



6. Clique em **Editor de configuração** e, na lista suspensa **Seção**, navegue até a seguinte seção:
 - **system.webServer/security/authentication/clientCertificateMappingAuthentication**
7. Defina o valor **enabled** como **True**.



8. Clique em **Editor de configuração** e, na lista suspensa **Seção**, navegue até a seguinte seção:

- **system.webServer/serverRuntime**

9. Defina o valor de **uploadReadAheadSize** para **10485760** (10 MB) ou **20971520** (20 MB) ou para um valor conforme exigido pela sua organização.

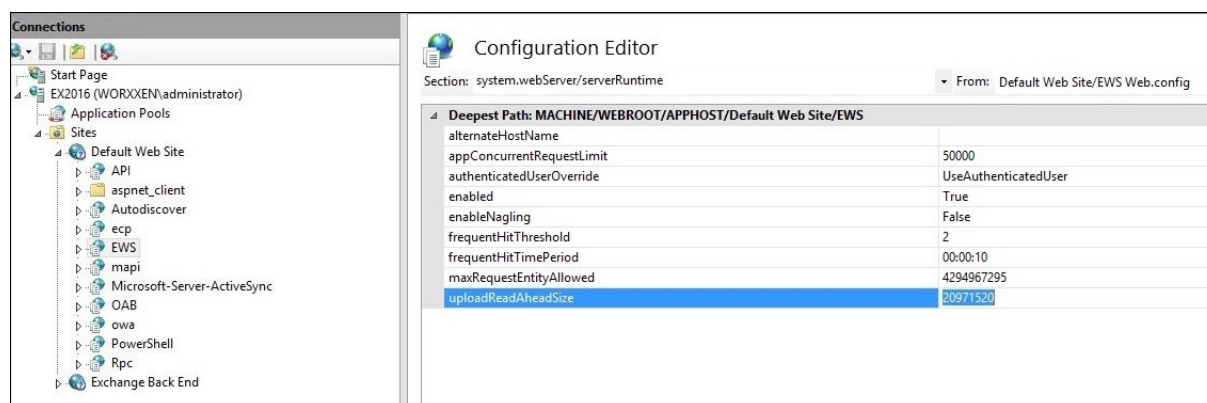
Importante:

Se você não definir esse valor corretamente, a autenticação baseada em certificado durante o registro nas notificações push do EWS poderá falhar com um código de erro 413.

Não defina esse valor como **0**.

Para mais informações, consulte os seguintes recursos de terceiros:

- [Tempo de execução do servidor Microsoft IIS](#)
- [Blog de Gerenciamento de Cliente Butsch](#)



Para obter mais informações sobre como solucionar problemas do Secure Mail com notificações por push do iOS, consulte este artigo do [Citrix Support Knowledge Center](#).

Informações correlatas

[Notificações por Push para o Secure Mail para iOS](#)

Integrar o Gerenciamento de Dispositivos Móveis (MDM) XenMobile com o Cisco Identity Services Engine (ISE)

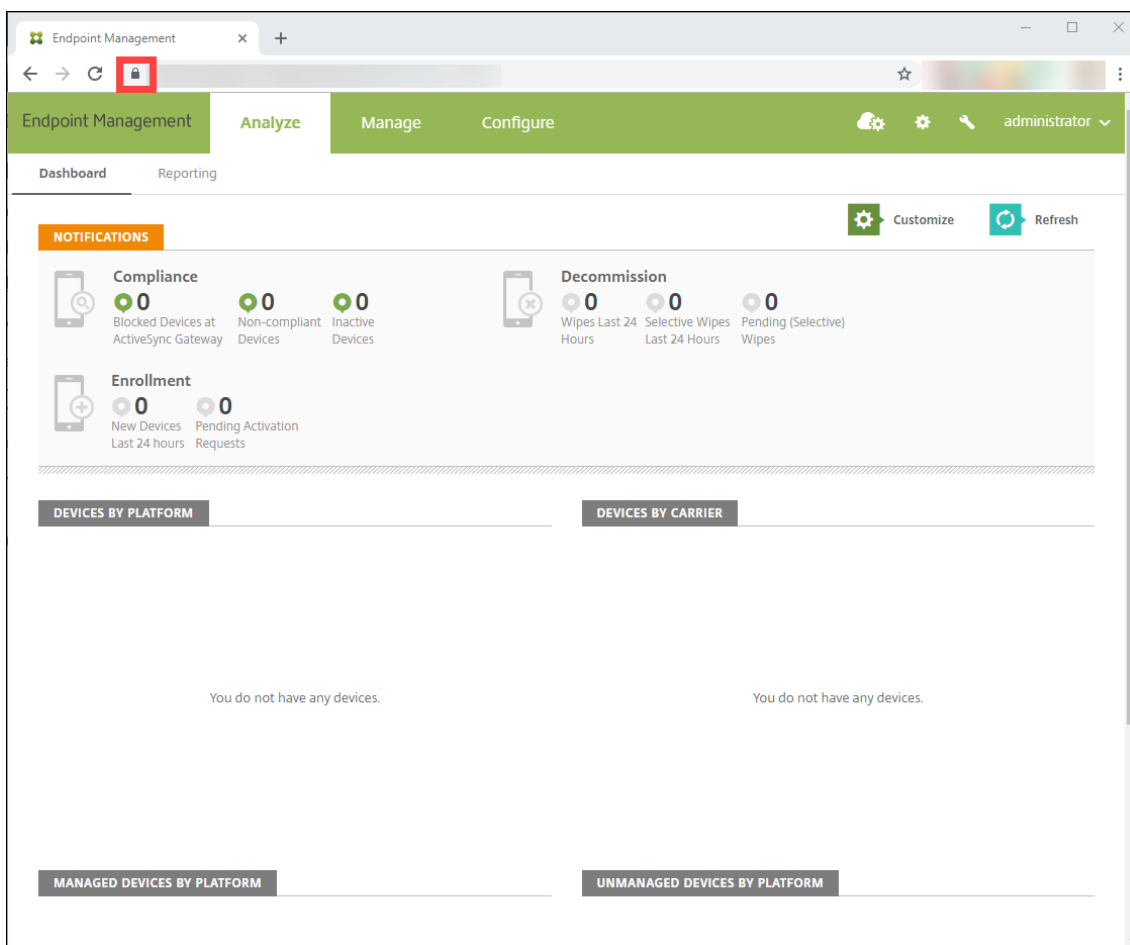
August 10, 2020

Contribuição de John Bartel III

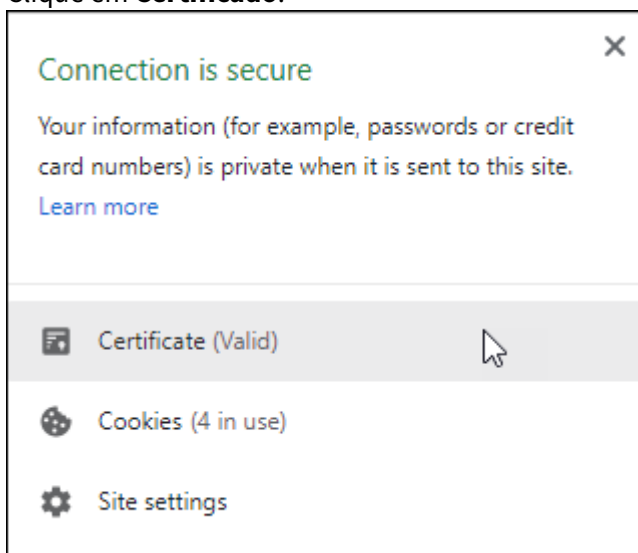
O Cisco ISE é usado para implantar, proteger, monitorar, integrar e gerenciar dispositivos móveis no local de trabalho. O software baixado para o dispositivo móvel controla a distribuição de aplicativos e patches e a configuração e dados de controle no endpoint. O XenMobile pode integrar-se ao Cisco ISE para gerenciar dispositivos não compatíveis e não gerenciados no console Cisco ISE. O XenMobile também permite que você permita, negue ou coloque em quarentena o acesso a serviços corporativos de forma seletiva.

Para configurar a integração com o XenMobile, crie uma conta de serviço local no XenMobile Server com a função RBAC de administrador atribuída a ela. Essa função permite que o Cisco ISE acesse a API do XenMobile. O ISE precisa confiar no certificado do XenMobile. Para baixar esse certificado, abra um navegador da Web e navegue até a URL do servidor e faça login.

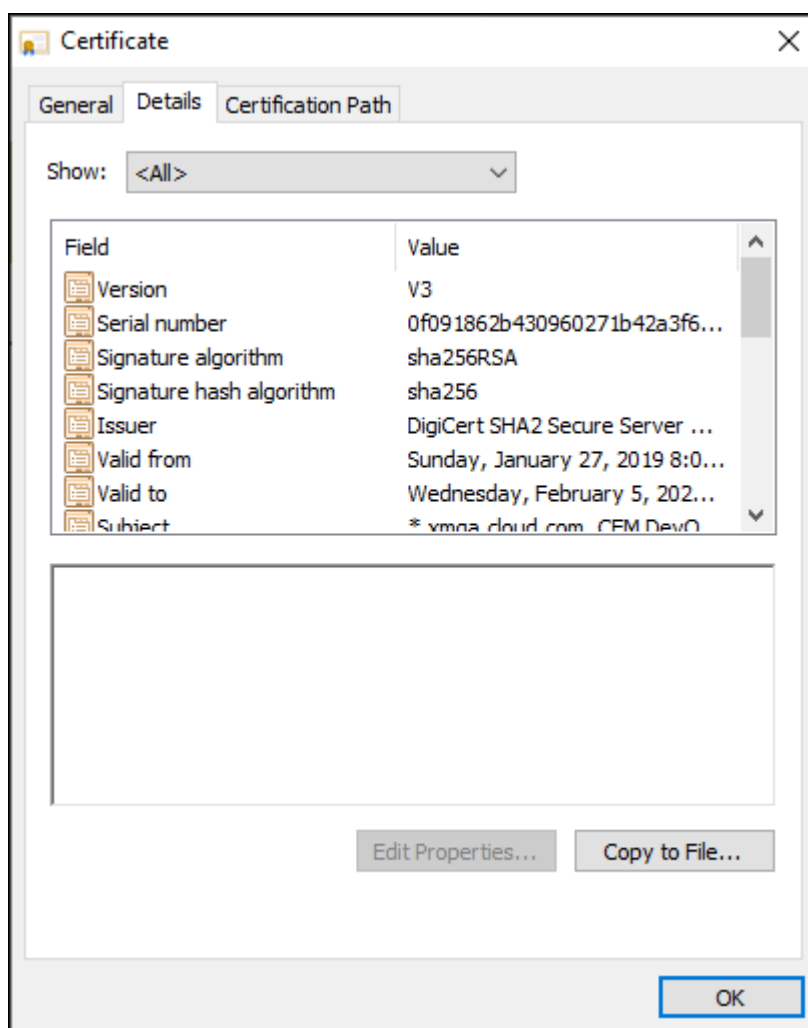
1. Depois de fazer login, clique no cadeado ao lado da URL na barra de endereços.



2. Clique em **Certificado**.



3. Selecione a guia **Detalhes** e clique em **Copiar para Arquivo**.



4. Siga o assistente para salvar o certificado localmente.
5. Faça login no console Cisco ISE e importe o certificado do XenMobile que você baixou anteriormente. Importe o certificado para a área de armazenamento de Certificados Confiáveis do Cisco ISE. Essa importação é necessária para que o Cisco ISE confie na comunicação com o XenMobile Server.
 - a) Navegue até **Administration > System > Certificates > Certificate Management > Trusted Certificates**. Clique em **Importar**.
 - b) Dê um nome ao certificado e marque as caixas **Trust for authentication within ISE** e **Trust for authentication of Cisco Services**.
6. Adicione o XenMobile como um MDM externo dentro do Cisco ISE.
 - a) Navegue até **Administration > Network Resource > External MDM**. Clique em **Add** e preencha o seguinte:
 - **Server Host:** o FQDN do seu XenMobile
 - **Porta:** 443
 - **Instance name:** o nome da instância do seu XenMobile Server. O nome da instância

é “zdm” por padrão na maioria das implantações.

- **User Name:** digite o nome do usuário que você criou para esta tarefa. O usuário deve ter uma conta de administrador local no grupo original de administradores RBAC.
- **Password:** a senha do usuário que você acabou de adicionar.
- Verifique se exibe **Enable**.

7. Se o teste for bem-sucedido, clique em **Submit**.

Para obter mais informações sobre o Cisco ISE, consulte a [Documentação da Cisco](#).

**Locations**

Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2021 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).