XenMobile Server

Feb 22, 2018

Versão atual: XenMobile Server 10.8

O XenMobile Server é uma solução de gerenciamento de mobilidade corporativa local que oferece recursos de gerenciamento de dispositivos móveis (MDM) e gerenciamento de aplicativos móveis (MAM).

A versão de serviço de nuvem do XenMobile Server é chamada de XenMobile Service. A documentação do servidor XenMobile se aplica ao XenMobile Service, a menos que indicado do contrário em artigos do XenMobile Server.

Os aplicativos XenMobile são aplicativos de produtividade e comunicação que são oferecidos como parte da solução XenMobile.

Para obter informações específicas sobre a oferta na nuvem do XenMobile, consulte XenMobile Service. Para obter informações sobre os aplicativos XenMobile, consulte Aplicativos XenMobile.

Para o XenMobile Server e os aplicativos, a Citrix oferece suporte à versão atual e às duas versões anteriores do XenMobile. Para obter uma lista dos novos recursos e de problemas conhecidos e corrigidos nas duas versões anteriores, consulte:

- Novidades no XenMobile Server 10.7
- Novidades no XenMobile Server 10.6

Para obter PDFs da documentação de todas as versões anteriores à mais recente, consulte a Archive List of Legacy Documents.

XenMobile 9. Esta versão atingiu o status de Fim da vida útil (EOL) em 30 de junho de 2017.Quando uma versão do produto atinge a EOL, você pode usar o produto de acordo com os termos do seu contrato de licença de produto, mas as opções de suporte disponíveis são limitadas. Informações de histórico aparecem no Knowledge Center ou em outros recursos online. A documentação não é mais atualizada e é fornecida no estado em que se encontra.Para obter mais informações sobre marcos de ciclo de vida útil de produtos, consulte a Product Matrix.

Por cinco anos além da data de EOL, você pode baixar um PDF da documentação do XenMobile 9 na Lista de arquivamento de documentos legados.

Para obter informações sobre a migração do XenMobile 9 para o XenMobile Service no Citrix Cloud, consulte a página Citrix.com.

Atualizações

> ## Important
>
> **Antes de atualizar para o XenMobile 10.8 (no local)**
>
> 1. Atualize o seu Citrix License Server para 11.14.x ou posterior antes de atualizar para a versão mais recente do XenMobile Server 10.8.
>   A versão mais recente do XenMobile exige o Citrix License Server 11.14.x (versão mínima). A data da Subscription Advantage

© 1999-2017 Citrix Systems, Inc. All rights reserved.

(SA) em sua licença Citrix deve ser posterior a 6 de junho de 2016. Você pode ver sua data de SA 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 da as em sua licença, baixe o último arquivo de licença do Portal Citrix e carregue o arquivo para o Servidor de Licenciamento. Para obter mais informações, consulte http://support.citrix.com/article/CTX209580.

2. Para um ambiente em cluster: Para instalar aplicativos da XenMobile Store em dispositivos iOS 11, você deve habilitar a porta 80 no 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. 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.

Após atualizar para o XenMobile 10.8 (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 quebrar sua implantação, altere a propriedade do servidor **disable.hostname.verification** para **verdadeiro**. O valor padrão desta propriedade é **falso**

Você pode atualizar diretamente para o XenMobile 10.8 do XenMobile 10.7.x ou 10.6.x. Use a página **Gerenciamento de versão** no console XenMobile.

Para executar a atualização, use o xms_10.8.0.23.bin ou o binário 10.8 mais recente disponível na página de download da Citrix. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console e clique em **Gerenciamento de versão**. Clique em **Atualização** e carregue o arquivo BIN. Os arquivos de atualização para hipervisores com suporte são:

xms_10.8.0.23.xenserver.xva
xms_10.8.0.23.HyperV.zip
xms_10.8.0.23.vmware.ova

Para obter mais informações sobre a atualização do XenMobile 10.7.x ou 10.6.x, consulte Atualizar.

Nota

Para atualizar de versões mais antigas do XenMobile, consulte o artigo sobre atualização no PDF do XenMobile Server 10.7, a partir da página 298.

Para concluir uma nova instalação da versão mais recente do XenMobile, consulte Instalar e configurar.

Informações correlatas

- XenMobile Support Knowledge Center

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix Blogs on XenMobile

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Novidades no XenMobile Server 10.8

Feb 22, 2018

Para obter informações sobre como atualizar, consulte Atualização.

> ## Important
>
> **Antes de atualizar para o XenMobile 10.8:**
>
> Atualize o seu Citrix License Server para 11.14.x ou posterior antes de atualizar para a versão mais recente do XenMobile Server 10.8.
>
> Para um ambiente em cluster: Para instalar aplicativos da XenMobile Store em dispositivos iOS 11, você deve habilitar a porta 80 no XenMobile Server.
>
> **Após uma atualização para o XenMobile 10.8:**
>
> Se a funcionalidade que envolve as conexões de saída deixar de funcionar e você não tiver alterado sua configuração de conexão, 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 ao assunto do certificado fornecido pelo par.
>
> Se você receber o erro de validação de certificado, desative a verificação de nome de 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**.

O XenMobile Server 10.8 inclui os novos recursos a seguir:

- Instalar mapas offline nos dispositivos de telefone supervisionados Windows 10
- Novas restrições para dispositivos supervisionados que executam o iOS
- Definir como as notificações do aplicativo são exibidas nos dispositivos iOS
- Suporte para o novo cliente Cisco AnyConnect VPN para iOS
- Criptografia do dispositivo FileVault em dispositivos macOS registrados.
- Suporte para Samsung Enterprise Firmware-Over-The-Air
- Segurança aprimorada de perfis de trabalho do Android for Work
- Cancelar o registro de um Android for Work Enterprise
- Especificar o comportamento quando aplicativos do Android for Work solicitam permissões perigosas
- SNMP Monitoring
- Suporte para o driver Microsoft JDBC para SQL Server
- Alterações na propriedade do servidor para melhorar o ajuste do servidor
- Pesquisa otimizada de propriedades de dispositivos
- Outras melhorias

Para obter correções de bugs, consulte Problemas resolvidos.

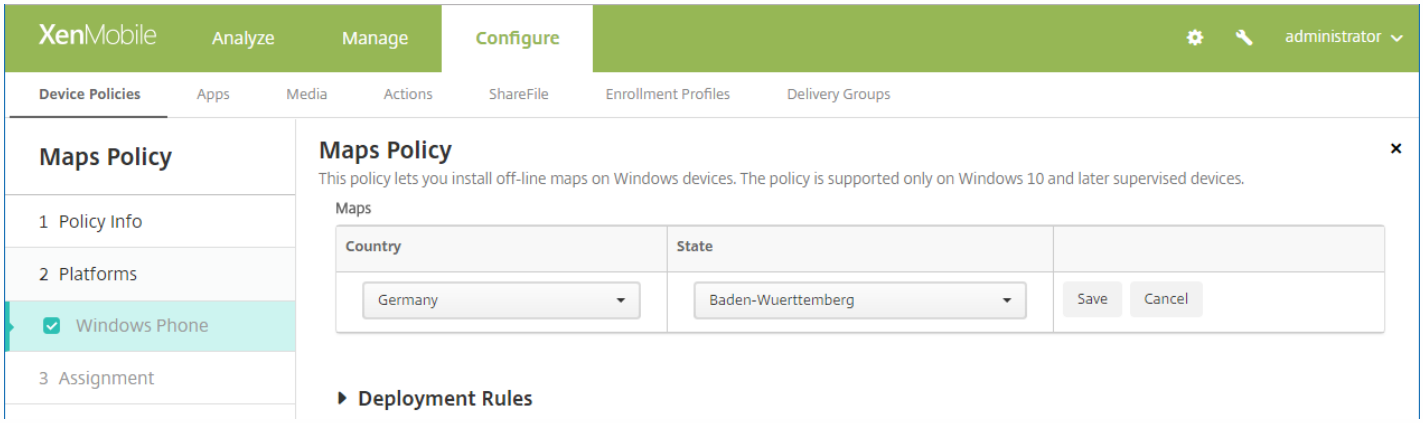
> ## Important
>
> O TouchDown da Symantec atingiu o fim da vida útil em 3 de julho de 2017, com fim de suporte padrão, fim de suporte estendido

© 1999-2017 Citrix Systems, Inc. All rights reserved.

e fim de suporte da vida útil em 2 de julho de 2018. Para obter mais informações, consulte o artigo de suporte da Symantec Aviso de Fim da vida, Fim de suporte e Fim da disponibilidade do TouchDown.

Instalar mapas offline nos dispositivos de telefone supervisionados Windows 10

Os dispositivos de telefone Windows 10 suportam mapas offline. Use a política de dispositivo Mapas para especificar quais mapas devem ser baixados para os dispositivos. O provedor de serviços de configuração (CSP) Microsoft Maps atualmente oferece suporte para mapas da Alemanha, do Reino Unido e dos Estados Unidos.



Novas restrições para dispositivos supervisionados que executam o iOS

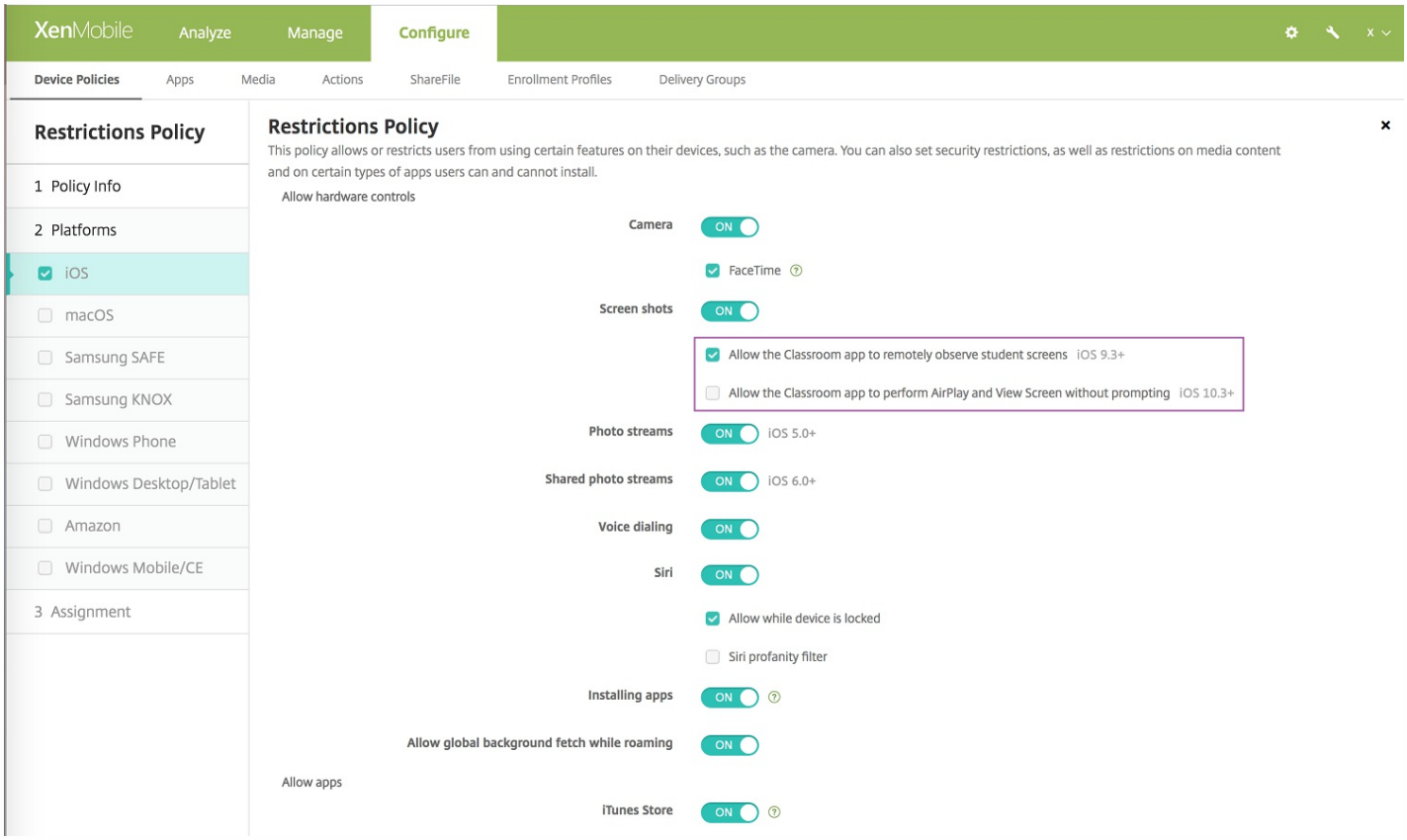
As seguintes restrições agora estão disponíveis para os dispositivos iOS executados no modo supervisionado. A versão mínima compatível para cada restrição é informada.

- **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 as telas dos alunos remotamente. 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 supervisionados executando o iOS 9.3 (versão mínima).
- **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 supervisionados executando o iOS 10.3 (versão mínima).
- **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).

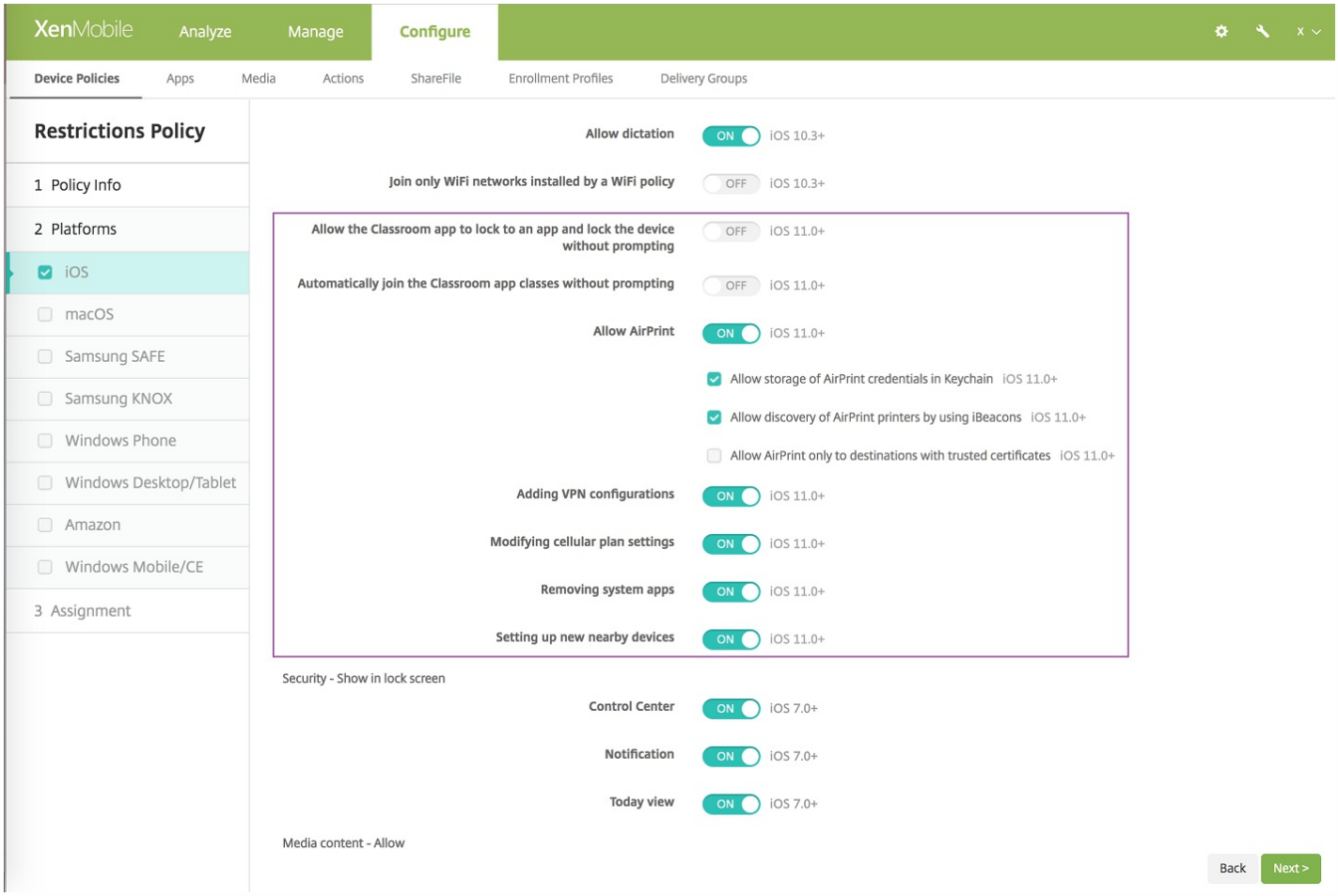
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Permitir a descoberta de impressoras AirPrint usando iBeacons**: se essa restrição não estiver selecionada, a descoberta do iBeacon de impressoras AirPrint será desativada. Desabilitar a descoberta 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 do 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).

Para configurar as restrições, vá para **Configurar > Políticas de dispositivo**. Para obter mais informações sobre como configurar restrições, consulte a política do dispositivo Restrições.



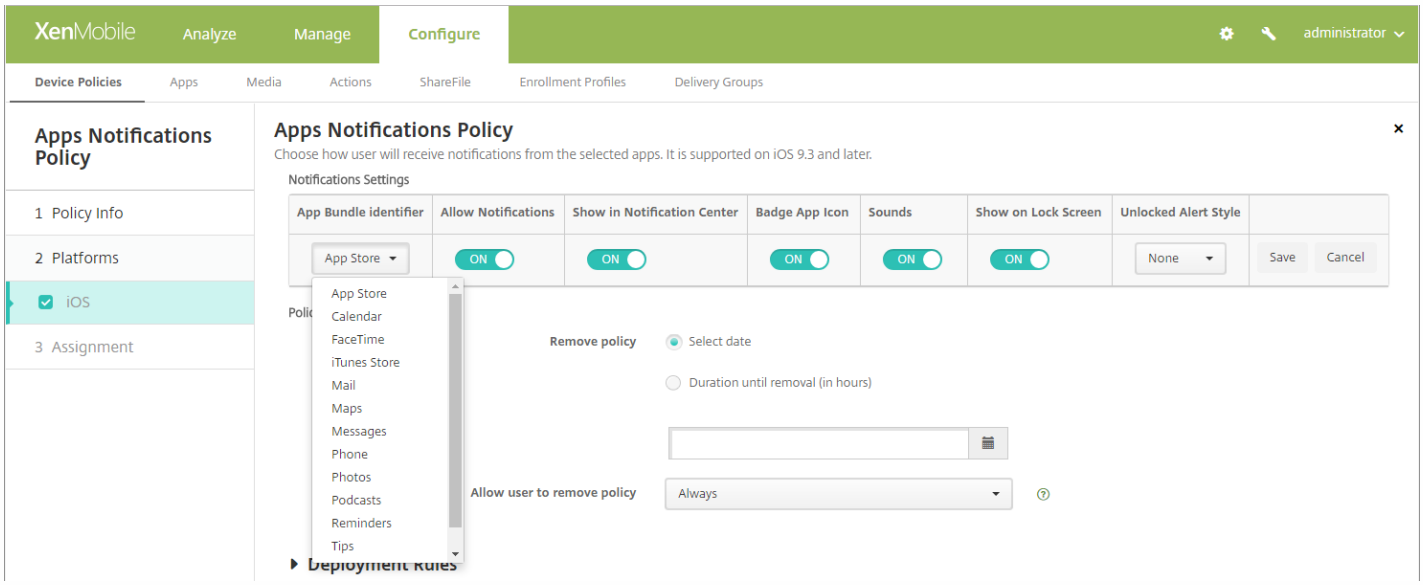
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Além disso, agora você pode pular a tela de seleção do teclado no Assistente de Configuração. Para fazer isso, edite a política de dispositivo Restrições para iOS e, na configuração do **Painel Preferências do Sistema**, selecione **Teclado**.

Definir como as notificações do aplicativo são exibidas nos dispositivos iOS

A política de Notificações de Aplicativos permite controlar como os usuários do iOS recebem notificações de aplicativos especificados. Essa política é compatível em dispositivos com o iOS 9.3 ou versões posteriores. Para adicionar a política, acesse **Configurar > Políticas de dispositivo**.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurações de notificação:

- **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.
- **Estilo de alerta desbloqueado**: na lista, selecione **Nenhum**, **Banner** ou **Alertas** para configurar a aparência dos alertas desbloqueados.

Suporte para o novo cliente Cisco AnyConnect VPN para iOS

A Cisco está desativando o cliente Cisco AnyConnect que foi baseado em uma estrutura VPN agora obsoleta. A Cisco renomeou esse cliente como Cisco Legacy AnyConnect. O ID do pacote está inalterado, com.cisco.anyconnect.gui.

A Cisco tem um novo cliente chamado Cisco AnyConnect. O novo cliente fornece uma conexão mais confiável para recursos internos e suporte para aplicativos de UDP e TCP que têm a VPN por aplicativo. O ID do pacote para o novo cliente é com.cisco.anyconnect. A Cisco suporta o novo cliente para iOS 10 (versão mínima).

- **Para continuar a usar o cliente AnyConnect legado**: se você ainda pode usar o cliente legado, não é necessário alterar a sua política de dispositivo VPN existente para iOS. A política continuará a funcionar até que a Cisco elimine o suporte ao cliente legado. A partir desta versão, a opção **Tipo de conexão Cisco AnyConnect** é renomeada para **Cisco Legacy AnyConnect** no console do XenMobile Server.
- **Para usar o novo cliente Cisco AnyConnect**: O novo cliente Cisco AnyConnect não detecta uma política de dispositivo XenMobile VPN criada com a opção **Tipo de conexão** como **Cisco AnyConnect**.

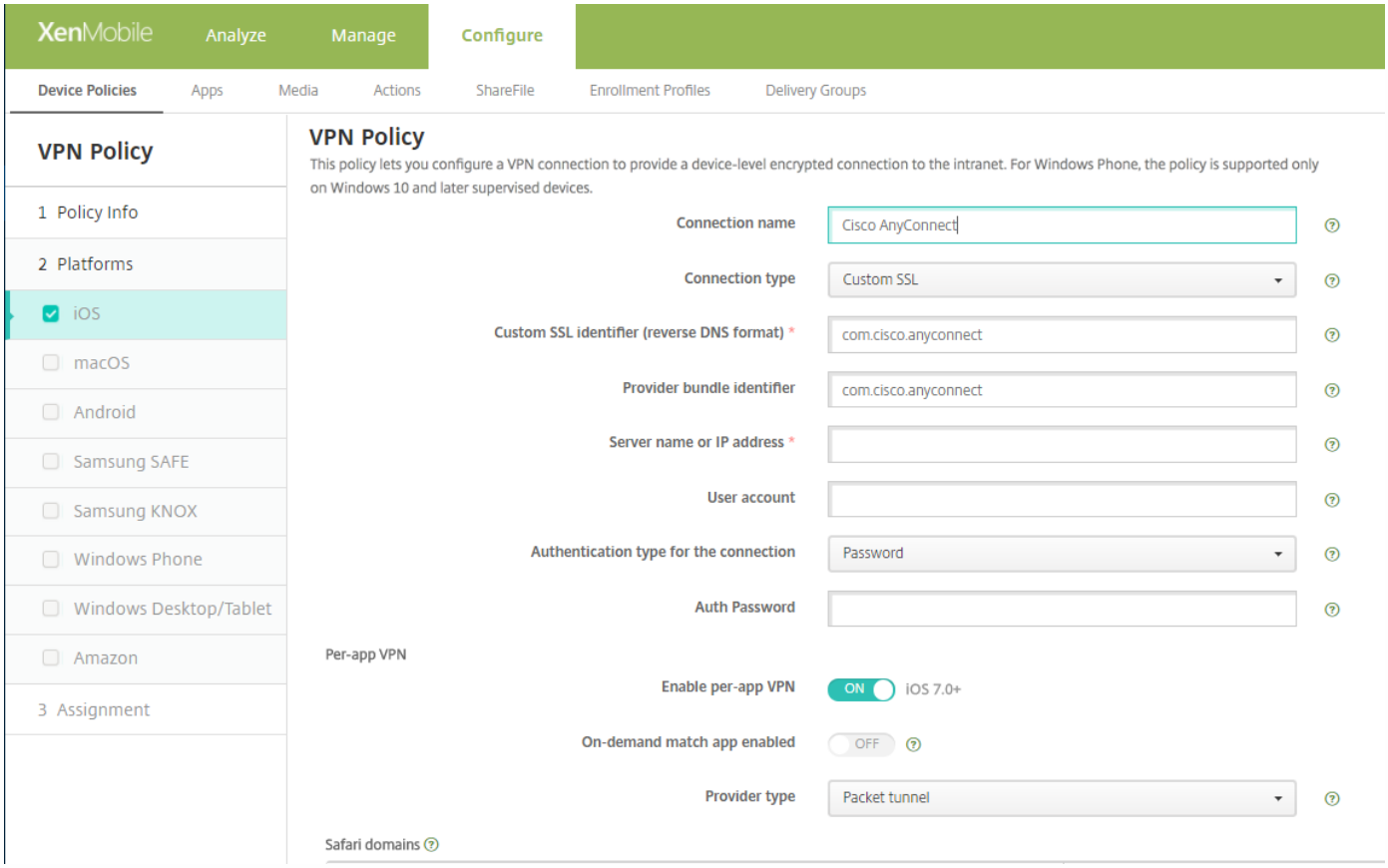
Para usar o novo cliente Cisco AnyConnect, configure o XenMobile Server da seguinte maneira.

1. Vá para **Configurar > Políticas de dispositivo** e adicione uma política de VPN para iOS.
2. Na página da plataforma **Política de VPN**, defina as configurações. As configurações listadas aqui são necessárias para o Cisco AnyConnect.

   - **Nome da conexão**: Cisco AnyConnect
   - **Tipo de conexão**: Custom SSL
   - **Identificador SSL personalizado (formato DNS inverso)**: com.cisco.anyconnect
   - **Identificador de pacote de provedor**: com.cisco.anyconnect
   - **Tipo de provedor**: Packet tunnel

   Outras configurações, como o **Tipo de autenticação para a conexão** e a **Habilitar VPN por aplicativo**, dependem do seu caso de uso. Para obter informações, consulte "Configurar o protocolo SSL personalizado" em Definir configurações do iOS.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. Configure regras de implantação e escolha grupos de entrega para a política de dispositivo VPN. Implemente essa política em dispositivos iOS.

4. Faça o upload do cliente Cisco AnyConnect em https://itunes.apple.com/us/app/cisco-anyconnect/id1135064690?mt=8, adicione o aplicativo ao XenMobile Server e implemente o aplicativo em dispositivos iOS.

5. Remova a política de dispositivo VPN antiga de dispositivos iOS.

Para obter mais informações, consulte o artigo de suporte do XenMobile em https://support.citrix.com/article/CTX227708.

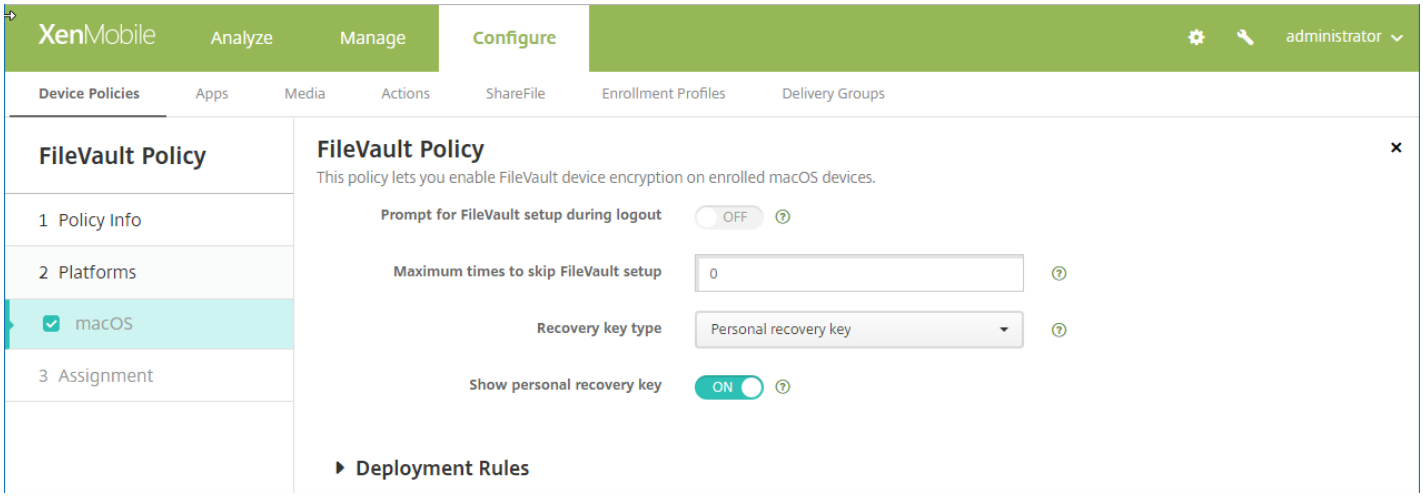
Criptografia do dispositivo FileVault em dispositivos macOS registrados.

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 artigo de suporte da Apple, https://support.apple.com/kb/PH25107.

Para adicionar a política, vá para **Configurar > Políticas de dispositivo**, adicione a política **FileVault** e defina estas configurações do macOS.

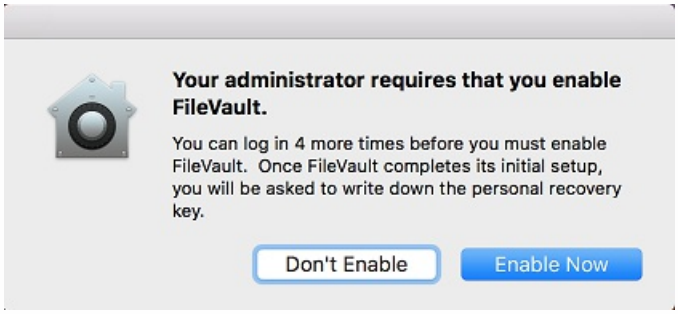
© 1999-2017 Citrix Systems, Inc. All rights reserved.



- **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 **o**, 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

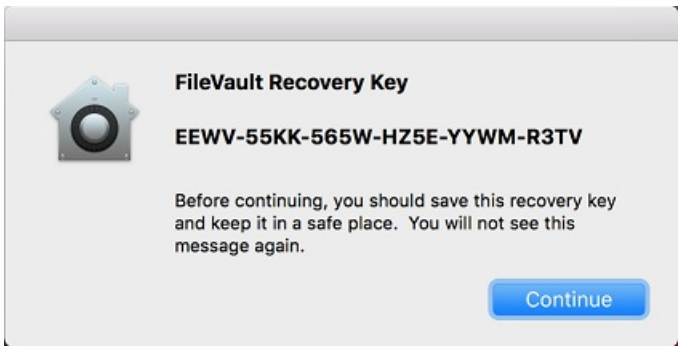
- **Número máximo de vezes para ignorar a configuração do FileVault**: o número máximo de vezes que o usuário pode ignorar a configuração do FileVault. Quando o usuário atinge o máximo, ele deve configurar o FileVault para efetuar login. Se o valor for **0**, o usuário deverá ativar o FileVault durante a primeira tentativa de login. O padrão é **0**.
- **Tipo de chave de recuperação**: um usuário que esquece sua senha pode digitar uma chave de recuperação para desbloquear o disco e redefinir sua senha. Opções de chave de recuperação:

  Chave de recuperação pessoal: uma chave de recuperação pessoal é exclusiva para um usuário. Durante a configuração do FileVault, um usuário escolhe se deseja criar uma chave de recuperação ou permitir que sua conta do iCloud desbloqueie os seus respectivos discos. Para mostrar a chave de recuperação ao usuário após a conclusão da configuração do FileVault, ative **Exibir a chave de recuperação pessoal**. Mostrar a chave permite que o usuário registre a chave para uso futuro. Para obter informações sobre o gerenciamento de chave de recuperação, consulte o artigo de suporte da Apple, https://support.apple.com/en-us/HT204837.

  Chave de recuperação institucional: você pode criar uma chave de recuperação institucional (ou principal) e o certificado FileVault, que você usa para desbloquear dispositivos. Para informações, consulte o artigo de suporte da Apple, https://support.apple.com/en-us/HT202385. Use o XenMobile para implantar o certificado FileVault nos dispositivos. Para obter informações, consulte Certificados e autenticação.

  Chave de recuperação pessoal e institucional: ao ativar os dois tipos de chave de recuperação, você deve desbloquear um dispositivo de usuário somente se o usuário perder sua chave de recuperação pessoal.

- **Exibir a chave de recuperação pessoal**: se estiver **Ativado**, exibe a chave de recuperação pessoal para o usuário depois de ativar o FileVault no dispositivo. O padrão é **Ativado**.



Suporte para Samsung Enterprise Firmware-Over-The-Air

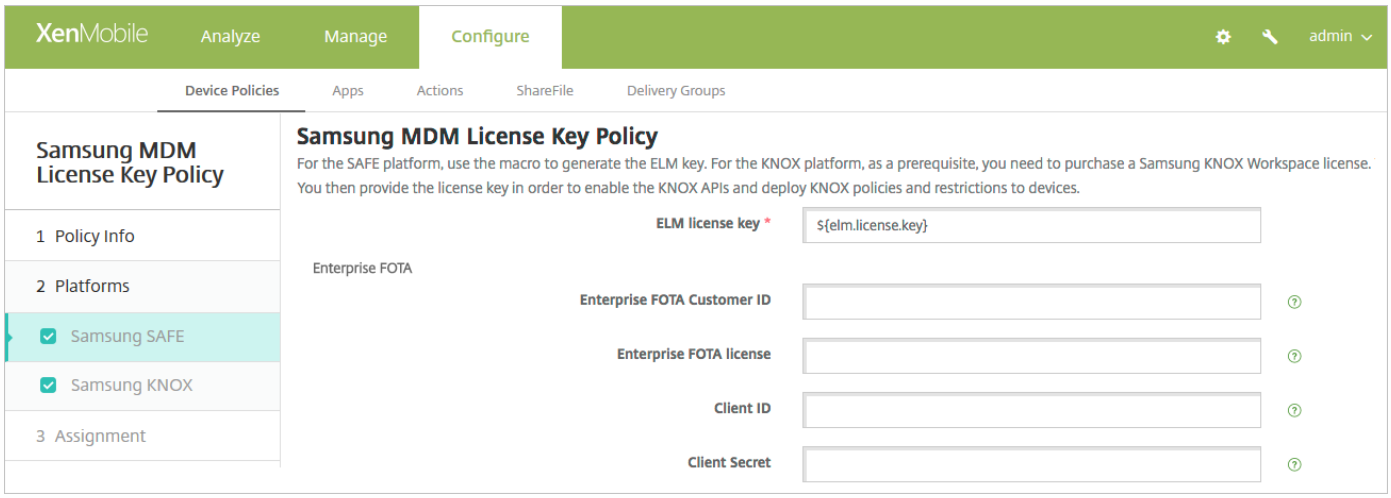
O Samsung Enterprise FOTA (E-FOTA) permite determinar quando os dispositivos são atualizados e a versão do firmware a ser usada. O E-FOTA permite que você teste as atualizações antes de implantá-las, para garantir que as atualizações sejam compatíveis com seus aplicativos. Você pode forçar os dispositivos 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para configurar uma política E-FOTA:

1. Crie uma política de 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.

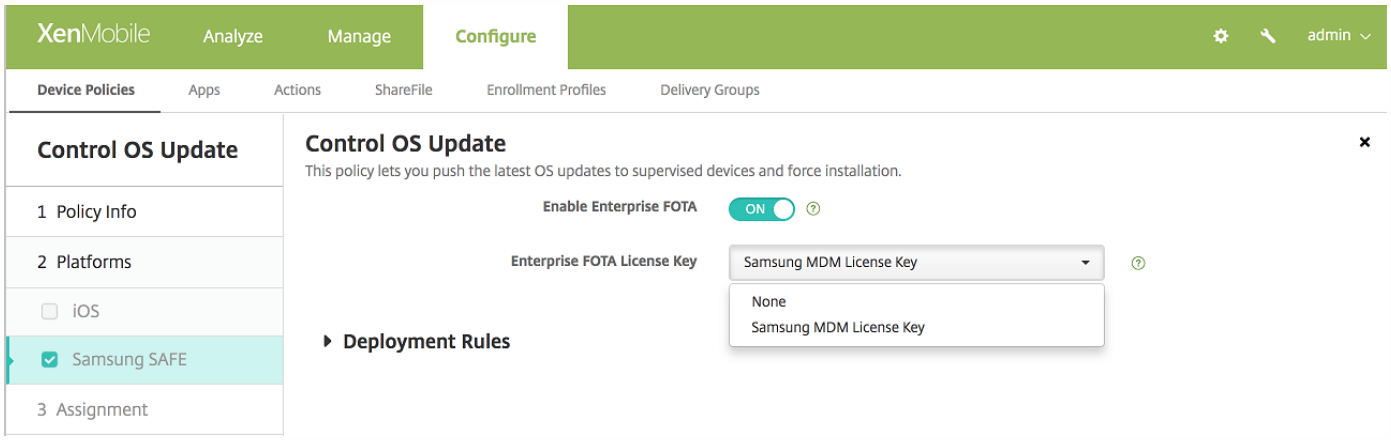


- **Chave de licença ELM**: esse campo contém a macro que gera a chave de licença ELM. Se o campo estiver em branco, digite a macro ${elm.license.key}.

  Digite as seguintes informações fornecidas pela Samsung quando você adquiriu um pacote E-FOTA:

  ID do cliente Enterprise FOTA
  Licença do Enterprise FOTA
  ID de cliente
  Segredo de cliente

2. Crie uma política de controle de atualização do sistema operacional.



Defina estas configurações:

- **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.

Segurança aprimorada de perfis de trabalho do Android for Work

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Código secreto de perfil de trabalho

Em dispositivos que executam o Android 7.0 e versões posteriores, você agora pode exigir um código secreto para aplicativos dentro de um perfil de trabalho do Android for Work. Os usuários são solicitados a inserir o código secreto quando tentam abrir os aplicativos no perfil de trabalho. Quando os usuários digitam o código secreto, eles podem acessar aplicativos no perfil de trabalho.

Você configura um requisito de código secreto somente para o perfil de trabalho ou para o dispositivo.

Para configurar um requisito de código secreto para o perfil de trabalho, vá para **Configurar > Políticas de dispositivo**, adicione a política de **Código secreto** e defina estas configurações:

- **Desafio de segurança do perfil de trabalho**: ative esta configuração para exigir que os usuários concluam um desafio de segurança para acessar aplicativos que são executados em um perfil de trabalho do Android for Work. Essa opção não está disponível para dispositivos Android anteriores ao Android 7.0. O padrão é **O**.
- **Requisitos de código secreto para desafio de segurança de perfil de trabalho**:
  - **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 ativar essa opção, o campo **Caracteres obrigatórios** estará oculto. O padrão é **O**. Esse recurso não é compatível no momento.
  - **Caracteres obrigatórios:** configura como os códigos secretos são compostos. Use **Sem restrições** somente para dispositivos que executam o Android 7.0. Android 7.1 e versões posterior não oferecem suporte à configuração **Sem restrições**. O padrão é **Letras e números**.

Políticas de segurança padrão

Por padrão, as configurações de **Depuração de USB** e **Fontes desconhecidas** são desativadas em um dispositivo quando ele é registrado no Android for Work no modo de perfil de trabalho.

Cancelar o registro de um Android for Work Enterprise

O XenMobile agora permite cancelar o registro de um enterprise do Android for Work usando o console do 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 branca de bloqueio de pop-up.

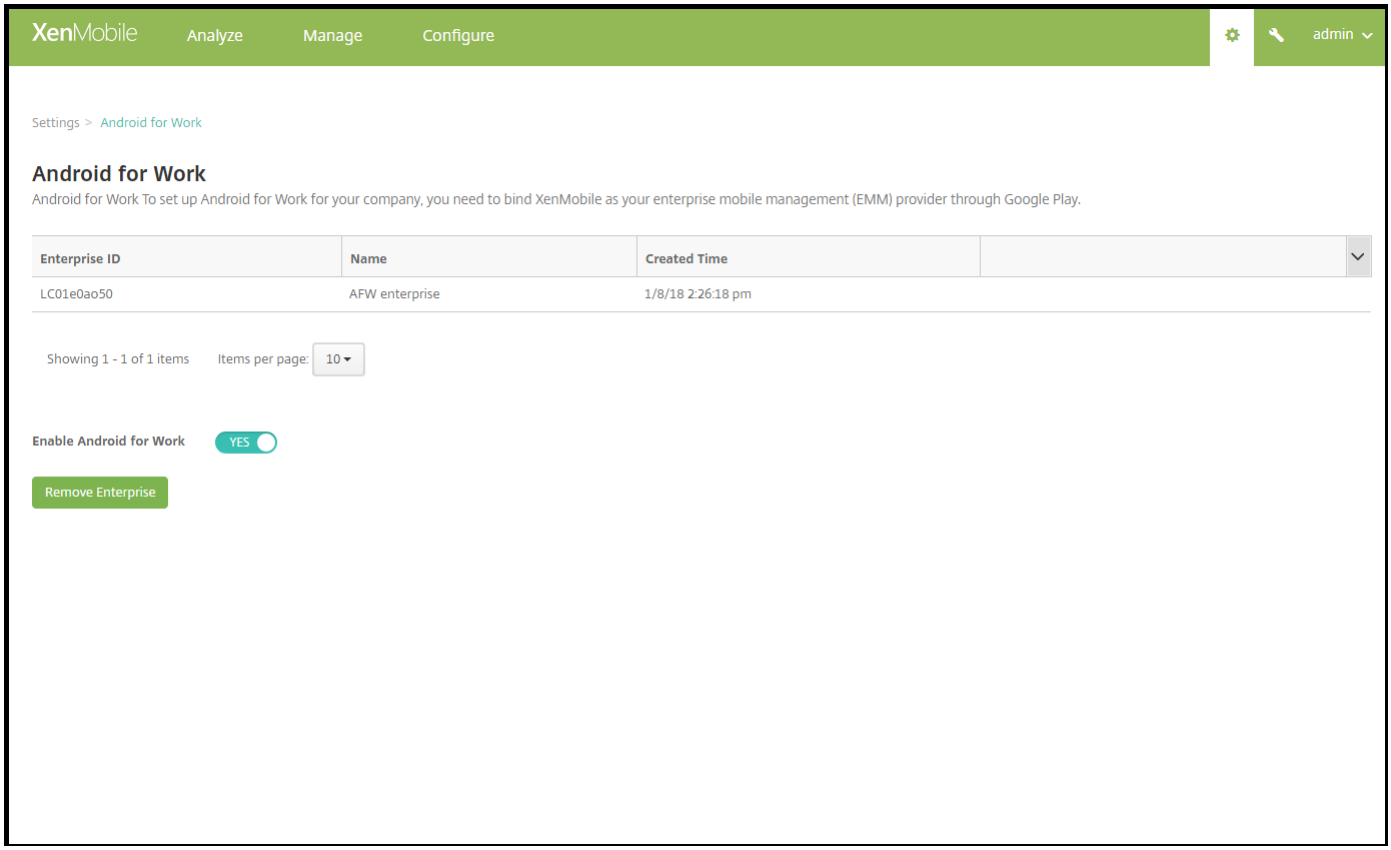
Depois que o registro do enterprise do Android for Work for cancelado:

- Dispositivos e usuários registrados pelo Enterprise têm os aplicativos do Android for Work redefinidos para o estado padrão. As políticas de Permissões de aplicativos do Android for Work e de Rrestrições de aplicativos do Android for Work aplicadas anteriormente não afetam mais as operações.
- Embora o XenMobile gerencie dispositivos inscritos no Enterprise, o Google não os gerencia. Você não pode adicionar novos aplicativos do Android for Work. Você não pode aplicar novas políticas de Permissões de aplicativos do Android for Work e de Rrestrições de aplicativos do Android for Work. Você ainda pode aplicar outras políticas, como Agendamento, Senha e Restrições a esses dispositivos. Os dispositivos precisam ser registrados novamente para permitir que novas políticas de aplicativos do Android for Work e políticas específicas do Android for Work sejam aplicadas.
- Se você tentar registrar dispositivos no Android for Work, eles serão registrados como dispositivos Android, não como dispositivos Android for Work.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

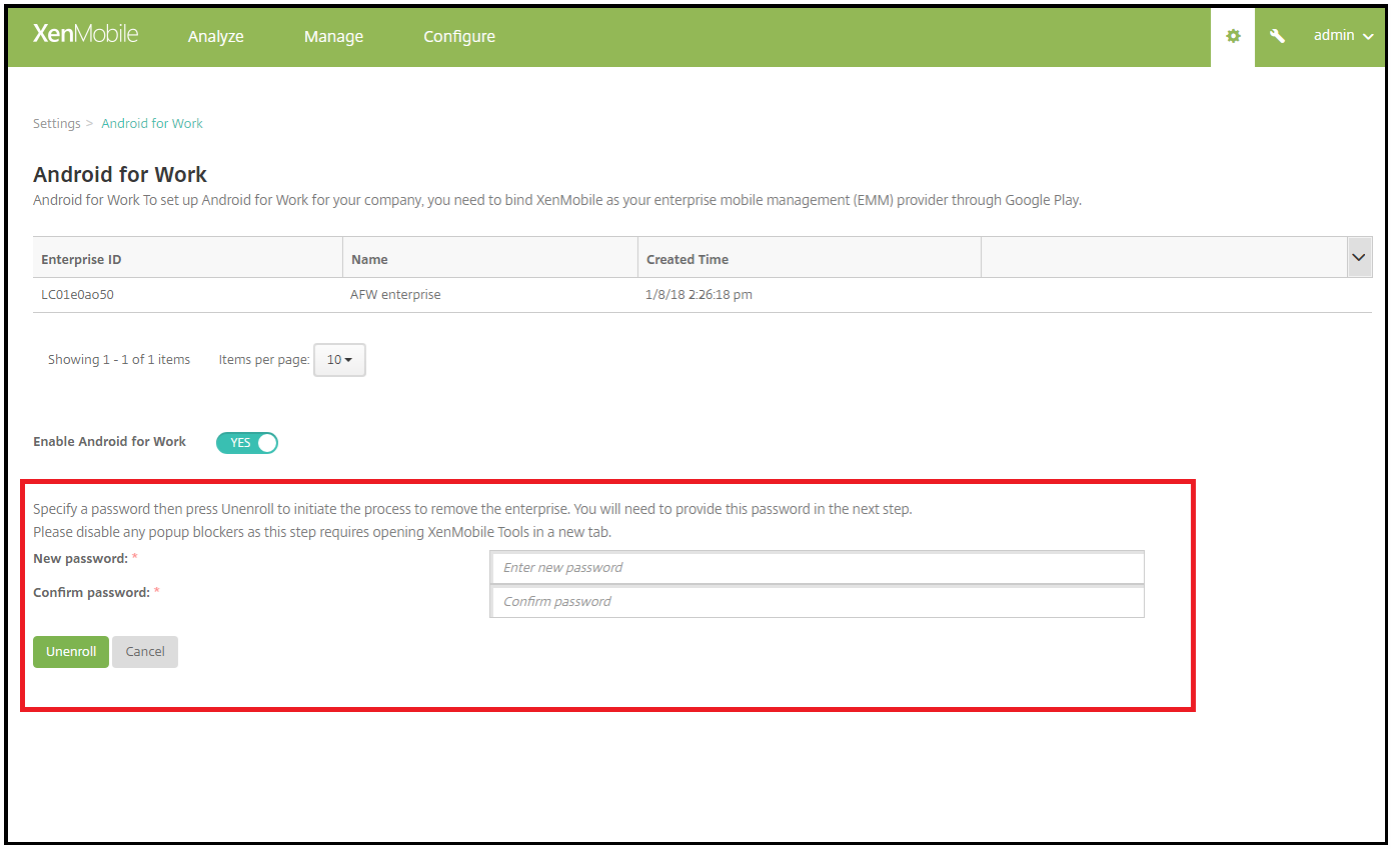
Para cancelar o registro de um Android for Work Enterprise:

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.
2. Na página Configurações, clique em **Android for Work**.
3. Clique em **Remover Enterprise**.

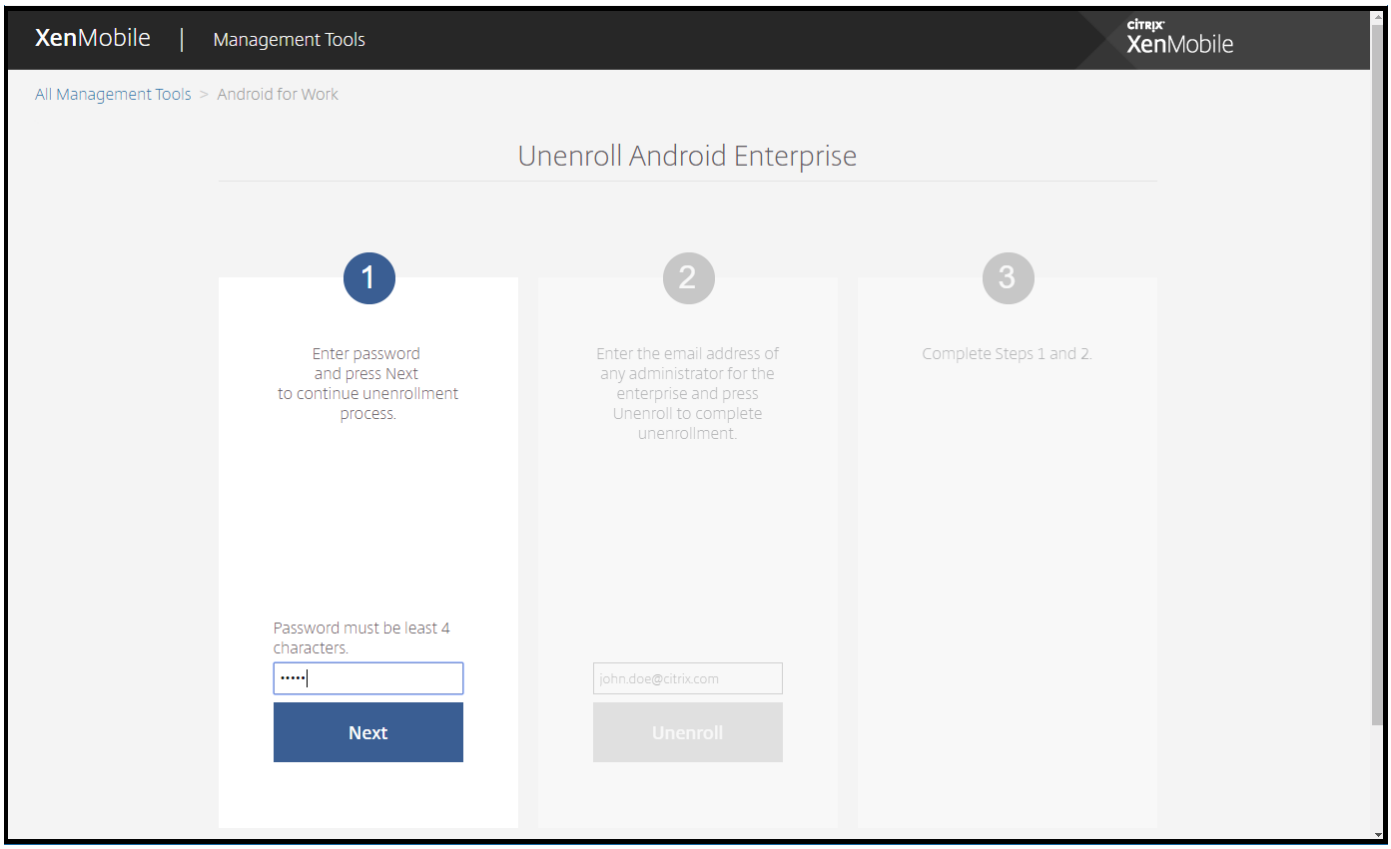


4. Especifique uma senha. Você precisará da senha na próxima etapa para concluir o cancelamento do registro. Em seguida, clique em **Cancelar registro**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

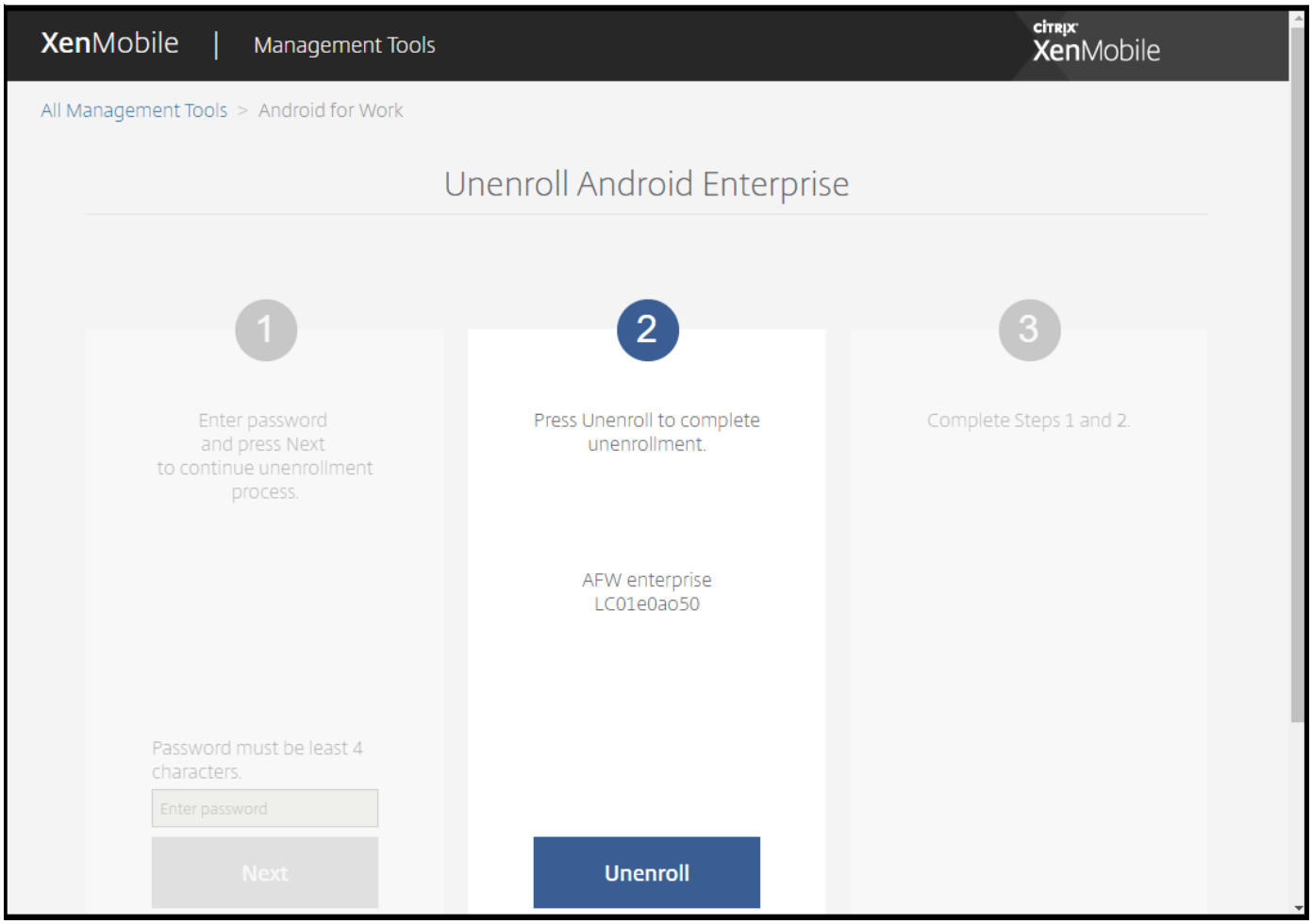


5. Quando a página do XenMobile Tools for aberta, insira a senha que você criou na etapa anterior.



6. Clique em **Cancelar registro**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Especificar o comportamento quando aplicativos do Android for Work solicitam permissões perigosas

Para solicitações a aplicativos do Android for Work que estão em perfis de trabalho: uma nova política de dispositivo permite configurar como essas solicitações lidam com o que o Google chama de permissões "perigosas". Você controla se os usuários devem conceder ou negar uma solicitação de permissão de aplicativos. Esse recurso é para dispositivos que executam o Android 7.0 e versões posteriores.

O Google define permissões perigosas como permissões que dão a um aplicativo acesso ao seguinte:

- Dados ou recursos que envolvem informações particulares do usuário.
- Recursos que podem afetar os dados armazenados de um usuário ou a operação de outros aplicativos. Por exemplo, a capacidade de ler contatos do usuário é uma permissão perigosa.

Para aplicativos do Android for Work que estão em perfis de trabalho: você pode configurar um estado global que controla o comportamento de todas as solicitações de permissões perigosas para os aplicativos. 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.

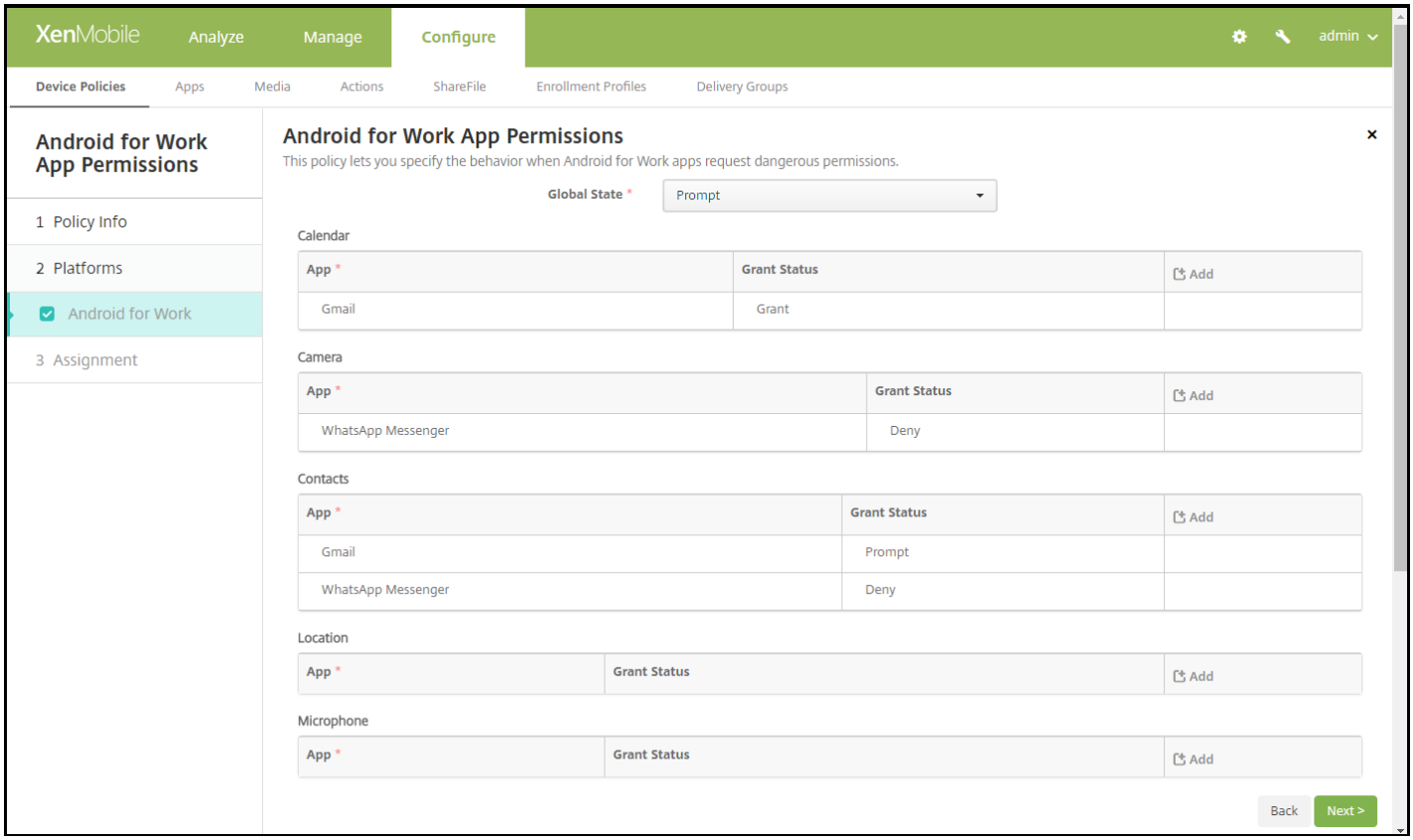
Para obter informações sobre como o Google define grupos de permissões, consulte "Grupos de permissões" no guia de desenvolvedores do Android.

Por padrão, os usuários são solicitados a conceder ou negar solicitações de permissões perigosas.

Para configurar permissões para aplicativos do Android for Work, vá para **Configurar > Políticas de dispositivos** e adicione

© 1999-2017 Citrix Systems, Inc. All rights reserved.

a política de **Permissões de aplicativos do Android for Work**. Essa política se aplica somente aos aplicativos que você adiciona e aprova no console do Google Play primeiro e, depois, adiciona ao XenMobile como aplicativos de loja pública.



Defina estas configurações.

- **Estado global:** controla o comportamento de todas as solicitações de permissões perigosas. Na lista, clique em **Solicitar**, **Conceder** ou **Negar**. O padrão é **Solicitar**.
  - **Solicitar**: solicita aos usuários para conceder ou negar solicitações de permissões perigosas.
  - **Conceder**: concede todas as solicitações de permissões perigosas sem avisar aos usuários.
  - **Negar**: nega todas as solicitações de permissões perigosas sem avisar aos usuários.
- Para substituir o **Estado global** de um grupo de permissões, defina um comportamento individual para o grupo de permissões. Para definir as configurações de um grupo de permissões, clique em **Adicionar**, escolha um aplicativo na lista e escolha um **Status de concessão**.

SNMP Monitoring

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.

Para mais informações sobre o SNMP Monitoring, consulte SNMP Monitoring.

Suporte para o driver Microsoft JDBC para SQL Server

O XenMobile Server agora suporta o driver JDBC (Microsoft Java Database Connectivity) para SQL Server. O driver jTDS permanece como o driver padrão quando você instala o XenMobile Server no local ou atualiza de um XenMobile Server que use o driver jTDS.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para ambos os drivers, o XenMobile é compatível com a autenticação do SQL Server ou com a autenticação do Windows, com SSL ativado ou desativado.

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 Microsoft JDBC, use SSH para todos os nós do XenMobile Server. Em seguida, use a CLI do XenMobile para definir as configurações. As etapas variam de acordo com a sua configuração do driver jTDS atual. Para obter mais informações, consulte Drivers do SQL Server.

Alterações na propriedade do servidor para melhorar o ajuste do servidor

Para várias propriedades do servidor usadas para ajustar as operações do XenMobile, os valores padrão agora correspondem às recomendações fornecidas em Aprimoramento das operações do XenMobile.

Aqui estão as propriedades de servidor atualizado, com seus novos valores padrão entre parênteses:

- hibernate.c3p0.timeout (120 segundos)
- Intervalo de pulsação de serviços de envio por push: ios.apns.heartbeat.interval, windows.wns.heartbeat.interval, gcm.heartbeat.interval (20 horas)
- auth.ldap.connect.timeout (60000)
- auth.ldap.read.timeout (60000)
- Tamanho do pool de conexão APNS de MDM iOS
- Implantação em segundo plano (1440 minutos)
- Inventário de hardware em segundo plano (1440 minutos)
- Intervalo para verificação de usuário do Active Directory excluído (15 minutos)

Além disso, o valor padrão da seguinte propriedade do servidor foi alterado para a configuração recomendada em Propriedades do Servidor:

- Bloquear registro de dispositivos Android com root e iOS com jailbreak (verdadeiro)

Agora você pode ajustar ainda mais o XenMobile Server por meio das seguintes propriedades de servidor personalizadas que antes não eram documentadas.

Chave personalizada: **hibernate.c3p0.min_size**

> Essa propriedade do XenMobile Server, uma chave personalizada, determina o número mínimo de conexões que o XenMobile abre no banco de dados do SQL Server. O padrão é **50**.
>
> Para alterar essa configuração, você deve adicionar uma propriedade de servidor ao XenMobile Server com a seguinte configuração:
>
> Chave: **chave personalizada**
>
> Chave: **hibernate.c3p0.min_size**
>
> Valor: **50**
>
> Nome de exibição: **hibernate.c3p0.min_size=*nnn***

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Descrição: **conexões de banco de dados com o SQL**

Chave personalizada: **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. O padrão é **30**.

Para alterar essa configuração, você deve adicionar uma propriedade de servidor ao XenMobile Server com a seguinte configuração:

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 em hibernação**

Pesquisa otimizada de propriedades de dispositivos

Anteriormente, uma pesquisa de dispositivos na página **Gerenciar > Dispositivos** incluía todas as propriedades do dispositivo por padrão, o que poderia retardar a pesquisa. Agora, o escopo de pesquisa padrão inclui apenas as seguintes propriedades do dispositivo:

- Número de série
- IMEI
- Endereço MAC WiFi
- Endereço MAC Bluetooth
- Active Sync ID
- Nome de usuário

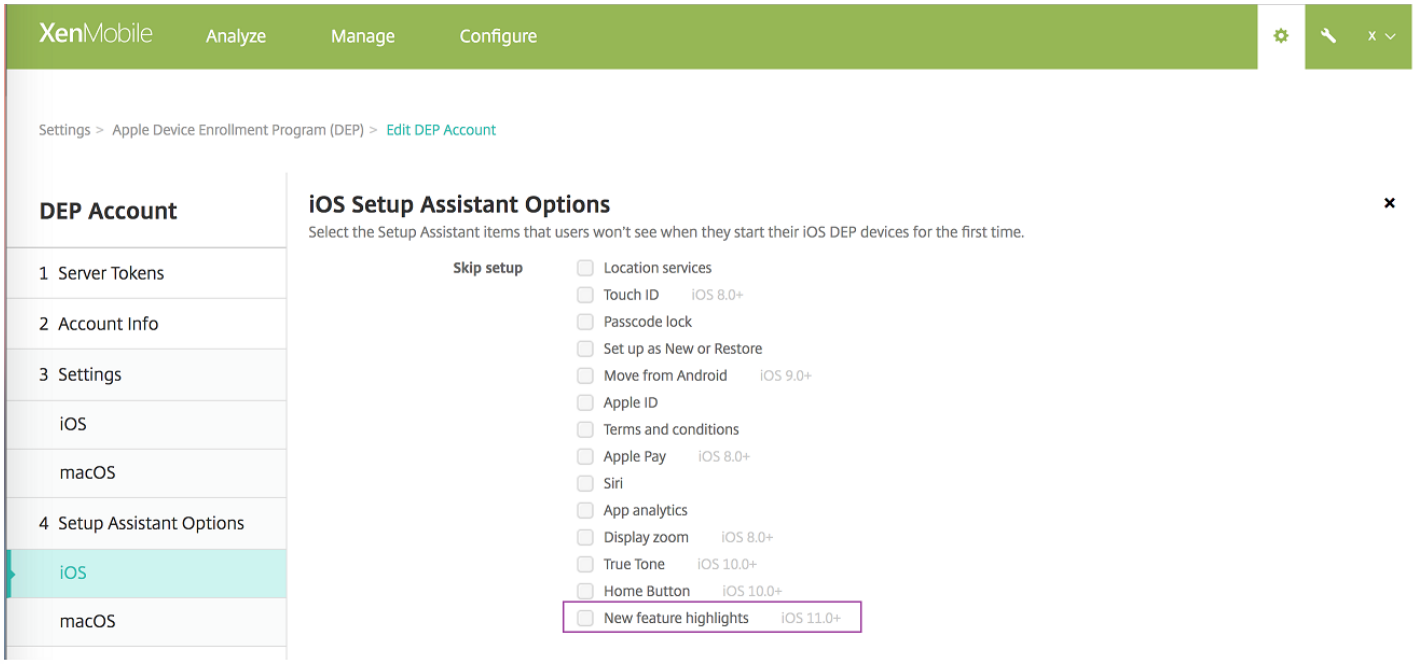
Você pode configurar o escopo da pesquisa usando uma nova propriedade do servidor, **include.device.properties.during.search**, cujo padrão é **false**. Para incluir todas as propriedades de dispositivo em uma pesquisa no dispositivo, altere a configuração para **true**.

Outras melhorias

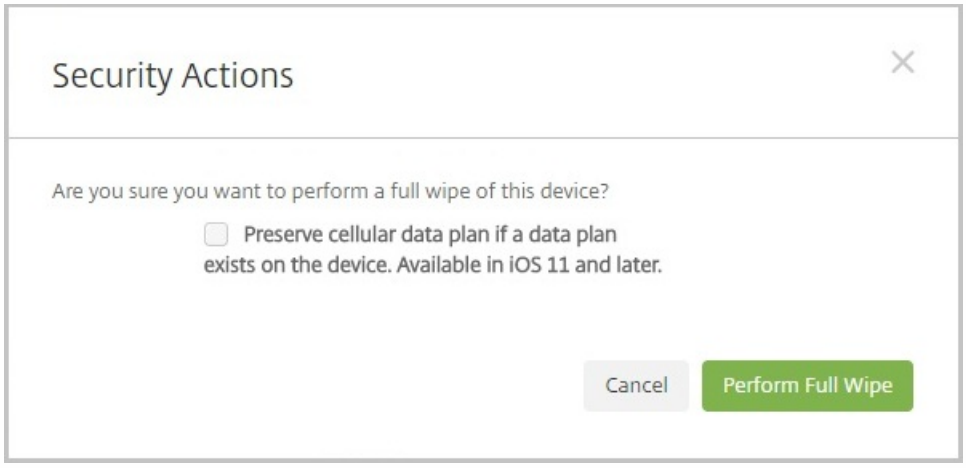
- **Nova Opção do Assistente de Instalação do iOS: Destaques do novo recurso.** O item Assistente de Instalação do iOS, **Destaques do novo recurso**, configura essas telas informativas de integração: acessar o Dock em qualquer lugar e alternar entre aplicativos recentes. Você pode optar por omitir essas telas de integração nas etapas do Assistente de Instalação do iOS, quando os usuários iniciarem seus dispositivos pela primeira vez.

  Destaques do novo recurso está disponível para iOS 11.0 (versão mínima). O padrão é desmarcar essa opção para todos os itens.

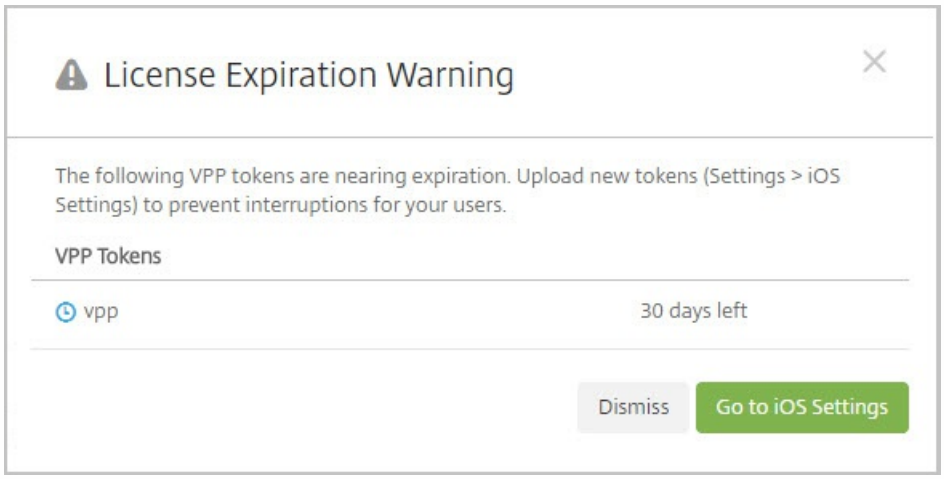
© 1999-2017 Citrix Systems, Inc. All rights reserved.



- Ao realizar um apagamento completo de um dispositivo iOS 11 que tenha um plano de dados celulares, você pode optar por preservar o plano de dados.



- O XenMobile agora exibe um Aviso de Expiração de Licença quando os tokens Apple VPP ou DEP estão prestes a expirar ou expiraram.

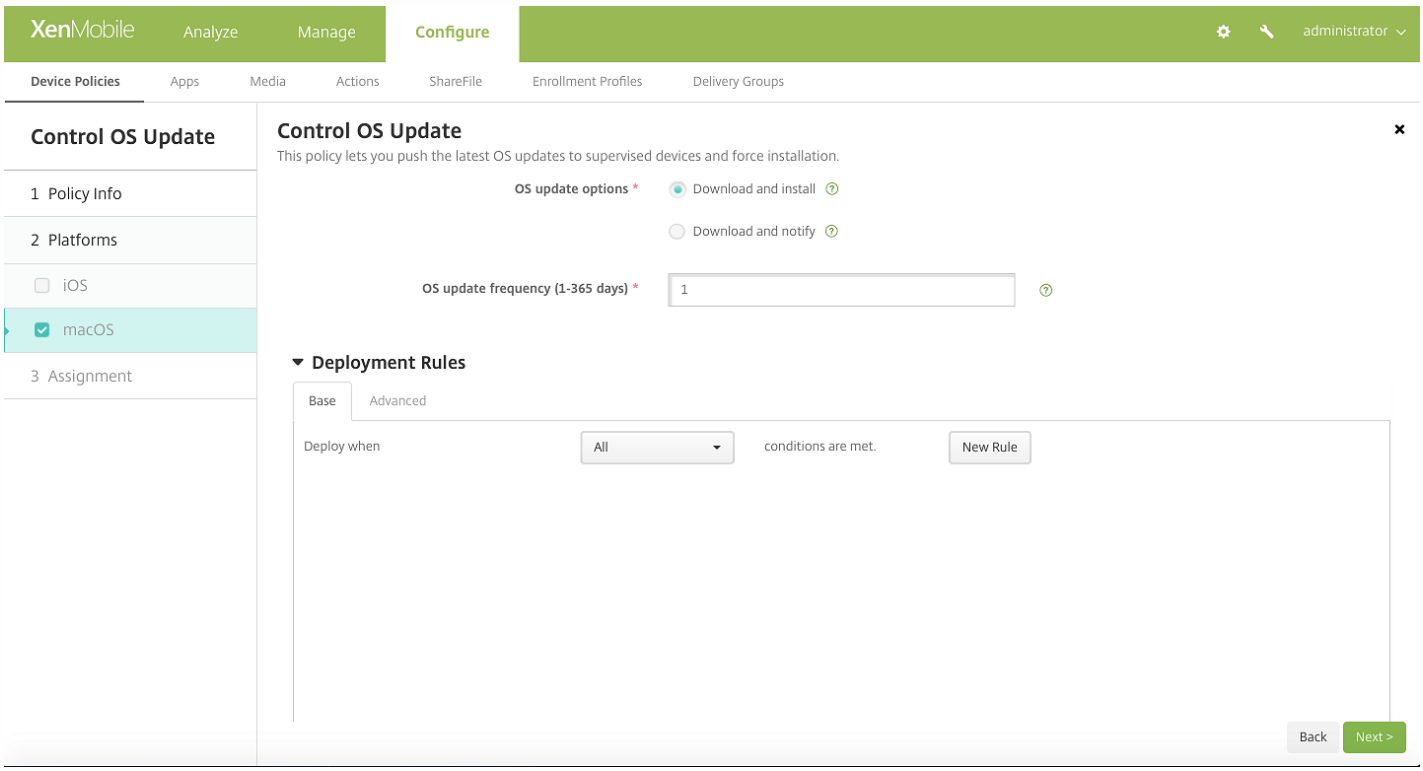


- A interface do console XenMobile para aplicativos macOS VPP mudou da seguinte forma:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Em Configurar > Apps, você pode filtrar aplicativos pelo macOS VPP.**Partes da interface que não se aplicam a um aplicativo macOS VPP agora são omitidas. Por exemplo, a seção de configuração da loja não aparece porque não existe um Secure Hub para macOS. A opção de importação de chaves VPP não é exibida.
- **Em Gerenciar > Dispositivos, as Propriedades do Usuário incluem Desativar conta VPP.**

- **Política de dispositivo Controlar atualização do sistema operacional para macOS**. Agora você pode usar a política de controle de atualização do sistema operacional para implantar atualizações de sistema operacional em dispositivos macOS que são supervisionados ou são implementados por meio do Apple DEP.



- **Opção para permitir que vários usuários usem um dispositivo Samsung SAFE.** A política de dispositivo Restrições agora inclui a opção de controle de hardware, **Permitir vários usuários**. Essa opção, para MDM 4.0 e posterior, tem o padrão **o**.
- **Desativar aplicativos em dispositivos Samsung SAFE**. Agora você usa a política de dispositivo Restrições para impedir que uma lista de aplicativos instalados sejam executados em dispositivos Samsung SAFE. As opções do **navegador**, do **YouTube** e do **Google Play/Marketplace** estão obsoletas.

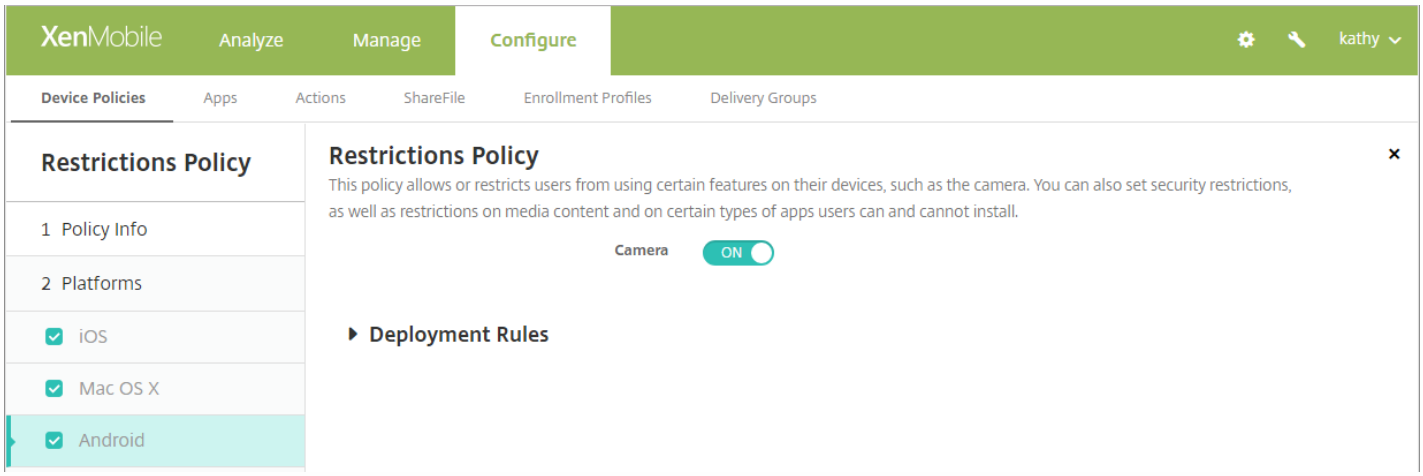
  Por padrão, a nova configuração **Desativar aplicativos** está **desativada**, o que significa que os aplicativos estão ativados. Para desabilitar um aplicativo instalado, altere a configuração para **Ativado**, clique em **Adicionar** na tabela **Lista de Aplicativos** e digite o nome do pacote do aplicativo.

  Alterar e implantar uma lista de aplicativos sobrescreve a lista de aplicativos anterior. Por exemplo: suponha que você desative com.example1 e com.example2. Depois, você altera a lista para com.example1 e com.example3. Nesse caso, o XenMobile ativa com.example.2.
- Agora, a página **Gerenciar> Dispositivos** inclui essas propriedades de dispositivo adicionais relatadas por dispositivos Android:

  Código de operadora (relatado somente por dispositivos que executam o Samsung MDM 5.7 ou superior)
  Número de modelo (relatados apenas por dispositivos que executam o Samsung MDM versão 2.0 ou superior)
- **Política de dispositivo Restrições agora inclui uma política para desativar a câmera nos dispositivos Android**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para configurar a política, vá para **Configurar > Políticas de dispositivo**, clique em **Adicionar** e clique em **Restrições**. Por padrão, o uso da câmera está ativado. Para desativar o uso da câmera, altere a configuração da **Câmera** para **desativado**.



- **Formatos de data e hora baseados em localização**. A data e a hora exibidas nas páginas Gerenciar> Dispositivos e Gerenciar> Usuários agora estão formatadas de acordo com a localidade. Por exemplo, 18h em 15 de outubro de 2017 é exibido da seguinte maneira:

  Estados Unidos (en-US): 10/15/17 06:00:00 pm
  Reino Unido (en-GB): 15/10/17 18:00:00
  África do Sul (en-ZA): 2017/10/15 06:00:00 pm

- A política de dispositivo Samsung SAFE Firewall é renomeada para a política de dispositivo Firewall.
- O número padrão de arquivos de backup incluídos nos pacotes de suporte foi reduzido para 100 nos arquivos a seguir. O tamanho padrão desses arquivos é 10 MB.
  - DebugLogFile
  - AdminAuditLogFile
  - UserAuditLogFile
  - 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 (Solução de problemas e suporte -> Configurações de log), os arquivos de log externos serão imediatamente excluídos daquele nó de servidor.

- A página **Configurações > Syslog** agora inclui uma opção para enviar logs de depuração do XenMobile Server para um servidor syslog.
- **Atualizações à API pública do XenMobile para serviços REST**.
- A API pública do XenMobile para serviços REST inclui essas novas APIs: Para obter mais informações, baixe o arquivo PDF XenMobile Public API for REST Services e consulte as seções indicadas a seguir.
  - Get Users by Filter (seção 3.12.1)

    Essa nova API substitui a API obsoleta para obter todos os usuários, Get All Users.
  - Revoke Enrollment Token (seção 3.19.6)
  - Remove Enrollment Token (seção 3.19.7)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Novidades no XenMobile Server 10.7

Feb 21, 2018

> ## Nota
>
> Para obter o conjunto completo da documentação do produto XenMobile Server 10.7, consulte o PDF.
>
> O Touchdown da Symantec atingiu o fim da vida útil em 3 de julho de 2017, com fim de suporte padrão, fim de suporte estendido e fim de suporte da vida útil em 2 de julho de 2018. Para obter mais informações, consulte o artigo de suporte da Symantec Aviso de Fim da vida, Fim de suporte e Fim da disponibilidade do Touchdown.

Para obter informações sobre como atualizar, consulte Atualização. Para acessar o console de gerenciamento do XenMobile, use somente o nome de domínio totalmente qualificado do XenMobile Server ou os endereços IP do nó.

> ## Important
>
> **Após uma atualização para o XenMobile 10.7:**
>
> Se a funcionalidade que envolve as conexões de saída deixar de funcionar e você não tiver alterado sua configuração de conexão, 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 ao assunto do certificado fornecido pelo par.
>
> Se você receber o erro de validação de certificado, desative a verificação de nome de 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**.

O XenMobile Server 10.7 inclui os novos recursos a seguir.

- Integrar-se com os recursos do Apple Educação
- Implantar iBooks nos dispositivos iOS
- Política de dispositivo BitLocker
- Novas restrições para dispositivos supervisionados que executam o iOS 10.3 e versões posteriores
- Reiniciar ou desligar um dispositivo iOS supervisionado
- Localizar ou chamar um dispositivo iOS supervisionado que está no modo perdido
- Suporte aprimorado do Android for Work
- Mais macros para modelos de registro
- Outras melhorias
- Mudanças na API pública REST

Para obter correções de bugs, consulte Problemas resolvidos.

> ## Important
>
> O TouchDown da Symantec atingiu o fim da vida útil em 3 de julho de 2017, com fim de suporte padrão, fim de suporte estendido

© 1999-2017 Citrix Systems, Inc. All rights reserved.

e fim de suporte da vida útil em 2 de julho de 2018. Para obter mais informações, consulte o artigo de suporte da Symantec Aviso de Fim da vida, Fim de suporte e Fim da disponibilidade do TouchDown.

Integrar-se com os recursos do Apple Educação

Você pode usar o XenMobile Server como sua solução de gerenciamento de dispositivos móveis (MDM) em um ambiente que usa o Apple Educação. O XenMobile suporta os aprimoramentos do Apple Educação introduzidos no iOS 9.3, incluindo o Apple School Manager e o aplicativo Classroom para iPad. A nova política de dispositivo de Configuração do XenMobile Education configura os dispositivos de instrutor e estudante para uso com o Apple Educação.

O seguinte vídeo fornece um tour rápido das alterações feitas ao Apple School Manager e ao XenMobile Server.

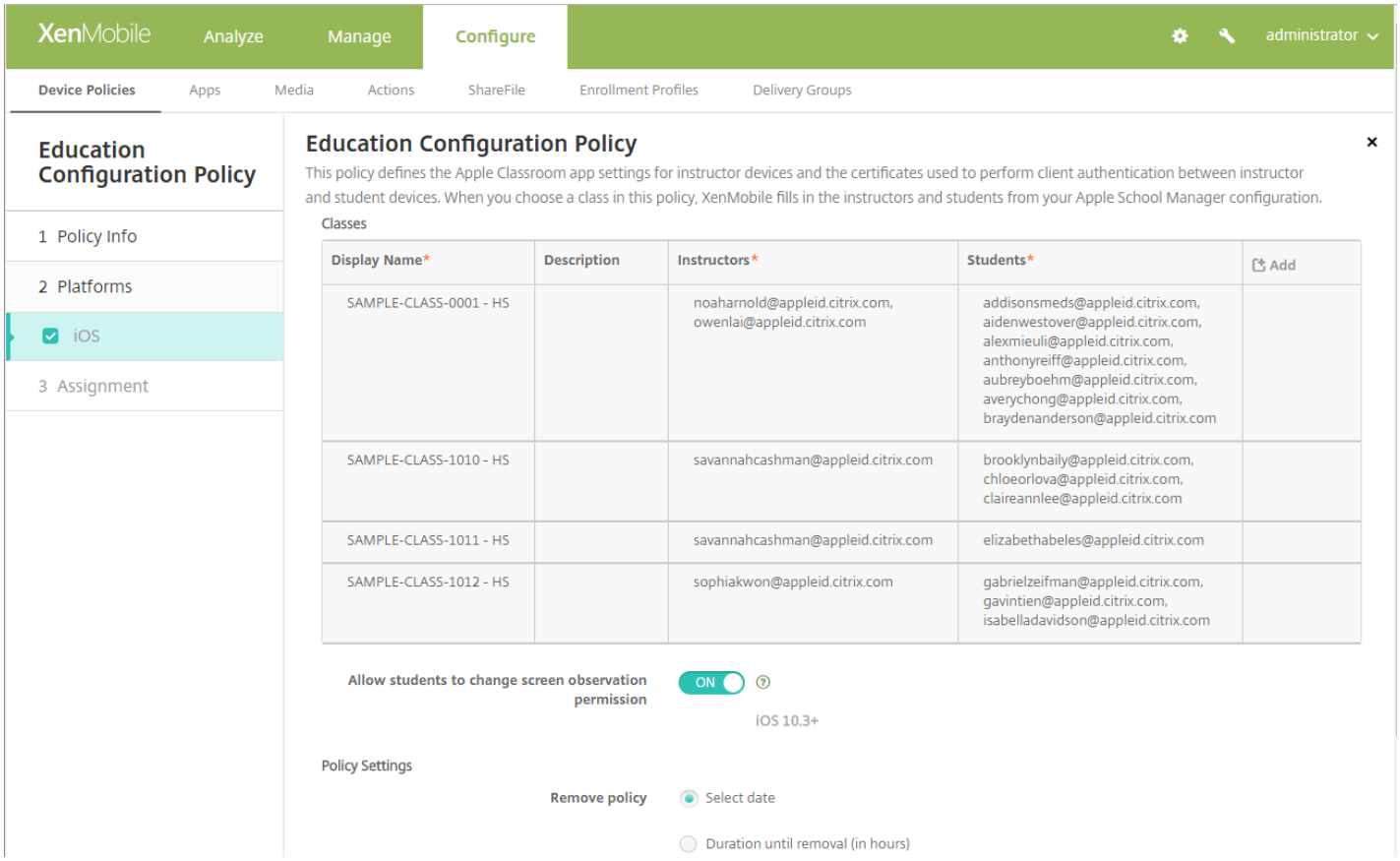
Configuração do Citrix XenMobile Education: integre os recursos do Apple Educação com o XenMobile

Você fornece iPads pré-configurados e supervisionados para instrutores e alunos. Essa configuração inclui:

- Registro do Apple School Manager DEP no XenMobile
- Uma conta do ID do Apple gerenciada e configurada com uma nova senha
- Aplicativos VPP e iBooks obrigatórios

Para obter detalhes sobre a integração com os recursos do Apple Educação, consulte Integrar-se com os recursos do Apple Educação e a Política do dispositivo Configuração de Educação.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Implantar iBooks nos dispositivos iOS

Você pode usar o XenMobile para implantar iBooks que obtém por meio do Programa Apple Volume Purchase (VPP). Depois de configurar uma conta VPP no XenMobile, seus livros comprados e gratuitos aparecem em **Configurar > Mídia**. Nas páginas de **Mídia**, você configura iBooks para implantação em dispositivos iOS escolhendo grupos de entrega e especificando regras de implantação.

A primeira vez que um usuário recebe um iBook e aceita a licença VPP, os livros implantados são instalados no dispositivo. Os livros aparecem no aplicativo Apple iBook. Você não pode desassociar a licença do livro do usuário ou remover o livro do dispositivo. O XenMobile instala iBooks como mídia necessária. Se um usuário exclui um livro instalado do seu dispositivo, o livro permanece no aplicativo iBook, pronto para download.

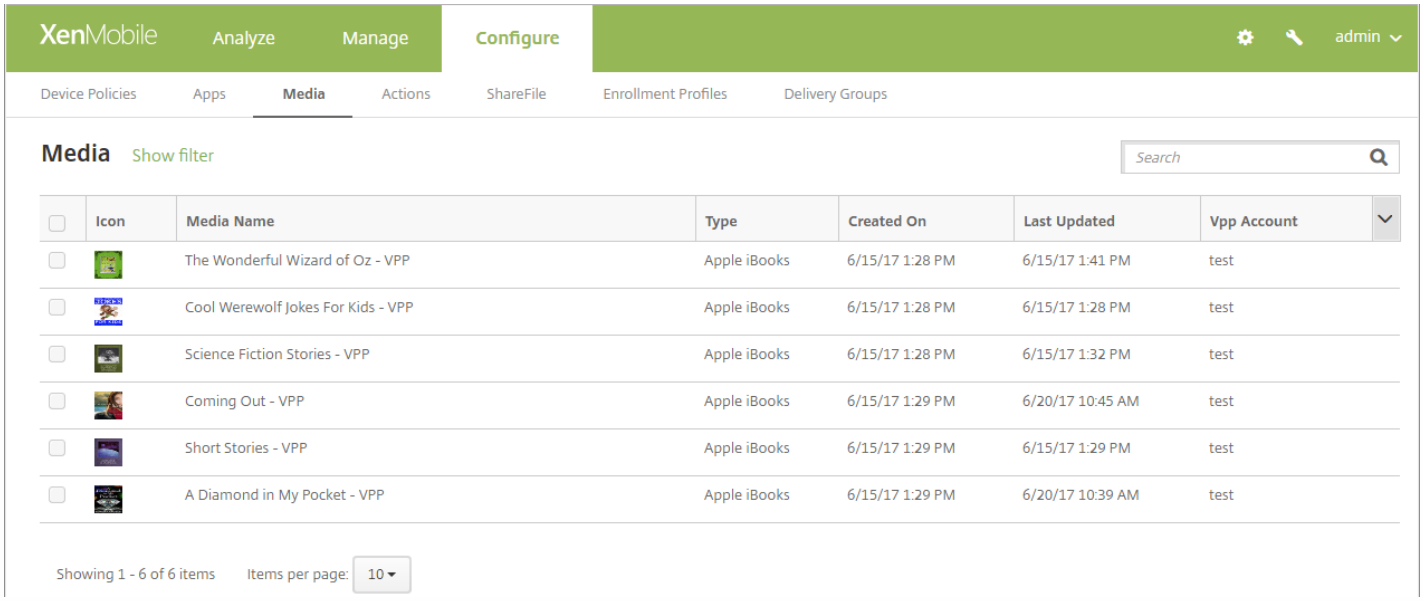
Pré-requisitos

- Dispositivos iOS (versão mínima iOS 8)
- Configurar o VPP do iOS no XenMobile, conforme descrito em Volume Purchase Plan do iOS.

Configurar iBooks

Os iBooks obtidos através do VPP aparecem na página **Configurar > Mídia**. Para obter mais informações, consulte Adicionar mídia.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Política de dispositivo BitLocker

O Windows 10 Enterprise 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 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.

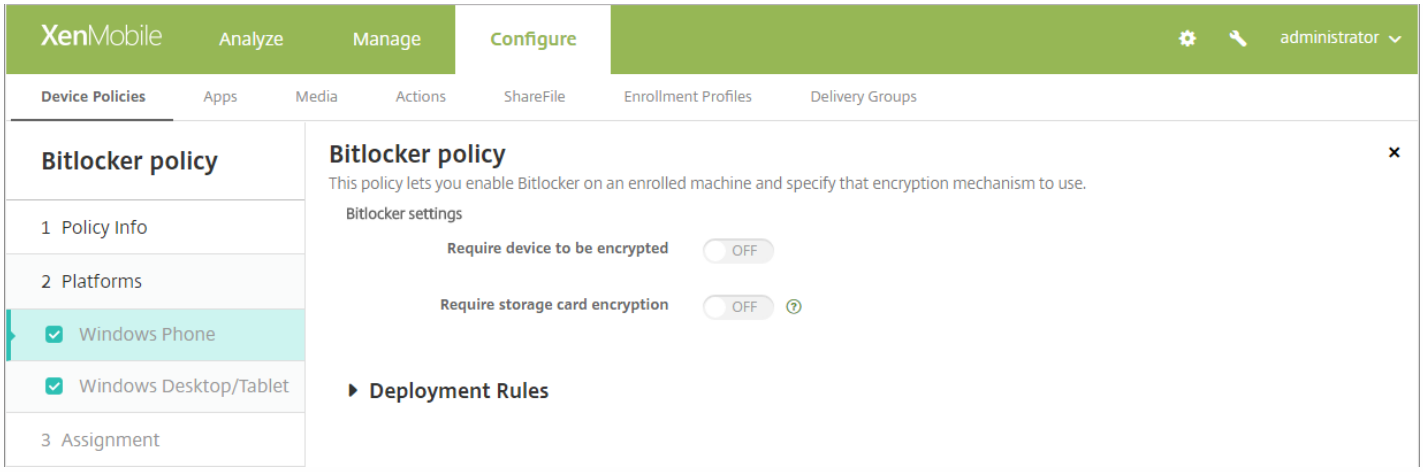
Começando com o Windows 10, compilação 1703, as políticas do MDM podem controlar o BitLocker. Você pode usar a política de dispositivo de BitLocker no XenMobile para definir as configurações disponíveis no Assistente de BitLocker nos dispositivos Windows 10. Por exemplo, em um dispositivo com o BitLocker habilitado, o BitLocker pode solicitar aos usuários:

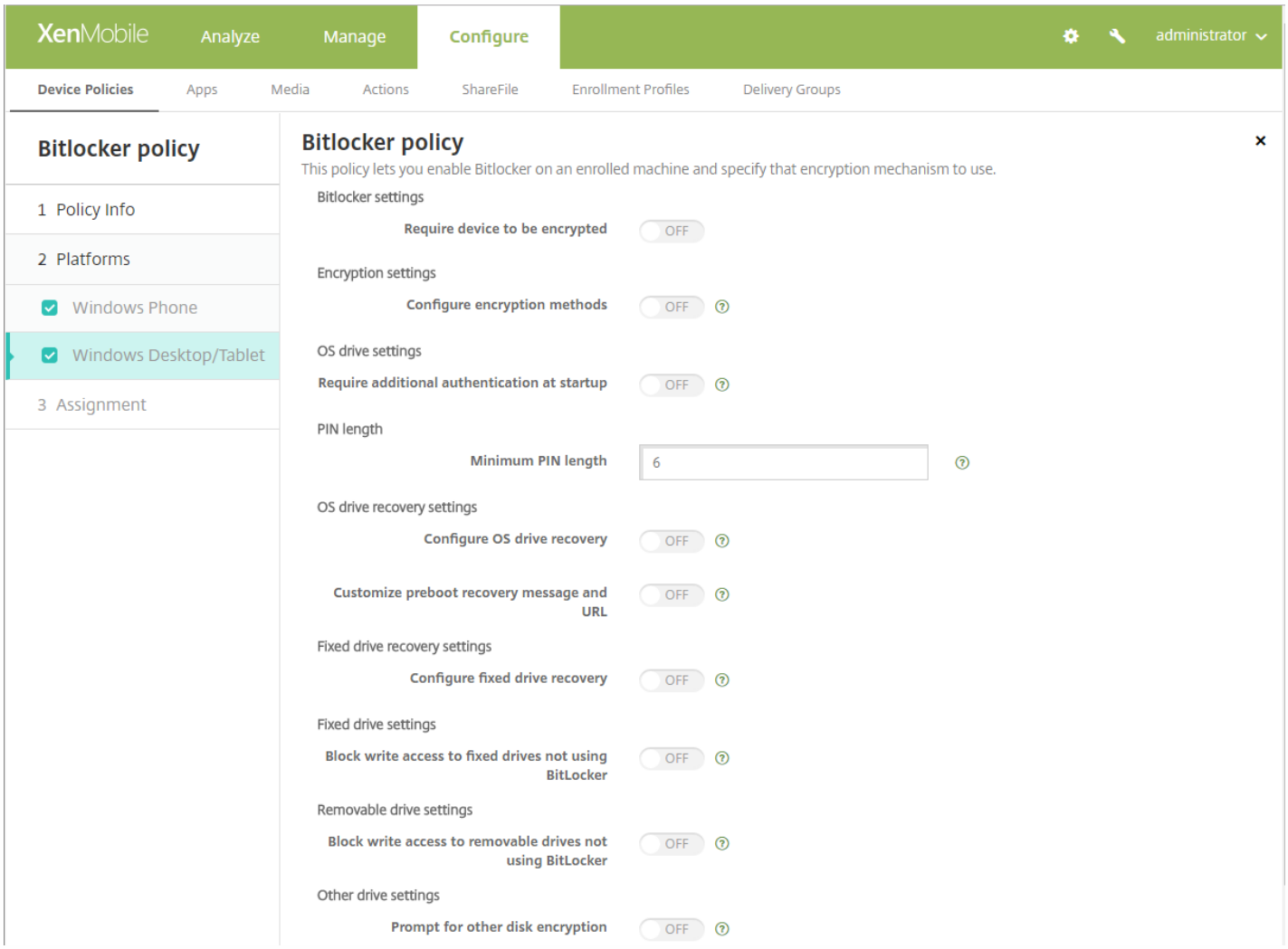
- Como eles querem desbloquear sua unidade na inicialização
- Como fazer backup da sua chave de recuperação
- Como desbloquear uma unidade fixa.

A configuração da política do dispositivo BitLocker também configura se:

- 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.





Para obter mais informações, consulte a Política de dispositivo do BitLocker.

Novas restrições para dispositivos supervisionados que executam o iOS 10.3 e versões posteriores

As restrições permitem impedir que os usuários executem certas ações em seus dispositivos e sejam implementadas através

© 1999-2017 Citrix Systems, Inc. All rights reserved.

de políticas de dispositivos.

As seguintes restrições agora estão disponíveis para os dispositivos que executam o iOS 10.3 e versões posteriores, no modo supervisionado:

- **Permitir ditado**: supervisionado somente. Se essa restrição é definida como **Desativado**, a entrada de ditado não é permitida. O padrão é **ON**. Para iOS 10.3 e posterior.
- **Forçar conexão de WiFi ao inserir na lista branca**: opcional. Apenas supervisionado. Se esta restrição estiver definida como **Ativar**, 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**. Para iOS 10.3 e posterior.

Para definir essas restrições:

1. No console XenMobile, selecione **Configurar > Políticas de dispositivo**. A página Políticas de dispositivo é exibida.
2. Selecione **Adicionar**. A página **Adicionar uma nova política** é exibida.
3. Clique em **Restrições**. A página de restrições **Informações sobre a política** é exibida.
4. No painel **Informações sobre a política**, digite as seguintes informações:

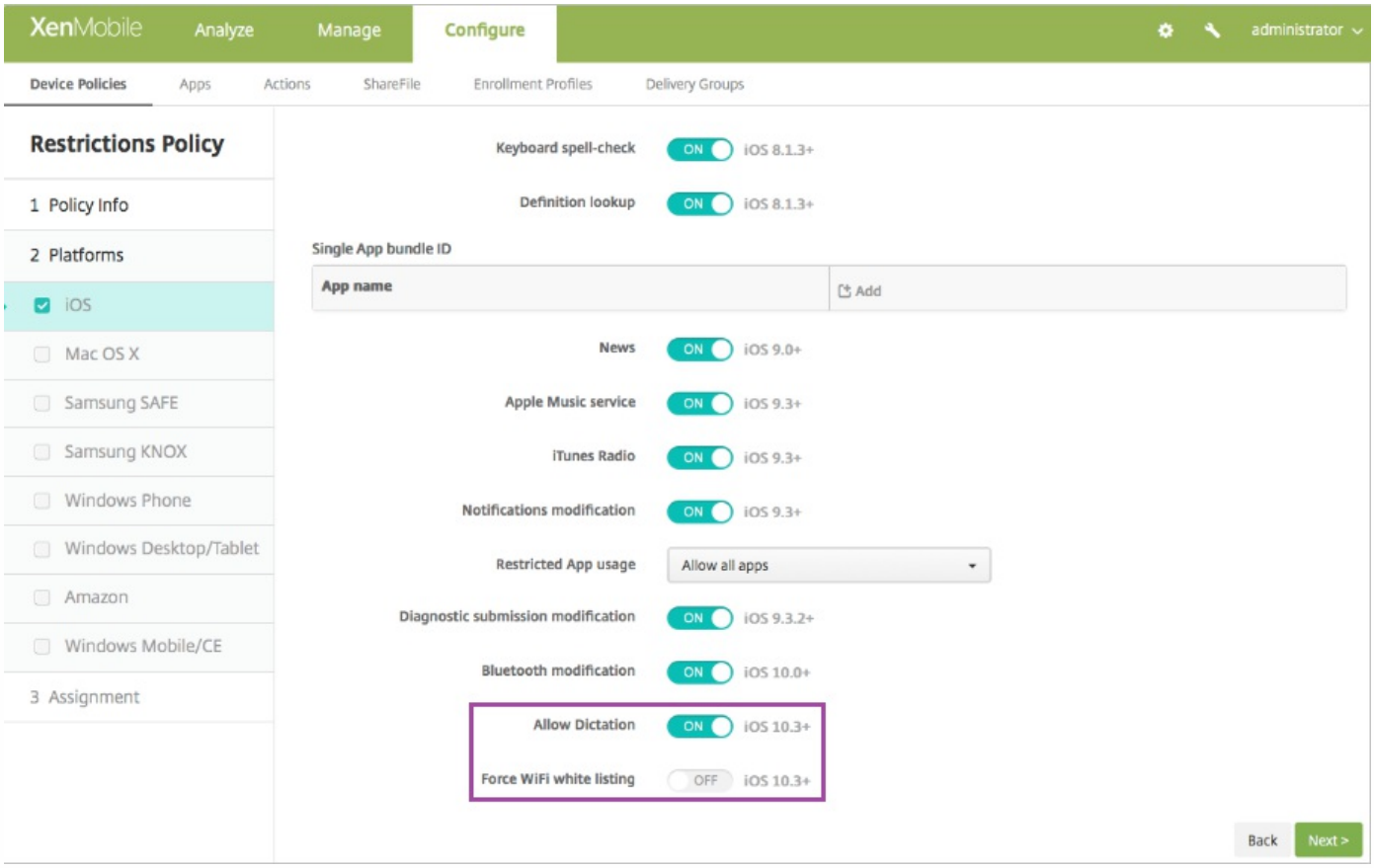
   Nome da política: digite um nome descritivo para a política.

   Descrição: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma de política** é exibida.

   Selecione **iOS**.
6.
7. Clique em **Avançar** até aparecer a página que mostra a seção única de ID do pacote do aplicativo. Defina as restrições.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

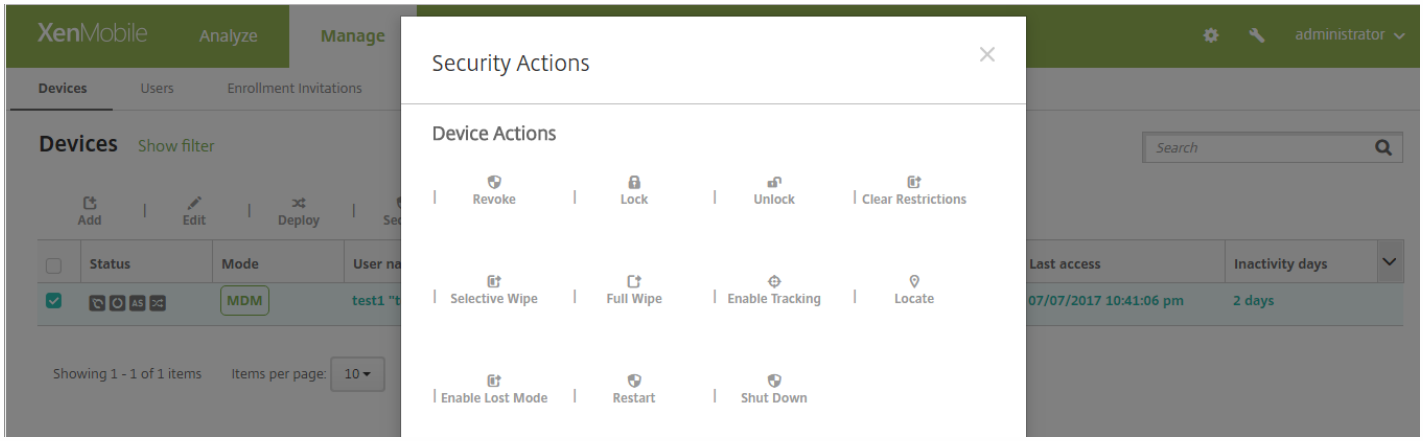


Para obter mais informações sobre como configurar restrições, consulte a política do dispositivo Restrições.

Reiniciar ou desligar um dispositivo iOS supervisionado

Você pode usar ações de segurança para reiniciar ou desligar um dispositivo iOS supervisionado (versão mínima 10.3). Acesse **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Segurança** e em **Reiniciar** ou **Desligar**.

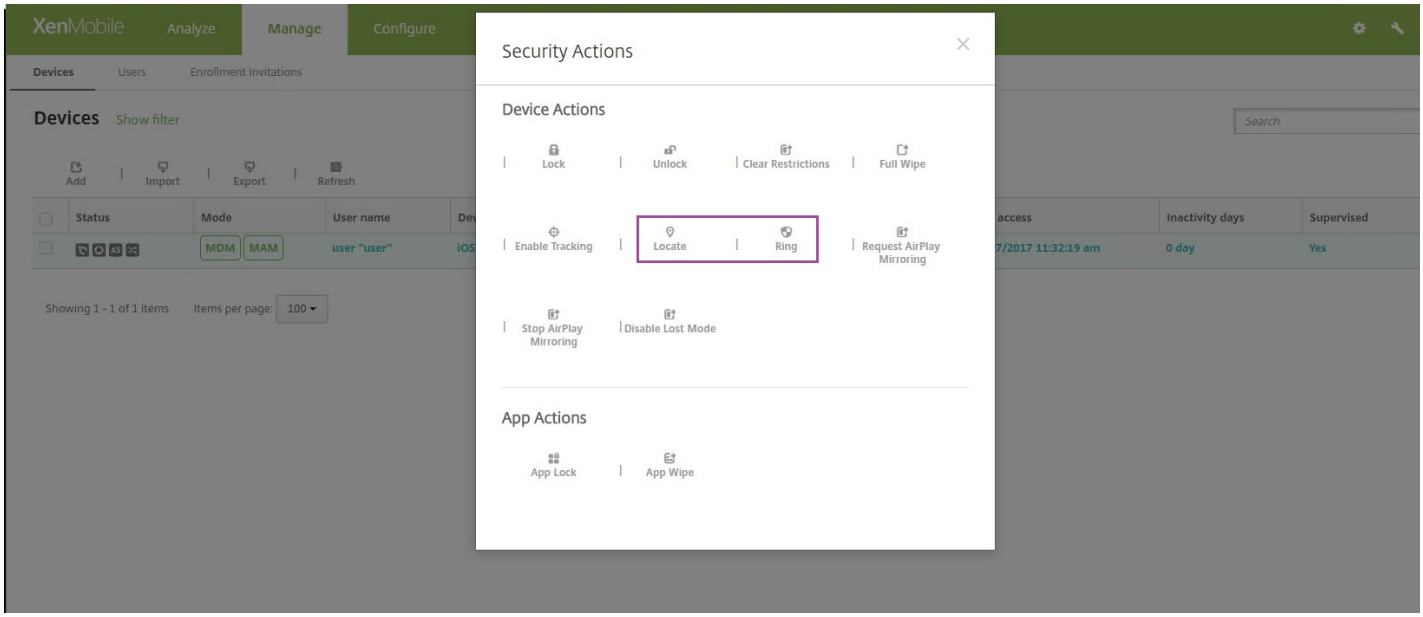
Um dispositivo é reiniciado imediatamente quando recebe o comando **Reiniciar**. Os dispositivos iOS bloqueados por senha não reingressam às redes Wi-Fi após o reinício, portanto, poderão não se comunicar com o servidor. Um dispositivo é desligado imediatamente quando recebe o comando **Desligar**.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Localizar ou chamar um dispositivo iOS supervisionado que está no modo perdido

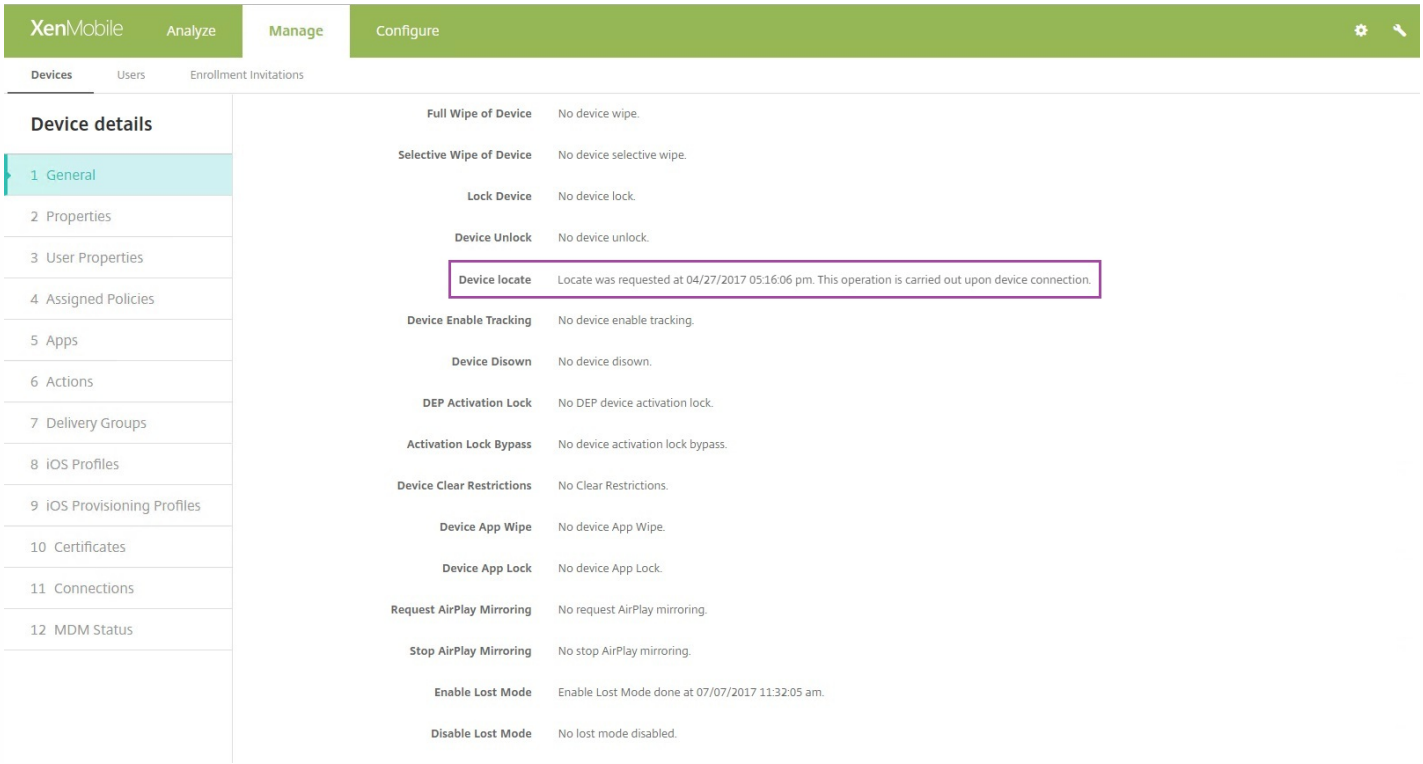
Depois de colocar um dispositivo iOS supervisionado no modo perdido, você pode usar ações de segurança para localizar ou fazer tocar o dispositivo. Um "toque" é o som do modo perdido que a Apple define para o dispositivo.



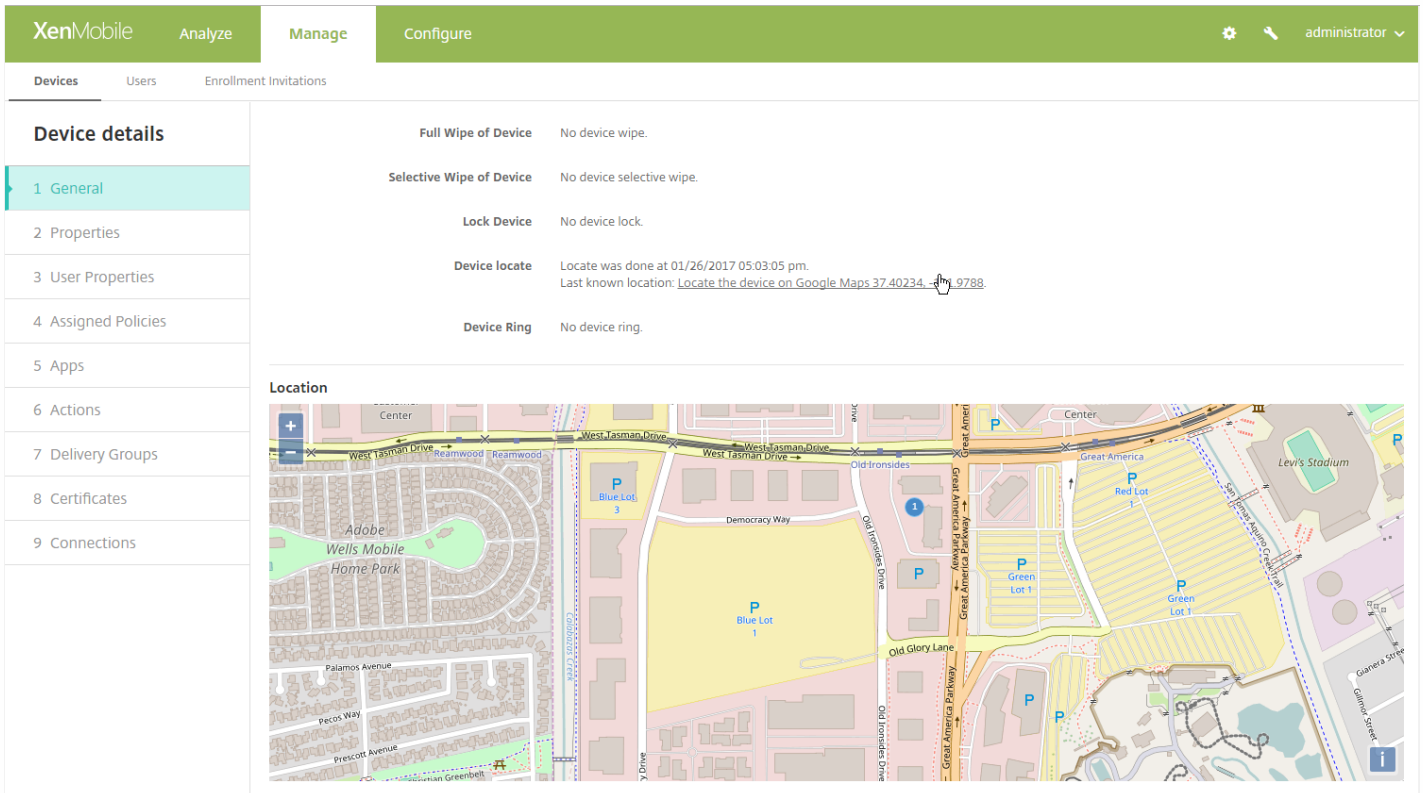
- Para localizar um dispositivo que está no modo perdido:

  Acesse **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Segurança** e em **Localizar**. A página **Detalhes do dispositivo** fornece um status da solicitação de localização.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Se o dispositivo estiver localizado, a página **Detalhes do dispositivo** inclui um mapa.



- Para chamar um dispositivo que está no modo perdido (versão mínima iOS 10.3):

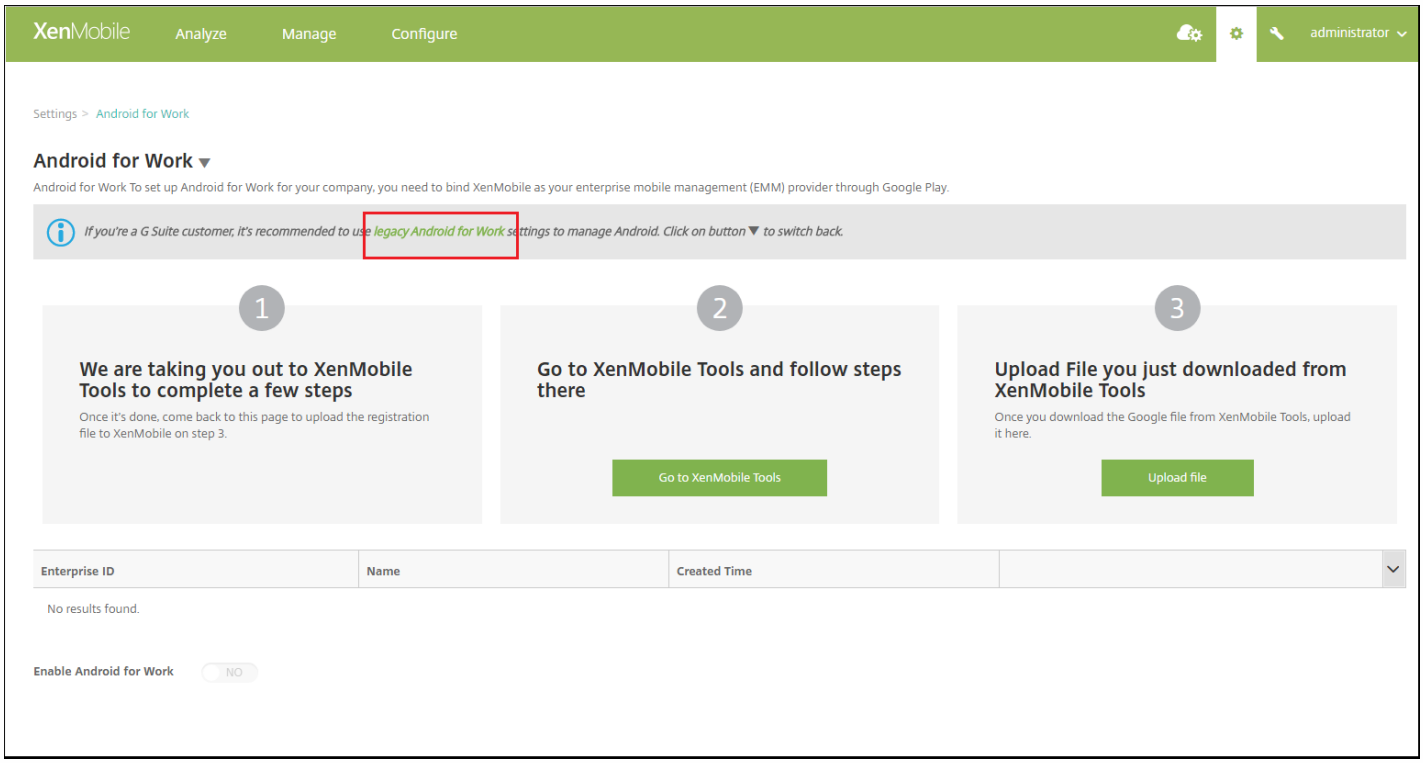
  Acesse **Gerenciar > Dispositivos**, selecione o dispositivo, clique em **Segurança** e em **Tocar**. Na próxima vez em que o dispositivo se conecta, ele toca. Para interromper a chamada, o usuário clica no botão de alimentação. Para parar o toque do console XenMobile, use a ação de segurança **Desativar o Modo Perdido**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Suporte aprimorado do Android for Work

O XenMobile agora fornece uma maneira simples de configurar o Android for Work para sua organização. Usando as Ferramentas de Gerenciamento do XenMobile, você vincula o XenMobile como seu provedor de gerenciamento de mobilidade empresarial através do Google Play e cria uma empresa para o Android for Work.

> ## Nota
>
> Os clientes do G Suite usam o legado de configurações do Android for Work para configurar o legado do Android for Work, como descrito no artigo Android for Work. Clique em **Android for Work legado** na página **Android for Work** nas configurações do XenMobile.



Você precisa:

- Suas credenciais de conta da Citrix para fazer logon no XenMobile Tools
- Suas credenciais corporativas de ID do Google para fazer login no Google Play

Para obter mais informações, consulte Android for Work.

Suporte de atestado de integridade de dispositivo (DHA) no local

Agora você pode ativar o atestado de integridade de dispositivo (DHA, Device Health Attestation) para dispositivos móveis

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Windows 10 por meio de um servidor do Windows no local. Anteriormente, o DHA para XenMobile podia ser habilitado somente através do Microsoft Cloud.

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.
Para configurar um DHA, você precisa de uma máquina executando o Windows Server 2016 Technical Preview 5 ou posterior. Você instala o DHA como uma função de servidor. Para obter instruções, consulte este artigo do Microsoft TechNet, Atestado de integridade de dispositivo.

Para a política do XenMobile Server habilitar o serviço DHA local:

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página Políticas de dispositivo é exibida.

2. Se você já criou uma política para habilitar o DHA através do Microsoft Cloud, vá para a etapa 8.

3. Clique em **Adicionar** para adicionar uma nova política. É exibida a caixa de diálogo **Adicionar uma nova política**.

4. Clique em **Mais** e, em **Personalizado**, clique em **Política de atestado de integridade de dispositivo**. A página de informações sobre a **Política de atestado de integridade de dispositivo** é exibida.

5. No painel Informações sobre a política, insira as seguintes informações:

   Nome da política: digite um nome descritivo para a política.

   Descrição: digite uma descrição opcional para a política.

6. Clique em **Avançar**. A página Plataforma de política é exibida.

7. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

8. Para cada plataforma escolhida:

   a. Defina **Ativar atestado de integridade do dispositivo** como **ON**.

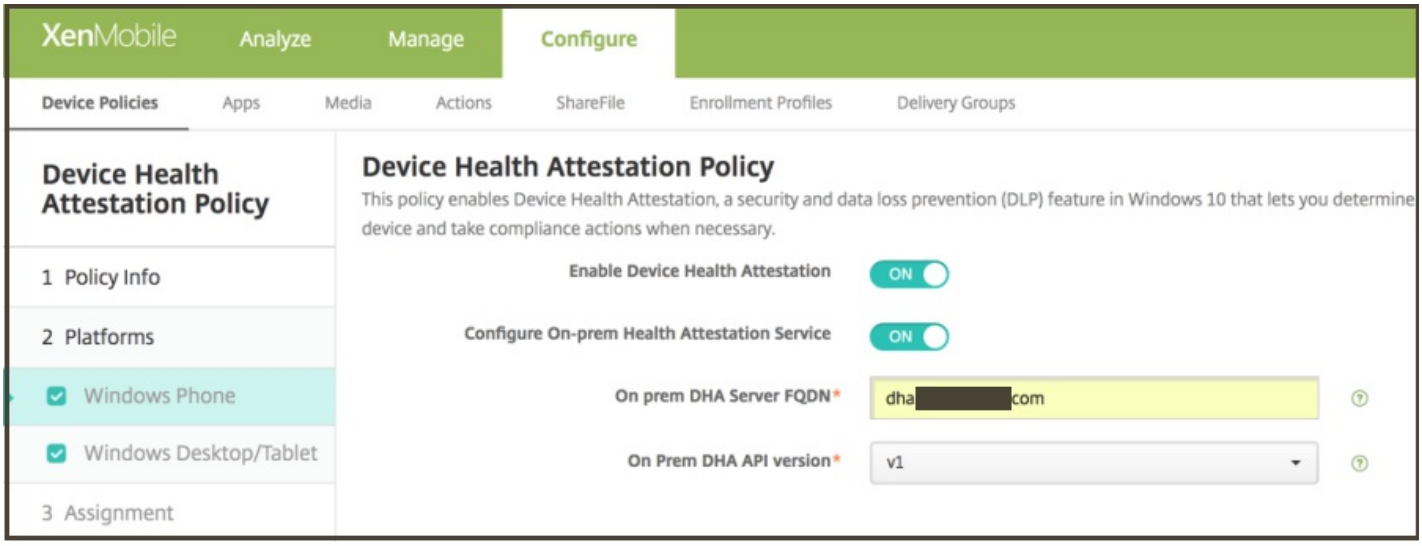
   b. Defina **Configurar o atestado de integridade de dispositivo local** como **ON**.

   c. Em **FQDN do Serviço DHA no local**, insira o nome de domínio totalmente qualificado do servidor DHA que você configurou.

   d. Em **Versão da API DHA local**, escolha a versão do serviço DHA instalado no servidor DHA.

9. Configure regras de implantação e escolha grupos de entrega.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Para confirmar que a política foi envia para um dispositivo Windows 10 Mobile:
1. No console XenMobile, clique em Gerenciar > Dispositivos.

2. Selecione o dispositivo.

3. Selecione **Propriedades**.

4. Role até "Atestado de integridade de dispositivo Windows".

Mais macros para modelos de registro

Você pode usar essas novas macros ao criar modelos de registro para convites de registro do dispositivo:

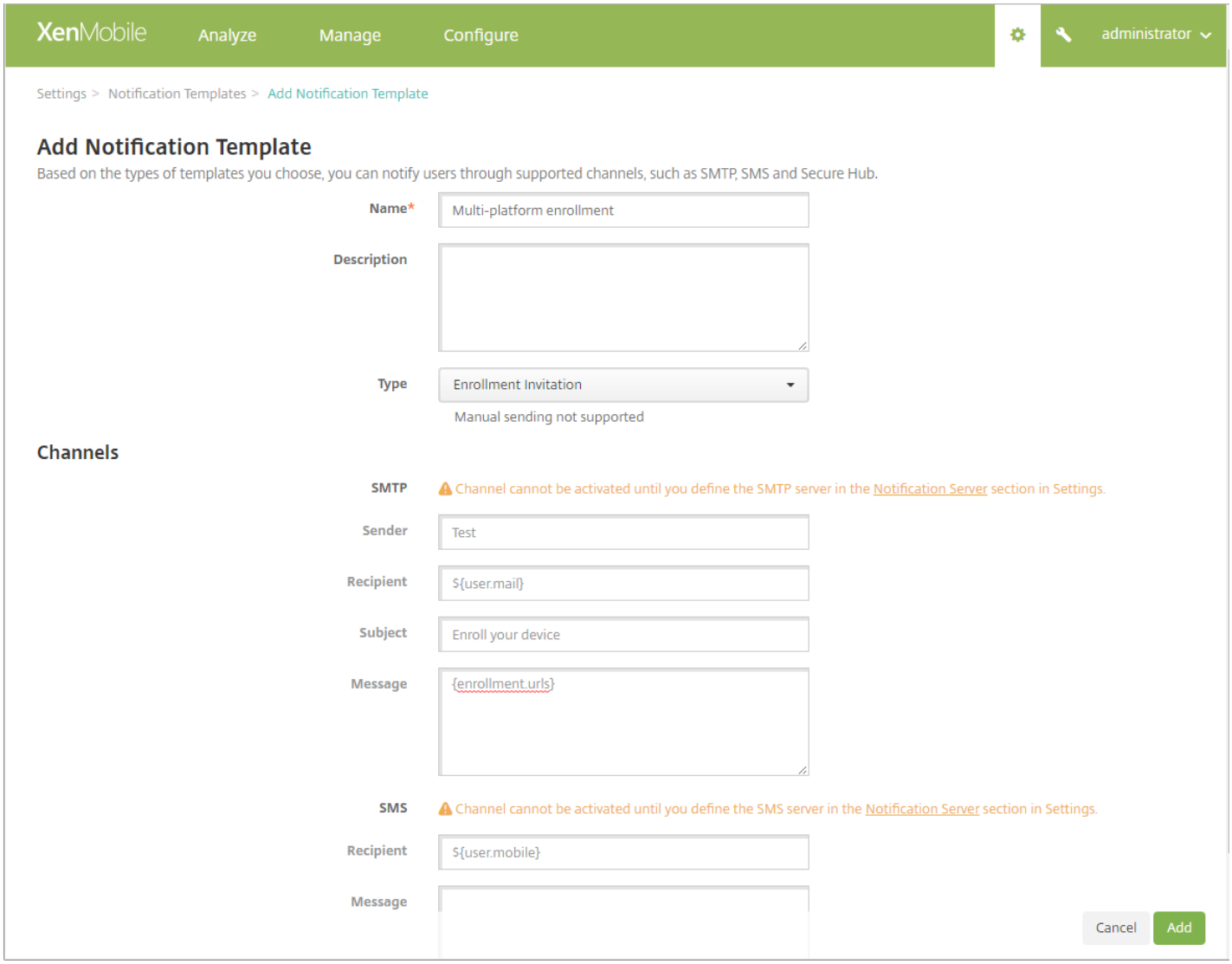
${enrollment.urls}
${enrollment.ios.url}
${enrollment.macos.url}
${enrollment.android.url}
${enrollment.ios.platform}
${enrollment.macos.platform}
${enrollment.android.platform}
${enrollment.agent}

Essas macros permitem que você crie modelos de registro que contêm URLs de registro para várias plataformas de dispositivos.

Este exemplo mostra como criar uma notificação que inclui URLs de registro para várias plataformas de dispositivo. A macro para a **Mensagem** é:

${enrollment.urls}

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Esses exemplos mostram como criar mensagens para notificações que levam os usuários a clicar na URL de registro para as plataformas de seus dispositivos:

Exemplo 1:

Para se registrar, clique no link abaixo que se aplica à plataforma do seu dispositivo:

${enrollment.ios.platform} - ${enrollment.ios.url}

${enrollment.macos.platform} - ${enrollment.macos.url}

${enrollment.android.platform} - ${enrollment.android.url}

Exemplo 2:

Para registrar um dispositivo iOS, clique no link ${enrollment.ios.url}.

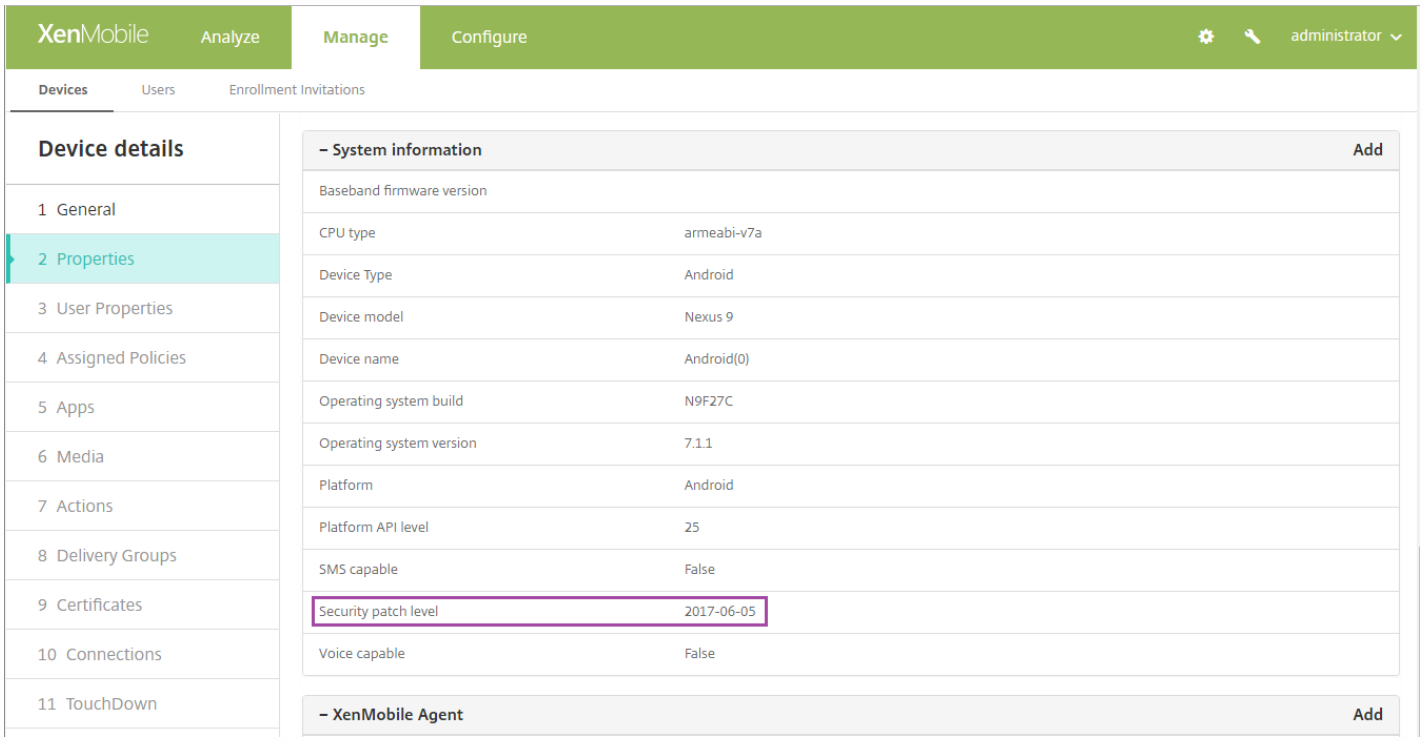
Para registrar um dispositivo macOS, clique no link ${enrollment.macos.url}.

Para registrar um dispositivo Android, clique no link ${enrollment.android.url}.

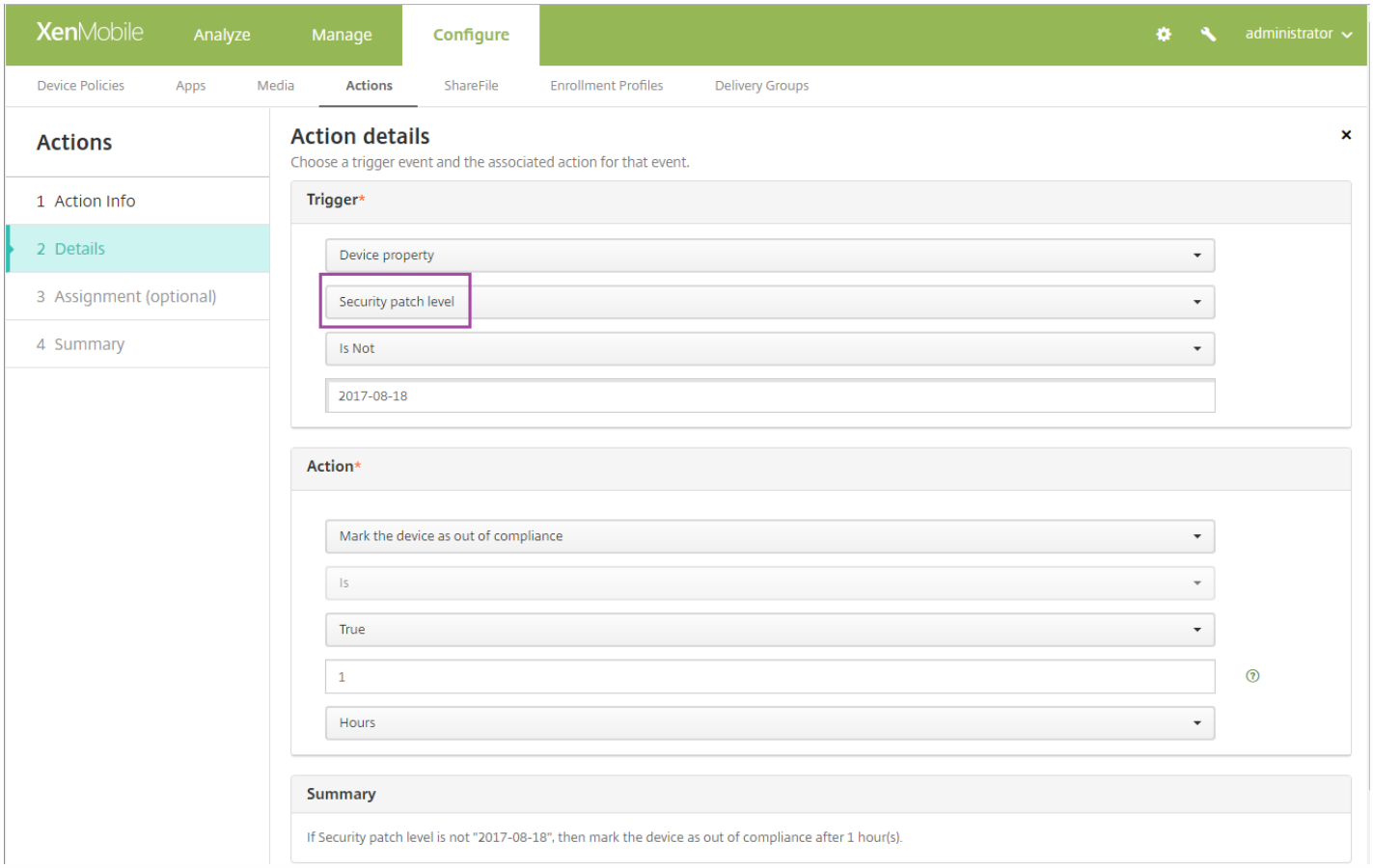
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Outras melhorias

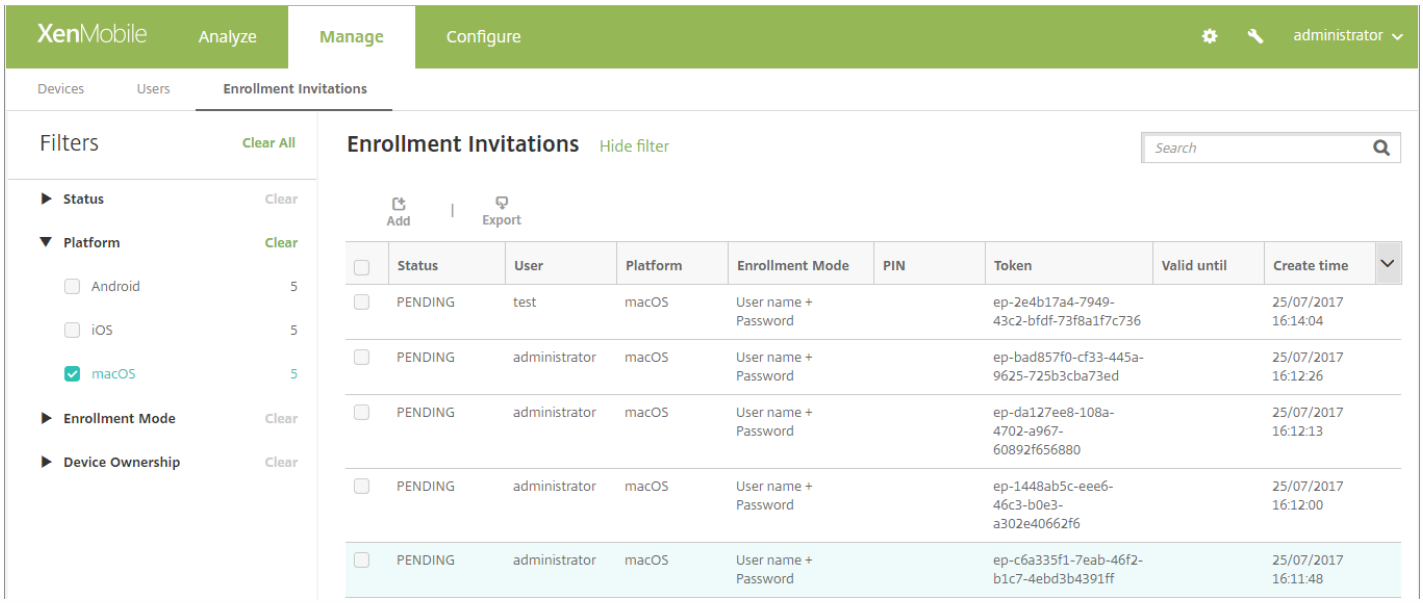
- O console XenMobile e o Portal de Ajuda automática estão agora disponíveis em espanhol.
- **XenMobile agora relata o nível de patch de segurança para dispositivos Android**. Você pode visualizar o **nível de patch de segurança** na página **Gerenciar > Dispositivos** e em **Detalhes do dispositivo**. Você também pode usar **Configurar > Ações** para criar uma ação que o nível de patch de segurança dispara.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

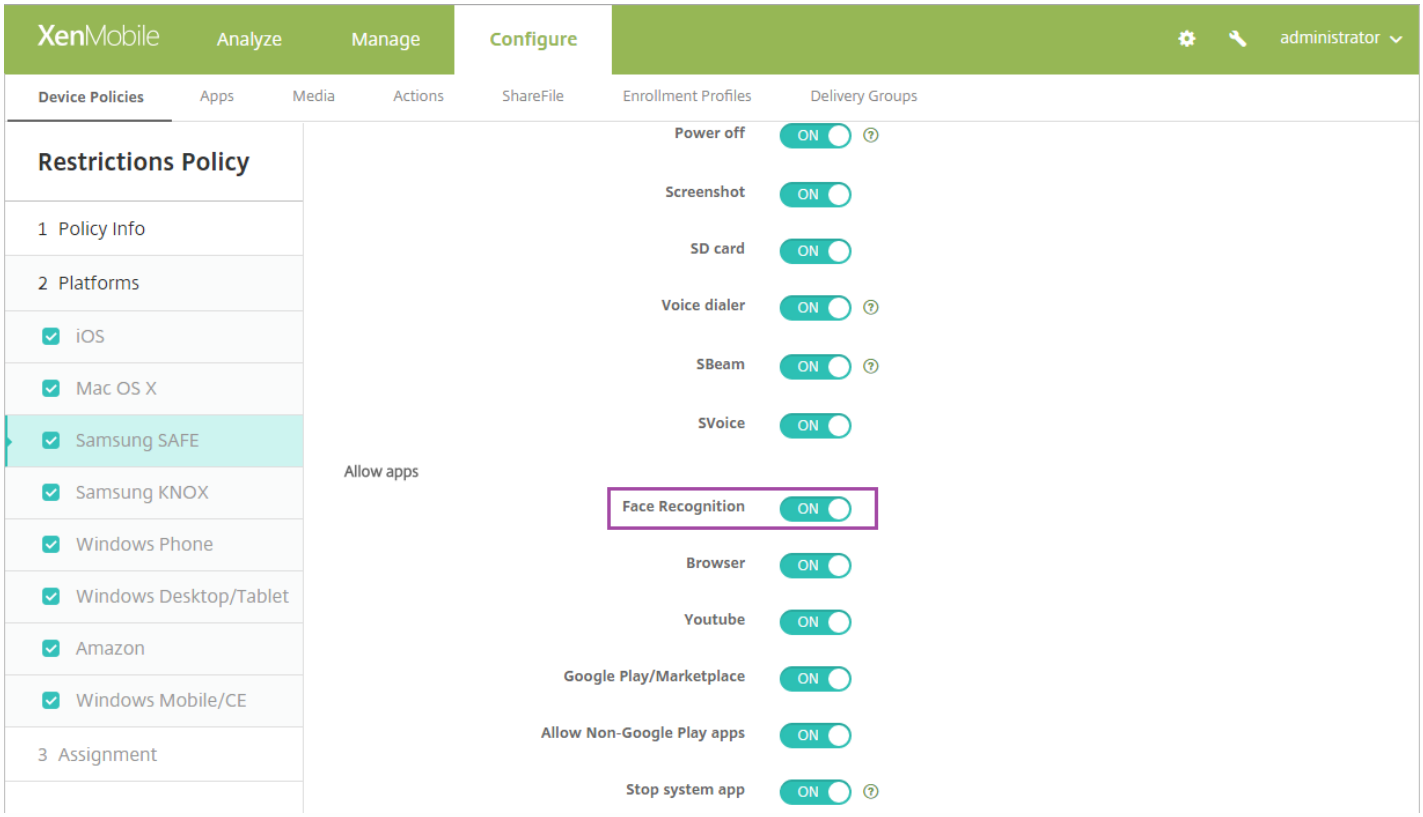


- **Filtrar convites de registro por macOS**. O filtro de plataforma de **Gerenciar > Convites para registro** agora inclui **macOS**.



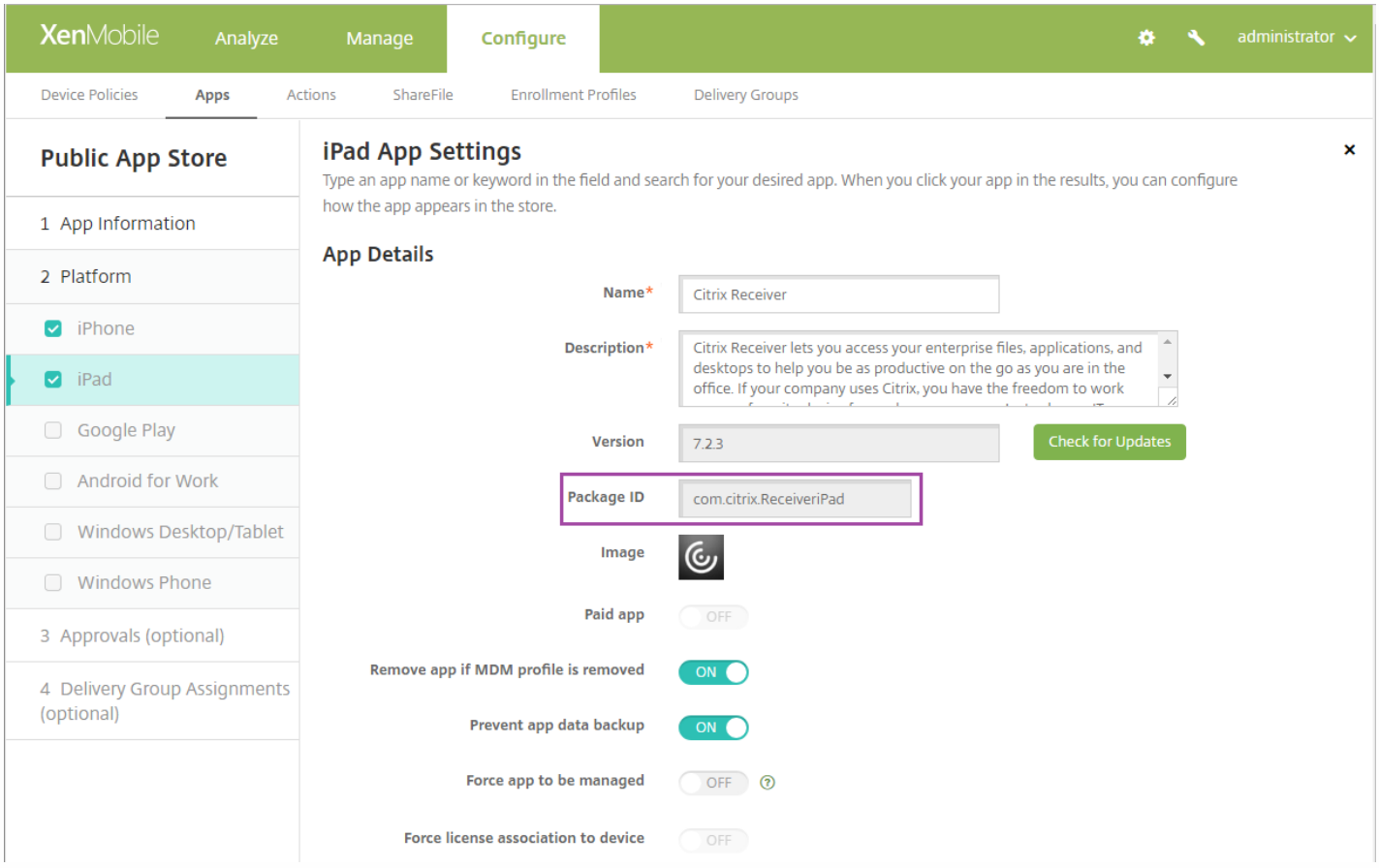
- **Configuração de política de Restrições para impedir que os usuários usem reconhecimento de rosto para desbloquear dispositivos Samsung Galaxy S8+**. A política de dispositivo de Restrições para Samsung SAFE agora inclui a configuração de **Reconhecimento de rosto**. Para bloquear o uso do reconhecimento de rosto para desbloquear o acesso ao dispositivo, vá em **Configurar > Políticas do Dispositivo** e edite a política de Restrições para definir **Reconhecimento de Rosto** como **Desativado**.

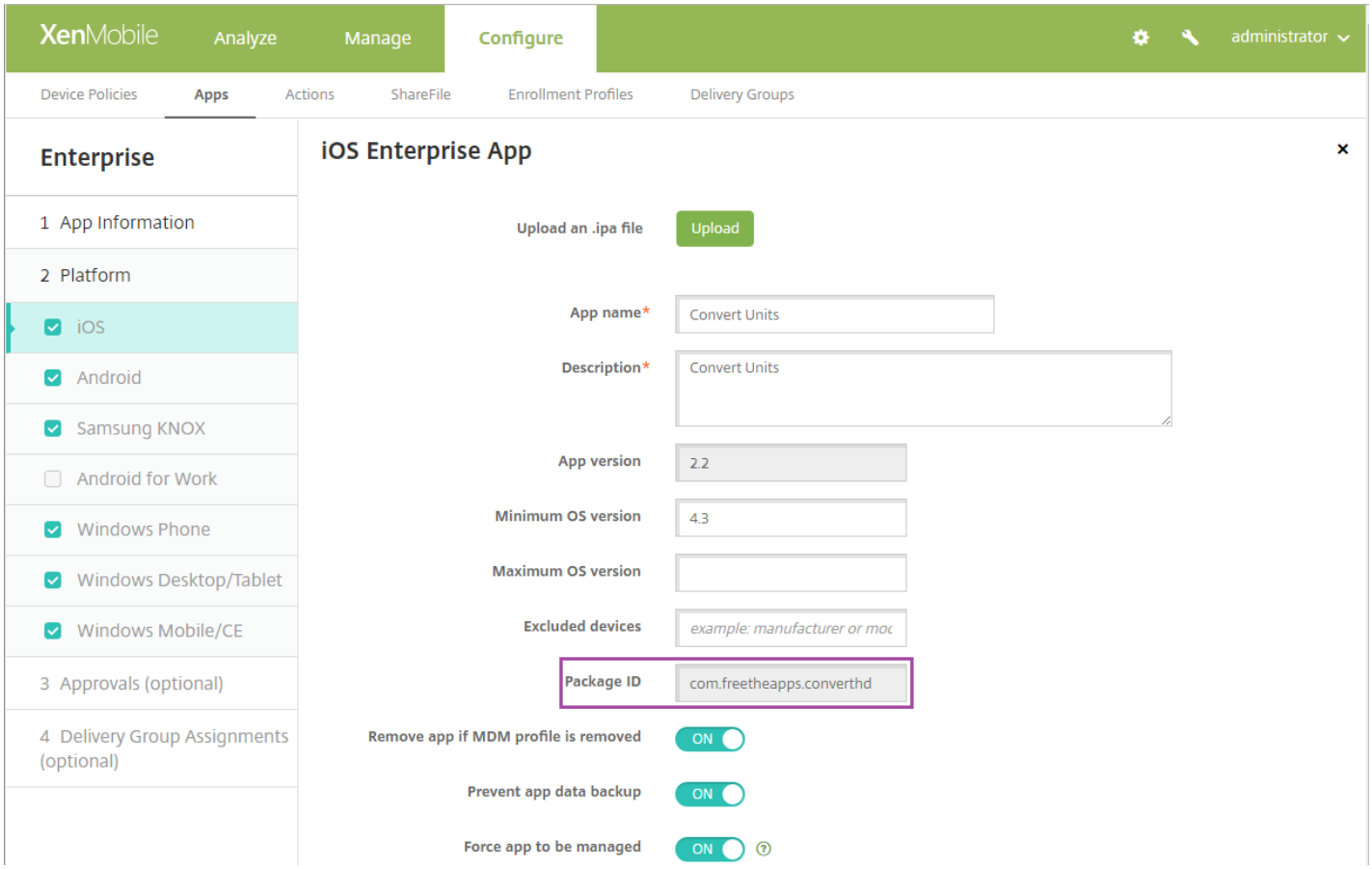
© 1999-2017 Citrix Systems, Inc. All rights reserved.



- **Os aplicativos macOS VPP necessários agora são suportados**. Agora você pode implantar aplicativos VPP do macOS como aplicativos necessários para usuários locais e Active Directory. Você pode visualizar os aplicativos VPP do macOS em **Configurar > Aplicativos**, onde pode filtrar os aplicativos por macOS VPP. Nessa página, a seção **Configuração da loja** não aparece para os aplicativos macOS VPP porque não existe um Secure Hub para macOS. Em **Gerenciar > Dispositivos**, as **Propriedades do Usuário** incluem Desativar conta VPP para as contas do macOS VPP.
- **Configurar > Aplicativos agora mostra o ID do pacote para aplicativos da loja de aplicativos pública e aplicativos empresariais**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

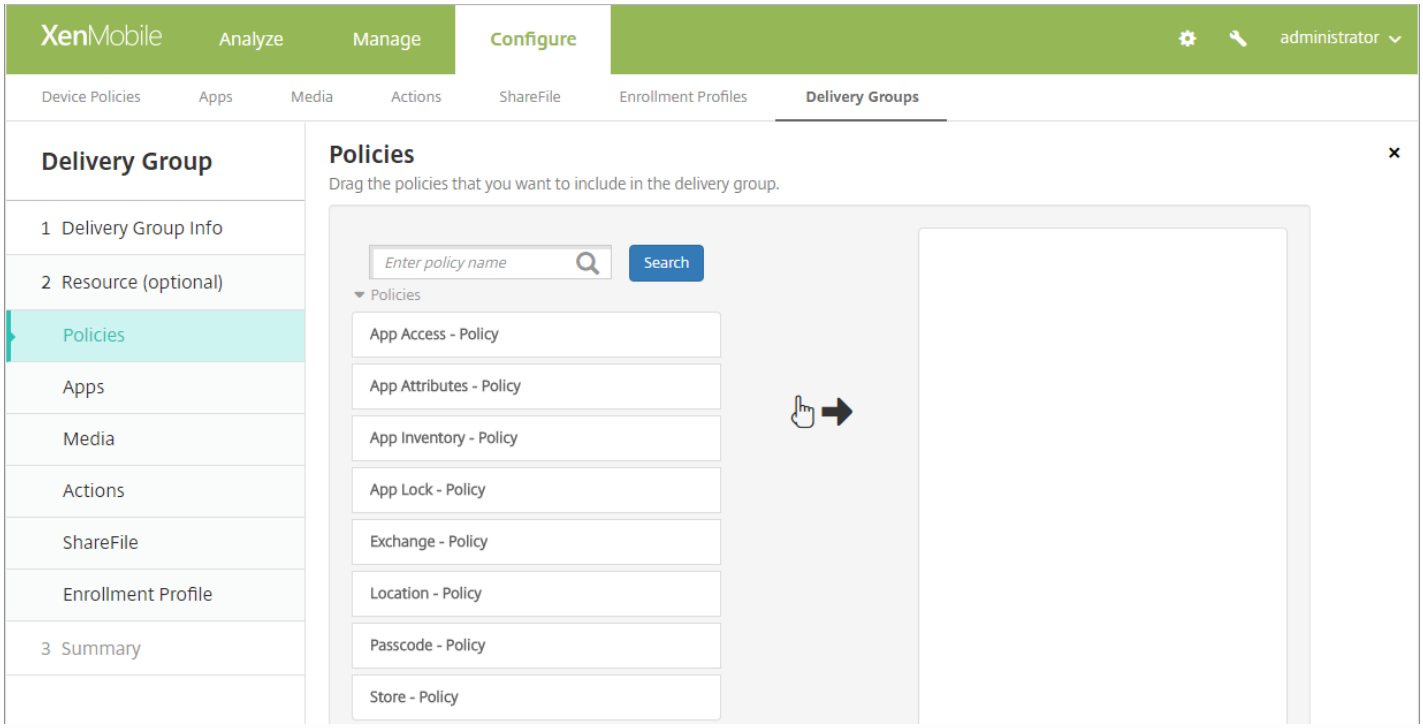


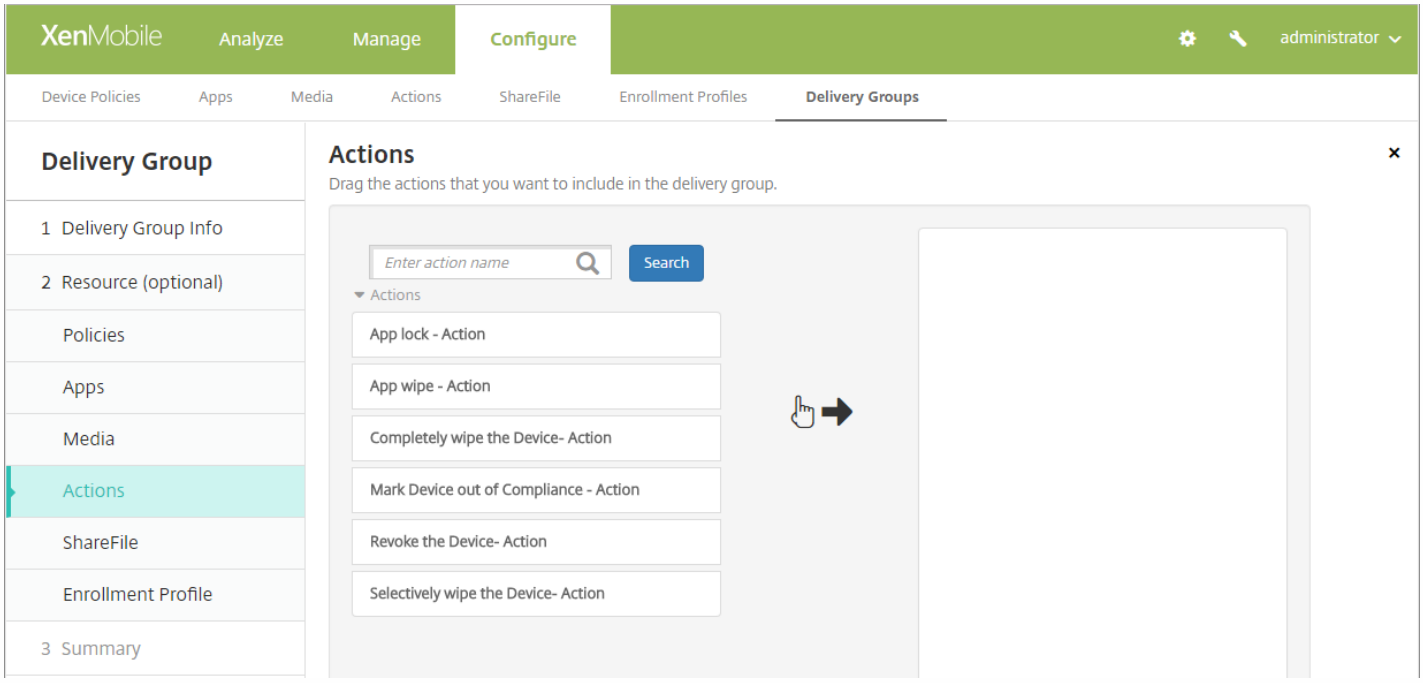


- **Lista de recursos em ordem alfabética para grupos de entrega.** Em **Configurar > Grupos de entrega**, todas as

© 1999-2017 Citrix Systems, Inc. All rights reserved.

listas de recursos e os resultados da pesquisa são exibidos em ordem alfabética.



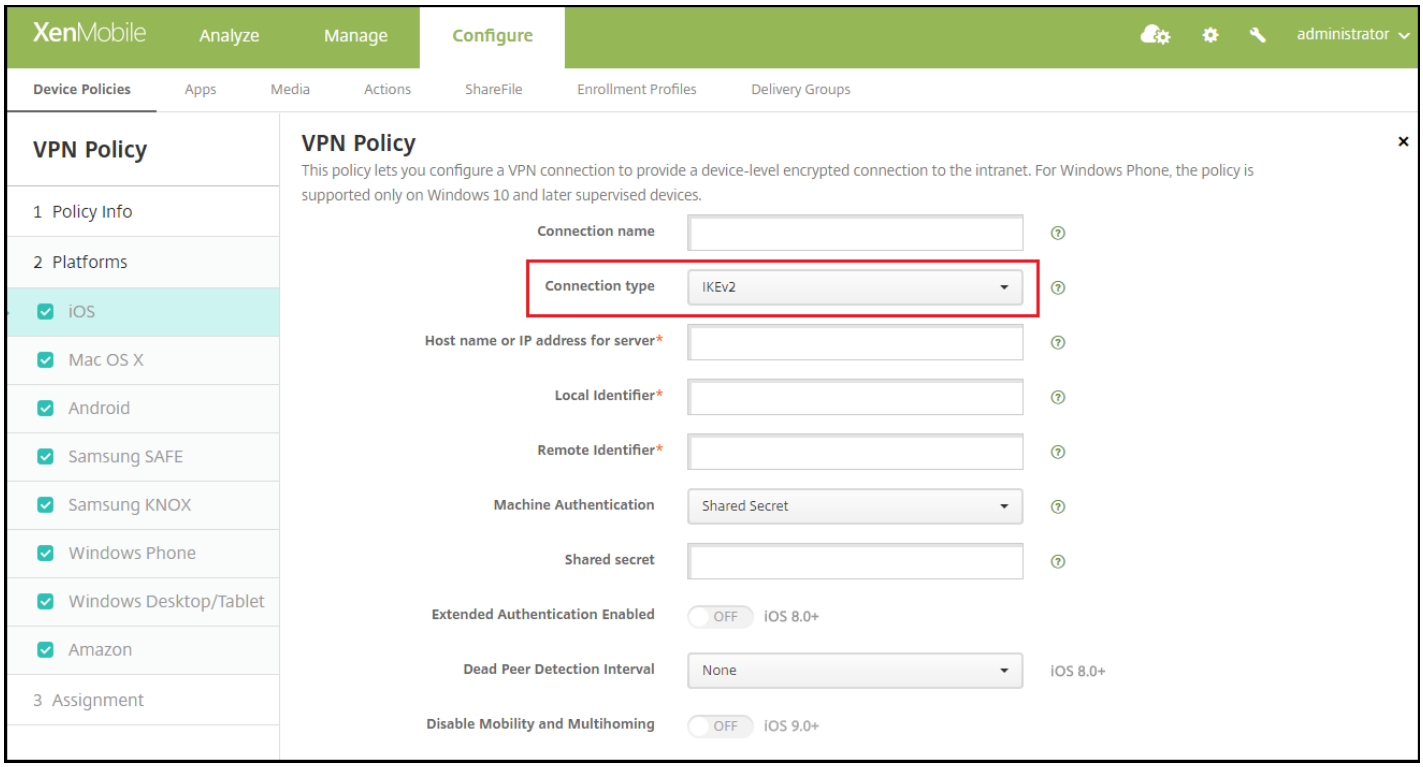


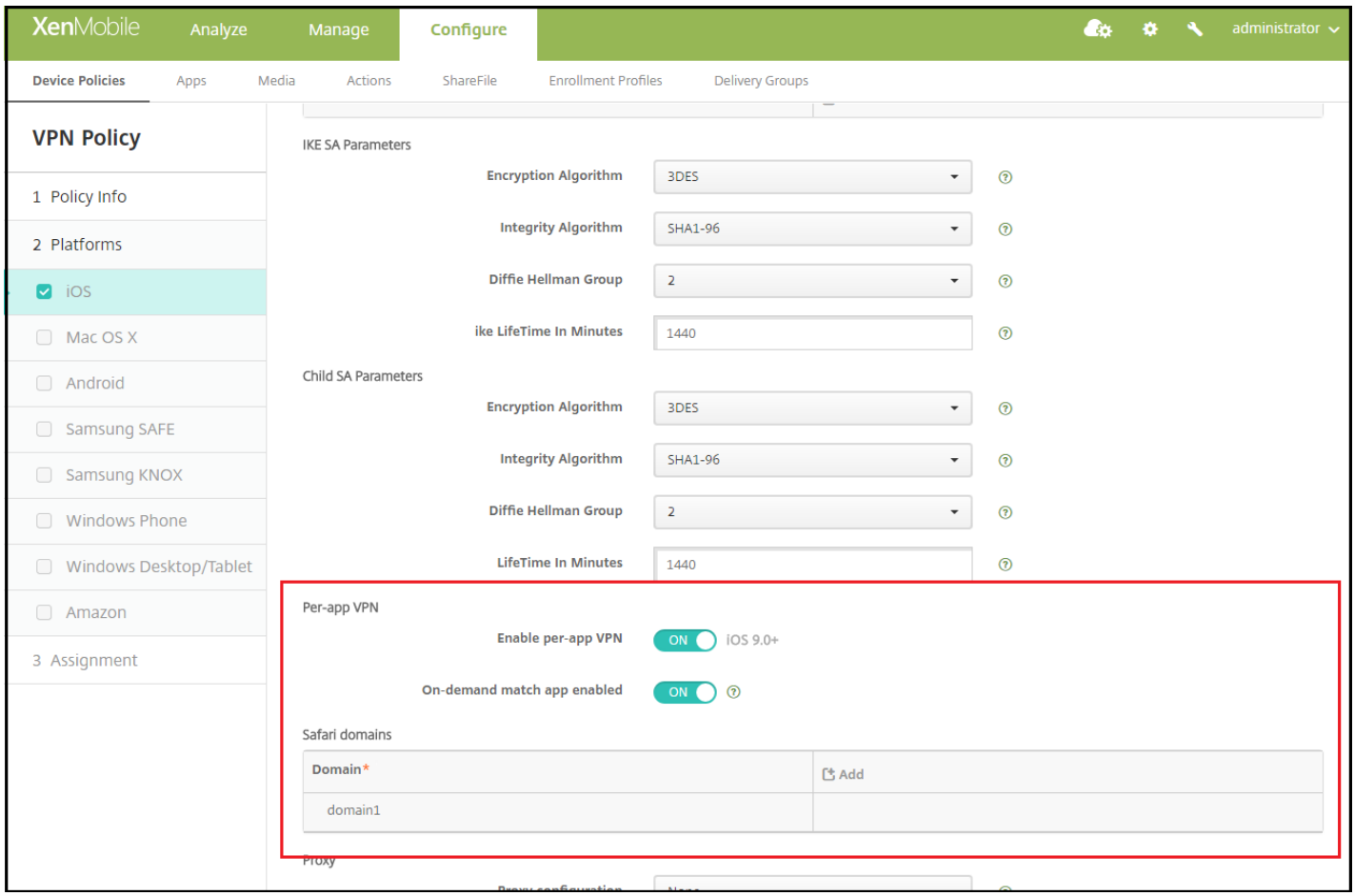
- Nas páginas **Gerenciar > Dispositivos** e **Gerenciar > Usuários**, as datas agora aparecem no formato de 24 horas, dd/mm/aaaa hh:mm:ss. As datas refletem o fuso horário local para usuários e dispositivos.

- **A política de VPN para dispositivos iOS agora oferece uma opção de VPN por aplicativo para políticas de VPN de tipo iKEv2**. Os dispositivos iOS 9.0 e posteriores suportam VPN por aplicativo para conexões iKEv2. As opções de **Ativar VPN por aplicativo** da VPN por aplicativo são:

  Ativar VPN por aplicativo
  Correspondência de aplicativo sob demanda ativada
  Domínios do Safari

© 1999-2017 Citrix Systems, Inc. All rights reserved.





Na seção "iOS", adicione à seção de tipo de conexão iKEv2:

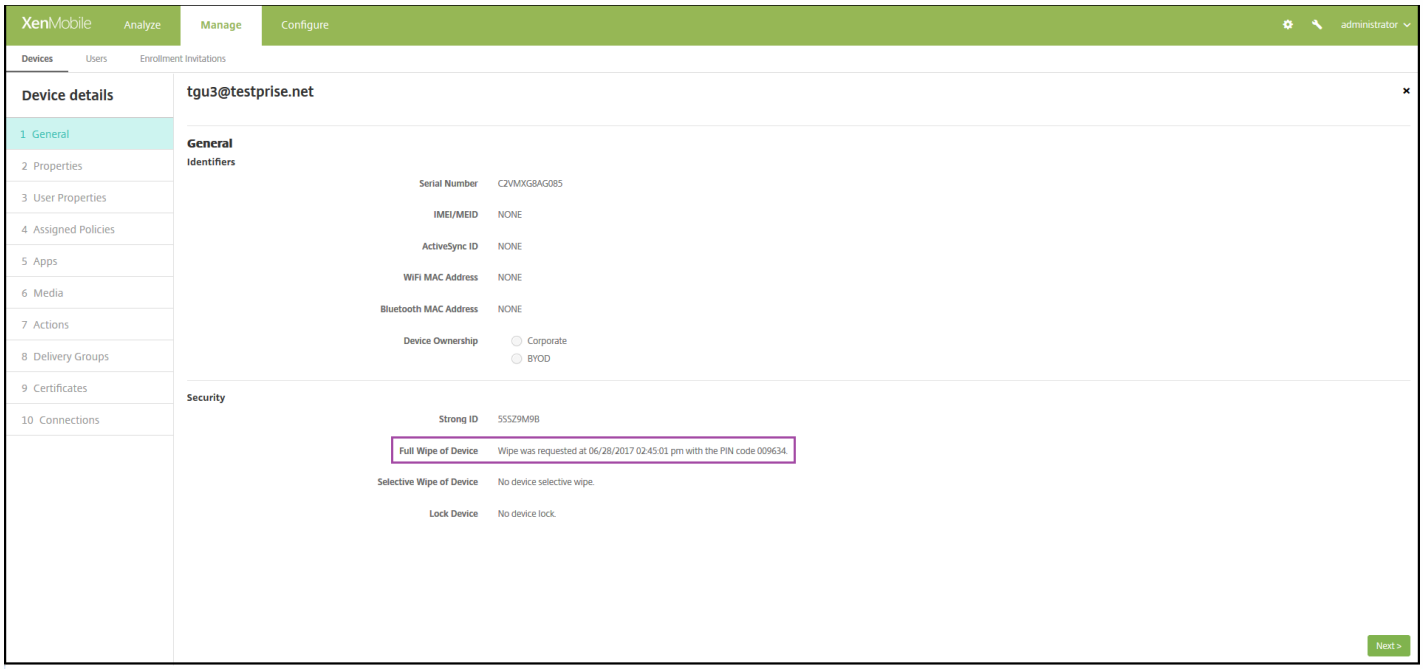
Ativar VPN por aplicativo: selecione se a VPN por aplicativo deve ser ativada. O padrão é **O**. Disponível apenas no iOS 9.0 e versões posteriores.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 **O**.

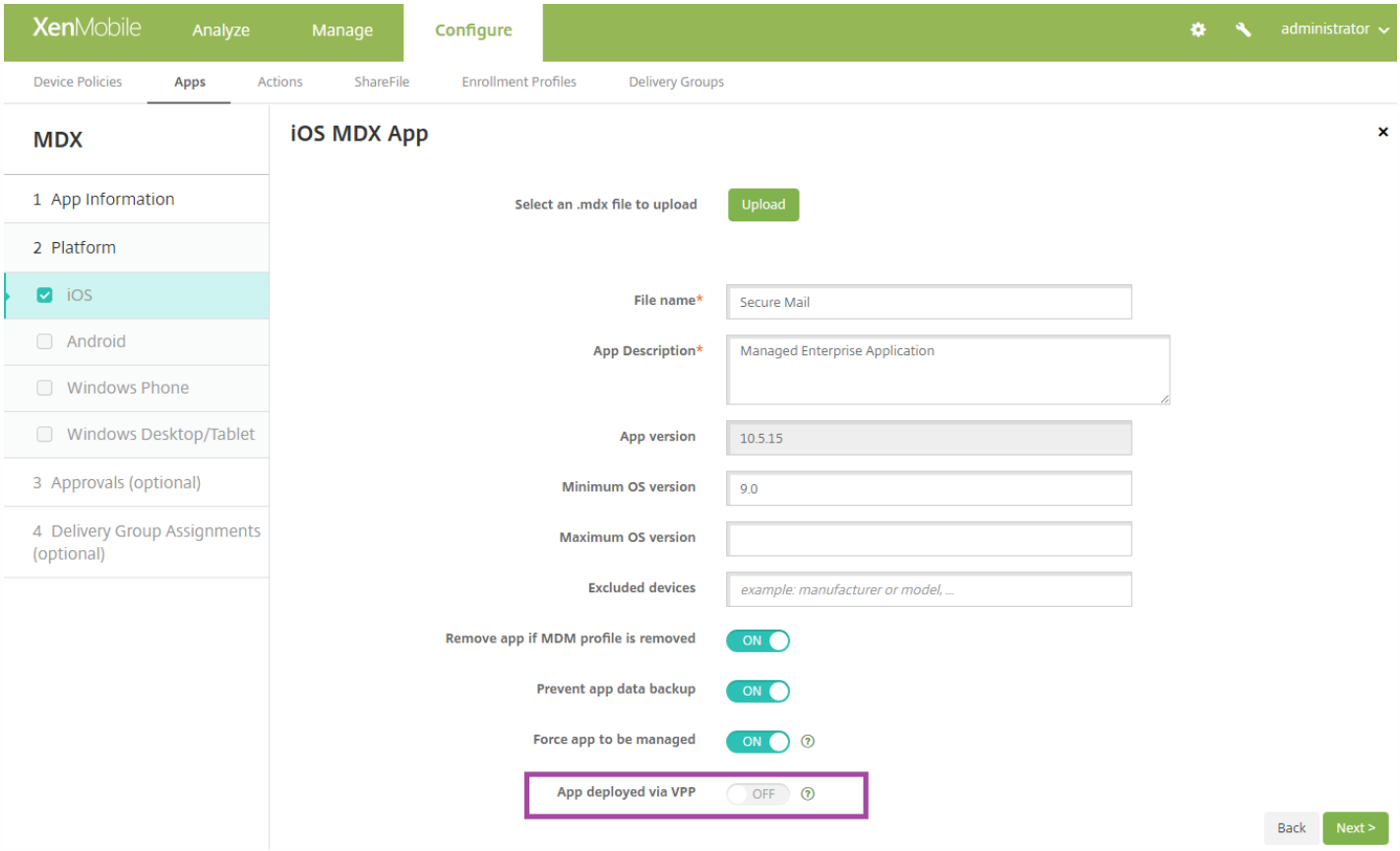
Domínios Safari: clique em **Adicionar** para adicionar um nome de domínio do Safari.

- **Limpe o código para dispositivos macOS mostrados no console XenMobile.** Os dispositivos macOS exigem que o usuário insira um código PIN depois que o dispositivo foi apagado. Se o usuário não se lembrar deste código, agora você pode procurar o código de limpeza na página de detalhes **Gerenciar > Dispositivo**.

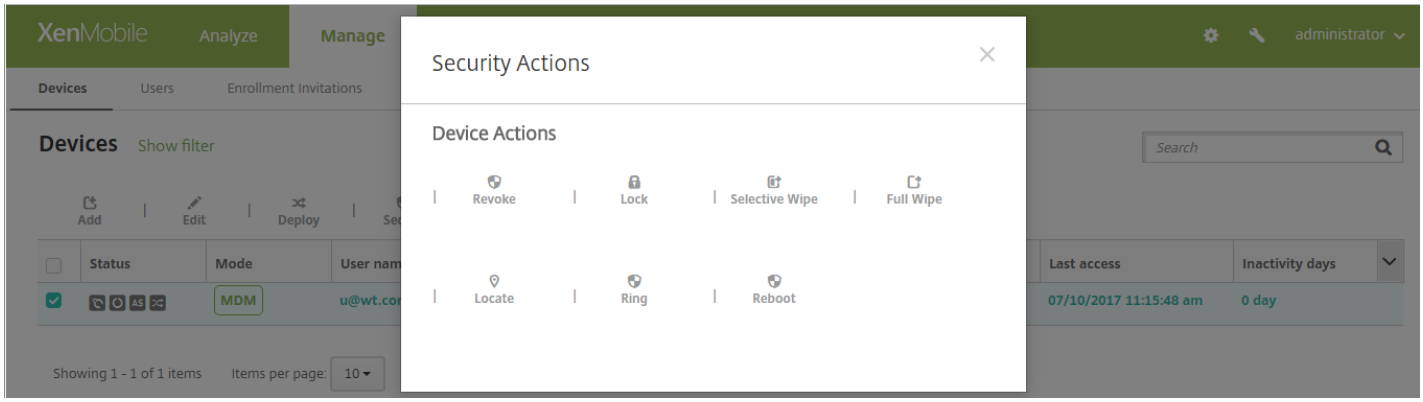


- **Quando você usa o VPP para implantar um aplicativo MDX, a loja do Secure Hub agora mostra apenas a instância VPP do aplicativo**. Anteriormente, aplicativos VPP e MDX eram exibidos na loja. Essa alteração impede que os usuários finais instalem a versão MDX do aplicativo, o que exige que o usuário tenha uma conta do iTunes. Quando você adiciona um aplicativo MDX, há uma nova configuração, **Aplicativo implantado via VPP**. Altere essa configuração para **ON** se você planeja implantar o aplicativo usando VPP.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- **Melhor desempenho ao importar muitas licenças do VPP**. Essa otimização usa multithreading. Uma nova propriedade de XenMobile Server, **MaxNumberOfWorker**, usa o padrão **3** (threads). Se precisar de mais otimização, você pode aumentar o número de threads. No entanto, com um número maior de threads, como 6, uma importação VPP resulta em uso de CPU muito alto.
- No console XenMobile, todas as referências a Mac OS X, OS X, OSX, MACOSX e MacOS agora são macOS.
- **Reinicie um dispositivo Windows 10**. Agora você pode enviar uma ação de segurança, Reinicializar, para reinicializar um dispositivo. Em Windows Tablet e PCs, a mensagem "Sistema reinicializará em breve" aparece e a reinicialização ocorre em cinco minutos. No Windows Phone, não há mensagem de aviso para usuários, e a reinicialização ocorre após alguns poucos minutos.



Mudanças na API pública REST

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para os serviços REST de notificação de dispositivo, você agora pode notificar um dispositivo usando a ID de dispositivo, sem a necessidade de o XenMobile enviar um token.

Quando você usar a API REST pública do XenMobile para criar convites para registro, agora você pode:

- **Especificar um PIN personalizado**. Se o modo de registro exigir um PIN, você pode usar um PIN personalizado em vez de um gerado aleatoriamente pelo XenMobile Server. O tamanho do PIN deve coincidir com a configuração definida para o modo de registro. O tamanho do PIN padrão é 8. Por exemplo, uma solicitação pode incluir: "pin": "12345678"

- **Selecione várias plataformas**. Anteriormente, você podia usar a API REST para especificar apenas uma plataforma para um convite de registro. O campo "plataforma" é obsoleto e substituído por "plataformas". Por exemplo, uma solicitação pode incluir: "plataformas": ["iOS", "MACOSX"]

A API pública XenMobile para REST Services agora inclui as seguintes APIs:

- Obter por ID de contêiner
  - Aplicativos móveis MDX
  - Aplicativos móveis empresariais
  - Aplicativos WebLink
  - Aplicativos Web/SaaS
  - Aplicativos da loja pública
- Carregar o aplicativo em contêiner novo ou existente
  - Aplicativos móveis MDX
  - Aplicativos móveis empresariais
- Atualizar detalhes da plataforma dentro do contêiner para aplicativos móveis MDX e aplicativos da loja pública
- Adicionar ou atualizar aplicativo
  - Aplicativos WebLink
  - Aplicativos Web/SaaS
  - Aplicativos da loja pública
- Obter todos os conectores Web/SaaS ou obter conectores Web/Saas por nome do conector
- Excluir o contêiner de aplicativo
  - Aplicativos móveis MDX
  - Aplicativos móveis empresariais
  - Aplicativos WebLink
  - Aplicativos Web/SaaS

Para obter detalhes, consulte XenMobile Public API for REST Services.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Novidades no XenMobile Server 10.6

Feb 21, 2018

> ## Nota
>
> Para obter o conjunto completo da documentação do produto XenMobile Server 10.6, consulte o PDF.Esse PDF inclui informações sobre a atualização de versões anteriores do XenMobile Server.
>
> Para atualizações e correções ao PDF do XenMobile Server 10.6, consulte as erratas da documentação do XenMobile Server 10.6.

Para obter informações sobre como atualizar para a versão mais recente do XenMobile Server, consulte Atualização. Para acessar o console de gerenciamento do XenMobile, use somente o nome de domínio totalmente qualificado do XenMobile Server ou os endereços IP do nó.

O XenMobile Server 10.6 inclui os novos recursos e os problemas corrigidos a seguir.

> ## Important
>
> O Touchdown da Symantec atingiu o fim da vida útil em 3 de julho de 2017, com fim de suporte padrão, fim de suporte estendido e fim de suporte da vida útil em 2 de julho de 2018. Para obter mais informações, consulte o artigo de suporte da Symantec Aviso de Fim da vida, Fim de suporte e Fim da disponibilidade do Touchdown.

Implantação aprimorada dos aplicativos necessários

XenMobile agora instala aplicativos necessários com uniformidade e rapidez nos dispositivos Android e iOS gerenciados. Essa melhoria resolve os problemas de implantação que ocorreriam principalmente no caso do XenMobile configurado no modo empresarial (XME). Os usuários mais recebem atualizações com mais prontidão 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.

Requisitos

- XenMobile Server 10.6
- Secure Hub (versões mínimas: 10.5.15 para iOS; 10.5.20 para Android)
- MDX Toolkit 10.6
- Propriedade personalizada de servidor, force.server.push.required.apps.

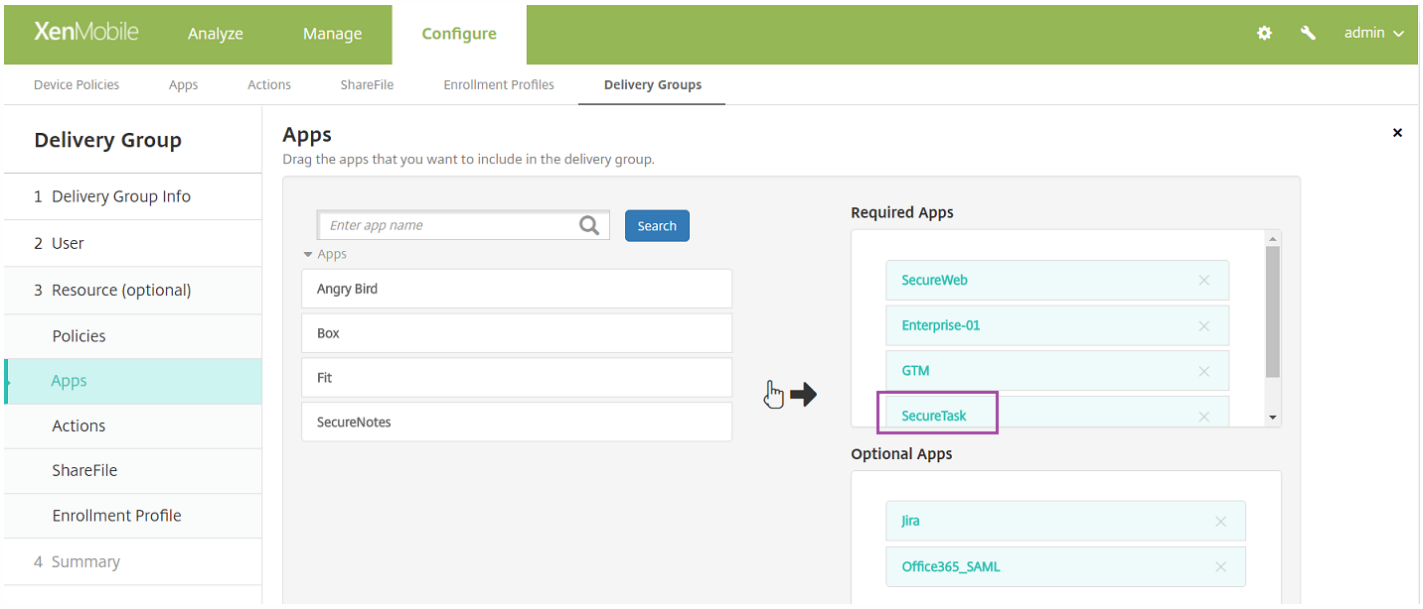
  A implantação forçada dos aplicativos necessários está desativada por padrão. Para ativar o recurso, crie uma propriedade personalizada de servidor principal. Defina a **Chave** e o **Nome de exibição** para **force.server.push.required.apps** e defina o **Valor** como **verdadeiro**.

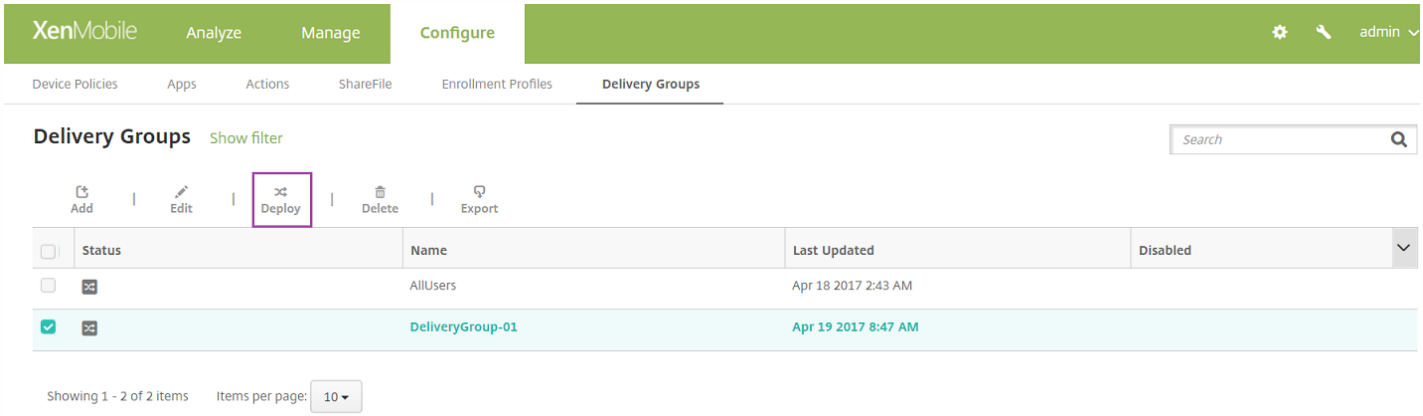
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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

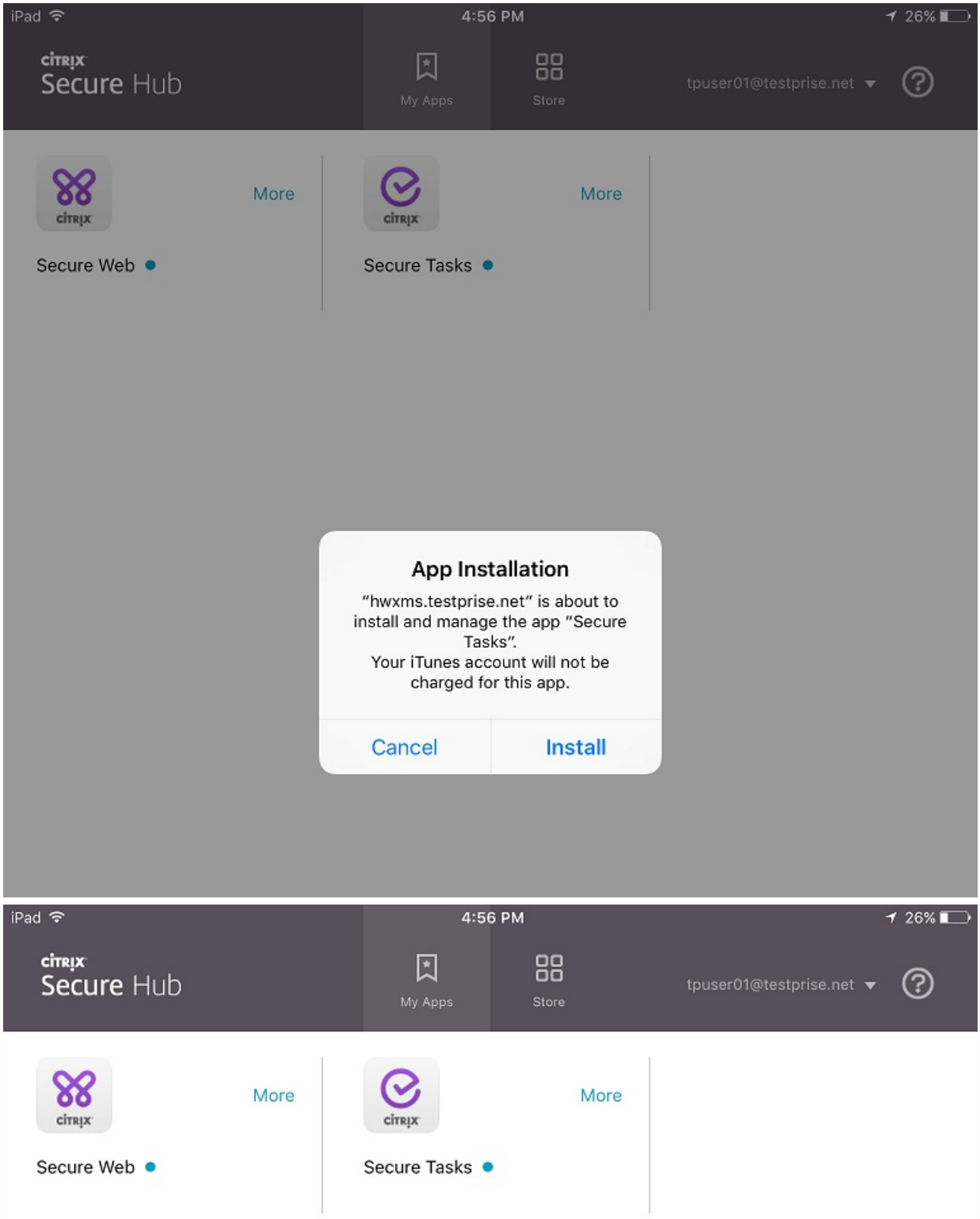
Os exemplos a seguir mostram a sequência de adicionar o aplicativo Secure Tasks a um grupo de entrega e, em seguida, implantar o grupo de entrega.





Depois que o aplicativo de exemplo, o Secure Tasks, implanta o dispositivo do usuário, o Secure Hub avisa ao usuário para instalar o aplicativo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Important

Os aplicativos necessários habilitados para MDX, incluindo aplicativos corporativos e aplicativos da loja de aplicativos pública, atualizam-se imediatamente, mesmo que você configure uma política MDX para um período de carência de atualização de aplicativo e o usuário opte por atualizar o aplicativo mais tarde.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

As tabelas a seguir descrevem o fluxo de trabalho de administrador e de usuário para aplicativos obrigatórios. As tabelas descrevem o comportamento em versões do servidor XenMobile anteriores à versão 10.6 em comparação com o comportamento na versão 10.6.

A primeira tabela descreve o fluxo de trabalho em dispositivos iOS. A segunda tabela descreve o fluxo de trabalho em dispositivos Android.

Fluxo de trabalho de aplicativo necessário em iOS

Enterprise apps		**Public app store apps**	
Versões anteriores	**A partir do XenMobile Server 10.6**	**Versões anteriores**	**A partir do XenMobile Server 10.6**
Implante o XenMobile App durante o registro inicial. O aplicativo necessário está instalado no dispositivo.	O mesmo.	Implante o XenMobile App durante o registro inicial. O aplicativo necessário está instalado no dispositivo.	O mesmo.
Atualize o aplicativo no console XenMobile.	O mesmo.	Atualize o aplicativo no console XenMobile.	O mesmo.
Abra a loja do Secure Hub no dispositivo. O ícone de atualização aparece na loja.	Clique em implantar no console XenMobile para implantar os aplicativos necessários.	Abra a loja do Secure Hub no dispositivo. O ícone de atualização aparece na loja	Clique em implantar no console XenMobile para implantar os aplicativos necessários.
O aplicativo na springboard é atualizado.	O aplicativo na springboard é atualizado.	O aplicativo na springboard é atualizado. A atualização é iniciada automaticamente. Os usuários não são solicitados a atualizar.	O aplicativo na springboard é atualizado. A atualização é iniciada automaticamente. Os usuários não são solicitados a atualizar.
Os usuários abrem o aplicativo na springboard. Os usuários são solicitados pelo aplicativo a atualizar em 7 dias.	Os usuários abrem o aplicativo na springboard. Os usuários são solicitados a atualizar em 7 dias. Na verdade, o aplicativo é atualizado mesmo quando os usuários clicam em Mais tarde.	Abra o aplicativo no dispositivo. O aplicativo está atualizado. Os usuários não são avisados após um período de tolerância.	O mesmo.
Os usuários clicam em Mais tarde, a atualização não é iniciada. Os usuários clicam em Atualizar agora, a atualização é iniciada.	O aplicativo está atualizado.	Os usuários clicam em Mais tarde, a atualização não é iniciada. Os usuários clicam em Atualizar agora, a atualização é iniciada.	O aplicativo está atualizado.

Fluxo de trabalho de aplicativo necessário em Android

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Enterprise apps		**Public app store apps**	
Versões anteriores	**A partir do XenMobile Server 10.6**	**Versões anteriores**	**A partir do XenMobile Server 10.6**
Implante o XenMobile App durante o registro inicial. O aplicativo necessário está instalado no dispositivo.	O mesmo.	O mesmo.	O mesmo.
Atualize o aplicativo no console XenMobile	Clique em implantar no console XenMobile para implantar os aplicativos necessários.	Atualize o aplicativo no console XenMobile	Atualize o aplicativo no console XenMobile
Abra a loja do Secure Hub no dispositivo. O ícone de atualização aparece na loja.	O aplicativo está atualizado. (Os dispositivos Nexus solicitam para instalar atualizações, mas dispositivos Samsung fazem uma instalação silenciosa).	Abra a loja do Secure Hub no dispositivo. O ícone de atualização aparece na loja.	Clique em **Implantar** ou entre na loja do Secure Hub no dispositivo. O ícone de atualização aparece na loja.
Nenhum aviso ou o atualização é exibida na springboard do dispositivo.	Os usuários abrem o aplicativo na springboard. Os usuários são solicitados a atualizar em 7 dias. Na verdade, o aplicativo é atualizado mesmo quando os usuários clicam em **Mais tarde**.	Os usuários devem clicar manualmente no ícone de atualização na loja do Secure Hub para atualizar. (O Nexus solicita que os usuários instalem atualizações.)	A atualização do aplicativo começa imediatamente. (Os dispositivos Nexus solicitam que os usuários instalem a atualização.)
Os usuários abrem o aplicativo na springboard. Os usuários são solicitados pelo aplicativo a atualizar em 7 dias.	O aplicativo está atualizado.	Abra o aplicativo na springboard. O aplicativo está atualizado. Os usuários não são avisados sobre um período de tolerância.	Abra o aplicativo na springboard. O aplicativo está atualizado. Os usuários não são avisados sobre um período de tolerância.
Os usuários clicam em **Mais tarde**, a atualização não é iniciada. Os usuários clicam em **Atualizar agora**, a atualização é iniciada. (Os usuários não são solicitados a instalar em dispositivos Samsung, mas o Nexus solicita uma atualização).	O aplicativo está atualizado. (Os dispositivos Samsung fazem uma instalação silenciosa.)	Os usuários clicam em **Mais tarde**, a atualização não é iniciada. Os usuários clicam em **Atualizar agora**. A atualização é iniciada.	O aplicativo é atualizado. (Os dispositivos Samsung fazem uma instalação silenciosa.)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurar um NetScaler Gateway local para uso com o XenMobile Server

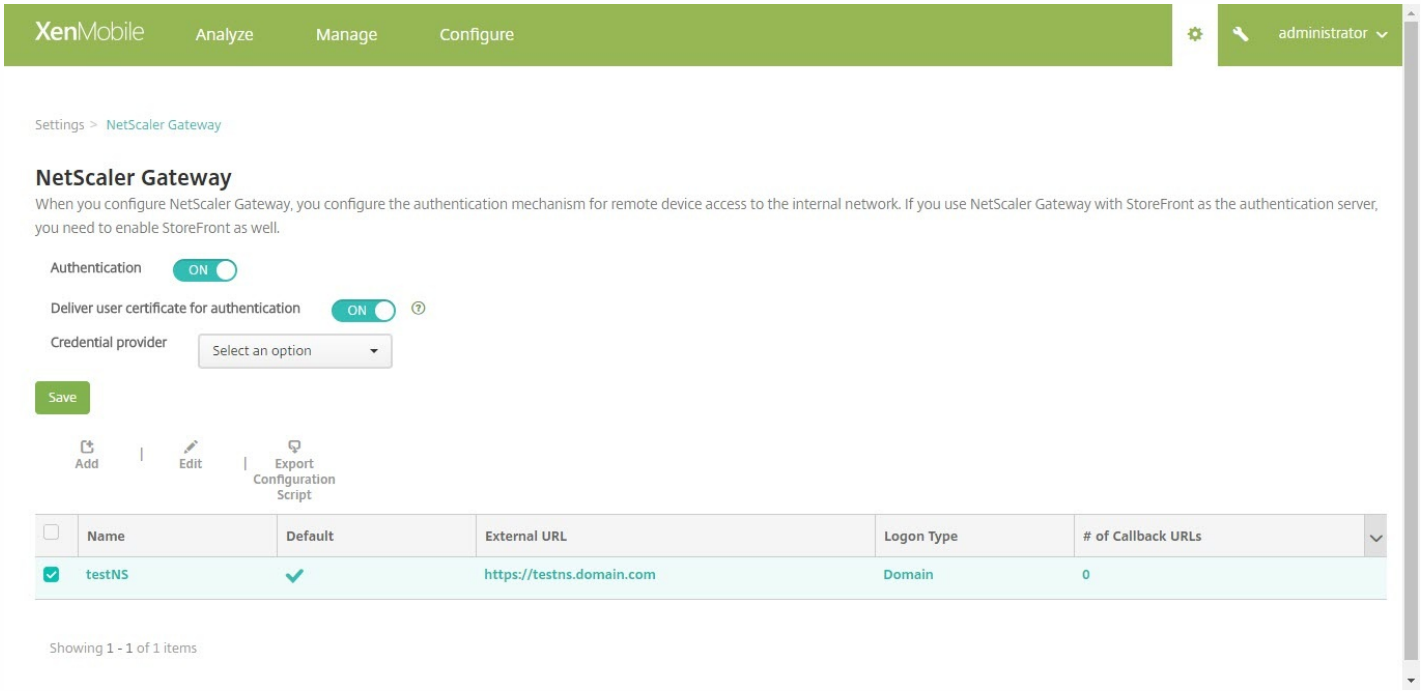
A partir do XenMobile 10.6, configure o NetScaler Gateway para uso com o XenMobile Server exportando um script do XenMobile que você executa no NetScaler Gateway. O script configura essas configurações do NetScaler Gateway exigidas pelo XenMobile:

- Servidores NetScaler Gateway necessários para MDM e MAM
- Políticas de sessão para os servidores virtuais do NetScaler Gateway
- Detalhes do XenMobile Server
- Políticas de autenticação e ações para o servidor virtual NSG.
  O script descreve as definições de configuração de LDAP.
- Ações e políticas de tráfego para o servidor proxy
- Perfil de acesso sem cliente
- Registro de DNS local estático no NetScaler
- Outras associações: política de serviço, certificado de CA

O script não manipula a seguinte configuração:

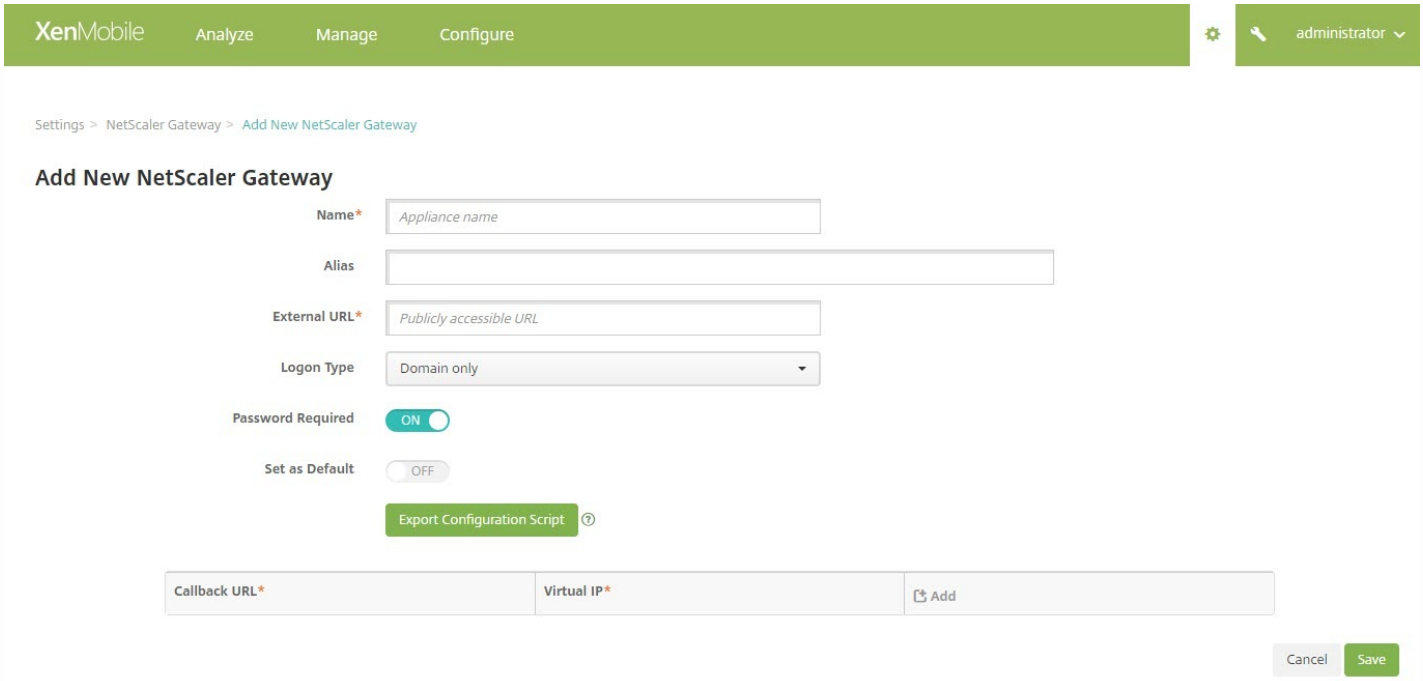
- Balanceamento de carga do Exchange
- Balanceamento de carga do ShareFile
- Configuração de proxy ICA
- Descarga de SSL

Se houver uma instância de NetScaler Gateway, a página **Configurações > NetScaler Gateway** agora tem um botãoo **Exportar Script de configuração**.



A página **Adicionar novo NetScaler Gateway** também inclui um link para exportar o script de configuração.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Para obter mais informações, consulte NetScaler Gateway e XenMobile.

Credenciais derivadas para registro de dispositivo iOS

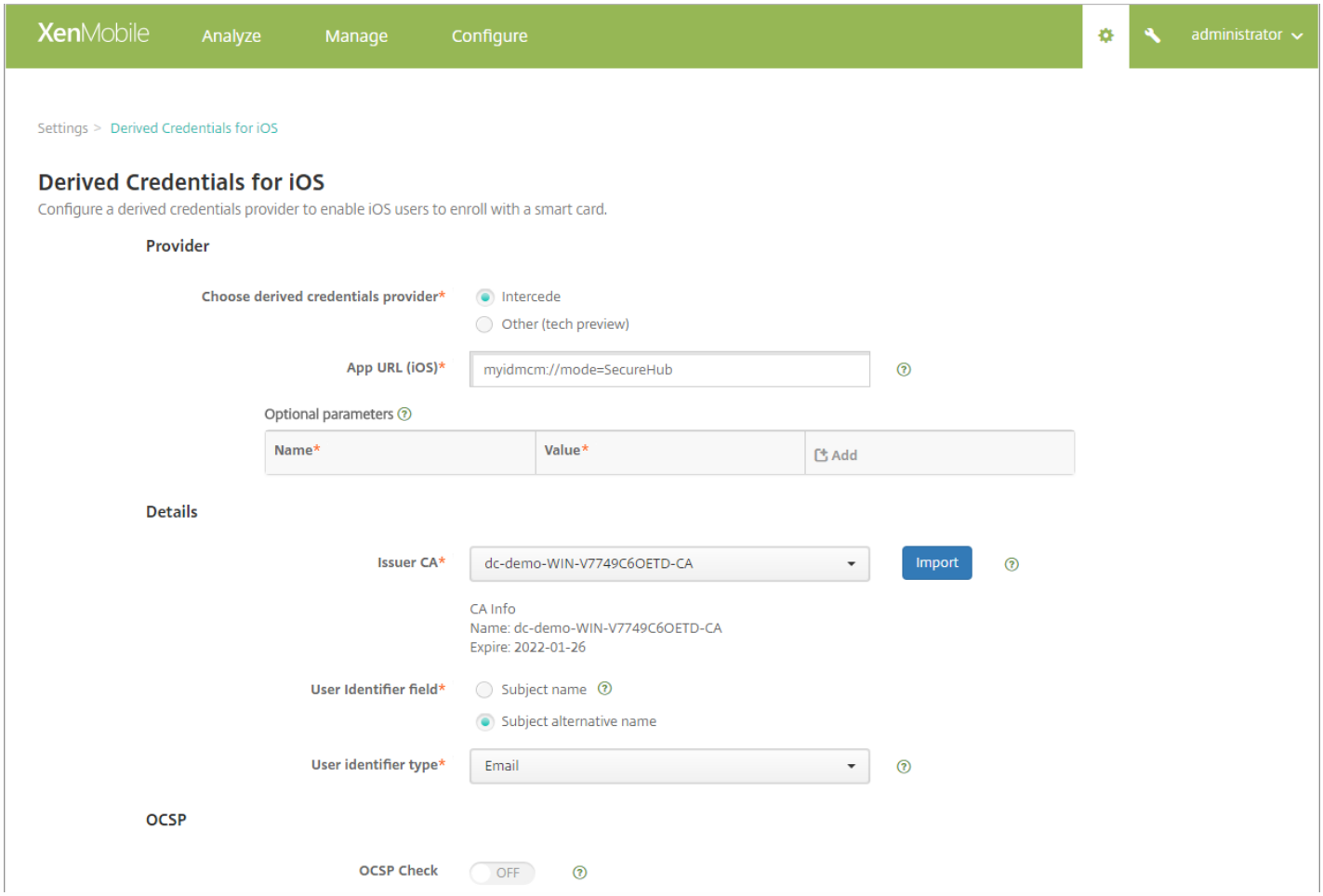
As credenciais derivadas fornecem autenticação forte para dispositivos móveis. As credenciais, derivadas de um cartão inteligente, residem em um dispositivo móvel em vez do cartão. O cartão inteligente é um Personal Identity Verification (PIV) ou um Common Access Card (CAC).

As credenciais derivadas são um certificado de registro que contém o identificador de usuário, como UPN. O XenMobile armazena as credenciais obtidas do provedor de credenciais em um cofre seguro no dispositivo.

O XenMobile pode usar credenciais derivadas para registro de dispositivo iOS Se configurado para credenciais derivadas, XenMobile não dá suporte a convites de registro ou outros modos de registro para dispositivos iOS. No entanto, você pode usar o mesmo XenMobile Server para registrar os dispositivos Android por meio de convites de registro e outros modos de registro.

Configure credenciais derivadas usando a página **Configurações > Credenciais derivadas para iOS**. Como padrão, o console do XenMobile não inclui **Configurações > Credenciais derivadas**. Para ativar a interface para credenciais derivadas, vá até **Configurações > propriedades do servidor,** adicione a propriedade de servidor **derived.credentials.enable** e defina-a como **verdadeira**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



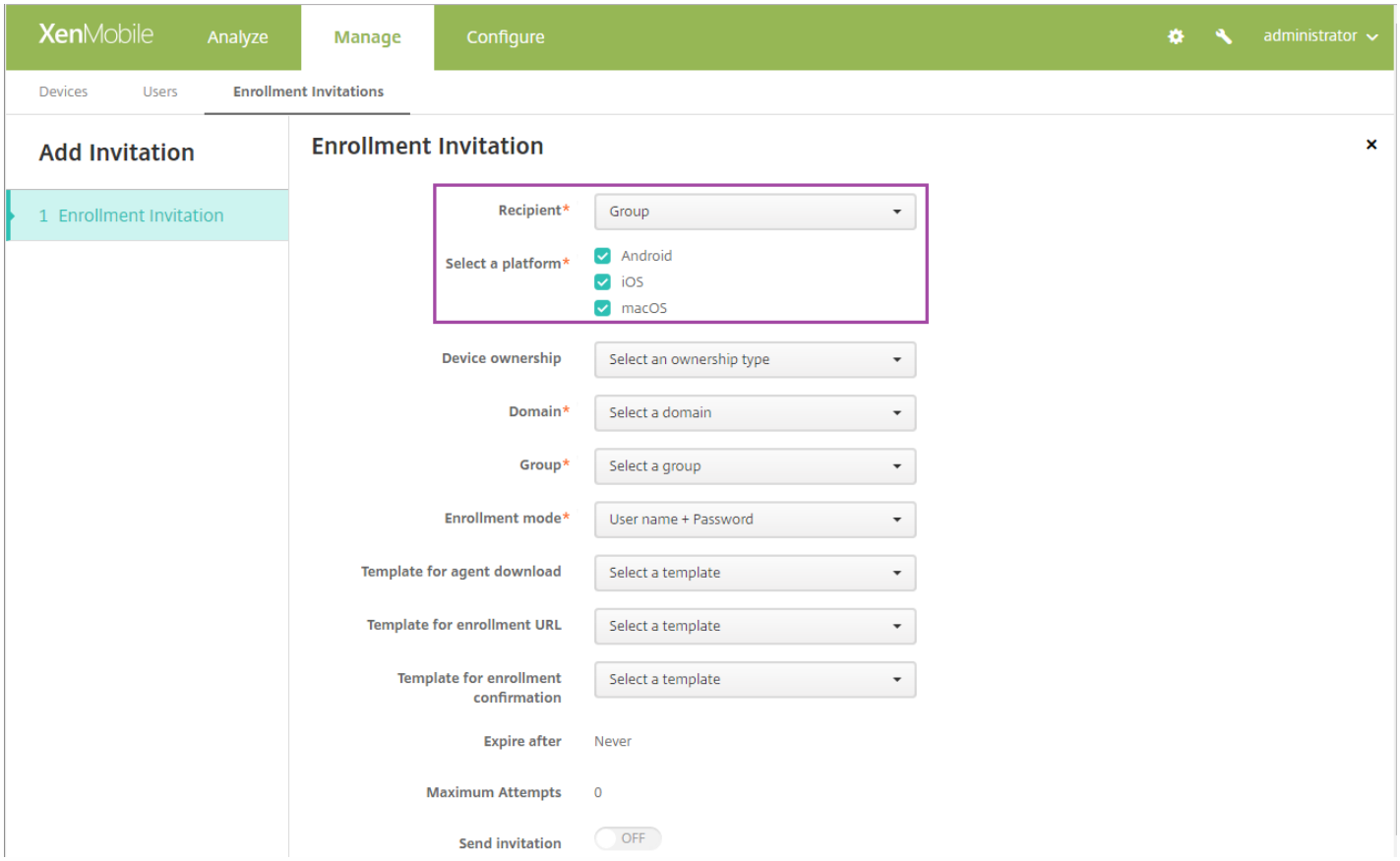
Para obter mais informações, consulte Credenciais derivadas para iOS. Para obter informações sobre a API REST para credenciais derivadas, consulte o PDF de referência da API REST do XenMobile.

Selecione várias plataformas de dispositivo de convites de registro

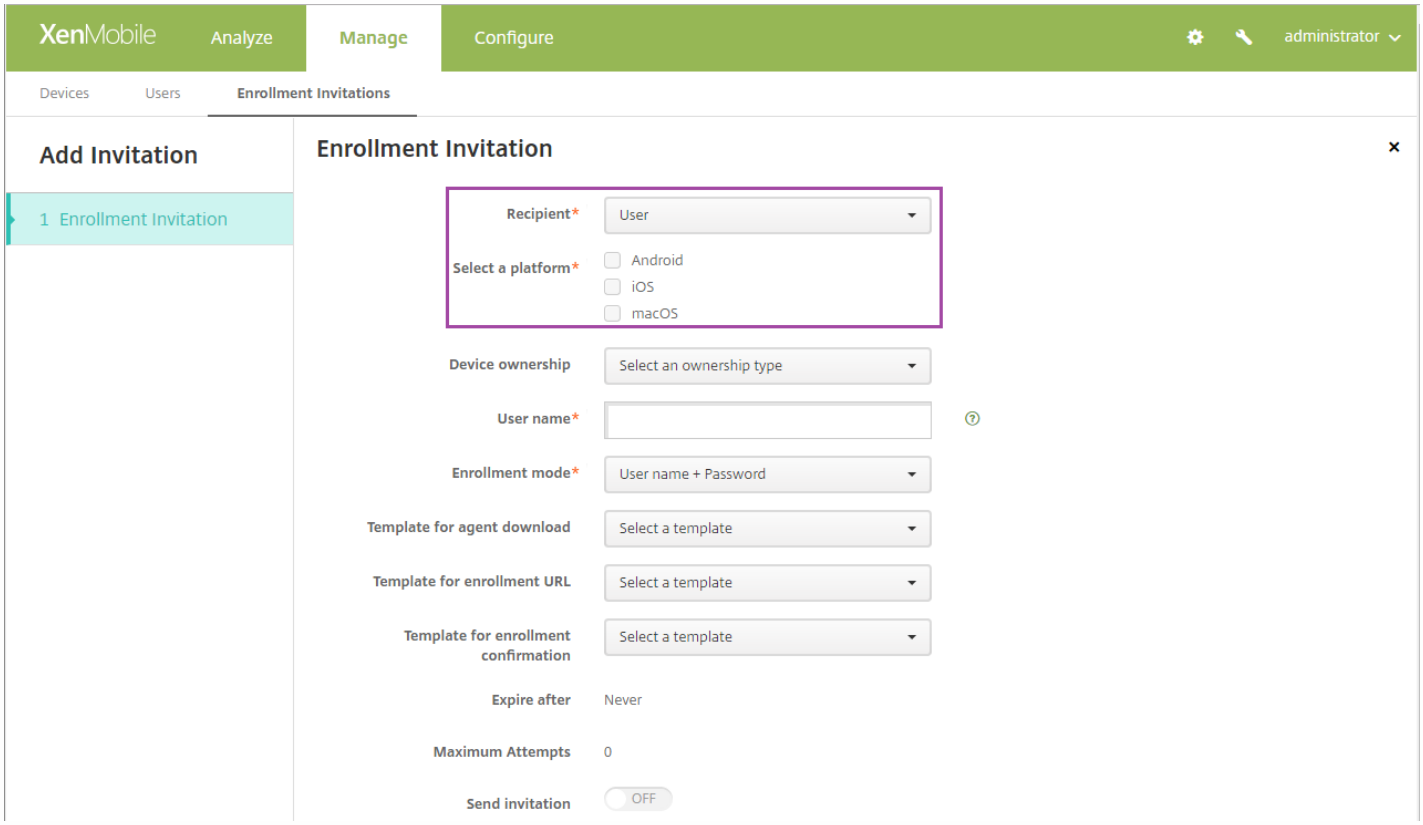
Agora você pode selecionar qualquer combinação de iOS, macOS e plataformas de dispositivo Android para um convite para registro. A página **Gerenciar > Convites de registro** inclui uma configuração **Selecionar uma plataforma**. As plataformas selecionadas determinam as opções de **Modo de registro** mostradas e se são exibidas algumas configurações, como **Informações do dispositivo**.

Se **Destinatário** é **Grupo**, todas as plataformas estão selecionadas como padrão.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



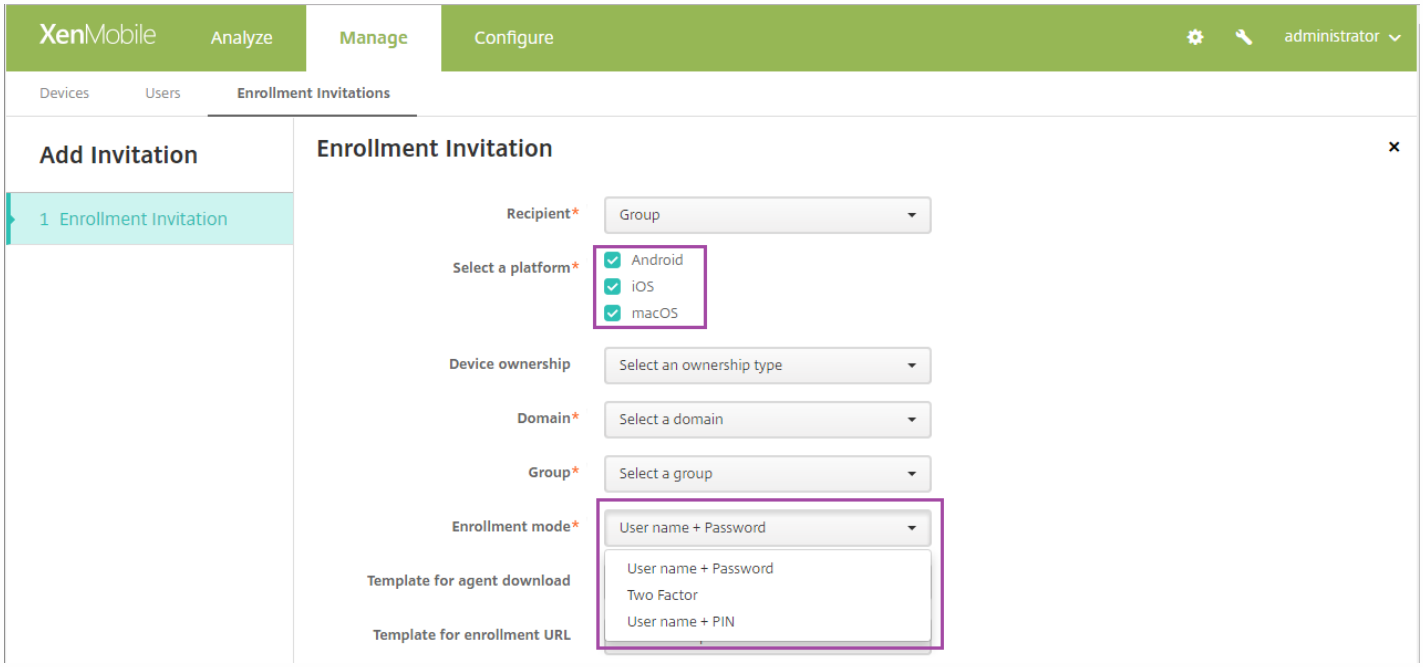
Se **Destinatário** é **Usuário**, nenhuma plataforma está selecionada como padrão.



Somente são exibidas as opções de **Modo de registro** que são válidas para cada uma das plataformas selecionadas. Por exemplo, se todas as plataformas estão selecionadas, os modos de registro válidos para essa combinação são Nome de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

usuário + Senha, Dois fatores e Nome de usuário + PIN.



Mais opções de registro de dispositivos macOS

Além de registrar os usuários do macOS enviando um link de registro, agora você pode registrar os usuários do macOS enviando um convite para registro. Os dois modos permite que os usuários de macOS façam o registro diretamente dos seus dispositivos pela rede celular.

Um convite para registro pode usar qualquer um dos seguintes modos de registro para dispositivos macOS:

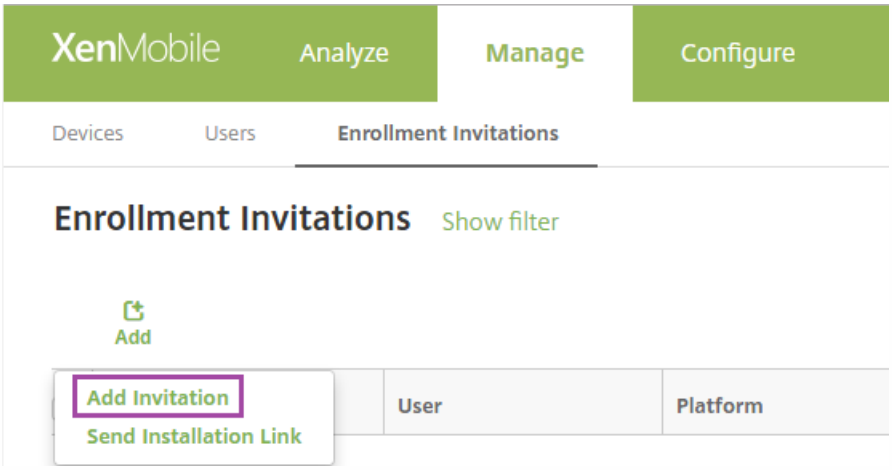
- Nome de usuário + PIN
- Nome de usuário + senha
- Dois Fatores

Quando o usuário segue as instruções no convite de registro, é exibida uma tela de logon com o nome de usuário preenchido.

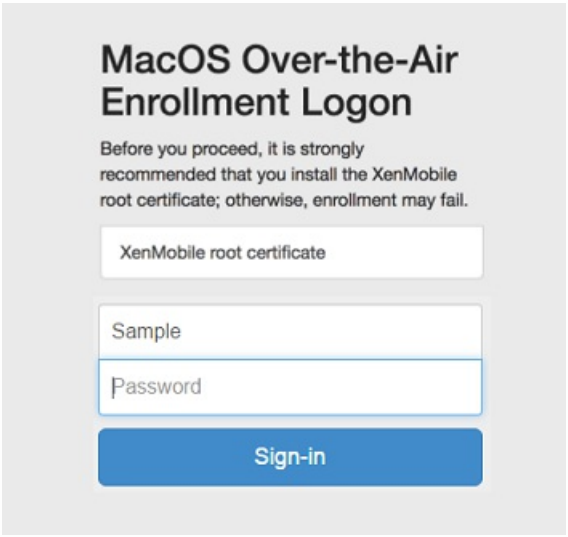
Para enviar um convite para registro de usuários de dispositivos macOS:

1. Adicione um convite para registro de usuário do macOS. Para obter informações, consulte Enviar aos usuários um convite para registro.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 registro, é exibido um campo adicional.



3. Os usuários instalam os certificados conforme necessário. Se você configurou um certificado SSL publicamente confiável e um certificado de assinatura digital confiável para macOS, o XenMobile não solicita aos usuários para que instalem um certificado. Para obter mais informações sobre certificados, consulte Certificados e autenticação.

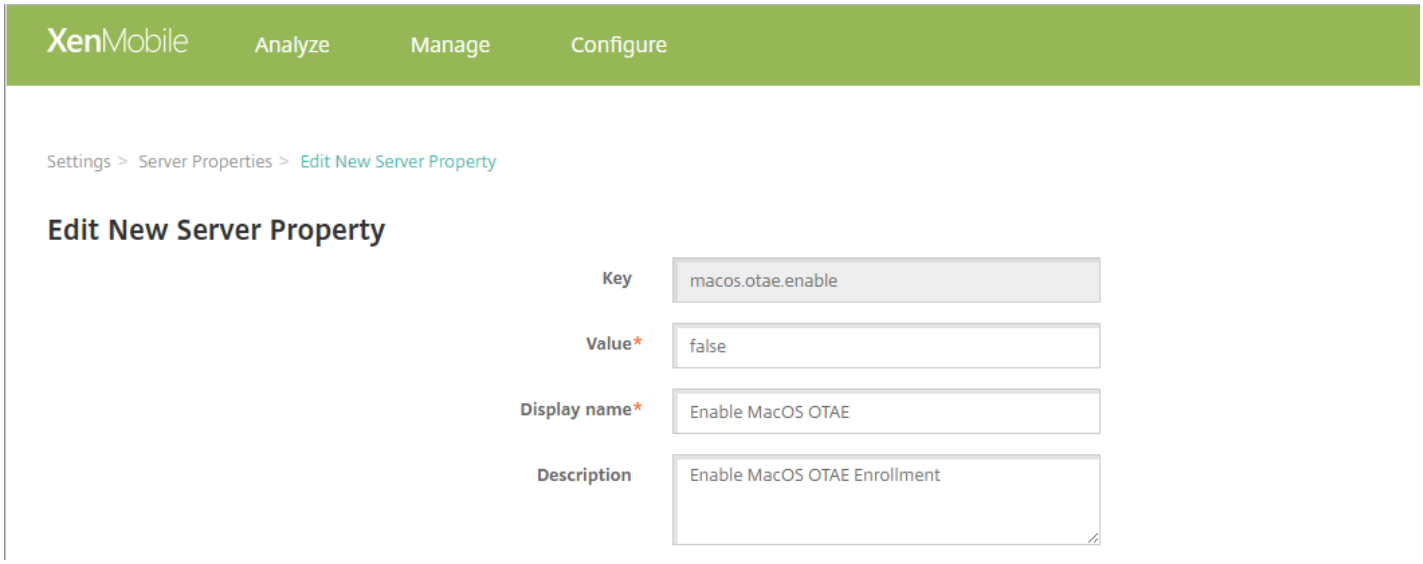
4. Os usuários fornecem as credenciais solicitadas.

   Agora você pode começar a gerenciar Macs com o XenMobile, da mesma forma como gerencia os dispositivos móveis.

Para impedir o registro com um link de instalação em dispositivos macOS:

Você pode impedir o uso de um link de registro em dispositivos macOS configurando a nova propriedade de servidor, **Ativar macOS OTAE** (**macos.otae.enable**), como **falsa**. Como resultado, os usuários do macOS apenas podem se registrar usando um convite para registro.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Política de dispositivo Proteção de informações do Windows

A Proteção de informações do Windows (WIP), conhecida anteriormente como proteção de dados empresariais (EDP), é uma tecnologia de Windows 10 que oferece proteção contra o potencial vazamento de dados corporativos. Pode ocorrer vazamento de dados por meio de compartilhamento de dados empresariais com aplicativos protegidos não empresariais, entre aplicativos ou fora da rede da sua organização. Para obter mais informações, consulte Protect your enterprise data using Windows Information Protection (WIP) no Microsoft TechNet.

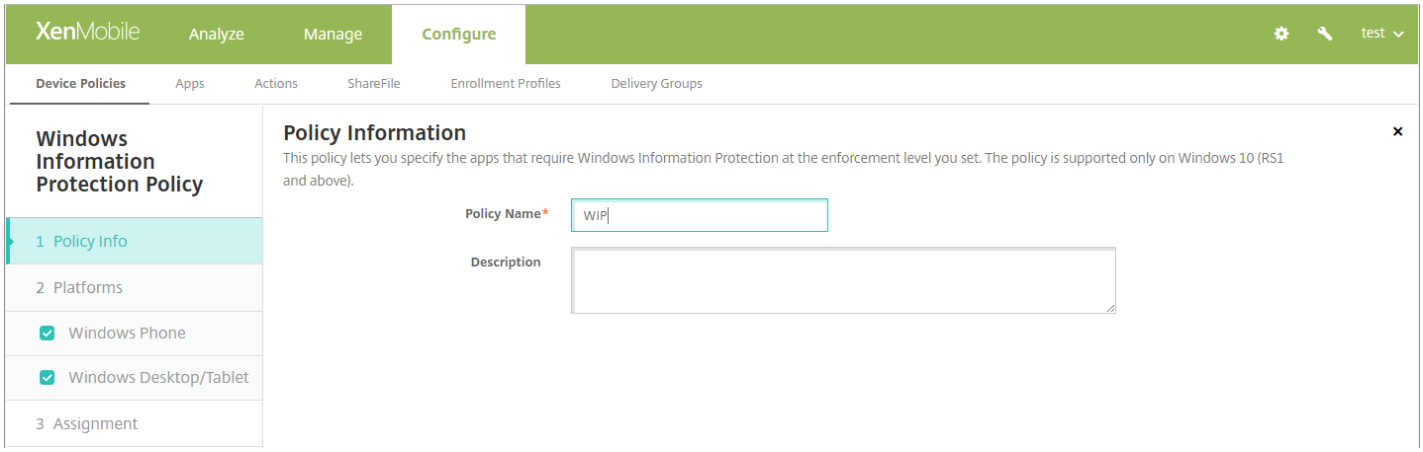
Você pode criar uma política de dispositivo no XenMobile para especificar os aplicativos que requerem Proteção de informações do Windows no nível de execução que você definir. A política Proteção de informações do Windows é para Windows 10 versão 1607 e posterior, telefone, tablet e área de trabalho supervisionadas.

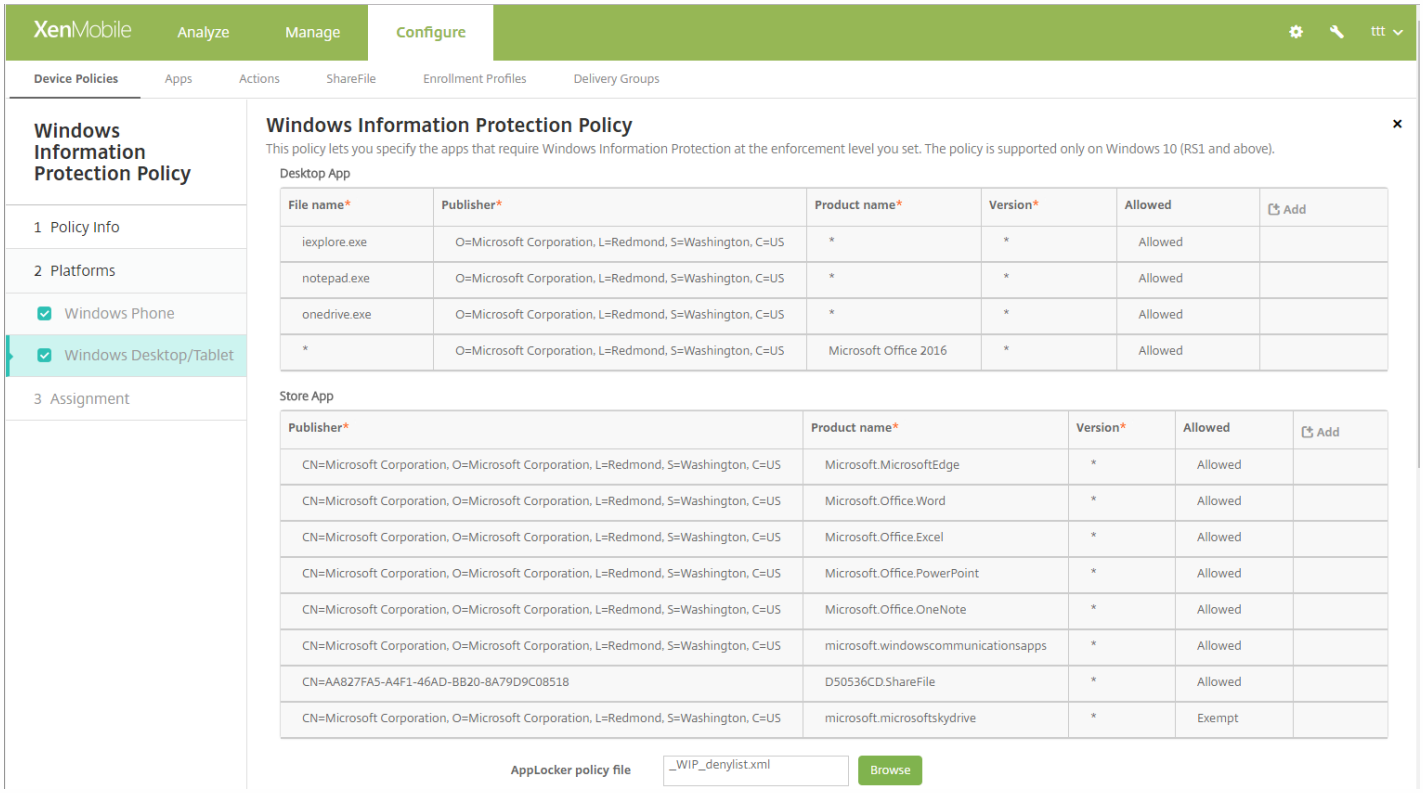
Especifique um nível de execução que afeta a experiência do usuário. Por exemplo, você pode:

- Bloquear qualquer compartilhamento de dados impróprio.
- Avisar sobre o compartilhamento de dados impróprio e permitir que os usuários substituam a política.
- Execute WIP silenciosamente durante o registro do log e permitindo o compartilhamento de dados impróprio.

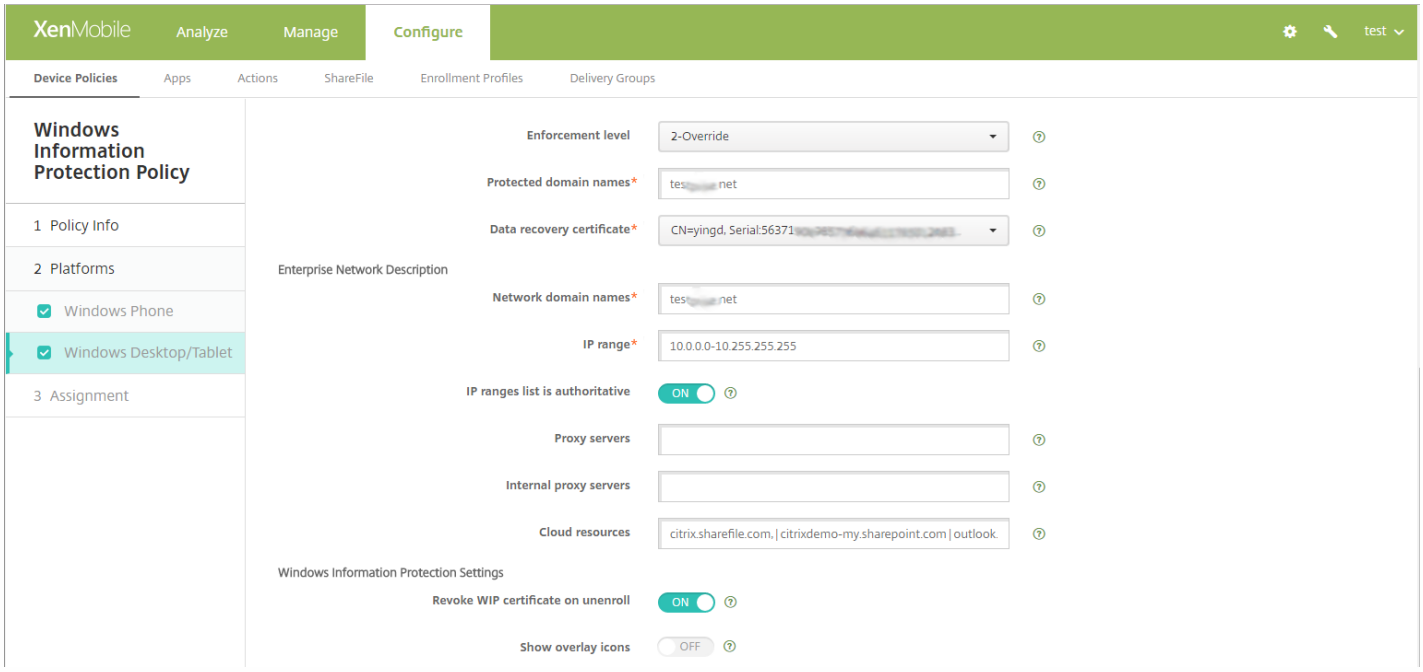
Para criar a política, vá até **Configurar > Políticas de dispositivo** e adicione a a política **Proteção de Informações do Windows**.

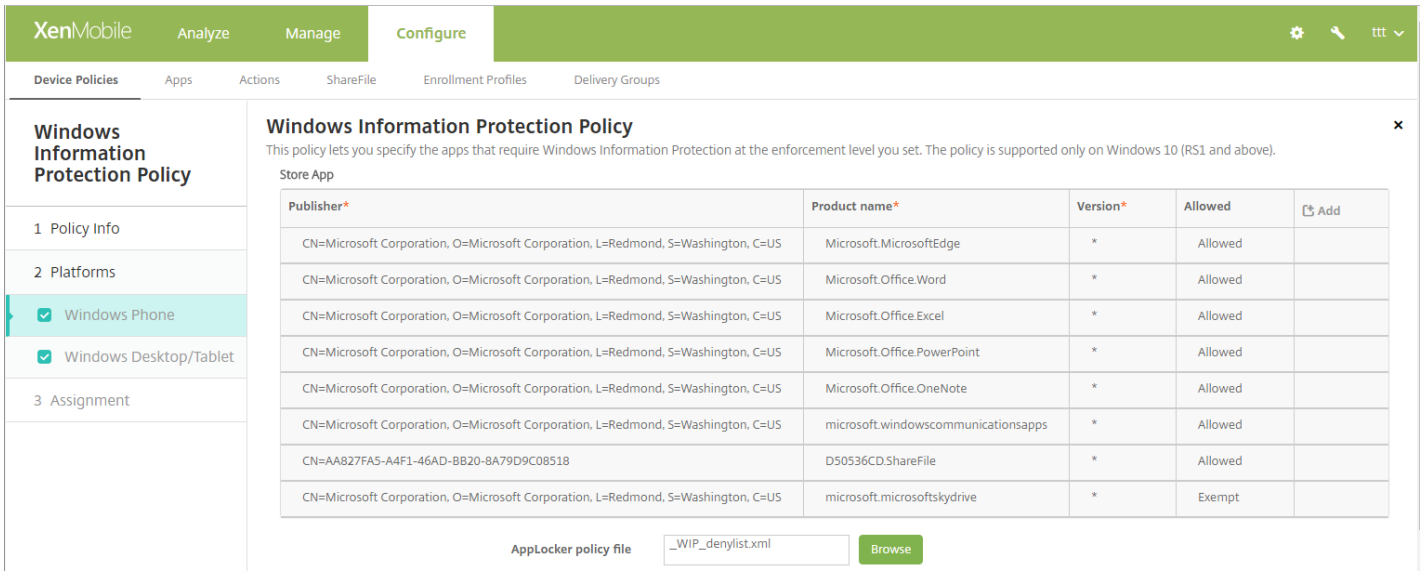
© 1999-2017 Citrix Systems, Inc. All rights reserved.





© 1999-2017 Citrix Systems, Inc. All rights reserved.





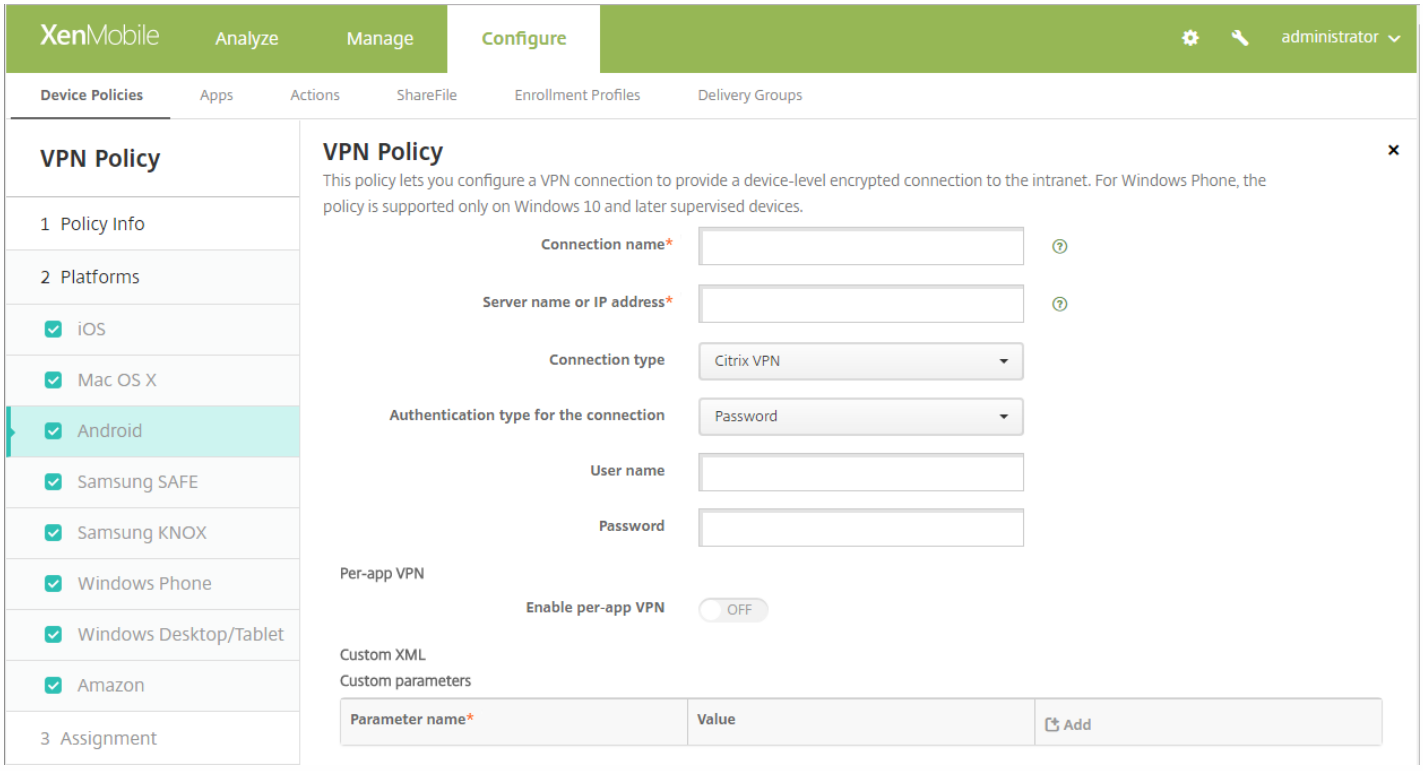
Para obter mais informações, consulte a política de Proteção de Informações do Windows.

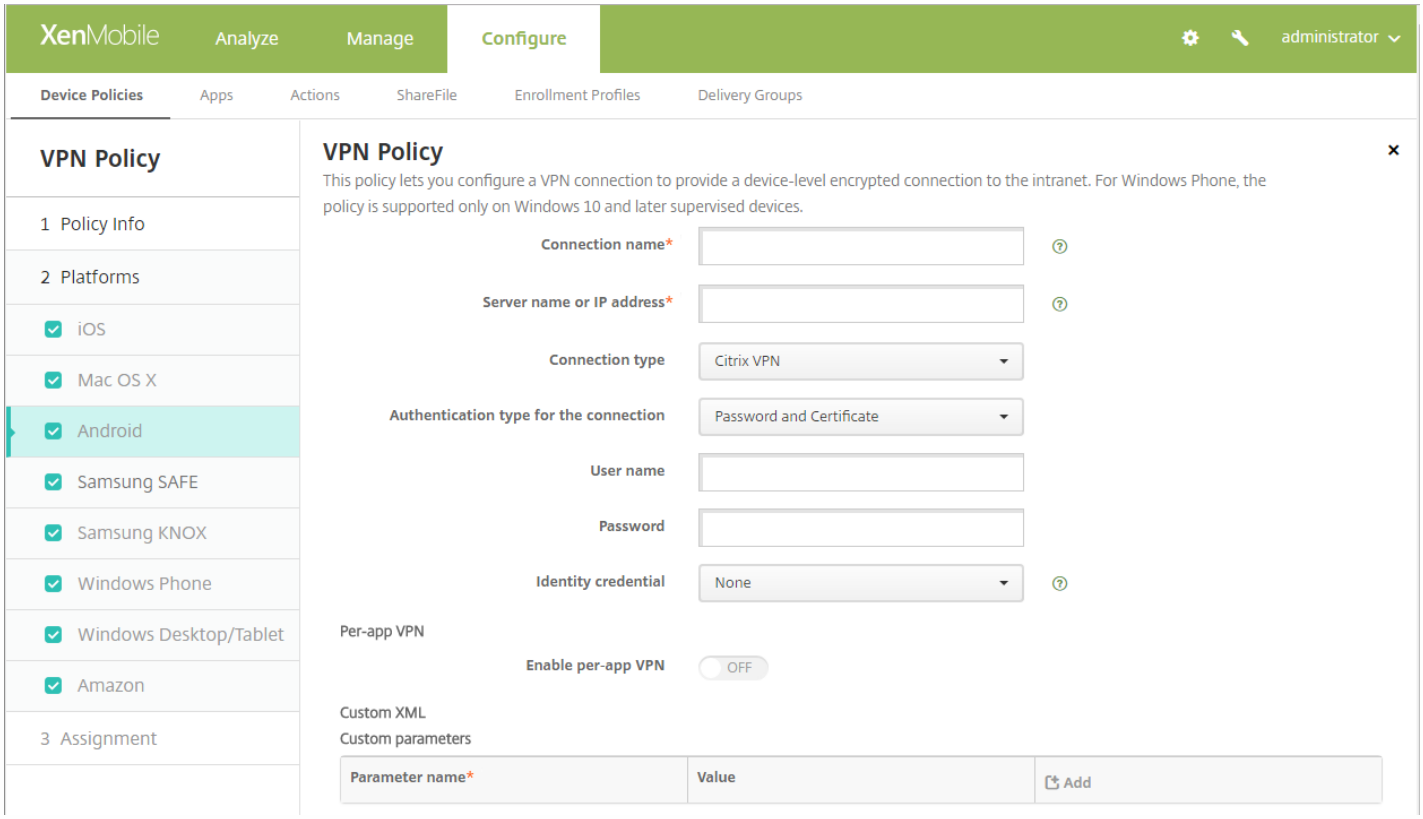
Tipo de conexão VPN Citrix para dispositivos Android

A política de dispositivo VPN para Android agora dá suporte à configuração de VPN Citrix. A Citrix VPN é um aplicativo móvel que se conecta ao NetScaler Gateway no modo VPN completo, em vez de uma VPN sem cliente ou o modo de proxy ICA. Este recurso requer o Secure Hub 10.6.

Na página **Configurar > Políticas de Dispositivo** para Android, o menu **Tipo de conexão** agora inclui **Citrix VPN.**

© 1999-2017 Citrix Systems, Inc. All rights reserved.



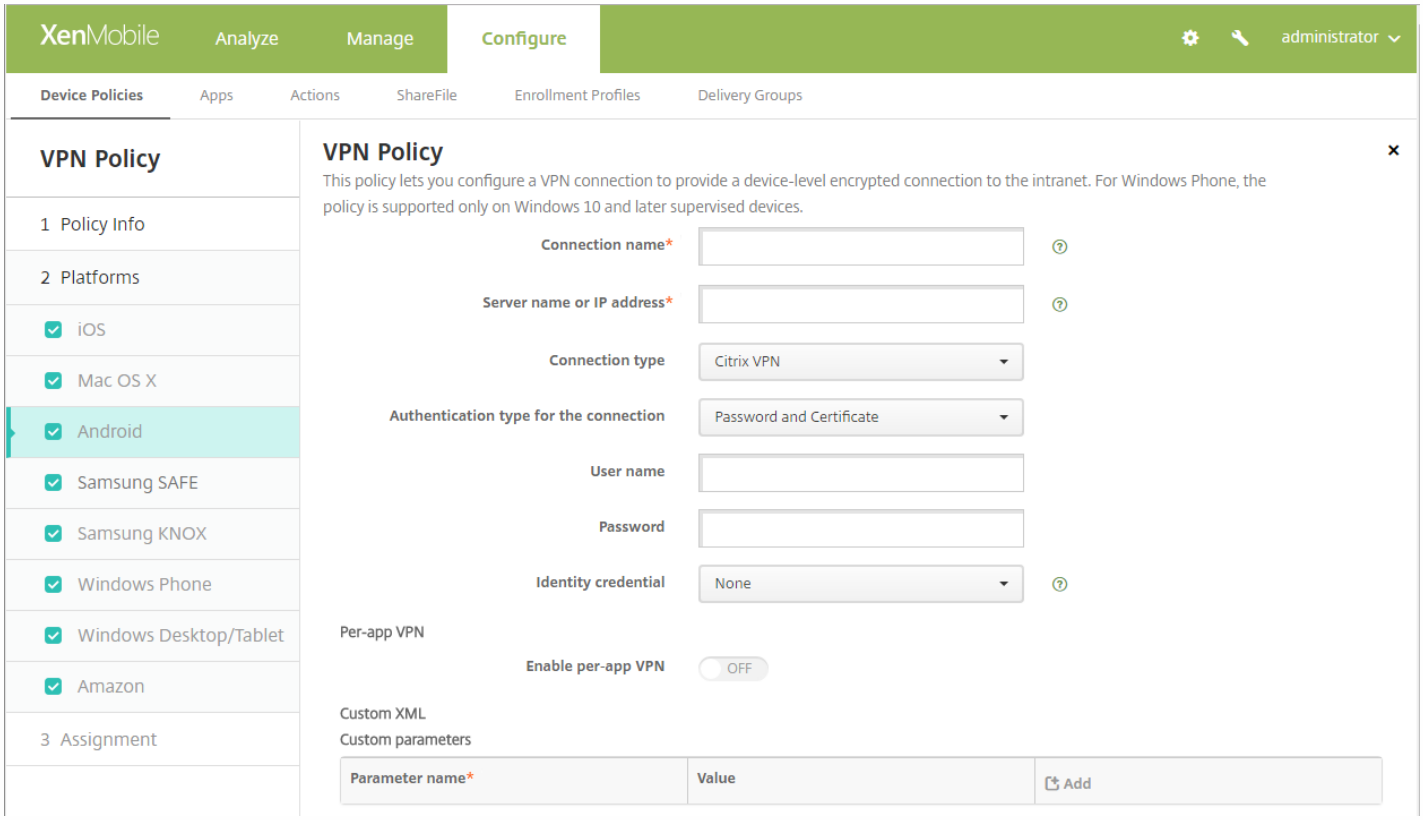


Configurações para o tipo de conexão de Citrix VPN:

- **Nome ou endereço IP do servidor**: digite o FQDN endereço IP do NetScaler Gateway.
- **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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Credencial de identidade**: é exibida para os **Tipos de autenticação** de **Certificado** ou **Senha e certificado**.
- **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 **O**.
  - **Lista branca** ou **Lista negra**: escolha uma configuração. Se **Lista branca**, todos os aplicativos em lista branca passam pelo túnel através dessa VPN. Se **Lista negra**, todos os aplicativos, exceto os que estão na lista negra, passam pelo túnel através dessa VPN.
  - **Lista de aplicativos:** especifique os aplicativos em lista branca ou lista negra. 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:
  - **disableL3Mode**: opcional. Para ativar esse parâmetro, digite **Sim** para o **Valor**. Se ativado, nenhuma conexão de VPN adicionada pelo usuário é exibida e o usuário não pode adicionar outra conexão. A restrição é global e se aplica a todos os perfis 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 do usuário existente do Citrix VPN.



Para obter mais informações, consulte a Política de dispositivo de VPN.

Integração do XenMobile com o Azure Active

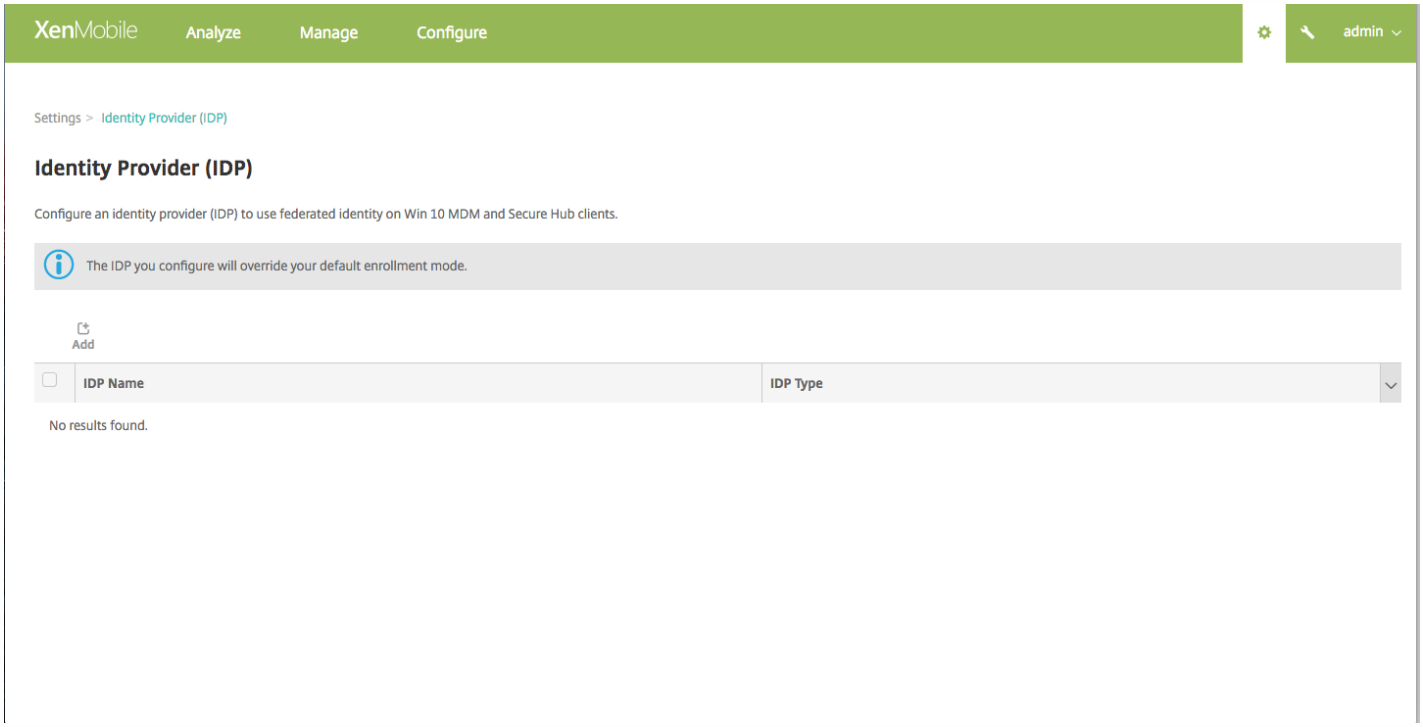
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Directory como IDP

Configurar o Azure Active Directory (AD) como seu provedor de identidade (IDP) permite que os usuários se registram 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.

Configure o Azure como 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** .



Para obter mais informações, consulte Integração do XenMobile com o Azure Active Directory como IDP.

Implantar políticas de dispositivo, aplicativos e ações inteligentes com base no ID de aplicativo

Você pode configurar o XenMobile para implantar políticas de dispositivo, aplicativos e ações inteligentes com base no ID de aplicativo Para fazer isso, você usar uma nova regra de implantação, **Nome do aplicativo instalado**.

Você pode usar esse novo recurso para migrar de distribuição em loja de aplicativos empresariais para distribuição em loja de aplicativos pública:

- Use a regra **Nome do aplicativo instalado** com a política de dispositivo de desinstalação de aplicativo. Isso faz com que o XenMobile remova os aplicativos empresariais dos dispositivos do usuário depois de ser instalada a versão de loja de aplicativos pública.
- Esse recurso está disponível somente para dispositivos iOS gerenciados conectados a um servidor XenMobile no modo enterprise (XME).

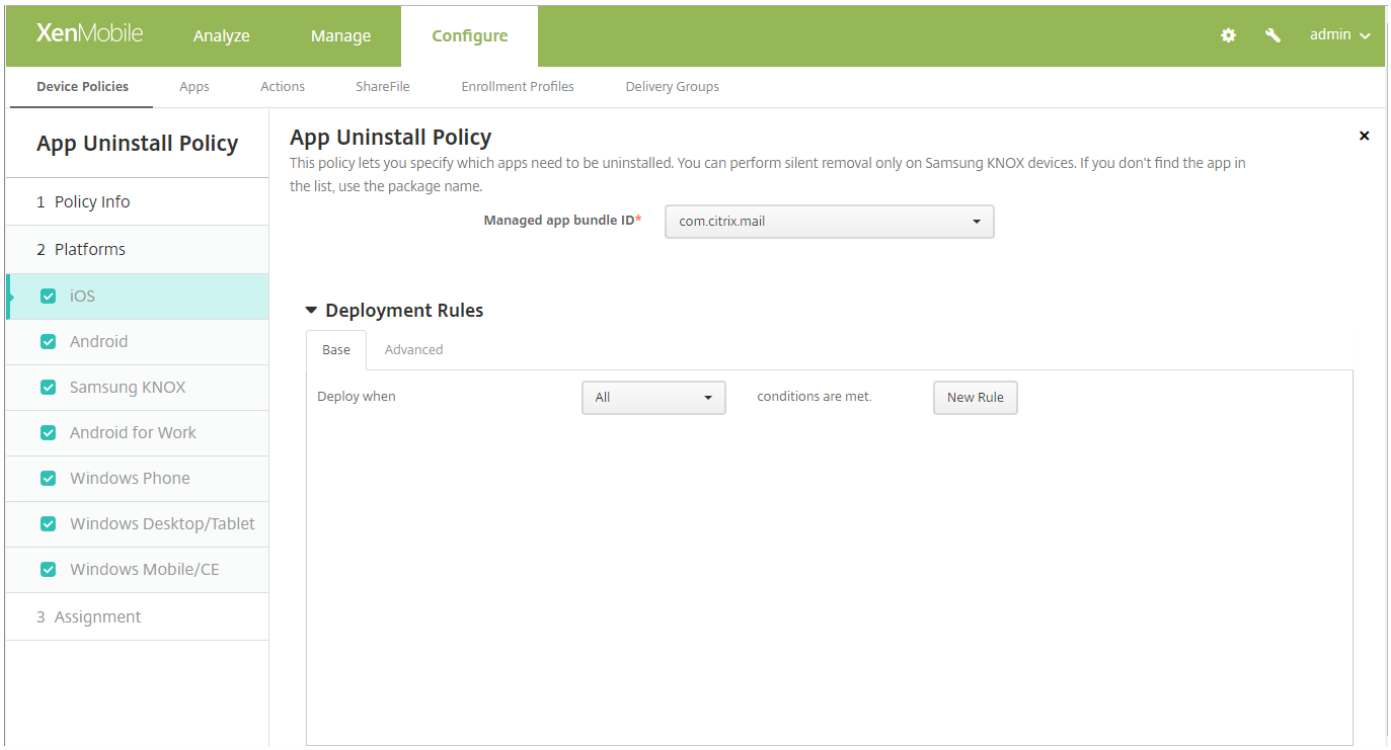
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nota

A Citrix exige que você use as versões da loja de aplicativos pública dos aplicativos Citrix, em vez de versões empresariais, até o final de 2017.

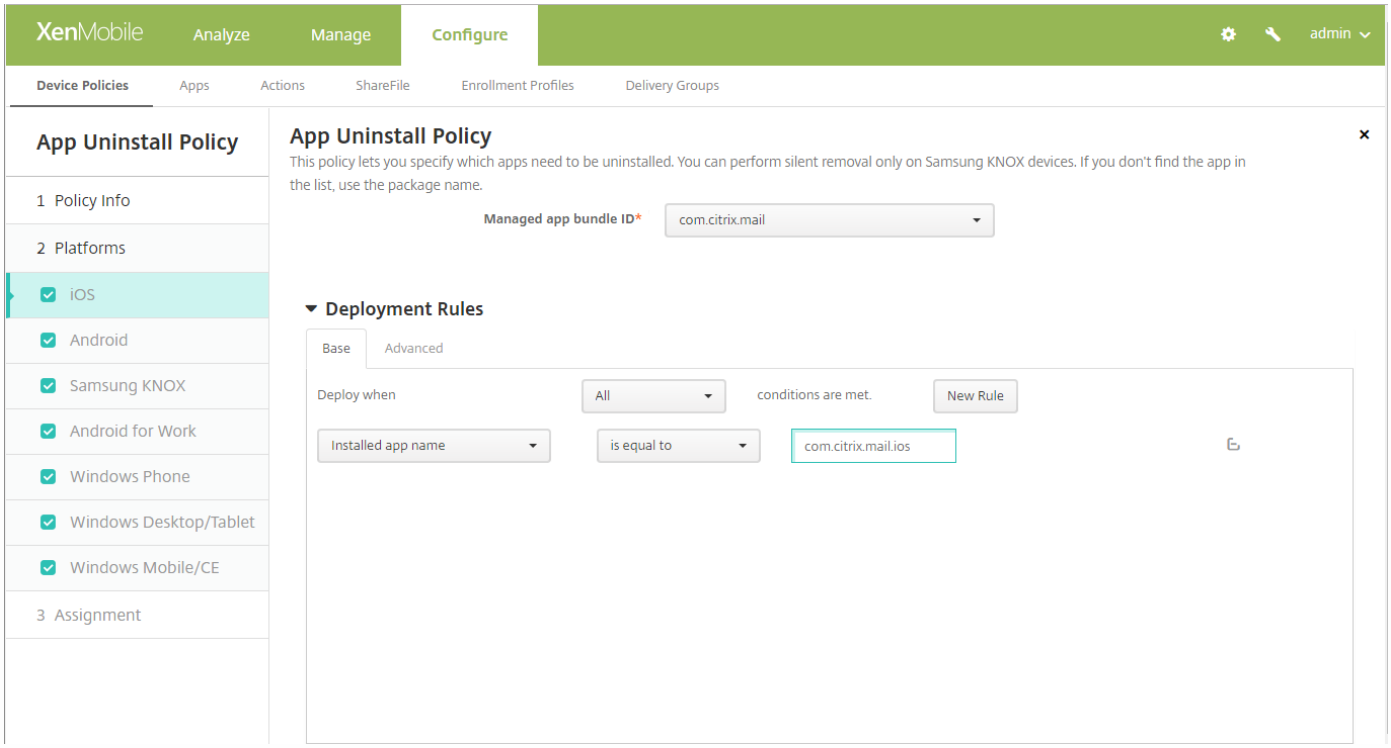
Para configurar a política de dispositivo de desinstalação de aplicativo para um aplicativo empresarial:

1. Em **Configurar > Políticas de dispositivo**, clique em **Adicionar** e, em seguida, clique em **Desinstalação de aplicativo**.
2. Dê um nome à política e, em seguida, remova as caixas de seleção de tudo exceto da plataforma **iOS**.
3. Na página **iOS**, escolha a ID do pacote de aplicativo do aplicativo empresarial antigo e, em seguida, expanda as **Regras de implantação**.



4. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. Preencha a página **Atribuição** e, em seguida, clique em **Salvar**.

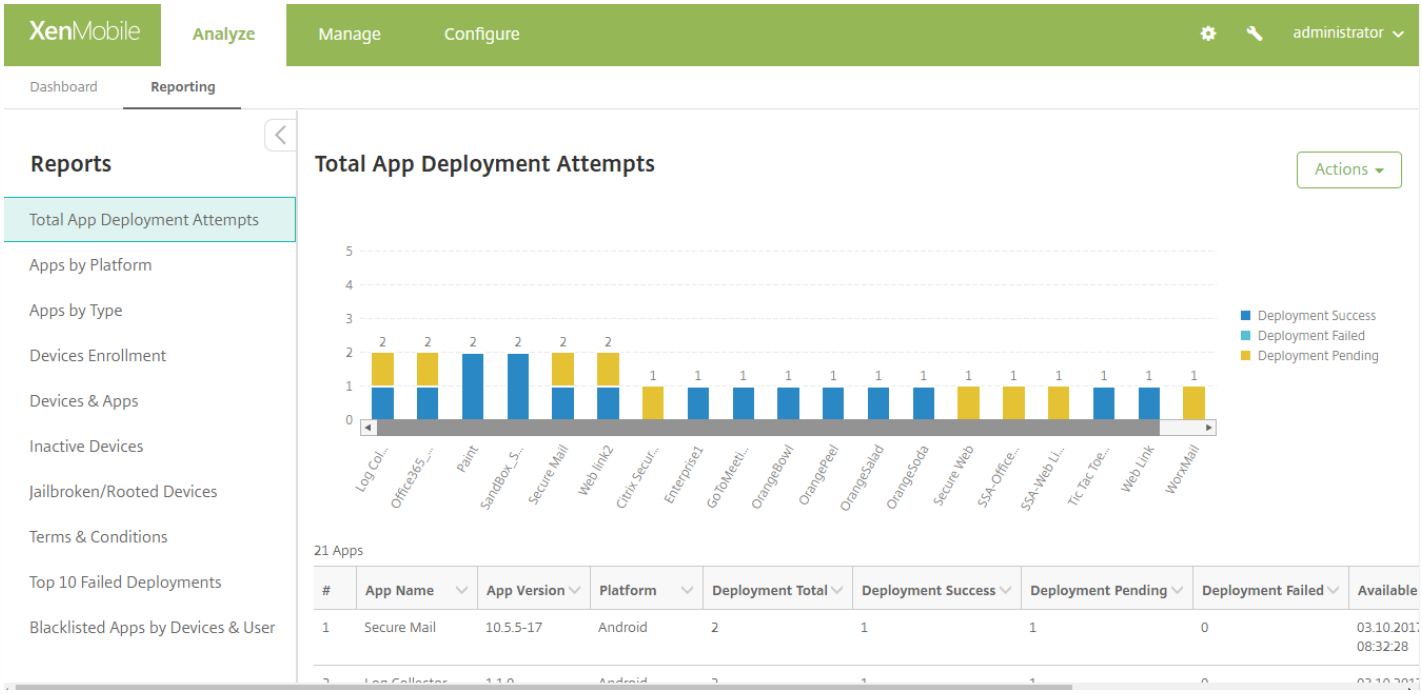
   No exemplo, após a instalação do aplicativo de loja de aplicativos pública (com.citrix.mail.ios) em um dispositivo em grupos de entrega especificado, o XenMobile remove a versão empresarial (com.citrix.mail).

Aprimoramentos no relatório

A página **Analisar > Relatórios** do XenMobile tem um design aprimorado e mais recursos para todos os relatórios predefinidos:

- Classificação e pesquisa usando filtros baseados no dispositivo.
- Filtrar relatórios por data
- Exportar relatórios em formato PDF.
- Gráficos interativos que representam dados do relatório visualmente.
- O relatório Os 25 aplicativos mais usados agora é chamado de Total de tentativas de implantação de aplicativos. Este relatório lista todos os aplicativos implantados e a porcentagem de usuários que tentou instalá-los em seus dispositivos.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



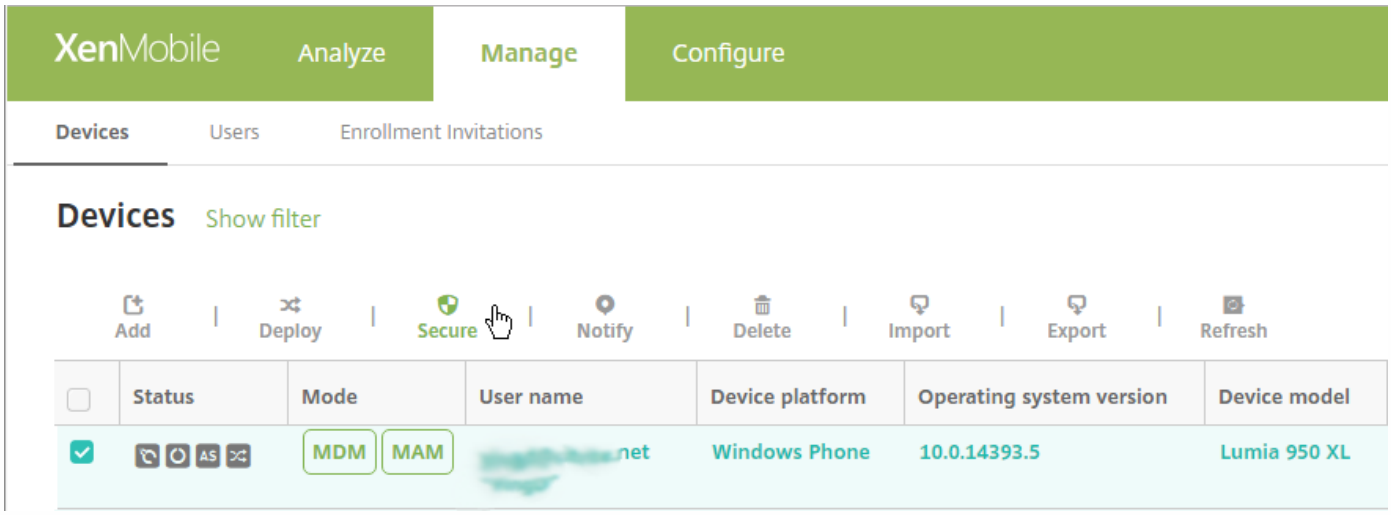
Para obter mais informações, consulte Relatórios.

Localizar dispositivos Windows 10

Os administradores do console do XenMobile e os usuários do Portal de autoajuda agora podem localizar telefones Windows 10, desktops e tablets. O recurso de localização já está disponível para dispositivos iOS e Android. Quando você executa um comando locate, o servidor XenMobile se comunica diretamente com o dispositivo.

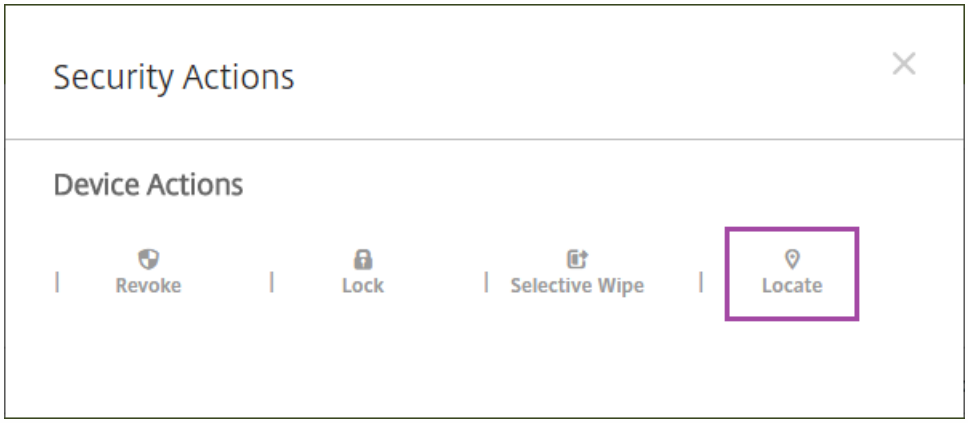
No console do XenMobile, envie a ação de localização para um dispositivo, da seguinte maneira.

1. Na página **Gerenciar > Dispositivos**, selecione o dispositivo e, em seguida, clique em **Seguro**.

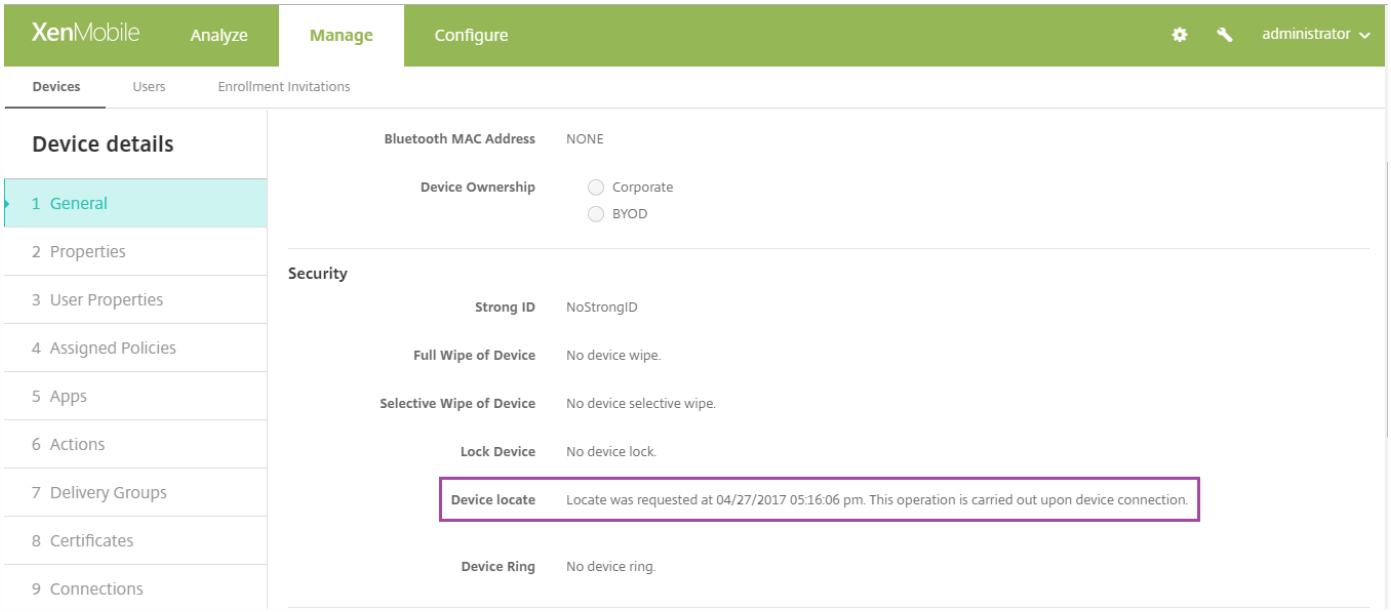


2. No **Ações de segurança**, clique em **Localizar**.

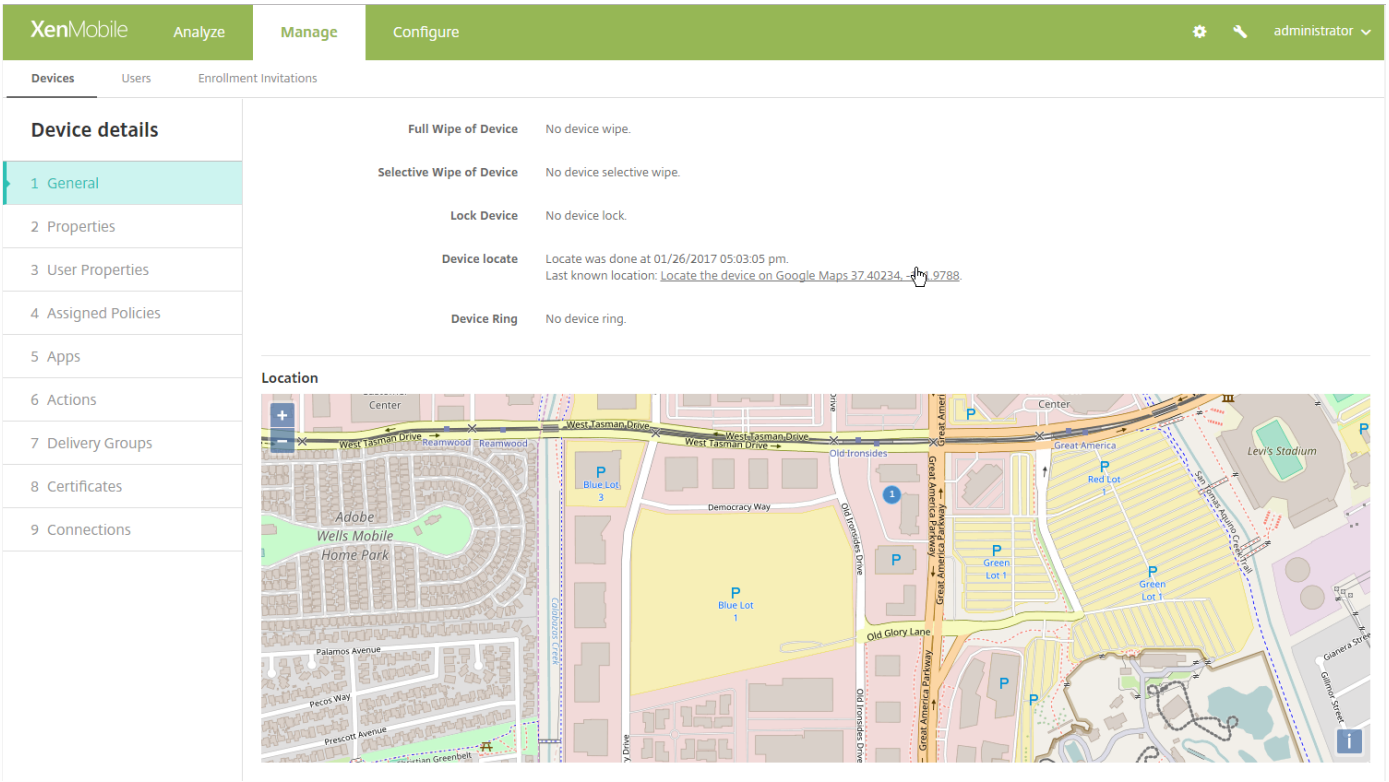
© 1999-2017 Citrix Systems, Inc. All rights reserved.



A página **Detalhes do dispositivo** fornece um status da solicitação de localização e mostra um mapa se o dispositivo for localizado.



© 1999-2017 Citrix Systems, Inc. All rights reserved.



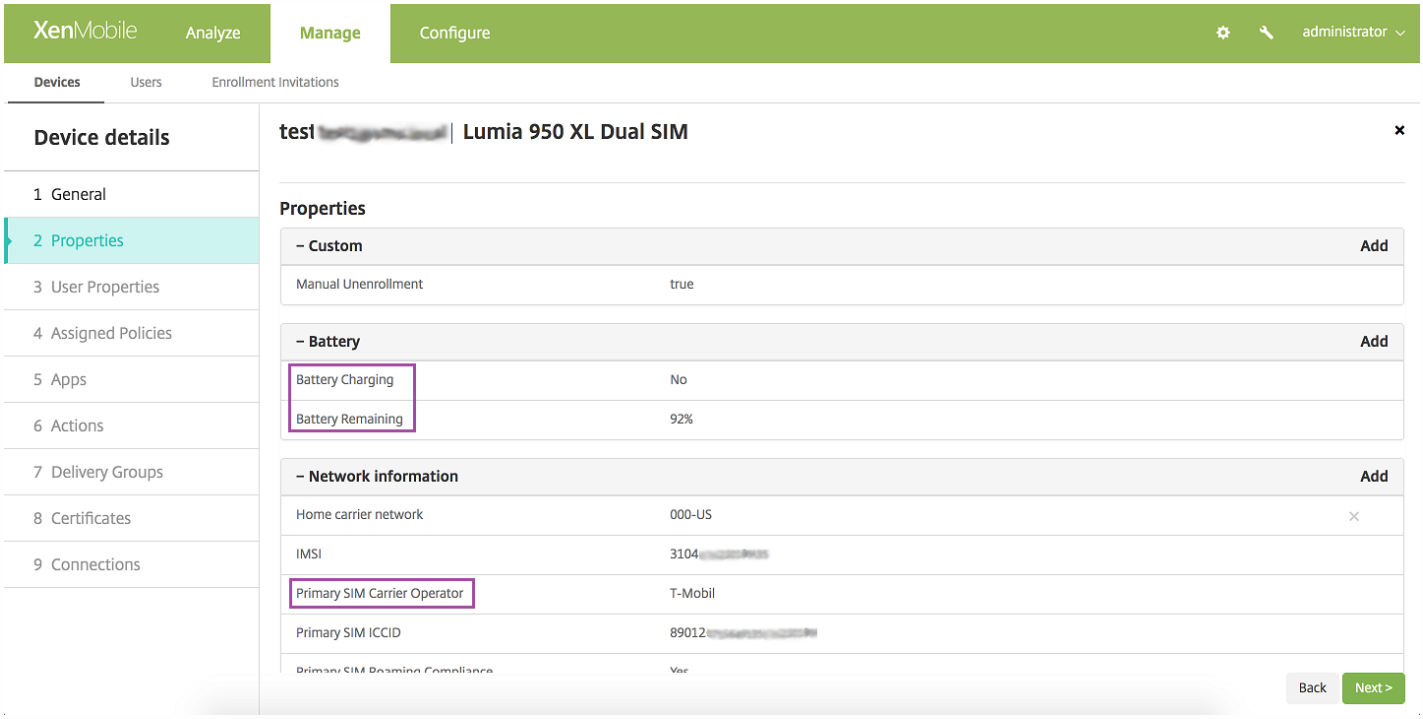
Mais propriedades de status de dispositivo para Windows 10 Phone e Tablet

A página **Gerenciar > Dispositivos** inclui mais propriedades de dispositivo para Windows. Estão disponívei as seguintes propriedades, fornecidas pelo provedor de serviço de configuração (CSP) do Windows 10 DeviceStatus.

Status da assinatura antispyware
Status do Antispyware
Status de assinatura de antivírus
Status de antivírus
Carregamento da bateria
Bateria restante
Conformidade de criptografia
Status de Firewall
Endereço IPV4
Endereço IPV6
Conexão de rede de endereço MAC
Tipo de endereço MAC
Edição do sistema operacional
Operador de operadora de SIM principal
ICCID de SIM principal
Conformidade Roaming de SIM principal
Status de inicialização segura
Versão de TPM
Status de controle de conta de usuário

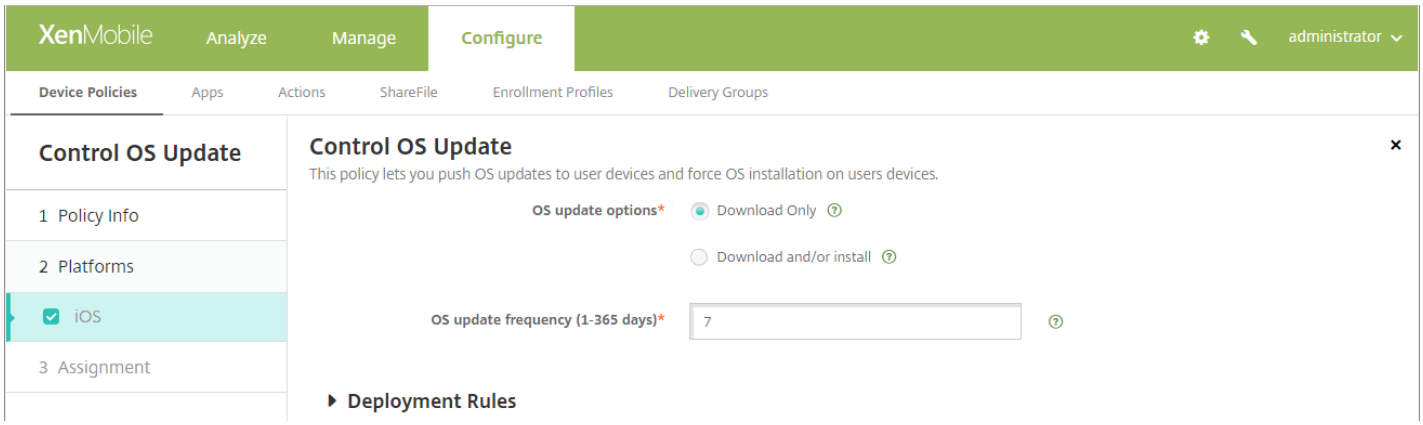
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para obter informações sobre essas propriedades, consulte o artigo da Microsoft DeviceStatus CSP. O exemplo a seguir mostra algumas das propriedades adicionadas.



Política de dispositivo para controlar as atualizações de sistema operacional em dispositivos iOS

Agora você pode configurar o XenMobile para enviar as mais recentes atualizações de sistema operacional para dispositivos iOS supervisionados. Você escolhe se as atualizações do sistema operacional devem ser implantadas para os dispositivos para que os usuários possam instalar as atualizações manualmente, ou se instalação em dispositivos deve ser forçada. Para configurar a nova política de dispositivo, vá para **Configurar > Políticas de dispositivo** e adicione **Controlar atualização de SO**.



Configure as opções:

- **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 sistema operacional**. O

© 1999-2017 Citrix Systems, Inc. All rights reserved.

dispositivo solicita que os usuários instalem atualizações. O aviso é visível depois que o usuário desbloqueia o dispositivo.

- **Frequência de atualização do SO (1-365 dias)**: determina a frequência XenMobile verifica e atualiza o sistema operacional do dispositivo. O padrão é **7** dias.

Mais opções de política de WiFi para iOS 10+

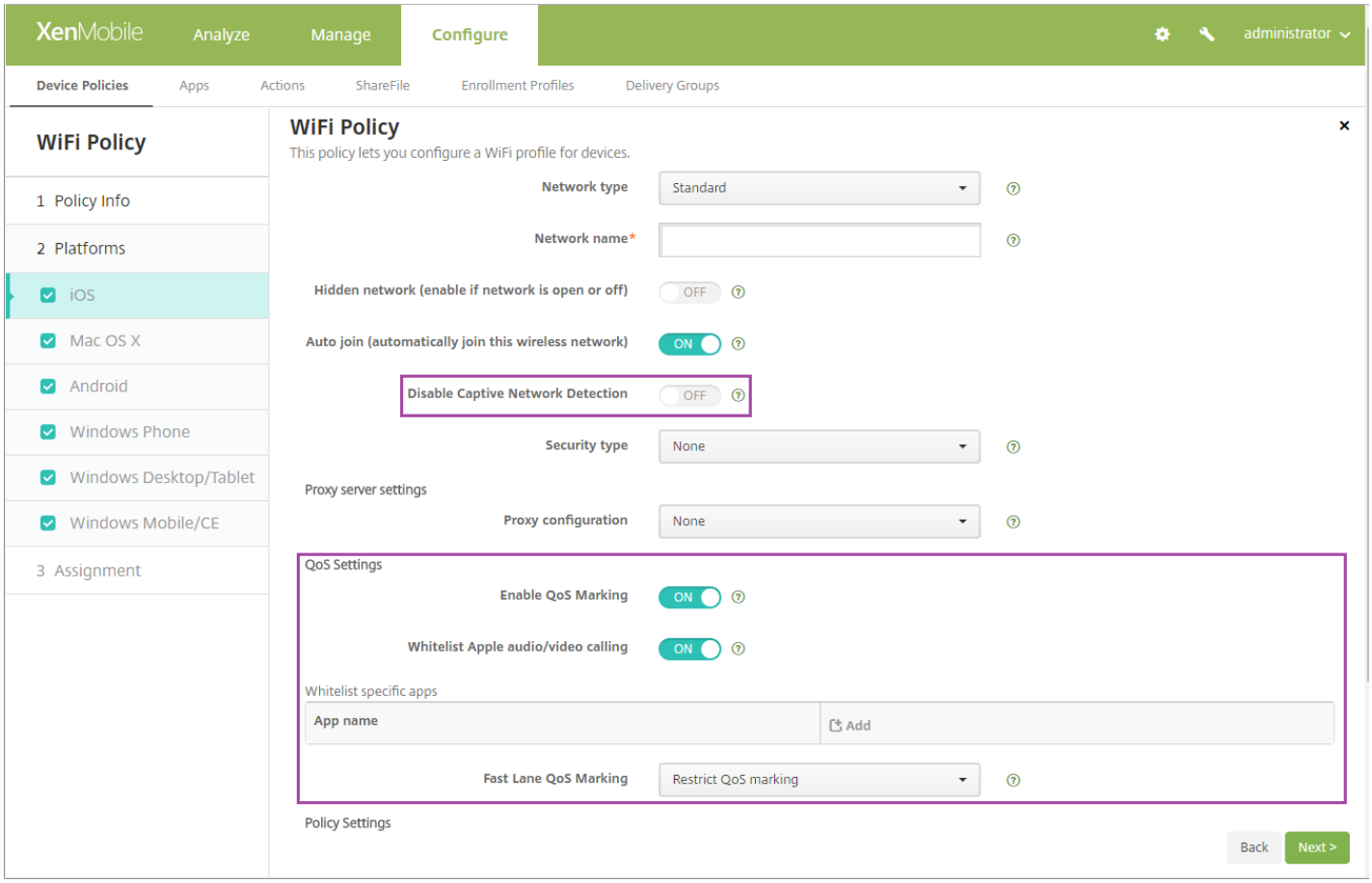
- **Desativar detecção de rede cativa**: se **I**, os usuários não podem entrar em redes que exigem contratos ou outras informações antes do acesso à rede. O valor padrão é **Desativado**.
- **Marcação de Fast Lane QoS**: a marcação de qualidade de serviço (QoS) permite que você priorize a largura de banda de rede para aplicativos de negócios específicos. Escolha entres restringir ou não restringir a marcação de Cisco Fast Lane QoS. Se você não restringir a marcação de QoS de uma rede WiFi que dá suporte a Cisco Fast Lane QoS, todos os aplicativos são inseridos na lista branca para usar marcação L2 e L3. Se você restringir a marcação QoS, especifique os aplicativos que podem usar marcação L2 e L3. O padrão é **Não restringir marcação de QoS**.

Se **Marcação de Fast Lane QoS** for **Restringir marcação QoS**, são exibidas as seguintes opções:

- **Ativar marcação de QoS**: opcional. Se o valor for **O**, a marcação de QoS está desativada. O valor padrão é **Ativado**.
- **Colocar em lista branca chama de áudio/vídeo da Apple**: opcional. Se o valor for **O**, a chamada de áudio e vídeo da Apple não estará na lista branca, o que significa que o tráfego não é priorizado. O valor padrão é **Ativado**.
- **Colocar aplicativos específicos na lista branca**: especifique os aplicativos que devem usar marcação L2 e L3.

Para obter mais informações sobre as políticas de WiFi para iOS, consulte Ajuda do Apple Configurator 2.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Mais opções de política VPN por aplicativo para iOS

A política de VPN inclui essas novas opções, que são usadas quando o cliente VPN em um dispositivo é compatível com vários provedores de VPN:

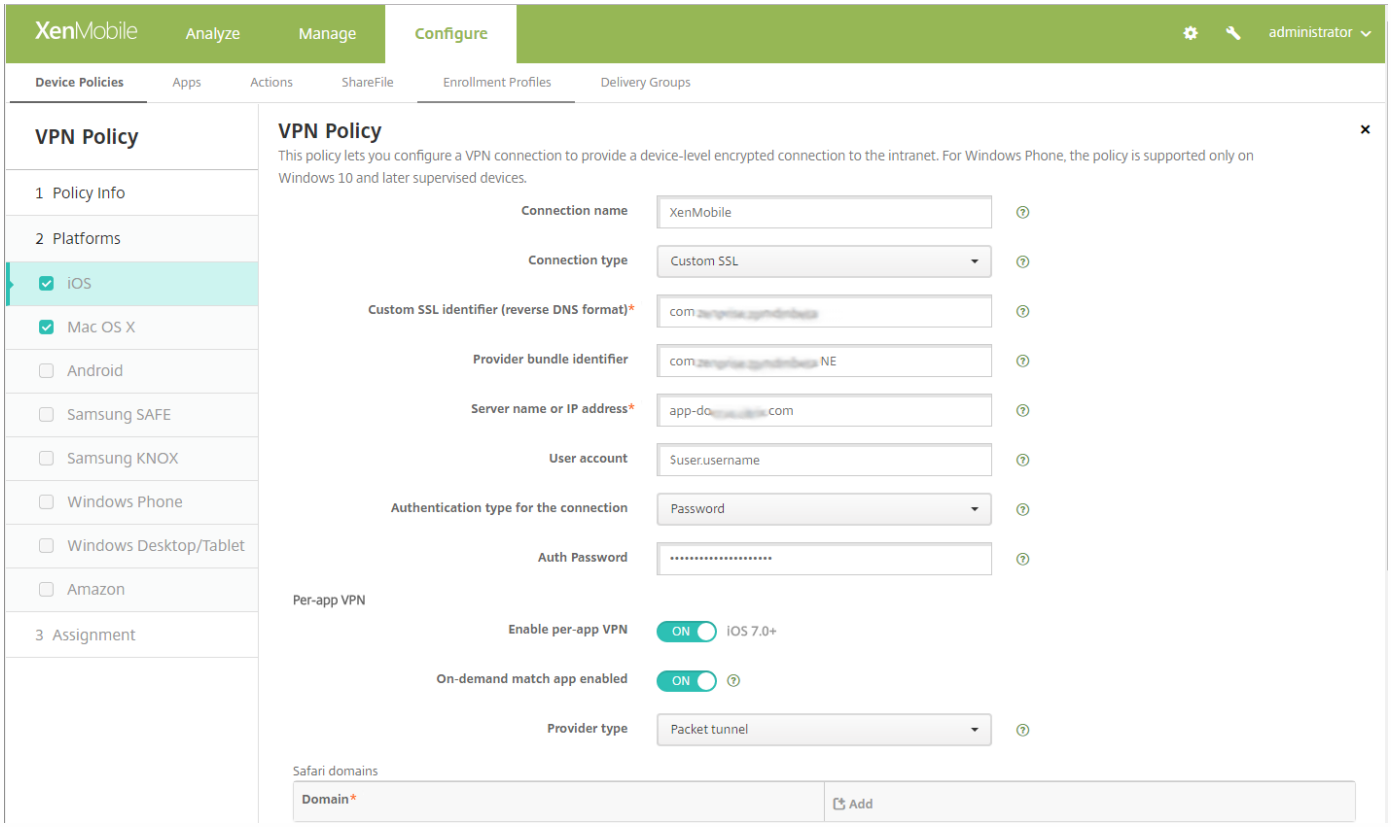
- **Identificador de pacote de provedor**: se o aplicativo especificado em **Identificador SSL personalizado** tiver vários provedores VPN do mesmo tipo (proxy de aplicativo ou túnel de pacote), especifique esse identificador de pacote.
- **Tipo de provedor**: um tipo de provedor indica se o provedor 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**. Essa opção está visível quando **Ativar VPN por aplicativo** for **I**.

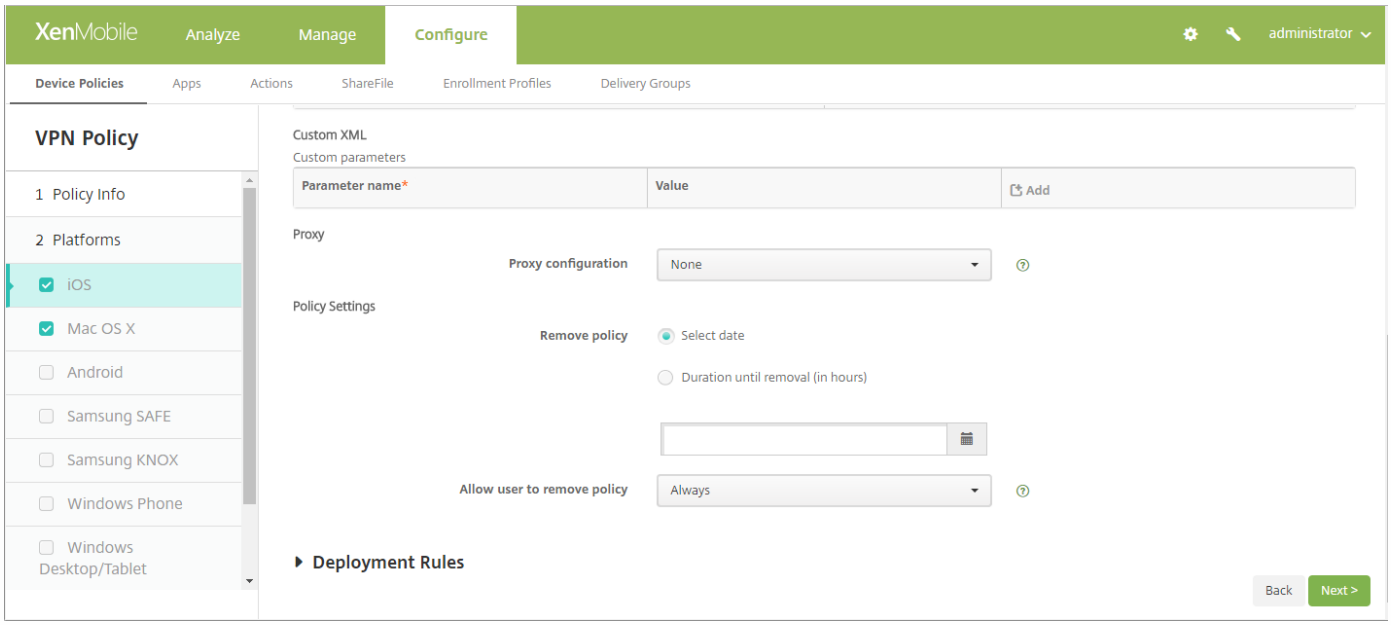
Estão disponíveis opções de VPN por aplicativo para esses tipos de conexão: Cisco AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix VPN e SSL personalizado.

Para configurar uma VPN por aplicativo:

1. Em **Configurar > Políticas de dispositivo**, crie uma política de VPN. Por exemplo:

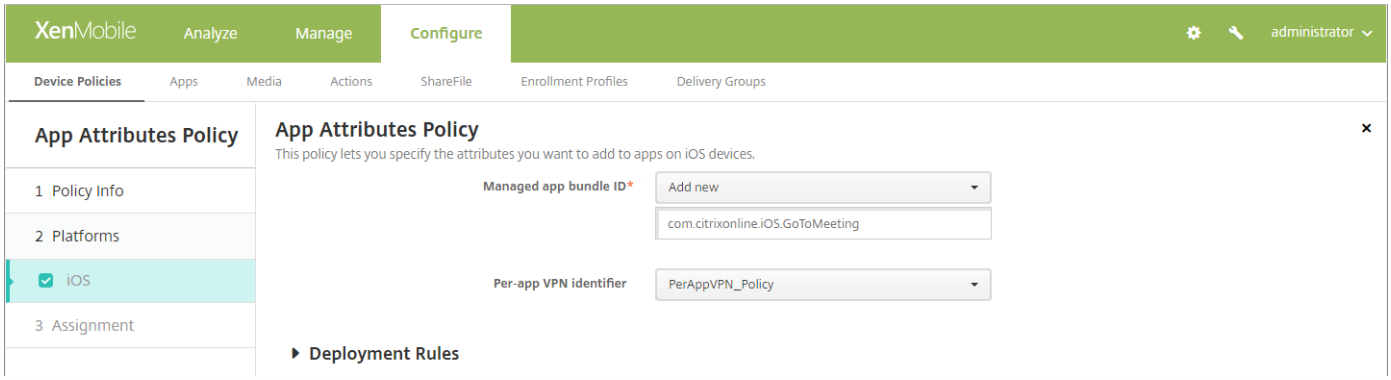
© 1999-2017 Citrix Systems, Inc. All rights reserved.





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 aplicativo. (Se você implantar um política de inventário de aplicativos iOS, a lista de aplicativos contém aplicativos).

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Mais opções de restrição de recursos para dispositivos macOS

A política de restrições de dispositivo tem as seguintes opções adicionais para macOS. Por padrão, o XenMobile permite esses recursos.

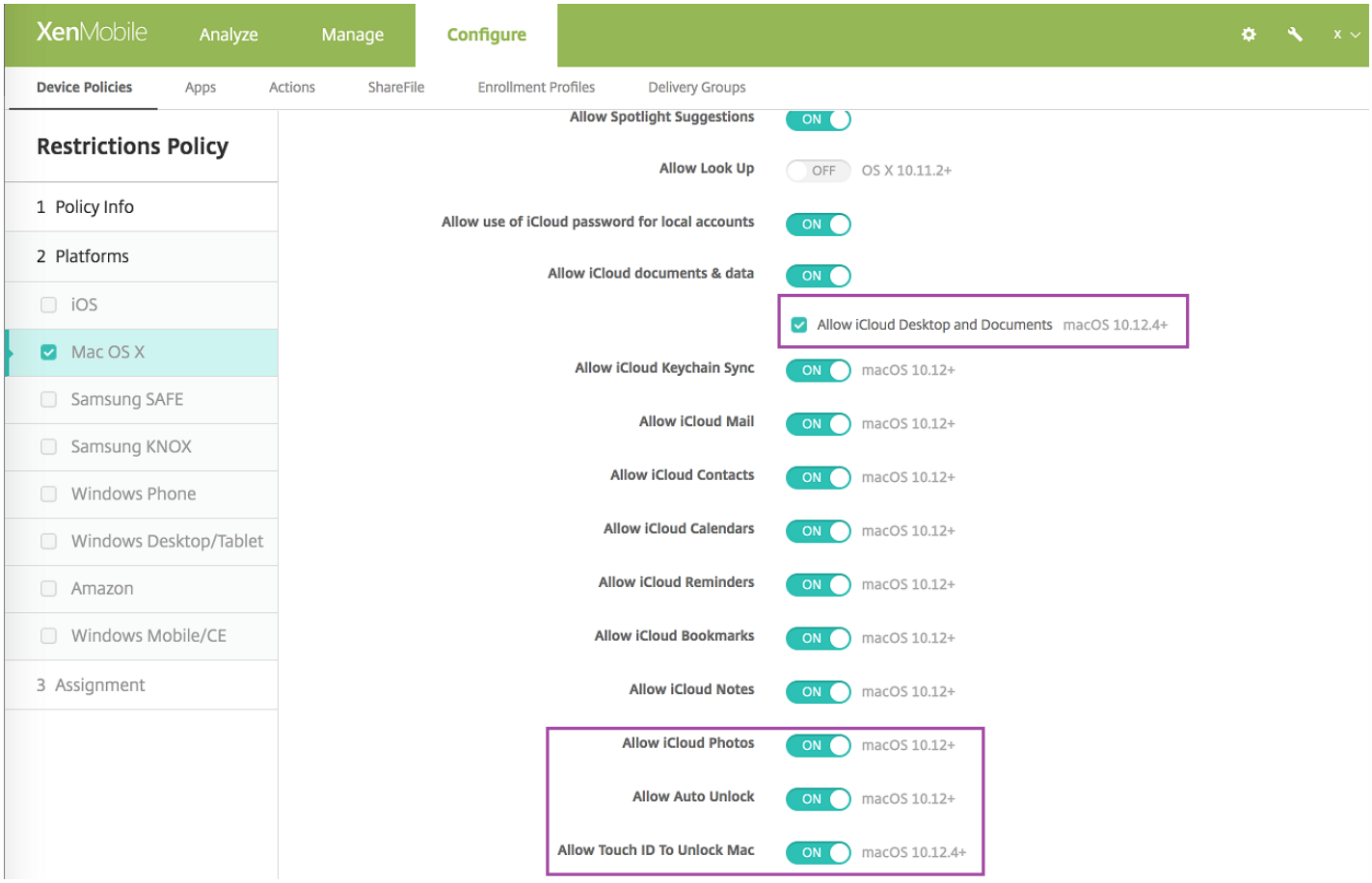
Para macOS 10.12.4 e versões posteriores:

- Permitir Touch ID desbloquear Mac
- Permitir iCloud área de trabalho e documentos

Para macOS 10.12 e versões posteriores:

- Permitir fotos do iCloud
  Se você alterar essa configuração para **Off**, as fotos não totalmente baixadas da biblioteca de fotos do iCloud são removidas do armazenamento do dispositivo local.
- Permitir desbloqueio automático
  Para obter informações sobre essa opção e o Apple Watch, consulte https://support.apple.com/en-ie/HT206995.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

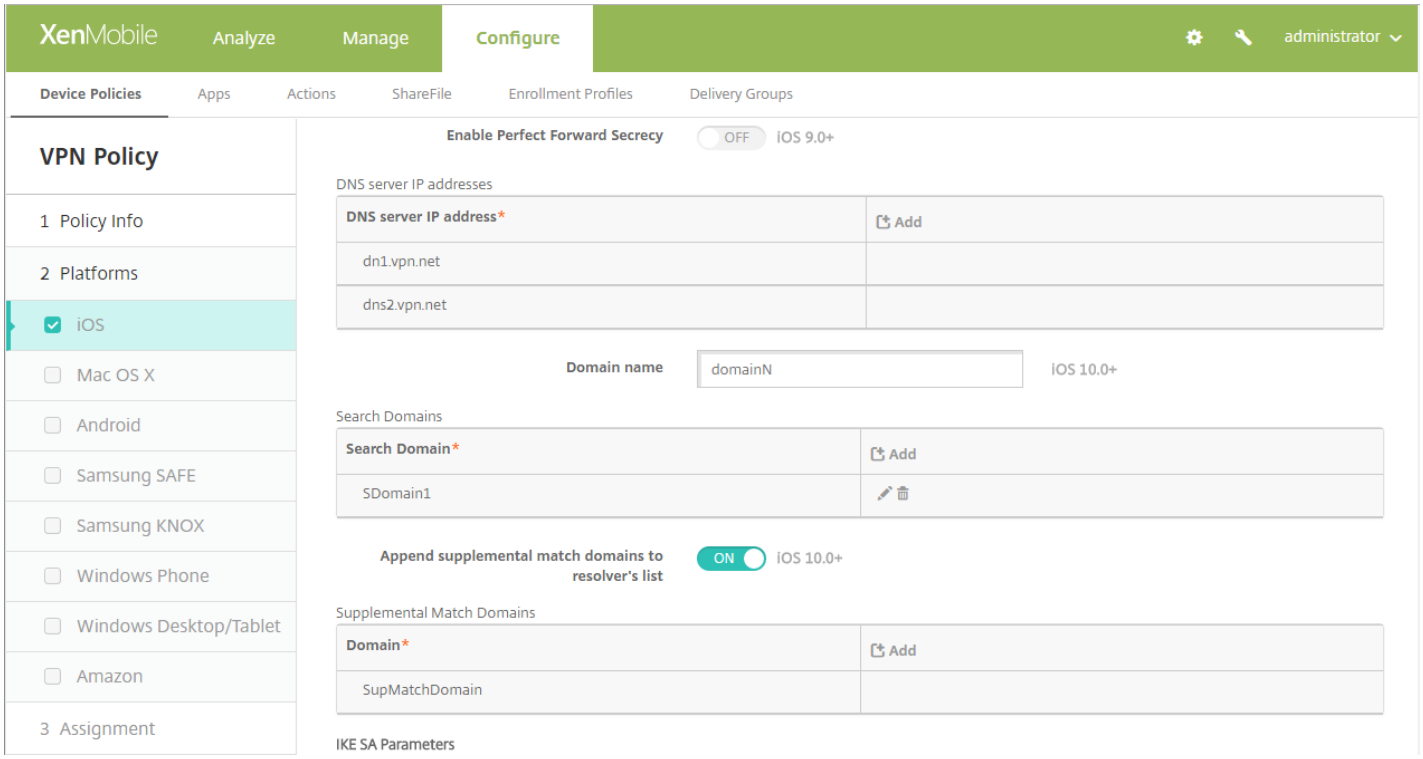


Mais parâmetros de IKEv2 para a política de dispositivo VPN

iOS 10.0

Os tipos de conexão IKEv2, AlwaysOn IKEv2 e configuração dupla de AlwaysOn IKEv2 têm mais parâmetros para iOS 10.0.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Endereços IP do servidor DNS: opcional. Uma lista de endereços IP do servidor DNS. Esses endereços IP podem incluir uma mistura de endereços IPv4 e IPv6.

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 devem ser acrescentados os domínios domínidos correspondentes suplementares aos domínidos de pesquisa para o resolvedor. **0** significa acrescentar; **1** significa que não acrescentar. O padrão é **0**.

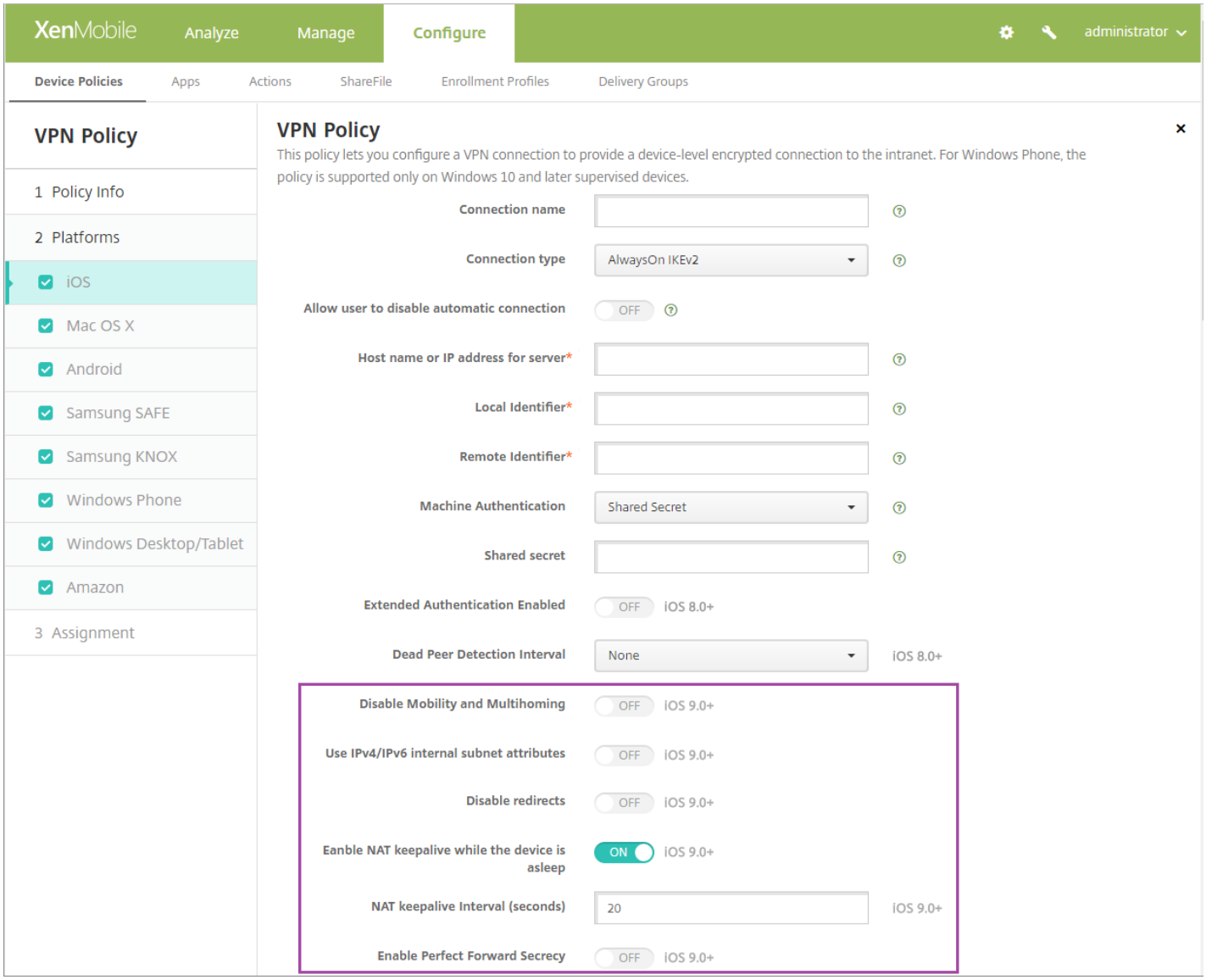
Domínios correspondentes suplementares: opcional. Uma lista de domínios usada para determinar as consultas DNS que devem usar as configurações de resolvedor DNS contidas nos endereços de servidor DNS. Essa chave cria uma configuração de DNS dividido em que somente os hosts em determinados domínios resolvem usando o resolvedor DNS do túnel. Os hosts que não estejam em um dos domínios nessa são resolvidos por meio do resolvedor padrão do sistema.

Se você salvar uma cadeia de caracteres vazia para esse parâmetro, o XenMobile usa essa cadeia de caracteres como o domínio padrão. Essa solução é como uma configuração de túnel dividido pode direcionar todas as consultas DNS primeiro para os servidores DNS VPN antes dos servidores DNS primários. Se o túnel VPN se tornar a rota padrão da rede, os servidores DNS listados serão o resolvedor padrão. Nesse caso, a lista de domínios correspondentes suplementares é ignorada.

iOS 9.0

Os tipos de conexão IKEv2, AlwaysOn IKEv2 e configuração dupla de AlwaysOn IKEv2 têm mais parâmetros para iOS 9.0.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Esses parâmetros se aplicam a todos os três tipos de conexão de IKEv2:

- **Desativar mobilidade e multihoming**
- **Use atributos de sub-rede interna IPv4/IPv6**
- **Desativar redirecionamentos**
- **Ativar Perfect Forward Secrecy**

Os dois tipos de conexão AlwaysOn IKEv2 também incluem:

- **Ativar NAT keepalive enquanto o dispositivo estiver no modo de suspensão**

  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 WiFi e 110 segundos via rede celular. Você pode alterar o intervalo usando o parâmetro **Intervalo de NAT keepalive**.

- **Intervalo de NAT keepalive (segundos)**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

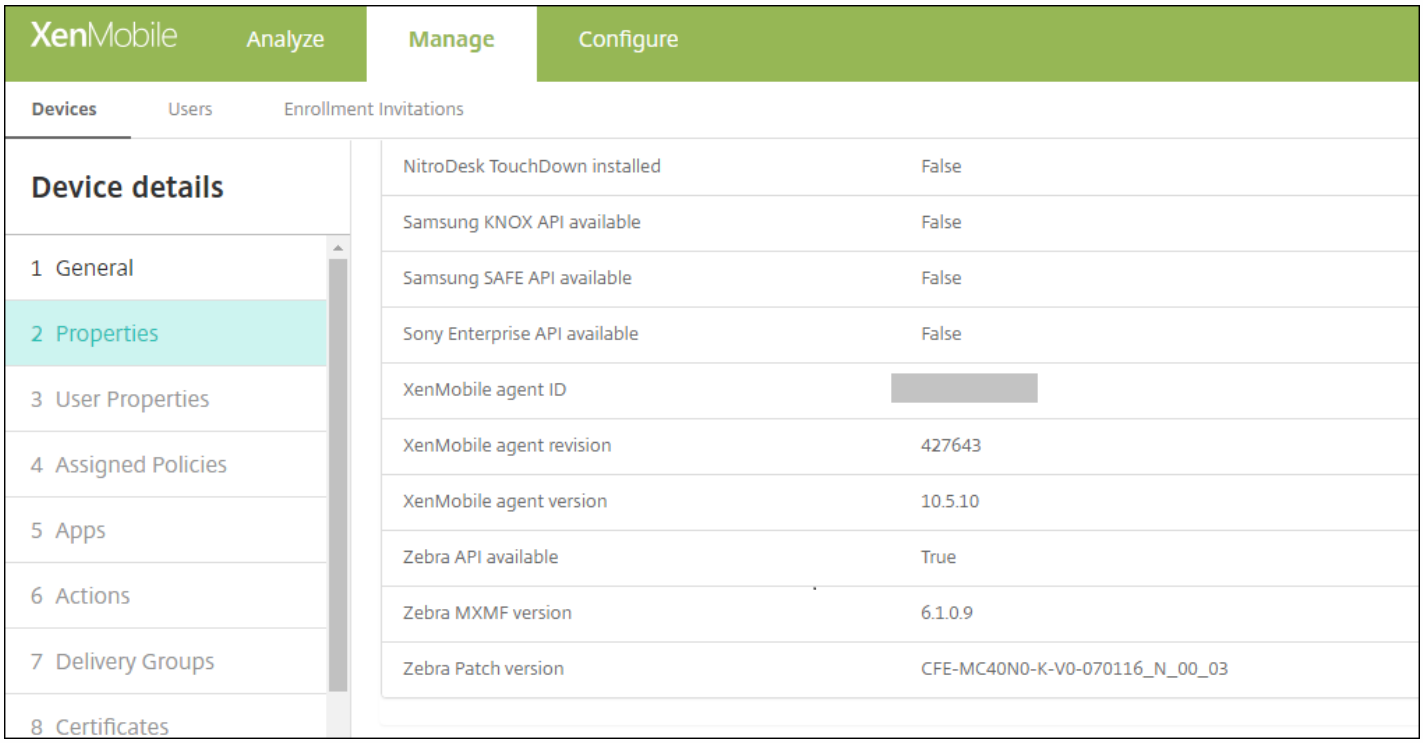
Padrão é **20** segundos.

Suporte para dispositivos móveis Zebra reforçados baseados em Android

O XenMobile agora oferece suporte a usuários com dispositivos com Android Zebra.

Importante: os dispositivos Zebra devem instalar o Secure Hub 10.5.10 para se registrar no XenMobile.

No console XenMobile, quando você gerenciar um dispositivo Zebra, várias propriedades são exibidas em **Gerenciar > Dispositivos**, em **Detalhes do dispositivo**, lista **Propriedades**.

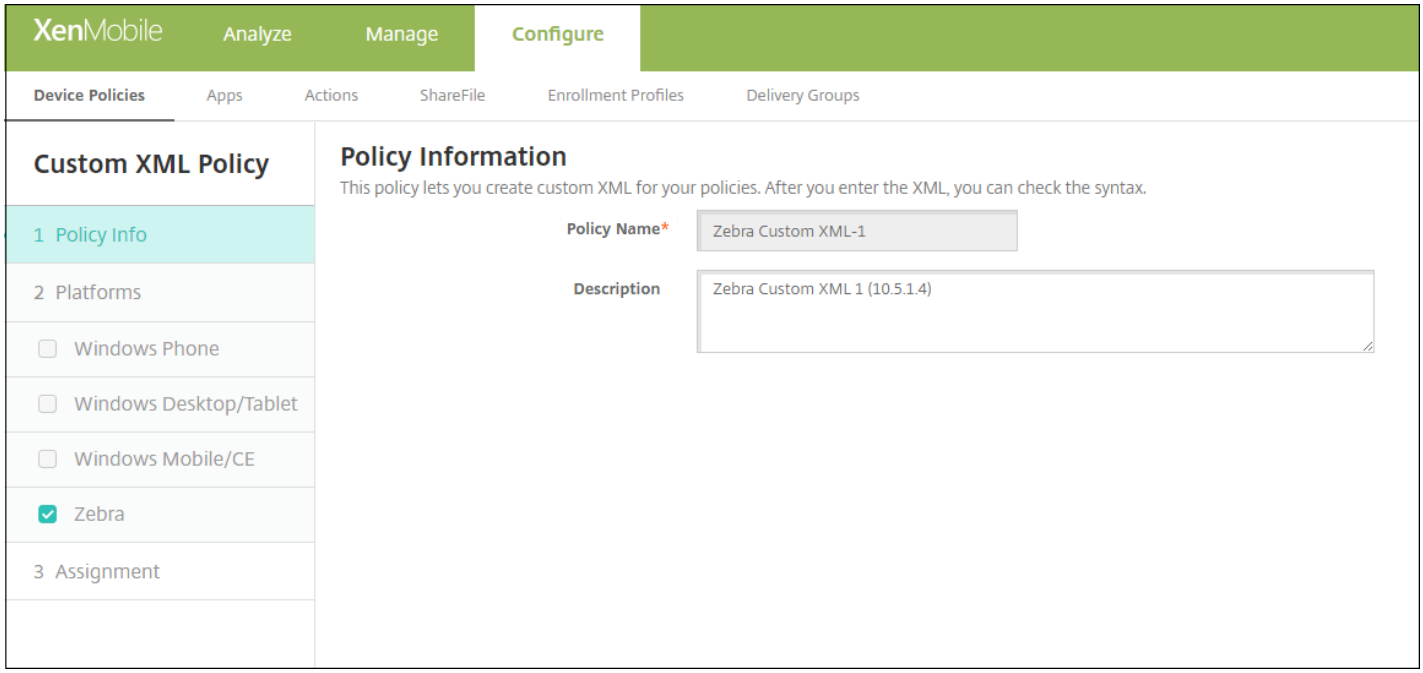


- **Zebra API**: indica que o dispositivo contém a API Zebra.
- **Versão Zebra MXMF**: indica o MX Management Framework (MXMF) disponível para a expor APIs e configurar e gerenciar dispositivos baseados em Zebra Android.
- **Versão do patch Zebra**: indica a versão de patch atualmente instalada no dispositivo.

Para obter mais detalhes sobre os dispositivos Zebra, consulte a documentação da Zebra Technologies.

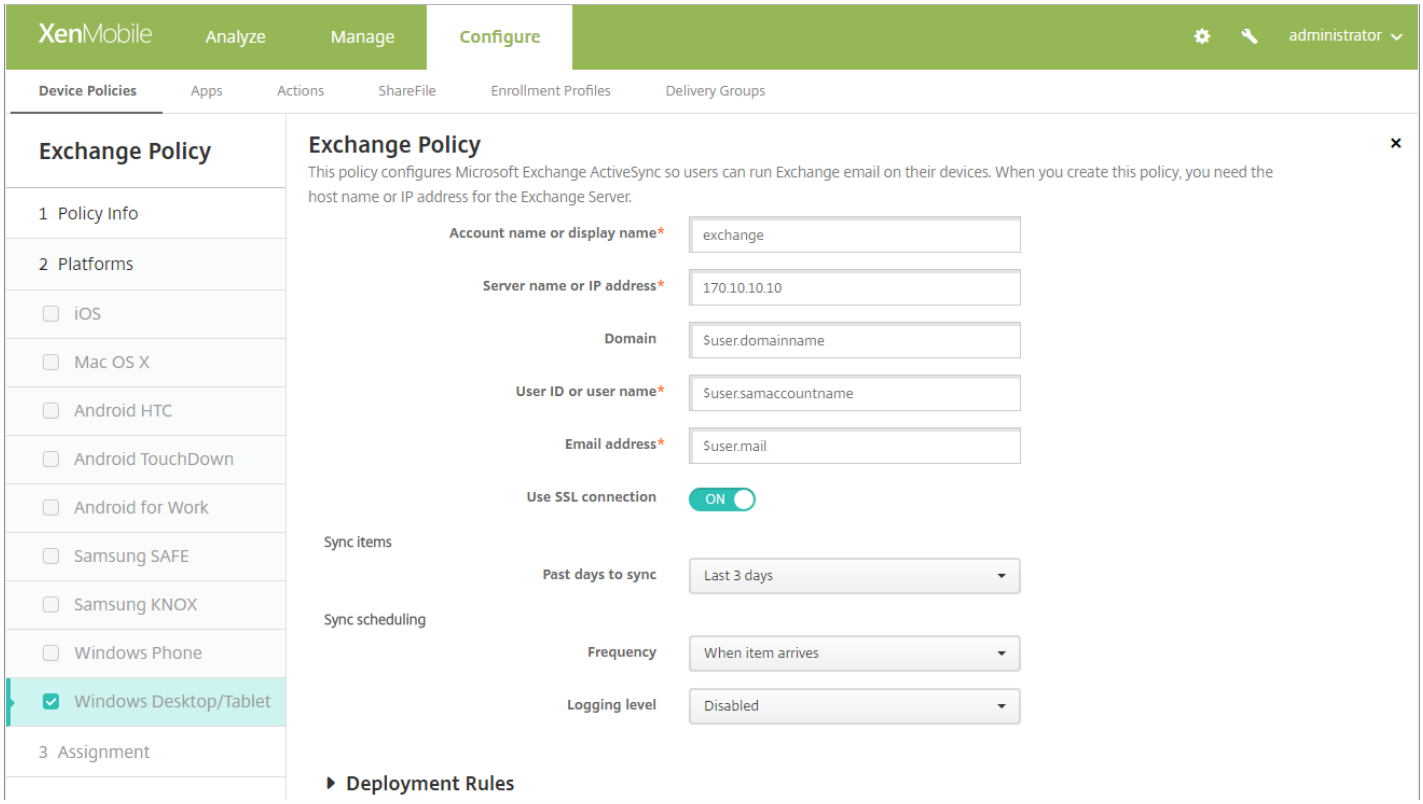
A política de MDM **XML personalizado** também está disponível para a plataforma Zebra.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Outras melhorias

- **A política do Exchange agora está disponível para o Windows 10 para Tablet.** Para adicionar a política, acesse **Configurar > Políticas de dispositivo**. As configurações são as mesmas que para o Windows 10 Phone. Para obtes os detalhes da configuração, veja Política de dispositivo do Microsoft Exchange ActiveSync.



- **Os nomes de usuário do Active Directory agora são armazenados com letras minúsculas.** A partir desta versão, o XenMobile armazena todos os nomes de usuário do Active Directory com letras minúsculas. Esta alteração se aplica a

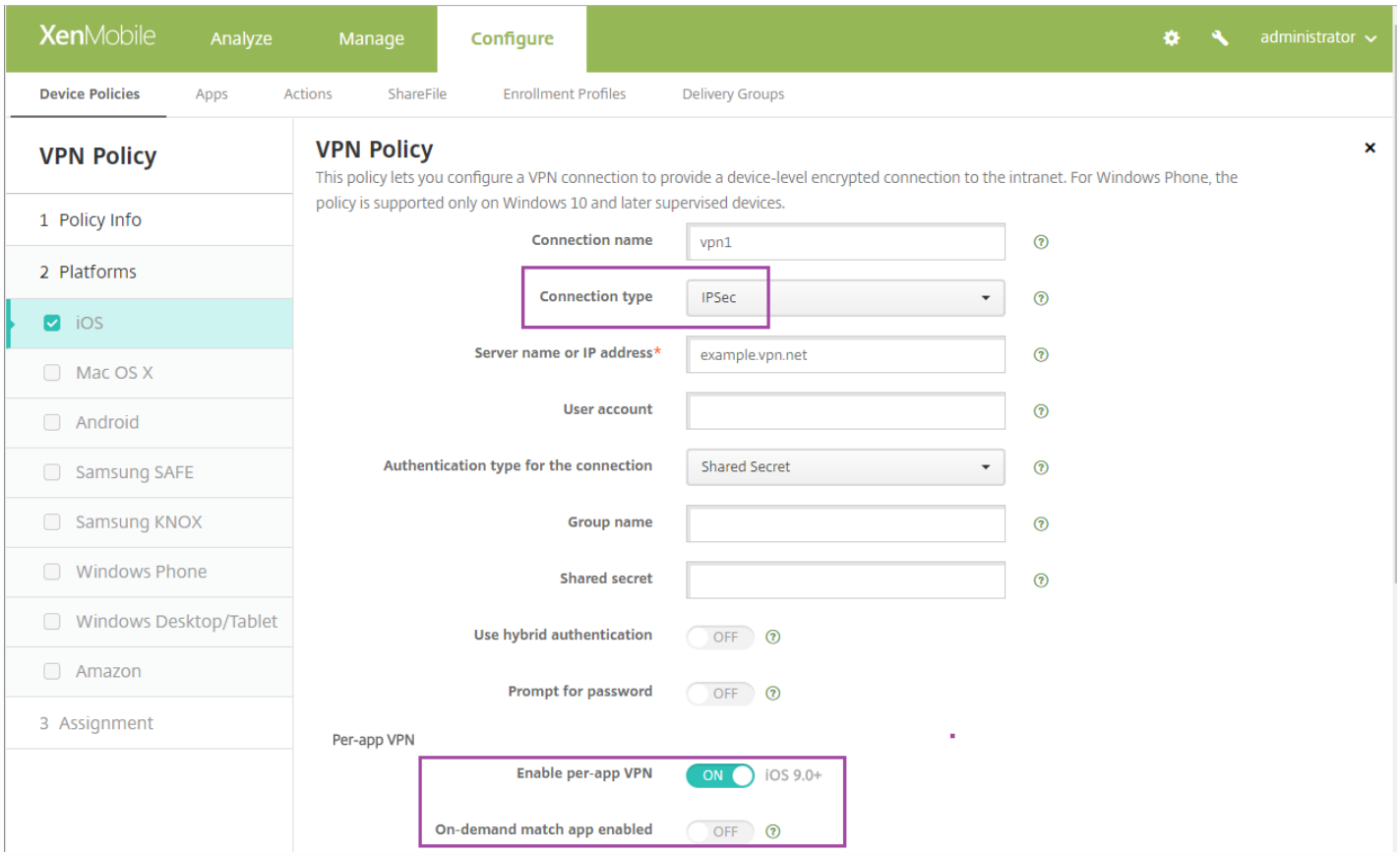
© 1999-2017 Citrix Systems, Inc. All rights reserved.

usuários do Active Directory no banco de dados XenMobile quando esse é atualizado e a novos usuários do Active Directory. Esta alteração não se aplica a nomes de usuário locais.

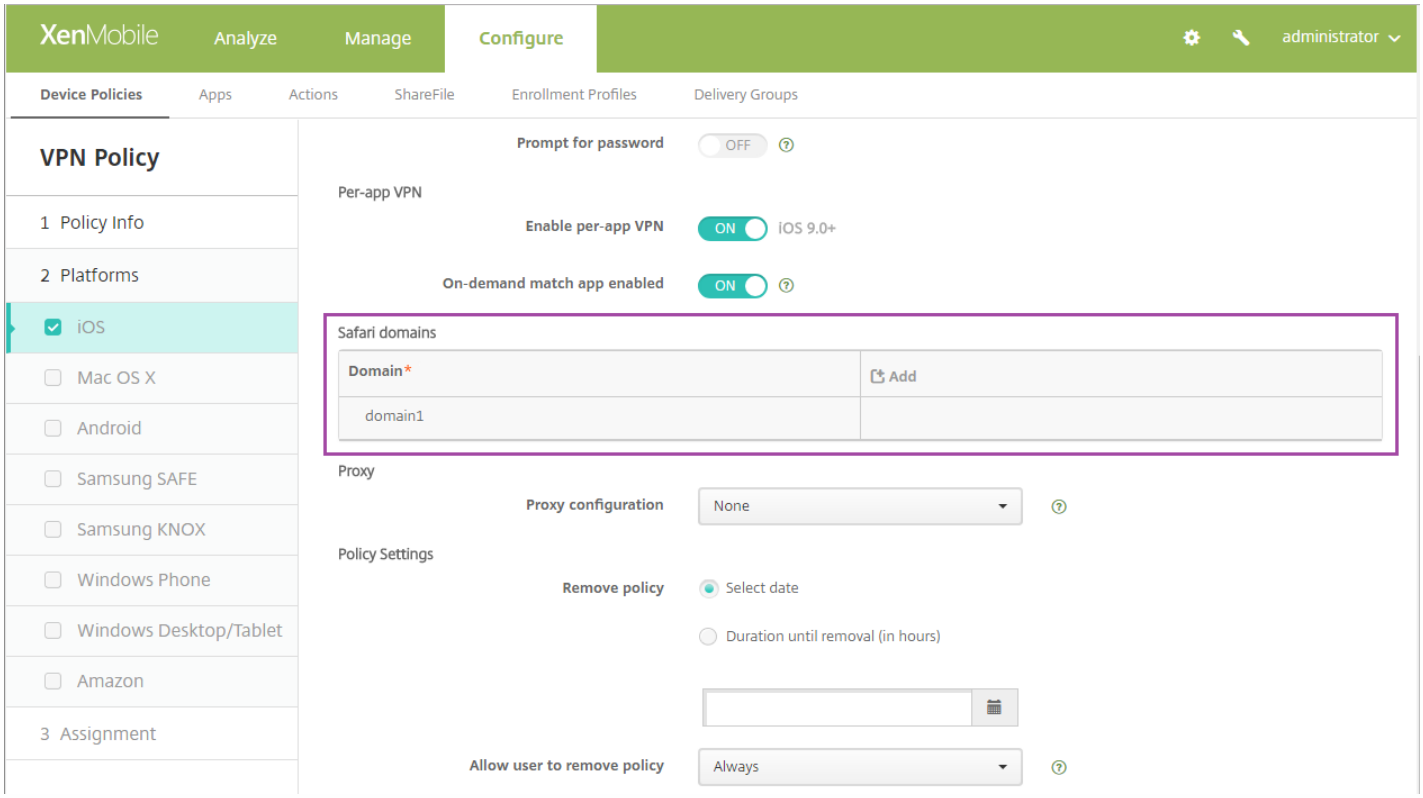
- **O carregamento de páginas, filtragem, classificação e consultas de busca de dispositivo agora são três vezes mais rápidos.** Essa otimização é resultado da separação da contagem de dispositivo e otimização de consulta ao consultar para obter uma lista de dispositivos com base em um determinado critério. O XenMobile Server pode agora obter contagens de dispositivos de forma dinâmica.

- **A política a VPN para dispositivos iOS agora tem opções de VPN por aplicativo para o tipo de conexão IPSec.** Os dispositivos iOS 9.0 e versões posteriores oferecem suporte a VPN por aplicativo para conexões de IPSec. O Netskope e outros Cloud Access Security Brokers (CASBs) podem recomendar conexões VPN por aplicativo para IPSec.

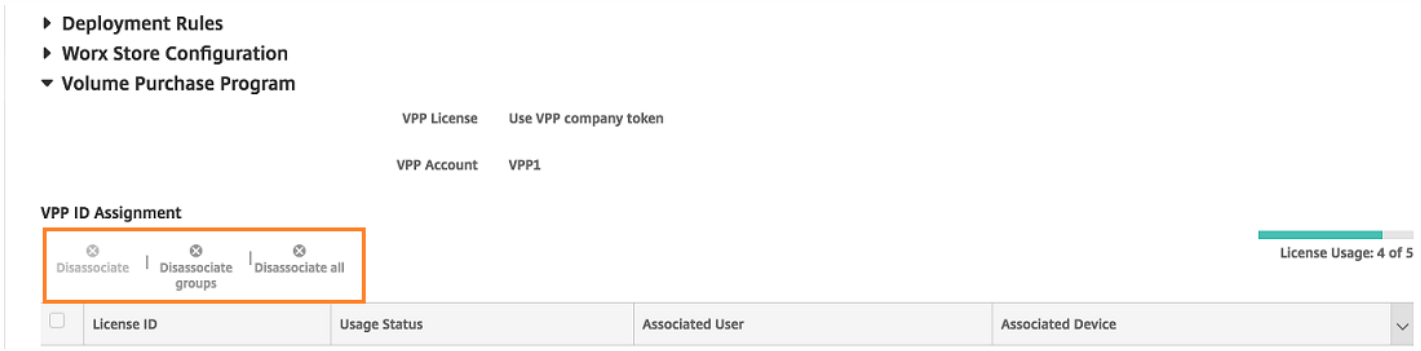
  As opções de VPN por aplicativo são **Ativar VPN por aplicativo**, **Correspondência de aplicativo sob demanda ativada**, e **Domínios do Safari**.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

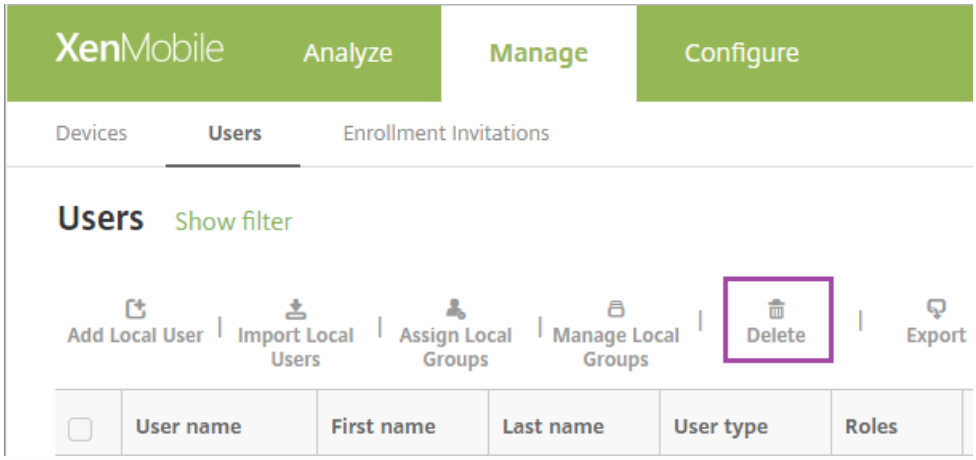


- Revogação de licença Volume Purchase Program da Apple para **iOS por grupos de usuários ou em massa**. Agora, você pode desassociar também licenças Volume Purchase Programe para grupos de usuários ou para todas as atribuições para liberar licenças em massa.



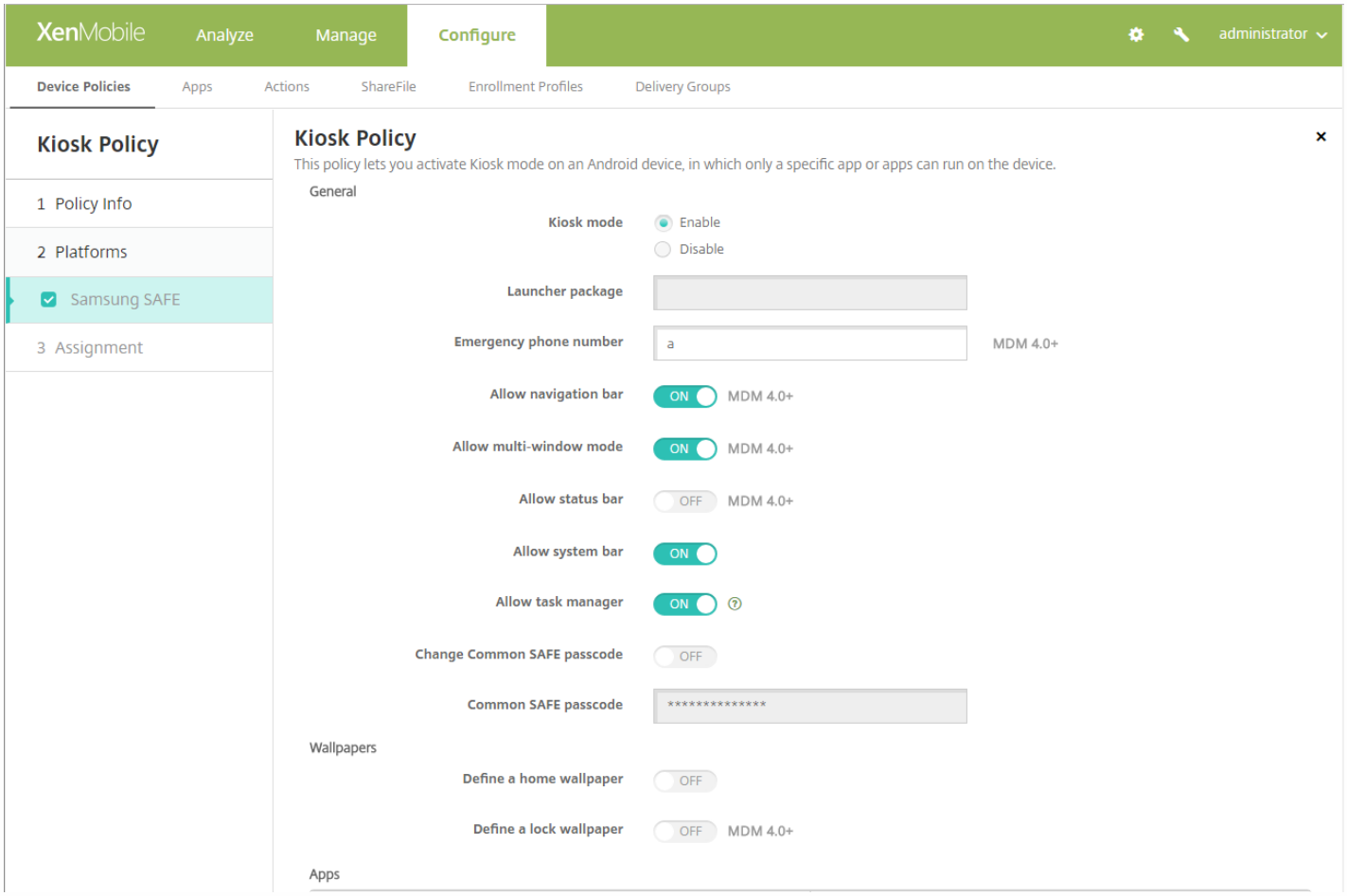
- **Excluir vários usuários do Active Directory ao mesmo tempo**. A barra de menu que é exibido quando você seleciona um ou mais usuários do Active Directory agora inclui o comando **Excluir**. Anteriormente, o comando **Excluir** aparecia somente no menu do botão direito do mouse para um único usuário.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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**.

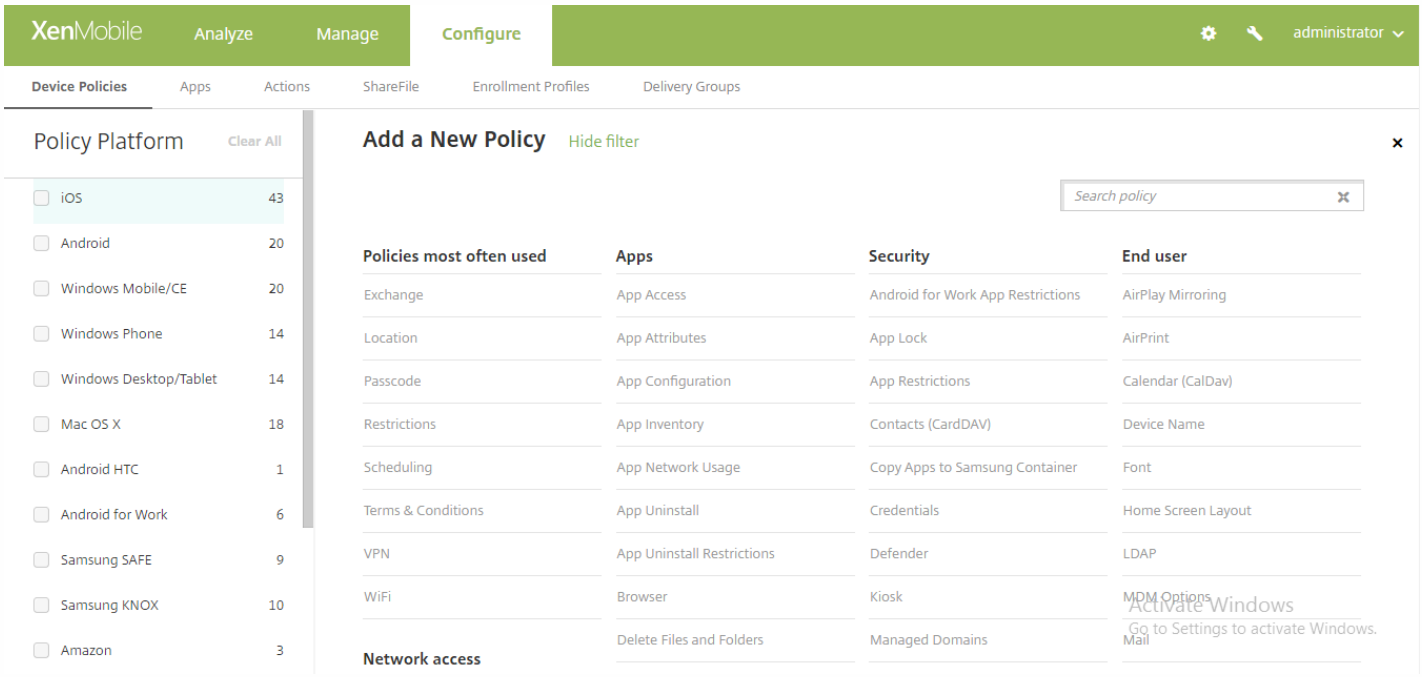
- **Controlar se o campo de código secreto SAFE comum é editável**. Para evitar alterações inadvertidas ao **código secreto SAFE comum**, a política de quiosque tem uma nova configuração, **Alterar código secreto SAFE comum**. Por padrão, a nova configuração é **O**. Para alterar o código secreto, defina **Alterar código secreto SAFE comum** para **I** e, em seguida, digite um valor para o código secreto.



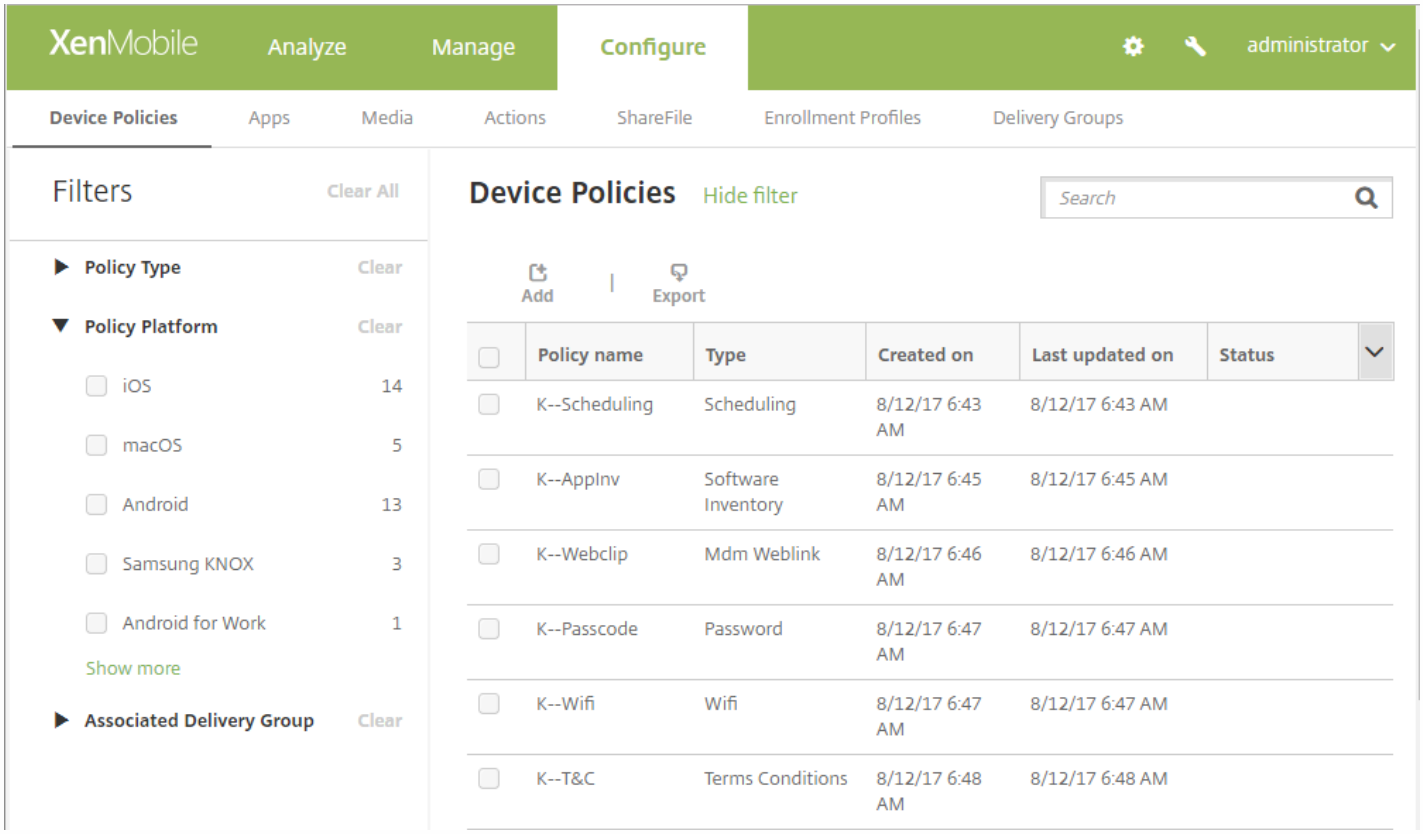
- **Filtrar a lista de política de dispositivo ao adicionar uma política**. Na página **Configurar > Políticas de dispositivo**, quando você clica em **Adicionar**, agora é exibida a seguinte página. Você pode procurar uma política por nome, como antes. Você também pode filtrar a lista para exibir as políticas de dispositivo para plataformas selecionadas.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

A página **Adicionar uma nova política** inicialmente mostra uma lista de dispositivos filtros de políticas e plataforma.

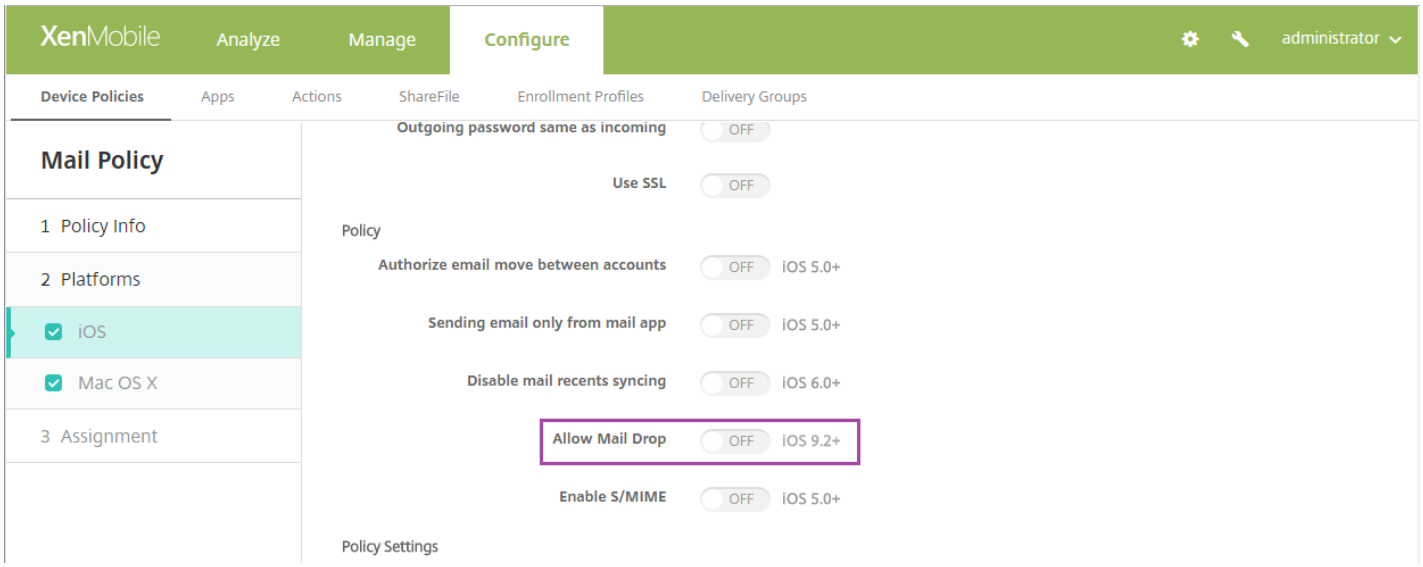


Clique em uma ou mais plataformas para exibir uma lista das políticas de dispositivo para as plataformas selecionadas. Clique em um nome de política para continuar adicionando a política.

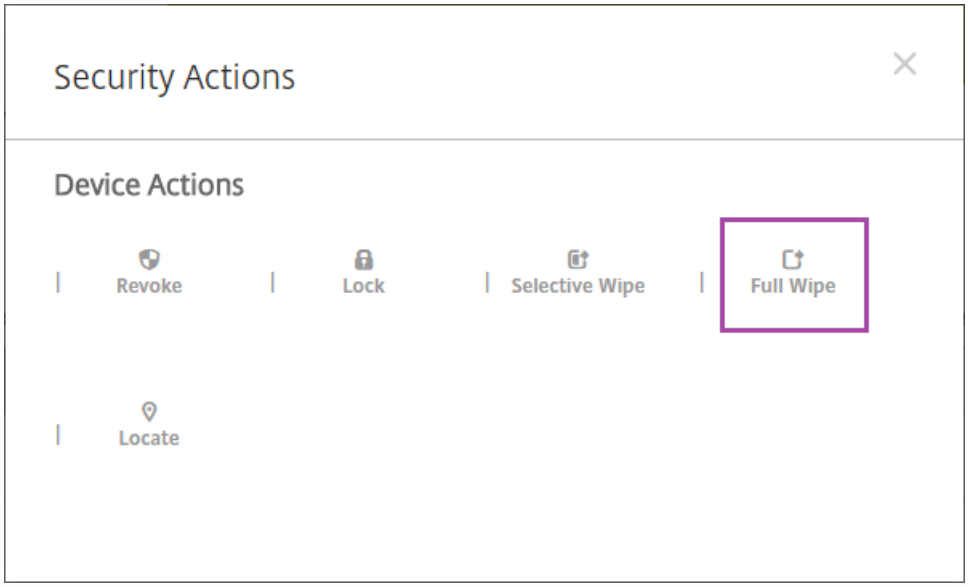


- **Suporte Apple Mail Drop adicionado à política de dispositivo de email**. Agora você pode permitir o uso do Apple Mail Drop para dispositivos que executam iOS 9.2 e versões posteriores. O Mail Drop permite que os usuários carreguem arquivos que são grandes demais para enviar como um anexo de email. Os usuários podem carregar arquivos até 5 GB e, em seguida, usar o aplicativo de email no seu dispositivo iOS para enviar um link ou uma visualização para os destinatários.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- **Detalhes do dispositivo registrados em log para um apagamento ou o bloqueio de dispositivos somente MAM**. Quando um dispositivo somente MAM é apagado ou bloqueado, os logs do XenMobile agora incluem o nome de usuário e a ID do dispositivo.
- **Suporte para o Windows 10 RS2**. Certificamos o XenMobile 10.5.3 e 10.5.2 com Windows 10 RS2 Phone e Tablet. XenMobile 10.5.1, 10.5.0, 10.4 e 10.3.x são compatíveis com Windows 10 RS2 Phone e Tablet.
- **Apagamento completo de dispositivos Tablet e Windows Desktop**. Agora você pode executar um apagamento completo para eliminar todos os dados pessoais e corporativos e aplicativos de um dispositivo Windows desktop oui tablet. Em **Gerenciar > Dispositivos**, selecione um dispositivo Windows Desktop/Tablet, clique em **Segurança** e, em seguida, clique em **Apagamento completo**. Em um dispositivo desktop, o apagamento remoto aciona o comando **Redefinir este PC** do Windows com a opção **Remover tudo**.



Depois de clicar em **Apagamento completo**, a lista **Ações do dispositivo** inclui **Cancelar o apagamento**. Você pode cancelar um apagamento antes que o XenMobile implante a solicitação de apagamento.

Os usuários também podem apagar o dispositivo Windows desktop ou tablet no portal de autoajuda.

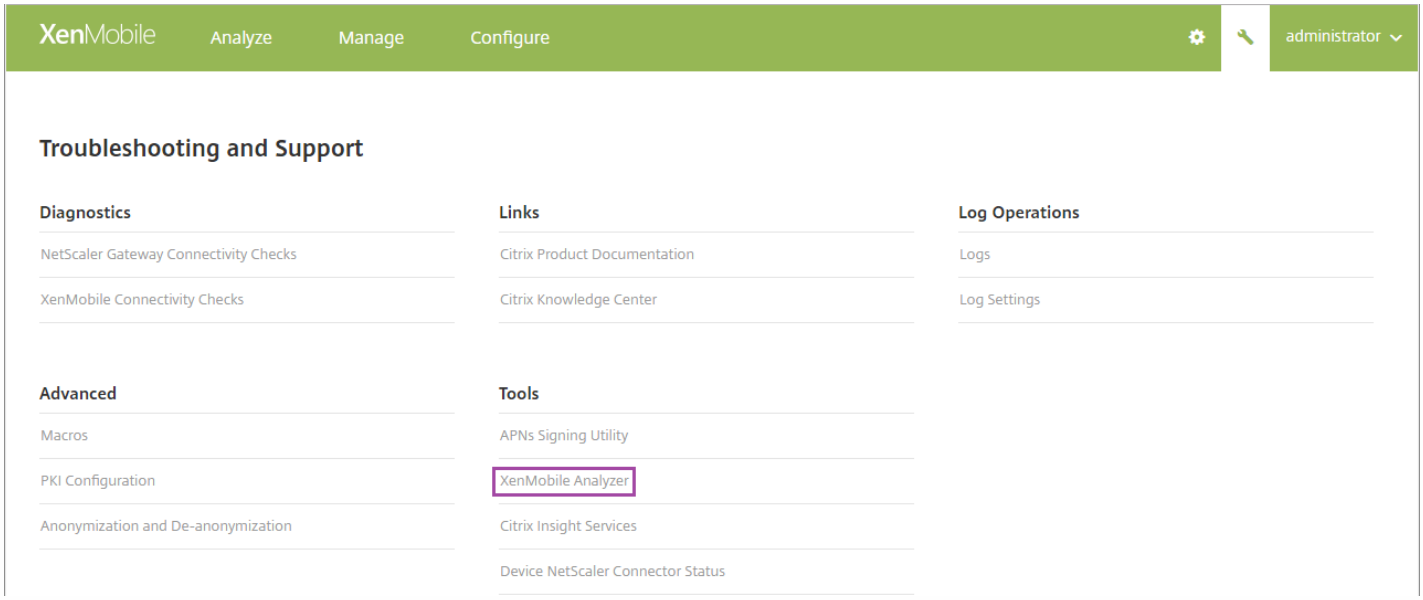
Os logs de XenMobile incluem eventos de apagamento e de cancelamento do apagamento.

- A opção **Duração até a opção de remoção** para todas as políticas de dispositvos iOS foram alteradas de dias para

© 1999-2017 Citrix Systems, Inc. All rights reserved.

horas. Esta versão mais recente do XenMobile converte os valores existentes em horas.

- **Melhor desempenho de consultas do dispositivo e expansão de filtro de dispositivo**. O XenMobile agora manipula consultas para contagens de filtro de dispositivo separadamente de consultas de dispositivo. Quando você expandir um filtro na página **Gerenciar > Dispositivos** são exibidos cataventos em vez de filtro de contagem até que a contagem esteja disponível.
- A página **Solução de problemas e suporte** agora inclui um link para o XenMobile Analyzer.



- **Nova opção CLI do XenMobile para especificar protocolos SSL**. Agora você pode usar o CLI para especificar quais protocolos de SSL o XenMobile usa. Os protocolos permitidos são:
  - TLSv1.2
  - TLSv1.1
  - TLSv1

  Por padrão, o XenMobile ativa cada um desses protocolos de SSL. Quando você altera a configuração de protocolo SSL, deve reiniciar o XenMobile Server.

  Para ativar ou desativar protocolos:

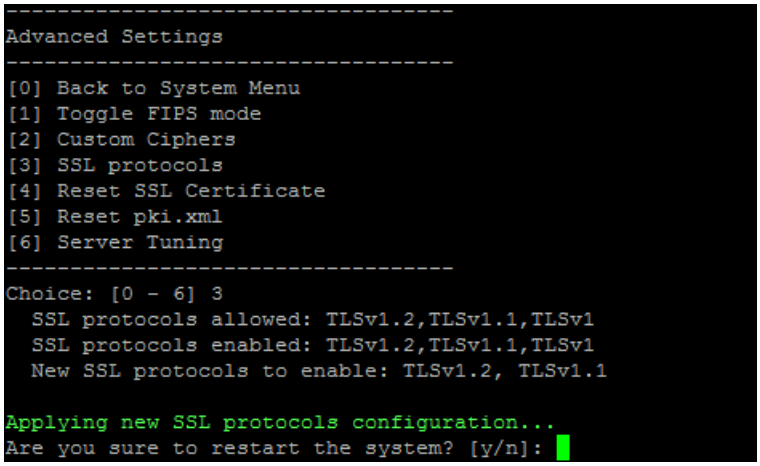
1. Abra a CLI do XenMobile, escolha **[2] System** e escolha **[12] Advanced Settings**.

```
********************** 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
---------------------------------
```

2. Escolha **[3] SSL protocols**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Após o aviso de **Ativar novos protocolos de SSL**, 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, em seguida, digite **y** para reiniciar o XenMobile Server.



Problemas resolvidos

O XenMobile 10.6 inclui os seguintes problemas resolvidos. Os problemas resolvidos da Ferramenta de atualização são exibidos em "Ferramenta de atualização do XenMobile", posteriormente neste artigo.

Para ver os problemas corrigidos relacionados aos XenMobile Apps, consulte Problemas corrigidos.

Quando os usuários se registram no XenMobile usando uma conta do Azure Active Directory, mesmo após o apagamento ou a revogação do dispositivo, eles podem se registrar novamente sem autorização. Esse é um problema de terceiros. [#628865, CXM-23203]

Após a atualização para o XenMobile Server 10.4:

- Se você clicar na guia **ShareFile**, talvez a página seja carregada, e as informações não serão exibidas.
- Se você tentar adicionar ou editar um grupo de entrega, a seguinte mensagem de erro poderá ser exibida: 500 Erro de servidor interno. [#663344, #663788, CXM-19085]

Se uma tabela de usuários ou convites para registro tiver várias páginas e você editar um item na segunda página ou na página seguinte, depois que você salvar a alteração, o XenMobile mostrará a primeira página da tabela e descartará as atualizações. [CXM-20209]

Se você mover um StorageZone Connector do grupo de entrega A para o grupo de entrega B, os usuários do ShareFile para iOS no grupo de entrega A poderão continuar a usar o conector. [CXM-21860]

Ao integrar o StoreFront com o XenMobile e implantar aplicativos HDX, depois que você altera uma senha do Active Directory, os aplicativos HDX desaparecem da XenMobile Store. [CXM-9859, CXM-22821]

Se uma tabela de usuários ou convites para registro se expandir por várias páginas, e você editar um item na segunda página ou na página seguinte, depois que você salvar a alteração, o XenMobile mostrará a primeira página da tabela e descartará as atualizações. [CXM-20209]

Se você remover usuários do Active Directory de um grupo com permissões para StorageZone Connectors, os usuários do

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ShareFile para iOS ainda poderão acessar Compartilhamentos de rede associados. Para solucionar esse problema, reinstale o aplicativo ShareFile para iOS. [CXM-21859]

Você não pode criar um pacote de suporte usando a interface de linha de comando do XenMobile. Como solução alternativa, use o console XenMobile: vá para **Suporte > Criar pacotes de suporte** e clique em **Criar**. [CXM-23091]

Para uma tabela de dispositivos com várias páginas no console XenMobile: depois que você salva uma edição em um item na segunda página ou na página seguinte, o XenMobile mostra a primeira página da tabela e descarta as atualizações. [CXM-23143]

Os downloads de aplicativos para implantações do MAM em dispositivos iOS e Android podem falhar. [CXM-23280]

Se o valor da propriedade de servidor **StorageZone Connectors supported** for **NOT SUPPORTED** e você configurar o ShareFile no console XenMobile, depois de navegar até uma página diferente e, em seguida, voltar para a página **Configurar > ShareFile**, a página do ShareFile não mostrará a configuração, embora ela esteja salva. Para solucionar esse problema, altere a propriedade de servidor, **Tipo de configuração do ShareFile**, para **EMPRESARIAL**. [CXM-23337]

Quando você configura uma política de dispositivo para Proteção de informações do Windows e habilita a configuração **Revogar o certificado WIP ou cancelar registro**, depois de apagar seletivamente uma conta de tablet do Windows 10, os usuários são capazes de acessar um arquivo seguro. Além disso, o arquivo não está criptografado conforme o esperado. Essa condição é um problema com o tablet Windows 10 RS1. [CXM-23362]

Para dispositivos que se conectam a um nó de cluster: quando você implanta políticas e aplicativos de outro nó de cluster, ocorrem problemas de cluster. [CXM-23737]

Quando os usuários cuja propriedade sAMAccountName é diferente do prefixo UPN no Active Directory tentam registrar seus dispositivos usando a URL de convite: o XenMobile tenta resolver sAMAccountName@domainname como o UPN e o registro falha. Como solução alternativa, no console XenMobile, crie convites por usuário em vez de por grupo. [CXM-24223]

Quando o XenMobile consulta o Active Directory para um grupo de usuários e recebe uma resposta vazia sem erros, ele interpreta a resposta de forma a indicar que o grupo está excluído do Active Directory. Em seguida, o XenMobile exclui o grupo de usuários do seu banco de dados, fazendo com que esses usuários percam o acesso. [CXM-24228]

O servidor Syslog não mostra o nome do aplicativo para downloads de aplicativos. [CXM-24620]

Se você criar um nome de função RBAC que inclui um E comercial (&), esse símbolo será codificado, e não será possível editar o nome. [CXM-24621]

Para uma política de dispositivo Webclip do XenMobile, se o nome e a URL incluírem caracteres especiais HTML, como o E comercial (&), o XenMobile codificará esses caracteres. Como resultado, a URL se quebrará quando você implantar a política em dispositivos gerenciados. [CXM-24622]

Quando você adiciona um aplicativo público da Google Play Store ao console XenMobile, a função de pesquisa de aplicativos não passa pelo proxy conforme esperado, e a pesquisa não retorna os aplicativos corretos. [CXM-24894]

Na página **Gerenciar > Dispositivos** do console XenMobile, classificar de acordo com as colunas **Dias de inatividade** e **Último acesso** na tabela resulta em um erro. [CXM-24895]

Para dispositivos Windows 10 registrados por meio do Azure Active Directory durante a instalação inicial do dispositivo, não é possível executar um apagamento seletivo do dispositivo no console XenMobile. Esse problema é uma limitação da Microsoft. [CXM-24899]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Poderão ocorrer problemas ao carregar alguns tokens do VPP em uma nova instalação do XenMobile 10 ou ao migrar alguns tokens do VPP do XenMobile 9 para o XenMobile 10.5. [CXM-25268]

Se você incluir um E comercial (&) em uma política de dispositivo ou um nome de função RBAC, o XenMobile salvará esse nome com **&** em vez de **&**. Por exemplo, **políticaa&b** se chamará **políticaa&b**. [CXM-25630]

Depois de atribuir dispositivos a outra conta DEP, o XenMobile remove esses dispositivos de seu banco de dados. [CXM-25692]

Na página **Configurar > Políticas de dispositivo** da política de dispositivo de VPN, as configurações a seguir são opcionais, embora a página do console indique que elas são obrigatórias (*): endereços IP do servidor DNS, Domínios de pesquisa, Domínios de correspondência suplementares. [CXM-25767]

Se você adicionar um token do VPP ao XenMobile, consumir uma licença do VPP com associação de dispositivo, excluir o token e depois adicionar o mesmo token: na tabela **Atribuição de ID de VPP** na página de configurações **Configurar > Aplicativos**, a coluna **Dispositivo associado** poderá incluir **Oculto** em vez do número de série do dispositivo. [CXM-25907]

Todas as propriedades de um dispositivo macOS registrado serão preenchidas no XenMobile somente se um grupo de entrega for associado ao dispositivo registrado e tiver um recurso implantado, como uma política. [CXM-25917]

Depois que você clica em **Adicionar** na página **Configurar > Políticas de dispositivo**, o XenMobile não filtra a lista de políticas e os resultados da pesquisa com base nas plataformas selecionadas. São exibidos somente os cinco primeiros resultados da pesquisa. [CXM-26354]

As propriedades Gerais no console VMware mostram incorretamente o sistema operacional convidado como um sistema operacional de 32 bits, em vez de 64 bits. Esse problema é resolvido quando você instala o arquivo atualizado do VMware (.ova). [CXM-28048]

Quando os usuários excluem um aplicativo do console XenMobile, esse aplicativo permanece no banco de dados. Como resultado, o console não é sincronizado com o banco de dados. [CXM-29613]

Ao filtrar um relatório por data na página **Analisar > Relatórios**, o Calendário no último acesso não é aberto depois que você clica no ícone de calendário. Como solução alternativa, clique no campo **Valor** para abrir o seletor de data. [CXM-29748]

No console XenMobile, quando você edita uma função de grupo de entrega, o nome desse grupo e o botão **Avançar** não aparecem intermitentemente. [CXM-30010]

Depois que você agrega e implanta recursos XenApp e XenDesktop no Secure Hub com a configuração associada no console XenMobile, os ícones de aplicativos HDX não aparecem na loja, e uma mensagem de erro é exibida quando os usuários iniciam os aplicativos. A mensagem é: XenApp - Falha ao obter detalhes do aplicativo. Tente novamente mais tarde. [CXM-30737]

Quando você configura e salva uma ação automatizada no console XenMobile 10.5, as Regras de implantação básicas ou avançadas não são salvas. O problema ocorre em todas as plataformas. [CXM-30742]

Em alguns ambientes do XenMobile Server em uma configuração em cluster, ocorrem problemas de alocação de memória em todos os nós. Quando esse problema ocorre, os servidores deixam de responder. [CXM-31283]

A exportação de um arquivo CSV para o widget de painel **Uso de licenças de aplicativos de VPP** resulta na alta utilização de CPU do servidor de banco de dados. [CXM-31917]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Ocasionalmente, ocorre um súbito aumento de memória e um erro de memória insuficiente em uma instância do XenMobile Server. Quando esse problema ocorre, o XenMobile Server deixa de responder. [CXM-31959]

Na página **Configurações > Registro de dispositivo do Apple Configurator**, depois que você altera uma configuração e clica em **Salvar**, é exibida uma mensagem de erro de servidor interno. O XenMobile salva as alterações. [CXM-32446]

No XenMobile, na página **Configurações > Credenciais do Google Play**: depois que você digita as configurações e clica em **Salvar**, a mensagem "Email ou senha incorreta" é exibida de modo intermitente. Esse erro ocorre devido a uma atualização do Google. [CXM-32847]

Ferramenta de Atualização do XenMobile

Após a atualização do XenMobile 9 para o XenMobile 10.4, os dispositivos Windows estão no modo MDM em vez de no modo MAM+MDM. Além disso, a XenMobile Store não abre. Como solução alternativa, os usuários podem registrar novamente um dispositivo migrado. [CXM-18532]

Poderão ocorrer problemas ao carregar alguns tokens do VPP em uma nova instalação do XenMobile 10 ou ao migrar alguns tokens do VPP do XenMobile 9 para o XenMobile 10.5. [CXM-25268]

Após uma atualização do XenMobile 9 para o XenMobile 10.x, um certificado pode não ser renovado devido a um problema com a conversão do período de renovação de certificado. [CXM-25637]

Se você usar o PostgreSQL com o XenMobile 9, o processo de atualização do XenMobile 9 para o XenMobile 10.x poderá falhar de modo intermitente porque o driver JDBC do PostgreSQL ignora o tamanho da busca. [CXM-25638]

Problemas conhecidos

No XenMobile 10.6 existem os seguintes problemas conhecidos. Problemas resolvidos da Ferramenta de atualização são exibidos sob o título "Ferramenta de atualização do XenMobile" neste artigo.

Para problemas conhecidos relacionados a XenMobile Apps, consulte Problemas conhecidos.

Alguns aplicativos corporativos para Android não são carregados em um console XenMobile configurado no modo MDM ou Corporativo (XME). [CXM-22377]

Quando você configura uma política de dispositivo para Proteção de informações do Windows e habilita a configuração **Revogar o certificado WIP ou cancelar registro**, depois de apagar seletivamente uma conta de tablet do Windows 10, os usuários são capazes de acessar um arquivo seguro. Além disso, o arquivo não está criptografado conforme o esperado. Essa condição é um problema da Microsoft com o tablet Windows 10 RS1. [CXM-23362]

Para dispositivos Windows 10 registrados por meio do Azure Active Directory durante a instalação inicial do dispositivo, não é possível revogar o dispositivo no console XenMobile. Esse problema é uma limitação da Microsoft. [CXM-24897]

Depois que você atualiza o arquivo APK ofuscado para alguns aplicativos Android no console XenMobile, a versão mais antiga é exibida nos detalhes, e a versão atualizada não é implantada nos dispositivos. [CXM-25629]

Para telefones Windows 10 RS2, quando você emite uma ação Fazer dispositivo tocar em **Gerenciar > Dispositivos**, o comando de toque falha e não é implantado no dispositivo. Esse é um problema de terceiros. [CXM-25888]

Para telefones e tablets Windows 10 RS2, durante o novo registro, um usuário não é solicitado a especificar a URL do

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 **URL do servidor**. Esse é um problema de terceiros. [CXM-25900]

Quando o XenMobile está no modo somente MAM, o registro falha após as etapas a seguir: [CXM-26481]

1. Um usuário registra um dispositivo iOS por meio de um convite por PIN ocasional.

2. O usuário remove sua conta do Secure Hub.

3. O usuário repete o registro com um tipo diferente de convite por PIN ocasional. Por exemplo, o primeiro modo de registro é Alta segurança e o segundo é URL de convite + PIN. O registro ocorre dentro do valor de tempo limite para Ativar reutilização da sessão do NetScaler, que é de dois minutos por padrão.

Quando credenciais derivadas estão ativadas no XenMobile Server, o Portal de autoajuda permite criar convites para registro do iOS. [CXM-29679]

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. [CXM-30053]

Em telefones Windows 10, se você implantar uma política de dispositivo para Proteção de informações do Windows que possua o OneDrive configurado como aplicativo permitido, ocorrerá o seguinte problema. Se você apagar seletivamente o dispositivo, o OneDrive falhará quando for aberto pelos usuários. Para solucionar esse problema, configure o OneDrive como um aplicativo isento na política de dispositivo para Proteção de informações do Windows. [CXM-30618]

Depois que o XenMobile usa credenciais derivadas para o registro de dispositivos iOS, se você atualizar mais tarde **Configurações > Credenciais derivadas** com um certificado não proveniente do seu provedor, o XenMobile continuará a usar as credenciais derivadas para o registro de dispositivos iOS. Para solucionar esse problema, depois de escolher um certificado diferente em **Configurações > Credenciais derivadas**, exclua o certificado de credenciais derivadas de **Configurações > Certificados**. [CXM-31540]

Em um dispositivo de tablet Windows RS2 registrado no XenMobile Server e conectado a uma conta do Exchange implantada, se você usar o console XenMobile para tornar o dispositivo não gerenciado (exceto para apagamento completo), a conta do Exchange permanecerá no dispositivo registrado. [CXM-31697]

Se a política preterida de Proteção de dados corporativos for configurada, e você atualizar para a versão mais recente do XenMobile, o console XenMobile exibirá este erro: "Ocorreu um erro de configuração. Tente novamente". Para solucionar esse problema, exclua a política de EDP antes de atualizar o XenMobile Server. [CXM-32132]

Ao procurar um aplicativo na Google Play Store com o console XenMobile, a mensagem "Erro ao fazer login com as credenciais do Google Play" é exibido de forma intermitente. Você pode fechar a mensagem de erro e continuar a procurar aplicativos. [CXM-32441]

Somente para implantações em nuvem do XenMobile fora dos Estados Unidos: ao procurar um aplicativo na Loja de aplicativos pública com o console XenMobile, é exibida a mensagem "Erro ao pesquisar aplicativo na plataformas da loja: windows_phone". [CXM-32444]

Nas versões em alemão, coreano e chinês simplificado do console XenMobile: na página da plataforma Android da política de dispositivo de VPN, para o tipo de conexão de VPN Citrix, os seguintes rótulos não estão traduzidos.

- Senha e certificado (uma opção de Tipo de autenticação)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Lista de aplicativos, Nome do pacote de aplicativos [CXM-33640]

Errata de documentação do XenMobile Server 10.6

Os itens a seguir são uma errata encontrada na documentação desde que foram publicadas pela última vez. Uma errata é uma lista de problemas de conteúdo, como erros ou informações ausentes, que podem afetar o uso do XenMobile Server.

- O XenMobile Server 10.6 é compatível com o VMWare ESXi 5.5.
- Na página 106, em requisitos de porta, as seguintes informações devem estar incluídas.

  A seguinte porta deve estar aberta para dispositivos e aplicativos se comunicarem com o XenMobile 10.x.
  - **Porta**: 30001
  - **Descrição**: API de gerenciamento para preparação inicial do serviço HTTPS
  - **Origem**: LAN interna
  - **Destino**: XenMobile Server

Informações relacionadas

> XenMobile Support Knowledge Center

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Problemas resolvidos

Feb 21, 2018

O XenMobile 10.8 inclui os seguintes problemas resolvidos.

Para ver os problemas corrigidos relacionados aos XenMobile Apps, consulte Problemas corrigidos.

Quando você carrega um aplicativo empresarial .IPA para o XenMobile Server, ocasionalmente o upload não acontece. A seguinte mensagem de erro é exibida: aplicativo móvel carregado é inválido. O ícone do aplicativo não foi encontrado. [#662026][CXM-43032]

Após uma atualização para o XenMobile server versão 10.5 ou versões posteriores: ocorre falha no registro do dispositivo e a mensagem de erro "Não foi possível assinar a CSR" aparece no log de depuração de configurações usando o PKI genérico (GPKI). Esse problema ocorre porque o protocolo GPKI falha ao recuperar um certificado de usuário assinado. [#690361]

os usuários de iOS não podem atualizar o Citrix Receiver para a versão 7.2.3. Quando você clica em **Verificar se há atualizações**, a mensagem "O aplicativo está atualizado com a versão mais recente" aparece mesmo quando você tem uma versão mais antiga. [#691529, CXM-38114]

Quando você clica com o botão esquerdo do mouse em Secure Mail ou Citrix Secure Web para Android na lista **Configurar** > **Aplicativos** e, em seguida, clica em **Mostrar mais**, o seguinte erro pode aparecer: "Ocorreu um erro de configuração. Tente novamente". Na seção de classificação de aplicativo, a guia Android é em branco. [#692848]

Quando você carrega um certificado de ouvinte SSL no XenMobile Server, o erro "Não foi possível importar o certificado" é exibido. [#692965]

Quando você registra dispositivos iOS no XenMobile Server, o registro falha intermitentemente e o erro "Não foi possível conectar" é exibido. [#693175]

O carregamento de certos arquivos APK para o console XenMobile pode falhar com um "500 Erro interno do servidor". [#693978, CXM-40333]

As ações de segurança não são executadas em um nó que já tenha sido inicializado para um determinado push, se a notificação for enviada de outro nó. [#695573, CXM-40418]

Nos dispositivos Android, os aplicativos gerenciados não aparecem durante as chamadas da API do XenMobile Server. [#695647]

O relatório que você pode exportar de **Gerenciar** > **Dispositivos** possui duas colunas denominadas "Tipo de dispositivo ASM DEP". [#695366, #695895]

Se um nome de Conexão VPN tem um espaço ou outros caracteres não alfanuméricos, o XenMobile não implanta a política para os dispositivos. [CXM-32538]

Depois que um usuário remove um livro do aplicativo iBook, o livro não é reinstalado automaticamente. Para baixar o livro novamente, pressione o ícone de download no iBooks. [CXM-34281]

Se você enviar a ação de segurança Ativar modo Perdido para um dispositivo iOS supervisionado sem o Secure Hub, o botão **Localizar** não aparece no dispositivo. [CXM-36106]

A ação de segurança de apagamento completo Full Wipe não ocorre em dispositivos registrados que executam o macOS

© 1999-2017 Citrix Systems, Inc. All rights reserved.

High Sierra (10.13 beta3) com o Apple File System (APFS). [CXM-36397]

Na página **Gerenciar > Dispositivos > Aplicativos**, o inventário mostra um número de versão incorreto para Boeing Toolbox Mobile Library. [CXM-37514]

Na página **Gerenciar > Dispositivos > Propriedades**: a propriedade de **Conformidade do código secreto** é definida como **Sim** para dispositivos Samsung que não atendem aos requisitos da política de código secreto. [CXM-37948]

Para dispositivos iOS 11 registrados no MDM 11, quando você implanta o XenMobile em uma configuração de cluster no modo MDM ou MDM + MAM, os comandos do MDM podem falhar. Como resultado, os seguintes problemas podem ocorrer:

- Você pode não conseguir enviar políticas do MDM ou implantar aplicativos
- Talvez não seja possível executar ações de segurança, como bloqueio ou apagamento, em dispositivos iOS 11.
- Nos dispositivos de usuário, os seguintes problemas podem ocorrer:
  - Os apps continuam tentando instalar
  - Configurações VPN ou WiFi não conseguem instalar
  - Ações de segurança, como bloqueio, ocorrem repetidamente.

Para obter mais detalhes e ação necessária, consulte este artigo da Citrix Knowledge Center. https://support.citrix.com/article/CTX227406. [CXM-38331]

Se uma função do RBAC não tiver acesso às ações apagamento App Wipe e de bloqueio App Lock: um usuário com essa função e conectado ao Portal de Autoajuda poderá realizar as ações de apagamento de aplicativos e bloqueio de aplicativos. [CXM-38348]

Usuários locais e do Active Directory com a permissão RBAC "ADD/EDIT/DELETE usuários e grupos locais" também podem excluir contas de administrador. Quando esses usuários estão conectados ao Console XenMobile, a página **Gerenciar > Usuários** inclui os botões **Editar** e **Excluir** das contas de administrador. [CXM-38350]

Uma limpeza de banco de dados agendada falha devido a muitos logs de transação excederem os limites de espaço em disco. [CXM-38439]

Se o gatilho para uma ação automatizada for baseado em um valor nulo para uma propriedade do dispositivo, a ação é realizada no dispositivo. Por exemplo, se uma ação for definida para apagar um dispositivo se a plataforma não for iOS, a ação apagará os dispositivos iOS. [CXM-38470]

Para administradores que possuem apenas as funções PKI Entities e Credential Providers em RBAC: o administrador é desconectado do console XenMobile ao adicionar uma Entidade PKI ou Provedor de credenciais. Para solucionar esse problema, adicione a permissão de Certificados à função RBAC do administrador. [CXM-38713]

Quando você configura o Mobile Service Provider (MSP) no XenMobile Server por meio de uma conexão segura, como https:// /services/zdmservice, a conexão falha e o seguinte erro é exibido: "Ocorreu um erro ao verificar a segurança da mensagem". [CXM-39048]

Em **Configurar > Políticas de dispositivos > Política de bloqueio de aplicativos**: depois de digitar o nome da política e ir para a página do iOS, os IDs dos pacotes não aparecem no menu **ID do pacote de aplicativos**. Depois que você alternar entre Android e iOS, os IDs dos pacotes de aplicativos serão exibidos. [CXM-39302]

Quando você importa um certificado de Ouvinte SSL renovado para o XenMobile, a mensagem "Não foi possível importar o certificado" é exibida. Depois de reiniciar o XenMobile Server, a página **Certificados** e o banco de dados do XenMobile

© 1999-2017 Citrix Systems, Inc. All rights reserved.

continuam a fazer referência ao certificado antigo. No entanto, o novo certificado é exibido em um navegador da web. [CXM-39409]

Se uma ação marcar os dispositivos registrados como Fora de conformidade quando eles não têm o Secure Hub instalado: dispositivos com o Secure Hub também são marcados como Fora de conformidade. Essa correção se aplica a ações com o seguinte padrão. Gatilho: se o **nome do aplicativo instalado: Não for** / **Não** contém . Ação: Executar depois de um atraso de **<5 a 10> minutos**. [CXM-39410]

Um problema do Servidor de Licenças faz com que XenMobile Servers em cluster sejam reiniciados depois que um administrador faz login no console do XenMobile Server. [CXM-39411]

O número de licenças XenMobile mostradas na página **Configurações > Licenças** inclui apenas as licenças perpétuas instaladas recentemente e não as licenças anuais. [CXM-39412]

Quando você clica com o botão esquerdo do mouse em Secure Mail ou Secure Web para Android na lista **Configurar > Aplicativos** e, em seguida, clica em **Mostrar mais**, o seguinte erro pode aparecer: "Ocorreu um erro de configuração. Tente novamente". Na seção de **classificação de aplicativo**, a guia **Android** está em branco. [CXM-40334]

O relatório que você pode exportar de **Gerenciar > Dispositivos** possui duas colunas denominadas "Tipo de dispositivo ASM DEP". [CXM-40872]

Os administradores do RBAC não podem ver os dispositivos gerenciados no console do XenMobile Server. Ocorre um erro 500 interno do servidor. [CXM-41147]

O XenMobile Store mostra "Remote Office XA%3D%3DTools" em lugar de "Remote Office\Tools" como a descrição de aplicação de XenApp and XenDesktop Apps. [CXM-41575]

Durante um download de um arquivo APK do Secure Hub para o console XenMobile, o seguinte erro ocorre: 500 Erro de servidor interno. [CXM-41855]

Ao configurar uma política de dispositivo de configuração de aplicativo para iOS: se o conteúdo do dicionário incluir o delimitador "&", o código XML não funcionará nos dispositivos. O erro de validação XML no log é: a referência à entidade "nome" deve terminar com o delimitador ";". [CXM-41883]

O número de apagamentos seletivos pendentes exibidos no painel não corresponde ao número exibido na guia de análise. [CXM-42020]

As ações de NAC gravadas nos arquivos de log do console resultam em arquivos grandes. [CXM-42071]

Quando você alterna para o driver JDBC (Microsoft Java Database Connectivity) com autenticação do Windows, a verificação de conectividade do banco de dados do XenMobile Server falha. [CXM-42271]

Um problema com um utilitário ps faz com que os nós do XenMobile Server sejam reinicializados. [CXM-42305]

Quando você atualiza do XenMobile Server 10.6 para o XenMobile Server 10.7, os dispositivos registrados no modo somente MAM podem falhar ao baixar aplicativos MDX. [CXM-42345]

Em determinados cenários de controle de versão, o recurso de verificação de atualizações de aplicativos não funciona corretamente. [CXM-42388]

ara uma política de dispositivo de restrições para o Samsung SAFE: as opções do **navegador**, do **YouTube** e do **Google Play/Marketplace** estão obsoletas. Use a opção **Desabilitar Aplicativos** para habilitar ou desabilitar esses recursos. [CXM-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

43043]

Quando o XenMobile Server é atualizado para 10.7 RP 1 ou RP 2, o registro do dispositivo é interrompido até você adicionar a propriedade do servidor ios.ssl.proxy.disable e reiniciar todos os XenMobile Servers em cluster. [CXM-43419, CXM-44293]

Em um ambiente configurado para o Android for Work: depois de registrar um dispositivo e, em seguida, adicionar um aplicativo, o aplicativo não aparece no Google Play no dispositivo. Se você cancelar o registro e depois registrar novamente o enterprise e, em seguida, adicionsr os aplicativos, o Google Play não mostrará os aplicativos. [CXM-43424]

O número padrão de arquivos de backup incluídos nos pacotes de suporte resulta em arquivos muito grandes. [CXM-43598]

O registro falha, com esta mensagem de log: com.zenprise.zdm.enroll.EnrollmentException: com.hazelcast.core.OperationTimeoutException: QueryPartitionOperation invocation failed to complete due to operation-heartbeat-timeout. [CXM-43779]

Em dispositivos Android com políticas de dispositivo Tunnel e Webclip: o Secure Hub trava após você abrir um webclip e voltar várias vezes no navegador. [CXM-43812]

Depois que a política de dispositivo Control OS Updates é implantada em dispositivos iOS: os ActiveSync IDs no XenMobile não correspondem aos ActiveSync IDs no dispositivo. Como resultado, os usuários não podem acessar o email. [CXM-43958]

O uso do console XenMobile para procurar um usuário ou dispositivo é lento. [CXM-44120]

Após a atualização de XenMobile Servers em cluster para 10.7 RP2, o registro falha com uma exceção de tempo limite. [CXM-45669]

As ações de controle do Network Access Control (NAC) gravadas nos arquivos de log do console resultam em arquivos grandes. [XMHELP-817]

A tabela do banco de dados,. EWDEPLOY_HISTO, não é limpa periodicamente, resultando em um tamanho de tabela grande. [XMHELP-827]

Informações relacionadas

- XenMobile Support Knowledge Center

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Problemas conhecidos

Feb 21, 2018

No XenMobile 10.8 existem os seguintes problemas conhecidos.

Para problemas conhecidos relacionados aos XenMobile Apps, consulte Problemas conhecidos.

Os convites de registro para dispositivos macOS se referem a MACOSX em vez de macOS. [CXM-32370]

Os administradores do RBAC podem atribuir a função de administrador padrão para os usuários novos ou existentes. Atribuir a função de administrador padrão deve ser restrita a super administradores. [CXM-37805]

Depois de atualizar para o XenMobile Server 10.7 ou posterior e registrar um dispositivo: a contagem de licenças mostrada no console XenMobile é muito maior do que o número real de dispositivos registrados. Esse problema é devido a um componente de terceiros. [CXM-40533]

Se o XenMobile Server estiver instalado no modo FIPS (Federal Information Processing Standards), você poderá alternar para o driver JDBC (Microsoft Java Database Connectivity) com a Autenticação do SQL. A mudança para o driver JDBC com a autenticação do Windows falha. [CXM-42619]

Se o SQL Server for implantado em um domínio filho ou se um logon de banco de dados do domínio filho for usado, o JDBC (Microsoft Java Database Connectivity) com a Autenticação do Windows falhará. [CXM-42969]

Nas páginas **Configurar > Políticas de dispositivo** e **Configurar > Aplicativos**: quando você classifica as listas pela coluna **Tipo**, os itens não aparecem na ordem correta. [CXM-43565]

Quando um usuário que não está registrado em um dispositivo compartilhado faz login no dispositivo: o Portal de autoajuda mostra os comandos de apagamento seletivo e apagamento completo como ativos. Os comandos devem estar inativos para um usuário que não está registrado no dispositivo compartilhado. [CXM-45365]

Ao usar a página **Analisar > Relatórios** no Safari, não é possível exportar um gráfico como PDF. [CXM-45716]

Quando você faz o carregamento do último arquivo .apk do Chrome (com.android.chrome_v64.0.3282.137-328213700_Android-4.1) para o XenMobile em **Configurar > Aplicativos**, esta mensagem é exibida: 500 Erro interno do servidor. [CXM-45722]

Registro OTA para dispositivos macOS tem suporte apenas nos navegadores Safari e Chrome. [CXM-45872]

XenMobile Server 10.7 e 10.8 não são compatíveis com o Remote PostgreSQL 10.1.3. Use Remote PostgreSQL 9.5.1 or 9.5.11. [CXM-46253]

XenMobile não dá suporte a gerenciamento de aplicativos auto-hospedados para Android for Work. Observe que isso não é novo no XenMobile Server 10.8. As alterações feitas pelo Google interrompem todos os servidores novos e existentes com esse recurso. [CXM-46413]

Informações relacionadas

- XenMobile Support Knowledge Center

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Arquitetura

Feb 21, 2018

Os componentes do XenMobile na arquitetura de referência do XenMobile que você optar por implantar se baseiam nos requisitos de gerenciamento de dispositivo ou aplicativo da sua organização. Os componentes do XenMobile são modulares e se baseiam uns nos outros. Por exemplo, para fornecer aos usuários na sua organização acesso remoto a aplicativos móveis e para acompanhar os tipos de dispositivo, você implanta o XenMobile com o NetScaler Gateway. O XenMobile é onde você gerencia os dispositivos e aplicativos, e o NetScaler Gateway permite que os usuários se conectem à sua rede.

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 NetScaler 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:

- NetScaler Gateway. Você pode definir as configurações do NetScaler 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 NetScaler 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.
- MDX Toolkit. O MDX Toolkit pode preparar com segurança os aplicativos criados dentro da sua organização ou fora da sua empresa. Depois preparar um aplicativo, use o console XenMobile para adicioná-lo ao XenMobile e alterar a configuração de política, conforme necessário. Você também pode adicionar categorias de aplicativo, aplicar fluxos de trabalho e implantar aplicativos em grupos de entrega. Consulte Sobre o MDX Toolkit.
- 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.
- ShareFile Enterprise (opcional). Se você implantar o ShareFile, 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 como configurar os provedores de identidade para o ShareFile, consulte o site de suporte do ShareFile.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 NetScaler pode reduzir ainda mais a carga no servidor XenMobile 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 NetScaler, consulte Clustering.

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 Reference Architecture for On-Premises Deployments e Reference Architecture for Cloud Deployments. Para obter uma lista completa de portas, consulte Requisitos de porta (no local) e Requisitos de porta (nuvem).

Modo de gerenciamento de dispositivo móvel (MDM)

> ## Important
>
> 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 Atualizar do XenMobile 10 MDM Edition para Enterprise Edition.

O XenMobile MDM Edition permite o gerenciamento de dispositivos móveis. Para obter suporte de plataforma, consulte Sistemas operacionais de dispositivos compatíveis. 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 NetScaler 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 de plataforma, consulte Sistemas operacionais de dispositivos compatíveis. 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 NetScaler Gateway na frente, o que oferece uma proteção adicional ao XenMobile.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 de plataforma, consulte Sistemas operacionais de dispositivos compatíveis. 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 NetScaler 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Requisitos do sistema e compatibilidade

Feb 21, 2018

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

- Compatibilidade do XenMobile
- Sistemas operacionais de dispositivos compatíveis
- Requisitos de porta
- Escalabilidade
- Licenciamento
- Conformidade com FIPS 140-2
- Suporte a idiomas

Para executar o XenMobile 10.8, você precisa atender aos seguintes requisitos mínimos do sistema:

- Uma das seguintes opções:
  - XenServer (versões com suporte: 6.5.x, 7.0, 7.1, 7.2, 7.3); para obter detalhes, consulte XenServer
  - VMware (versões com suporte: ESXi 5.5, ESXi 6.0 ou ESXi 6.5.0); para obter detalhes, consulte VMware
  - Hyper-V (versões com suporte: Windows Server 2012 R2 ou Windows Server 2016); para obter detalhes, consulte Hyper-V.
- 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 11.14.x ou posterior

Requisitos do sistema do NetScaler Gateway

Para executar o NetScaler Gateway com o XenMobile 10.8, você precisa atender aos seguintes requisitos mínimos do sistema.

- NetScaler Gateway (no local). Versões com suporte: 12.0, 11.1
- 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 10.8

O XenMobile requer um dos seguintes bancos de dados:

- Microsoft SQL Server

  O repositório do XenMobile dá suporte a um banco de dados do Microsoft SQL Server em execução em uma das seguintes versões com suporte. Para obter mais informações sobre bancos de dados do Microsoft SQL Server, consulte Microsoft SQL Server:

  Microsoft SQL Server 2016
  Microsoft SQL Server 2014 SP1
  Microsoft SQL Server 2012 R2 SP3
  Microsoft SQL Server 2012

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Nota: verifique se a conta de serviço do SQL Server que deve ser usada no XenMobile tem a permissão da função DBcreator. Para obter mais informações sobre as contas de serviço do SQL Server, consulte as páginas abaixo no site da Microsoft Developer Network. 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**:

Configuração do servidor - Contas de serviço

Configurar contas de serviço e permissões do Windows

Funções de nível de servidor

- 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.

  Nota: todas as edições do XenMobile dão suporte ao Remote PostgreSQL 9.5.1 e 9.5.11 para Windows, com as seguintes limitações: suporte para até 300 dispositivos. Uso do SQL Server no local por mais de 300 dispositivos; sem suporte para clustering.

Compatibilidade do StoreFront

StoreFront 3.13
StoreFront 3.12
StoreFront 3.0.5000.1
XenApp e XenDesktop 7.16
XenApp e XenDesktop 7.15 Long Term Service Release (LTSR)
XenApp and XenDesktop 7.6 LTSR CU5

Outra compatibilidade

XenMobile Mail Manager 10.1.1.149

XenMobile NetScaler Connector 8.5.0.051

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Compatibilidade do XenMobile

Mar 06, 2018

Para usar novos recursos, correções e atualizações de políticas, a Citrix recomenda que você instale a versão mais recente do MDX Toolkit, do Secure Hub e dos XenMobile Apps. Você pode usar o MDX Service em vez do MDX Toolkit.

> **Important**
>
> Citrix dará suporte tanto para distribuição empresarial quanto a distribuição de loja de aplicativos pública de aplicativos de produtividade XenMobile até 31 de dezembro de 2017. Para obter detalhes, consulte a Matriz de produtos Citrix. Agora, os produtos Citrix dão suporte apenas à distribuição pela loja de aplicativos pública.

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 XenMobile Apps são compatíveis com a versão mais recente, além das duas versões anteriores do XenMobile Server.

A versão mais recente dos XenMobile Apps requer a versão mais recente do Secure Hub. As duas versões anteriores dos aplicativos são compatíveis com o Secure Hub mais recente.

XenMobile Server (no local)

- A Citrix oferece suporte a atualizações das duas últimas versões do XenMobile Server.
- Última versão do XenMobile Server:
  - XenMobile Server 10.8
- Atualizar de:
  - XenMobile Server 10.7.x
  - XenMobile Server 10.6.x

MDX Toolkit

O MDX Toolkit 10.7.10 é a versão final compatível com a preparação de XenMobile Apps. Os usuários obtêm os XenMobile Apps da versão 10.7.5 e versões posteriores da loja pública de aplicativos. Os usuários acessam o ShareFile para XenMobile nas lojas de aplicativos públicas após a versão 6.5.

- A Citrix oferece suporte para as três versões mais recentes (n.n.n) do MDX Toolkit.
- A versão mais recente do toolkit é 10.8.5 do MDX Toolkit (para iOS e Android). Não use esta versão para preparar as versões empresarias dos XenMobile Apps. Você pode atualizar para o MDX Toolkit 10.8.5 do MDX Toolkit 10.7.20, 10.7.10, do MDX Toolkit 10.6.20 (iOS) e do MDX Toolkit 10.6.20 (Android).
- A última versão do toolkit com suporte para preparação de XenMobile Apps, como o Secure Mail e o Secure Web, é MDX Toolkit 10.7.10 (para iOS e Android). Você pode atualizar para o MDX Toolkit 10.7.10 do MDX Toolkit 10.7.5.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile Apps de lojas de aplicativos públicas

Os usuários obtêm os XenMobile Apps da versão 10.7.25 e versões posteriores da loja de aplicativos pública. Os usuários acessam o ShareFile para XenMobile nas lojas de aplicativos públicas após a versão 6.5.

- A Citrix oferece suporte a atualizações das duas últimas versões.
  - Os usuários que têm atualizações automáticas ativadas recebem a versão mais recente da loja de aplicativos
  - O aplicativo mais recente é compatível com os dois arquivos MDX anteriores.
- Versões mais recentes de Secure Hub, Secure Mail e Secure Web para Android:
  - 10.8.5
  - 10.7.30
  - 10.7.25
- Versões mais recentes do Secure Hub, Secure Mail e Secure Web para iOS:
  - 10.8.5
  - 10.7.30
  - 10.7.25
- Atualizar de:
  - Secure Hub 10.7.30 ou 10.8.5
  - Secure Mail 10.7.30 ou 10.8.5
  - Secure Web 10.7.30 ou 10.8.5

Para XenMobile Apps

A tabela a seguir lista as versões empresariais finais do XenMobile App que você pode preparar com o MDX Toolkit 10.7.10.

XenMobile App	Versão do iOS	Versão do Android
Secure Forms	10.7.0.13, 10.7.0.67	-
Secure Mail	10.7.20, 10.7.25, 10.7.30	10.7.20, 10.7.25, 10.7.30
Secure Notes	10.7.0	10.6.20
Secure Tasks	10.7.0	10.6.20
Secure Web	10.7.20, 10.7.25, 10.7.30	10.7.20, 10.7.25, 10.7.30
QuickEdit	6.15.2	6.16.2
ScanDirect	1.3.6	-
ShareConnect	3.5	3.5

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ShareFile	6.6	6.6

[1] O ShareFile pode ser compatível com uma versão do MDX Toolkit posterior à 10.7.10.

Suporte a navegadores

O XenMobile 10.8 é compatível com os seguintes navegadores:

- Internet Explorer, mas não as versões 9 ou anteriores
- Chrome
- Firefox
- Safari em dispositivos móveis para uso com o Portal de autoatendimento

O XenMobile 10.8 é compatível com a versão mais recente do navegador e com uma versão anterior à atual.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Plataformas de dispositivo com suporte

Feb 26, 2018

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 plataformas de dispositivo com suporte neste artigo também se aplicam ao XenMobile Mail Manager e ao XenMobile NetScaler Connector.

> **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 XenMobile funcionam em versões de plataformas mais antigas. Este artigo detalha o suporte da Citrix para cada sistema operacional. Este artigo também inclui modelos de dispositivos Citrix testados. Em caso de problemas com outros modelos de dispositivos, entre em contato com o suporte da Citrix.

Android

Com o lançamento do Android O (versão 8):

- o Android 5 torna-se a versão mínima suportada pelo XenMobile.
- O suporte terminou para o Android 4.4x a partir da versão 10.6.20 da versão da loja de aplicativos pública do XenMobile Apps.

XenMobile 10.x

Sistemas operacionais com suporte para todos os modos: Android 5.x, 6.x, 7.x, 8.x

Sistemas operacionais com suporte para o modo somente MDM: Android 4.4, 5.x, 6.x, 7.x, 8.x

Aplicativos XenMobile e aplicativos preparados com MDX estão disponíveis em dispositivos Android com processadores baseados em ARM.Eles não são suportados em dispositivos Android com base em Intel x86 ou x64.

Dispositivos e sistemas operacionais Android testados especificamente no XenMobile 10.x no modo MDM+MAM (corporativo)

- Tablet Google Nexus 9 (sistema operacional 7.0)
- Google Nexus 5 (sistema operacional 6.0.1)
- Google Nexus 5X (sistema operacional 7.1.1 e 8.0)
- Google Nexus 9 Tab (sistema operacional 5.0.1)
- Google Nexus 9 Tab (sistema operacional 5.1.1)
- Google Nexus 6P (sistema operacional 7.1.1 e 8.0)
- Google Nexus 6 (sistema operacional 6.0.1 e 7.0)
- Google Nexus 5 (sistema operacional 8.0)
- Google Pixel (sistema operacional 7.0 e 8.0)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Google Pixel C (sistema operacional 8.0)
- Google Pixel XL (sistema operacional 8.0)
- Google Pixel 2 (sistema operacional 8.0)
- Google Pixel 2 XL (sistema operacional 8.0)
- Galaxy S8 (sistema operacional 7.1.1, 8.0.0)
- Galaxy S7 (sistema operacional 7.0)
- Galaxy S6 (sistema operacional 6.0.1, 5.0)
- Galaxy Tab A (sistema operacional 6.0)
- Galaxy Note3 modelo SM-N900 (sistema operacional 5.0)
- Galaxy S6 Edge, SM-G925F (sistema operacional 6.0.1)
- Galaxy S5 SM-G900F (sistema operacional 6.0.1)
- Galaxy S5 SM-G900H (sistema operacional 6.0.1)
- Huawei P10 Lite
- Huawei P10
- Huawei P8 Lite 2017
- Moto Turbo (sistema operacional 6.0.1)
- OnePlus (sistema operacional 5, 6, 7 e 8)
- Sony Xperia, Modelo: SGP311 (sistema operacional 5.0.1)
- Zebra (todos os modelos e sistemas operacionais)

Dispositivos e sistemas operacionais Android testados especificamente no XenMobile 10.x no modo somente MDM

- Tablet Google Nexus 7 (sistema operacional 4.4.4)
- Tablet Google Nexus 9 (sistema operacional 7.0)
- Google Nexus 5 (sistema operacional 6.0.1)
- Google Nexus 5X (sistema operacional 7.1.1 e 8.0)
- Google Pixel (sistema operacional 7.0 e 8.0)
- Google Pixel C (sistema operacional 8.0)
- Google Pixel XL (sistema operacional 8.0)
- Google Pixel 2 (sistema operacional 8.0)
- Galaxy S7 (sistema operacional 7.0)
- Galaxy S8 (sistema operacional 7.1.1, 8.0.0)
- Galaxy S6 (sistema operacional 6.0.1, 5.0)
- Galaxy Tab A (sistema operacional 6.0)
- Galaxy Note3 modelo SM-N900 (sistema operacional 5.0)
- Galaxy S6 Edge, SM-G925F (sistema operacional 6.0.1)
- Galaxy S5 SM-G900F (sistema operacional 6.0.1)
- Galaxy S5 SM-G900H (sistema operacional 6.0.1)
- Huawei Nexus 6 (sistemas operacionais 6.0.1 e 7.0)
- Huawei P10 Lite
- Huawei P10
- Huawei P8 Lite 2017
- Nexus 9 Tab (sistema operacional 5.0.1)
- Nexus 9 Tab (sistema operacional 5.1.1)
- Nexus 7 (sistema operacional 4.4)
- Nexus 5 (sistema operacional 8.0)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- OnePlus (sistema operacional 5, 6, 7 e 8)
- Sony Xperia, Modelo: SGP311 (sistema operacional 5.0.1)
- Zebra (todos os modelos e sistemas operacionais)

Além disso, os seguintes tipos de dispositivo são testados com o Secure Mail.

Device type	Operating system
Google Pixel	7.0 e 8.0
Samsung S8	7.0
Samsung S7	7.0
Samsung S6	6.0.1
Samsung S5	5
Samsung Tab A	6.0.1
Google Pixel 2	8.0

SAFE e KNOX

Em dispositivos Samsung compatíveis, o XenMobile 10.x 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. Para ativar a API Samsung KNOX:

1. Compre uma licença do Samsung KNOX usando o Samsung KNOX License Management System (KLMS).

2. Implante a chave Samsung ELM.

Para políticas específicas da HTC, o XenMobile dá suporte à API da HTC versão 0.5.0. Para políticas específicas da Sony, o XenMobile dá suporte ao Sony Enterprise SDK 2.0.

iOS

Com o lançamento do iOS 11:

- O suporte a XenMobile para dispositivos iOS 8 terminou.
- O suporte a XenMobile para dispositivos iOS 9 que executam XenMobile Apps terminou em 31 de outubro de 2017.
- O suporte a XenMobile continua para os dispositivos iOS 9 no modo MDM.
- O Secure Hub não oferece mais suporte a certificados de SHA-1 em dispositivos com iOS 11. Para evitar problemas relacionados, os usuários devem atualizar para o Secure Hub 10.6.10 ou posterior antes de atualizar seus dispositivos para o iOS 11. Para obter mais informações sobre prever essa alteração, consulte o artigo do Knowledge Center em XenMobile iOS 11 and Android O Support.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile 10.7 e 10.8

- iOS 11.x
- iOS 10. x
- iOS 9.x (somente MDM)

Alguns dispositivos iOS para os quais o XenMobile 10.7 e 10.8 oferecem suporte:

- iPhone X
- iPhone 8, 8 Plus
- iPhone 7 Plus 10.2.1 (XenMobile 10.5 e versões posteriores)
- iPhone 6, 6 Plus, 6S Plus, 6S+, 5s
- iPhone 5, 5c (somente iOS 9.x)
- iPad 2, 3
- iPad Air, iPad Air-2, iPad Mini-4, Mini-3, Mini-2
- iPad Pro

macOS

XenMobile 10.8

- macOS 10.11 El Capitan
- macOS 10.12 Sierra
- macOS 10.13 High Sierra

XenMobile 10.7

- macOS 10.11 El Capitan
- macOS 10.12 Sierra
- macOS 10.13 High Sierra

Windows Phone e Tablet

XenMobile 10.6, 10.7 e 10.8

- Windows 10 RS1, RS2, e RS3 Phone e Tablet
  - Não tem suporte quando o XenMobile está no modo somente MAM.
- Windows Phone 10
- Windows Phone 8.1
  - Para o modo somente MDM
- Windows Mobile/CE
  - Não tem suporte se o XenMobile está no modo somente MAM.

Symbian

XenMobile 10.7 e 10.8

© 1999-2017 Citrix Systems, Inc. All rights reserved.

A seguinte lista inclui alguns dos dispositivos Symbian para os quais o XenMobile 10.7 e 10.8 oferecem suporte.

- Symbian 3
- Symbian S60 5th Edition
- Symbian S60 3rd Edition, Pacote de recursos 2
- Symbian S60 3rd Edition, Pacote de recursos 1
- Symbian S60 3rd Edition
- Symbian S60 2nd Edition, Pacote de recursos 3
- Symbian S60 2nd Edition, Pacote de recursos 2

BlackBerry

O gerenciamento de dispositivos BlackBerry é fornecido por meio do XenMobile Mail Manager. Para obter detalhes, consulte XenMobile Mail Manager.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Requisitos de porta

Feb 21, 2018

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. Para conhecer os requisitos de porta do XenMobile Service, consulte Requisitos de porta.

Abrir portas para o NetScaler Gateway e o XenMobile gerenciarem aplicativos

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

- XenMobile
- StoreFront
- XenDesktop
- XenMobile NetScaler Connector
- Outros recursos da rede internos, como sites da intranet

Para ativar o tráfego para iniciar Darkly do NetScaler, você pode usar os endereços IP anotados neste artigo de suporte do Knowledge Center.

Para obter mais informações sobre o NetScaler Gateway, consulte Configuration Settings for your XenMobile Environment na documentação do NetScaler Gateway. Para obter mais informações sobre o endereço IP pertencente ao NetScaler, consulte How a NetScaler Communicates with Clients and Servers na documentação do NetScaler. Essa seção contém informações sobre o os endereços IP do NetScaler (NSIP), IP de servidor virtual (VIP) e IP de subnet (SNIP).

TCP port	Description	Source	Destination
21 ou 22	Usada para enviar pacotes de suporte para um servidor FTP ou SCP.	XenMobile	Servidor FTP ou SCP
3 (TCP e UDP)	Usada para conexões DNS.	NetScaler Gateway XenMobile	Servidor DNS
80	O NetScaler Gateway transmite a conexão VPN para o recurso da rede interna por meio do segundo firewall. Geralmente, essa sitiuação ocorre quando os usuários fazem login com o NetScaler Gateway Plug-in.	NetScaler 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 do Web Interface XML NetScaler Gateway STA	XenDesktop ou XenApp
		NetScaler	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

UDP) TCP port	Description	Source XenMobile	Destination
389	Usada para conexões LDAP não seguras	NetScaler Gateway XenMobile	Servidor de autenticação LDAP ou Microsoft Active Directory
443	Cada item abaixo corresponde ao mesmo item nas colunas à direita. • Usada para conexões com o StoreFront do Citrix Receiver ou com Receiver para Web para XenApp e XenDesktop. • Usada para conexões com o XenMobile para entrega Web, móvel e de aplicativo SaaS. • Usado para comunicação geral de dispositivo com o XenMobile Server • Usada para conexões de dispositivos móveis com o XenMobile para registro. • Usada para conexões entre o XenMobile e o XenMobile NetScaler Connector. • Usada para conexões entre o XenMobile NetScaler Connector e o XenMobile. • Usado para URL de retorno de chamada em implantações sem autenticação de certificado.	• Internet • Internet • XenMobile • Internet • XenMobile • XenMobile NetScaler Connector • XenMobile	• NetScaler Gateway • NetScaler Gateway • XenMobile • XenMobile • XenMobile NetScaler Connector • XenMobile • NetScaler Gateway
514	Usada para conexões entre o XenMobile e um servidor syslog.	XenMobile	Servidor Syslog
636	Usada para conexões LDAP seguras.	NetScaler Gateway XenMobile	Servidor de autenticação LDAP ou Active Directory
1494	Usada para conexões ICA com aplicativos baseados em Windows na rede interna. A Citrix recomenda manter essa porta aberta.	NetScaler Gateway	XenApp ou XenDesktop
1812	Usada para conexões RADIUS.	NetScaler 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.	NetScaler Gateway	XenApp ou XenDesktop
3268	Usada para conexões LDAP inseguras do Microsoft Global Catalog.	NetScaler Gateway XenMobile	Servidor de autenticação LDAP ou Active Directory
3269	Usada para conexões LDAP seguras do Microsoft Global Catalog.	NetScaler Gateway XenMobile	Servidor de autenticação LDAP ou Active Directory

© 1999-2017 Citrix Systems, Inc. All rights reserved.

TCP port	Description	Source	Destination
	Connector.		Connector
30001	API de gerenciamento para preparação inicial do serviço HTTPS	LAN interna	Servidor XenMobile
9443	Usada para tráfego HTTPS entre o NetScaler e o XenMobile NetScaler Connector.	NetScaler	XenMobile NetScaler Connector
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 • NetScaler Gateway • Dispositivos • Internet	XenMobile
4443	• Usada para acesso ao console XenMobile por um administrador usando o navegador. • Usado 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
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.

TCP port	Description	Source	Destination
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
			• Apple iTunes App Store (ax.itunes.apple.com e *.mzstatic.com)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

TCP port	Description	Source	Destination
80 e 443	(ax.itunes.apple.com), Google Play (deve usar a porta 80) ou o Windows Phone Store. Usada para publicar aplicativos das lojas de aplicativos usando o Citrix Mobile Self-Serve no iOS, o Secure Hub para Android ou o Secure Hub para Windows Phone.	XenMobile	Purchase Program (vpp.itunes.apple.com) • Para Windows Phone: login.live.com e *.notify.windows.com • Google Play (play.google.com)
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. • Usada para registro e instalação do agente para dispositivos Android e Windows, o console Web XenMobile e o Cliente de Suporte Remoto do MDM.	• Internet • Internet LAN e Wi-Fi	XenMobile
1433	Usada como padrão para conexões com um servidor do banco de dados remoto (opcional).	XenMobile	Servidor SQL
2195	Usada para as conexões de saída do serviço Apple Push Notification (APNs) com gateway.push.apple.com para notificações de dispositivo e envio por push da política de dispositivo iOS.	XenMobile	Internet (hosts APN que usam o endereço IP público 17.0.0.0/8)
2196	Usada para conexões de saída de APNs com feedback.push.apple.com para notificação de dispositivo e envio por push da política de dispositivo iOS.		
5223	Usada para conexões de saída de APNs de dispositivos iOS em redes WiFi com *.push.apple.com.	Dispositivos iOS em redes WiFi	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 WiFi	

Requisito de porta para conectividade do Auto Discovery Service

Essa configuração de porta garante que os dispositivos Android que se conectam do Secure Hub para Android possam acessar o Citrix Auto Discovery Service (ADS) na rede interna. A capacidade de acessar o ADS é importante ao baixar

© 1999-2017 Citrix Systems, Inc. All rights reserved.

qualquer atualização de segurança disponibilizada por meio 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, oss seguintes pré-requisitos devem ser atendidos:

- **Colete certificados do XenMobile Server e do NetScaler**. Os certificados precisam estar no formato PEM e devem ser um certificado público e não a chave privada.
- **Entre em contato com o suporte Citrix 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 ao Secure Hub para o ambiente no qual o dispositivo está se registrando. 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	IP address	Port	IP and port usage
discovery.mdm.zenprise.com	52.5.138.94	443	Secure Hub - ADS Communication
discovery.mdm.zenprise.com	52.1.30.122	443	Secure Hub - ADS Communication
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

* A versão de Secure Hub 10.6.15 e versões posteriores usam ads.xm.cloud.com.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Escalabilidade e desempenho

Feb 21, 2018

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.
- A *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 NetScaler Gateway 8200. Do dispositivo NetScaler com capacidade semelhante ou superior pode-se esperar que produza escalabilidade semelhante ou maior.

Esta tabela resume os resultados do teste de escalabilidade:

Escalabilidade	**Até 75.000 dispositivos**	
Taxa de login	Taxa de reconexão de usuários existentes	Até 9.375 dispositivos por hora
Configuração	NetScaler 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

Esta tabela fornece resultados de teste de escalabilidade para implantação de populações de dispositivo e configurações de hardware testadas.

Número de dispositivos em operação	12.500	30.000	60.000	75.000
Taxa de reconexão de	1.250	3.750	7.500	9.375

© 1999-2017 Citrix Systems, Inc. All rights reserved.

dispositivos existentes por hora				
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
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

Essas tabelas contêm um resumo do perfil de teste usado para obter os dados deste artigo:

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

Configuração do XenMobile Server	Total	Por usuário
Políticas	20	20
Aplicativos	270	50
Aplicativo público	200	0
MDX	50	30

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 Reference Architecture for On-Premises Deployments.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Licenciamento

Feb 21, 2018

O licenciamento é diferente entre o XenMobile Service e o XenMobile Server:

- A Citrix Cloud Ops manipula o licenciamento do XenMobile Service.
- O XenMobile Server e o NetScaler Gateway requerem licenças.

  Para obter mais informações sobre o licenciamento de NetScaler Gateway, consulte Licenças na documentação do NetScaler Gateway. O XenMobile usa o Citrix Licensing para gerenciar licenças. 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.

Para obter uma ficha técnica do XenMobile que mostra os recursos disponíveis em cada edição do XenMobile, consulte este PDF.

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 Licenciando o seu produto.

> **Nota**
>
> Atualize o seu Citrix License Server para 11.14.x ou posterior antes de atualizar para a versão mais recente do XenMobile Server 10.8. Versões mais antigas de servidor de licenças não funcionam com a versão mais recente do XenMobile.

> **Important**
>
> 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.

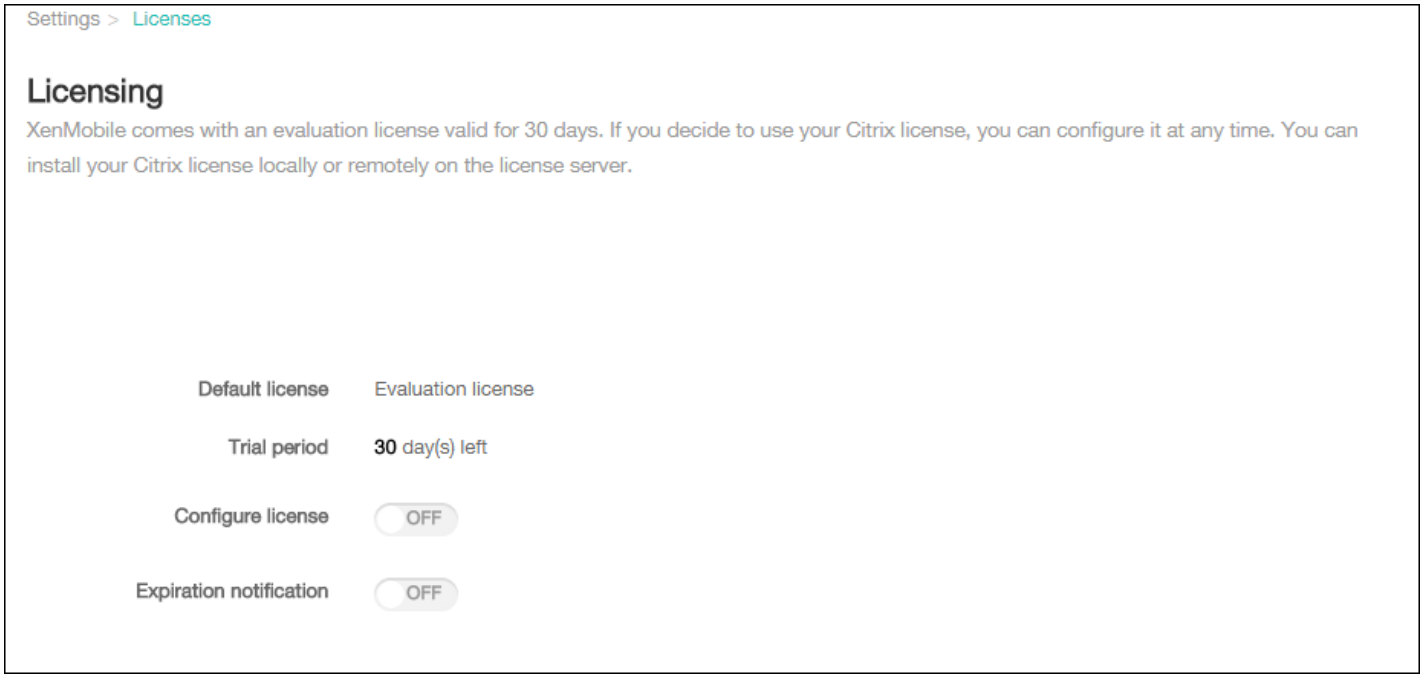
© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 **Configurações** é exibida.

2. 3. 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 Obter seus arquivos de licença.

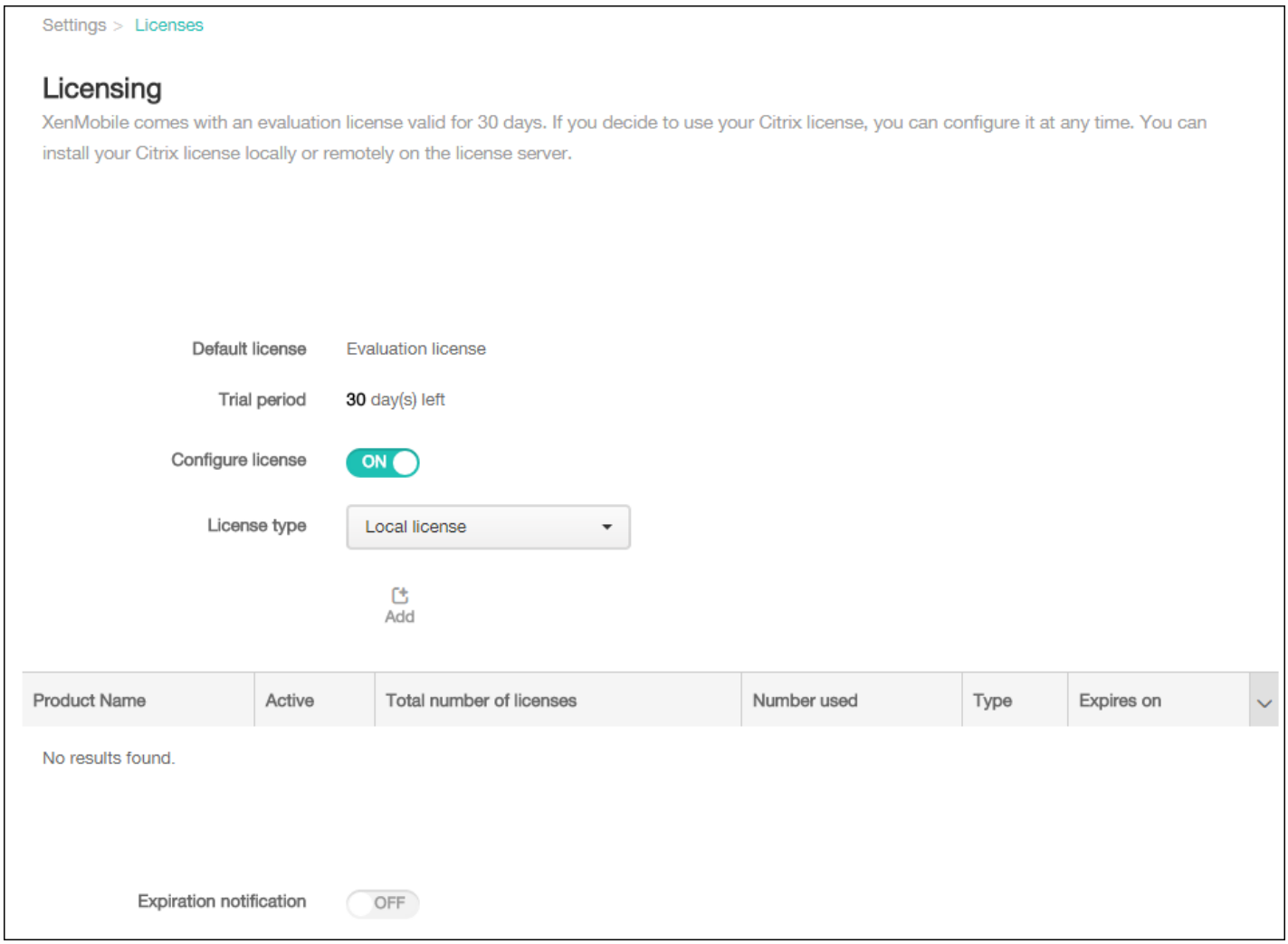
2. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.

3. 3. Clique em **Licenciamento**. A página **Licenciamento** é exibida.

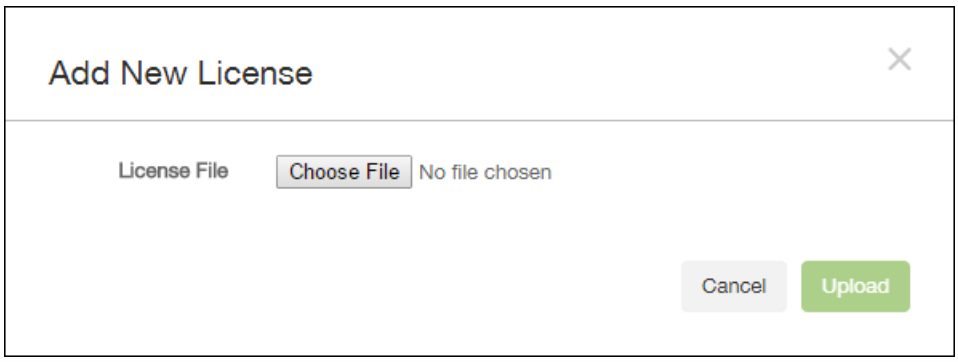
4. Defina **Configurar licença** como **Ativada**. Aparecem a lista **Tipo de licença**, o botão **Adicionar** e a tabela **Licenciamento** A tabela **Licenciamento** contém as licenças que você usou com o XenMobile. Se você ainda não tiver

© 1999-2017 Citrix Systems, Inc. All rights reserved.

adicionado uma licença Citrix ainda, a tabela estará vazia.



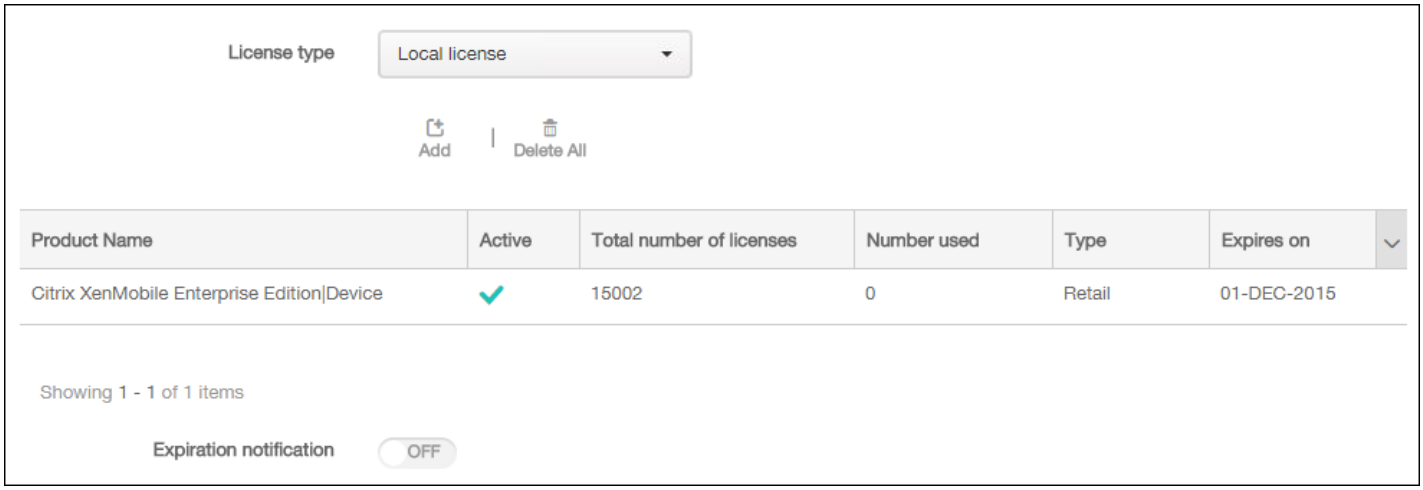
5. Verifique se **Tipo de licença** está definido como **Licença local** e clique em **Adicionar**. A caixa de diálogo **Adicionar nova licença** é exibida.



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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 Licenciando o seu produto.

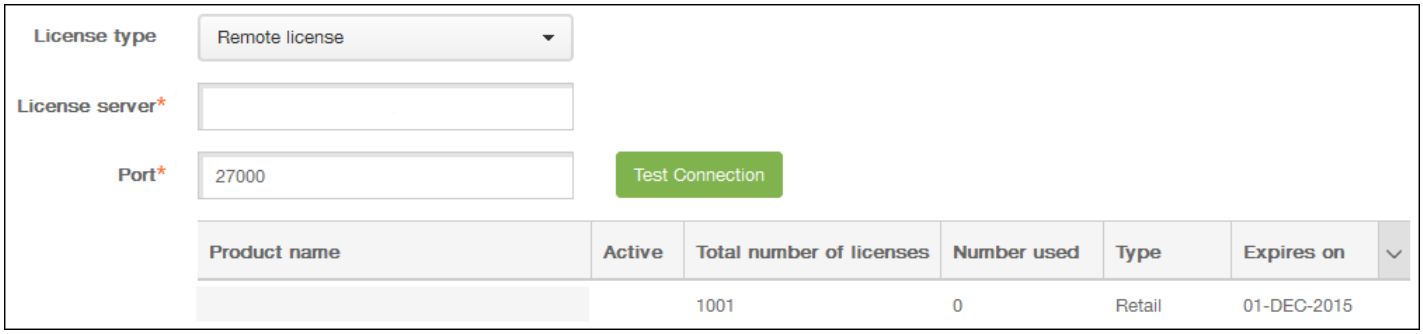
1. Importe o certificado do servidor de licença para o XenMobile Server (**Configurações> Certificados**).

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 quebrar sua implantação, altere a propriedade do servidor **disable.hostname.verification** para **verdadeiro**. O valor padrão desta propriedade é **falso**.

Quando a verificação de nome de host falha, o log do servidor inclui erros como: "Não é possível conectar com o servidor VPP: o nome de host '192.0.2.0' não corresponde à entidade do certificado fornecida pelo par correspondente"

3. 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.

4. Defina **Tipo de licença** como **Licença remota**. Os campos **Servidor de licença** e **Porta** e o botão **Testar conexão** substituem o botão **Adicionar**.



5. 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.

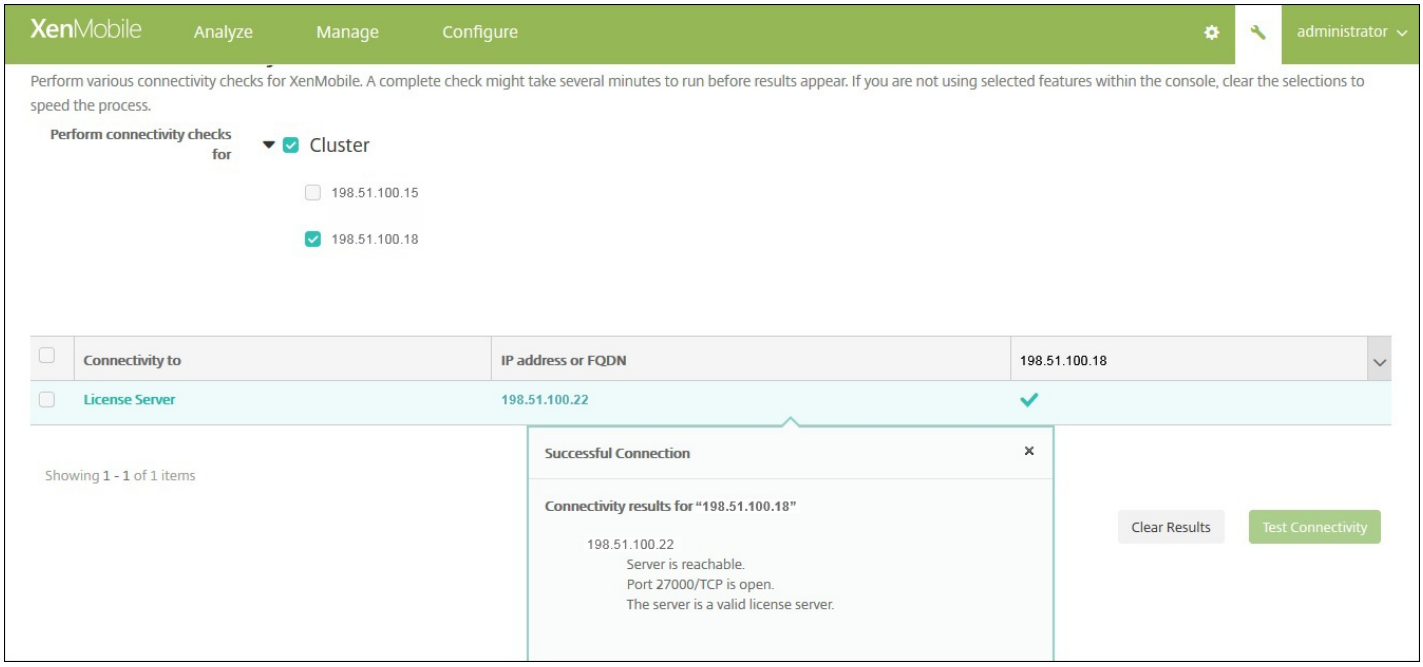
© 1999-2017 Citrix Systems, Inc. All rights reserved.

6. 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.

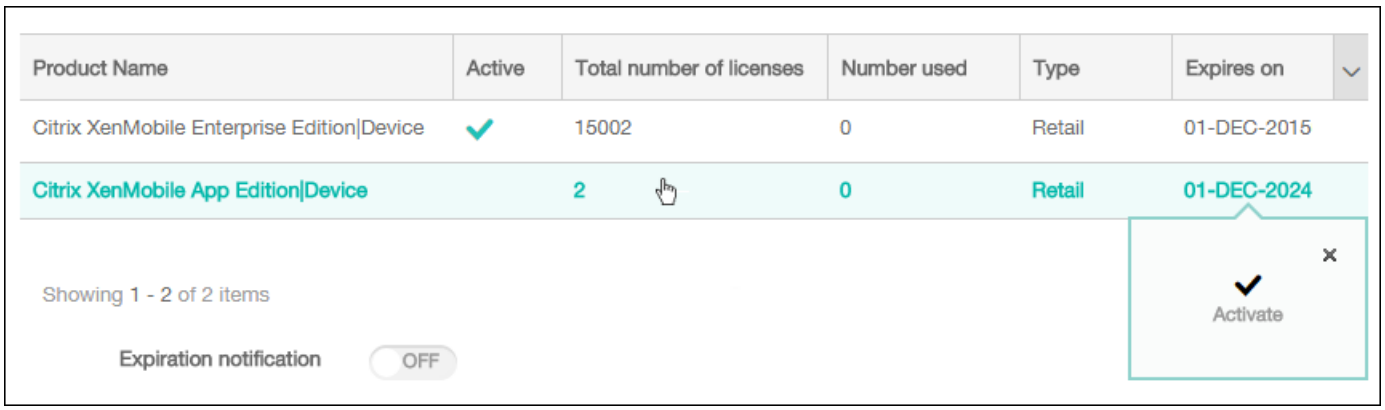
Se a conexão não for bem-sucedida, revise a mensagem de erro exibida, faça as correções necessárias e clique em **Testar conexão**.



Para ativar uma licença diferente

Se você tiver várias licenças, poderá escolher a licença que desejar 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 desejar ativar. Uma janela de confirmação **Ativar** é exibida ao lado da linha.



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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

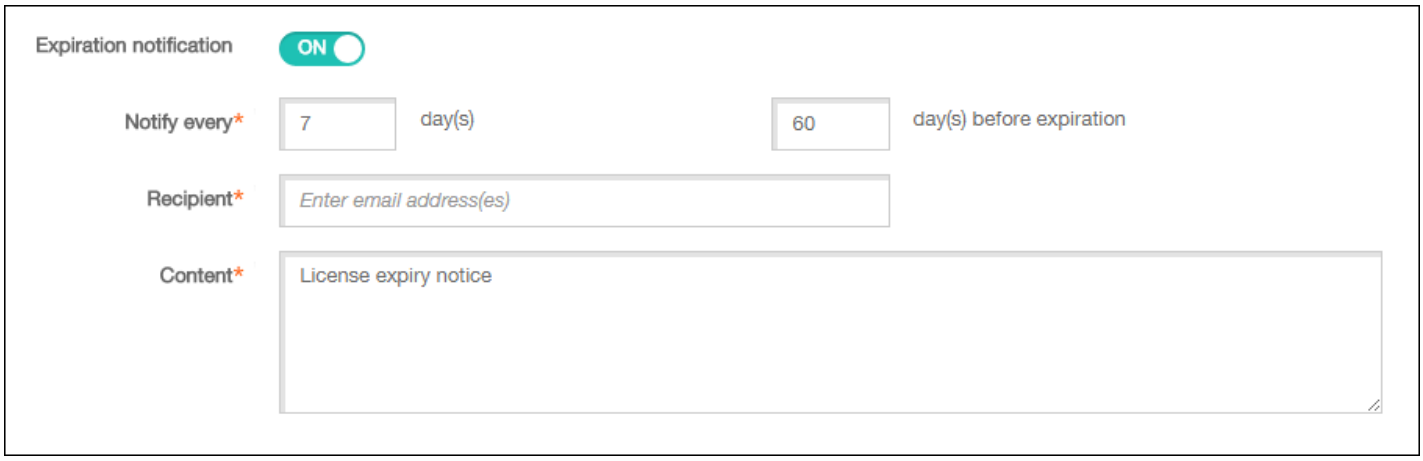
3. 3. Clique em **Ativar**. A licença selecionada é ativada.

> **Important**
>
> 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.



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 inserido em **Conteúdo** ao destinatário inserido em **Destinatário**. As notificações são enviadas com a frequência que você definir.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Conformidade com FIPS 140-2

Feb 21, 2018

O Federal Information Processing Standard (FIPS), emitido pelo US National Institute of Standards and Technologies (NIST), 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 de FIPS 140 validados pelo NIST, consulte http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1747.pdf.

Importante: o suporte ao FIPS está disponível somente para instalações no local do XenMobile Server. Você pode ativar o modo FIPS do XenMobile somente durante a instalação inicial.
Nota: o gerenciamento somente de dispositivo móvel do XenMobile, o gerenciamento somente de aplicativo móvel do XenMobile e o XenMobile Enterprise 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 certificados pelo FIPS e fornecidos pelo OpenSSL e pela Apple. No Android, todas as operações de criptografia de dados em repouso e de dados em trânsito do dispositivo móvel para o NetScaler Gateway usam módulos criptográficos certificados pelo FIPS e fornecidos pelo OpenSSL.

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 certificados pelo FIPS e fornecidos pela Microsoft.

Todas as operações de criptografia de dados em repouso e dados em trânsito no XenMobile Device Manager usam módulos criptográficos certificados pelo FIPS e fornecidos pelo OpenSSL. Combinados com as operações de criptografia descritas acima para dispositivos móveis e entre os dispositivos móveis e o NetScaler Gateway, todos os dados em repouso e dados em trânsito para fluxos do MDM usam módulos criptográficos compatíveis com FIPS de ponta a ponta.

Todas as operações de criptografia de dados em trânsito entre os dispositivos móveis iOS, Android e Windows e o NetScaler Gateway usam módulos criptográficos certificados pelo FIPS. O XenMobile usa um dispositivo NetScaler FIPS Edition hospedado no DMZ, equipado com um módulo FIPS certificado para proteger esses dados. Para obter mais informações, consulte a documentação do FIPS do NetScaler.

Os aplicativos MDX são compatíveis com o Windows Phone e usam bibliotecas de criptografia e APIs que são compatíveis com FIPS no Windows Phone. Todos os dados em repouso para aplicativos MDX no Windows Phone e todos os dados em trânsito entre o dispositivo Windows Phone e o NetScaler Gateway são criptografados usando essas bibliotecas e APIs.

O MDX Vault criptografa os aplicativos preparados pelo MDX e os dados em repouso associados em dispositivos iOS e Android usando módulos criptográficos certificados pelo FIPS e fornecidos pelo OpenSSL.

Para obter a declaração de conformidade completa com o FIPS 140-2 do XenMobile, incluindo os módulos específicos usados em cada caso, contate o seu representante da Citrix.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Suporte a idiomas

Feb 21, 2018

Os aplicativos XenMobile 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 http://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 XenMobile

Um X indica que o aplicativo está disponível neste determinado idioma. No momento, o aplicativo Secure Forms está disponível apenas em inglês.

Nota: A partir do lançamento da versão 10.4, os aplicativos móveis Worx foram renomeados como aplicativos XenMobile. A maioria dos aplicativos individuais do XenMobile também são renomeados. Para obter detalhes, consulte Sobre os aplicativos XenMobile.

iOS e Android

	Secure Hub	Secure Mail	Secure Web	Secure Notes	Secure Tasks	QuickEdit
Japonês	X	X	X	X	X	X
Chinês simplificado	X	X	X	X	X	X
Chinês tradicional	X	X	X	X	X	X
Francês	X	X	X	X	X	X
Alemão	X	X	X	X	X	X

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Espanhol	X	X	X	X	X	X
Coreano	X	X	X	X	X	X
Português	X	X	X	X	X	X
Holandês	X	X	X	X	X	X
Italiano	X	X	X	X	X	X
Dinamarquês	X	X	X	X	X	X
Sueco	X	X	X	X	X	X
Hebraico	X	X	X	X	X	iOS somente
Árabe	X	X	X	X	X	X
Russo	X	X	X	X	X	X
Turco	X	X	Somente Android			

Windows

	Secure Hub	**Secure Mail**	**Secure Web**
Francês	X	X	X
Alemão	X	X	X
Espanhol	X	X	X
Italiano	X	X	X
Dinamarquês	X	X	X
Sueco	X	X	X

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

	iOS	Android
Secure Hub	X	X
Secure Mail	X	X
secure Web	X	X
Secure Tasks	X	X
Secure Notes	X	X
QuickEdit	X	X

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Instalar e configurar

Feb 21, 2018

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. 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 XenMobile Deployment Handbook.

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 NetScaler Gateway	
	Anote o endereço IP público e local. Você precisa desses endereços IP para configurar o firewall para instalar a conversão de endereços de rede (NAT).	XenMobile NetScaler Gateway	
	Anote a máscara de sub-rede.	XenMobile NetScaler Gateway	
	Anote os endereços IP de DNS.	XenMobile NetScaler Gateway	
	Anote os endereços IP do servidor WINS (se aplicável).	NetScaler Gateway	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Identifique e anote o nome de host do NetScaler Gateway. Nota: esse 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 de host usando o Setup Wizard no NetScaler Gateway.	NetScaler Gateway	
	Anote o endereço IP do XenMobile. Reserve um endereço IP se você instalar uma instância do XenMobile. Se configurar um cluster, anote todos os endereços IP necessários.	XenMobile	
	• Um endereço IP público configurado no NetScaler Gateway • Uma entrada DNS externa para o NetScaler Gateway	NetScaler Gateway	
	Anote o endereço IP do servidor proxy Web, a porta, lista de hosts do proxy e o nome do usuário e a senha de administrador. Essas configurações serão opcionais se você implantar um servidor proxy na sua rede (se aplicável). Nota: você pode usar o sAMAccountName ou o nome UPN ao configurar o nome do usuário do proxy Web.	XenMobile NetScaler Gateway	
	Anote o endereço IP do gateway padrão.	XenMobile NetScaler Gateway	
	Anote o endereço IP do sistema (NSIP) e a máscara de sub-rede.	NetScaler Gateway	
	Anote o endereço IP da sub-rede (SNIP) e a máscara de sub-rede.	NetScaler Gateway	
	Anote o endereço IP e o FQDN do servidor virtual do NetScaler Gateway do certificado. Para configurar vários servidores virtuais, anote todos os endereços IP virtuais e FQDNs dos certificados.	NetScaler Gateway	
	Anote as redes internas que os usuários podem acessar por meio do NetScaler Gateway. Exemplo: 10.10.0.0/24	NetScaler Gateway	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	Insira todas as redes internas e segmentos de rede que os usuários precisam acessar nesses casos: quando os usuários se conectam ao Secure Hub ou ao NetScaler Gateway Plug-in quando o encapsulamento dividido está definido como Ativado.		
	Verifique se a conectividade de rede entre o servidor XenMobile, o NetScaler Gateway, o Microsoft SQL Server externo e o servidor DNS está acessível.	XenMobile NetScaler Gateway	

Licenciamento

O XenMobile exige a compra de opções de licenciamento para o NetScaler 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 Licensing na documentação do NetScaler Gateway.	NetScaler Gateway XenMobile Citrix License Server	

Certificados

O XenMobile e NetScaler Gateway exigem certificados para permitir conexões com outros produtos e aplicativos Citrix e de dispositivos de usuário. Para obter detalhes, consulte Certificados e autenticação na documentação do XenMobile.

	Pré-requisito	Componente	Observações
	Obtenha e instale os certificados necessários.	XenMobile NetScaler Gateway	

Portas

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

	Pré-requisito	Componente	Observações
	Portas abertas para o XenMobile	XenMobile NetScaler Gateway	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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. O PostgreSQL é incluído com o XenMobile e deve ser usado localmente ou remotamente somente em ambientes de teste.

Por padrão, o XenMobile usa o driver do banco de dados jDTS. Para usar o driver Microsoft JDBC para instalações no XenMobile Server no local, consulte os drivers do SQL Server.

•	Pré-requisito	Componente	Anote a configuração
	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	Anote a configuração
	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 NetScaler Gateway	
	Anote o nome de domínio do Active Directory.	XenMobile NetScaler Gateway	
	Anote a conta de serviço do Active Directory, que exige um ID do usuário, uma senha e o alias de domínio. A conta de serviço do Active Directory é a conta que o XenMobile usa para consultar o Active Directory.	XenMobile NetScaler Gateway	
	Anote o DN Base de Usuários. O nível de diretório no qual os usuários estão localizados: por exemplo, cn=users,dc=ace,dc=com. O NetScaler Gateway e o XenMobile usam isso para consulta de DN ao Active Directory.	XenMobile NetScaler Gateway	
	Anote o DN Base de Grupo.	XenMobile	

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	O nível de diretório no qual os grupos estão localizados. O NetScaler Gateway e o XenMobile usam esse DN para consultar o Active Directory.	NetScaler Gateway	

Conexões entre o XenMobile e o NetScaler 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	
	Identifique os aplicativos que os usuários podem acessar.	NetScaler Gateway	
	Anote a URL de Retorno de Chamada.	XenMobile	

Conexões de usuário: acesso ao XenDesktop, ao XenApp e ao Citrix Secure Hub

A Citrix recomenda que você use o assistente Quick Configuration no NetScaler para definir as configurações de conexão entre o XenMobile e o NetScaler 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 XenApp e XenDesktop. A Citrix recomenda que você também use o assistente Quick Configuration no NetScaler para definir essas configurações.

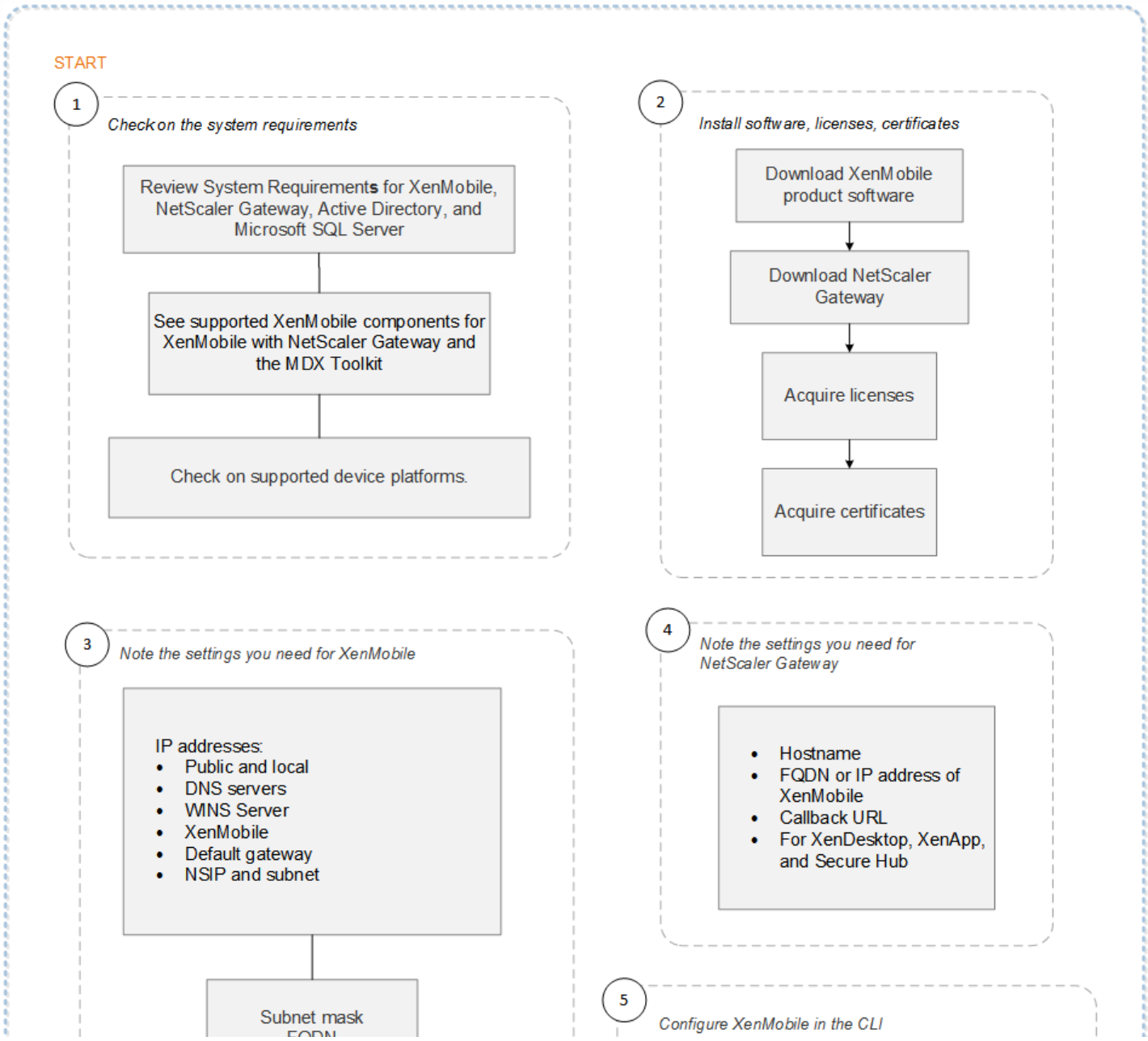
•	Pré-requisito	Componente	Anote a configuração
	Anote o nome de host e a URL externa do NetScaler Gateway. A URL externa é o endereço da Web ao qual os usuários se conectam.	XenMobile	
	Anote a URL de retorno de chamada do NetScaler Gateway.	XenMobile	
	Anote os endereços IP e as máscaras de sub-rede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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

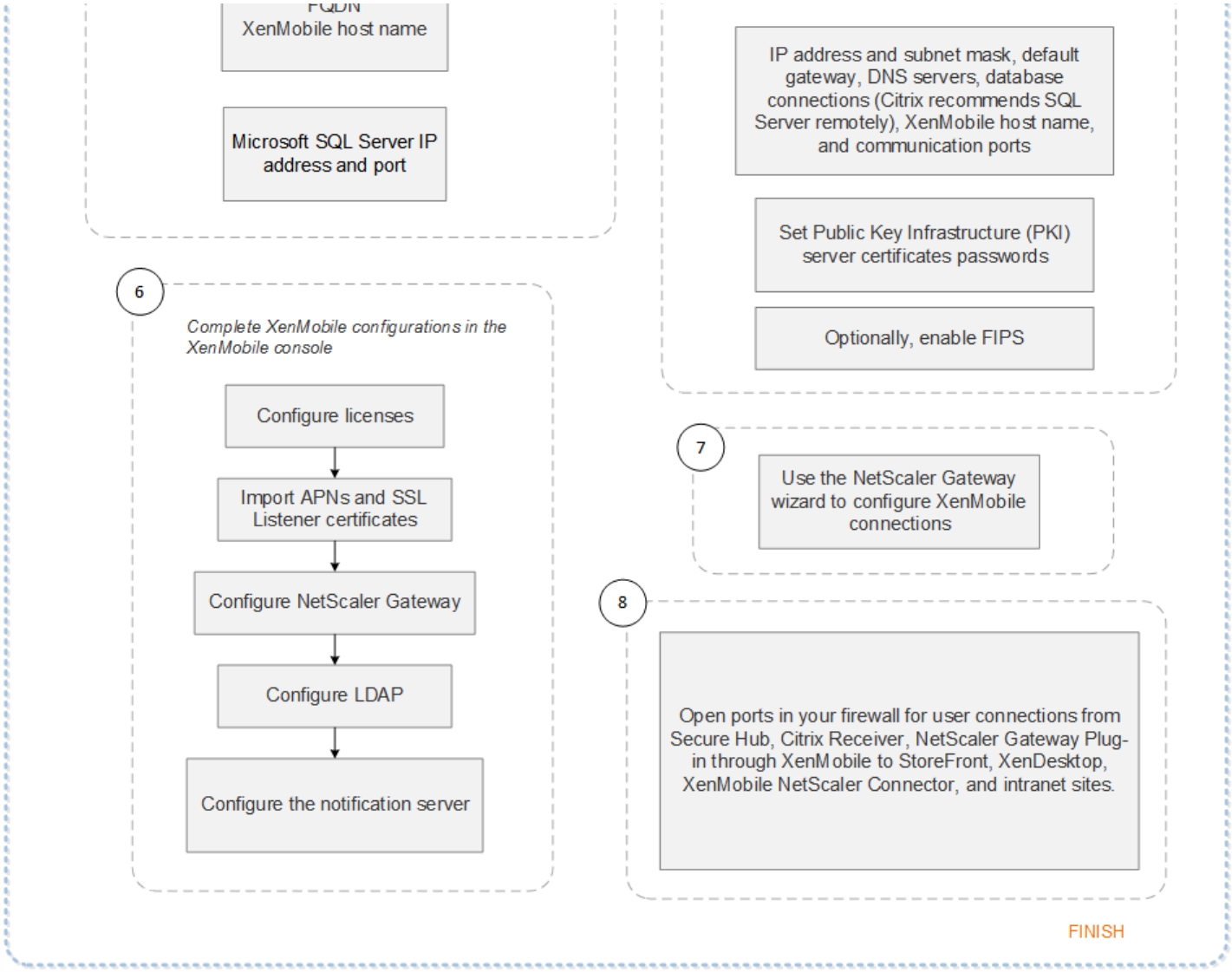
	Anote o FQDN público do XenMobile.	NetScaler Gateway	
	Note o FQDN público do Secure Hub.	NetScaler Gateway	

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.



© 1999-2017 Citrix Systems, Inc. All rights reserved.



1: Requisitos de 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 para o seu ambiente XenMobile

8: Requisitos de porta

O fluxograma também está disponível em formato PDF.

PDF Fluxograma de implantação do XenMobile

Instalar o XenMobile

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 executar estes procedimentos. Para obter detalhes, consulte a documentação do XenServer ou da 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 executar estes procedimentos. 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, tenha o cuidado de especificar as placas de interface de rede (NICs) no servidor que o Hyper-V usará para criar as redes virtuais. É possível reservar alguns NICs para o host.
- - Exclua o arquivo Virtual Machines/.xml
  - Mova o arquivo Legacy/.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: se você pretender instalar o XenMobile Server no modo FIPS, precisará atender a um grupo de pré-requisitos, conforme discutido em Configuração de FIPs.

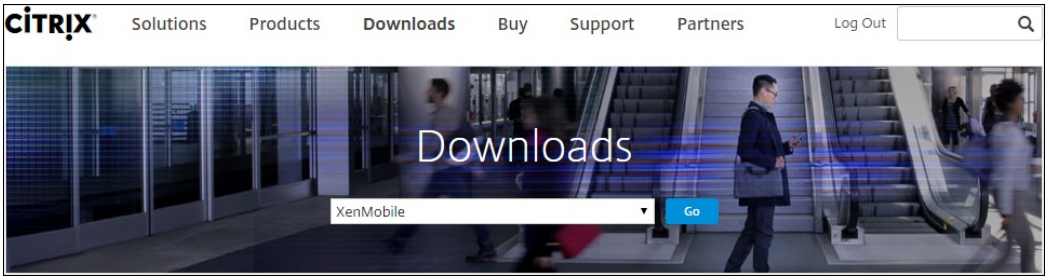
Baixar o software do produto XenMobile

Você pode baixar o software do produto no site da Citrix. Você precisa fazer login no site primeiro e, em seguida, usar o link Downloads na página da Web da Citrix para navegar até a página que contém o software que você desejar baixar.

Para baixar o software do XenMobile

1. Acesse 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 XenMobile.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. Clique em **Ir**. A página XenMobile é exibida.
6. Expanda **XenMobile Server**.
7. Expanda **Software do produto**.
8. Clique em **XenMobile Server 10**.
9. 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.
10. Siga as instruções na tela para baixar o software.

Para baixar o software do NetScaler Gateway

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

1. Acesse 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 Selecionar um produto, clique em NetScaler Gateway.
5. Clique em Ir. A página NetScaler Gateway é exibida.
6. Na página NetScaler Gateway, expanda a versão do NetScaler Gateway que você executa.
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 NetScaler VPX. Quando 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 desejar 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. Configure o endereço IP e a máscara de sub-rede, o gateway padrão, os servidores DNS do XenMobile e assim por diante usando 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

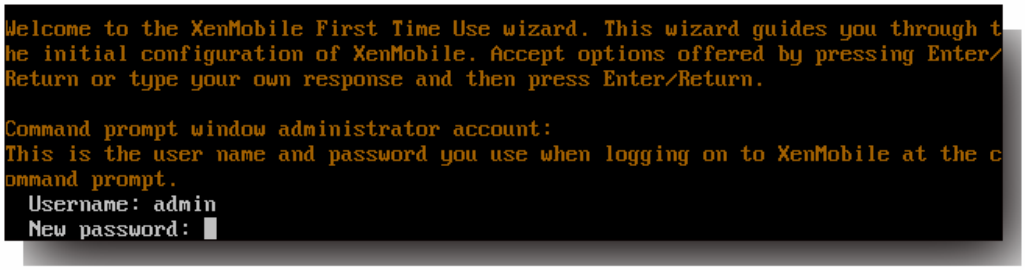
XenMobile.

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, do Hyper-V ou da 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.
   Importante:
   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 no mínimo oito caracteres e 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 !, $, #, %)

   Nota: nenhum caractere (como asteriscos) é exibido quando você digita a nova senha. Nada é exibido.

4. Forneça as seguintes informações da rede e, em seguida, digite y para confirmar as configurações:
   1. Endereço IP do servidor XenMobile
   2. Máscara de rede
   3. Gateway padrão, que é o endereço IP do gateway padrão no DMZ
   4. Servidor DNS principal, que é o endereço IP do servidor DNS
   5. Servidor DNS secundário (opcional)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

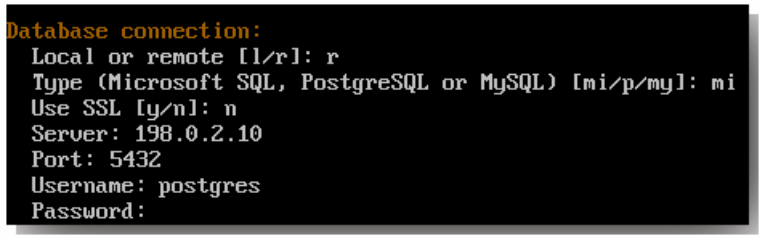
Nota: os endereços mostrados nesta e nas imagens a seguir são não funcionais e fornecidos somente como exemplo.

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.

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 Configuração do modo FIPs.

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



   1. O seu banco de dados pode ser local ou remoto. Digite l para local ou r para remoto.
   2. 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. O PostgreSQL é incluído com o XenMobile e deve ser usado localmente ou remotamente somente 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.
   3. Opcionalmente, digite y para usar a autenticação do SSL no seu banco de dados.
   4. Forneça o nome de domínio totalmente qualificado (FQDN) do servidor que hospeda o XenMobile. Esse servidor de

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

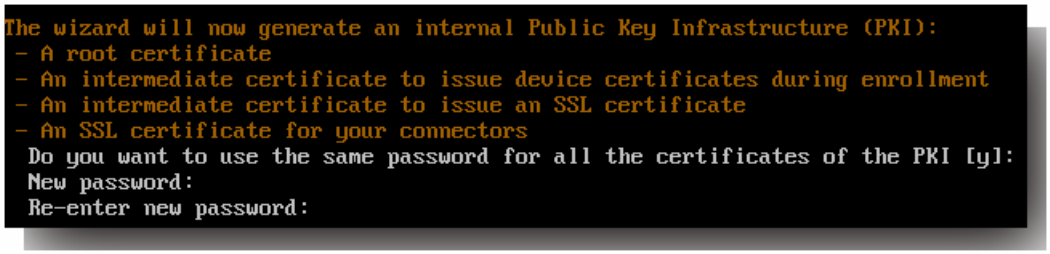
host fornece os serviços de gerenciamento de dispositivo e gerenciamento de aplicativo.

5. 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.
6. Digite o nome de usuário do seu administrador de banco de dados.
7. Digite a senha do seu administrador de banco de dados.
8. Digite o nome do banco de dados.
9. 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 servidor XenMobile.

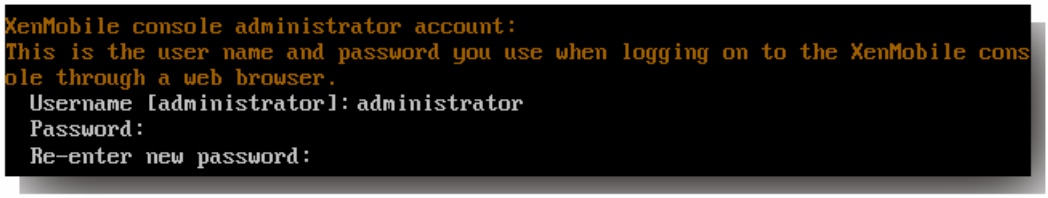
10. Pressione **Enter** para confirmar as configurações.
11. Identifique as portas de comunicação. Para obter detalhes sobre portas e seus respectivos usos, consulte Requisitos de porta.
    Nota: aceite as portas padrão pressionando **Enter** (Return em um Mac).

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 quiser 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.



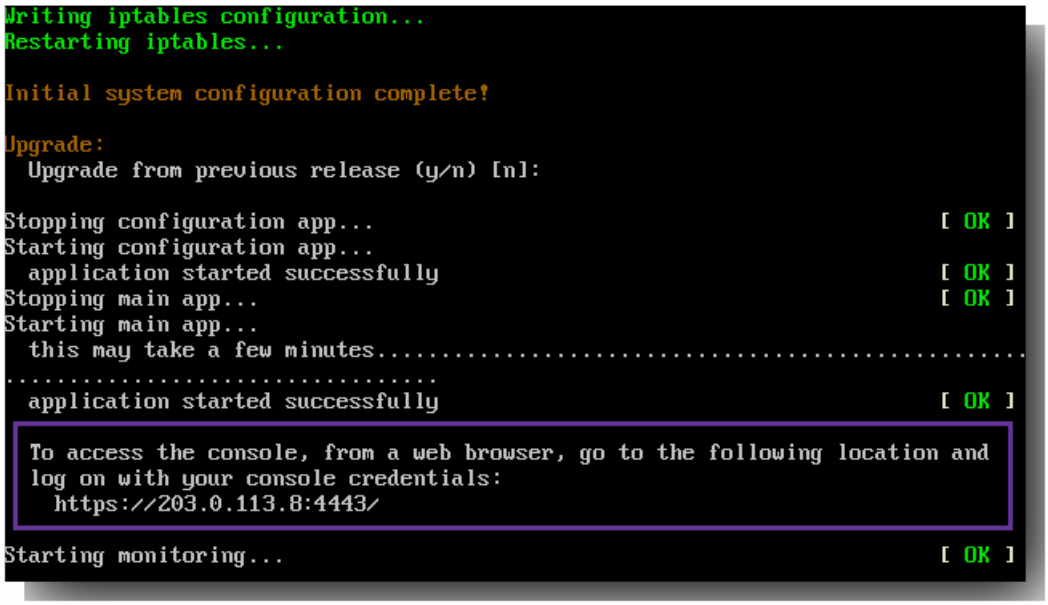
    Importante: Se você pretende realizar o clustering de nós ou instâncias do XenMobile juntos, deverá fornecer senhas idênticas para os nós subsequentes.
14. Digite a nova senha e, em seguida, redigite-a para confirmá-la.
    Nota: nenhum caractere (como asteriscos) é exibido quando você digita a nova senha. Nada é exibido.
15. Pressione **Enter** para confirmar as configurações.
16. Crie uma conta de administrador para fazer login no console XenMobile usando um navegador da Web. Memorize essas credenciais para uso posterior.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Nota: nenhum caractere (como asteriscos) é exibido quando você digita a nova senha. Nada é exibido.

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



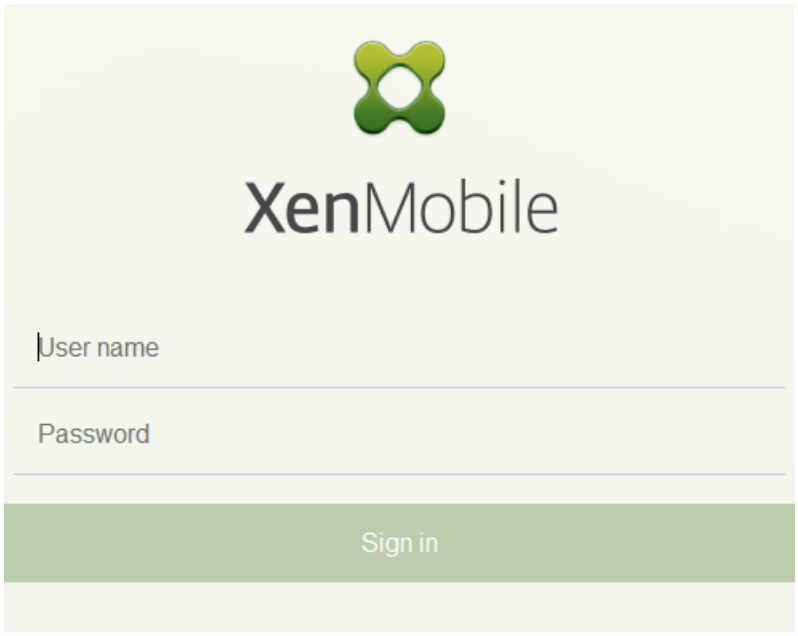
Configurar o XenMobile em um navegador da Web

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 Certificado, clique em Importar. A caixa de diálogo Importar é exibida.

6. Importe seus certificados de APNs e Ouvinte SSL. Se você gerenciar dispositivos iOS, você precisa de 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 NetScaler Gateway. Para obter detalhes sobre como configurar o NetScaler Gateway, consulte NetScaler Gateway e XenMobile e Configuring Settings for Your XenMobile Environment.

Nota:

- Você pode implantar o NetScaler 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 NetScaler Gateway antes que possam acessar qualquer recurso da rede interna.
- Embora o NetScaler 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 servidor XenMobile para ativar seus certificados.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurar o modo FIPS com o XenMobile

Feb 21, 2018

> **Nota**
>
> Os componentes do lado do servidor do XenMobile Service não são compatíveis com FIPS 140-2.

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

Antes de instalar um Servidor XenMobile no modo FIPS, você precisa concluir os pré-requisitos a seguir.

- Você deve usar um SQL Server 2012 ou 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 os Manuais online sobre o SQL Server.
- A comunicação SSL segura exige que um certificado SSL seja instalado no seu SQL Server. O certificado SSL pode ser um certificado público de uma AC comercial ou um certificado autoassinado de uma AC interna. Observe que 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.
- Se você usar um certificado autoassinado para o SQL Server, precisará de uma cópia do certificado de AC raiz que emitiu o certificado autoassinado. O certificado de AC raiz deve ser importado para o servidor XenMobile durante a instalação.

Configuração do modo FIPS

Você pode ativar o modo FIPS somente durante a instalação inicial do servidor XenMobile. Não é possível ativar o modo FIPS após a conclusão da instalação. Portanto, se você planeja usar o modo FIPS, deverá instalar o servidor XenMobile com o modo FIPS do início. Além disso, se você tiver um cluster do XenMobile, todos os nós do cluster deverão ser ativados para FIPS; você não pode ter uma mistura de servidores XenMobile FIPS e não FIPS no mesmo cluster.

Há uma opção **Alternar modo FIPS** 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 servidor XenMobile de produção.

1. Durante a instalação inicial, ative o **Modo FIPS**.

2. Carregue o certificado de AC raiz para o SQL Server. Se você tiver usando um certificado SSL autoassinado em vez de um certificado público no seu SQL Server, selecione **Sim** para essa opção e siga um dos seguintes procedimentos:

    a. Copie e cole o certificado de AC.

    b. Importe o certificado de AC. Para importar o certificado de AC, você deve publicá-lo em um site que possa ser acessado do servidor XenMobile usando uma URL HTTP. Para obter detalhes, consulte Upload do certificado no XenMobile.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 **Arquivo** > **Adicionar/remover snap-in** e clique duas vezes no item de certificados para adicionar o snap-in de certificados. Selecione a conta de computador e o computador local nas duas páginas do assistente.

   d. Clique em **OK**.

   e. Expanda **Certificados (computador local)** > **Pessoal** > **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 **Todas as tarefas** > **Gerenciar chaves privadas**.

   g. Em **Nomes de grupos ou usuários**, clique em **Adicionar**.

   h. Insira o nome da conta de serviço do SQL que você copiou na etapa anterior.

   i. Desmarque a opção **Permitir controle total**. 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)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Baixe o rootcert (base 64).

2. Copie o rootcert para o site padrão no servidor IIS, C:\inetpub\wwwroot.

3. Marque a caixa de seleção **Autenticação** do site padrão.

4. Defina **Anônimo** como **atiavado**.

5. Marque a caixa de seleção de regras **Acompanhamento de solicitações com falha**.

6. O arquivo .cer não pode estar bloqueado.

7. Navegue até a localização do .cer em um navegador Internet Explorer do servidor local, http://localhost/certname.cer. O texto do certificado raiz deve ser exibido no navegador.

8. Se o certificado raiz não for exibido no navegador Internet Explorer, 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. Abra o Internet Explorer e acesse http://localhost/cert.cer.

Para obter mais informações, consulte servidor Web (IIS).

> **Nota**
>
> Você pode usar a instância do IIS da AC 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
- Insira a URL HTTP a ser importada: http://*FQDN do servidor IIS*/cert.cer
- Servidor: *FQDN do SQL Server*
- Porta: 1433
- User name: a conta de serviço que tem a capacidade de criar o banco de dados (domínio\nome do usuário).
- Password: a senha da conta de serviço.
- Database Name: esse é um nome que você escolher.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 **verdadeiro**. Para obter mais informações, consulte Propriedades do cliente.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurar o clustering

Feb 21, 2018

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

- **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 NetScaler Gateway se comunique com os nós do XenMobile que estão configurados em um cluster. No XenMobile, por padrão, todo o tráfego do NetScaler Gateway é roteado para o endereço IP virtual do balanceamento de carga na porta 8443.

Os procedimentos neste artigo explicam o método de criação de uma nova máquina virtual (VM) do XenMobile e de ingresso da nova VM em uma VM existente, criando assim 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. Armazenamento em cluster não funciona corretamente, a menos que todos os servidores têm 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 NetScaler Gateway.
- Com o XenMobile é implantado em uma configuração de cluster e no modo somente MDM ou Enterprise (MDM+MAM): você deve modificar a configuração do balanceador de carga do NetScaler para usar a **Persistência do IP de origem** para todos os balanceadores de carga do NetScaler MDM, ou seja, servidores virtuais configurados para portas 8443 e 443. Conclua essa configuração antes de dispositivos de usuários atualizarem para o iOS 11. Para obter mais informações, consulte este artigo da 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 os diagramas de arquitetura de referência para o XenMobile 10.x nas configurações de cluster, consulte Arquitetura.

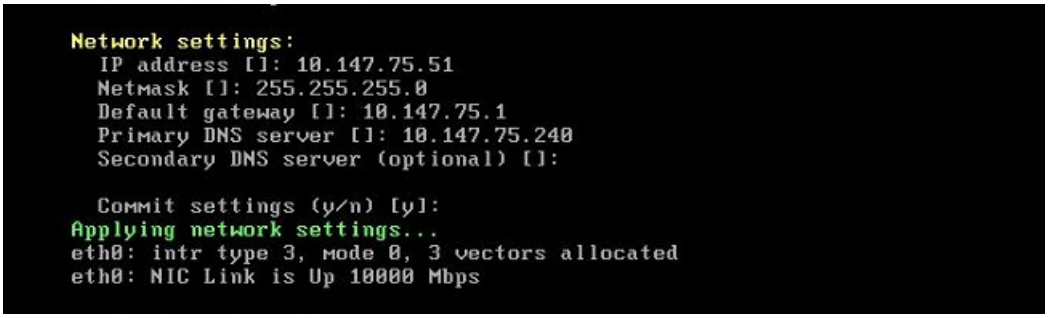
Instalando os nós de cluster do XenMobile

Com base no número de nós que você exigir, crie novas 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

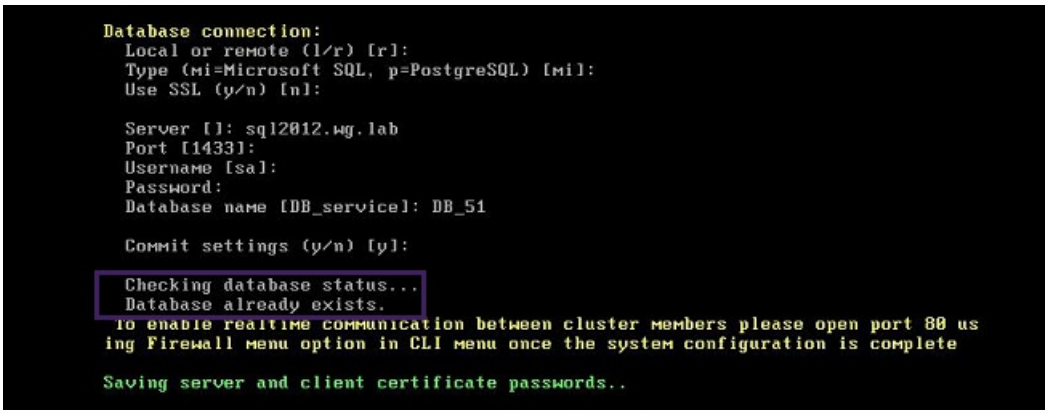
2. Forneça os detalhes de configuração de rede, conforme mostrado na figura a seguir.



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

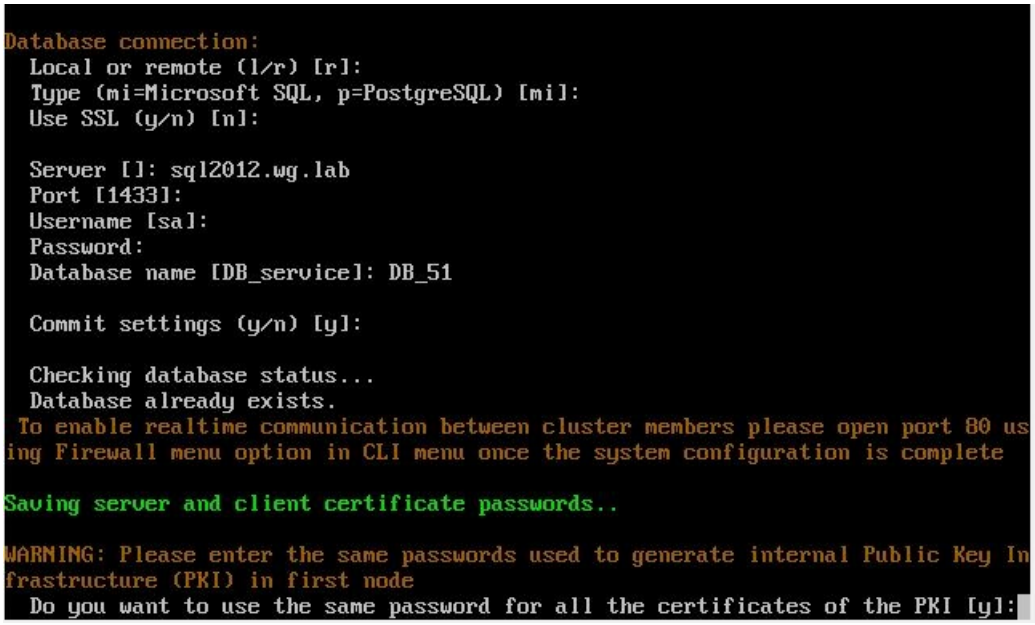
4. Se quiser usar o modo FIPS, digite y; caso contrário, n.

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.



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

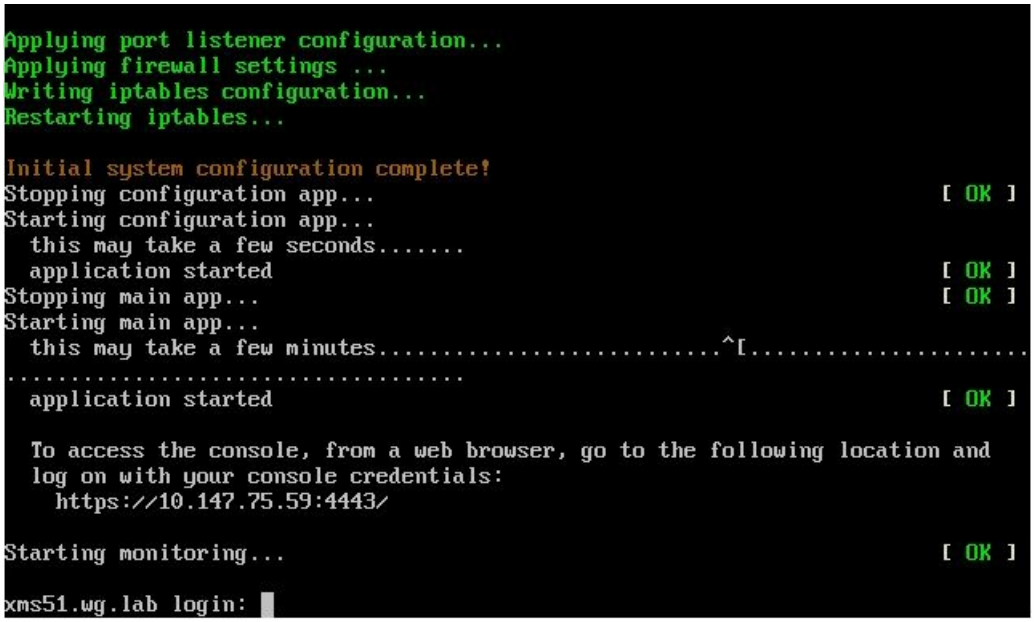
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.



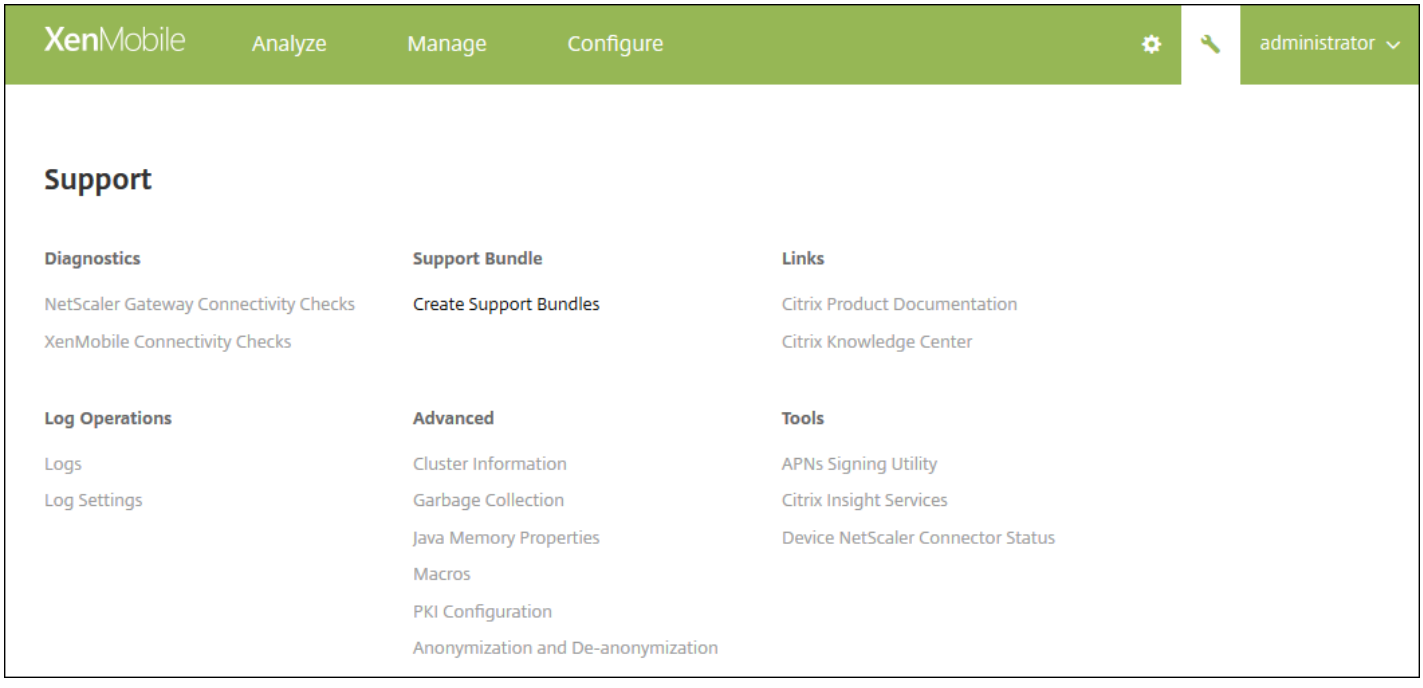
Nota: a caixa de diálogo de login é idêntica à caixa de diálogo de login da primeira VM. A correspondência é uma maneira de confirmar que ambas as VMs usam o mesmo servidor do banco de dados.

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 fenda no canto superior direito do console.

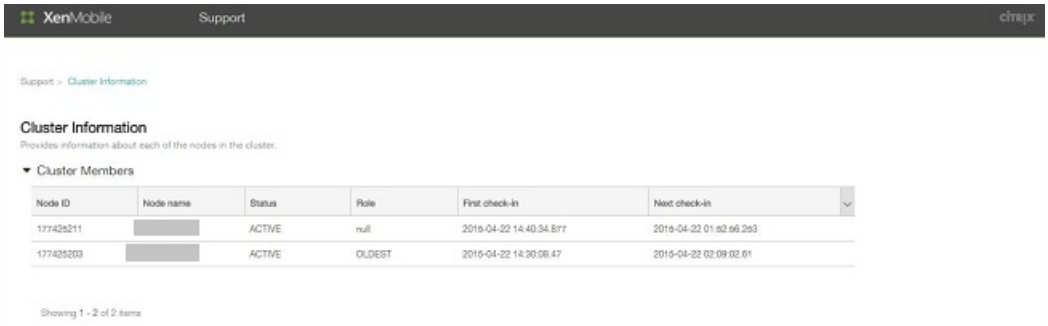
A página **Suporte** é aberta.

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



© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.



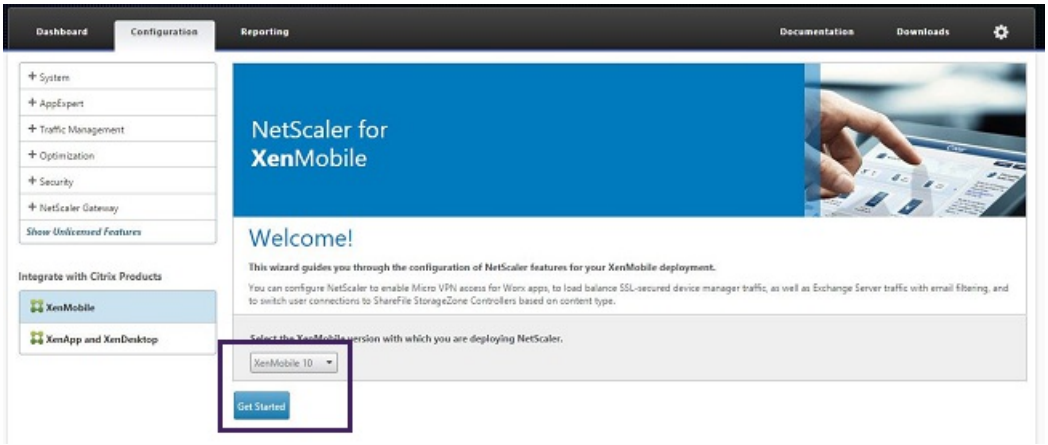
Você pode adicionar outros nós seguindo as mesmas etapas. O primeiro cluster adicionado ao nó tem uma Função de **MAIS ANTIGO**. Clusters adicionados depois disso mostrarão uma Função de **NENHUM** ou **nulo**.

Para configurar o balanceamento de carga do cluster do XenMobile no NetScaler

Depois de adicionar os nós como membros do cluster do XenMobile, você precisará balancear 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 NetScaler 10.5.x. Você pode seguir as etapas neste procedimento para balancear a carga do XenMobile usando o assistente.

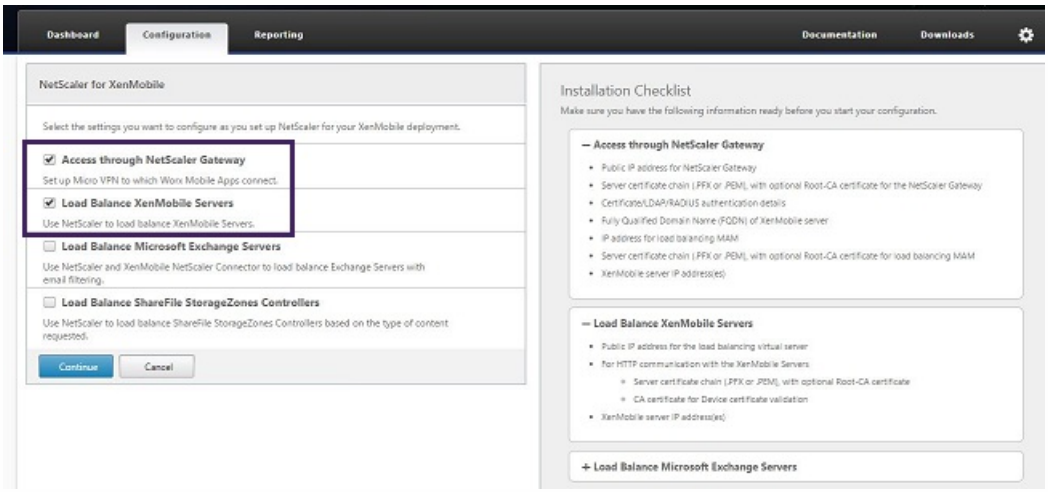
1. Faça login no NetScaler.

2. Na guia Configuração, clique em XenMobile e em Introdução.

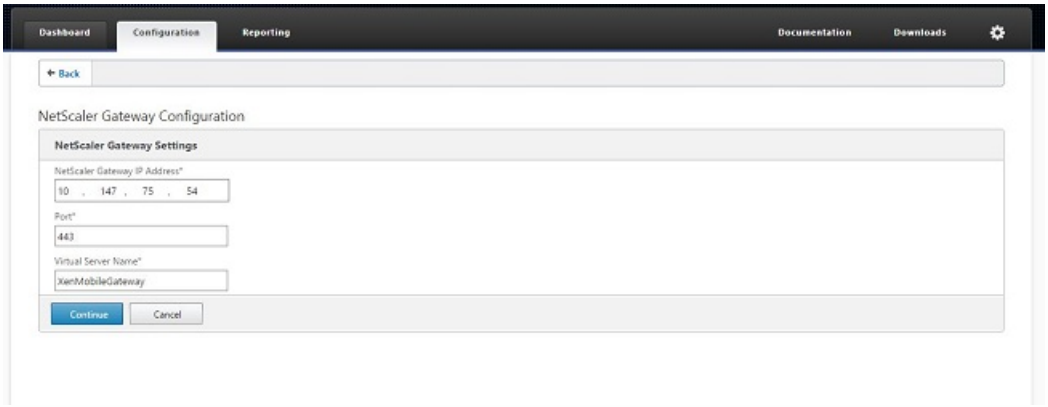


© 1999-2017 Citrix Systems, Inc. All rights reserved.

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



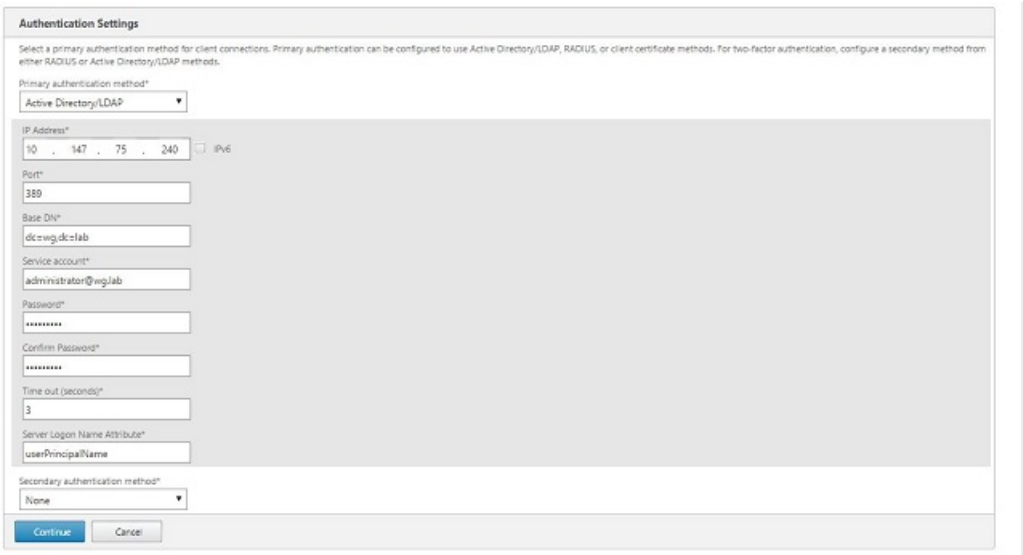
4. Insira o endereço IP do NetScaler Gateway e clique em Continue.



5. Associe o certificado de servidor ao endereço IP virtual do NetScaler 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.

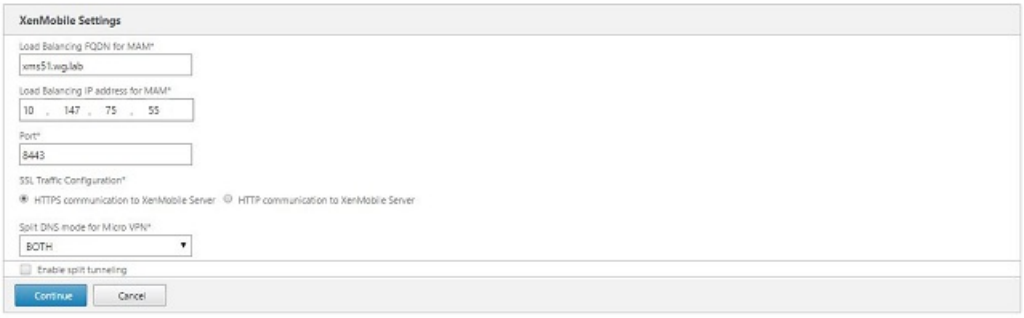
6. Insira os detalhes do servidor de Autenticação e clique em Continue.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Nota: verifique se o Server Logon Name Attribute é o mesmo que você forneceu na configuração LDAP do XenMobile.

7. Em XenMobile settings, insira o Load Balancing FQDN for MAM e clique em Continue.



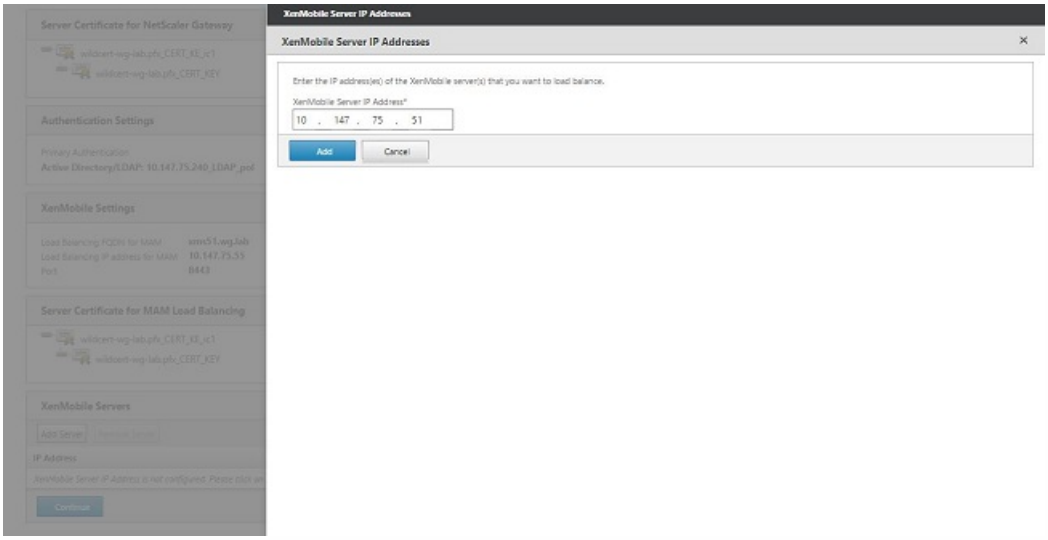
Nota: verifique se o FQDN do endereço IP virtual de balanceamento de carga MAM e o FQDN do XenMobile são os mesmos.

8. Se quiser usar o modo SSL Bridge (HTTPS), selecione HTTPS communication to XenMobile Server. No entanto, se quiser 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.

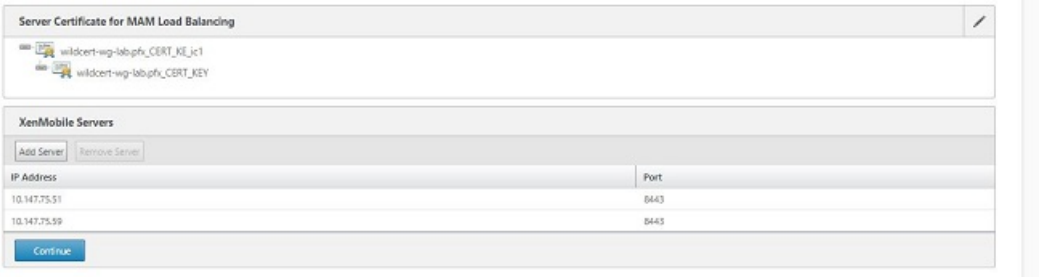
10. Em XenMobile Servers, clique em Add Server para adicionar os nós XenMobile.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

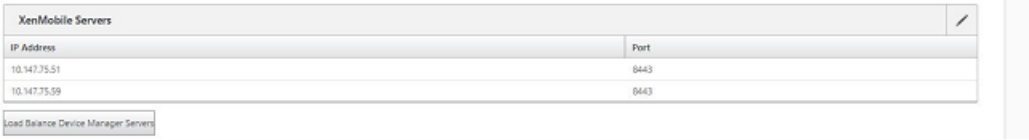
11. Insira o endereço IP do nó do XenMobile e clique em Add.



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

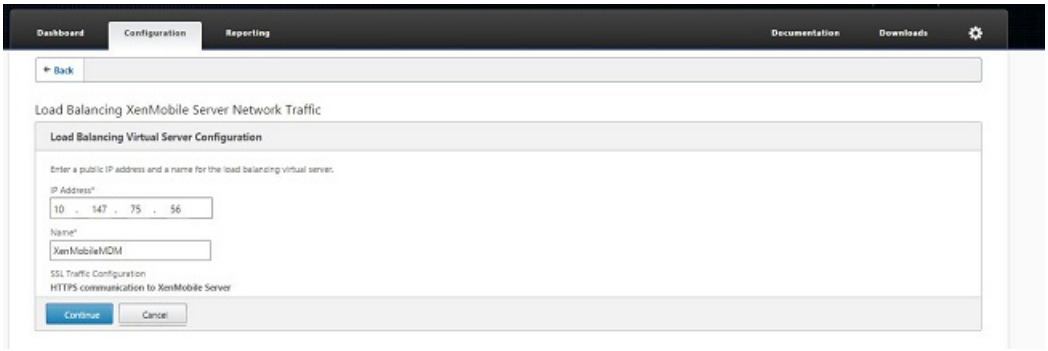


13. Clique em Load Balance Device Manager Servers para continuar com a configuração do balanceamento de carga MDM.

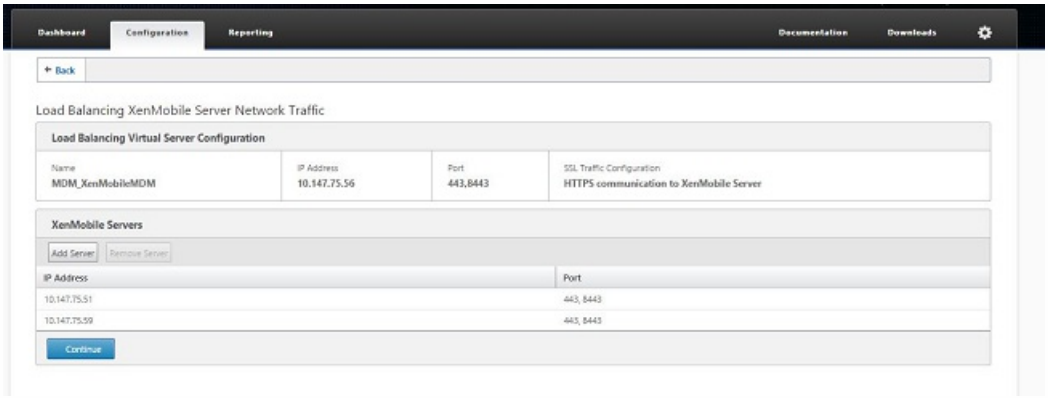


14. Insira o endereço IP a ser usado para o endereço IP de balanceamento de carga MDM e, em seguida, clique em Continue.

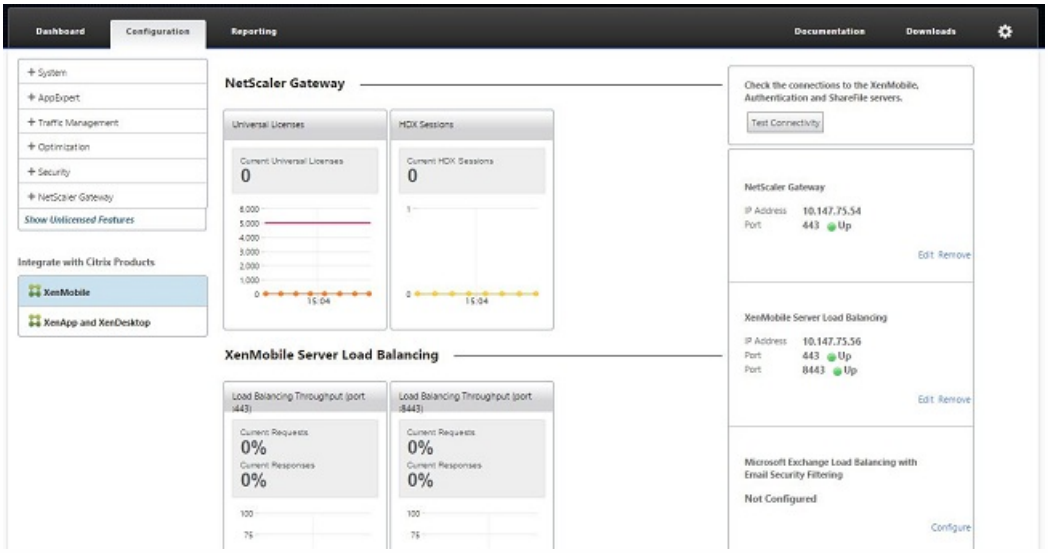
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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

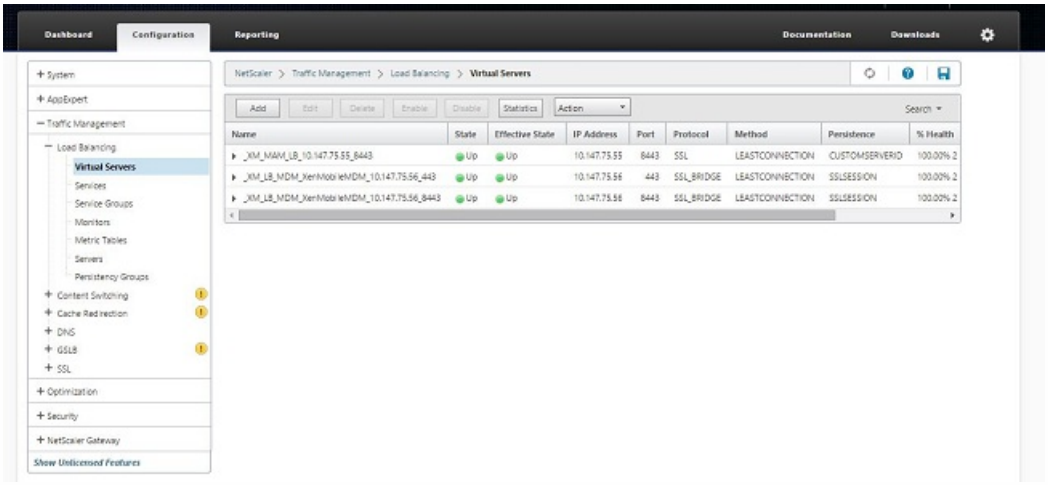


Você verá o status do endereço IP virtual na página XenMobile.

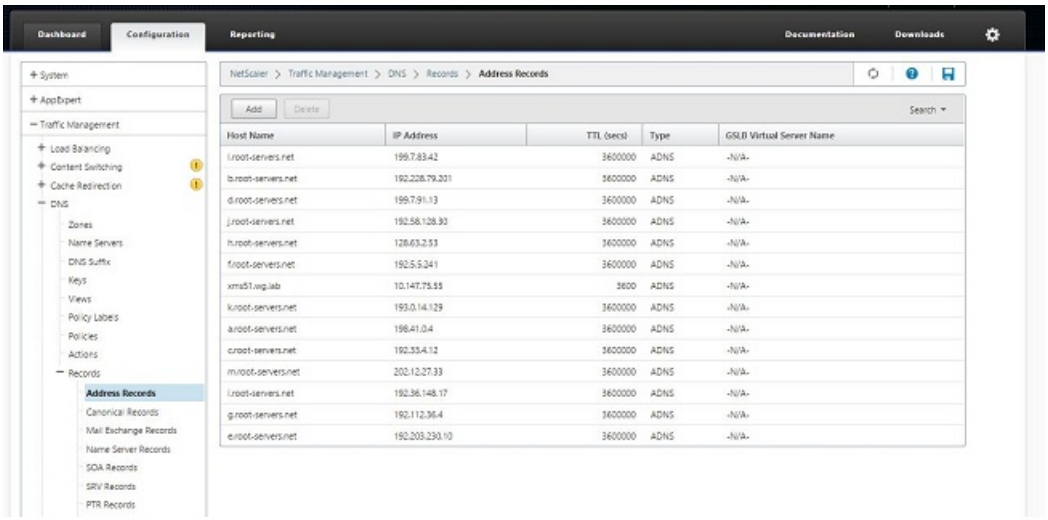


16. Para confirmar se os endereços IP virtuais estão em execução, clique na guia Configuration e navegue até Traffic Management > Load Balancing > Virtual Servers.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Você também verá se a entrada DNS no NetScaler aponta para o endereço IP virtual do balanceamento de carga MAM.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Guia de recuperação de desastres

Feb 21, 2018

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 manual de implantação do XenMobile recuperação de desastres artigo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

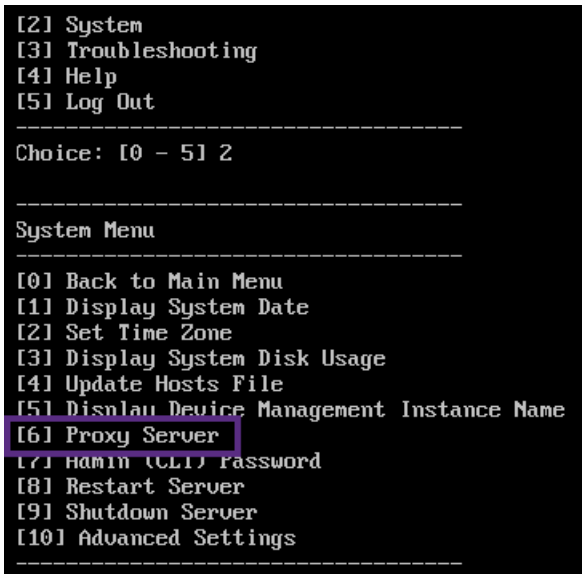
Ativar servidores proxy

Feb 21, 2018

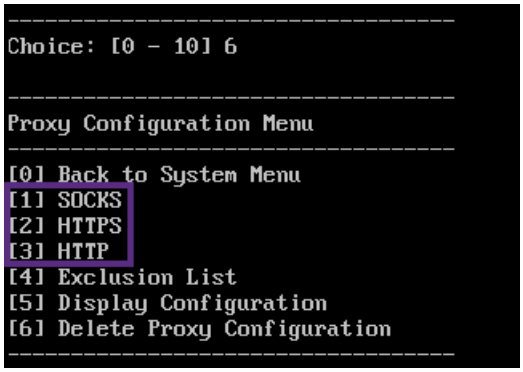
Quando você desejar controlar o tráfego de saída da Internet, poderá configurar um servidor proxy no XenMobile para transportar o tráfego. Para fazê-lo, você precisa configurar o servidor proxy usando a interface de linha de comando (CLI). Observe que a configuração do servidor proxy exige que você reinicie 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.



3. No menu Proxy Configuration, digite **1** para selecionar SOCKS, **2** para selecionar HTTPS ou **3** para selecionar HTTP.

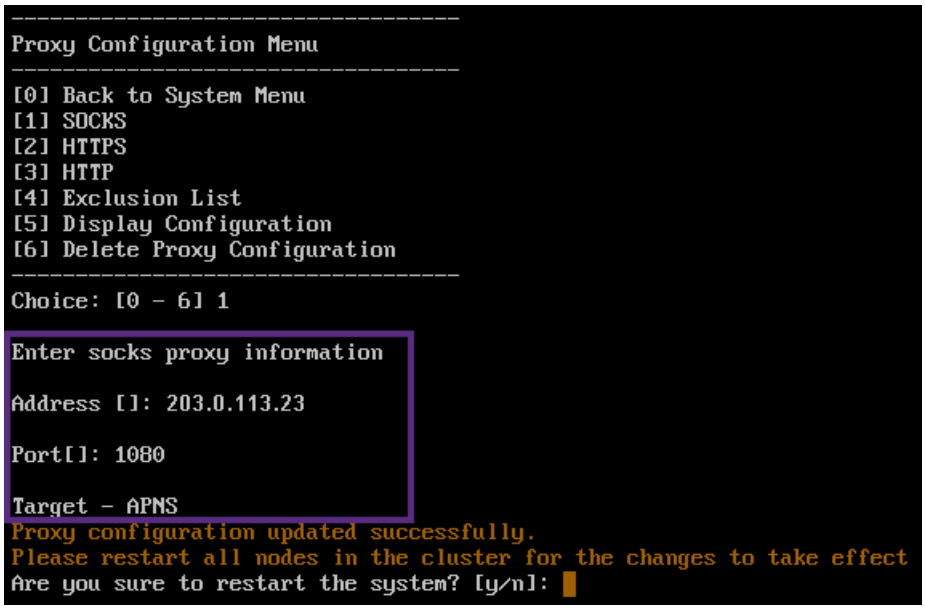


4. Digite o endereço IP, o número de porta e o destino do seu servidor proxy. Consulte a tabela a seguir para conhecer os tipos de destino compatíveis com cada tipo de servidor proxy.

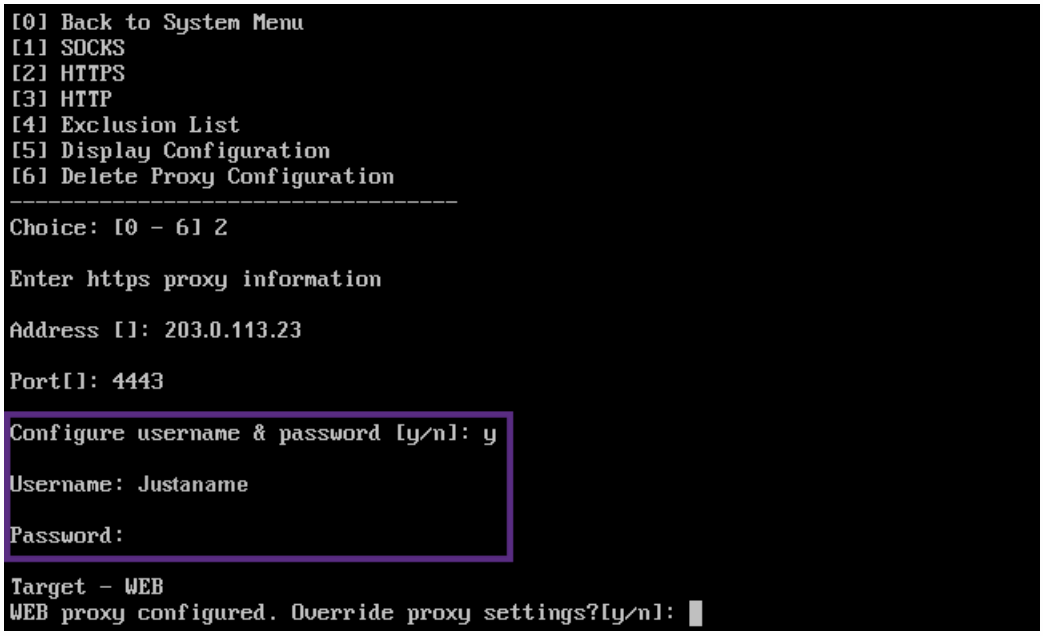
Tipo de proxy	Destinos compatíveis
SOCKS	APNS
HTTP	APNS, Web. PKI

© 1999-2017 Citrix Systems, Inc. All rights reserved.

HTTPS	Web, PKI
HTTP com autenticação	Web, PKI
HTTPS com autenticação	Web, PKI



5. Se você optar por configurar um nome do usuário e uma senha para autenticação no servidor proxy HTTP ou HTTPS, digite **y** e, em seguida, digite o nome do usuário e a senha.



6. Digite **y** para terminar de configurar o servidor proxy.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Drivers do SQL Server

Feb 21, 2018

XenMobile Service usa o driver jTDS para conexões com o SQL Server. Para mudar para o driver Microsoft JDBC, entre em contato com a Citrix Cloud Operations.[KP(1]

Para conexões com o SQL Server de um XenMobile Server no local, você pode usar o driver padrão, jTDS ou o driver Microsoft Java Database Connectivity (JDBC). O driver jTDS é o padrão quando você instala o XenMobile Server no local ou atualiza de um XenMobile Server que está 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.

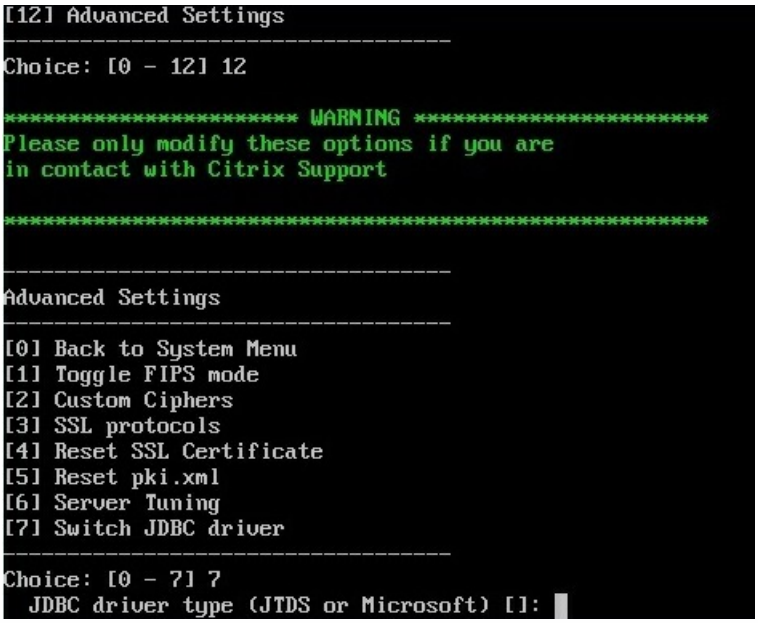
Quando você usa a autenticação do Windows com o driver Microsoft JDBC, o driver usa a autenticação integrada com o Kerberos. O XenMobile contata o Kerberos para obter os detalhes do Centro de Distribuição de Chave (KDC) Kerberos. Se os detalhes necessários não estiverem disponíveis, a CLI do XenMobile 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 menu System.
3. Digite **12** para selecionar Configurações avançadas.
4. Digite **7** para selecionar Mudar para driver JDBC e digite **m** para Microsoft.



5. Quando solicitado, digite **y** para escolher a autenticação SQL e, em seguida, digite o nome de usuário do SQL Server e a

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 menu System.
3. Digite **12** para selecionar Configurações avançadas.
4. Digite **7** para selecionar Alternar 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Propriedades do servidor

Feb 27, 2018

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 a Propriedades do servidor no manual virtual do XenMobile.

Definições de propriedade de servidor

Sempre adicionar dispositivo:

- Se **true**, XenMobile adiciona um dispositivo no console XenMobile, mesmo que o processo de inscrição falhe, para que você possa ver quais dispositivos tentaram 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.

Data/hora de execução de limpeza de logs 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. Assume **1** como padrão.

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 auditora (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**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Descrição: tempo limite de conexão LDAP

Chave: **Chave personalizada**
Chave: **auth.ldap.read.timeout**
Valor: **60000**
Nome de exibição: **auth.ldap.read.timeout**
Descrição: tempo limite de leitura 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 de conexão esgotado:

- 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**.

Limpeza do log de implantação (em dias):

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

Desativar verificação do nome do host:

- Por 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 VPP: 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

O padrão é **True**.

Ativar console:

- Se for **true**, permitirá o acesso do usuário ao console do Portal de autoatendimento. 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. Valor padrão: **true**.

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

- Se **True**, ativa 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 podem registrar apenas usando um convite para registro. O padrão é **true**.

Ativar gatilho de notificação:

- 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 necessários é **false** por padrão. Crie a chave personalizada e defina **Valor** como **true** para ativar a implantação forçada. Durante a implantação forçada, os aplicativos necessários habilitados para MDX, incluindo aplicativos corporativos e aplicativos da loja de aplicativos pública, atualizam-se imediatamente, mesmo que você configure uma política MDX para um período de tolerância de atualização de aplicativo e o usuário opte por atualizar o aplicativo mais tarde.

  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 necessários

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

permitidos e negados. 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 de chave personalizada**
: **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 Aprimoramento 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 ociosidade 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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 logoff 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). 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). 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. Padrão é **SCEP** .

Tamanho de chave de identidade de gerenciamento de dispositivo iOS:

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

Dias de renovação de identidade de gerenciamento de dispositivos iOS:

- 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 é **10** dias, quando um dispositivo se conecta 9 dias antes da expiração, XenMobile emite um novo certificado. 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:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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 inscrições ilimitadas do dispositivo.

  Chave = **number.of.mam.devices.per.user**
  Valor = **5**
  Nome de exibição = **Máximo de dispositivos somente MAM**
  Descrição = Limita o número de dispositivos MAM que cada usuário pode registrar.

MaxNumberOfWorker:

- O número de threads utilizados ao importar um grande número de licenças VPP. 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 VPP resulta em uso de CPU muito alto.

Single Sign-On do NetScaler:

- Se for **False**, desativará o recurso de retorno de chamada do XenMobile durante o logon único do NetScaler para XenMobile. Se a configuração de NetScaler Gateway incluir uma URL de retorno de chamad, o XenMobile usa o recurso de retorno de chamada para verificar o ID da sessão do NetScaler 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**. 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. 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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Recupera informações de dispositivos em blocos de tamanho especificad :

- 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 de logs de sessão (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 ShareFile :

- Especifica o tipo de armazenamento do ShareFile. **EMPRESARIAL** ativa o modo Empresarial do ShareFile. **CONECTORES** fornece acesso somente para StorageZone Connectors que você cria por meio do console XenMobile. Padrão é **NENHUM**, que mostra a exibição inicial da tela **Configurar > ShareFile** em que você escolher entre ShareFile Enterprise e Conectores. O padrão é **NENHUM**.

Tempo limite estático em minutos:

- Se a propriedade **Tipo de tempo limite de WebServices** for **STATIC_TIMEOUT:** Essa propriedade define o número de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

minutos após os quais o XenMobile faz logoff 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** permite mensagens. O padrão é **true**.

Disparar supressão de som de agente:

- Ativa ou desativa os sons de cliente do Secure Hub. O valor **false** permite 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 for Work. O XenMobile precisa dessa propriedade se a opção do Android for Work 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 o ID do ActiveSync para realizar um apagamento do ActiveSync do dispositivo:

- Se for **true**, o XenMobile Mail Manager 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 usuários para usuários do ActiveSync Exchange. O padrão é **false**.

Intervalo de linha de base do VPP:

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Se você tem muitas licenças do VPP 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 do VPP 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 do VPP for de 60 minutos, o intervalo entre linhas de base poderá ser atrasado até 119 minutos.

Tipo de tempo limite dos serviços da Web:

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

  Se **INACTIVITY_TIMEOUT**, o XenMobile considera um token de autenticação como expirado após o valor especificado na propriedade de servidor **Tempo limite de inatividade em minutos**. O padrão é **STATIC_TIMEOUT**.

Validade estendida do certificado MDM do Windows Phone (5 anos, 5y)):

- 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 dowloads de aplicativos não autenticados. O padrão é **3600000**.

Intervalo máximo de inatividade do console do portal de autoatendimento do 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

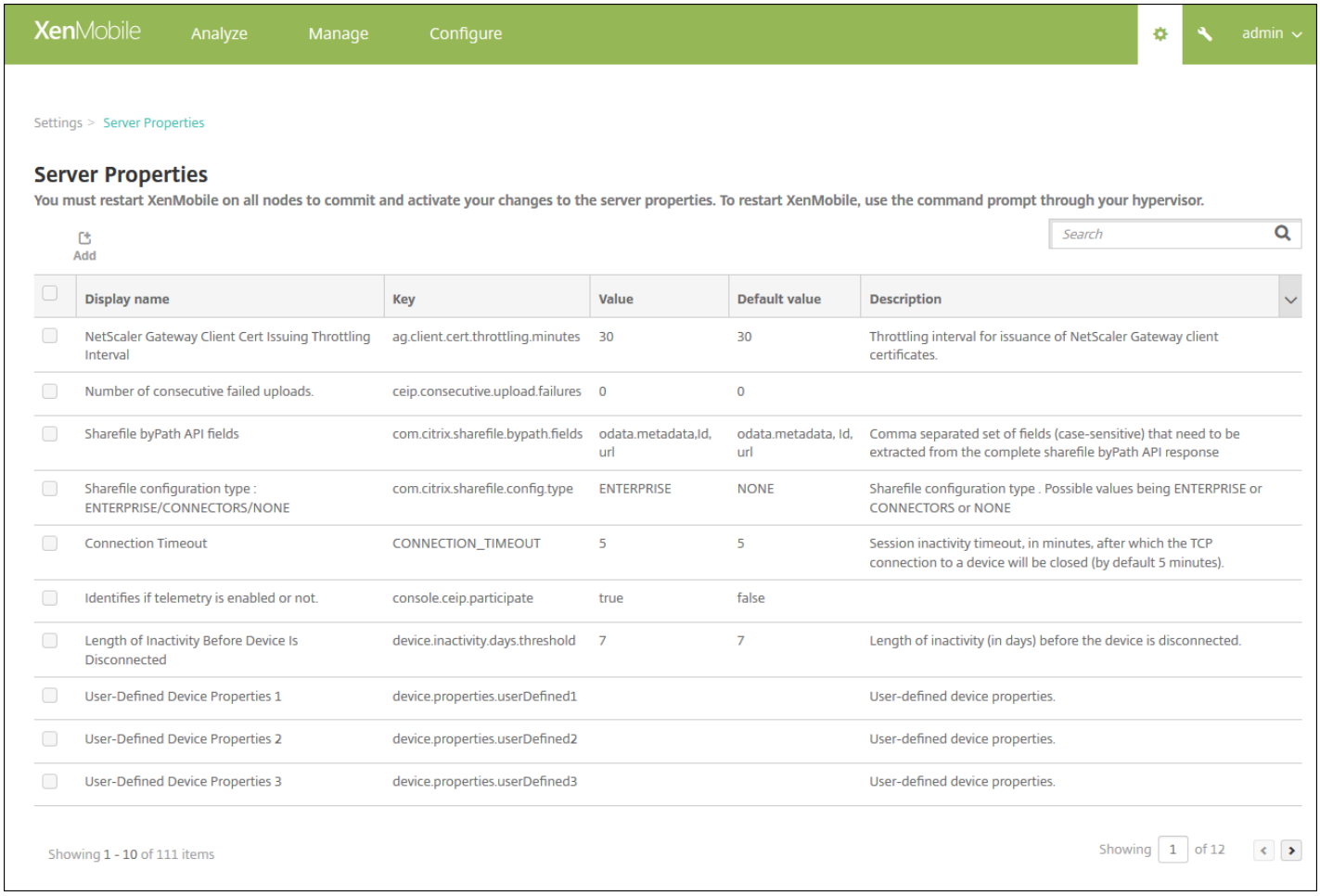
© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 **Configurações** é exibida.

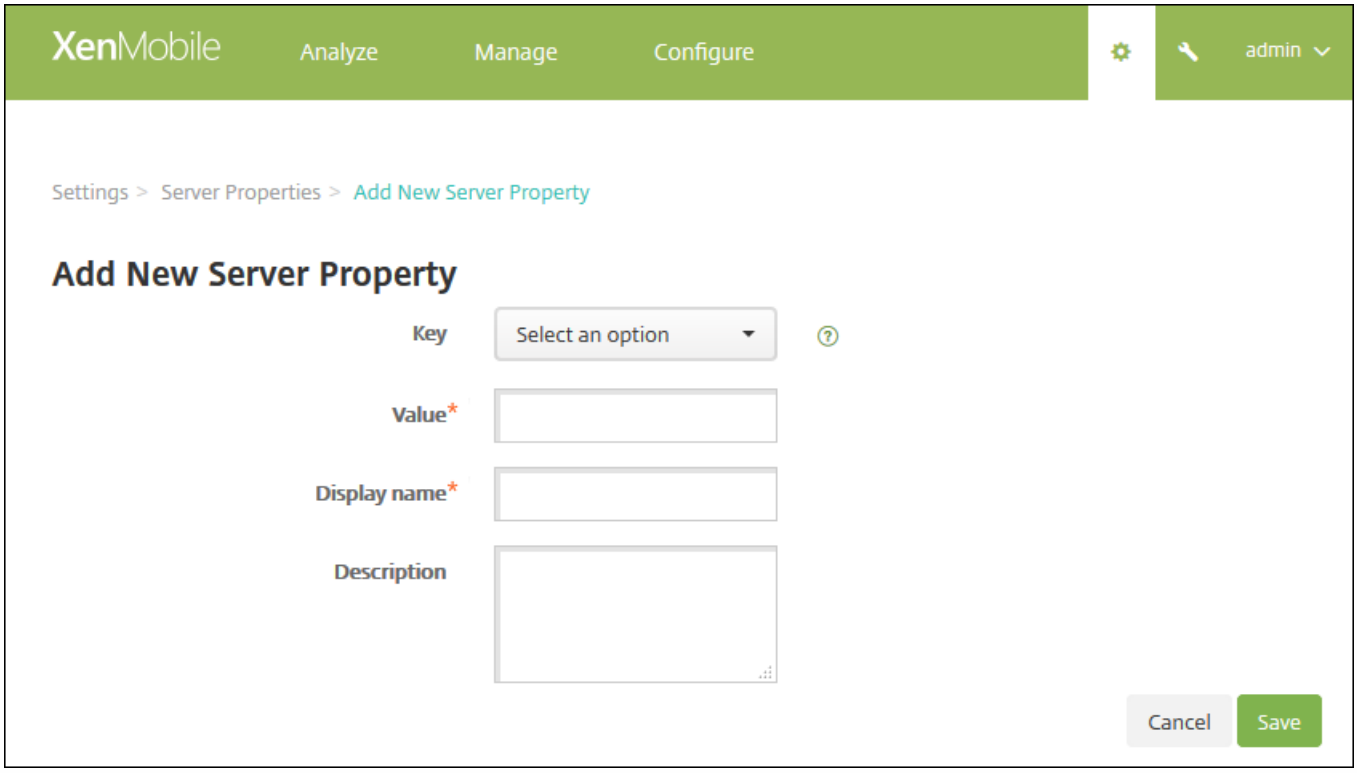
2. Em **Servidor**, clique em **Propriedades do servidor**. A página **Propriedades do servidor** é exibida. Você pode adicionar, editar ou excluir propriedades do servido nessa página.



Para adicionar uma propriedade de servidor

1. Clique em **Adicionar**. A página **Adicionar nova propriedade de servidor** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 novo valor da propriedade que é exibido na tabela **Propriedades do servidor.**
- **Descrição**: opcionalmente, digite uma descrição para a nova propriedade de servidor.

3. Clique em **Salvar**.

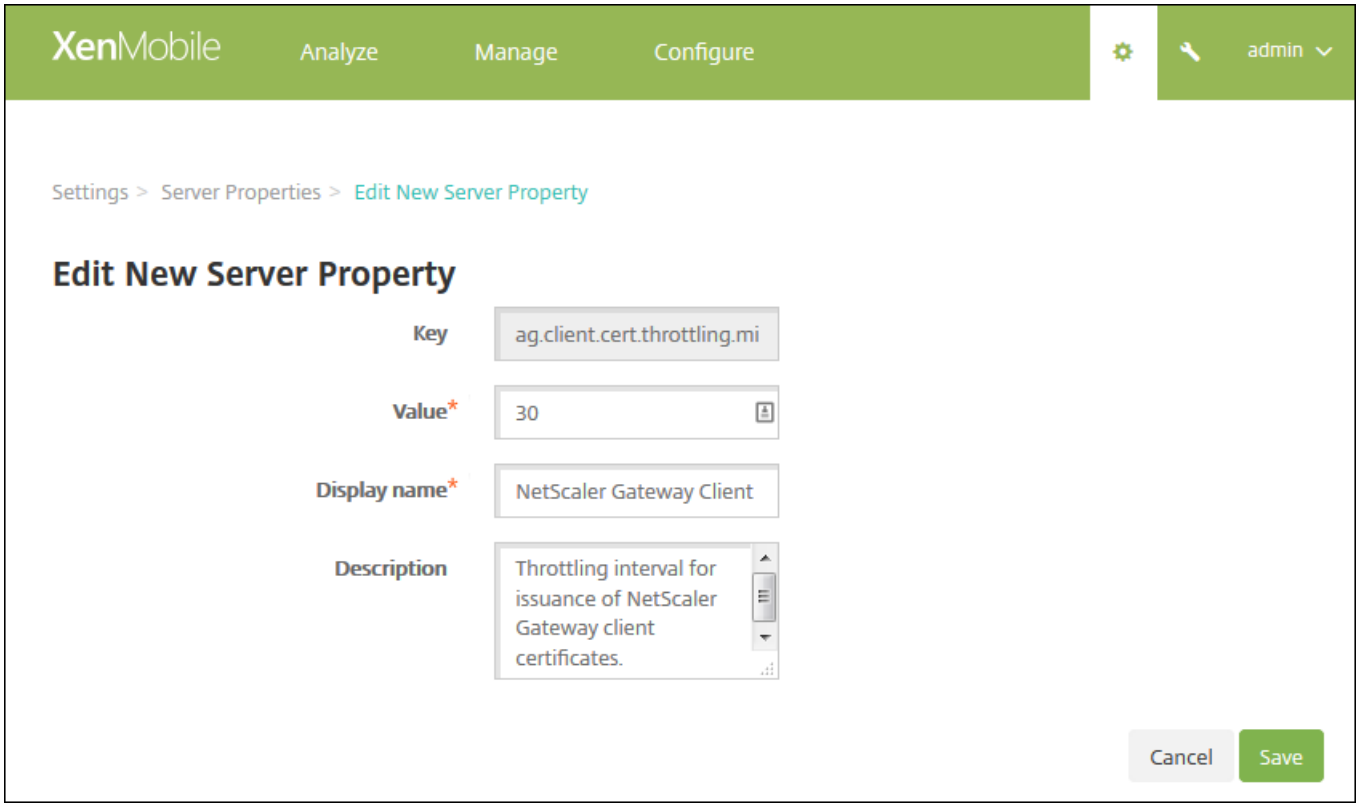
Para editar uma propriedade de servidor

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

   Nota: 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. 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 nova propriedade de servidor** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 desejar excluir.

   Nota: 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Opções da interface de linha de comando

Feb 21, 2018

Para uma instalação no local do XenMobile Server, você pode acessar as opções de CLI a qualquer momento 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 logon sua conta de administrador para o XenMobile. Para obter detalhes, consulte a documentação do hipervisor.
- **SE o SSH está ativado no firewall, usando o SSH**. Faça logon sua conta de administrador para o XenMobile.

Você pode executar uma variedade de tarefas de configuração e resolução de problemas por meio do CLI. Veja a seguir é o menu de nível superior para 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 Configuração** e as configurações exibidas para cada opção.

```
-----------------------------------
Configuration Menu
-----------------------------------
[0] Back to Main Menu
[1] Network
[2] Firewall
[3] Database
[4] Listener Ports
-----------------------------------
```

[1] Rede

```
 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]:
```

firewall [2]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
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] Banco de dados

```
  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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
---------------------------------
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:

> Para ativar a comunicação em tempo real entre os membros de cluster, abra a porta 80 usando a opção de menu de Firewall no menu CLI. Também configure Access white list em configurações de Firewall para o acesso restrito.

Quando você opta por desativar clusters, a seguinte mensagem é exibida:

> Você escolheu desativar clusters. Acesso à porta 80 não é necessário. Desativá-la.

[3] Cluster member white lista

```
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] Ativar ou desativar SSL offload

Quando você seleciona ativar ou desativar a descarga de SSL, a seguinte mensagem é exibida:

> Ativar SSL offload abre a porta 80 para todos. Configure a lista branca do Access em configurações de Firewall para o acesso restrito.

[5] Display Hazelcast Cluster

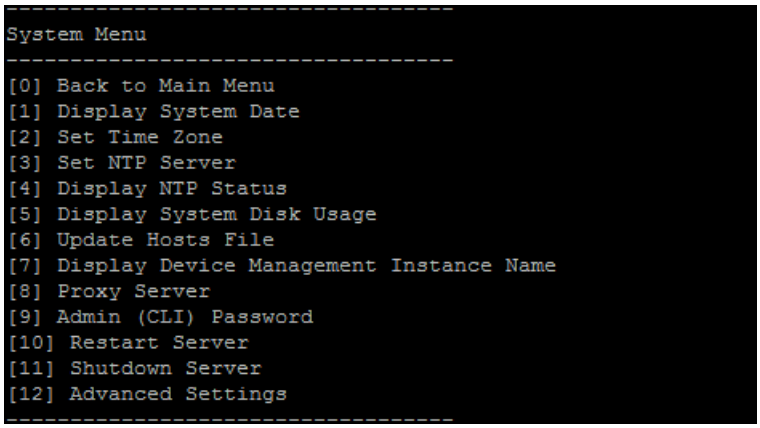
Quando você seleciona exibir o Hazelcast Cluster, as seguintes opções são exibidas:

> Membros do cluster Hazelcast:
>
> [Endereços IP listados]
>
> Nota: Se um nó configurado não fizer parte do cluster, reinicialize o nó.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

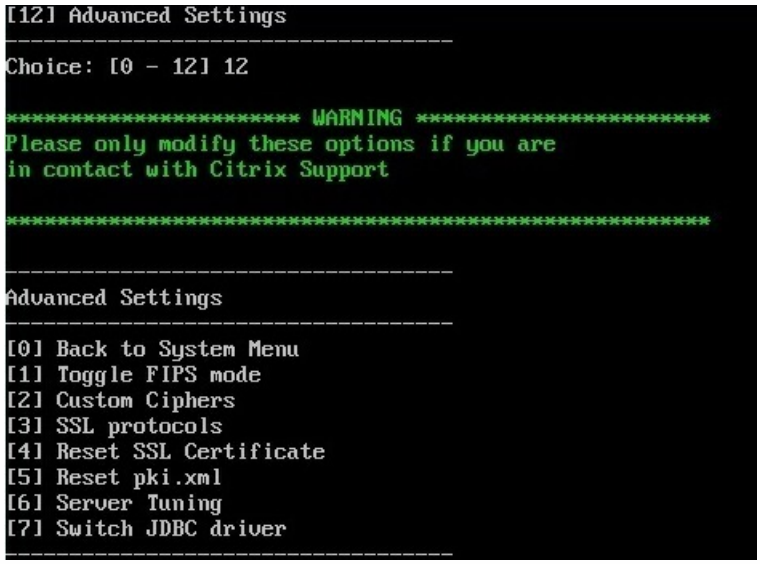
Opções do sistema

No **Menu System**, você pode exibir ou definir informações no nível do sistema, reiniciar ou desligar o servidor ou ter acesso ao menu **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.

[12] Configurações avançadas



As opções de **Protocolos SSL** assumem como padrão todos os protocolos permitidos. Após o aviso de **Ativar novos protocolos de SSL**, 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, em seguida, digite **y** para reiniciar o XenMobile Server.

Server Tuning opções incluem o limite de conexão do servidor, máximo de conexões (pela porta), e maximum threads (pela porta).

As opções **Switch JDBC driver** são **jTDS** e **Microsoft** JDBC. 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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
---------------------------------
```

[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] Pacote de suporte

```
---------------------------------
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
---------------------------------
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Introdução aos fluxos de trabalho para o console XenMobile

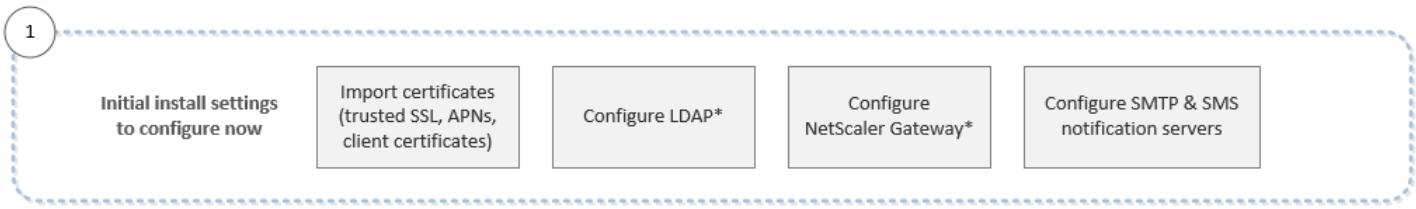
Feb 21, 2018

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:

- Autenticação
- NetScaler 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 for Work. Para obter detalhes, consulte Android for Work.
- Verifique o seu nome de domínio junto ao Google. Para obter detalhes, consulte Verify your domain for G Suite.
- Ative APIs e crie uma conta de serviço do Android for Work. Para obter detalhes, consulte a Android enterprise Help.

iOS

- Crie um ID Apple e uma conta de desenvolvedor. Para obter detalhes, consulte o site do Apple Developer Program.
- Crie um certificado Apple Push Notification Service (APNs). Se você planeja gerenciar dispositivos iOS com a sua implantação do XenMobile Service (nuvem), precisará de um certificado Apple APNS. Se usar notificações por push para a implantação do WorxMail, você também precisa de um certificado de 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 WorxMail para iOS.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Crie um token de empresa do Volume Purchase Program (VPP). Para obter detalhes, consulte o Apple Volume Purchase Program.

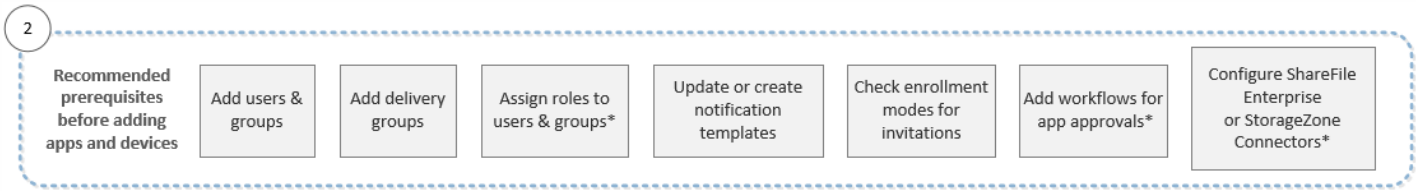
Windows

- Crie uma conta de desenvolvedor da Microsoft Windows Store. Para obter detalhes, consulte o Centro de Desenvolvimento do Microsoft Windows.
- Obtenha um ID de Publicador da Microsoft Windows Store. Para obter detalhes, consulte o Centro de Desenvolvimento do Microsoft Windows.
- Adquira um certificado empresarial da Symantec. Para obter detalhes, consulte o Centro de Desenvolvimento do Microsoft Windows.
- 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 o Centro de Desenvolvimento do Microsoft Windows.

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.



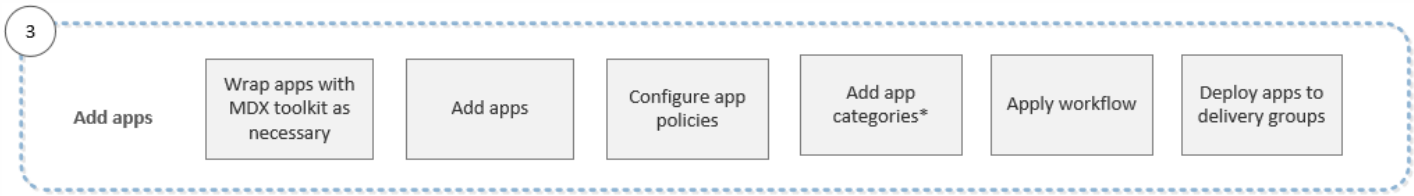
Para obter mais informações sobre cada configuração, juntamente com procedimentos passo a passo, consulte os seguintes artigos e seções da Documentação de Produtos Citrix:

- Contas de usuário, funções e registro
- Implantar recursos
- Configurar funções com RBAC
- Notificações
- Criar e gerenciar fluxos de trabalho
- Uso do ShareFile com o 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:

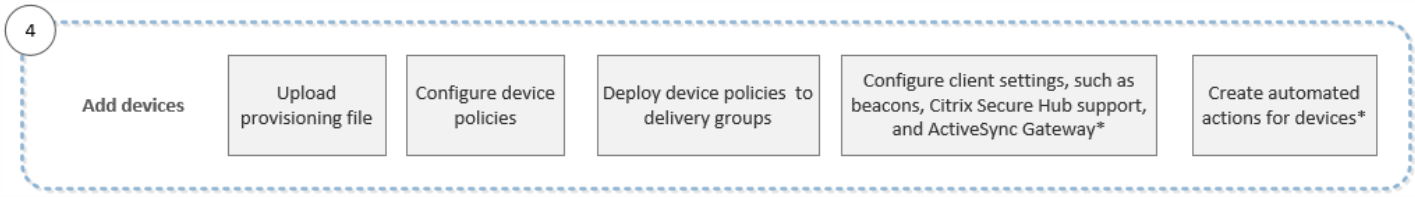
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Sobre o MDX Toolkit
- Adicionar aplicativos
- Resumo das políticas do MDX
- Criar e gerenciar 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.

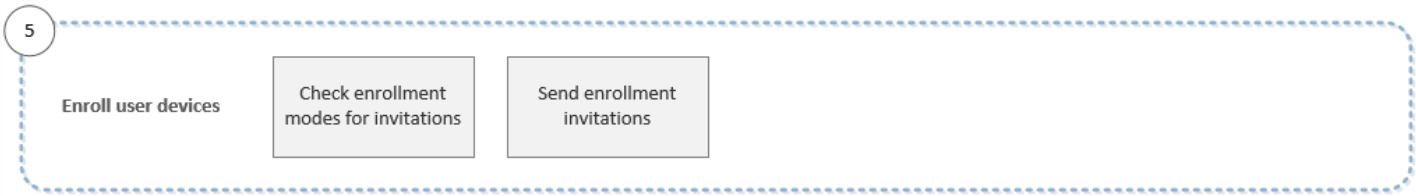


Para obter mais informações sobre cada configuração, juntamente com procedimentos passo a passo, consulte os seguintes artigos e seções da Documentação de Produtos Citrix:

- Dispositivos
- Sistemas operacionais de dispositivos compatíveis
- 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:

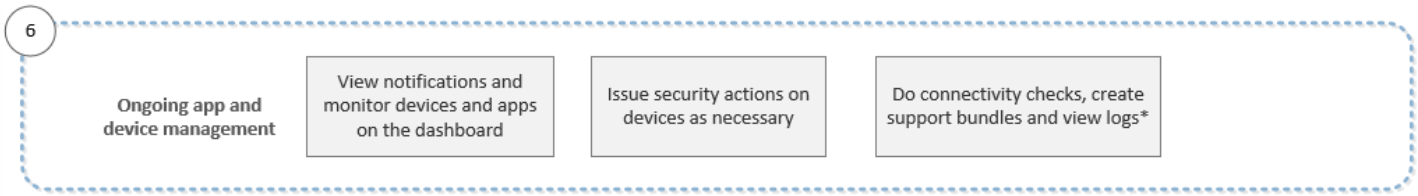
- Contas de usuário, funções e registro
- Notificações

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Para obter mais informações sobre as opções de suporte encontradas ao clicar no ícone de chave inglesa no canto superior direito do console XenMobile, consulte Monitoramento e suporte.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Certificados e autenticação

Feb 21, 2018

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. As opções para os usuários que entram são: se desejam tornar o processo de inscrição aberto para todos os registros ou apenas por convite e se deve ser exigida uma autenticação de dois ou uma autenticação 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.
- **NetScaler**: o NetScaler oferece o encerramento de sessões de micro VPN SSL. O NetScaler 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 funciona com o XenMobile Server em operações de registro. O Secure Hub é a entidade em um dispositivo que se comunica com o NetScaler: quando uma sessão expira, o Secure Hub obtém um tíquete de autenticação do NetScaler e passa o tíquete para os aplicativos MDX. A Citrix recomenda o uso de certificate pinning, o que impede ataques de intermediários. Para obter mais informações, consulte a seção sobre certificate pinning no artigo Secure Hub.

  O Secure Hub também facilita o contêiner de segurança MDX contêiner: o Secure Hub envia as políticas, cria uma sessão com o NetScaler 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 NetScaler, impõem restrições de modo offline como tempos limite.

Para obter mais informações sobre as considerações sobre como configurar a autenticação, incluindo uma visão geral dos métodos de autenticação de fator único e dois fatores, consulte o artigo Authentication 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 login único com ShareFile
- Configurações do servidor do Active Directory do Microsoft Azure

Certificados

Por padrão, o XenMobile vem com um certificado de Protocolo SSL gerado durante a instalação para proteger os fluxos de comunicação com o servidor. A Citrix recomenda substituir o certificado SSL por um certificado SSL confiável de uma autoridade de certificação (AC) conhecida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

> **Nota**
>
> Os dispositivos iOS 10.3 não oferecem suporte a certificados autoassinados. Se o XenMobile usa certificados autoassinados, os usuários não podem registrar dispositivos iOS 10.3 para o XenMobile. Para registrar dispositivos que executam o iOS 10.3 ou posterior no XenMobile, você deve usar certificados confiáveis do SSL no XenMobile.

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 criar um certificado de serviço de Notificação por Push da Apple (APNs) da Apple. Para conhecer as etapas, consulte Certificados de 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**
NetScaler Gateway	PEM (BASE64), PFX (PKCS#12)	SSL, Root: o NetScaler 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 dá suporte a certificados com uma extensão .pem. Para usar um certificado .pem, divida o arquivo .pem em um certificado e uma chave e importe cada um para o servidor XenMobile.
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. Note que 1024 bits certificados são vulneráveis.

Para o NetScaler 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 NetScaler 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 NetScaler Gateway ou no XenMobile.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Carregando certificados no XenMobile

Cada certificado que você carrega tem uma entrada na tabela de Certificados, que resume o 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 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 que você carrega.

Carregando certificados para o console

Ao carregar certificados para o console, você tem duas opções principais:

- Você pode clicar para importar um keystore. Em seguida, você deve identificar a entrada no repositório keystore que deseja instalar, a menos que você está carregando um formato PKCS#12.
- Você pode 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.

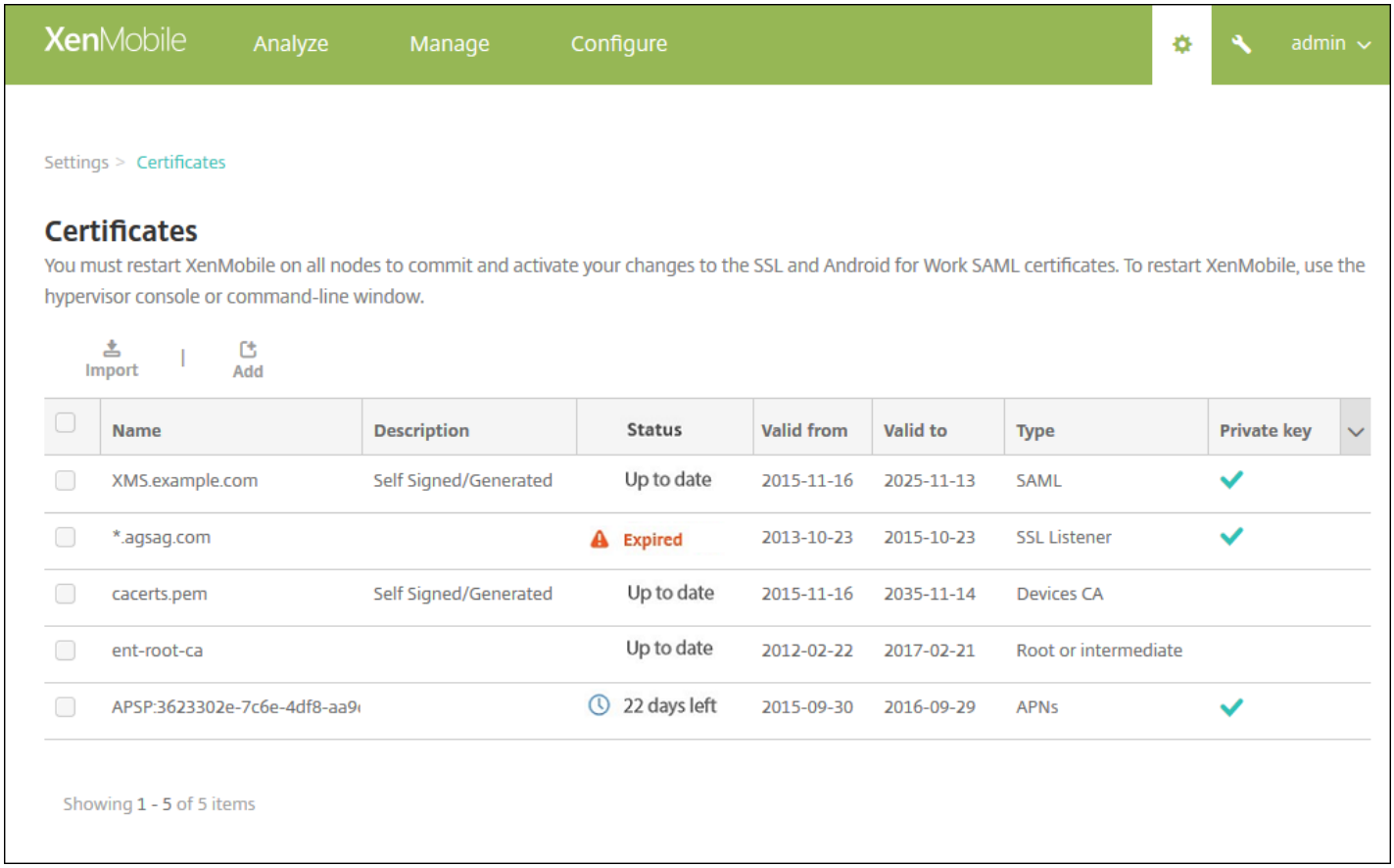
Para importar um keystore

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 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 **Configurações** é exibida.

2. Clique em **Certificados**. A página **Certificados** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

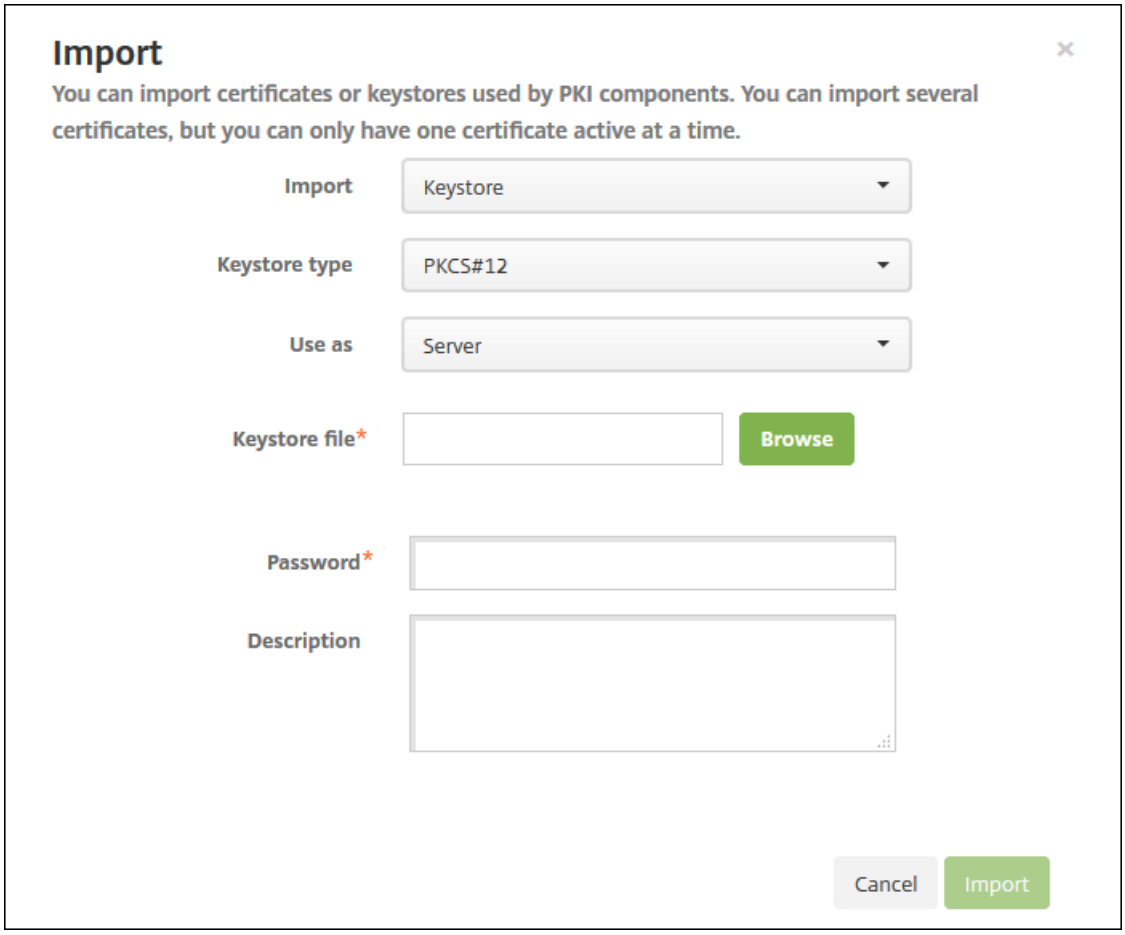


3. Clique em **Importar**. A caixa de diálogo **Importar** é exibida.

4. Defina estas configurações:

- **Importar**: na lista, clique em **Keystore**. A caixa de diálogo **Importar** é alterada para refletir as opções de keystore disponíveis.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- **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 uma entrada de keystore, o XenMobile tenta construir uma cadeia de certificados da entrada e importa todos os certificados dessa cadeia (criando uma entrada de certificado de servidor para cada uma). Essa operação só funcionará se os certificados na entrada do arquivo ou repositório de chaves formarem uma

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 para fins heurísticos. 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**, clique em como você usará 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.

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, você pode 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.

Administração de certificado do XenMobile

Recomendamos que você liste os certificados que usar na implantação do XenMobile, especialmente quanto às suas datas

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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:

XenMobile Server
Certificado SSL para FQDN de MDM
Certificado SAML (para ShareFile)
Certificados de AC Intermediária e Raiz para os certificados acima e quaisquer outros recursos internos (StoreFront/Proxy, e assim por diante)
Certificado de APN para o gerenciamento de dispositivos iOS
Certificados de APNs internos para notificações do Secure Hub do XenMobile Server
Certificado de usuário de PKI para conectividade com PKI

Toolkit MDX
Certificado de desenvolvedor da Apple
Perfil de provisionamento da Apple (por aplicativo)
Certificado Apple APNs (para uso com o Citrix Secure Mail)
Arquivo Keystore do Android
Windows Phone – Certificado Symantec

NetScaler
Certificado SSL para FQDN de MDM
Certificado SSL para FQDN de Gateway
Certificado SSL para FQDN do ShareFile SZC
Certificado SSL para balanceamento de carga do Exchange (configuração de descarregamento)
Certificado SSL para balanceamento de carga do StoreFront
Certificados de CA raiz e intermediários para os certificados anteriores

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

Como os certificados do serviço de Notificação por Push da Apple (APNs) expiram a cada ano, crie um certificado SSL do serviço de Notificação por Push da Apple e atualize-o no portal Citrix antes da expiração do certificado. 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

iOS. Para obter detalhes, consulte Certificados de APNs.

Você pode exibir o status do certificado de APNs e data de vencimento fazendo logon no Apple Push Certificates Portal. Você deve fazer logon como o mesmo usuário que criou o certificado.

Você também recebe uma notificação por email da Apple 30 e 10 dias antes da data de expiração com as seguintes informações:

O seguinte certificado de Serviço de Notificação por Push da Apple, criado para ID Apple de CustomerID expirará na Data. Se você revogar ou permitir que este certificado expire, os dispositivos existentes terão de ser registrados novamente com um novo certificado de push.

Entre em contato com o fornecedor para gerar uma nova solicitação (uma CSR assinada) e depois visite https://identity.apple.com/pushcert para renovar seu certificado de Serviço de Notificação por Push da Apple.

Obrigado,

Serviço de Notificação por Push da Apple

MDX Toolkit (certificado de distribuição do iOS)

Um aplicatrivo executado em um dispositivo iOS físico (além dos aplicativos na Apple App Store) deve ser assinado com um perfil de provisionamento. O aplicativo também deve ser assinado com um certificado correspondente de distribuição.

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.NomeDaEmpresa.NomeDoProduto.
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** e, em seguida, clique em **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 Symantec para Windows Phones

A Symantec 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 Certificados de autenticação de código Symantec para Windows Phone na documentação da Symantec.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

NetScaler

Para obter detalhes sobre como tratar de expiração do certificado do NetScaler, consulte Como lidar com de expiração de certificado no NetScaler, no Citrix Support Knowledge Center.

Um certificado NetScaler expirado impede que os usuários se registrem e acessem o armazenamento. 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 NetScaler. O Centro notificará você quando o certificado expirar. Essas ferramentas auxiliam na monitoração dos seguintes certificados do NetScaler:

- 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

NetScaler Gateway e XenMobile

Feb 21, 2018

Quando você configura o NetScaler 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 NetScaler Gateway.

Você configura o NetScaler Gateway para uso com o XenMobile Server exportando um script do XenMobile executado no NetScaler Gateway. Este artigo contém as seguintes seções:

Pré-requisitos para usar o script de configuração do NetScaler Gateway

Configurar a autenticação para o acesso de dispositivos remotos à rede interna

Adicionar uma instância do NetScaler Gateway

Configurar um NetScaler Gateway para uso com o XenMobile Server

Adicionar uma URL de retorno de chamada ao IP virtual da VPN do NetScaler Gateway

Pré-requisitos para usar o script de configuração do NetScaler Gateway

Requisitos do NetScaler:

- NetScaler (versão mínima 11.0, Compilação 70.12).
- O endereço IP do NetScaler deve estar configurado e ter conectividade com o servidor LDAP, a menos que o LDAP tenha balanceamento de carga.
- O endereço IP do NetScaler 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 NetScaler 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 NetScaler Gateway deve estar carregado e instalado no NetScaler. Para obter informações, consulte https://support.citrix.com/article/CTX136023.

Requisitos do XenMobile:

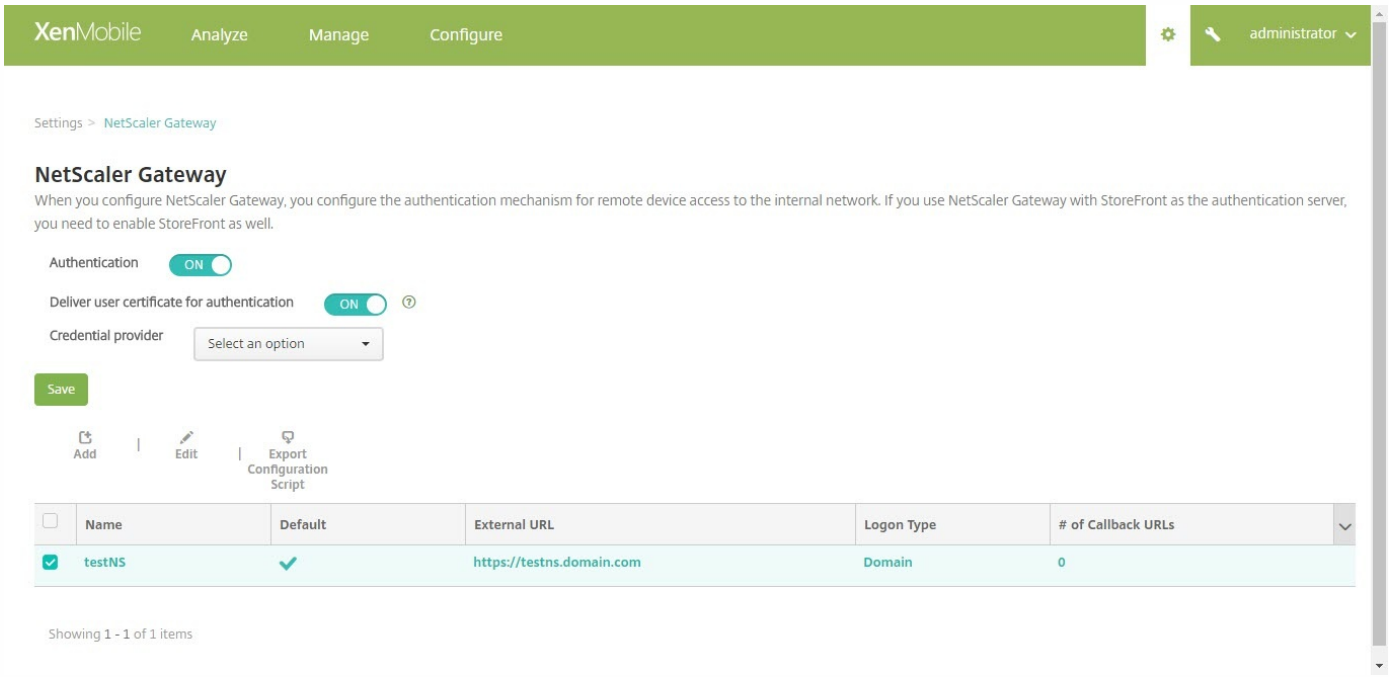
- XenMobile Server (versão mínima 10.6).
- O servidor LDAP deve estar configurado.

Configurar a autenticação para o acesso de dispositivos remotos à rede interna

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. No console da Web do XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.

2. Em **Servidor**, clique em **NetScaler Gateway**. A página **NetScaler Gateway** é exibida. No exemplo a seguir, existe uma instância do NetScaler 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 que o NetScaler Gateway manipule 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 NetScaler Gateway

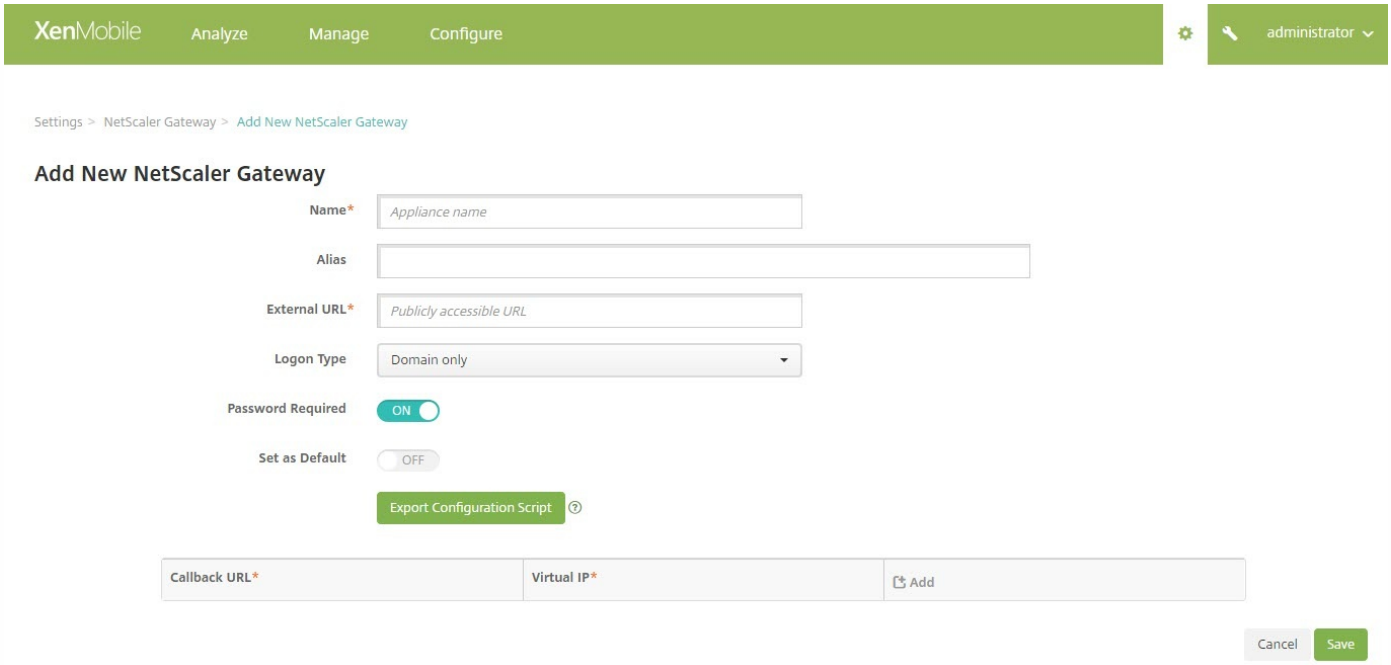
Depois de salvar as configurações de autenticação, adicione uma instância do NetScaler Gateway ao XenMobile.

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 **NetScaler Gateway**. A página **NetScaler Gateway** é exibida.

3. Clique em **Adicionar**. A página **Adicionar novo NetScaler Gateway** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. Defina estas configurações:

- **Nome**: digite um nome para a instância do NetScaler Gateway.
- **Alias**: inclua opcionalmente um nome de alias para o NetScaler Gateway.
- **URL externa**: digite a URL acessível publicamente do NetScaler Gateway. Por exemplo, https://receiver.com.
- **Tipo de logon**: escolha um tipo de logon. 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 logon** selecionado. O padrão é **Somente domínio**.

Se você tiver vários domínios, use **Certificado e domínio**.

Se você usar **Certificado e token de segurança**, não necessárias configurações adicionais no NetScaler Gateway para dar suporte ao Secure Hub. Para obter informações, consulte Configuring XenMobile for Certificate and Security Token Authentication.

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 NetScaler 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 NetScaler Gateway para defini-lo com as configurações do XenMobile. Para obter informações, consulte "Configurar um NetScaler 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 e um IP virtual de VPN do NetScaler Gateway", mais adiante neste artigo.

5. Clique em **Salvar**. O novo NetScaler Gateway é adicionado e exibido na tabela. Você pode editar ou excluir uma instância clicando no nome na lista.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurar um NetScaler Gateway para uso com o XenMobile Server

Para configurar um NetScaler Gateway local para uso com o XenMobile Server, realize as seguintes etapas gerais, detalhadas neste artigo:

1. Baixe um script e os arquivos relacionados do XenMobile Server. Consulte o arquivo leiame 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 NetScaler.
5. Teste a configuração.

O script configura essas configurações do NetScaler Gateway exigidas pelo XenMobile:

- Servidores NetScaler Gateway necessários para MDM e MAM
- Políticas de sessão para os servidores virtuais do NetScaler Gateway
- Detalhes do XenMobile Server
- Políticas de autenticação e ações para o servidor virtual NSG.
  O script descreve as definições de configuração de LDAP.
- Ações e políticas de tráfego para o servidor proxy
- Perfil de acesso sem cliente
- Registro de DNS local estático no NetScaler
- Outras associações: política de serviço, certificado de CA

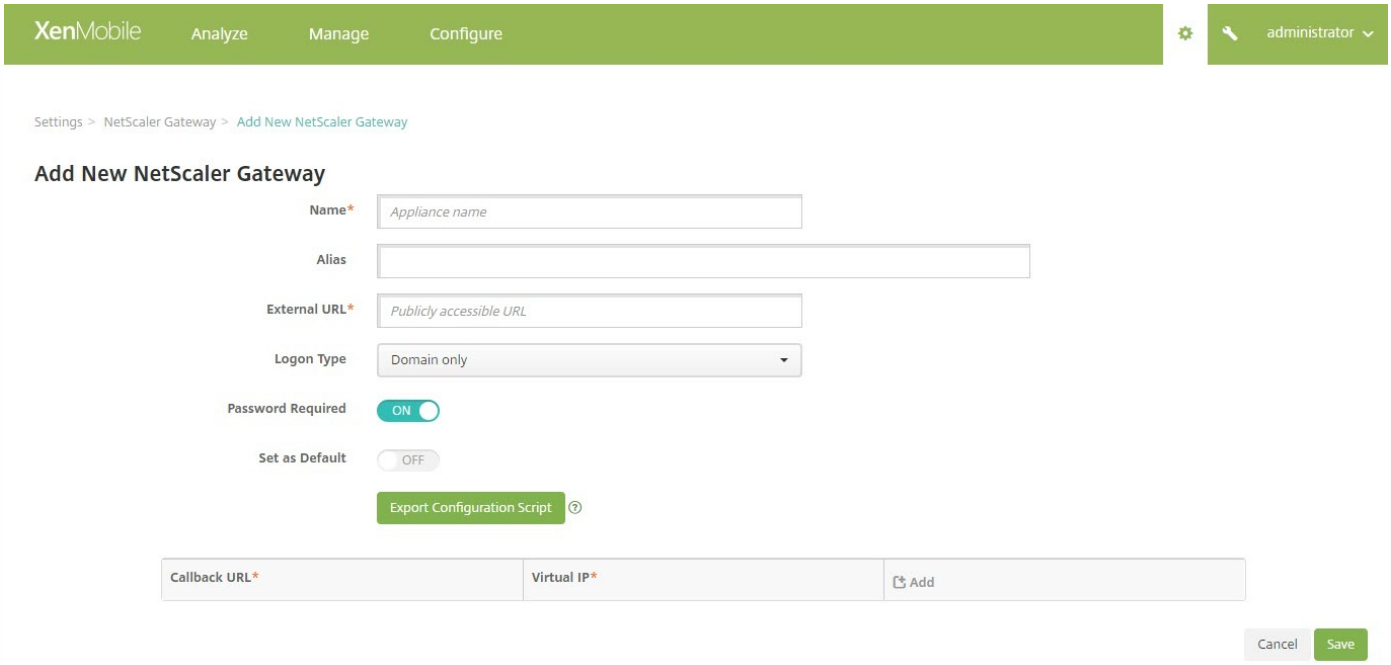
O script não manipula a seguinte configuração:

- Balanceamento de carga do Exchange
- Balanceamento de carga do ShareFile
- Configuração de proxy ICA
- Descarga de SSL

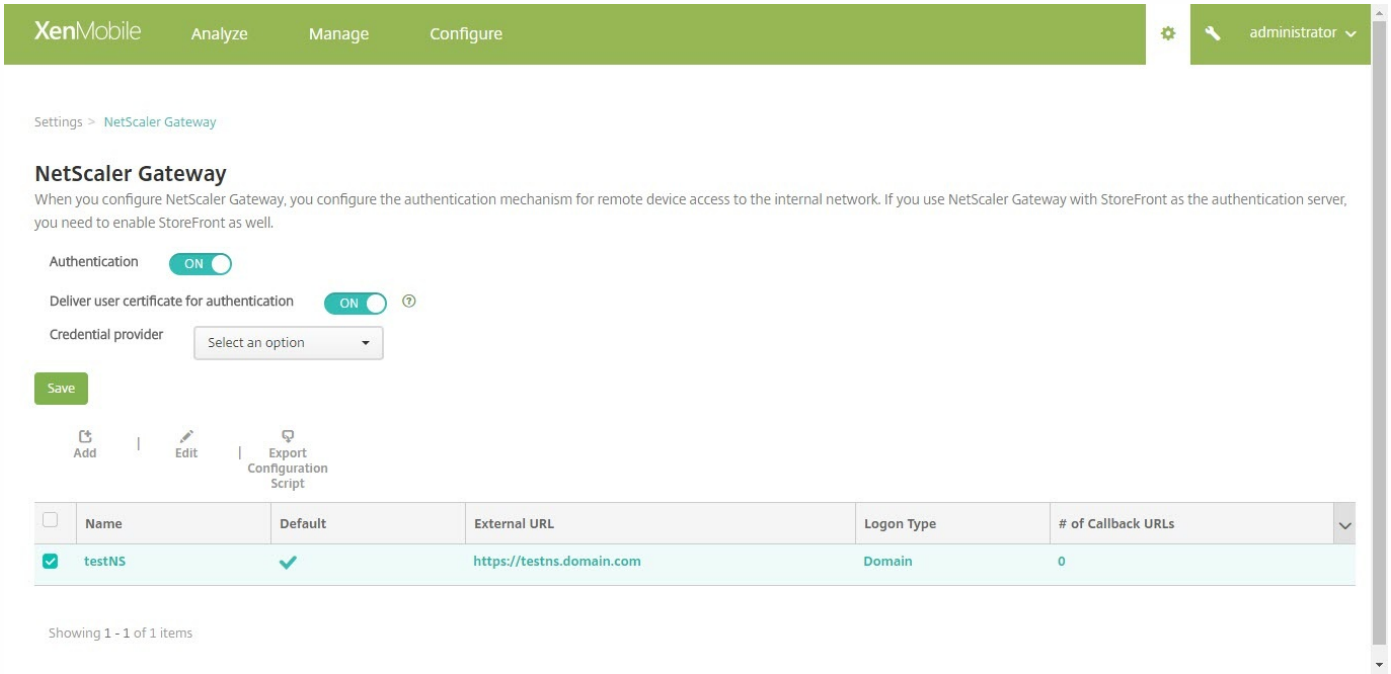
Para baixar, atualizar e executar o script:

1. Se estiver adicionando um NetScaler Gateway, clique em **Exportar script de configuração** na página **Adicionar novo NetScaler Gateway**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Ou, se você adicionar uma instância do NetScaler Gateway e clicar em **Salvar** antes de exportar o script, retorne à página **Configurações > NetScaler Gateway**, selecione o NetScaler, clique em **Exportar script de configuração** e, em seguida, clique em **Download**.



Depois de clicar em **Exportar script de configuração**, o XenMobile criará um pacote de script .tar.gz. O pacote de script inclui:

- Arquivo Leiame com instruções detalhadas
- Script que contém comandos da CLI do NetScaler usados para configurar os componentes necessários no NetScaler
- 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 NetScaler para remover a configuração do NetScaler

2. Edite o script (NSGConfigBundle_CREATESCRIPT.txt) para substituir todos os espaços reservados por detalhes do seu

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ambiente.

```
# <LDAP_SECURE_PORT> -- LDAP Server Secure Port.
# <NSG_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 o
f 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 o
f private IP addresses.
# <RADIUS_SERVER_IP> -- Radius Server IP Address.
# <LDAP_PASSWORD> -- LDAP Service Account Password.
# <NS_SERVER_CERT_TAG> -- NetScaler Server Certificate Tag.
# <NSG_VIP> -- Virtual IP Address to be assigned to the NetScaler Gateway virtual server. This IP address must be reacha
ble from your devices either directly or via a NAT.
```

3. Execute o script editado no bash shell NetScaler, conforme descrito no arquivo leiame incluído no pacote de script. Por exemplo:

   /netscaler/nscli -U :: 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"
```

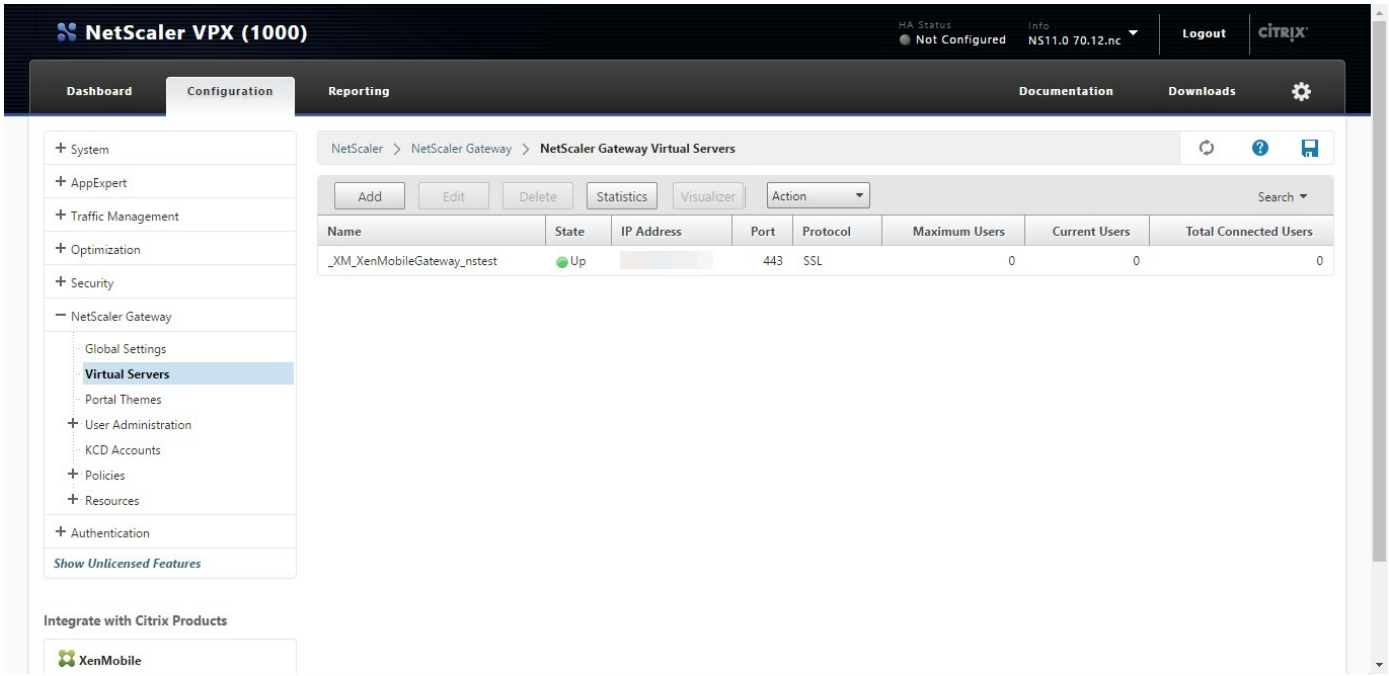
   Quando o script for concluído, as seguintes linhas aparecerão.

```
exec: save ns config
 Done
 Done
root@ns#
```

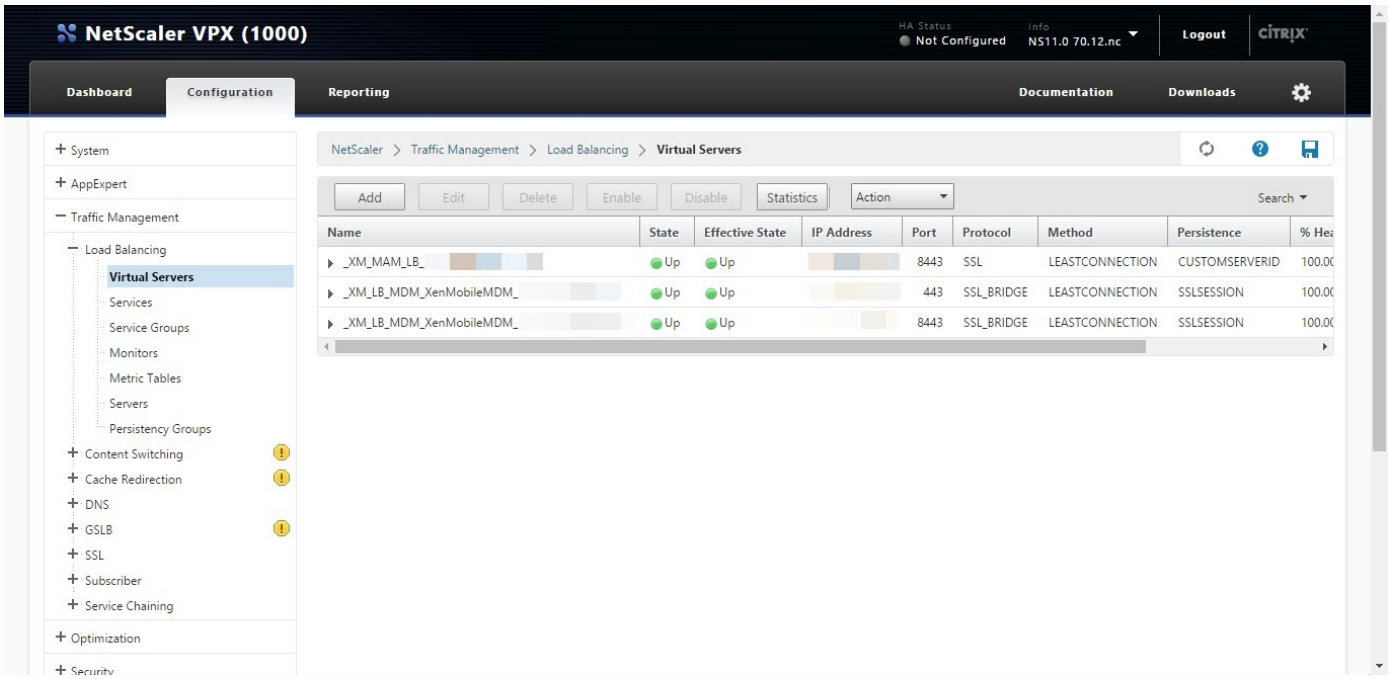
Testar a configuração

1. Valide se o servidor virtual do NetScaler Gateway mostra um estado de **UP**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Valide se o servidor virtual de balanceamento de carga proxy mostra um estado de **UP**.



3. Abra um navegador da Web, conecte-se à URL do NetScaler 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 NetScaler Gateway

Depois de adicionar a instância do NetScaler Gateway, você poderá adicionar uma URL de retorno de chamada e especificar

© 1999-2017 Citrix Systems, Inc. All rights reserved.

um endereço IP virtual do NetScaler Gateway. **Nota**: essas configurações são opcionais, mas podem ser definidas para obter segurança extra, especialmente quando o XenMobile Server está na DMZ.

1. Em **Configurações > NetScaler Gateway**, selecione o NetScaler 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 NetScaler Gateway. Certifique-se de que a URL de retono de chamada seja resolvida para um endereço IP acessível no XenMobile Server. A URL de retorno de chamada pode ser uma URL externa do NetScaler Gateway ou alguma outra URL.
4. Digite o endereço **IP virtual** do NetScaler Gateway e clique em **Salvar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configure autenticação de domínio ou de domínio de segurança

Feb 21, 2018

O XenMobile dá suporte a autenticação baseada em domínio com relação a um ou mais diretórios, como o Active Directory, que estão em conformidade com o protocolo LDAP. Você pode configurar uma conexãono 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 o logon único (SSO) aos usuários, no qual uma única senha (por usuário) é compartilhada entre vários serviços, permitindo que um usuário faça login uma vez no site da Web de uma empresa e, em seguida, seja automaticamente autenticado na intranet empresarial.

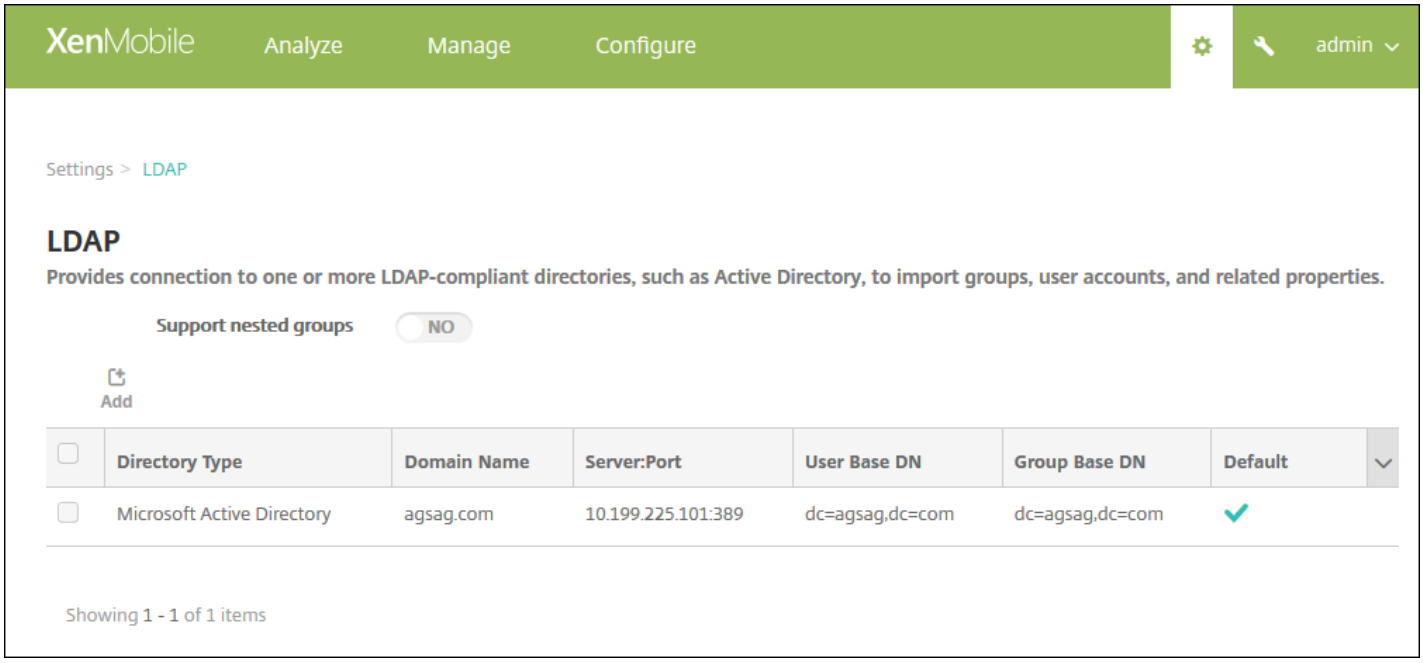
Um cliente inicia uma sessão do LDAP conectando-se a um servidor LDAP, chamado de Directory System Agent (DSA). O cliente envia uma solicitação de operação para o servidor, e o servidor responde com a autenticação adequada.

> ## Important
>
> 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 registraram 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 **Configurações** é exibida.
2. Em **Servidor**, clique em **LDAP**. A página **LDAP** é exibida. Você pode adicionar, editar ou excluir diretórios compatíveis com LDAP nessa página.

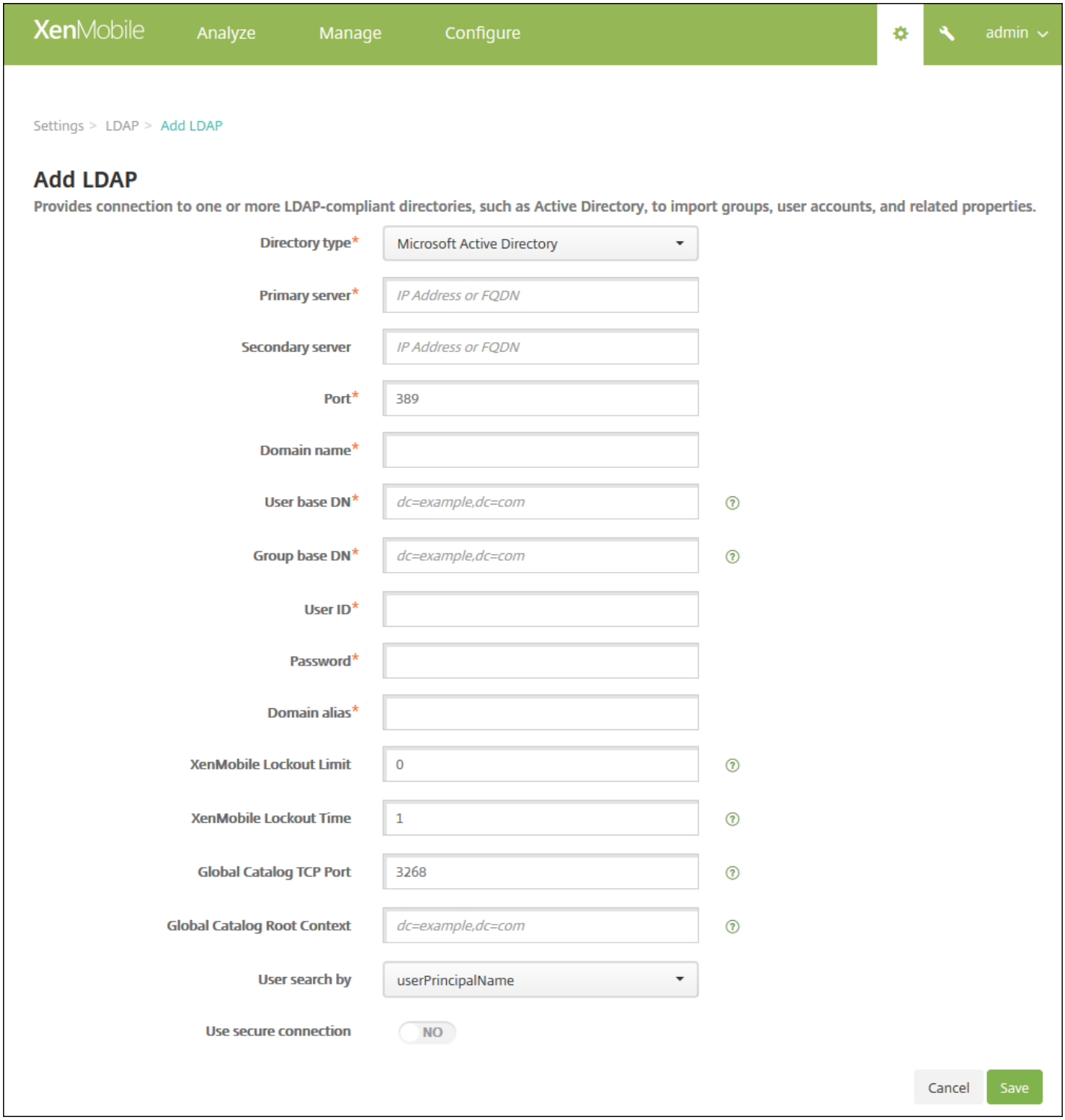
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Para adicionar um diretório compatível com LDAP

1. Na página **LDAP**, clique em **Adicionar**. A página **Adicionar LDAP** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 de 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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. Os exemplos de sintaxe incluem: ou=users, dc=example, or dc=com.
- **DN base de grupo** : digite a localização dos grupos do Active Directory. Por exemplo, cn = users, dc = domain, dc = NET, no qual cn = usuários representa o nome do contêiner dos grupos e dc representa o componente de domínio do Active Directory.
- **ID de 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.
- **Limite de bloqueio do XenMobile**: digite um número entre 0 e 999 para ser o número de tentativas de login com falha. Definir esse campo como 0 significa que o XenMobile nunca bloqueará o usuário com base nas 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. Definir esse campo como 0 significa que o usuário não será forçado a esperar depois de 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**.
- **Usar conexão segura**: Selecione se devem ou não ser usadas conexões seguras. O padrão é **NÃO**.

3. Clique em **Salvar**.

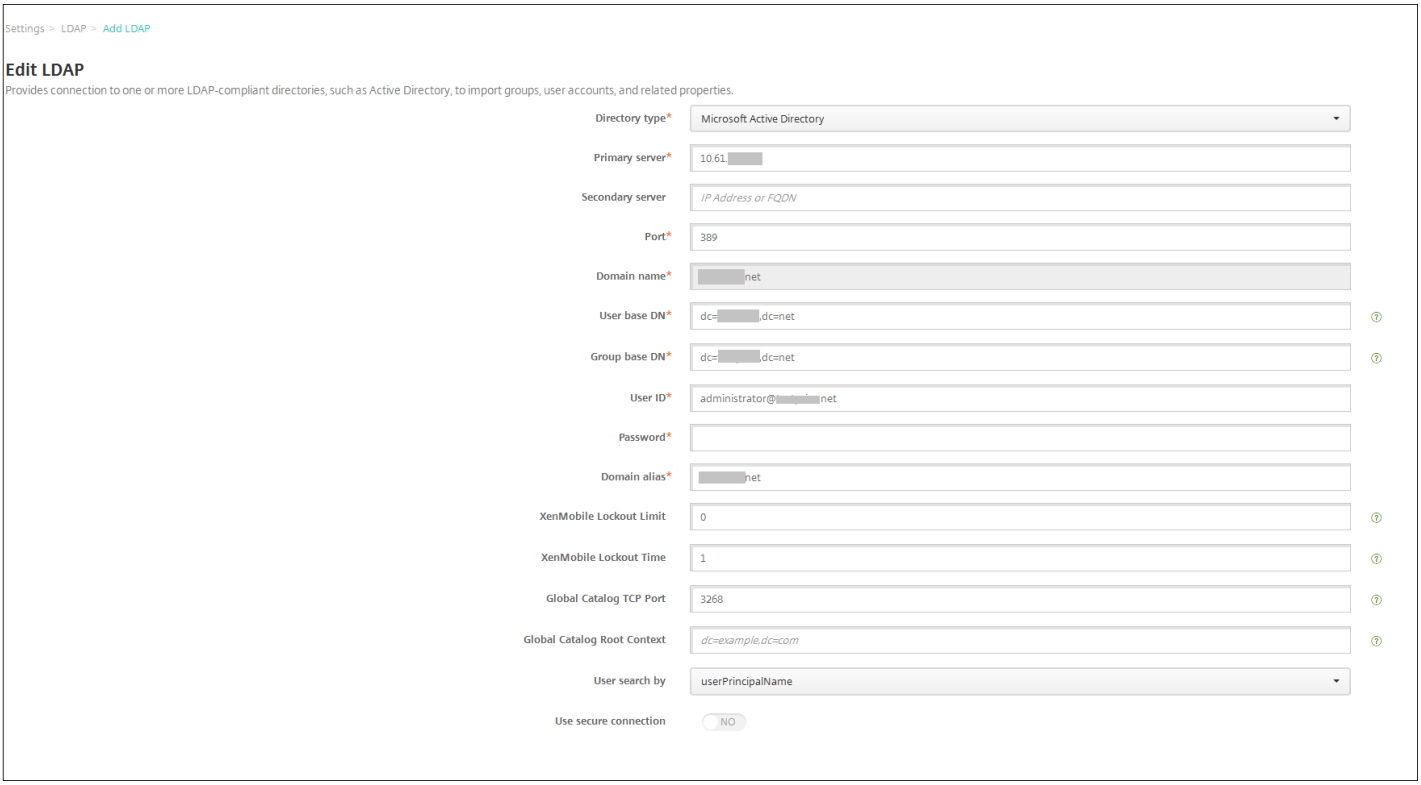
Para editar um diretório compatível com LDAP

1. Na tabela **LDAP**, selecione o diretório que você desejar editar.

   Nota: quando você marca a caixa de seleção ao lado de um diretório, o menu de opções é exibido acima da lista LDAP; quando você clica em qualquer outro lugar na lista, o menu de opções é exibido à direita da listagem.

2. Clique em **Editar**. A página **Editar LDAP** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 de 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. Os exemplos de sintaxe incluem: ou=users, dc=example, or 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, no qual cn=users é o nome do grupo; DN e servername representam o nome do servidor que executa o Active Directory.
- **ID de 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.
- **Limite de bloqueio do XenMobile**: digite um número entre 0 e 999 para ser o número de tentativas de login com falha. Definir esse campo como 0 significa que o XenMobile nunca bloqueará o usuário com base nas 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. Definir esse campo como 0 significa que o usuário não será forçado a esperar depois de 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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**.
- **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 desejar excluir.

> **Nota**: 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.

Configure 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.

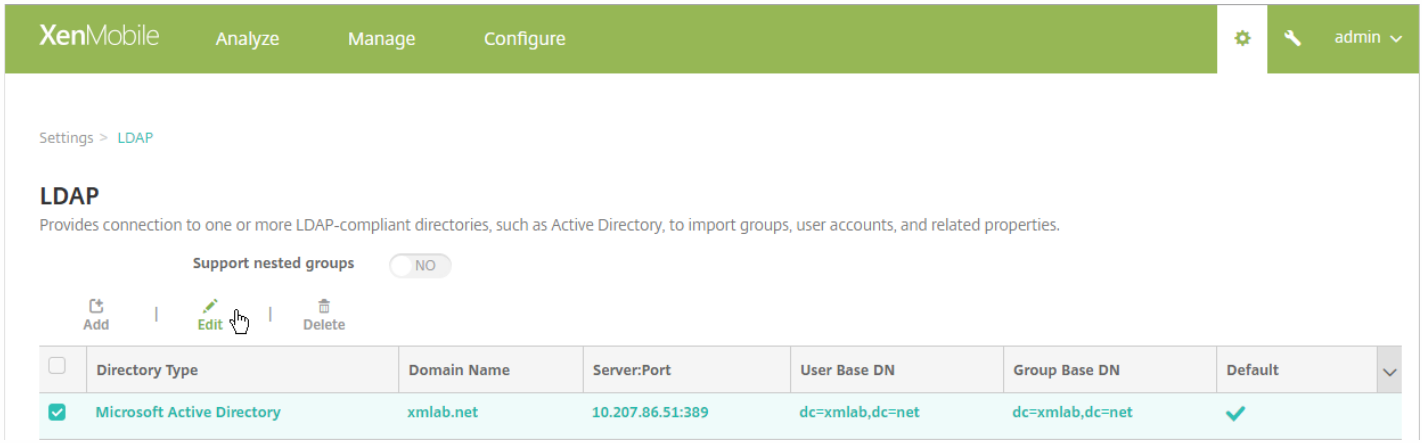
Para melhor usabilidade, você pode combinar essa configuração com o PIN da Citrix e armazenamento em cache de senha do Active Directory de forma que os usuários não tenham que digitar repetidamente seus nomes de usuário e senhas do Active Directory. Os usuários precisarão inserir seus nomes de usuário 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 Upload de certificados no XenMobile.

1. Em **Configurações**, clique em **LDAP**.

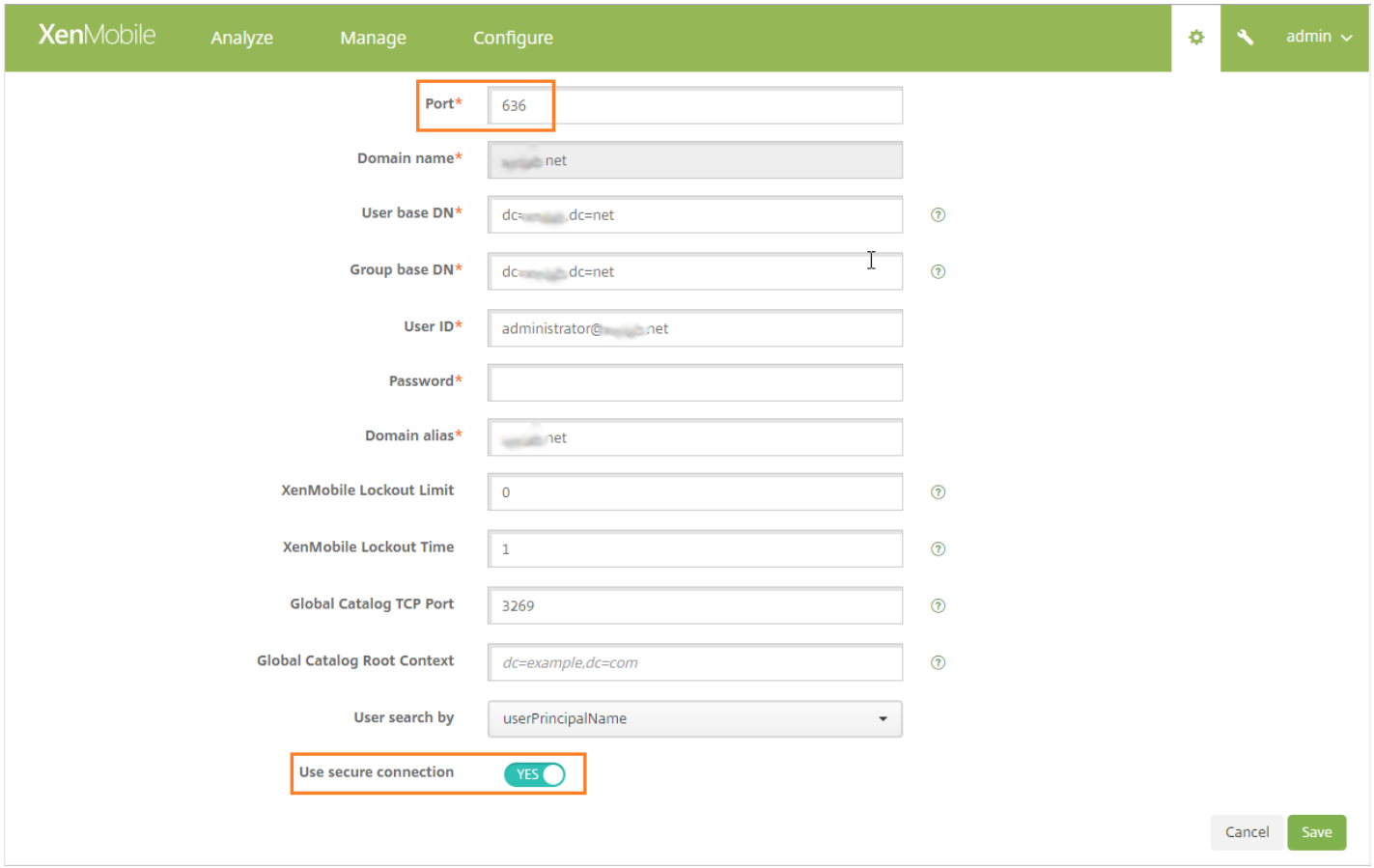
2. Selecione **Microsoft Active Directory** e, em seguida, clique em **Editar**.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

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**.



Definir as configurações do NetScaler Gateway

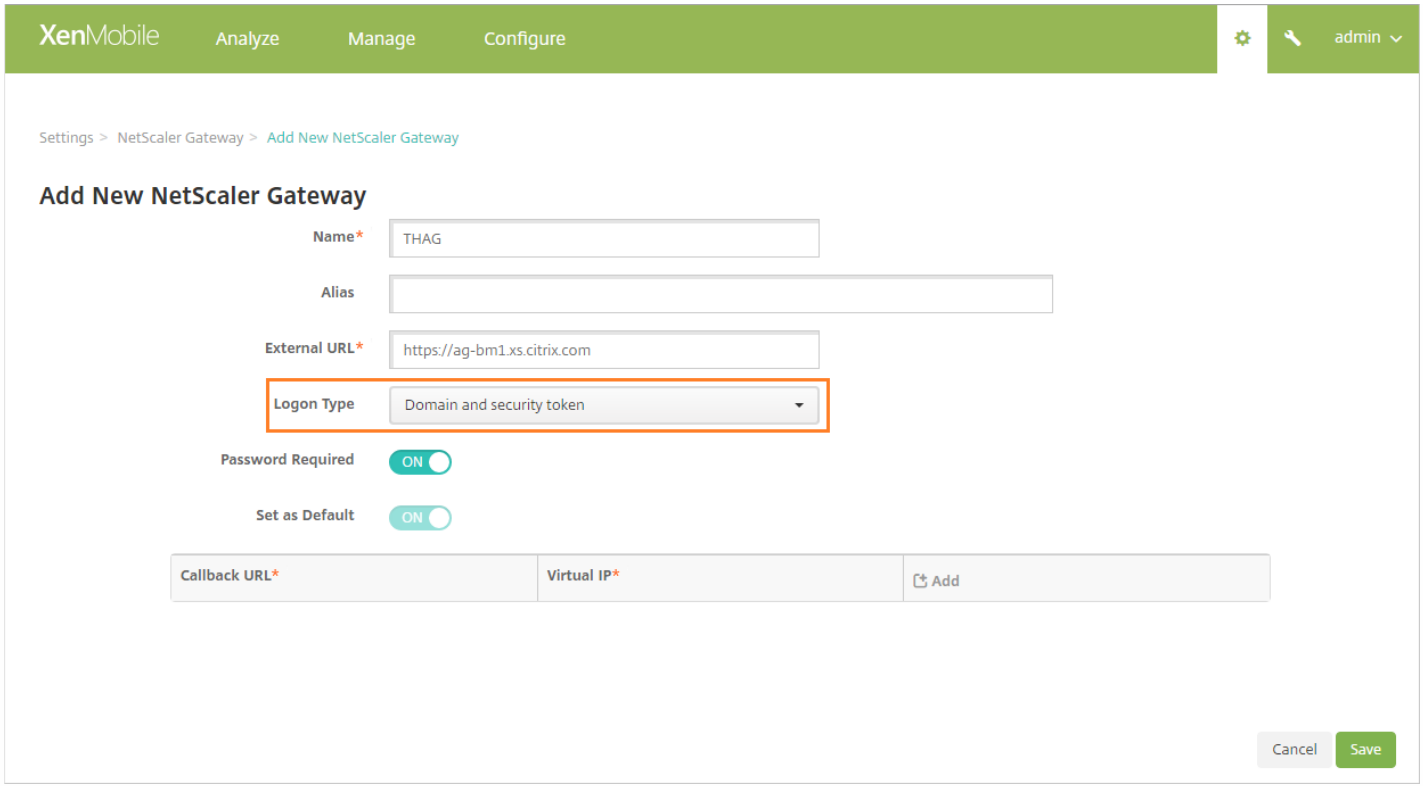
As seguintes etapas pressupõem que você já tenha adicionado uma instância do NetScaler Gateway ao XenMobile. Para adicionar uma instância do NetScaler Gateway, consulte Para configurar uma nova instância do NetScaler Gateway.

1. Em **Configurações**, clique em **NetScaler Gateway**.

2. Selecione o **NetScaler Gateway** e clique em **Editar**.

3. Em **Tipo de logon**, selecione **Domínio e token de segurança**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Ativar o PIN da Citrix e o cache de senha de usuário

Para ativar o PIN da Citrix e o cache de senha de usuário, vá para **Configurações > Propriedades do cliente** e marque as caixas de seleção: **Ativar autenticação com PIN da Citrix** e **Ativar armazenamento em cache da senha do usuário**. Para obter mais informações, consulte Propriedades do cliente.

Configurar o NetScaler Gateway para autenticação de domínio e de token de segurança

Configure perfis de sessão do NetScaler Gateway e as políticas de seus servidores virtuais usados com o XenMobile. Para obter informações, consulte Configuração de domínio e autenticação de token de segurança para o XenMobile na documentação do NetScaler Gateway.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Autenticação de certificado cliente ou certificado e domínio

Feb 21, 2018

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 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 fornecidas pela autenticação de dois fatores no NetScaler.

Para melhor usabilidade, você pode combinar essa configuração com o PIN da Citrix e armazenamento em cache de senha do Active Directory de forma que os usuários não tenham que digitar repetidamente seus nomes de usuário e senhas do Active Directory. Os usuários precisarão inserir seus nomes de usuário e senhas para registro, expiração de senha e bloqueio de conta.

> ## Important
>
> 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 registraram 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 subsequentemente implanta o certificado usado para autenticar no ambiente XenMobile.

Você pode usar o assistente NetScaler para o XenMobile para executar a configuração necessária para o XenMobile ao usar autenticação de NetScaler de certificate apenas ou autenticação de certificado mais domínio. Você pode executar o NetScaler para o assistente do XenMobile apenas uma vez.

Em ambientes altamente seguros em que o uso de credenciais LDAP fora de uma organização em redes públicas ou sem segurança é considerada uma ameaça importante à segurança da organização, a autenticação de dois fatores que usa um certificado cliente e um token de segurança é uma opção. 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 servidor XenMobile e o NetScaler 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

No servidor XenMobile:

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 NetScaler Gateway para fornecer um certificado de usuário para autenticação.

No NetScaler Gateway, configure como descrito em Configuring Client Certificate or Client Certificate and Domain Authentication na documentação do NetScaler Gateway.

Pré-requisitos

- Quando você cria um modelo de Entidade de Serviços de Certificado Microsoft, para evitar possíveis problemas de autenticação com dispositivos registrados, evite usar caracteres especiais, tais como :, !, $, (), #, %, +, *, ~, ?, |, { } e [] no nome do modelo.
- Para dispositivos Windows Phone 8.1 que usam autenticação de certificado de cliente e a descarga de SSL, é preciso desabilitar a reutilização de sessão SSL para a porta 443 nos servidores virtuais de balanceamento de carga e no NetScaler. Para fazer isso, execute o seguinte comando nos vservers para a porta 443:

  set ssl vserver sessReuse DISABLE

  Nota: a desativação da reutilização da sessão SSL desativa algumas das otimizações que o NetScaler oferece, o que pode resultar em uma redução no desempenho no NetScaler.

- Para configurar a autenticação baseada em certificado para o Exchange ActiveSync, consulte este blog da Microsoft.
- Se você estiver usando 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. 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**.
- Verifique se o Secure Mail está preparado com o MDX Toolkit mais recente, se necessário para o método de implantação.

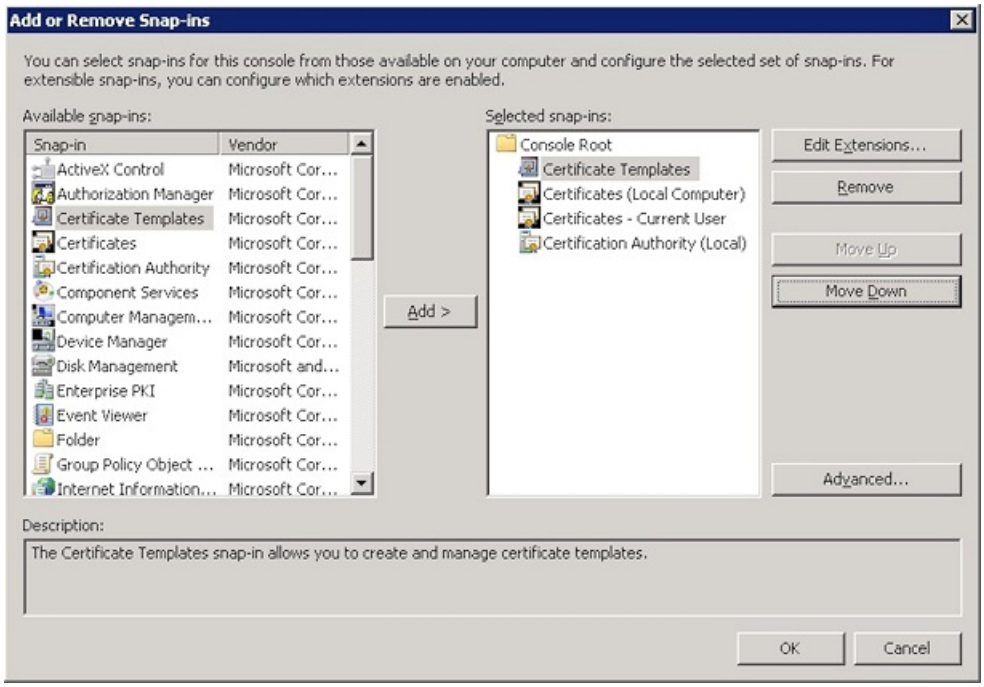
Adicionar um snap-in de certificado ao Console de Gerenciamento Microsoft

1. Abra o console e, em seguida, clique em **Adicionar ou remover snap-ins**.

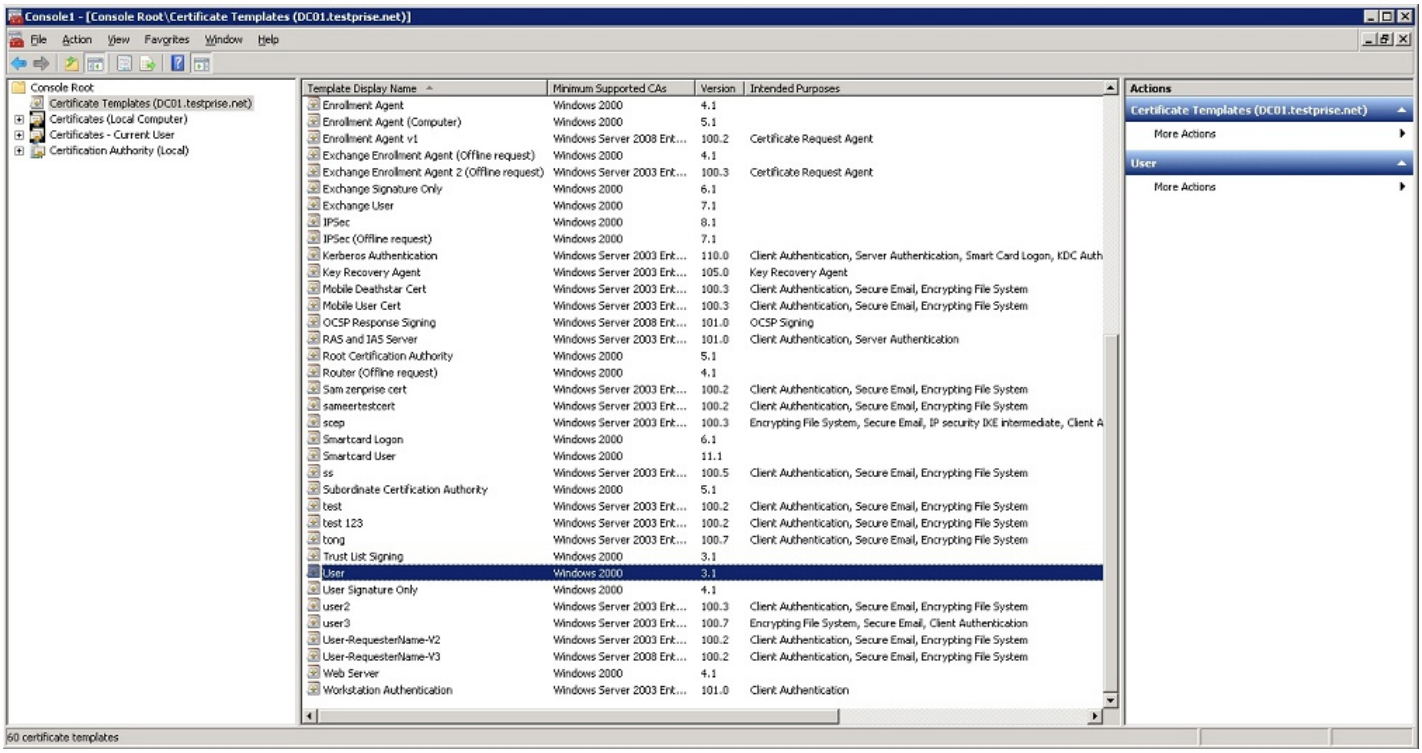
2. Adicione os seguintes snap-ins:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Modelos de certificado
Certificados (computador local)
Certificados - usuário atual
Autoridade de certificação (local)

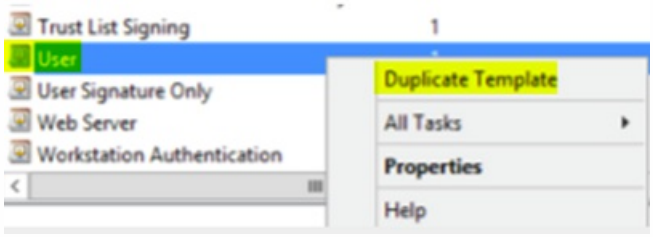


3. Expanda **Modelos de certificado**.



4. Selecione o modelo **Usuário** e **Modelo duplicado**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

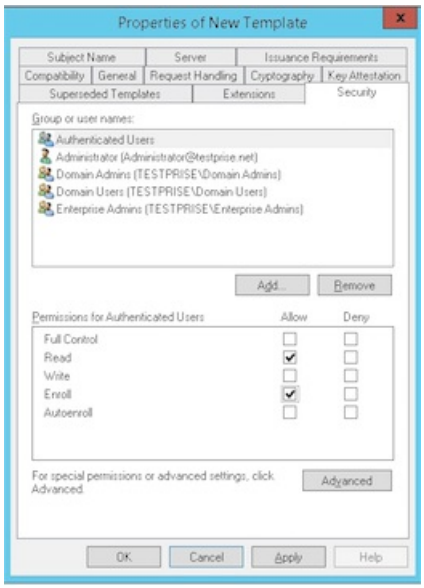


5. Forneça o nome para exibição do Modelo.

> **Importante**: não marque a caixa de seleção **Publicar o certificado no Active Directory** a menos que seja necessário. Se essa opção estiver marcada, todos os certificados cliente do usuário serão enviados/criados no Active Directory, o que pode atravancar o banco de dados do Active Directory.

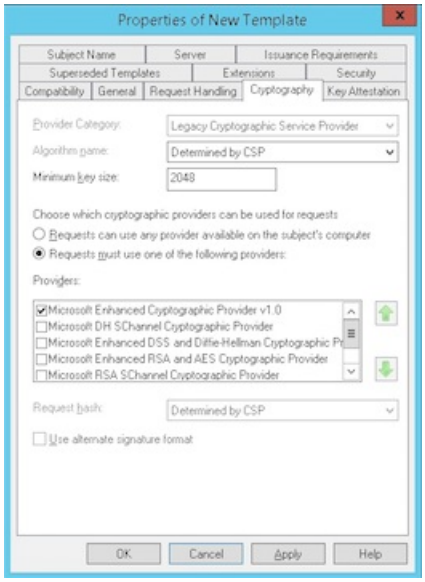
6. Selecione **Windows 2003 Server** como o tipo de modelo. No servidor Windows 2012 R2, em **Compatibilidade**, selecione **Autoridade de certificação** e defina o destinatário como **Windows 2003**.

7. Em **Segurança**, selecione a opção **Registrar** na coluna **Permitir** dos usuários autenticados.

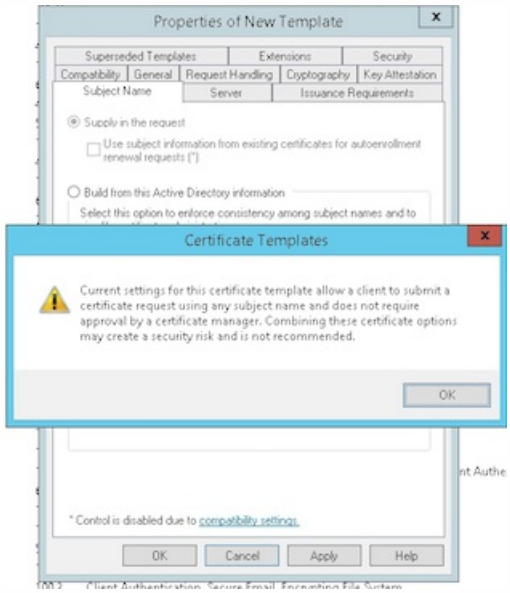


8. Em **Criptografia**, verifique se você forneceu o tamanho de chave que precisará inserir durante a configuração do XenMobile.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. Em **Nome da entidade**, selecione **Fornecer na solicitação**. Aplique as alterações e, em seguida, salve.

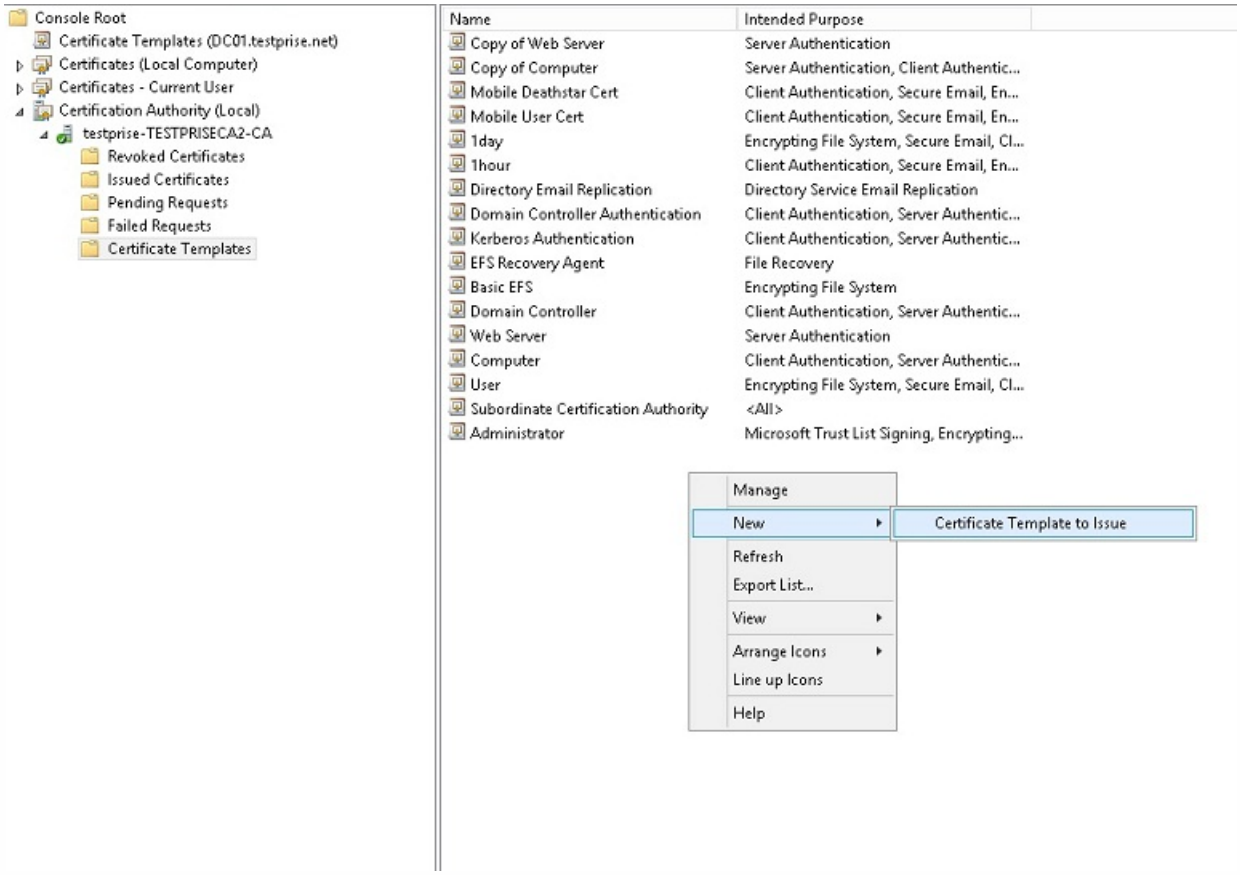


Adição de um modelo à Autoridade de Certificação

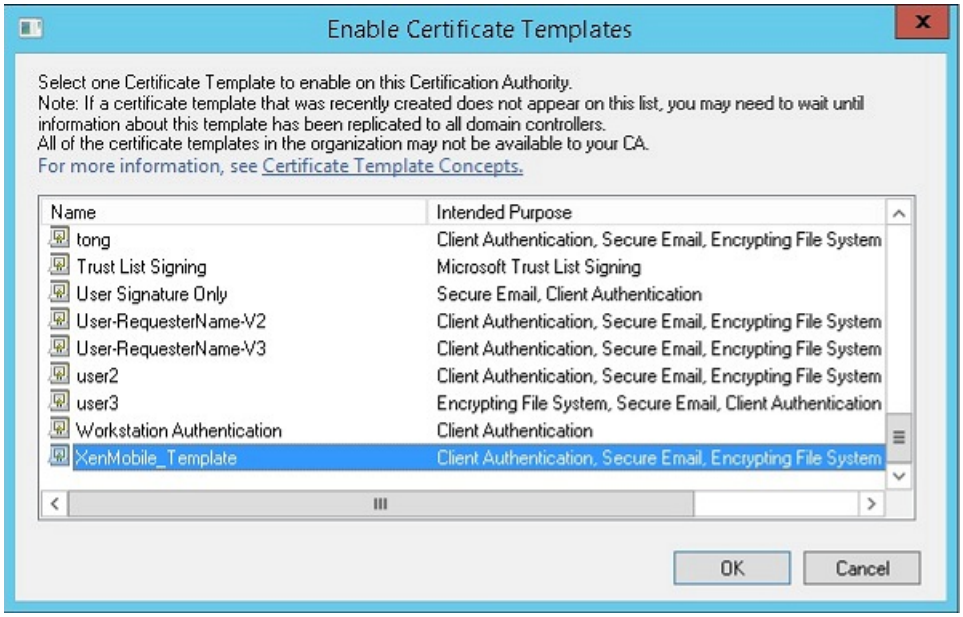
1. Vá para **Autoridade de certificação** e selecione **Modelos de certificado**.

2. Clique com o botão direito do mouse no painel direito e selecione **Novo > Modelo de certificado a ser emitido**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. Selecione o modelo que você criou na etapa anterior e clique em **OK** para adicioná-lo à **Autoridade de certificação**.



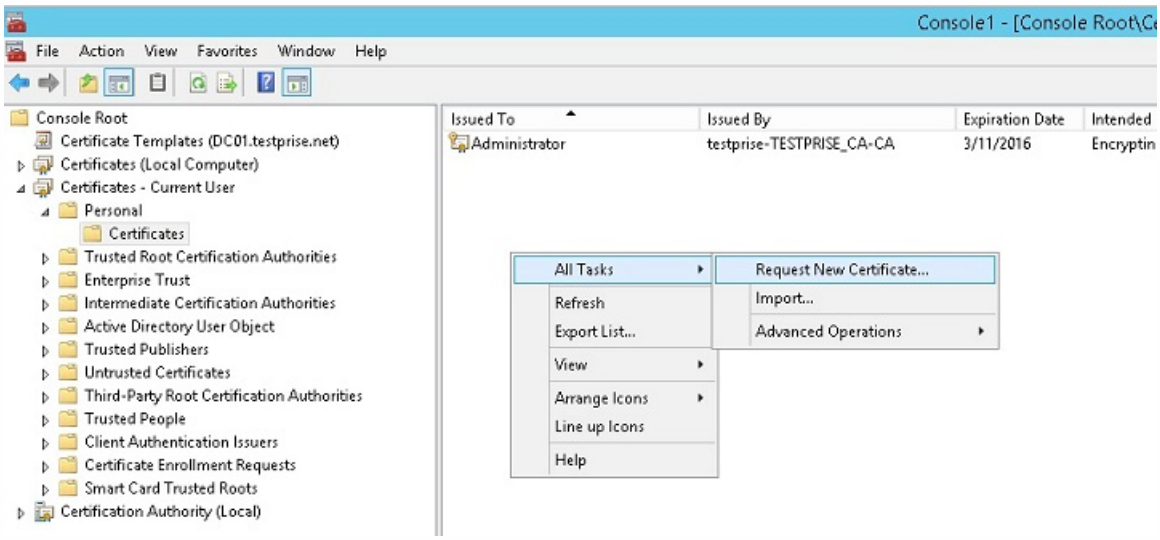
Criação de um certificado PFX do servidor de AC

1. Crie um certificado .pfx de usuário usando a conta de serviço com a qual você fez login. Esse .pfx será carregado no XenMobile, que solicitará um certificado de usuário em nome dos usuários que registrarem os respectivos dispositivos.

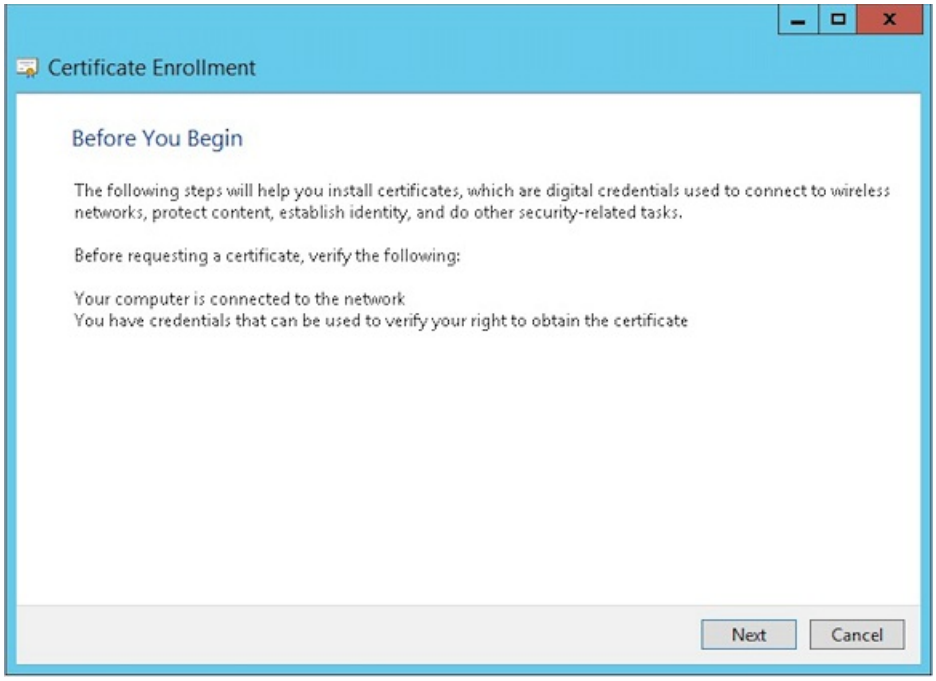
2. Em **Usuário atual**, expanda **Certificados**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Clique com o botão direito do mouse no painel direito e clique em **Solicitar novo certificado**.

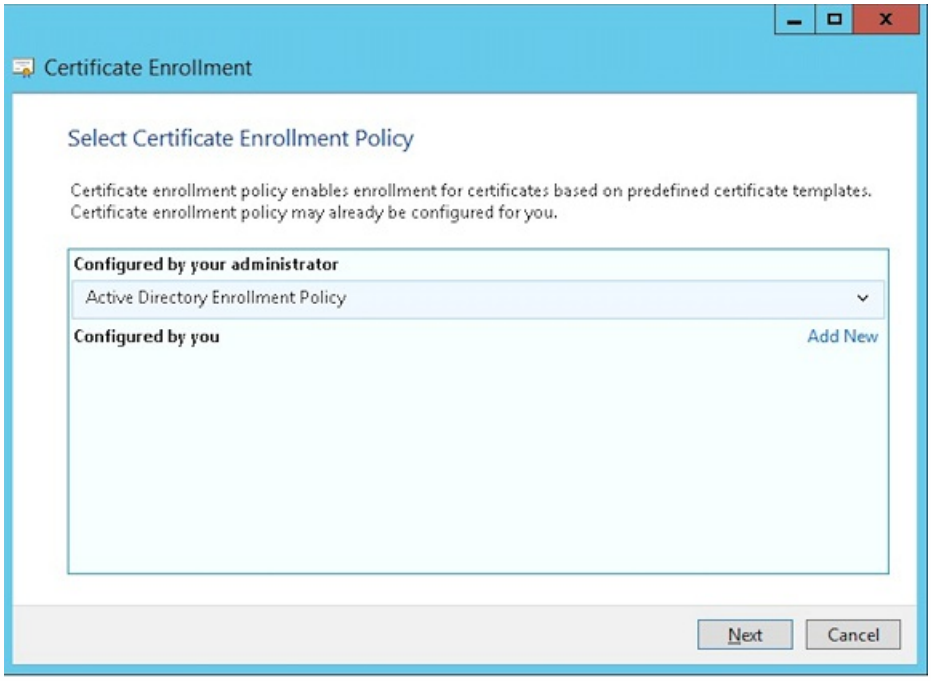


4. A tela **Registro de certificado** é exibida. Clique em **Avançar**.

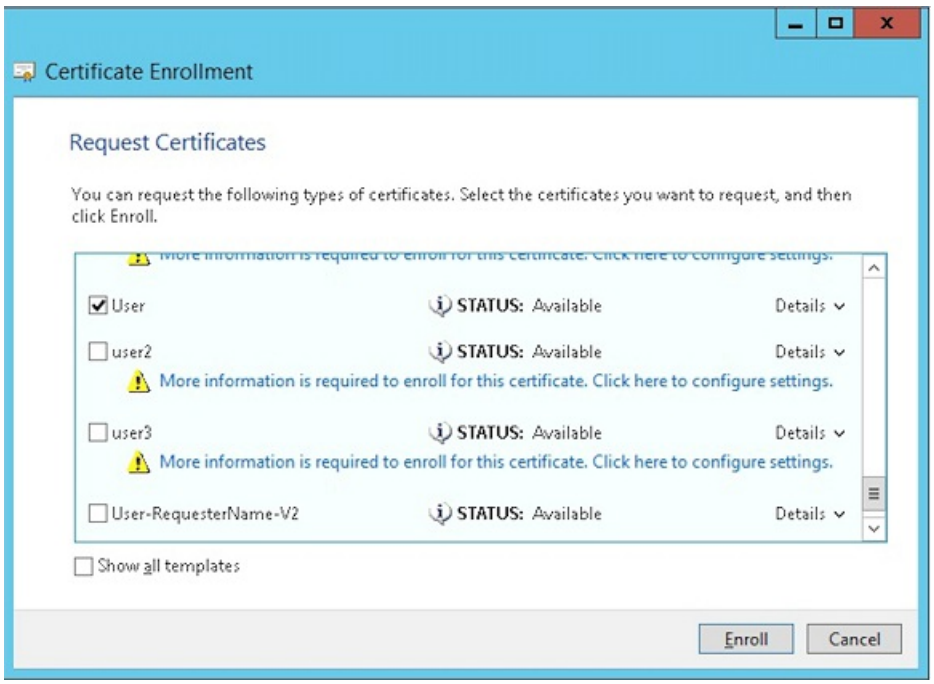


5. Selecione **Política de registro do Active Directory** e clique em **Avançar**.

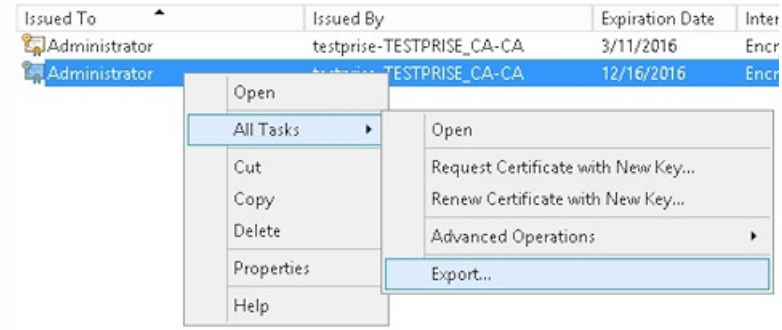
© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. Selecione o modelo **Usuário** e clique em **Registrar**.

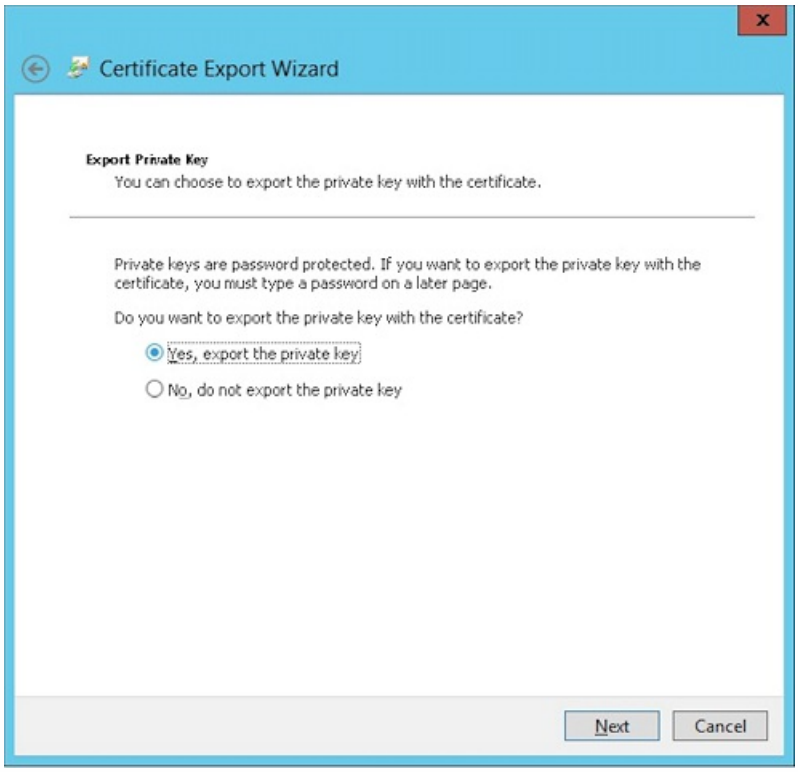


7. Exporte o arquivo .pfx criado na etapa anterior.

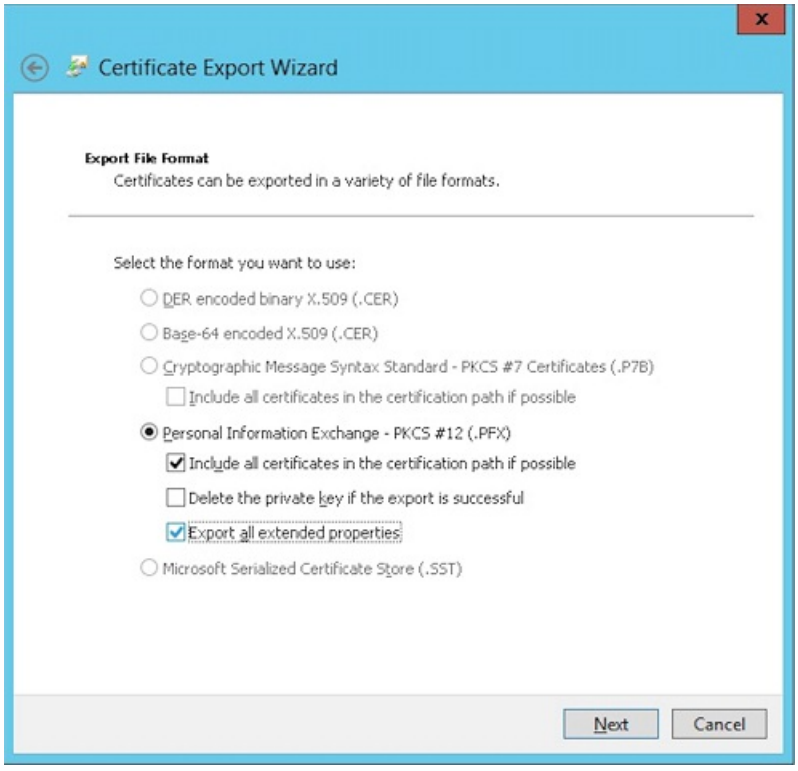


8. Clique em **Sim, exportar a chave privada**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

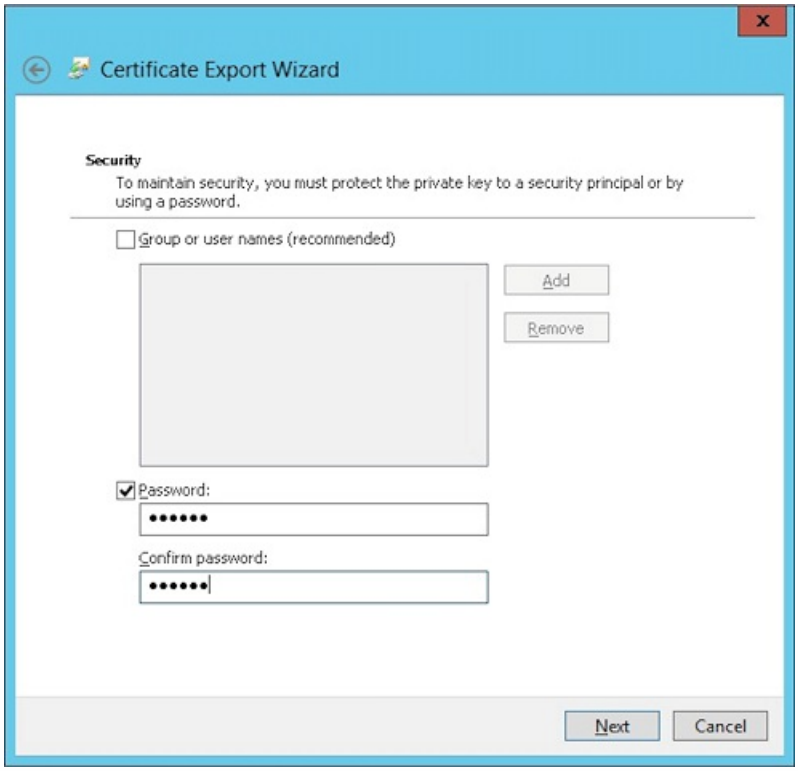


9. Selecione **Incluir todos os certificados no caminho de certificação, se possível** e marque a caixa de seleção **Exportar todas as propriedades estendidas**.



10. Defina uma senha que você usará quando carregar o certificado para o XenMobile.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



11. Salve o certificado no seu disco rígido.

Upload do certificado no XenMobile

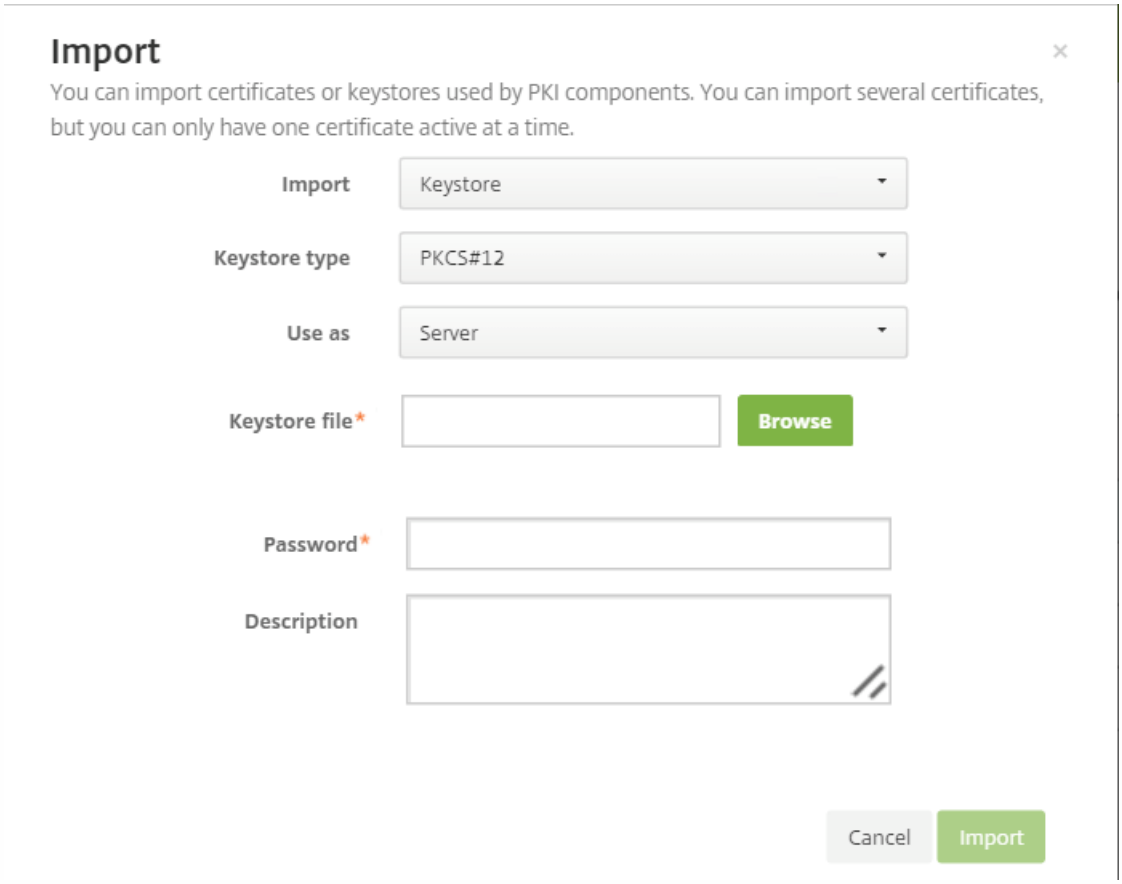
1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A tela **Configurações** é exibida.

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 acabou de criar.
- **Senha**: insira a senha criada para esse certificado.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. Clique em **Importar**.

5. Verifique se o certificado foi instalado corretamente. Ele deve ser exibido como um certificado de Usuário.

Criação da entidade PKI de autenticação baseada em certificado

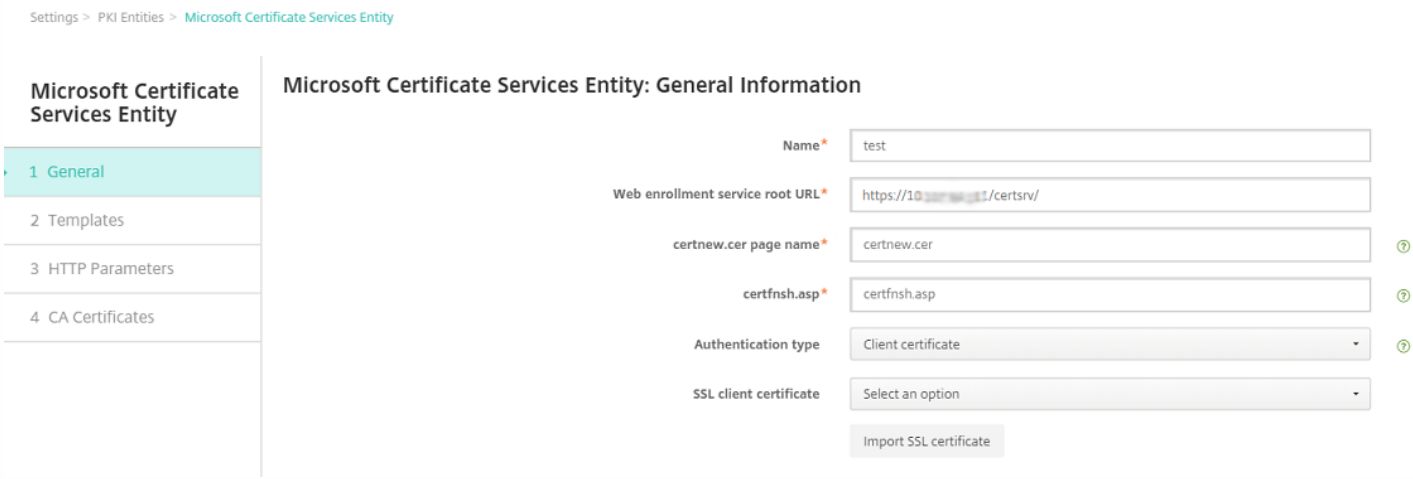
1. Em **Configurações**, vá para **Mais > Gerenciamento de certificados > Entidades PKI**.

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.

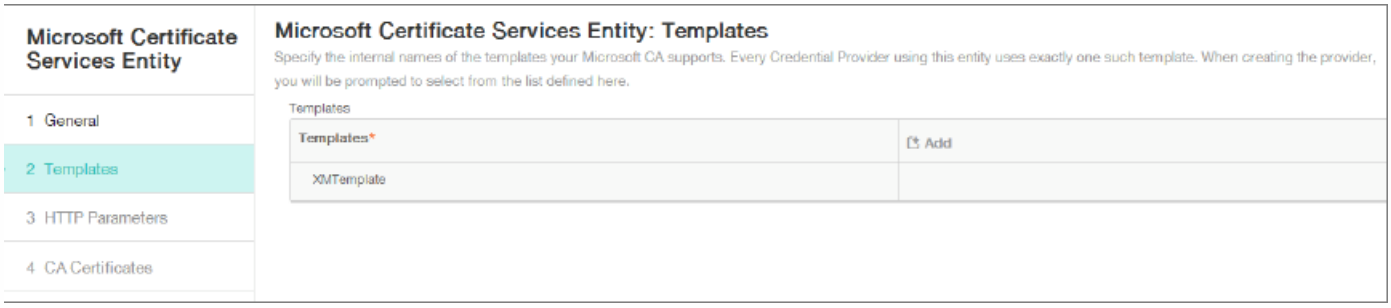
3. Insira os seguintes parâmetros:

- **Nome**: digite qualquer nome
- **URL raiz do serviço de registro na Web**: https://RootCA-URL/certsrv/
  Lembre-se de adicionar a última barra (/) no caminho 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

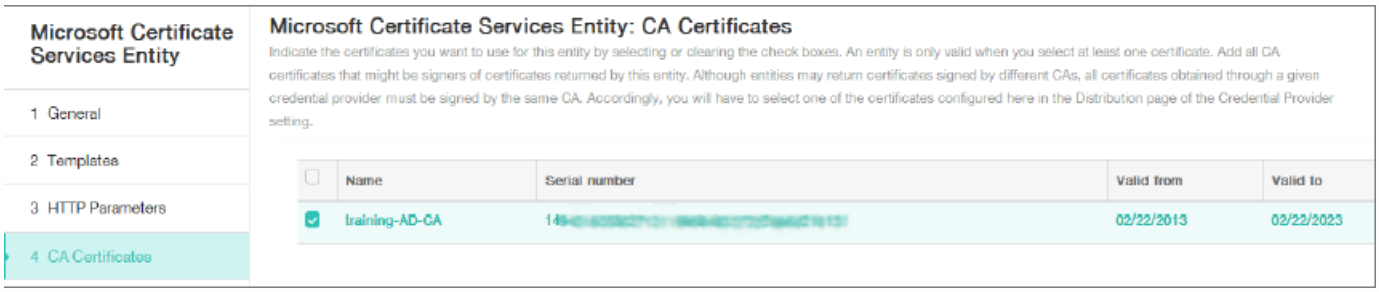


4. Em **Modelos**, adicione o modelo que você criou ao configurar o certificado da Microsoft. Tenha o cuidado de não adicionar espaços.



5. Ignore os Parâmetros HTTP e, em seguida, clique em **Certificados AC**.

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.



7. Clique em **Salvar**.

Configuração dos provedores de credenciais

1. Em **Configurações**, vá para **Mais > Gerenciamento de certificados > Provedores de credenciais**.

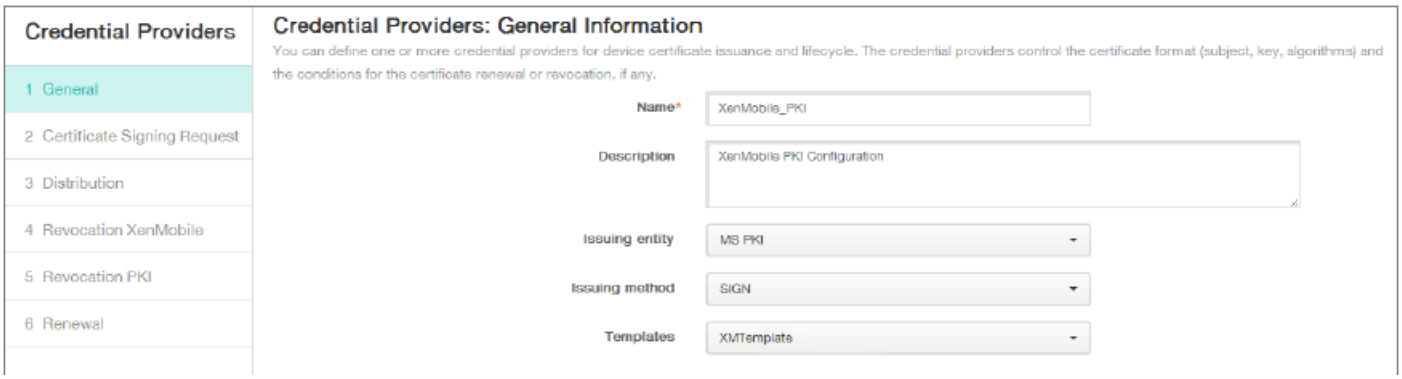
2. Clique em Adicionar.

3. Em **Geral**, insira os seguintes parâmetros:

- **Nome**: digite qualquer nome.
- **Descrição**: digite qualquer descrição.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Entidade de emissão**: selecione a entidade PKI criada anteriormente.
- **Método de emissão**: SIGN
- **Modelos**: selecione o modelo adicionado sob a entidade PKI.

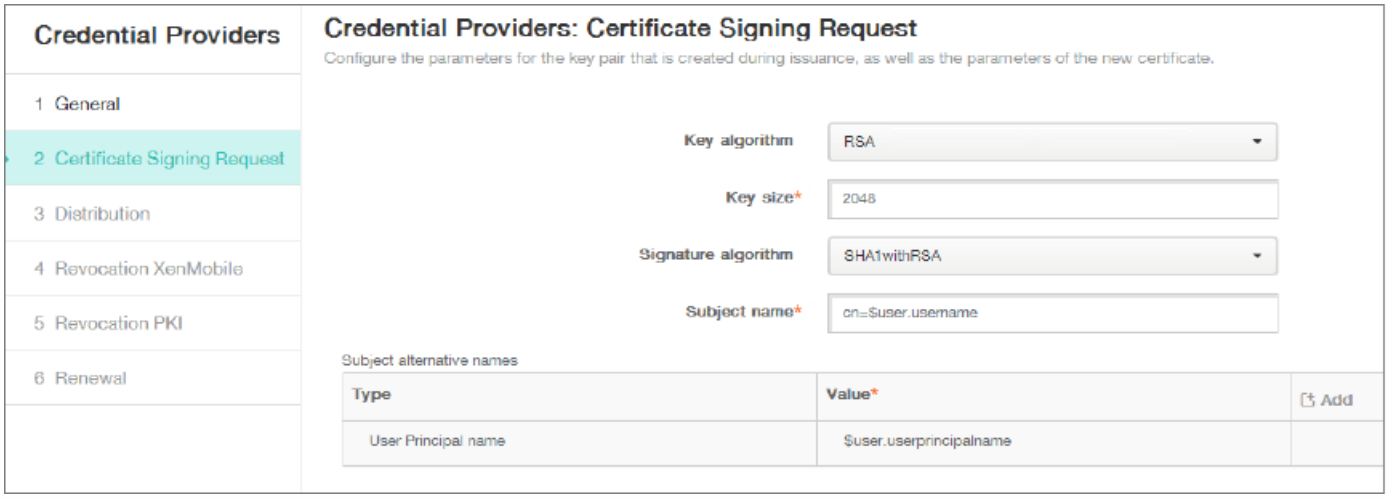


4. Clique em **Solicitação de assinatura de certificado** e insira os seguintes parâmetros:

- **Algoritmo de chave**: RSA
- **Tamanho da chave**: 2048
- **Algoritmo de assinatura**: SHA1withRSA
- **Nome de entidade**: cn=$user.username

Para **Nomes de entidade alternativos**, clique em **Adicionar** e insira os seguintes parâmetros:

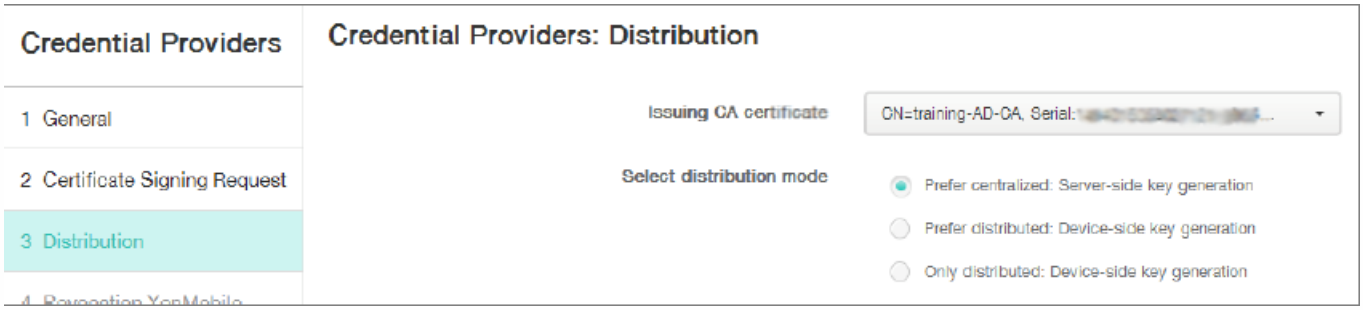
- **Tipo**: nome UPN
- **Valor**: $user.userprincipalname



5. Clique em **Distribuição** e insira os seguintes parâmetros:

- **Emissão de certificado AC**: selecione a AC emissora que assinou o Certificado cliente do XenMobile.
- **Selecionar modo de distribuição**: selecione **Preferir modo centralizado: geração de chaves do lado do servidor**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

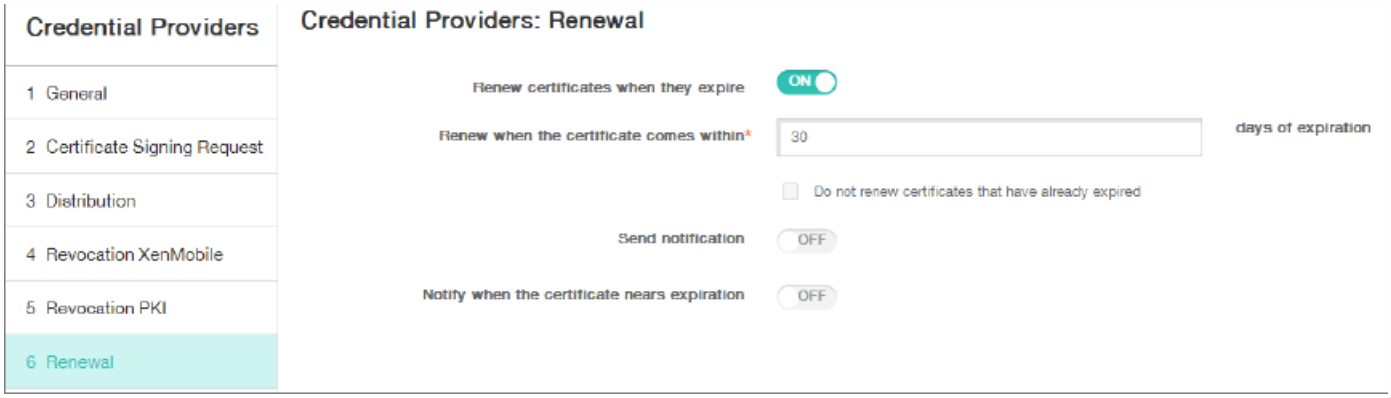


6. Para as duas próximas seções -- **Revogação XenMobile** e **Revogação PKI** -- defina os parâmetros conforme necessário. Para a finalidade deste artigo, ambas as opções são ignoradas.

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.

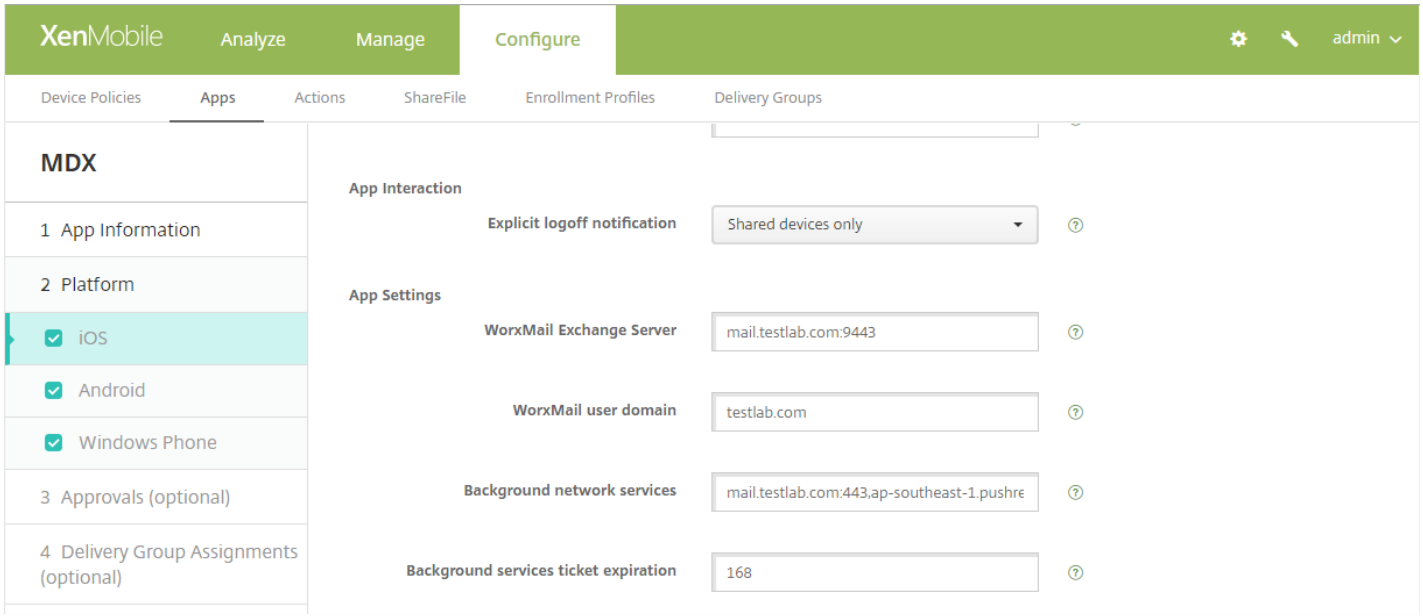


10. Clique em **Salvar**.

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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Configuração da entrega de certificado do NetScaler no XenMobile

1. Faça login no console XenMobile e clique no ícone de engrenagem no canto superior direito. A tela **Configurações** é exibida.

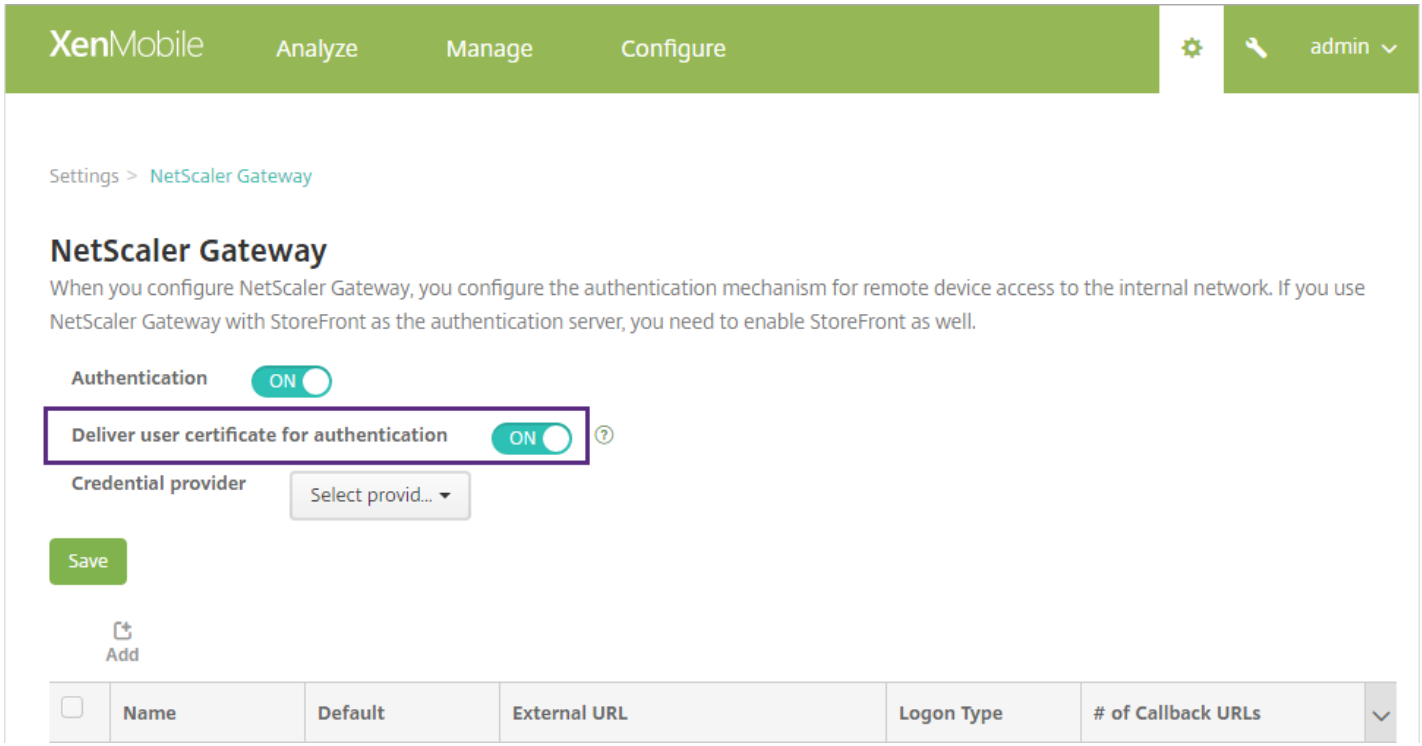
2. Em **Servidor**, clique em **NetScaler Gateway**.

3. Se o NetScaler Gateway já não estiver adicionado, clique em **Adicionar** e especifique as configurações:

- **URL externa**: https://YourNetScalerGatewayURL
- **Tipo de login**: Certificado
- **Requisito de senha**: O
- **Definir como padrão**: I

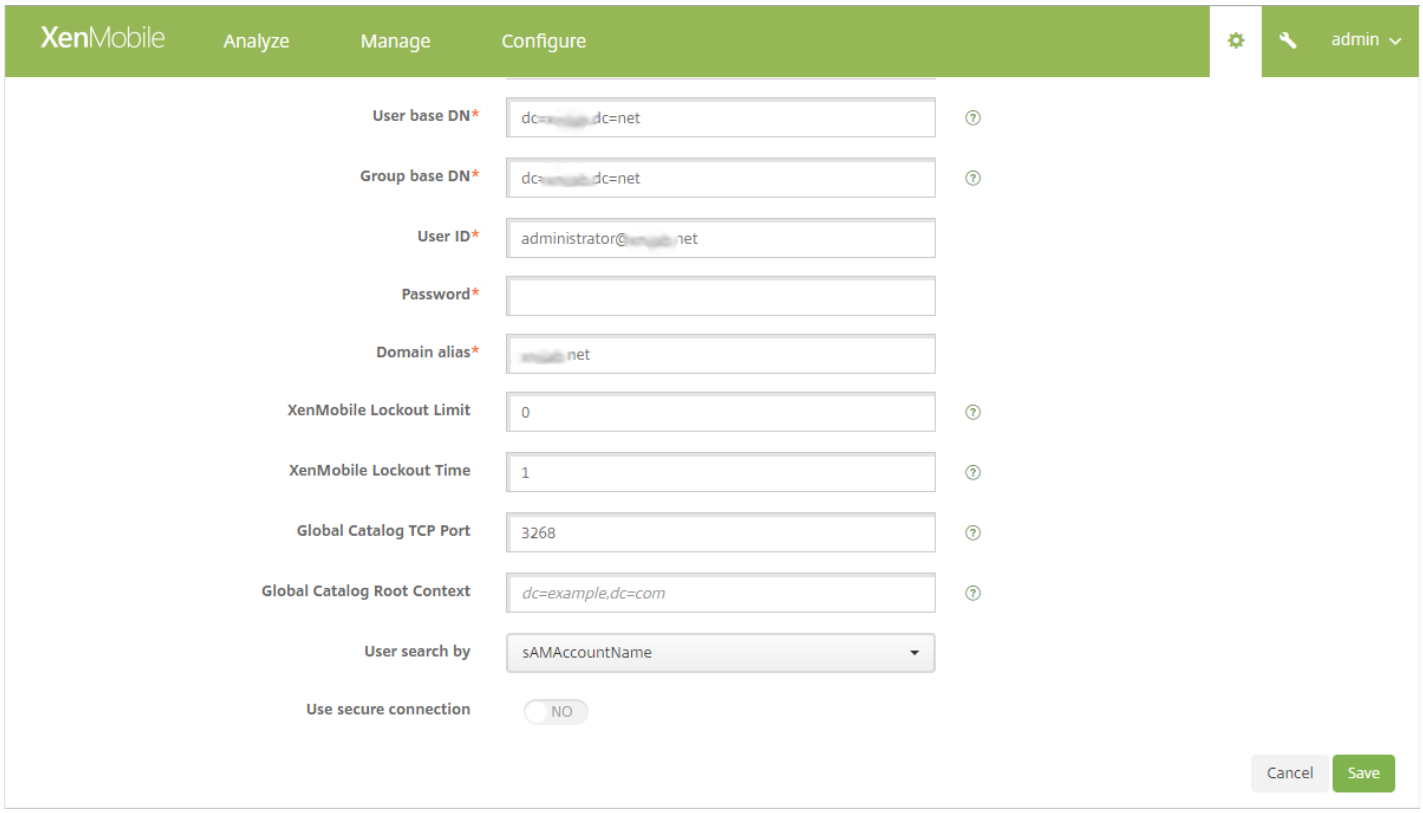
4. Para **Entregar certificado de usuário para autenticação**, selecione **I**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. Para **Provedor de credenciais**, selecione um provedor e clique em **Salvar**.

6. Se você 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**.



Ativar o PIN da Citrix e o cache de senha de usuário

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para ativar o PIN da Citrix e o cache de senha de usuário, vá para **Configurações > Propriedades do cliente** e marque as caixas de seleção: **Ativar autenticação com 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

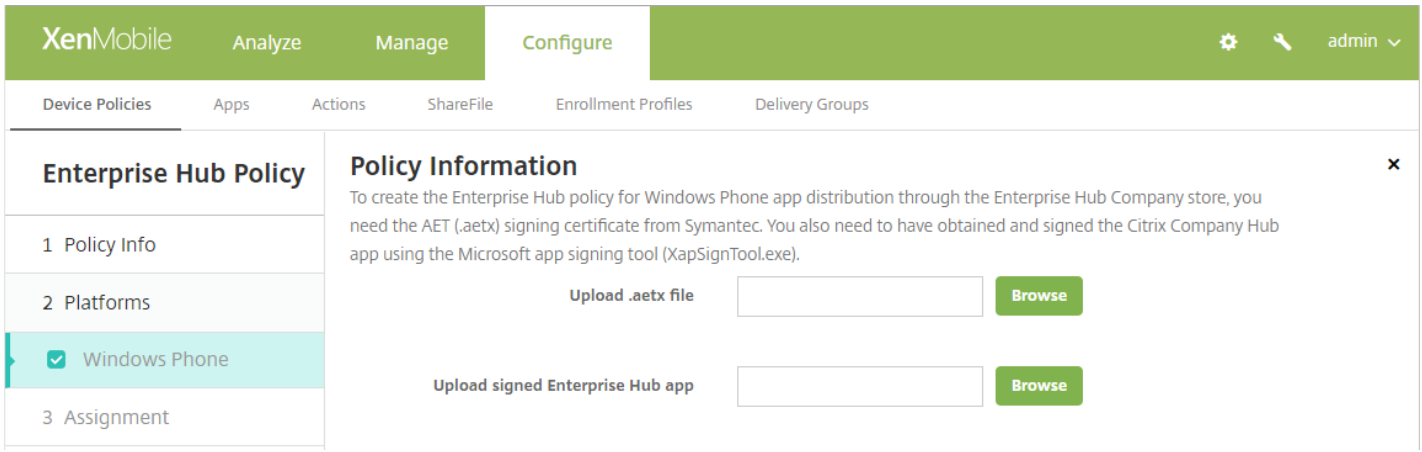
Para dispositivos Windows Phone, você deve criar uma política de dispositivo de Hub Empresarial para fornecer o arquivo AETX e o Secure Hub cliente.

> **Nota**
>
> Verifique se o arquivo AETX e o Secure Hub estavam usando o mesmo certificado empresarial do provedor de certificados e a mesma ID do 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.



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 NetScaler Gateway, o usuário fluxo de trabalho é o seguinte:

1. Os usuários registram seus dispositivos móveis.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. O XenMobile solicita que os usuários criem um PIN da Citrix.

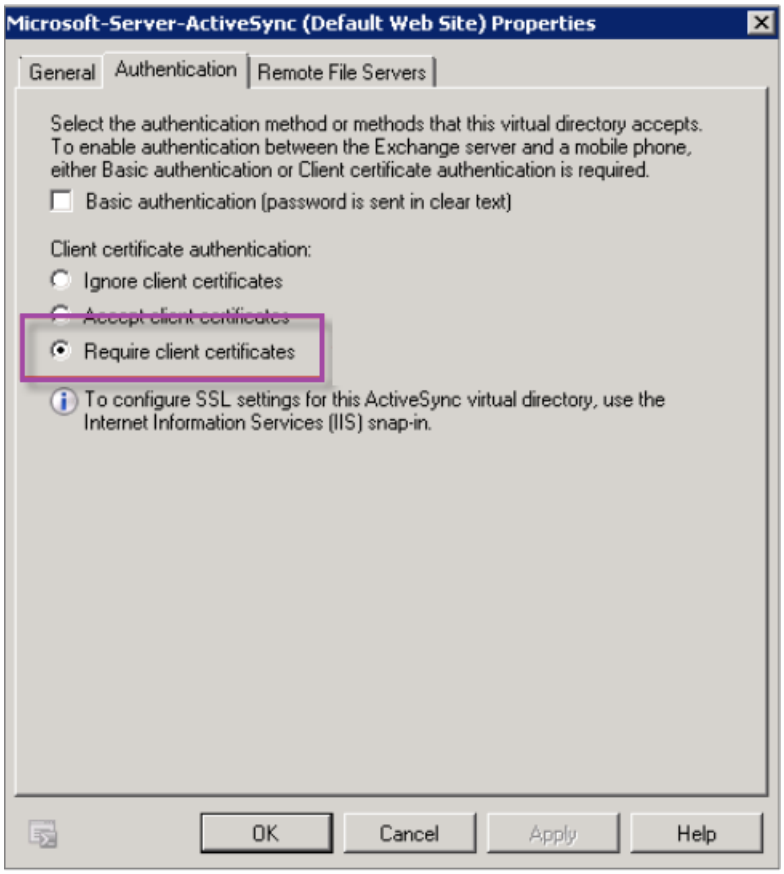
3. Os usuários são redirecionados para a XenMobile Store.

4. Quando os usuários iniciam o Secure Mail, o XenMobile não solicita credenciais de usuário para configurar suas caixas 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:

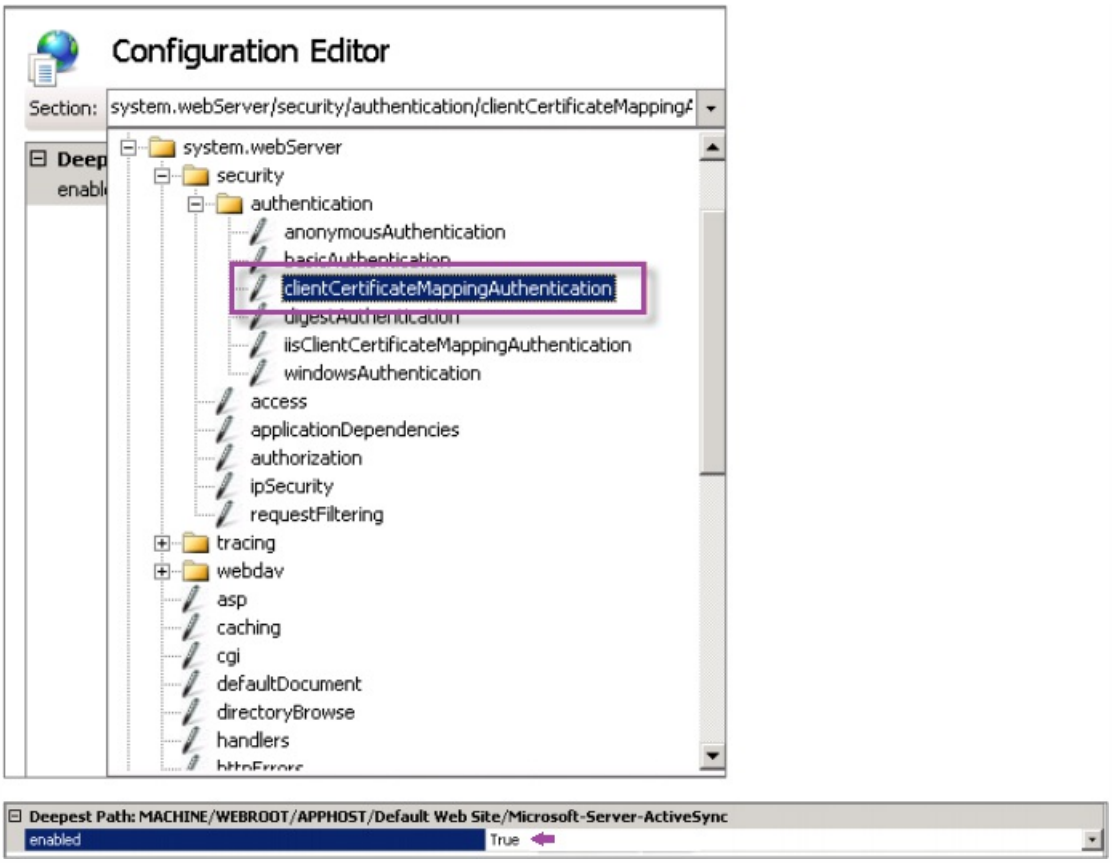
1. Se o Microsoft Exchange Server estiver usando certificados de servidor SSL privados para proteger o tráfego, verifique se a os certificados raiz/intermediário estão instalados no dispositivo móvel.

2. Verifique se o tipo de autenticação selecionado para o ActiveSync é **Exigir certificados de cliente**.



3. No Microsoft Exchange Server, verifique se o site **Microsoft-Server-ActiveSync** tem a autenticação de mapeamento de certificado de cliente habilitada (por padrão está desabilitada). A opção está em **Editor de configurações > Segurança > Autenticação**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Nota: depois de selecionar **True**, clique em **Aplicar** para que as alterações tenham efeito.

4. Verifique as configurações do NetScaler Gateway no console XenMobile: verifique se **Entregar certificado de usuário para autenticação** está definido como **I** e se **Provedor de credenciais** e tem o perfil correto selecionado, conforme descrito anteriormente em "Para configurar a entrega de certificado do NetScaler no XenMobile".

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 NetScaler 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 ligada 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

verifyclientcertrevocation=Enable VerifyRevocationWithCachedClientCertOnly=Disable UsageCheck=Enable clientcertnegotiation=Enable

Por exemplo:

netsh http add sslcert ipport=0.0.0.0:443 certhash=609da5df280d1f54a7deb714fb2c5435c94e05da 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 se o arquivo Application Enrollment Token (.AETX) é entregue por meio do XenMobile usando a política de dispositivo de hub empresarial.
- Verifique se 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.
- Verifique se a mesma ID do editor está sendo usado para assinar e preparar o Secure Hub, o Secure Mail e o Application Enrollment Token.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Entidades PKI

Feb 21, 2018

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 Symantec.

- 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.

> **Important**
>
> Quando você cria um modelo de Entidade de Serviços de Certificado Microsoft, para evitar possíveis problemas de autenticação com dispositivos registrados, evite usar caracteres especiais no nome do modelo. Por exemplo: ! : $ ( ) # % + * ~ ? | { } [ ]

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

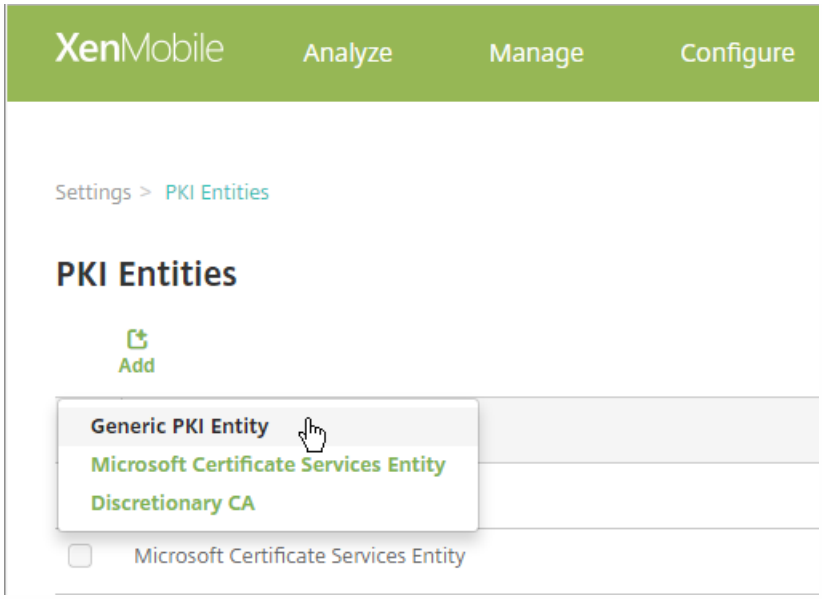
Para adicionar uma PKI genérica

1. No console XenMobile, clique em **Configurações** > **Entidades PKI**.

2. Na página **Entidades PKI**, clique em **Adicionar**.

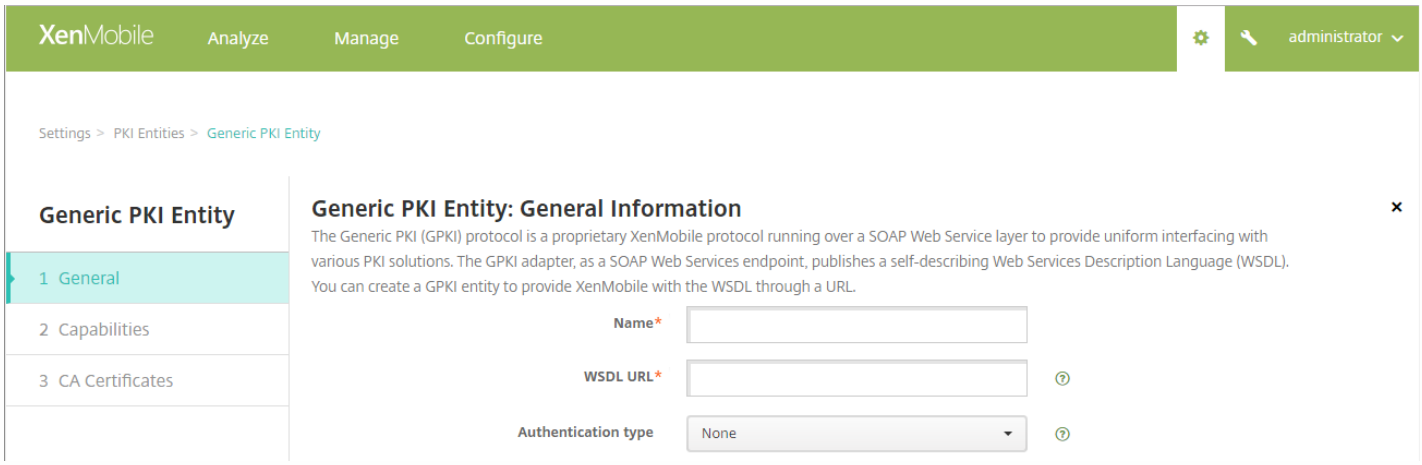
É exibido um menu de tipos de entidade PKI.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 de 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

entidade.

Nota: 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 pela Symantec

O suporte do XenMobile Server GPKI inclui PKI gerenciada da Symantec, também chamada MPKI. Esta seção descreve como configurar o Windows Server e o XenMobile Server para PKI gerenciada da Symantec.

Pré-requisitos

- Acesso a infraestrutura de PKI gerenciada da Symantec
- Servidor do Windows Server 2012 R2 com os seguintes componentes instalados:
  - Java
  - Apache Tomcat
  - Cliente PKI da Symantec
  - Portecle

    Para obter informações sobre como instalar os componentes, consulte "Configurar o Windows Server" a seguir.
- Acesso ao site de downloads XenMobile

Configurar o Windows Server

Esta seção ajuda você a configurar o Windows Server para que atenda aos requisitos do XenMobile para o suporte a GPKI.

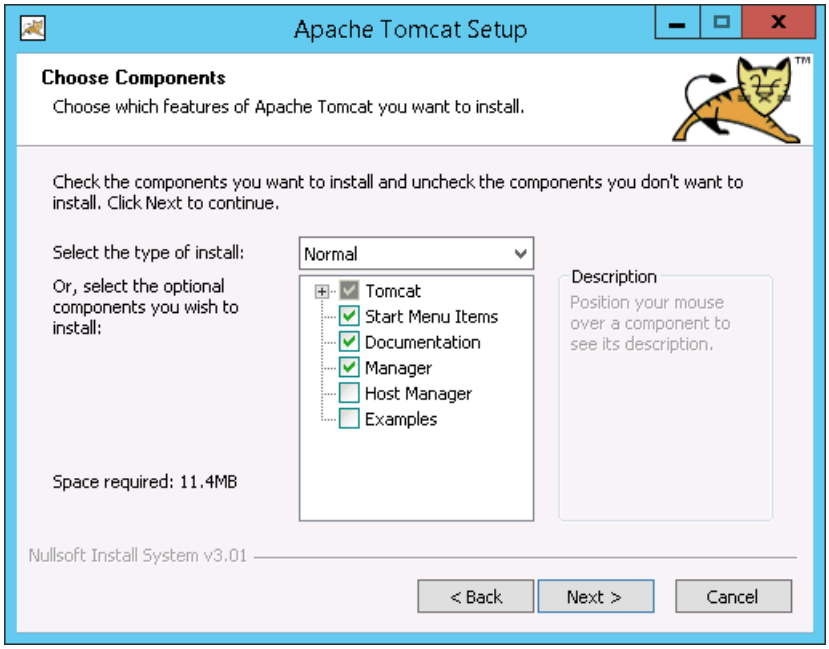
Instalar o Java no Windows Server

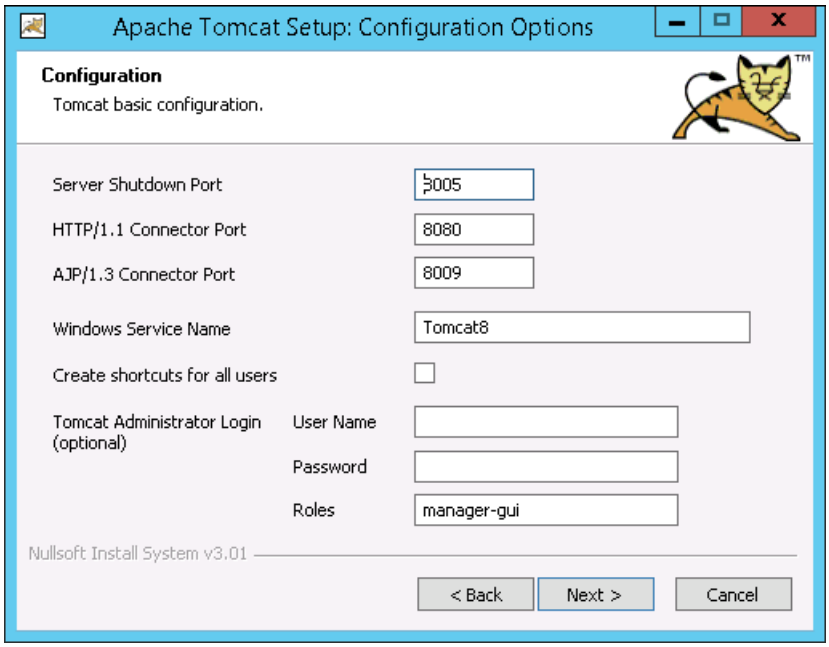
Baixe o Java de https://java.com/en/download/faq/java_win64bit.xml e instale-o. Na caixa de diálogo Aviso de segurança, certifique-se de clicar em **Executar**.

Instalar o Apache Tomcat no Windows Server

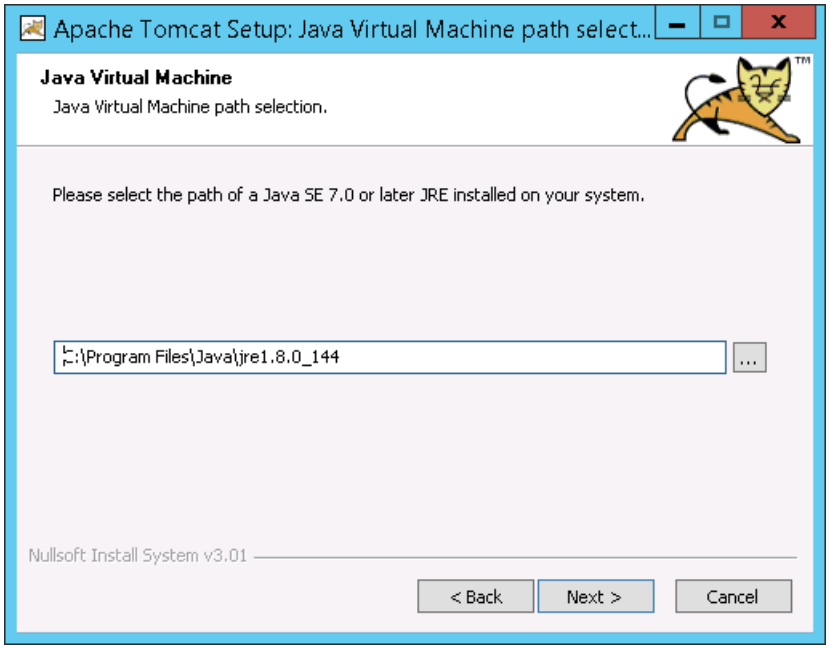
Baixe o instalador de serviços do Windows Apache Tomcat de 32/64 bits em https://tomcat.apache.org/download-80.cgi e depois instale-o. Na caixa de diálogo Aviso de segurança, certifique-se de clicar em **Executar**. Complete a configuração do Apache Tomcat, usando os seguintes exemplos como um guia.

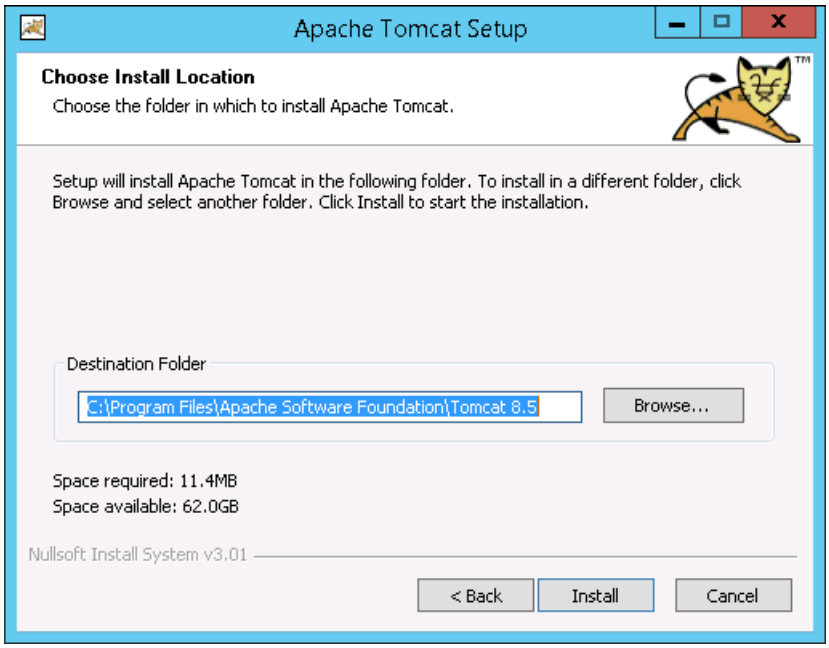
© 1999-2017 Citrix Systems, Inc. All rights reserved.



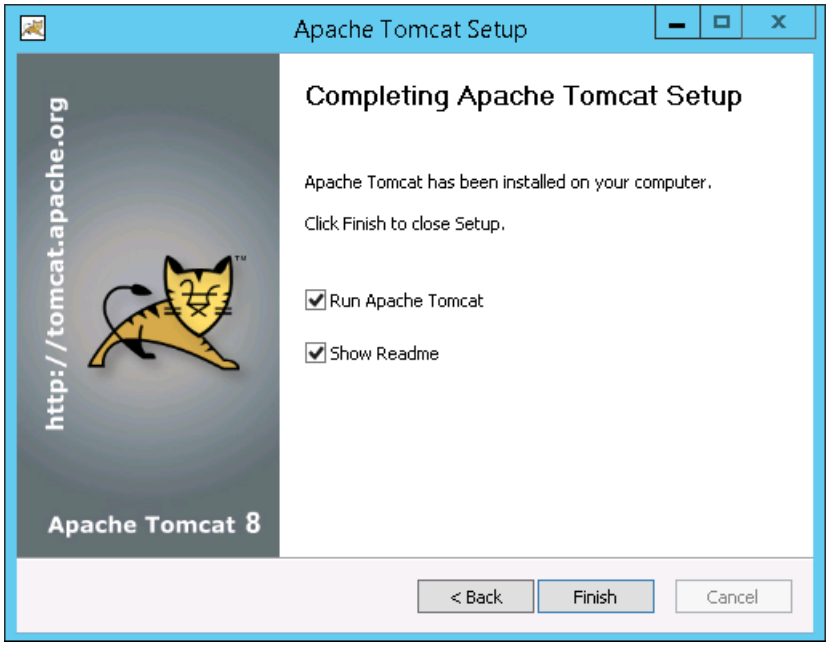


© 1999-2017 Citrix Systems, Inc. All rights reserved.

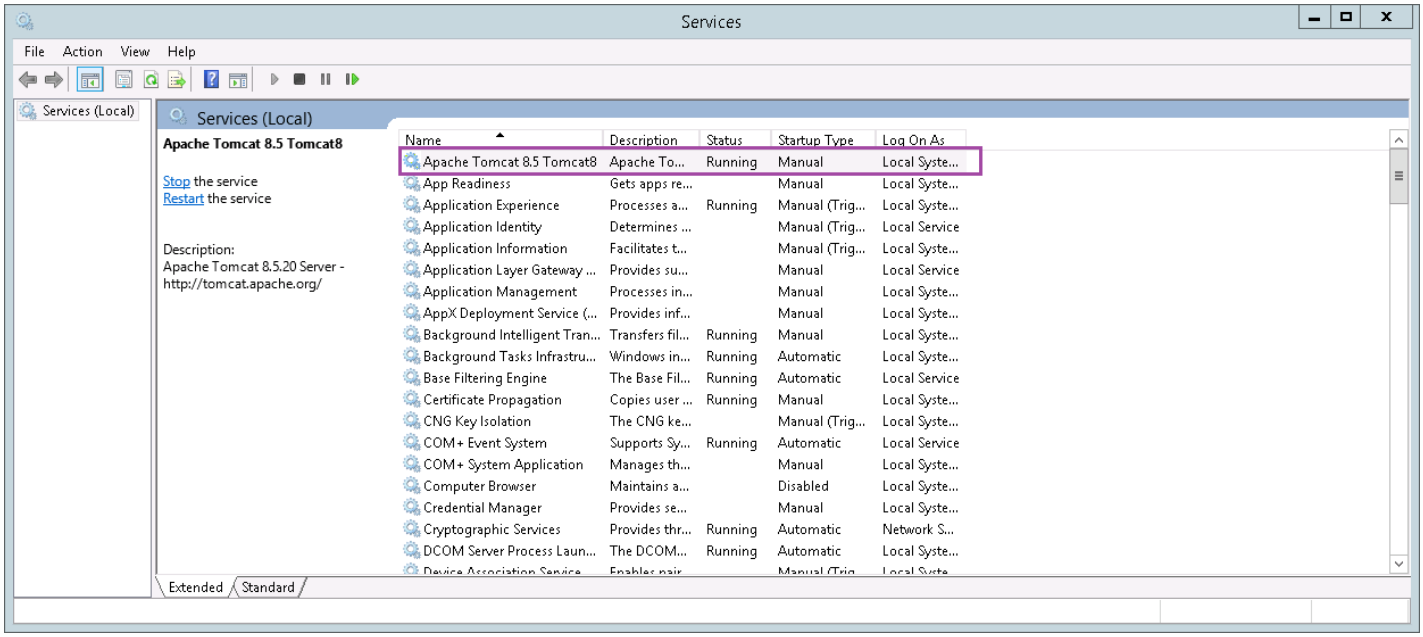




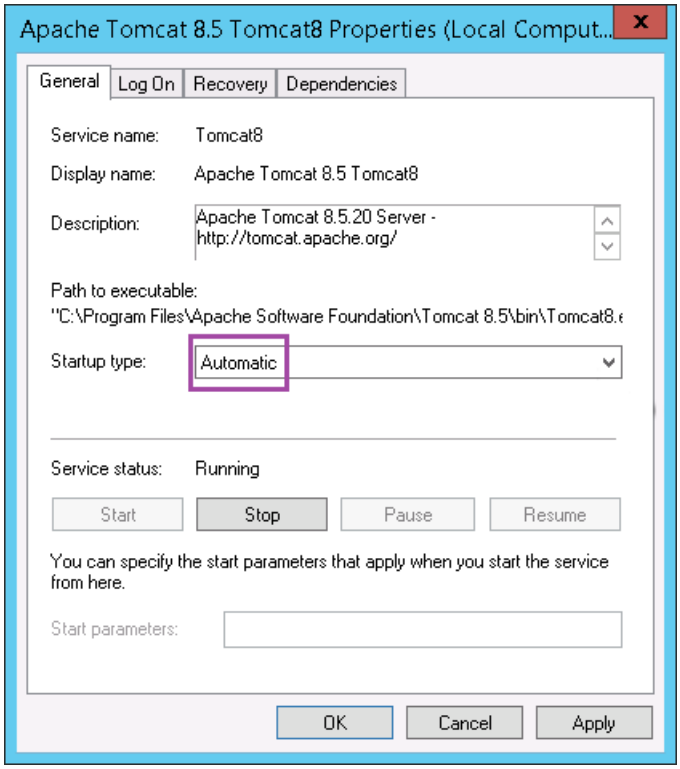
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Em seguida, vá até os Serviços do Windows e altere o **Tipo de inicialização** de **Manual** para **Automático**.

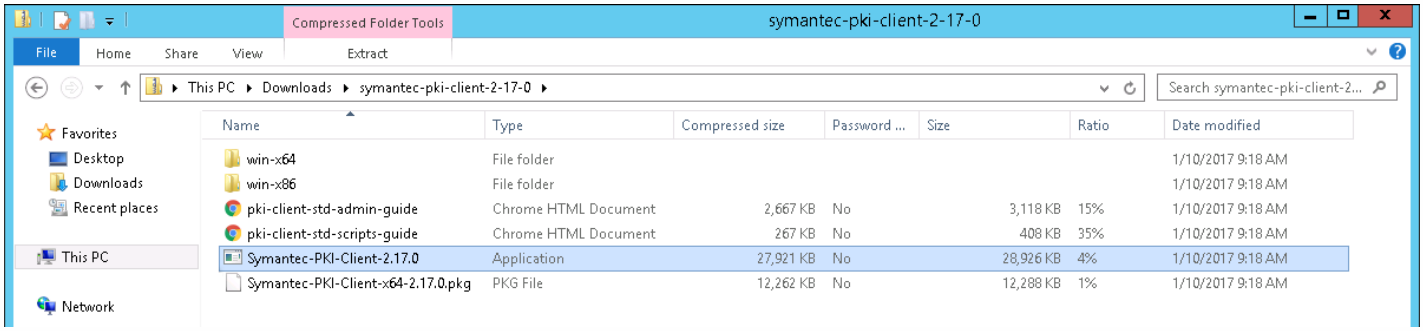


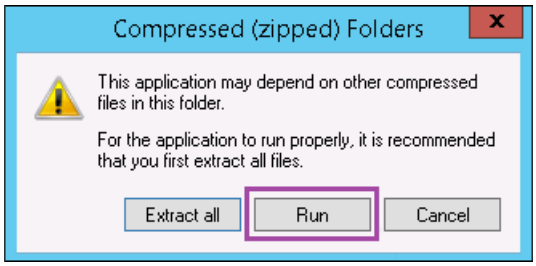
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Instalar o cliente Symantec 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 Symantec Como baixar o Symantec PKI Cliente. Descompacte e execute o instalador.





Na caixa de diálogo Aviso de segurança, certifique-se de clicar 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, em seguida, descompacte e execute o instalador.

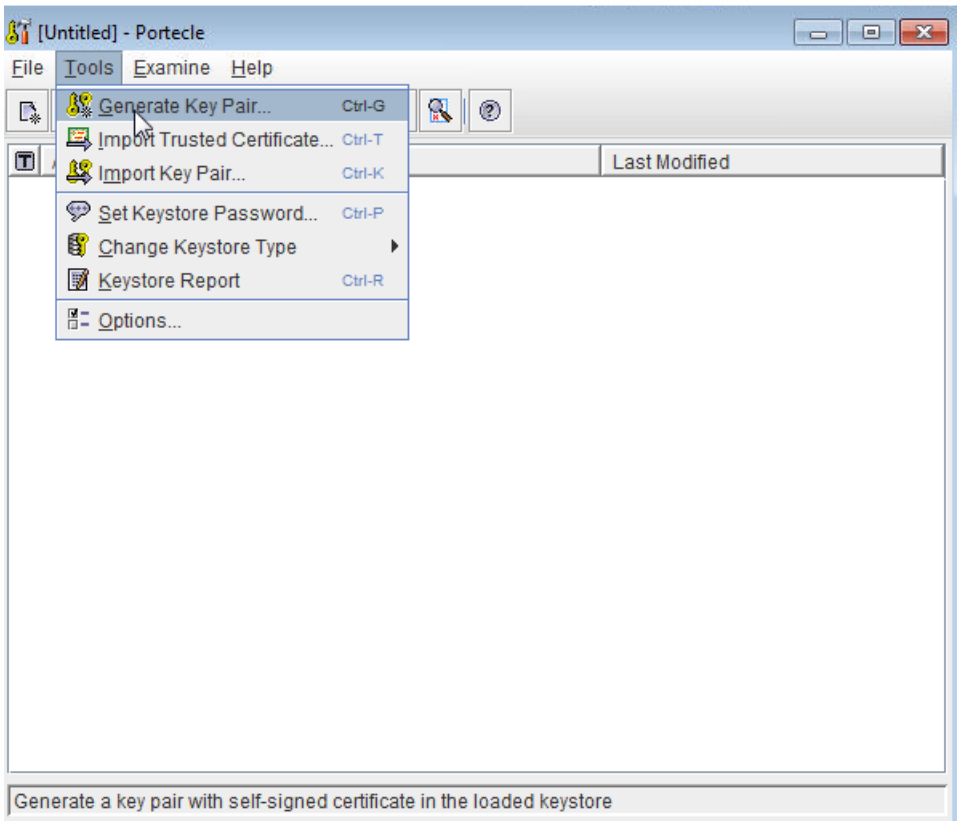
Gere o certificado de autoridade de registro (RA) para o PKI gerenciado da Symantec

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

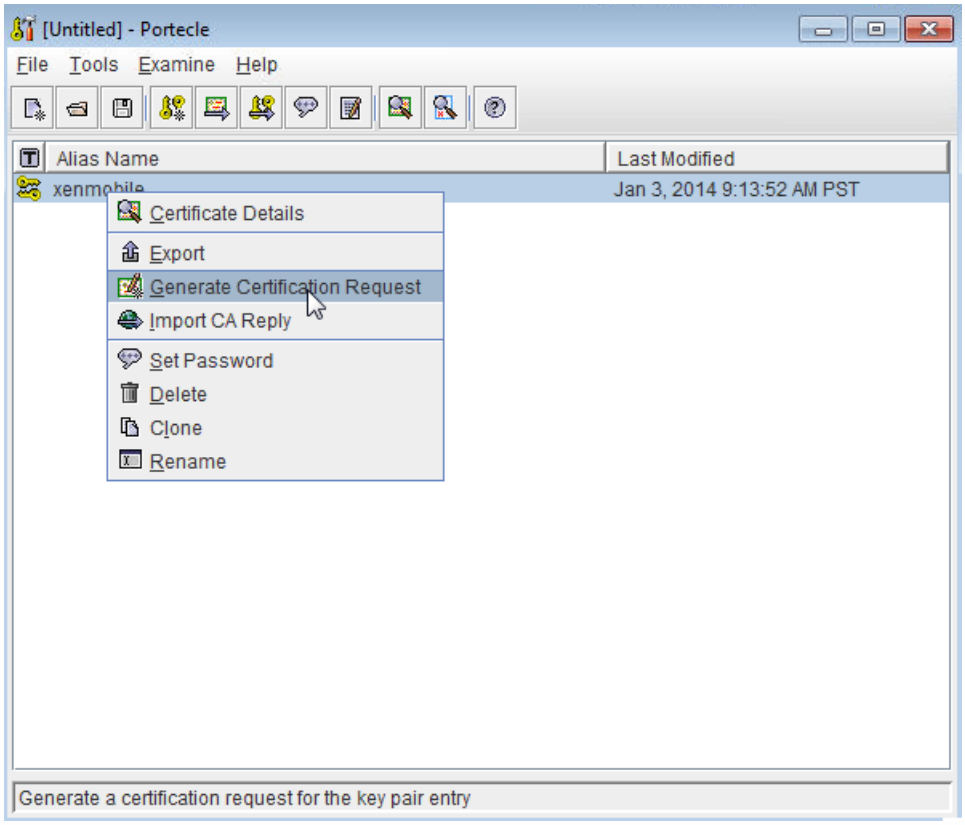
Este artigo também descreve como carregar o RA e os certificados públicos.

1. No Portecle, vá para **Tools** > **Generate Key Pair**, forneça as informações necessárias e gere um par de chaves.



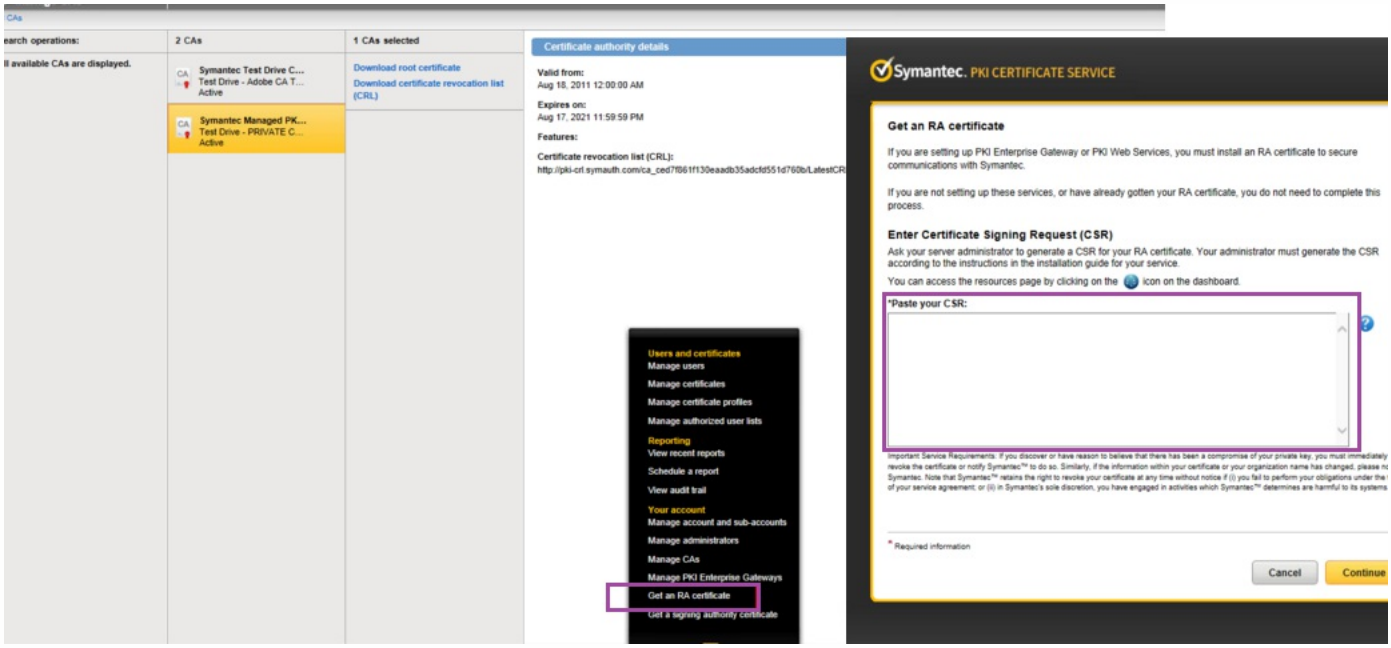
2. Clique com o botão direito do mouse no par de chaves e clique em **Generate Certification Request**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



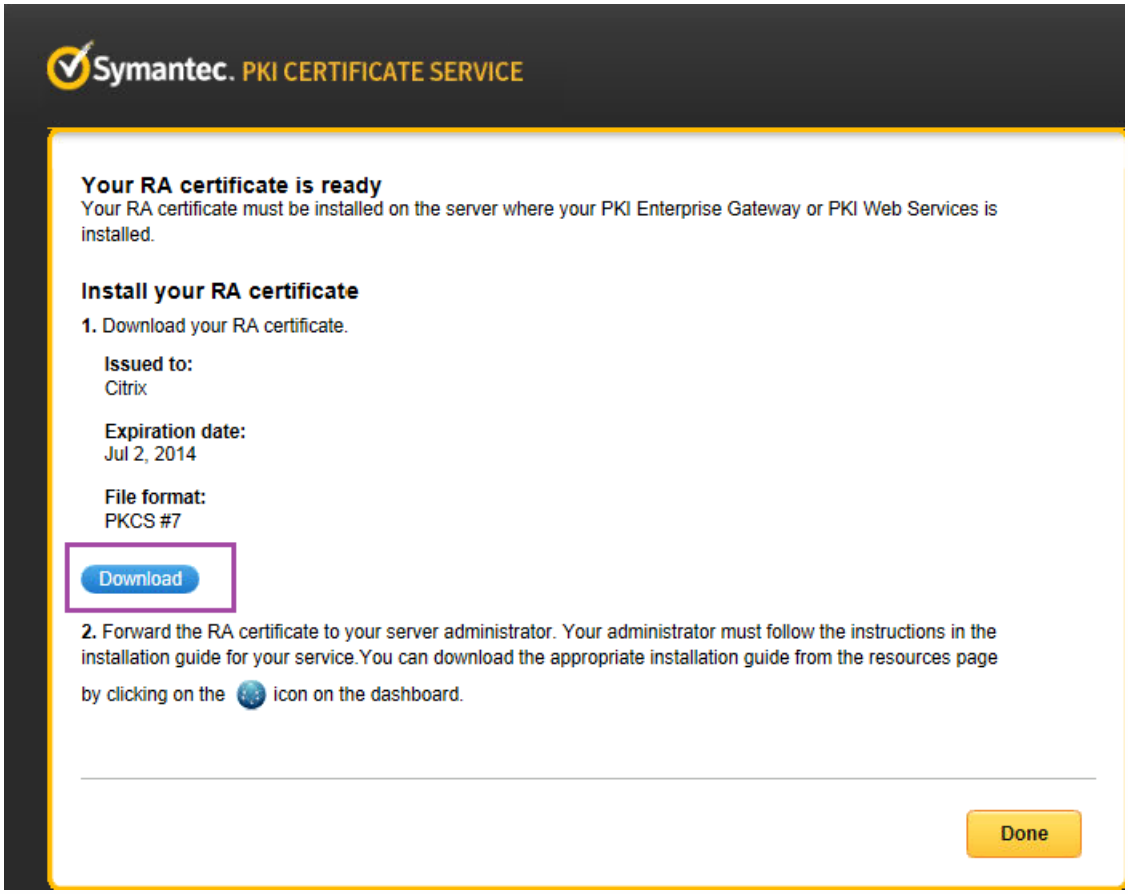
3. Copie o CSR.

4. No Symantec PKI Manager, gere um certificado de RA: clique em **Configurações**, clique em **Obter um Certificado RA**, cole o CSR e clique em **Continuar**.

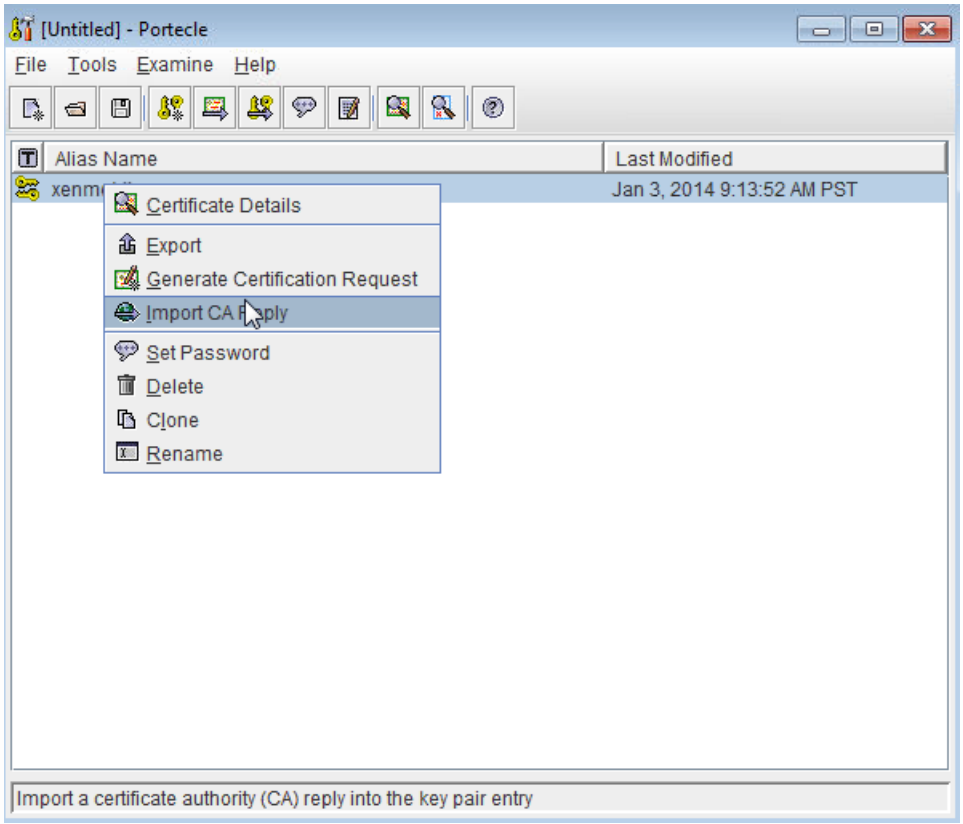


5. Clique em **Download** para baixar o certificado de RA gerado.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

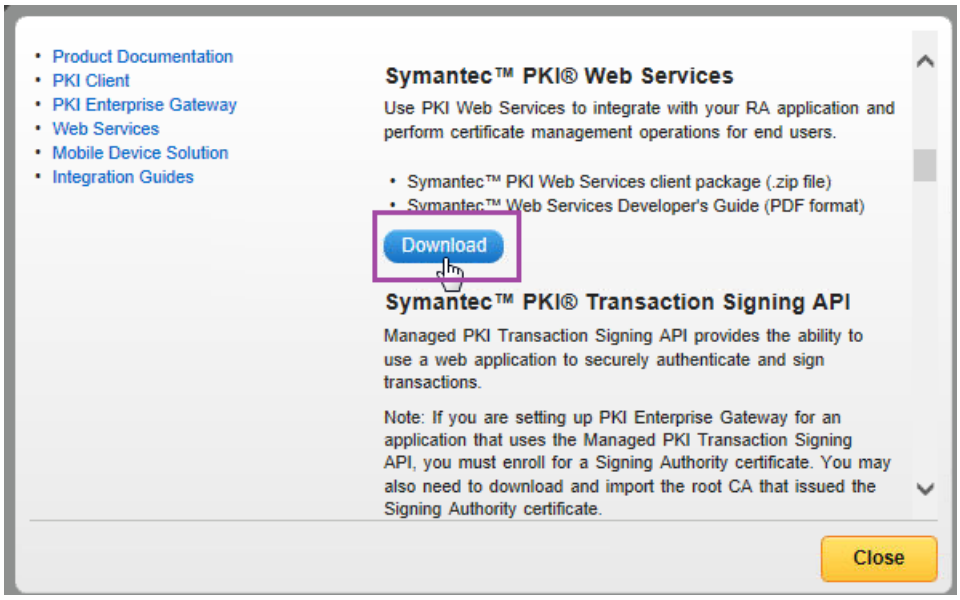


6. No Portecle, importe o certificado RA: clique com o botão direito do mouse no par de chaves e depois clique em **Import CA Reply**.

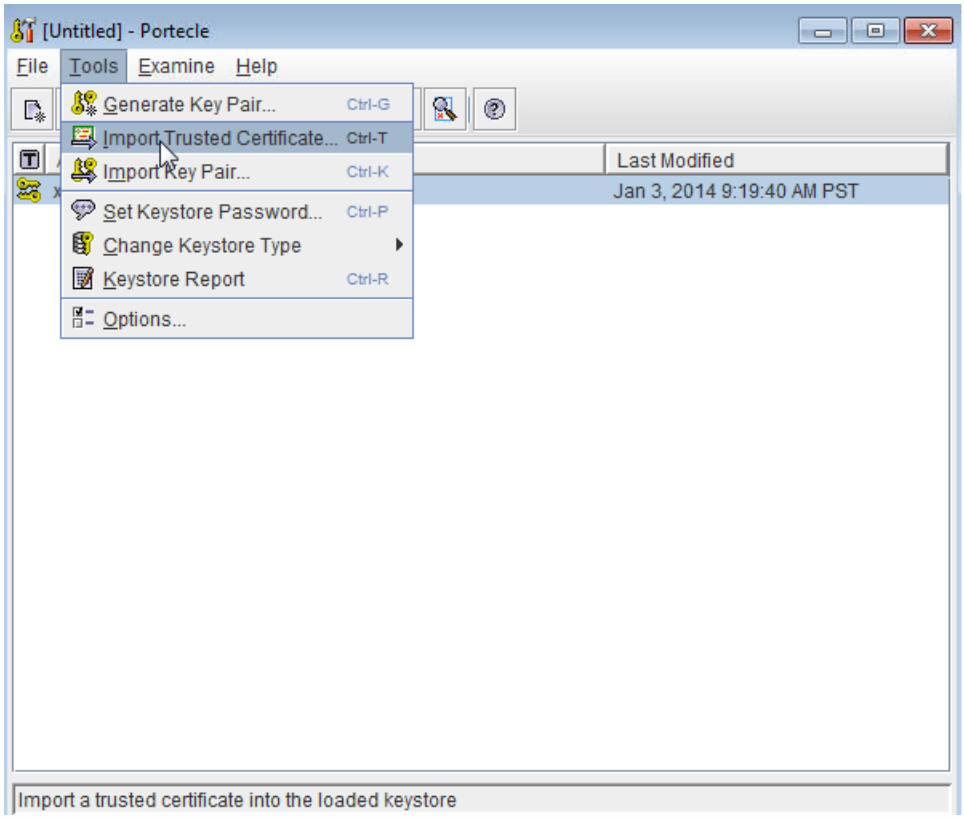


7. No Symantec PKI Manager: vá para **Recursos > Serviços da Web** e, em seguida, baixe os certificados da CA.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

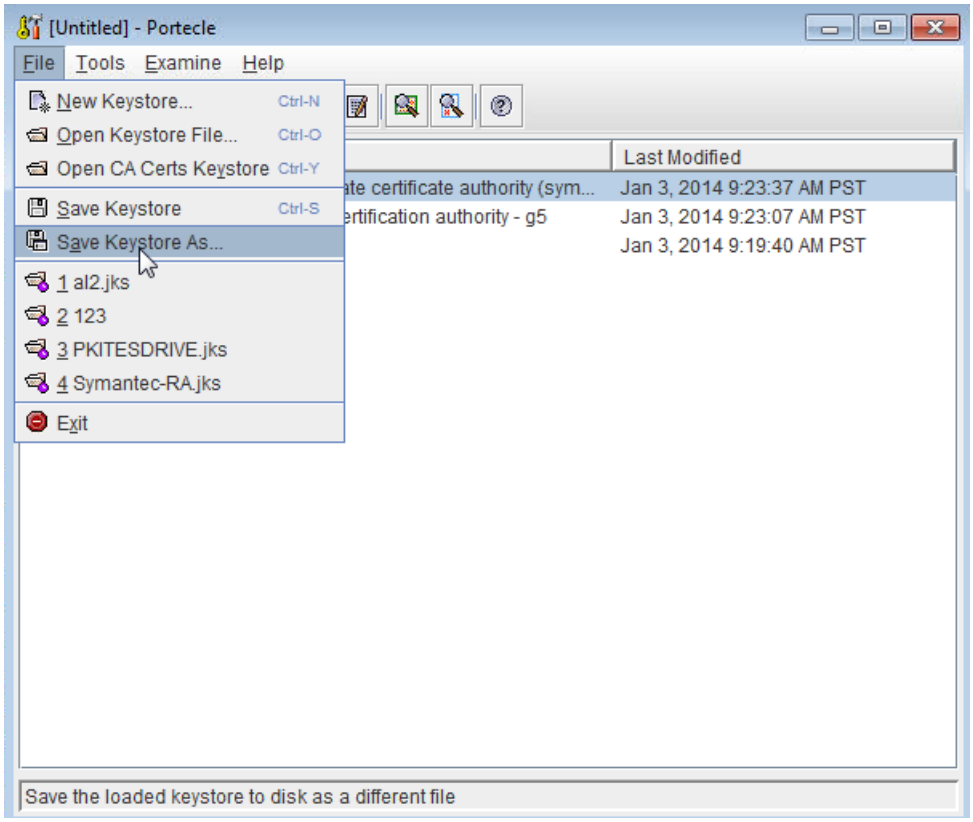


8. No Portecle, importe os certificados de RA intermediário e raiz para o keystore: vá para **Tools > Import Trusted Certificates**.



9. Depois de importar os CAs, salve o keystore como RA.jks na pasta C:\Symantec no Windows Server.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Configurar o Symantec 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. Na página de download do XenMobile Server 10, expanda **ferramentas** e baixe o arquivo do Symantec PKI Adapter. O nome do arquivo é XenMobile_Symantec_PKI_Adapter.zip. Descompacte o arquivo e copie esses arquivos para a unidade C: do Windows Server:
   - custom_gpki_adapter.properties
   - Symantec.war
4. Abra custom_gpki_adapter.properties no Bloco de Notas e edite os seguintes valores:

   Gpki.CaSvc.Url=https://

   # keystore para client-cert auth

   keyStore=C:\\Symantec\\RA.jks

   # truststore para servidor com CA raiz autoassinado

   trustStore=C:\\Symantec\\cacerts.jks
5. Copie Symantec.war sob a pasta \webapps e, em seguida, inicie o Tomcat.

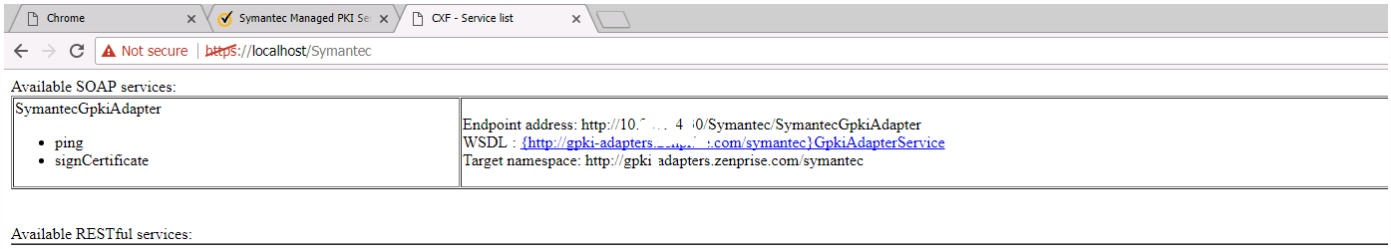
© 1999-2017 Citrix Systems, Inc. All rights reserved.

6. Verifique se o aplicativo foi implantado: abra um navegador da Web e vá até http://localhost/Symantec.

7. Vá até a pasta \webapps\Symantec\WEB-INF\classes e edite gpki_adapter.properties. Modifique a propriedade **CustomProperties** para apontar para o arquivo custom_gpki_adapter sob a pasta C:\Symantec:

   CustomProperties=C:\\Symantec\\custom_gpki_adapter.properties

8. Reinicie o Tomcat, navegue até http://localhost/Symantec, e, em seguida, copie o endereço de ponto de extremidade. Na próxima seção, você cola esse endereço ao configurar o adaptador PKI.

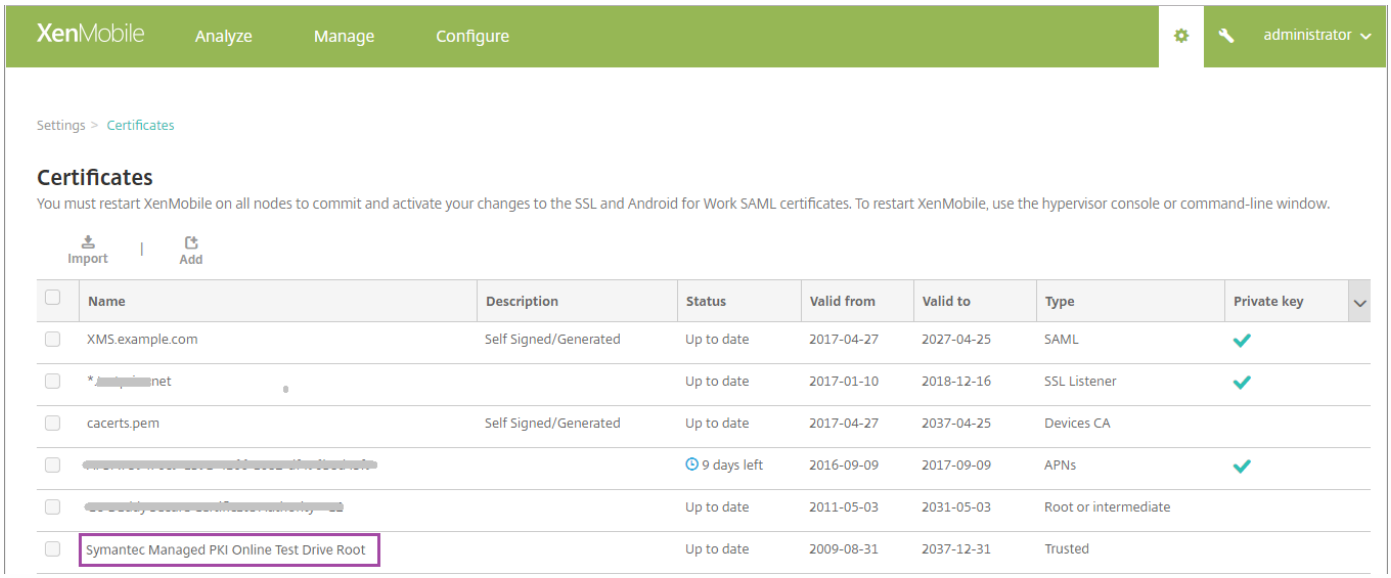


Configurar o XenMobile Server para PKI gerenciado da Symantec

Conclua a instalação do Windows Server antes de executar a configuração de XenMobile Server a seguir.

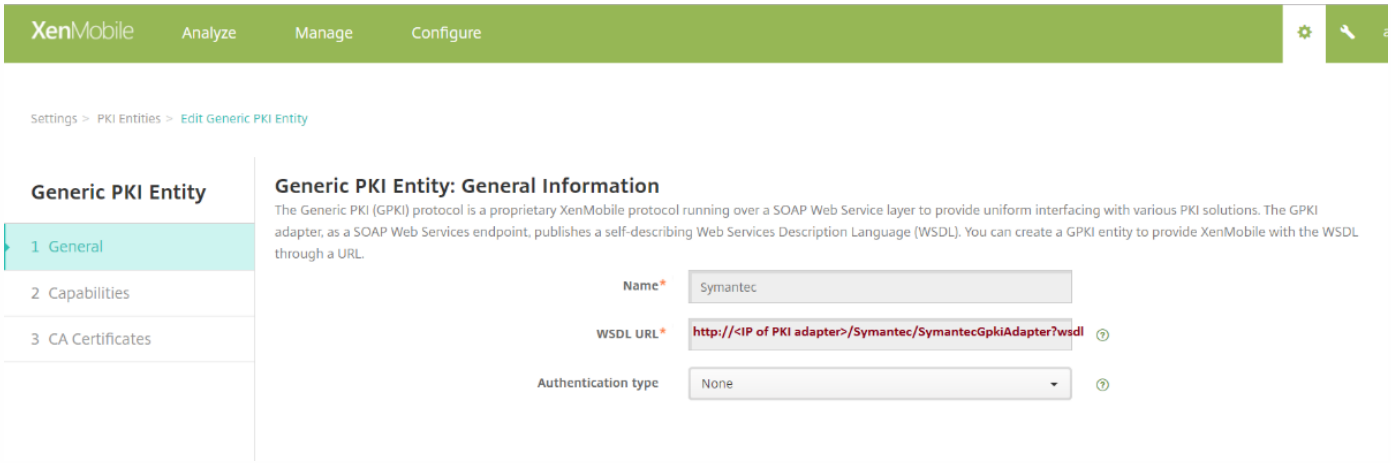
Para importar os certificados de AC da Symantec e configurar a entidade PKI

1. Importe os certificados de AC da Symantec que emitem o certificado do usuário final: no console do XenMobile Server, vá para **Configurações > Certificados** e clique em **Importar**.

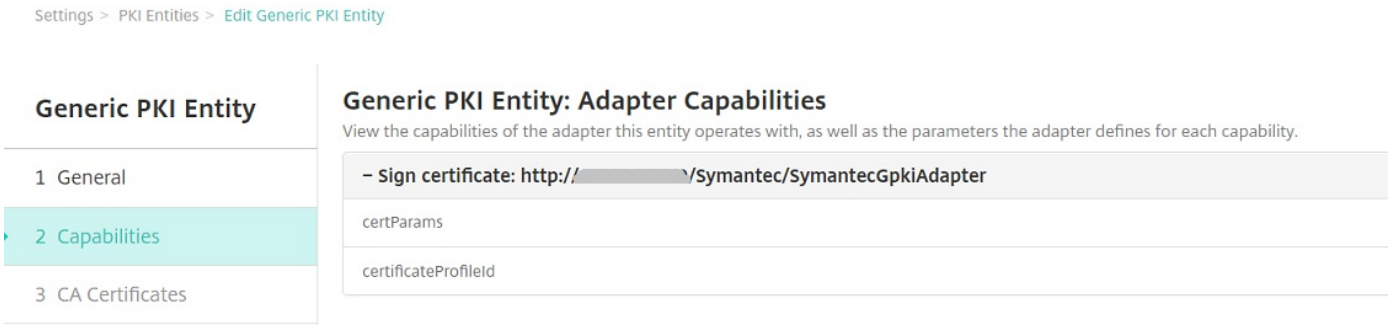


2. Adicione e configure a Entidade PKI: Vá para **Configurações > Entidades PKI**, clique em **Adicionar** e, em seguida, escolha **Entidade Genérica PKI**. Em **URL WSDL**, cole o endereço do ponto de extremidade que você copiou quando configurou o adaptador PKI na seção anterior e, em seguida, acrescente **?wsdl** conforme mostrado abaixo.

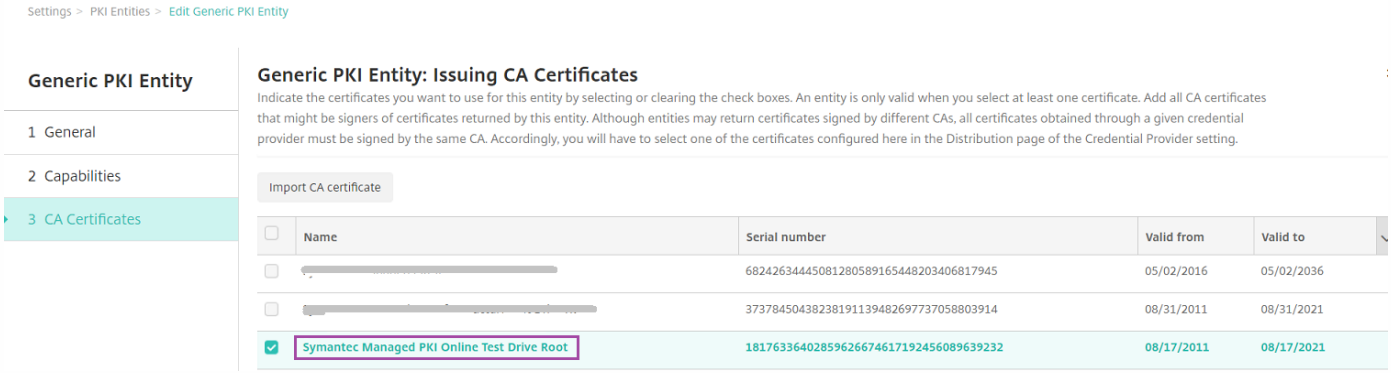
© 1999-2017 Citrix Systems, Inc. All rights reserved.



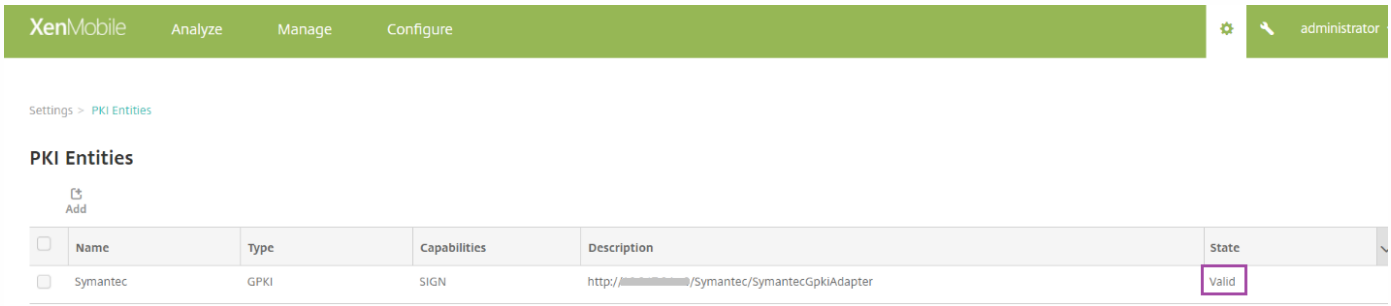
3. Clique em **Avançar**. O XenMobile preenche os nomes dos parâmetros do WSDL.



4. Clique em **Avançar**, selecione o certificado da autoridade de certificação correto e, em seguida, clique em **Salvar**.



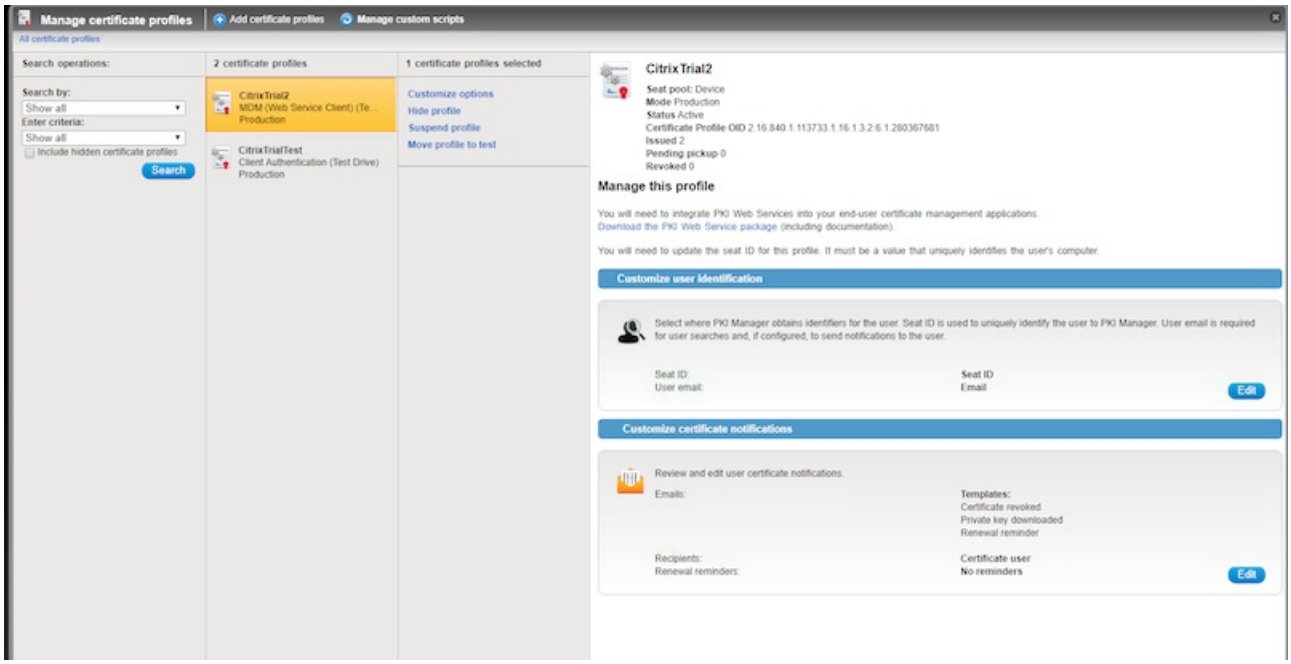
5. Na página **Configurações > Entidades de PKI**, verifique se o **Estado** da Entidade PKI que você adicionou é **Válido**.



Para criar o provedor de credenciais para PKI gerenciado da Symantec

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. No console do Symantec PKI Manager, copie o **OID do Perfil de Certificado** do Modelo de Certificado.



2. No console do XenMobile Sever, vá para **Configurações > Provedores de credenciais**, clique em **Adicionar**e, em seguida, defina as configurações da seguinte maneira.

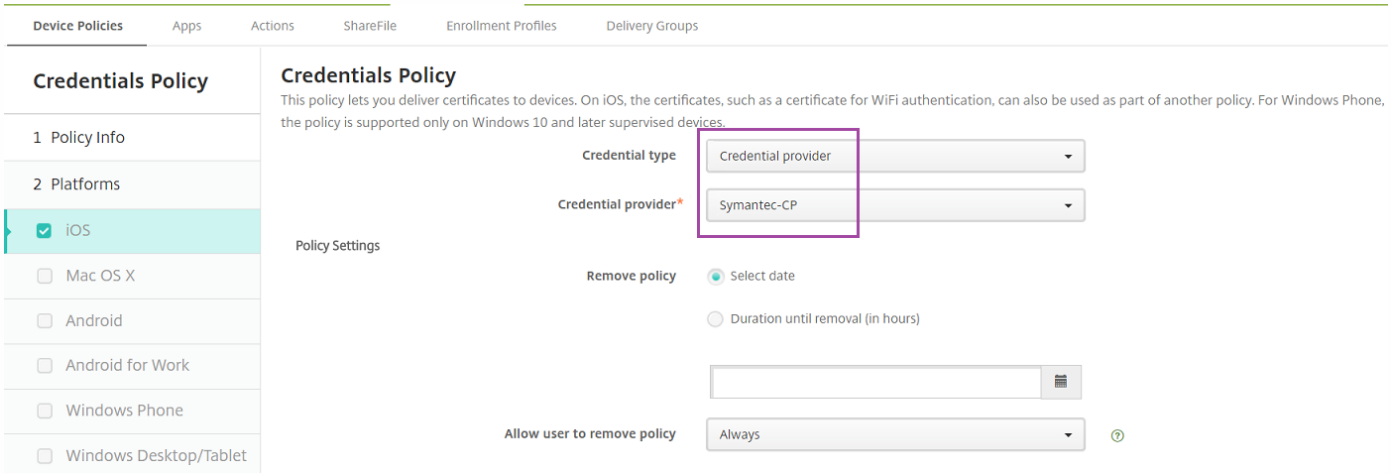
- **Nome**: digite um nome exclusivo para a nova configuração do provedor. Este nome é usado para referir-se à configuração em outras partes do console XenMobile.
- **Descrição**: descreva o provedor de credenciais. Embora esse campo seja opcional, uma descrição pode ser útil para quando você precisar 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.userprincipalname},mail=${user.mail}**
- **certificateProfileid**: cole o OID de perfil de certificado que você copiou na etapa 1.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

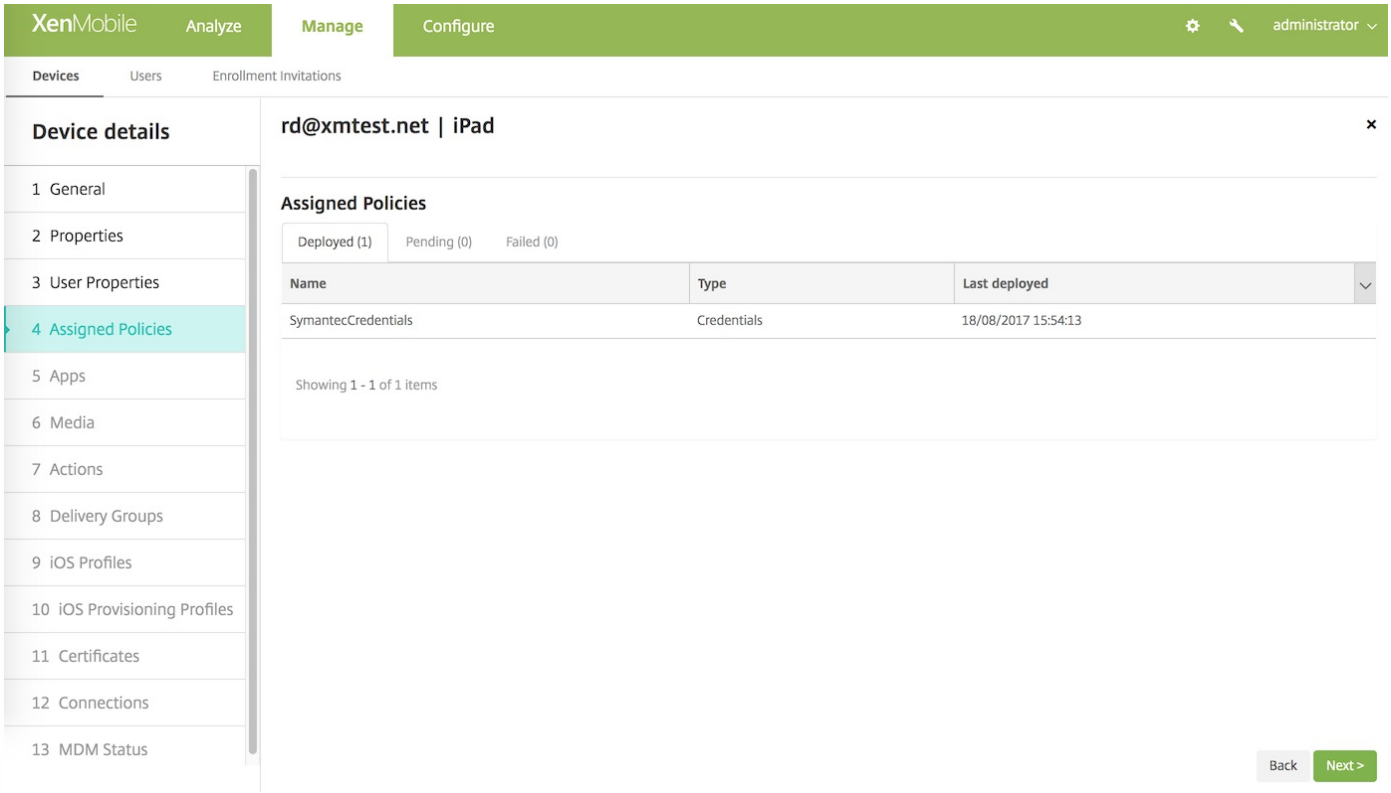
1. Criar uma política de dispositivo de credenciais: vá para **Configurar > Políticas de dispositivo**, clique em **Adicionar**, comece a digitar **Credenciais** e, em seguida, clique em **Credenciais**.
2. Especifique o **Nome da Política**.
3. Defina as configurações da plataforma, como se seguem:
   - **Tipo de credencial**: escolha **Provedor de credenciais**.
   - **Provedor de credenciais**: escolha o provedor Symantec.



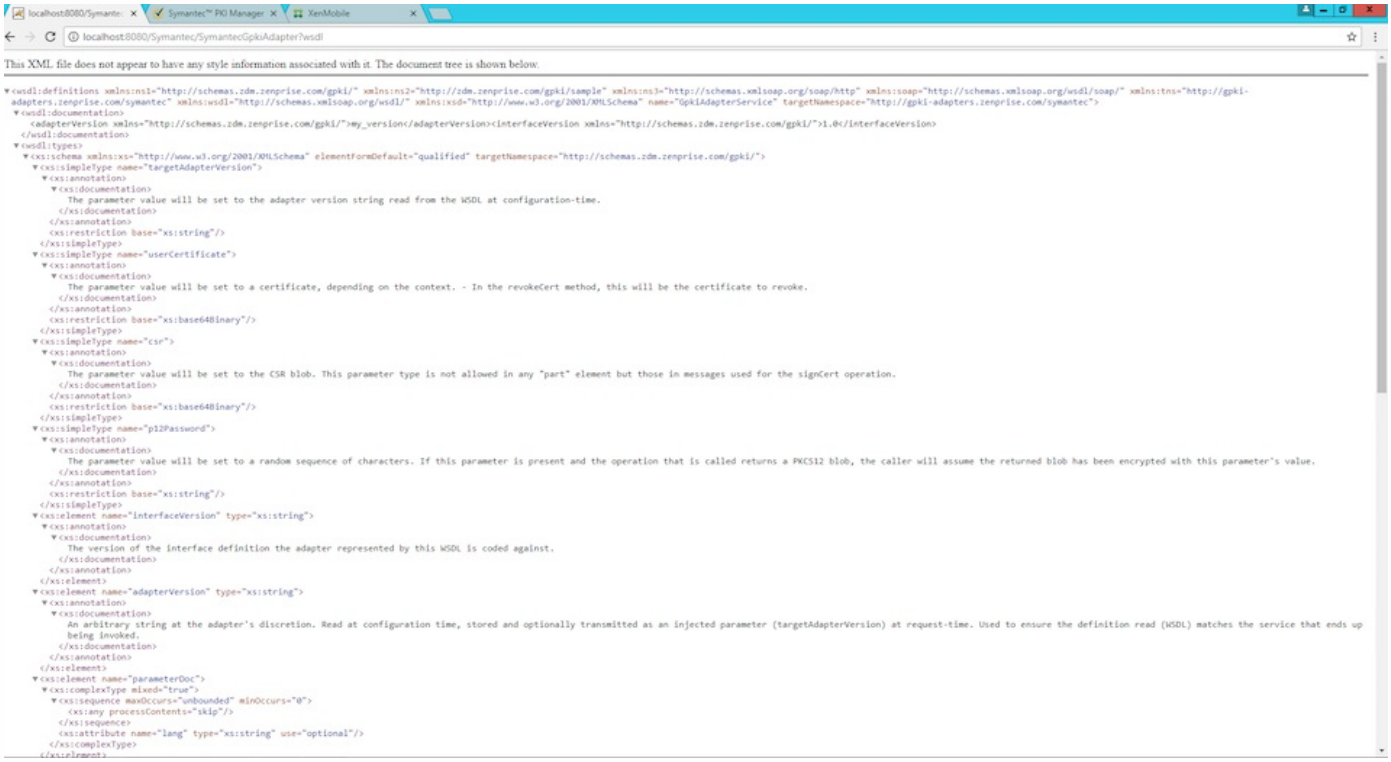
4. Depois de completar as configurações da plataforma, vá para a página **Atribuição**, atribua a política aos grupos de entrega e clique em **Salvar**.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Se a política não foi implantada, faça login no Windows Server e verifique se o WSDL está sendo carregado corretamente.



Para obter mais informações sobre a solução de problemas, verifique os logs do Tomcat em \logs\catalina..

Serviços de Certificado da Microsoft

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 NetScaler Gateway, o NetScaler Gateway é compatível com 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 Mais > **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 certnew.asp. Use o nome padrão a menos que você o tenha renomeado por algum motivo.
- **Tipo de autenticação**: escolha o método de autenticação que você deseja usar.
  - **Nenhum**
  - **HTTP básico**: digite o nome do usuário e a senha necessários para se conectar.
  - **Certificado de cliente**: escolha o certificado de 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 o certificado indicados em Certificados.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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** aparece. Nessa página, você pode especificar parâmetros personalizados que o XenMobile deve injetar na solicitação HTTP para a interface do 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**.

A página **Entidade de serviços de certificado da Microsoft: Certificados CA** é exibida. Nessa página, você deve informar ao XenMobile dos signatários dos certificados que o sistema obtém por meio dessa entidade. Quando o seu certificado de AC for renovado, atualize-o no XenMobile e, em seguida, a alteração será aplicada 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 NetScaler

O XenMobile dá suporte a lista de certificados revogados (CRL) somente para uma Autoridade de Certificação terceira. Se você tiver configurado uma AC da Microsoft, o XenMobile usa o NetScaler para gerenciar a revogação.

Quando você configurar a autenticação baseada em certificado de cliente, decida se quer definir a configuração de CRL (Lista de revogação de certificados do NetScaler), **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 de 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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Quando você configurae 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 AC discricionária.
- **Certificado AC para assinar solicitações de certificado**: clique em um certificado da AC 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 AC discricionária gera números de série para os certificados que ela emite. Nessa lista, clique em **Sequencial** ou **Não sequencial** para determinar como os números são 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 AC 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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

A página **AC 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 o keyUsage keyEncryption e um certificado de assinatura RA com o 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 **AC 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Provedores de credenciais

Feb 21, 2018

Os provedores de credenciais são as configurações reais de certificado que você usa em várias partes do sistema XenMobile. Eles definem as origens, os parâmetros e os ciclos de vida dos certificados, quer eles façam parte das configurações do dispositivo ou sejam autônomos, ou seja, enviados como são 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 e, em seguida, as configurações de emissão para P determinarem 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 D é revogado.

Com isso em mente, a configuração do provedor de credencial no XenMobile realiza o seguinte:

- Determina a fonte dos certificados.
- Determina o método pelo qual os certificados são obtidos: assinando um novo certificado ou obtendo (recuperando) um certificado e um par de chaves existentes.
- Determina os parâmetros para emissão ou recuperação. Por exemplo, os parâmetros de CSR (Solicitação de Assinatura de Certificado), como tamanho da chave, algoritmo de chave, nome diferenciado, extensões e assim por diante.
- Determina a forma como os certificados são entregues ao dispositivo.
- Determina as 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, 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 no XenMobile pode causar a respectiva revogação na PKI.
- Determina as configurações de renovação. Os certificados obtidos por meio de um determinado provedor de credenciais podem ser renovados automaticamente quando estiverem perto do vencimento ou, de modo independente dessa situação, poderão ser enviadas notificações quando o vencimento estiver próximo.

Até que ponto as várias opções de configuração estão disponíveis 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, chamado de métodos de emissão, de duas maneiras:

- **assinar**. Com esse método, a emissão envolve a criação de uma nova chave privada, a criação de um CSR e o envio do CSR para uma Autoridade de Certificação (AC) 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 AC discricionária).
- **obter**. Com esse método, a emissão, para fins do XenMobile, é uma recuperação de um par de chaves existente. O XenMobile é compatível com o método obter somente para PKI Genérica.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 sempre é enviado para o dispositivo como um PKCS#12, o equivalente ao modo de entrega centralizado do método assinar.

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 deve carregar os certificados para o XenMobile e criar 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 SHTP	Não	Não
Configuração SHTP	Não	Não
Registro de telefone e tablet com Windows	Não	Não

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Contexto	SCEP com suporte	SCEP necessário
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. Esse status é levado em consideração quando o XenMobile avalia um certificado apresentado a ele ou quando o XenMobile deve fornecer as informações de status OCSP de algum certificado. A configuração do provedor de credenciais determina como o status é afetado sob várias condições. Por exemplo, o provedor de credenciais pode especificar que os certificados obtidos por meio do provedor de certificados devem ser sinalizados como revogados quando os certificados tiverem sido 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 ele foi revogado internamente pelo XenMobile, 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 o revogará internamente. Esse mecanismo usa o protocolo OCSP.

Esses três tipos não são exclusivos, mas, em vez de aplicá-los em conjunto: a revogação interna é causada por uma revogação externa ou por descobertas independentes e, por sua vez, a revogação interna possivelmente afeta 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.

Observe que o XenMobile primeiro tenta obter o novo certificado antes de revogar o certificado anterior para evitar a descontinuação do serviço se a emissão falhar. Se for usada a entrega distribuída (compatível com SCEP), a revogação também ocorrerá somente depois que o certificado tiver sido instalado com êxito no dispositivo; caso contrário, ela ocorrerá antes que o novo certificado seja enviado para o dispositivo e de forma independente do êxito ou da falha da respectiva instalação.

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. Em caso positivo, ocorre uma tentativa de renovação.

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 de uma entidade discricionária é sempre assinar, o que significa que a cada operação de emissão, o XenMobile assina um novo par de chaves com o certificado de AC selecionado para a entidade. A geração do par de chaves no dispositivo ou no servidor

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 Symantec, incluindo a criação do provedor de credenciais, consulte "Symantec Managed PKI" nas entidades PKI.

1. No console Web XenMobile, clique no ícone de engrenagem no canto superior direito do console e clique em **Mais** > **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 referir-se à configuração em outras partes do console XenMobile.
- **Descrição**: descreva o provedor de credenciais. Embora esse seja um campo opcional, uma descrição pode ser útil no futuro para ajudar você a se lembrar de detalhes 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 a autenticação de certificado de cliente, use **Assinar**.
- Se a lista de **Modelos** estiver disponível, selecione o modelo que você adicionou sob a entidade PKI para o provedor de credenciais.

4. Clique em **Avançar**.

Nota: esses modelos são disponibilizados quando as Entidades de serviços de certificado da Microsoft são adicionadas em **Configurações** > **Entidades PKI**.

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. Esse campo é necessário.
  Observação: os valores permissíveis dependerão do tipo de chave; por exemplo, o tamanho máximo de chaves DSA é 1024 bits. Para evitar falsos negativos, o que dependerá do hardware e do software subjacentes, o XenMobile não impõe tamanhos de chave. Você deverá sempre testar 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 chaveA: RSA
  Tamanho da chave: 2048

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Algoritmo de assinatura: SHA1withRSA
Nome da entidade: cn=$user.username

6. Para adicionar uma nova 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

Observação: assim como o nome de entidade, você pode usar macros do XenMobile no campo de valor.

7. Clique em **Avançar**.

A página **Provedores de credenciais: distribuição** é exibida.

8. Na página **Provedores de credenciais: distribuição**, faça o seguinte:

- Na lista **Emissão de certificado AC**, clique no certificado AC oferecido. Como o provedor de credenciais usa uma entidade de AC discricionária, o certificado de AC do provedor de credenciais sempre será o certificado de AC configurado na entidade em si; ele será apresentado aqui para obter consistência com as 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 NetScaler 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 trata-se de “Somente” em vez de “Preferir”, nenhuma opção estará disponível se a geração de chaves 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.

9. 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.

12. Na página **Provedores de credenciais: revogação XenMobile**, faça o seguinte:

- Em **Revogar certificados emitidos**, selecione uma das opções que indicam quando os certificados devem ser revogados.
- Se você desejar que o XenMobile envie uma notificação quando o certificado for revogado, defina o valor de **Enviar**

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

notificação como **Ativado** e escolha um modelo de notificação.

- Se você desejar 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.

13. 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.

14. Na página **Provedores de credenciais: revogação PKI**, faça o seguinte se você deseja revogar os certificados da PKI:

- Altere a configuração **Ativar verificações de revogação externa** para **Ativado**. São exibidos campos adicionais relacionados à revogação PKI.
- Na lista **Certificado AC do respondedor OCSP**, clique no nome distinto (DN) da entidade do certificado. **Observação**: 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}\endquotation
- 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.

- Se você desejar 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 você 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.

15. 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, enviando opcionalmente uma notificação quando a renovação é concluída (notificação na renovação) e excluindo opcionalmente certificados já vencidos da operação.
- Emitir uma notificação para os certificados que estão perto do vencimento (notificação antes da renovação).

16. Na página **Provedores de credenciais: renovação**, faça o seguinte se você desejar renovar os certificados quando eles expirarem: defina **Renovar os certificados** quando eles expirarem como **Ativado**.

Campos adicionais são exibidos.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- No campo **Renovar quando o certificado expirar em**, digite quantos dias antes da expiração a renovação deve ser realizada.
- Opcionalmente, selecione **Não renovar certificados que já expiraram**. **Observação**: nesse caso, "já expiraram" significa que a data NotAfter do certificado está no passado, não que ele foi revogado. O XenMobile não renovará certificados depois que eles tiverem sido revogados internamente.

17. Se você desejar que o XenMobile envie uma notificação quando o certificado tiver sido renovado, defina **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 você 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.

18. Se você desejar que o XenMobile envie uma notificação quando o certificado estiver prestes a expirar, defina **Notificar quando o certificado estiver prestes a expirar** 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.

19. No campo **Notificar quando o certificado expira em**, digite quantos dias antes da expiração do certificado a notificação deve ser enviada.

20. Clique em **Salvar**.

O provedor de credenciais é adicionado à tabela Provedor de credenciais.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Certificados APNs

Mar 13, 2018

Para registrar e gerenciar dispositivos iOS com o XenMobile, você precisa configurar e criar um certificado de serviço de Notificação por Push da Apple (APNs) da Apple. Esta seção descreve as seguintes etapas básicas para solicitar o certificado de APNs:

- Use um Windows Server 2012 R2 ou um Windows 2008 R2 Server e os Serviços de Informações da Internet (IIS) da Microsoft ou um computador Mac para gerar uma Solicitação de Assinatura de Certificado (CSR).
- Faça a Citrix assinar a CSR.
- Solicite um certificado de APNs junto à Apple.
- Importe o certificado para o XenMobile.

Nota:

- O certificado de APNs da Apple permite o gerenciamento de dispositivo móvel por meio da Rede Push da Apple. Se você acidentalmente ou intencionalmente revogar o certificado, perderá a capacidade de gerenciar os seus dispositivos.
- Se você tiver usado o iOS Developer Program Enterprise para criar um certificado de envio por push do gerenciador de dispositivos móveis, talvez você precise tomar uma ação devido à migração dos certificados existentes no Apple Push Certificate Portal.

Os tópicos que descrevem os procedimentos passo a passo estão listados em ordem nesta seção da seguinte maneira:

Etapa 1: Para Windows, gere uma CSR usando o Windows Server 2012 R2 ou o Windows 2008 R2 Server, e o Microsoft IIS. Para Mac, gere uma CSR em um computador Mac. A Citrix recomenda esse método.

- Para criar uma CSR usando o Microsoft IIS
- Para criar uma CSR em um computador Mac

Etapa 2: Envie a CSR para a Citrix no site XenMobile APNs CSR Signing (o ID do MyCitrix é necessário). 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. Para obter mais informações, consulte Para assinar a CSR

Etapa 3: Envie a CSR assinada para a Apple no Apple Push Certificate Portal (o ID Apple é necessário) e baixe o certificado de APNs da Apple. Para obter mais informações, consulte Enviar CSR assinada para a Apple.

Etapa 4: Exporte o certificado de APNs como um certificado PCKS #12 (.pfx) (no IIS, Mac ou SSL). Consulte:

- Para criar um certificado de APNs .pfx usando o Microsoft IIS
- Para criar um certificado de APNs .pfx em um computador Mac
- Criar um certificado de APNs .pfx usando o OpenSSL

Etapa 5: Importe um certificado de APNs para o XenMobile.

Informações de migração de certificado de envio por push do Apple MDM

Os certificados de envio por push do gerenciamento de dispositivo móvel (MDM) criados no iOS Developer Program Enterprise foram migrados para o Apple Push Certificate Portal. Essa migração afeta a criação de novos certificados de envio por push do MDM e a renovação, a revogação e o download de certificados de envio por push do MDM existentes. A migração não afeta outros certificados de APNs (não MDM).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Se o seu certificado de envio por push do MDM tiver sido criado no iOS Developer Program Enterprise, as seguintes situações se aplicarão:

- O certificado foi migrado automaticamente para você.
- Você pode renovar o certificado no Apple Push Certificates Portal sem afetar os seus usuários.
- Você precisa usar o iOS Developer Program Enterprise para revogar ou baixar um certificado preexistente.

Se nenhum dos seus certificados de envio por push do MDM estiver perto de expirar, você não precisará fazer nada. Se você tiver um certificado de envio por push do MDM que está perto de expirar, entre em contato com seu provedor de soluções de MDM. Em seguida, faça com que o seu iOS Developer Program Agent faça login no Apple Push Certificate Portal com o seu ID Apple.

Todos os novos certificados de envio por push do MDM devem ser criados no Apple Push Certificate Portal. O iOS Developer Program Enterprise não permitirá mais a criação de um ID de Aplicativo com um Identificador de Pacote (tópico de APNs) que contém com.apple.mgmt.

Nota: você deve rastrear o ID Apple usado para criar o certificado. Além disso, o ID Apple deve ser um ID corporativo, e não um ID pessoal.

Para criar uma CSR usando o Microsoft IIS

A primeira etapa para gerar uma solicitação de certificado de APNs para dispositivos iOS é criar uma Solicitação de Assinatura de Certificado (CSR). Em um Windows 2012 R2 ou Windows 2008 R2 Server, você pode gerar 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, **2048** como o comprimento de bit e, em seguida, clique em **Avançar**.
6. Insira um nome de arquivo, especifique uma localização para salvar a CSR e clique em **Concluir**.

Para criar uma CSR em um computador Mac

1. Em um computador Mac que executa o macOS, em **Aplicativos** > **Utilitários**, inicie o aplicativo Keychain Access.
2. Abra o menu de **Keychain Access** e clique em **Preferences**.
3. Clique na guia **Certificates**, altere as opções **OCSP** e **CRL** para **Off** e feche a janela Preferences.
4. No menu de **Keychain Access**, clique em **Certificate Assistant** > **Request a Certificate From a Certificate Authority**.
5. O Certificate Assistant solicita que você insira as seguintes informações:
    1. **Endereço de email**. O endereço de email do indivíduo ou da conta de função responsável por gerenciar o certificado.
    2. **Nome comum**. O nome comum do indivíduo ou da conta de função responsável por gerenciar o certificado.
    3. **Endereço de email da CA**. O endereço de email da Certificate Authority.
6. Selecione as opções **Saved to disk** e **Let me specify key pair information** e clique em **Continue**.
7. Insira um nome para o arquivo da CSR, salve o arquivo no seu computador e clique em **Save**.
8. Especifique as informações de par de chaves selecionando um **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.
9. Clique em **Done** quando o Certificate Assistant concluir o processo da CSR.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para criar uma CSR usando o OpenSSL

Se você não puder usar um Windows 2012 R2 ou um Windows 2008 R2 Server e os Serviços de Informações da Internet (IIS) da Microsoft ou um computador Mac para gerar uma Solicitação de Assinatura de Certificado (CSR) para enviar para o certificado do serviço de Notificação por Push da Apple (APNs), você poderá usar o OpenSSL.

Nota: para usar o OpenSSL para criar uma CSR, você precisa primeiro baixar e instalar o OpenSSL no site do OpenSSL.

1. No computador no qual você instalou o OpenSSL, execute o seguinte comando de um prompt de comando ou 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.
   Você está prestes a ser solicitado a inserir informações que serão incorporadas
   na sua solicitação de certificado.
   O que você está prestes a inserir é chamado de Nome diferenciado, ou DN.
   Há muitos campos, mas você pode deixar alguns em branco
   Para alguns campos, haverá um valor padrão,
   Se você inserir '.', o campo será deixado em branco.

   Nome do país (código de 2 letras) [AU]:US
   Nome do estado (nome completo) [Algum estado]:CA
   Nome da localidade (ex: cidade) []:RWC
   Nome da organização (ex: empresa) [Internet Widgits Pty Ltd]:Cliente
   Nome da unidade organizacional (ex: seção) []:Marketing
   Nome comum (ex: SEU nome []:John Doe
   Endereço de email []:john.doe@customer.com

3. Na mensagem seguinte, insira uma senha para a chave privada da CSR.
   Insira os seguintes atributos 'extras'
   a serem enviados com a sua solicitação de certificado
   Um desafio de senha []:
   Um nome de empresa opcional []:

4. Envie a CSR resultante para a Citrix.

A Citrix prepara a CSR assinada e retorna o arquivo para você por email.

Para assinar a CSR

Antes de enviar o certificado para a Apple, ele precisa ser assinado pela Citrix para que possa ser usado com o XenMobile.

1. No seu navegador, acesse o site XenMobile APNs CSR Signing.
2. Clique em **Upload the CSR**.
3. Procure e selecione o certificado.
   Nota: o certificado deve estar no formato .pem/txt.

4. Na página XenMobile APNs CSR Signing, clique em **Sign**. A CSR é assinada e salva automaticamente na sua pasta configurada de downloads.

Para enviar a CSR assinada para a Apple para obter o certificado de APNs

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

Depois de receber a sua Solicitação de Assinatura de Certificado (CSR) assinada da Citrix, você precisará enviá-la para a Apple para obter o certificado de APNs.

Nota: alguns usuários relataram problemas ao fazer login no Apple Push Portal. Como alternativa, você pode fazer login no Apple Developer Portal (http://developer.apple.com/devcenter/ios/index.action) antes de seguir o link para identity.apple.com na Etapa 1.

1. Em um navegador, acesse https://identity.apple.com/pushcert.
2. Clique em **Create a Certificate**.
3. Se esta for a primeira vez 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 deve ser exibida para informar que o carregamento foi bem-sucedido.
5. Clique em **Download** para recuperar o certificado .pem.
   Nota: se você estiver usando o Internet Explorer e a extensão do arquivo estiver ausente, clique em **Cancel** duas vezes e baixe da janela seguinte.

Para criar um certificado de APNs .pfx usando o Microsoft IIS

Para usar o certificado de APNs da Apple com o XenMobile, você precisa concluir a solicitação de certificado no Microsoft IIS, exportar o certificado como um arquivo de PCKS #12 (.pfx) e importar o certificado de APNs para o XenMobile.

Importante: você precisa usar para essa tarefa o mesmo servidor IIS que 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 uma localização e um nome do arquivo para o certificado .pfx, além de uma senha e clique em **OK**.
   Nota: você precisará da senha do certificado durante a instalação do XenMobile.
7. Copie o certificado .pfx para o servidor no qual o XenMobile será instalado.
8. Faça logon no console XenMobile como um administrador.
9. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.
10. Clique em **Certificados**. A página **Certificados** é exibida.
11. Clique em **Importar**. A caixa de diálogo **Importar** é exibida.
12. No menu **Importar**, escolha **Keystore**.
13. Em **Usar como**, escolha **APNs**.
14. No arquivo **Keystore** , selecione o arquivo de keystore a ser importado clicando em **Procurar** e navegando até a localização do arquivo.
15. Em **Senha**, digite a senha atribuída ao certificado.
16. Clique em **Importar**.

Para criar um certificado de APNs .pfx em um computador Mac

1. No mesmo computador Mac que executa o macOS que você usou para gerar a CSR, localize o certificado de Identidade de produção (PEM) que você recebeu da Apple.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

2. Clique duas vezes no arquivo de certificado para importá-lo para as chaves.
3. Se você for solicitado a adicionar o certificado a chaves específicas, mantenha as chaves de login padrão selecionado e clique em **OK**. O certificado recém-adicionado será exibido na sua lista de certificados.
4. Clique no certificado e, no menu **File**, clique em **Export** para iniciar a exportação do certificado em um certificado PCKS #12 (.pfx).
5. Dê ao arquivo de certificado um nome exclusivo para uso com o XenMobile Server. 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. Insira a senha e clique em **OK**. O certificado salvo agora está pronto para ser usado com o servidor XenMobile.
   Nota: se você não pretende manter e preservar o computador e a conta de usuário que usou originalmente para gerar a CSR e concluir o processo de exportação de certificado, a Citrix recomenda salvar ou exportar as Chaves Pública e Pessoal do sistema local. Caso contrário, o acesso aos certificados de APNs para reutilização será anulado e você precisará repetir todo o processo da CSR e APNs.

Para criar um certificado de APNs .pfx usando o OpenSSL

Depois de usar o OpenSSL para criar uma Solicitação de Assinatura de Certificado (CSR), você também poderá usar o OpenSSL para criar um certificado de APNs .pfx.

1. Em um prompt de comando ou shell, execute o comando a seguir.
   openssl pkcs12 -export -in MDM_Zenprise_Certificate.pem -inkey Customer.key.pem -out apns_identity.p12

2. Insira uma senha para o arquivo de certificado .pfx. Guarde essa senha, pois você precisará usá-la novamente quando enviar o certificado para o XenMobile.
3. Anote a localização do arquivo de certificado .pfx e copie o arquivo para o servidor XenMobile para que você possa usar o console XenMobile para carregar o arquivo.

Para importar um certificado de APNs para o XenMobile

Depois de solicitar e receber um 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 no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.
2. Clique em **Certificados**. A página **Certificados** é exibida.
3. Clique em **Importar**. A caixa de diálogo **Importar** é exibida.
4. No menu **Importar**, escolha **Keystore**.
5. Em **Usar como**, escolha **APNs**.
6. Navegue até o arquivo .p12 no seu computador.
7. Insira uma senha e clique em **Importar**.

Para obter mais informações sobre certificados, consulte Certificados.

Para renovar um certificado de APNs

Para renovar um certificado de APNs, você precisa realizar as mesmas etapas que usaria para criar um novo certificado. Em seguida, visite o Apple Push Certificates Portal e carregue o novo certificado. Depois de fazer login, você vê o seu certificado existente ou pode ver um certificado que foi importado da sua conta anterior do Apple Developers. No

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Certificates Portal, a única diferença durante a renovação do certificado é que você clica em **Renew**. Você deve ter uma conta de desenvolvedor no Certificates Portal para acessar o site. Quando renovar seu certificado, lembre-se de usar o mesmo nome da organização e ID Apple.

Nota: para determinar quando o certificado de APNs expira, no console XenMobile, clique em **Configurar** > **Configurações** > **Certificados**. No entanto, se o certificado tiver expirado, não o revogue.

1. Gere um CSR usando o IIS (Microsoft), o OpenSSL ou o Keychain Access (MacOS).
2. No site XenMobile APNs CSR Signing, selecione **Solicitar assinatura de certificado de notificação por push**.
3. Clique em **+ Upload the CSR**. Em seguida, na caixa de diálogo, navegue até o CSR, clique em **Abrir** e clique em **Login**.
4. Quando você receber um arquivo .plist, salve-o.
5. Clique em **Apple Push Certificates Portal** e faça logon.
6. Selecione o certificado que deseja renovar e clique em **Renovar**.
7. Carregue o arquivo .plist. Você deve receber um arquivo .pem como resultado. Salve o arquivo .pem.
8. Usando esse arquivo .pem, preencha o CSR (de acordo com o método usado para criar o CSR na Etapa 1).
9. Exporte o certificado como um arquivo .pfx.

No console XenMobile, importe o arquivo .pdx e conclua a configuração da seguinte maneira:

1. Vá para **Configurações > Gerenciamento de certificados**.
2. Na página **Certificados**, clique em **Importar**.
3. No **menu Importar**, escolha **Keystore**.
4. No **Tipo de Keystore**, escolha **PKCS#12.**
5. Em **Usar como**, escolha **APNs**.
6. Em **Arquivo de keystore**, clique em **Procurar** e navegue até o arquivo.
7. Em **Senha**, digite a senha do certificado.
8. Digite uma **Descrição** opcional.
9. Clique em **Importar**.

   O XenMobile redireciona você de volta à página **Certificados**. Os campos **Nome**, **Status**, **Válido de** e **Válido até** são atualizados.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

SAML para login único com ShareFile

Feb 21, 2018

Você pode configurar o XenMobile e o ShareFile para usar a SAML (Security Assertion Markup Language) para fornecer acesso via logon único (SSO) a aplicativos do ShareFile Mobile. Essa funcionalidade inclui aplicativos do ShareFile preparados com o MDX Toolkit e clientes ShareFile não preparados, como o site da Web, o plug-in do Outlook ou os clientes de sincronização.

- **Para aplicativos do ShareFile preparados**. Os usuários que fazem login no ShareFile por meio do aplicativo móvel do ShareFile 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 ShareFile envia o token SAML para o ShareFile. Após o logon inicial, os usuários podem acessar o aplicativo móvel do ShareFile por meio de SSO. Eles também podem anexar documentos do ShareFile a emails do Secure Mail sem fazer login todas as vezes.
- **Para clientes ShareFile não preparados**. Os usuários que fazem login no ShareFile usando um navegador da Web ou outro cliente ShareFile são redirecionados para o XenMobile para autenticação do usuário e para obter um token SAML. Após a autenticação bem-sucedida, o token SAML é enviado para o ShareFile. Após o login inicial, os usuários podem acessar os clientes ShareFile por meio de SSO sem fazer login toda vez.

Para usar o XenMobile como um provedor de identidade de SAML (IdP) para o ShareFile, você deve configurar o XenMobile para usar o ShareFile Enterprise, conforme descrito neste artigo. Como alternativa, você pode configurar o XenMobile para funcionar apenas com os StorageZone Connectors. Para obter mais informações, consulte Uso do ShareFile com o XenMobile.

Para obter um diagrama detalhado da arquitetura de referência, consulte o artigo do XenMobile Deployment Handbook, Reference Architecture for On-Premises Deployments.

Pré-requisitos

Conclua os pré-requisitos antes de configurar o SSO com aplicativos XenMobile e ShareFile:

- O MDX Service ou uma versão compatível do MDX Toolkit (para aplicativos do ShareFile Mobile).

  Para obter detalhes, consulte Compatibilidade com o XenMobile.

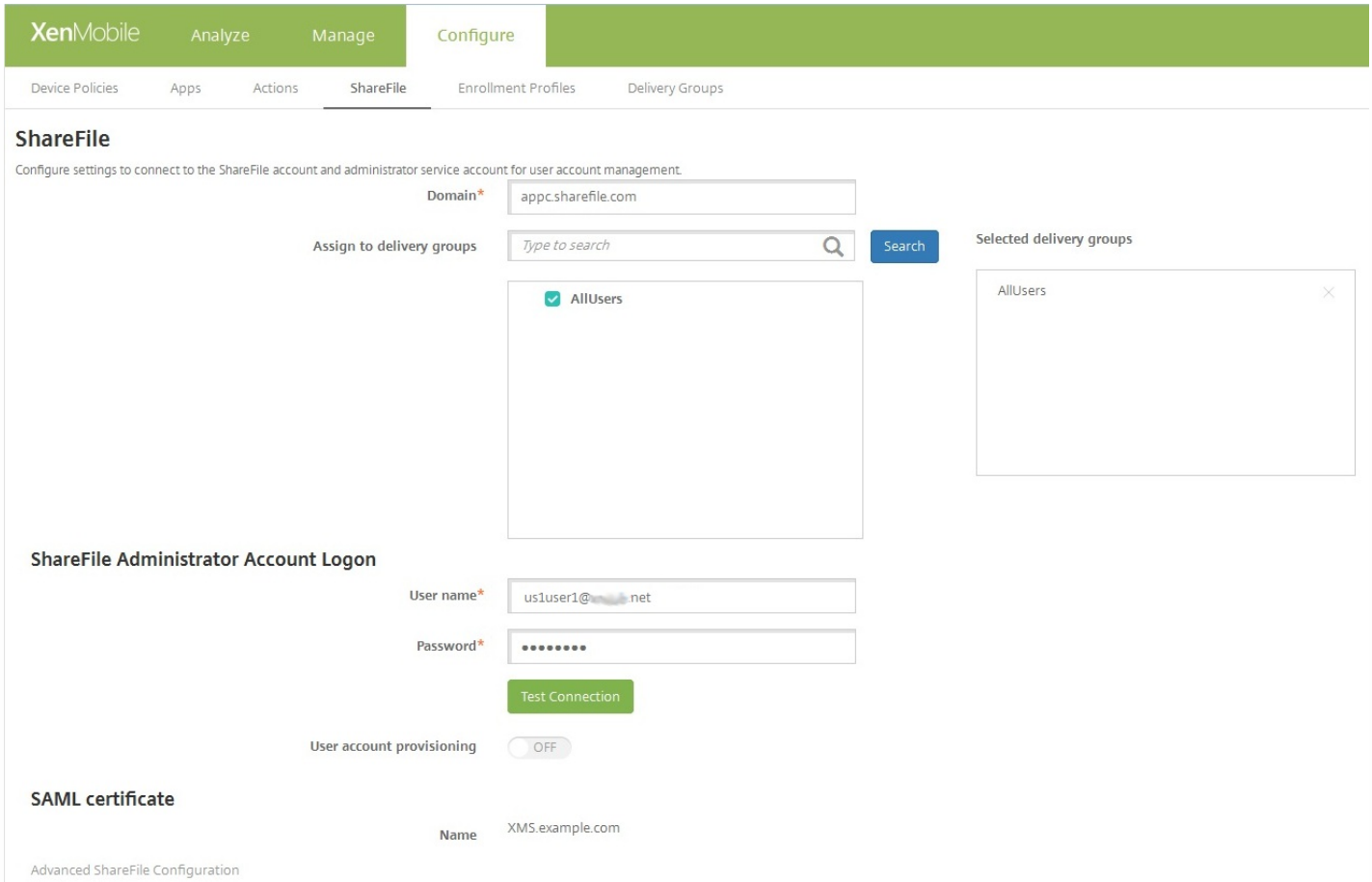
- Uma versão compatível de aplicativos do ShareFile Mobile e do Secure Hub.
- Conta de administrador do ShareFile.
- Conectividade verificada entre o XenMobile e o ShareFile.

Configurar o acesso ao ShareFile

Antes de configurar SAML para ShareFile, forneça as informações de acesso ao ShareFile da seguinte maneira:

1. No console da Web do XenMobile, clique em **Configurar > ShareFile**. A página de configuração do **ShareFile** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Defina estas configurações:

- **Domínio**: digite seu nome de subdomínio do ShareFile; por exemplo, exemplo.sharefile.com.
- **Atribuir a grupos de entrega**: selecione ou pesquise os grupos de entrega nos quais você deseja usar o SSO com o ShareFile.
- **Login de conta de administrador do ShareFile**
  - **Nome de usuário**: digite o nome de usuário do administrador do ShareFile. Esse usuário deve ter privilégios de administrador.
  - **Senha**: digite a senha de administrador do ShareFile.
  - **Provisionamento de conta de usuário**: ative essa opção se você deseja permitir o provisionamento de usuários no XenMobile; deixe-a desativada se planeja usar a ShareFile User Management Tool para provisionamento de usuários.

    Nota: se um usuário sem uma conta do ShareFile for incluído nas funções selecionadas, o XenMobile provisionará automaticamente uma conta do ShareFile para que você ative o provisionamento de conta de usuário. A Citrix recomenda que você use uma função com uma pequena associação para testar a configuração. Isso evita a presença de um grande número de usuários sem contas do ShareFile.

3. Clique em **Testar conexão** para verificar se o nome de usuário e a senha para a conta de administrador do ShareFile autenticam a conta especificada do ShareFile.

4. Clique em **Salvar**. O XenMobile sincroniza com o ShareFile e atualiza as configurações do ShareFile **Emissor de ShareFile / ID de entidade** e **URL de Login**.

Configurar SAML para aplicativos ShareFile MDX preparados

As etapas a seguir se aplicam aos aplicativos e dispositivos iOS e Android.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Com o MDX Toolkit, prepare o aplicativo do ShareFile Mobile. 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 preparado do ShareFile Mobile. Para obter informações sobre como carregar aplicativos MDX, consulte Para adicionar um aplicativo MDX ao XenMobile.

3. Verifique as configurações de SAML, fazendo login no ShareFile com o nome de usuário e a senha do administrador que você configurou acima.

4. Verifique se o ShareFile e o XenMobile estão configurados para o mesmo fuso horário.

Nota: verifique se o XenMobile mostra a hora correta com relação ao fuso horário configurado. Caso contrário, poderá ocorrer falha de SSO.

Validar o aplicativo móvel do ShareFile

1. No dispositivo do usuário, caso ainda não tenha sido feito, instale e configure o Secure Hub.

2. Na XenMobile Store, baixe e instale o aplicativo do ShareFile Mobile.

3. Inicie o aplicativo do ShareFile Mobile. O ShareFile é iniciado sem a necessidade de informar o nome do usuário ou a 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 ShareFile**. Os arquivos disponíveis para serem anexados ao email são mostrados sem a necessidade de informar nome do usuário ou senha.

Configurar o NetScaler Gateway para outros clientes do ShareFile

Se você desejar configurar o acesso aos clientes do ShareFile não preparados, como site da Web, plug-in do Outlook ou clientes de sincronização, você deve configurar o NetScaler Gateway para dar suporte ao uso do XenMobile como um provedor de identidade SAML da seguinte maneira:

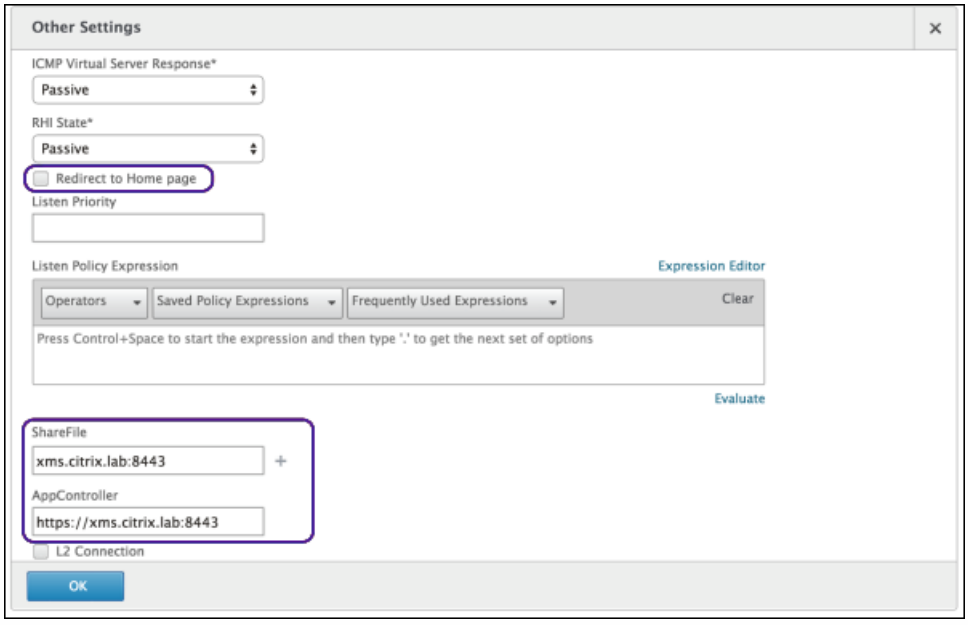
- Desative o redirecionamento de página inicial.
- Crie uma política de sessão e um perfil do ShareFile.
- Configure políticas no servidor virtual do NetScaler Gateway.

Desative o redirecionamento de página inicial

Você deve desativar o comportamento padrão das solicitações que chegam por meio do caminho /cginfra para que o usuário veja a URL interna solicitada originalmente em vez da página inicial configurada.

1. Edite as configurações do servidor virtual do NetScaler Gateway usado para logins no XenMobile. No NetScaler 10.5, acesse **Other Settings** e desmarque a caixa de seleção **Redirect to Home Page**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Em **ShareFile**, digite o nome e o número da porta do servidor interno do XenMobile.

3. Em **AppController**, digite seu URL do XenMobile.

Essa configuração autoriza as solicitações da URL inserida por meio do caminho /cginfra.

Criar uma política de sessão e um perfil de solicitação do ShareFile

Defina estas configurações para criar uma política de sessão e um perfil de solicitação do ShareFile:

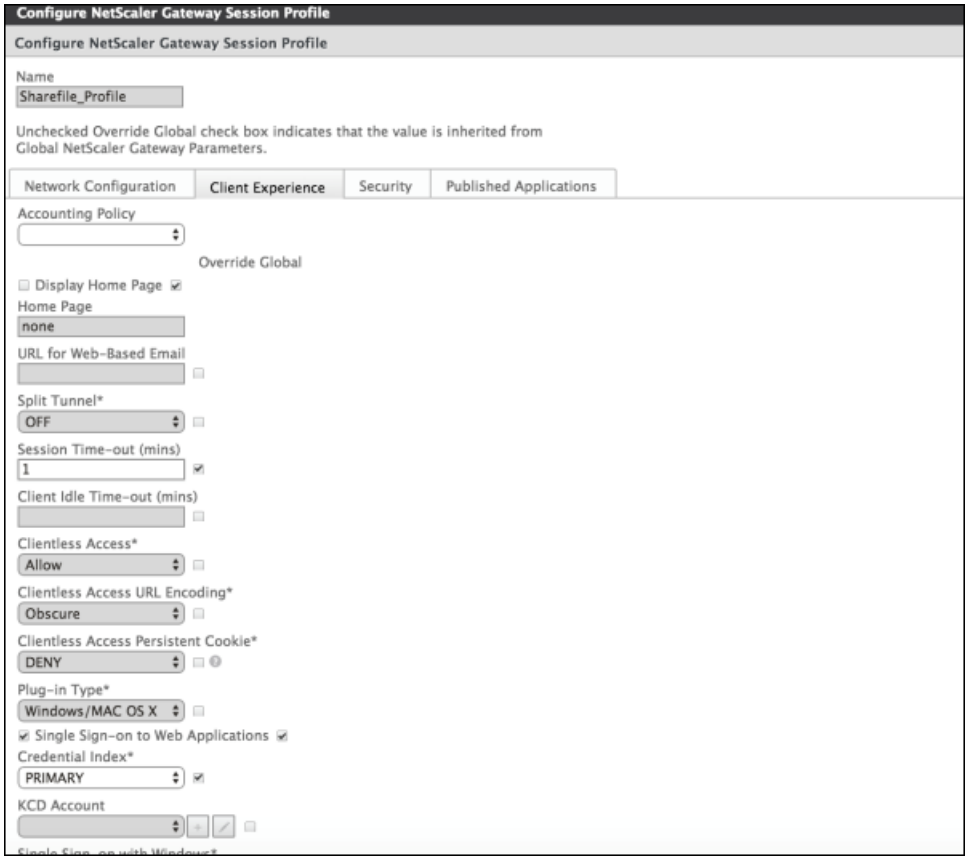
1. No utilitário de configuração do NetScaler Gateway, no painel de navegação esquerdo, clique em **NetScaler Gateway > Policies > Session**.

2. Crie uma nova política de sessão. Na guia **Policies**, clique em **Add**.

3. No campo **Nome**, digite **ShareFile_Policy**.

4. Crie uma nova ação clicando no botão **+**. A página **Create NetScaler Gateway Session Profile** é exibida.

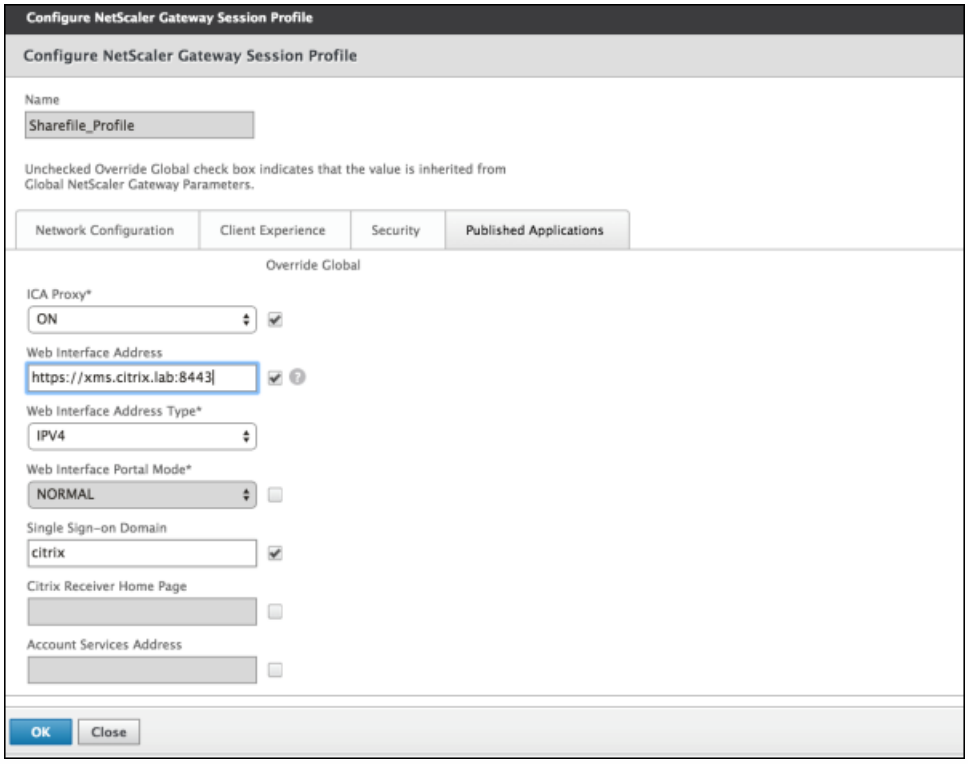
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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**: na lista, clique em PRIMARY.
- Clique na guia **Published Applications**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



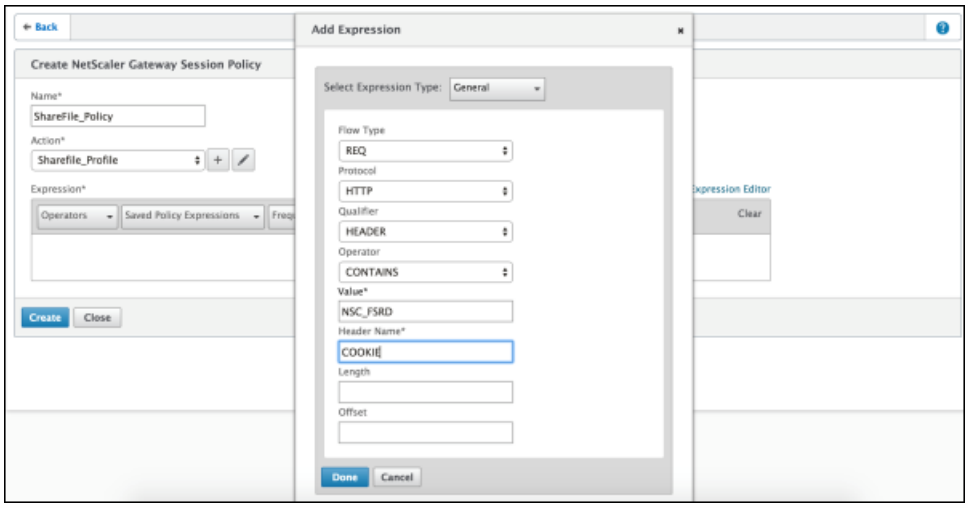
Defina estas configurações:

- **ICA Proxy**: na lista, clique em **ON**.
- **Web Interface Address**: digite o URL do XenMobile Server.
- **Single Sign-on Domain**: digite o nome do domínio do Active Directory.

  Nota: durante a configuração do NetScaler 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Clique em **Done**.

7. Clique em **Create** e em **Close**.

Configure políticas no servidor virtual do NetScaler Gateway

Defina estas configurações no servidor virtual do NetScaler Gateway.

1. No utilitário de configuração do NetScaler Gateway, no painel de navegação esquerdo, clique em **NetScaler Gateway > Virtual Servers**.

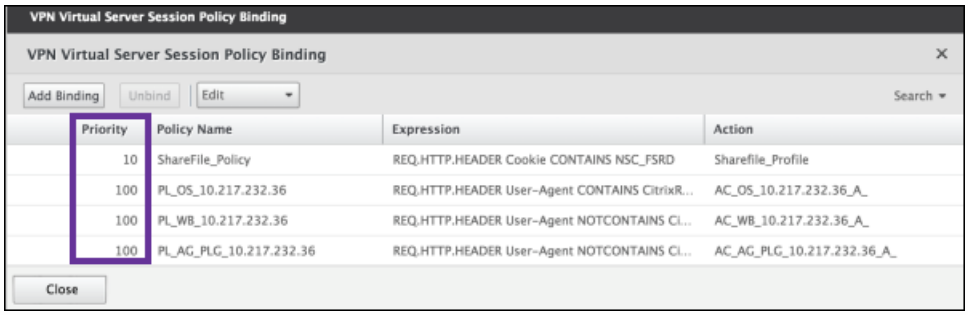
2. No painel **Details**, clique em seu servidor virtual do NetScaler Gateway.

3. Clique em **Editar**.

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, como mostrado na figura abaixo.



7. Clique em **Done** e salve a configuração do NetScaler em execução.

Configurar SAML para aplicativos ShareFile não MDX

Use as etapas abaixo para encontrar o nome do aplicativo interno para sua configuração do ShareFile.

1. Faça login na ferramenta de administrador do XenMobile usando o URL **https://:4443/OCA/admin/**. Não se esqueça de inserir “OCA” em letras maiúsculas.

2. Na lista **Exibir**, clique em **Configuração**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Clique em **Aplicativos > Aplicativos** e observe o **Nome do aplicativo** com o **Nome de exibição** "ShareFile".

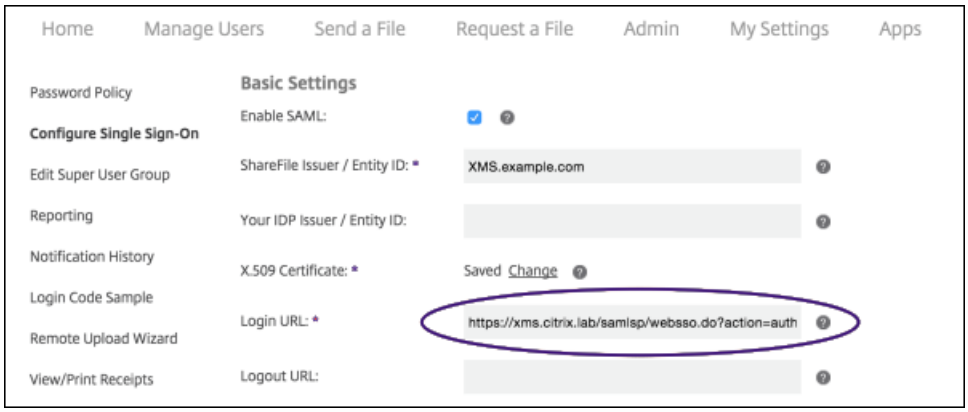
Modificar as configurações de SSO do ShareFile.com

1. Faça login em sua conta do ShareFile (https://.sharefile.com) como um administrador do ShareFile.

2. Na interface da Web do ShareFile, clique em **Administrador** e selecione **Configurar logon único**.

3. Edite o **URL de login** da seguinte maneira:

O **URL de login** deve ser parecido com: https://xms.citrix.lab/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML_SP&reqtype=1.



- Insira o FQDN externo do servidor virtual do NetScaler Gateway mais "/cginfra/https/" na frente do FQDN do servidor XenMobile e adicione "8443" após o FQDN do XenMobile.

  Agora, o URL deve ser semelhante a este:
  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 ShareFile interno da etapa 3 em SAML para

© 1999-2017 Citrix Systems, Inc. All rights reserved.

logon único com ShareFile. O nome interno é **ShareFile_SAML** por padrão; no entanto, toda vez que você altera sua configuração, um número é acrescentado ao nome interno (ShareFile_SAML_2, ShareFile_SAML_3 etc.).

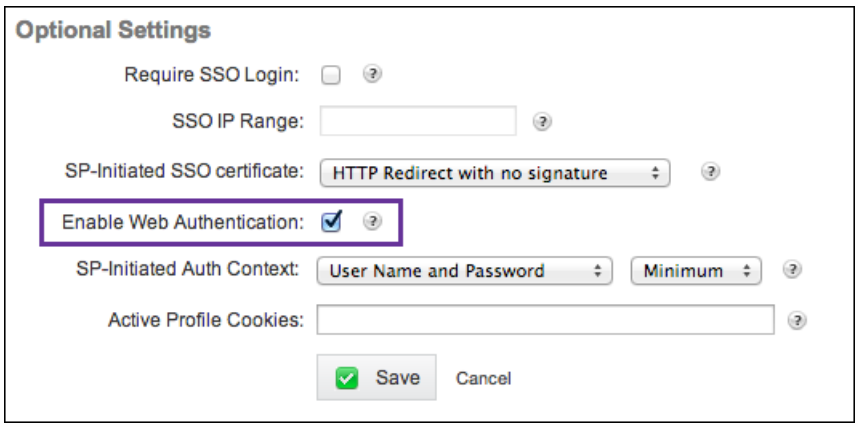
Agora, o URL deve ser semelhante a este:
https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser**r&app=ShareFile_SAML**&reqtype=1

- Adicione "&nssso=true" ao final da URL.

  Agora, o URL modificado deve ser semelhante a:
  https://nsgateway.acme.com/cginfra/https/xms.citrix.lab:8443/samlsp/websso.do?action=authenticateUser&app=ShareFile_SAML&reqtype=1**&nssso=true**.

  Importante: toda vez que você edita ou recria o aplicativo do ShareFile ou altera as configurações do ShareFile no console XenMobile, um novo número é acrescentado ao nome do aplicativo interno, o que significa que você deve também atualizar o URL de login no site do ShareFile para refletir o nome do aplicativo atualizado.

4. Em **Configurações opcionais**, marque a caixa de seleção **Ativar autenticação da Web**.



Validar a configuração

Siga os procedimentos a seguir para validar a configuração.

1. Aponte seu navegador para https://sharefile.com/saml/login.

Você será redirecionado para o formulário de logon do NetScaler Gateway. Se você não for redirecionado, verifique as definições de configuração anteriores.

2. Insira o nome do usuário e a senha do NetScaler Gateway e do ambiente do XenMobile configurado.

Suas pastas do ShareFile no .sharefile.com são exibidas. Se você não vir as pastas do ShareFile, verifique se inseriu as credenciais de login corretas.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurações do servidor do Active Directory do Microsoft Azure

Feb 21, 2018

Configurar o Azure Active Directory (AD) como seu provedor de identidade (IDP) permite que os usuários se registram 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.

Configure o Azure como 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 o NetScaler para autenticação, o NetScaler deverá 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 um nome de usuário e uma senha 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 Add your own domain name to Azure Active Directory.

2. Estenda seu diretório local para o Active Directory do Azure usando ferramentas de integração de diretório. Para obter detalhes, consulte Integração de diretório.

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**, selecione **Aplicativo MDM no local** e salve as configurações. Salve as configurações.
   Nota: escolha um aplicativo local mesmo ao se inscrever para o Citrix XenMobile Cloud, pois, na terminologia da Microsoft, qualquer aplicativo não que não seja de vários locatários 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 dio ID de aplicativo, da seguinte forma:
   • **URL de descoberta do MDM**: https://:8443/*instanceName*/wpe
   • **URL de termos de uso do MDM**: https://:8443/*instanceName*/wpe/tou
   • **URI do ID de aplicativo**: https://: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 para dispositivos Windows 10, consulte o artigo da Microsoft Azure Active Directory integration with MDM.

Configurar o AD do Azure como seu IDP

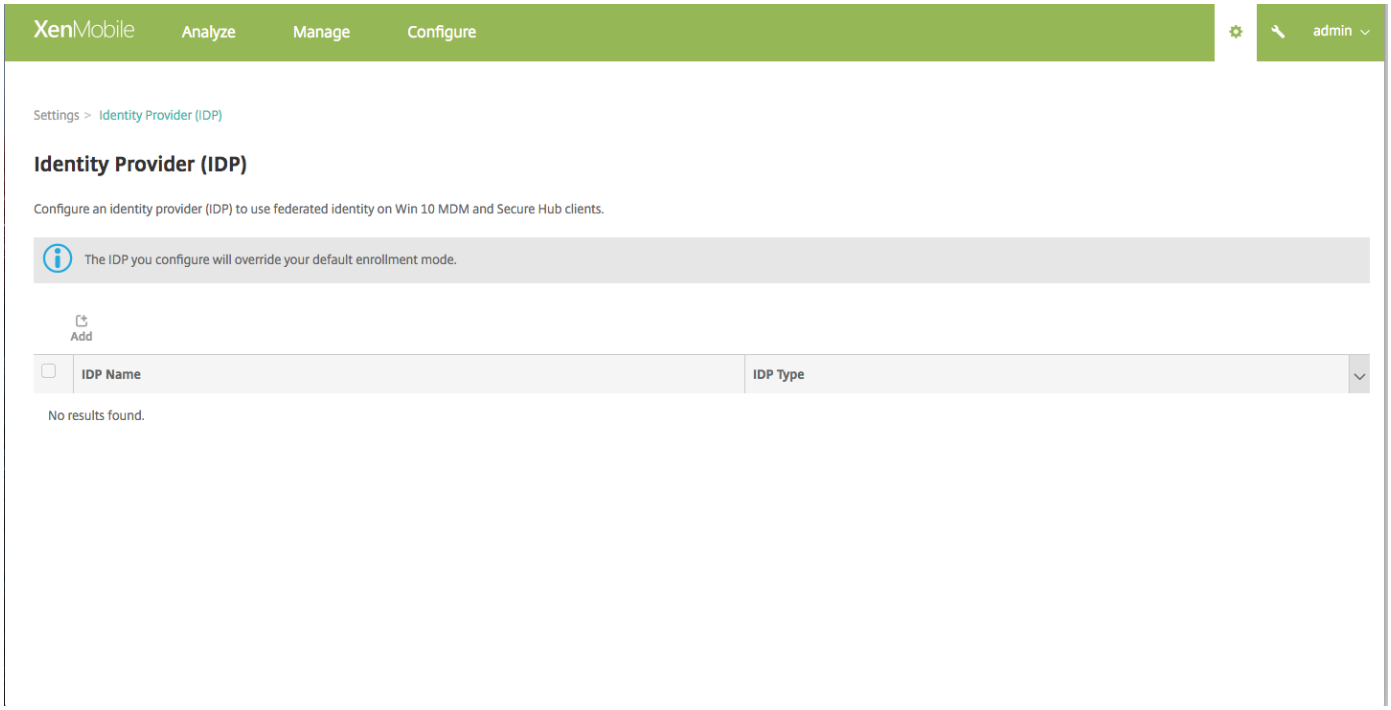
1. Localize ou anote as informações necessárias da sua conta do Azure:

   - 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 **Configurações** é exibida.

3. Em **Autenticação**, clique em **Provedor de identidade (IDP)**. A página **Provedor de identidade** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



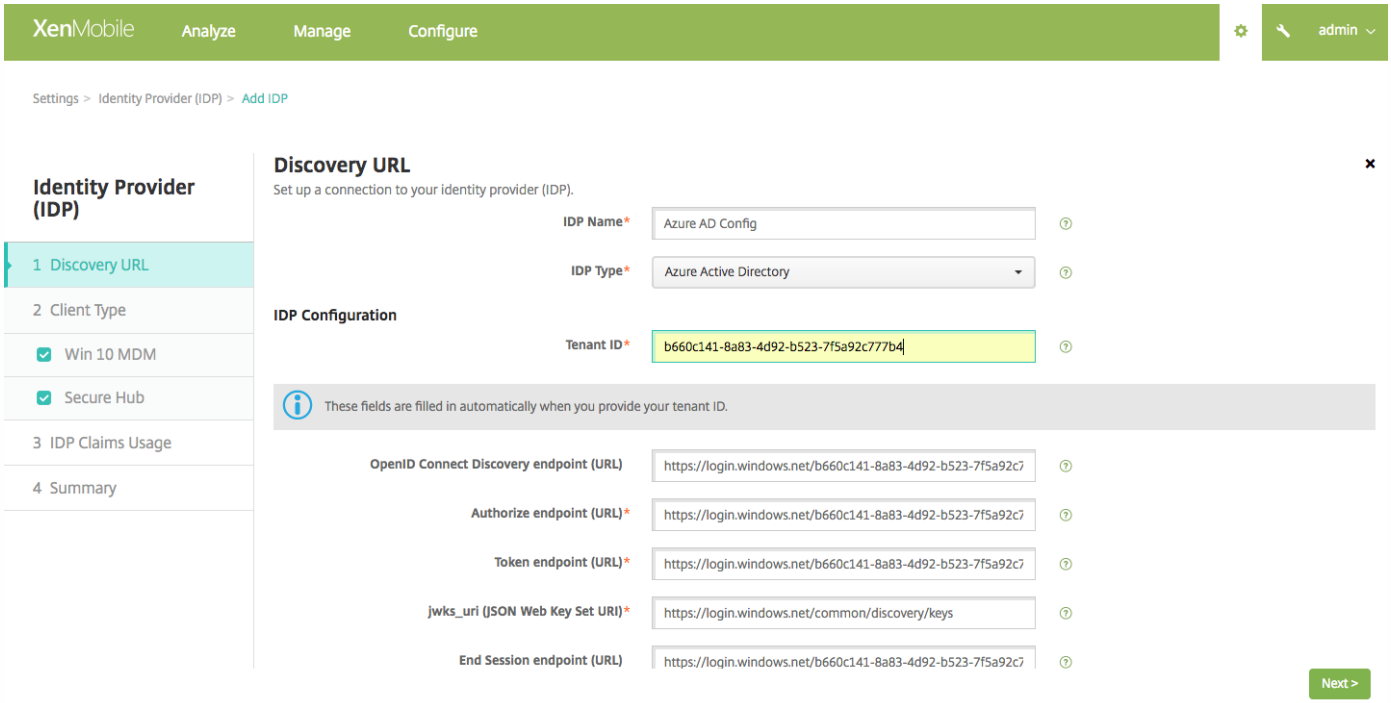
4. Clique em **Adicionar**. A página **Configuração do IDP** é exibida.

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.windowszaure.com/acmew.onmicrosoft.com#workspaces/ActiveDirectoryExtensin/Directory/abc213-abc123-abc123/onprem..., a ID de locatário é: abc123-abc123-abc123.

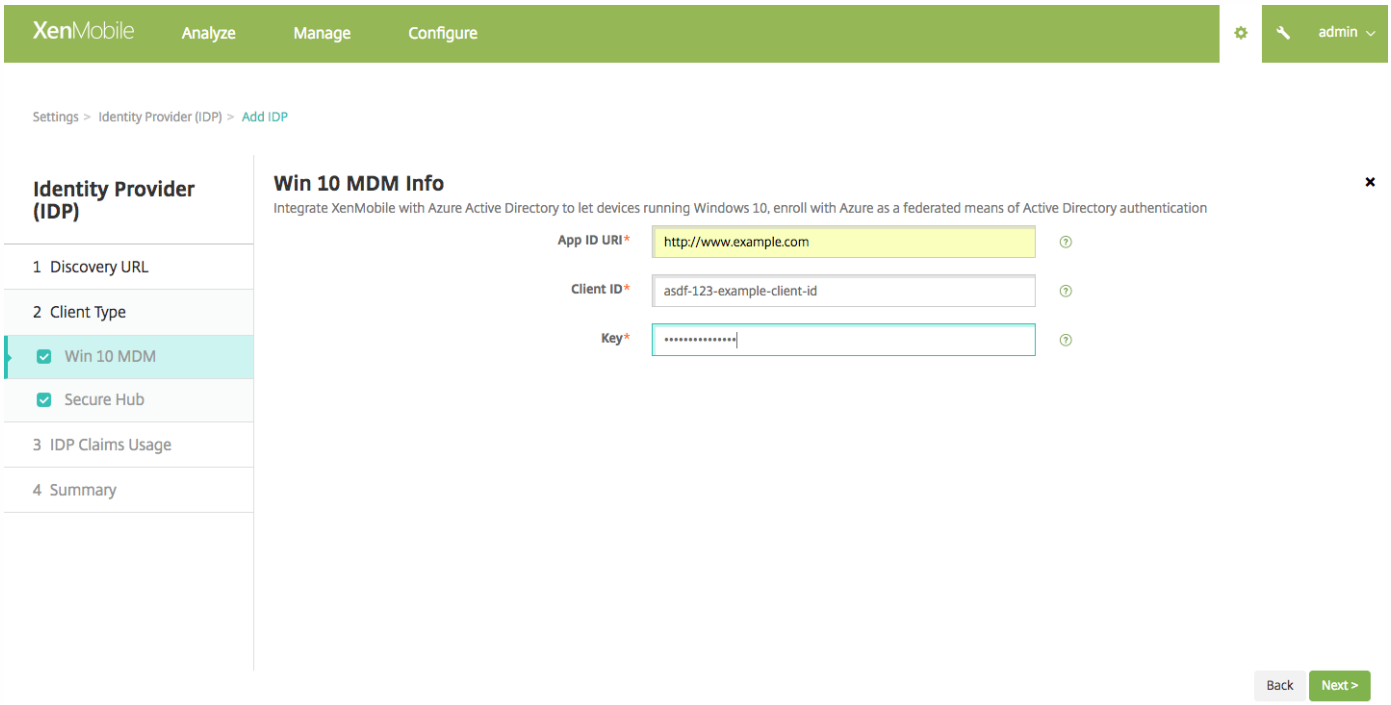
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.

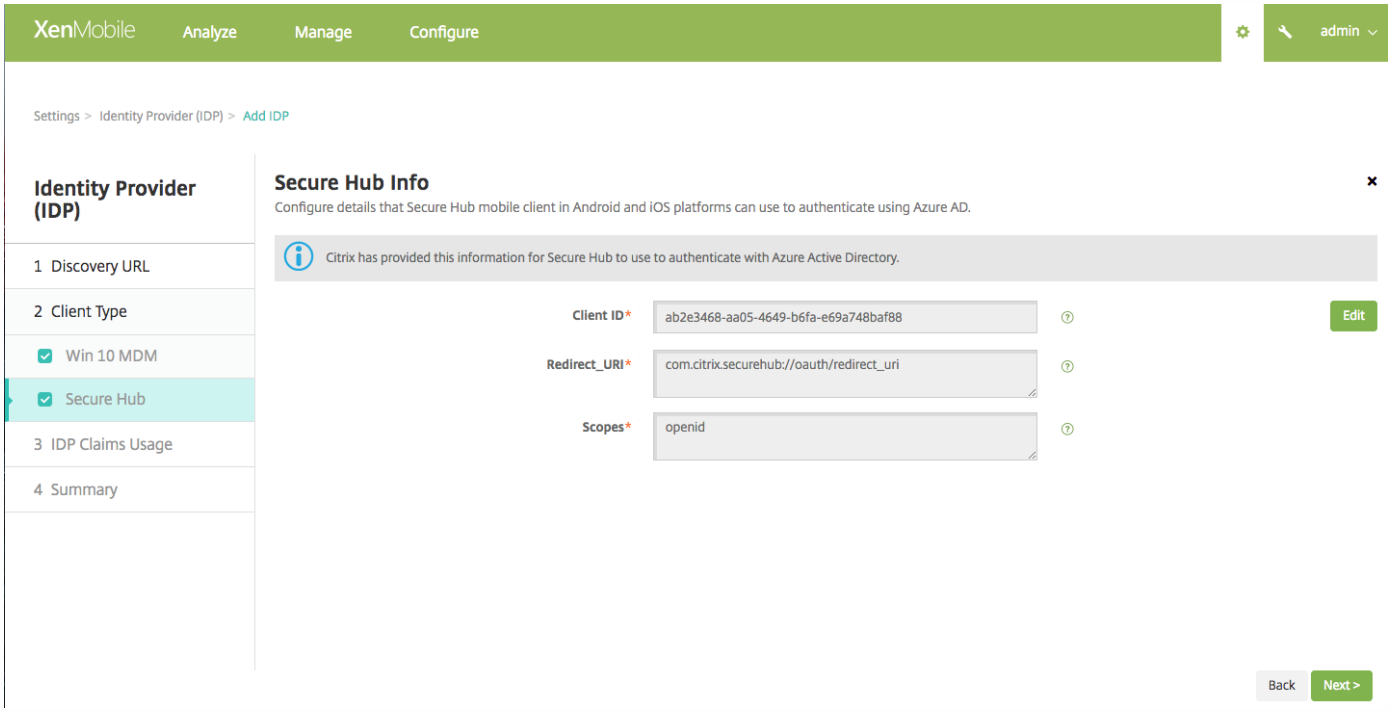


© 1999-2017 Citrix Systems, Inc. All rights reserved.

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**.

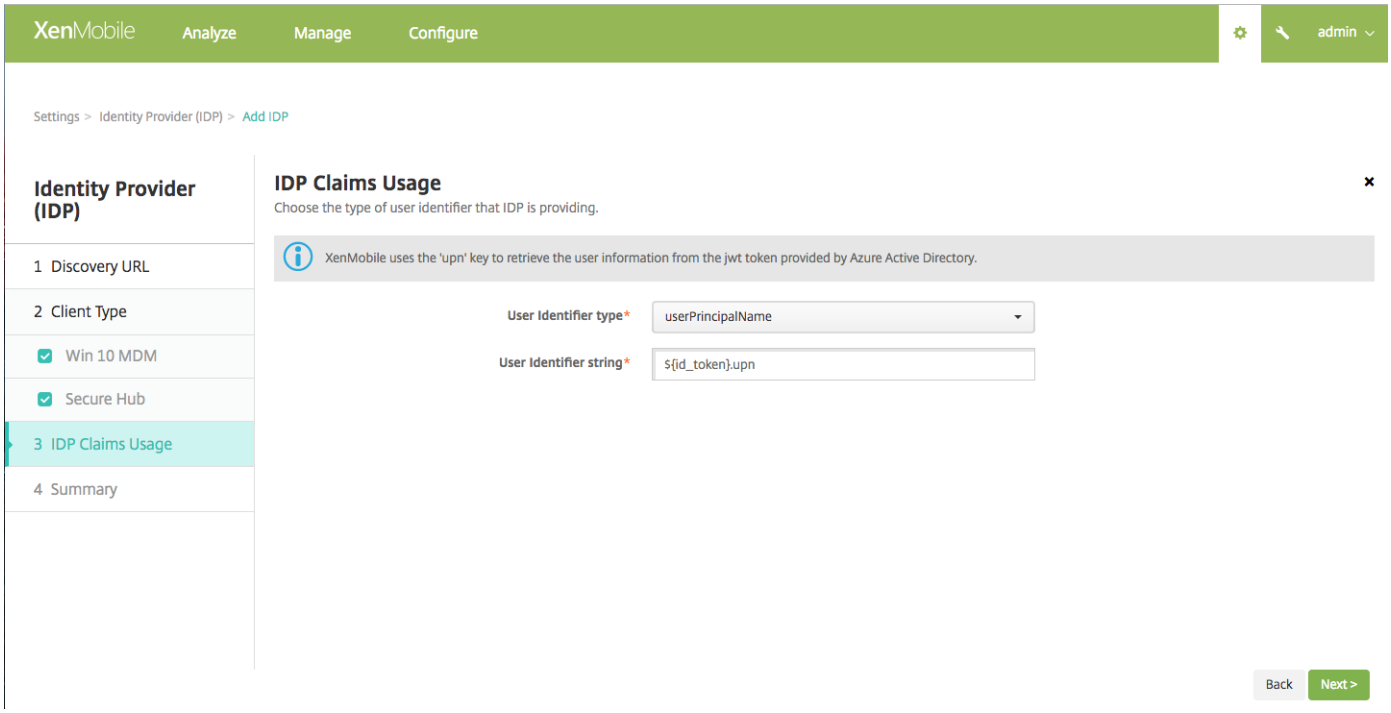


10. Configure o tipo de identificador de usuário fornecido pelo seu IDP:

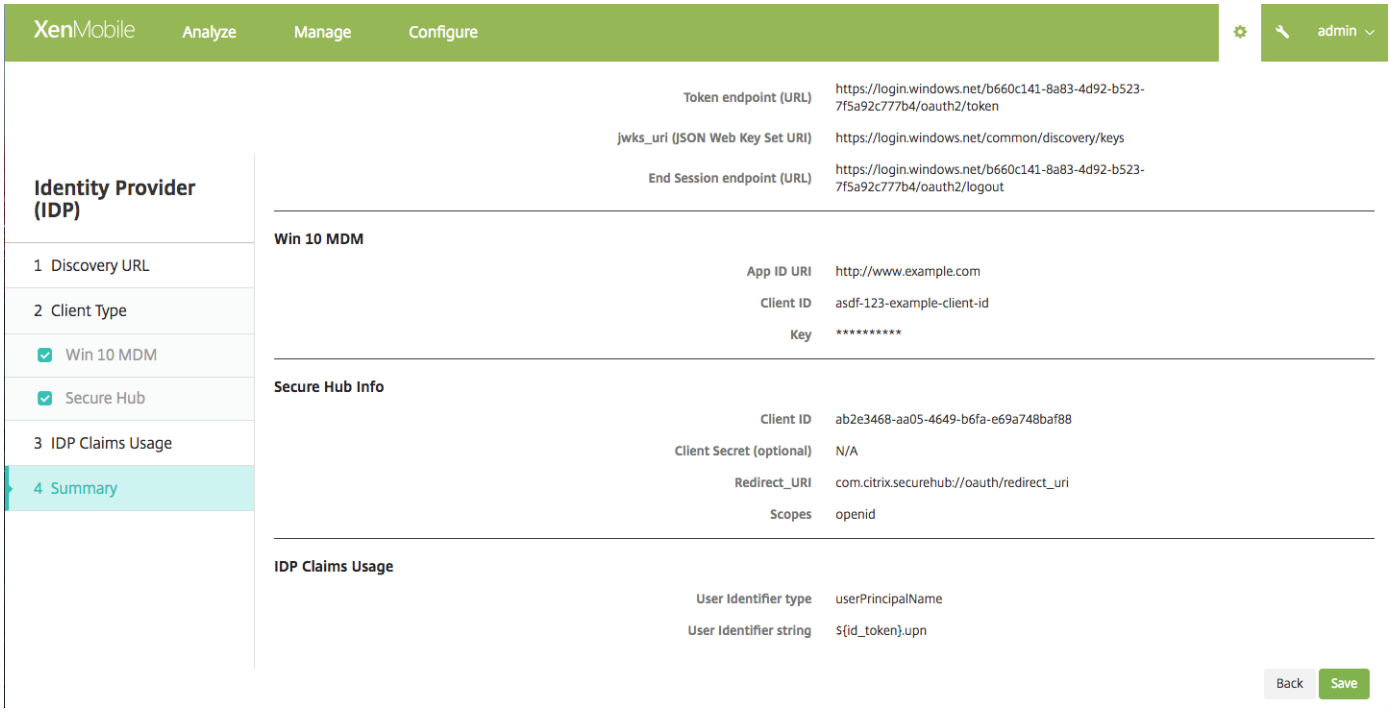
- **Tipo de identificador do usuário**: escolha **userPrincipalName** na lista suspensa.
- **Sequência de caracteres do identificador do usuário**: esse campo é preenchido automaticamente.

11. Clique em **Avançar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



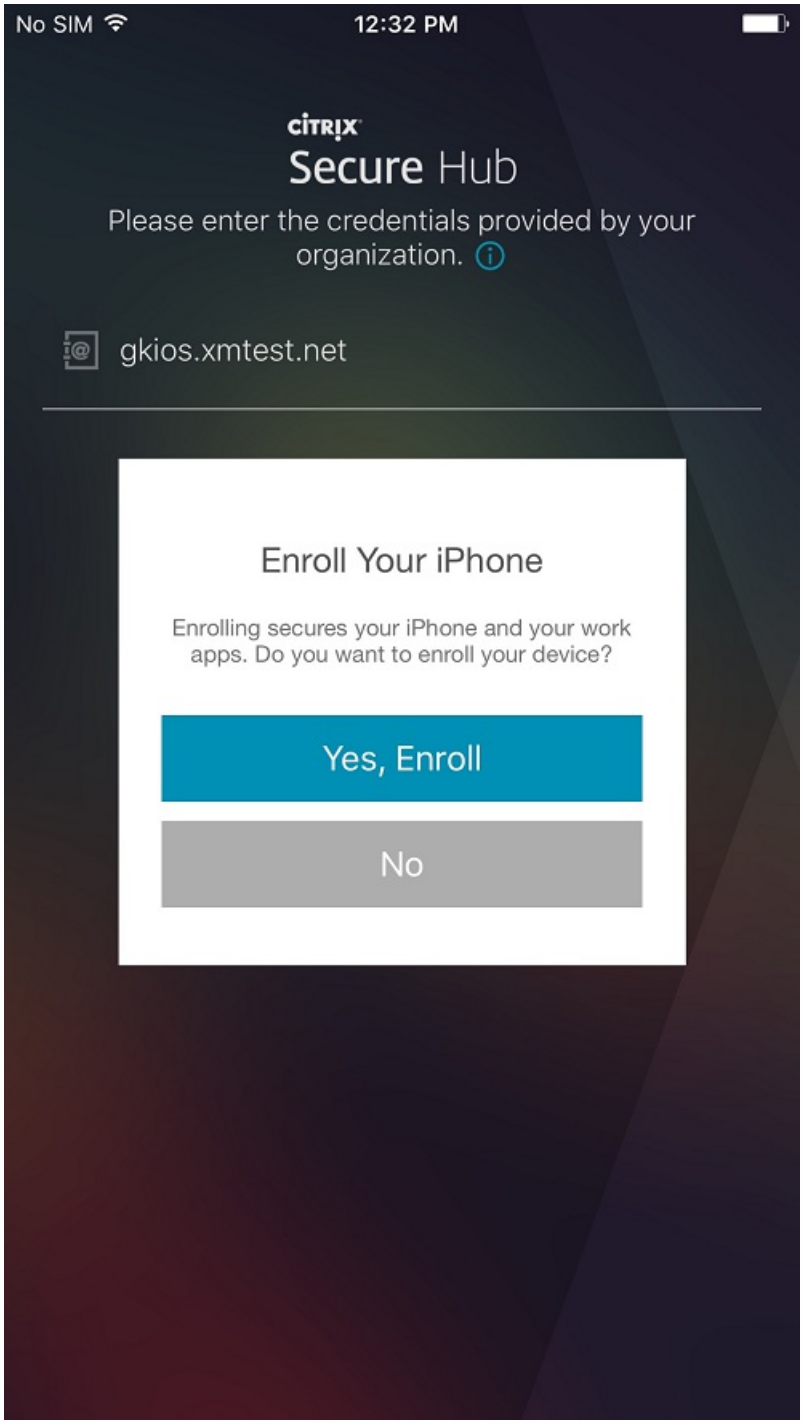
12.Reveja a página **Resumo** e clique em **Salvar**.



Experiência dos usuários

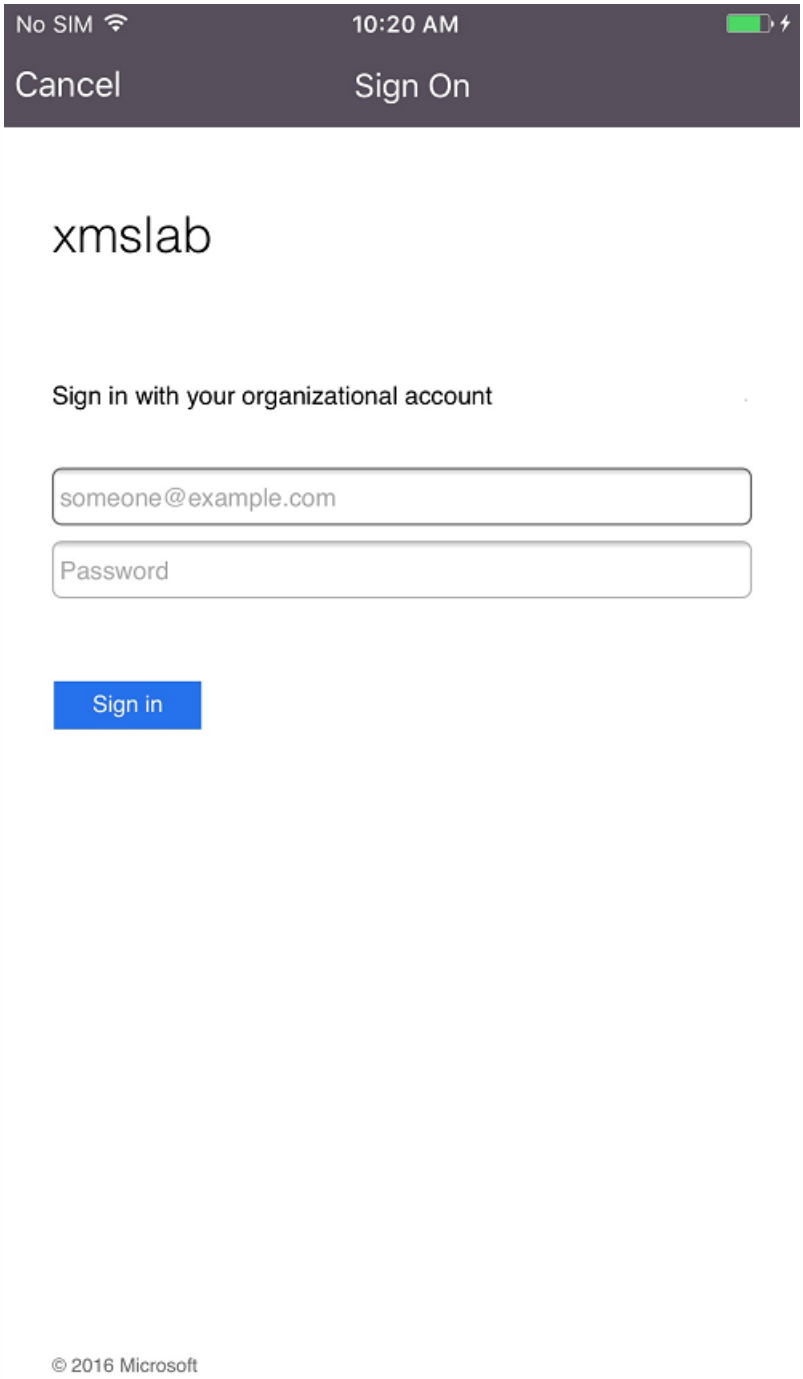
1. Os usuários iniciam o Secure Hub. Em seguida, eles inserem o nome de domínio totalmente qualificado (FQDN) do XenMobile Server, nome UPN ou endereço de email.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



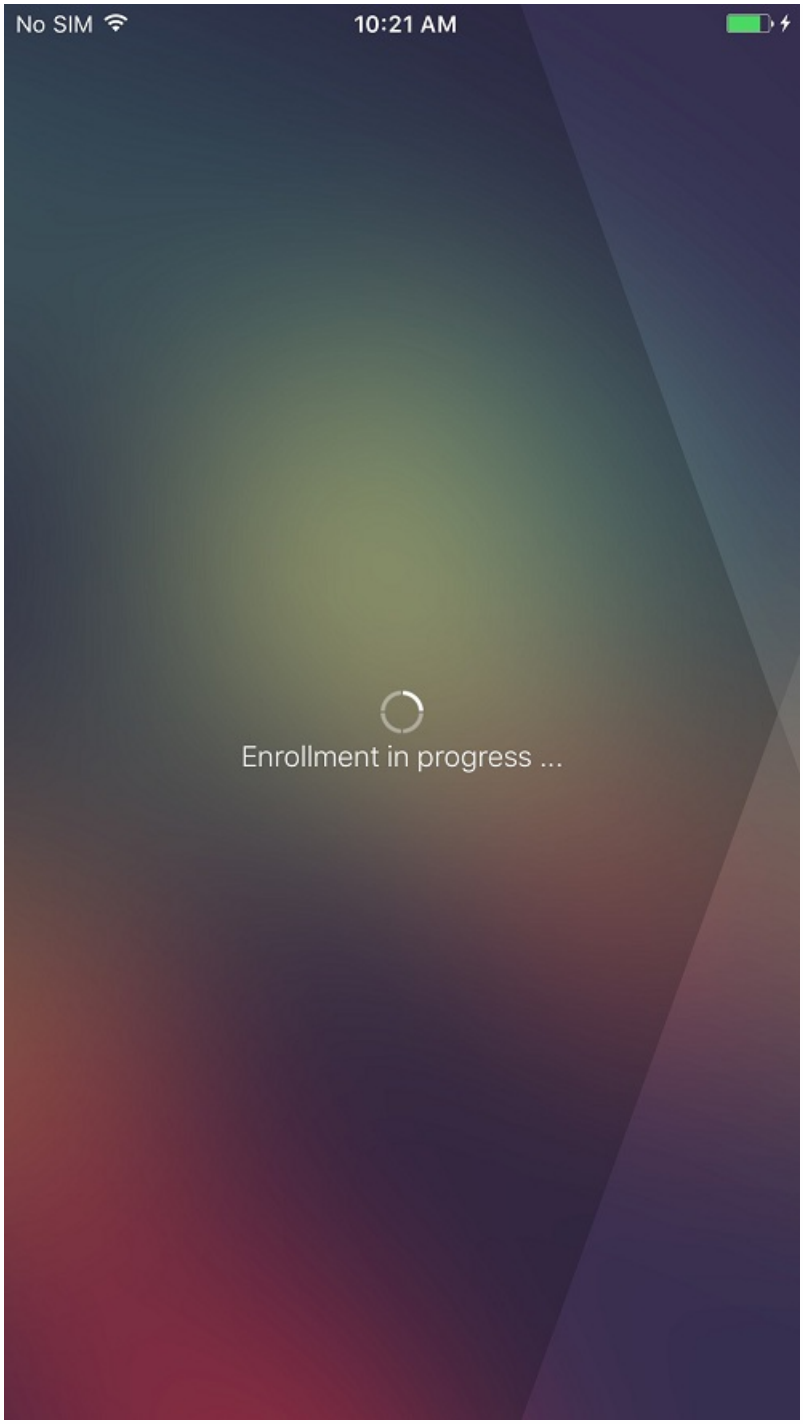
2. Em seguida, eles clicam em **Sim, registrar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

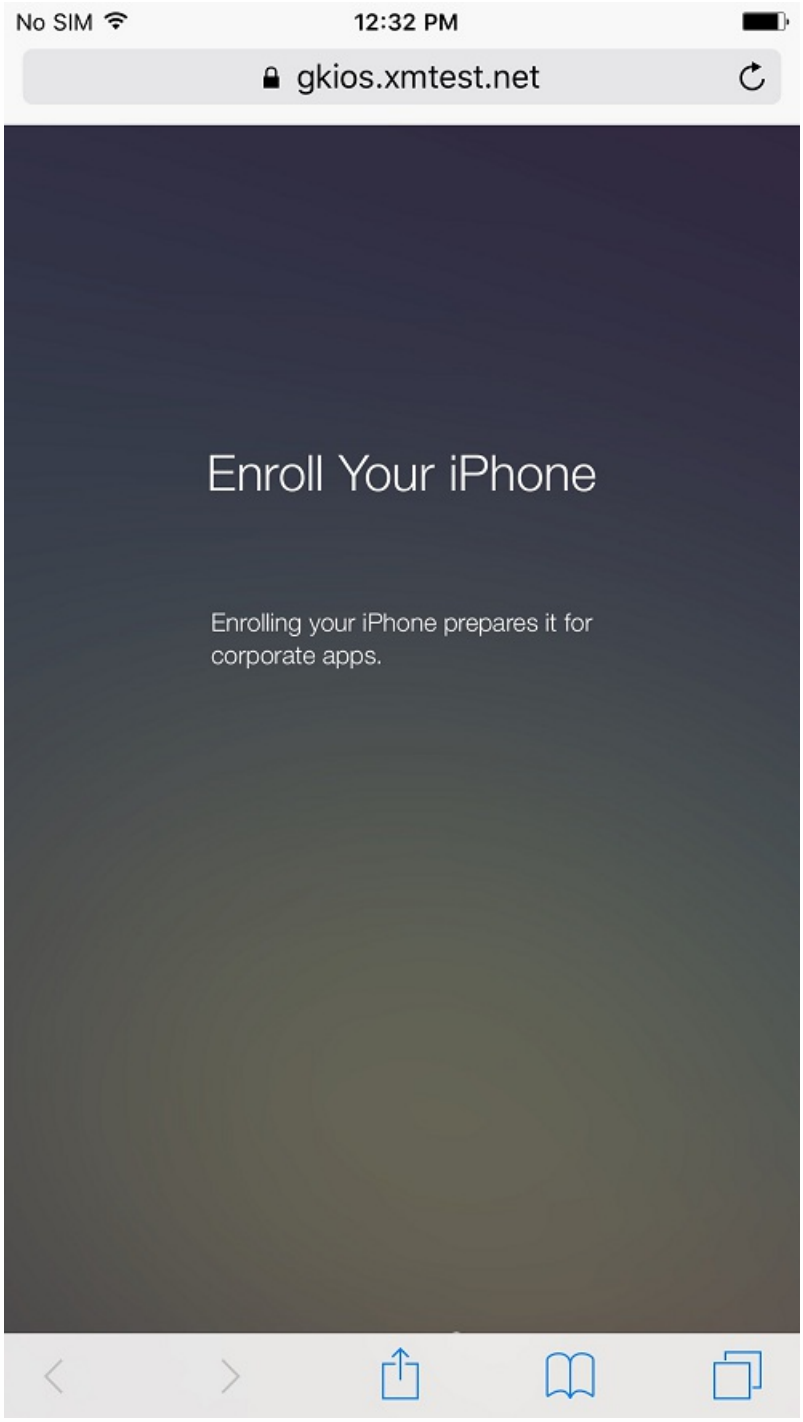


3. Os usuários fazem logon usando suas credenciais do AD do Azure.

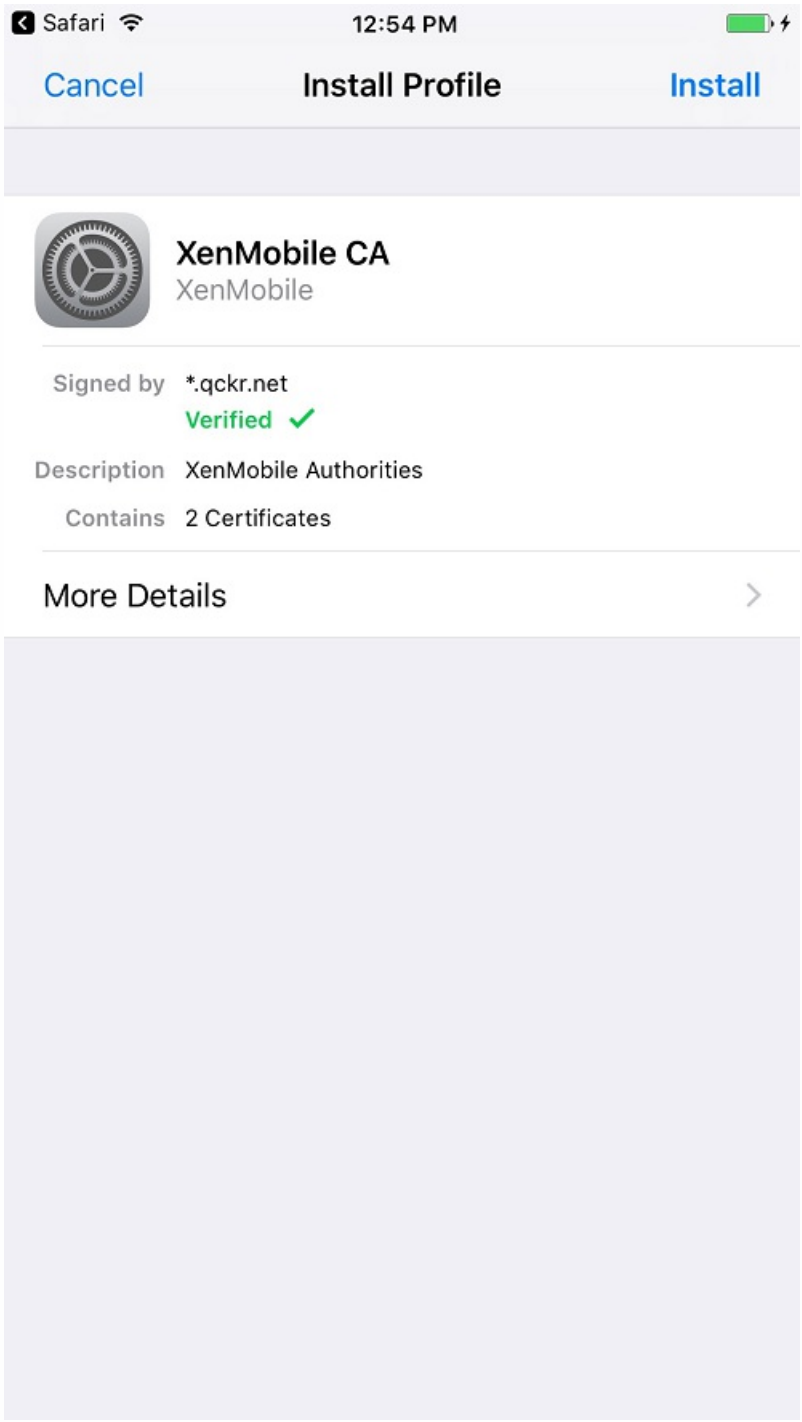
© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Derived credentials for iOS

Feb 21, 2018

As credenciais derivadas fornecem autenticação forte para dispositivos móveis. As credenciais, derivadas de um cartão inteligente, residem em um dispositivo móvel em vez do cartão. O cartão inteligente é um Personal Identity Verification (PIV) ou um Common Access Card (CAC).

As credenciais derivadas são um certificado de registro que contém o identificador de usuário, como UPN. O XenMobile armazena as credenciais obtidas do provedor de credenciais em um cofre seguro no dispositivo.

O XenMobile pode usar credenciais derivadas para registro de dispositivo iOS Se configurado para credenciais derivadas, XenMobile não dá suporte a convites de registro ou outros modos de registro para dispositivos iOS. No entanto, você pode usar o mesmo XenMobile Server para registrar os dispositivos Android por meio de convites de registro e outros modos de registro.

Requisitos

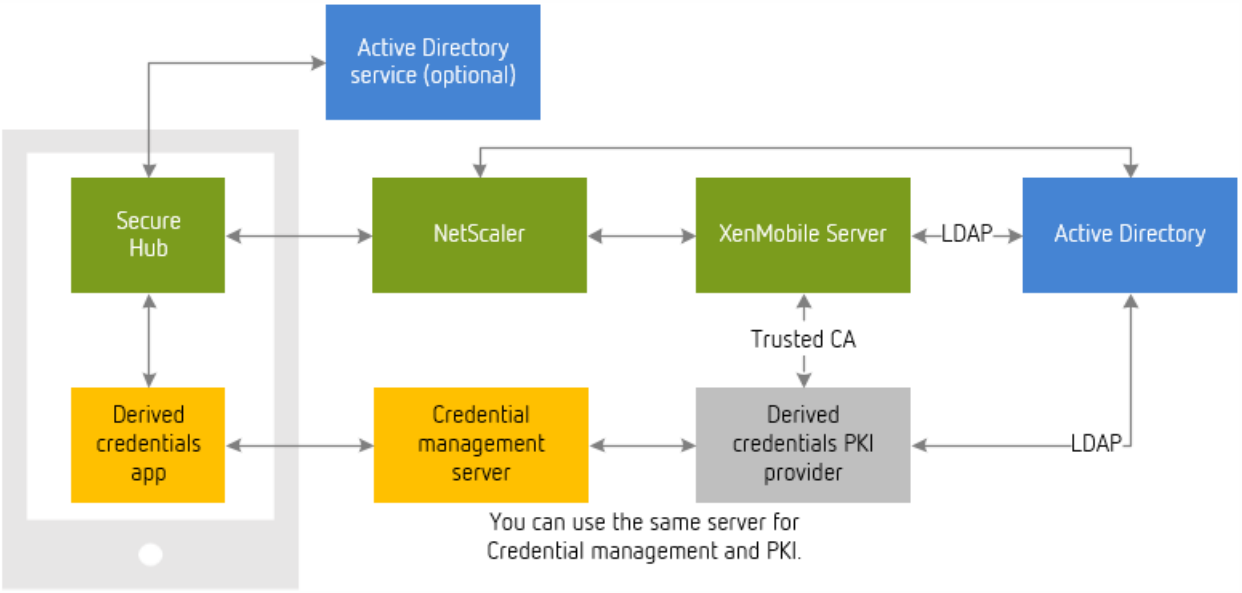
- Uma das seguintes soluções de credenciais derivadas:
  - Intercede 3.12
    A Citrix confirmou que o XenMobile funciona com a solução Intercede de credenciais derivadas. O nome do aplicativo na Apple App Store é MyID for Citrix.
    Nota: os usuários devem instalar o MyID for Citrix em seus dispositivos *antes* de se registrarem no XenMobile.
- Outras soluções de credenciais derivadas
  Embora seja provável que a maioria das outras soluções de credenciais seja compatível com o XenMobile, teste a integração antes de implantá-la em produção.
- XenMobile Server 10.6 (versão mínima)
  - Configurado para o modo Empresarial (XME)
  - 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 myID.com e o nome do domínio LDAP for sample.com, defina **Alias de domínio** como **sample.com, myID.com**.
  - Não é possível usar 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.
  - Atualmente, não há suporte para o campo Entidade em Email ou CN.
- NetScaler Gateway configurado para autenticação de certificado ou autenticação de certificado mais token de segurança
  Para obter informações sobre a configuração de PKIs, consulte Entidades PKI.
- Secure Hub 10.6 (versão mínima)
- XenMobile Apps 10.6 (versão mínima)
  - O Secure Mail não usa credenciais derivadas e continua a funcionar como antes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Use o mesmo certificado de desenvolvedor para assinar todos os aplicativos na Apple App Store.

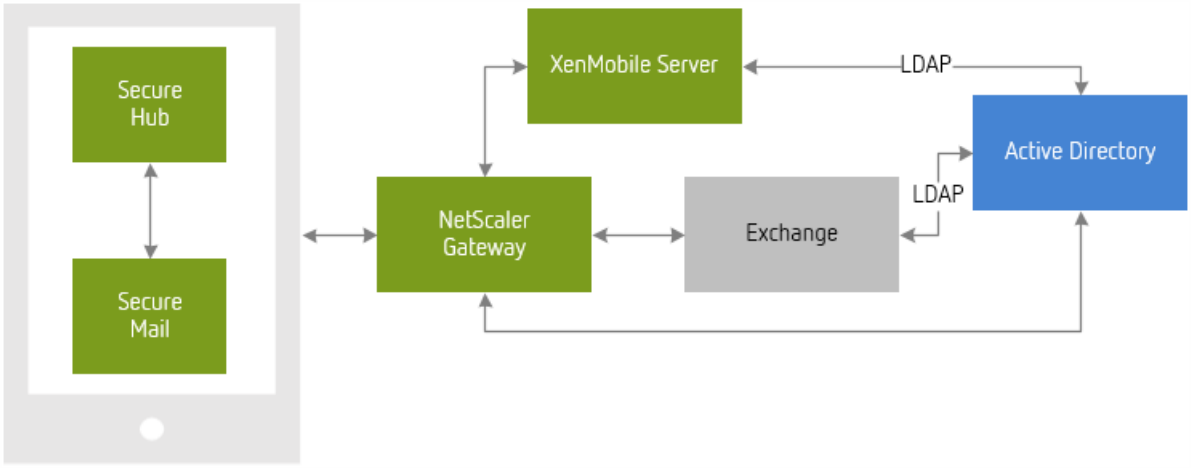
Arquitetura

Para registro, o XenMobile Server se conecta aos componentes descritos na seção "Requisitos", 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.

Após o registro, os componentes se conectam conforme mostrado no diagrama a seguir.

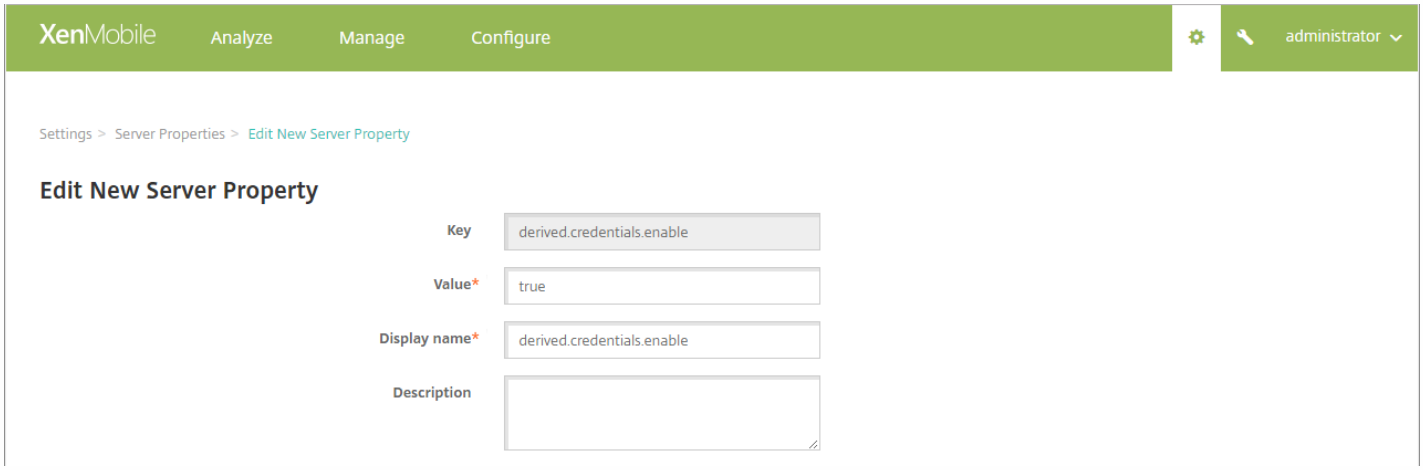


As seções a seguir descrevem como configurar o XenMobile com um provedor de credenciais derivadas, ativar credenciais derivadas para registro e gerenciar dispositivos que usam credenciais derivadas.

Ativar credenciais derivadas

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 a propriedade de servidor **derived.credentials.enable** e defina-a como **true**.



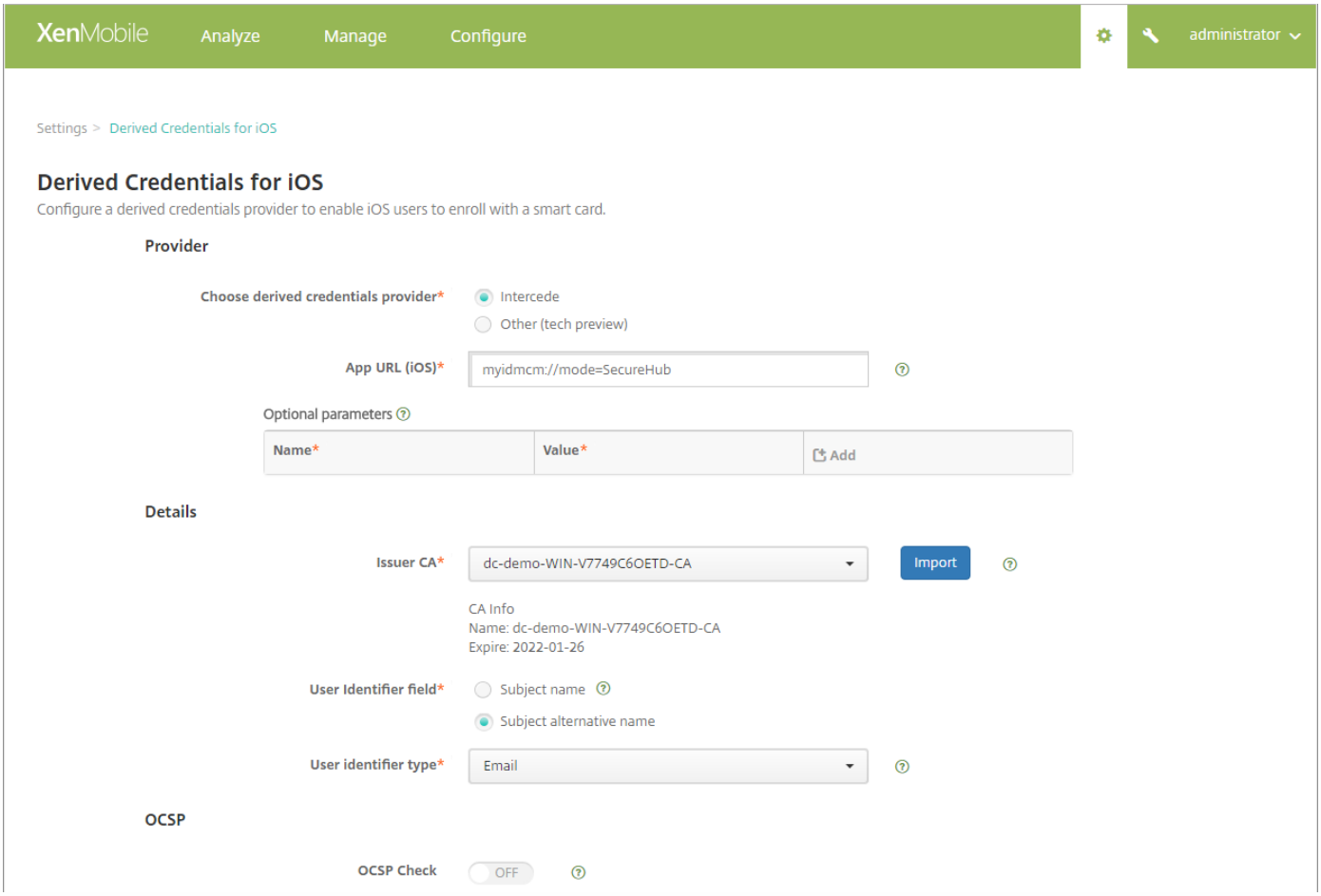
Configurar credenciais derivadas

Estas instruções pressupõem que você tenha uma configuração funcional para o provedor de credenciais derivadas que planeja integrar com o XenMobile. Em seguida, você poderá configurar o XenMobile para se comunicar com esse servidor. Você também escolhe um certificado de CA de credenciais derivadas já adicionado ao XenMobile ou importa esse 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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Em **Provedor**:

- **Escolher o provedor de credenciais derivadas**. A Citrix valida se o XenMobile funciona com o **Intercede**. Se você escolher **Outros** para o provedor, teste a integração antes de colocar seu servidor em produção.
- **URL do aplicativo (iOS)**: se você escolher **Intercede** como o provedor, o XenMobile preencherá a **URL do aplicativo**. Se você escolher **Outros** como provedor, obtenha a URL do aplicativo com o provedor de credenciais derivadas.

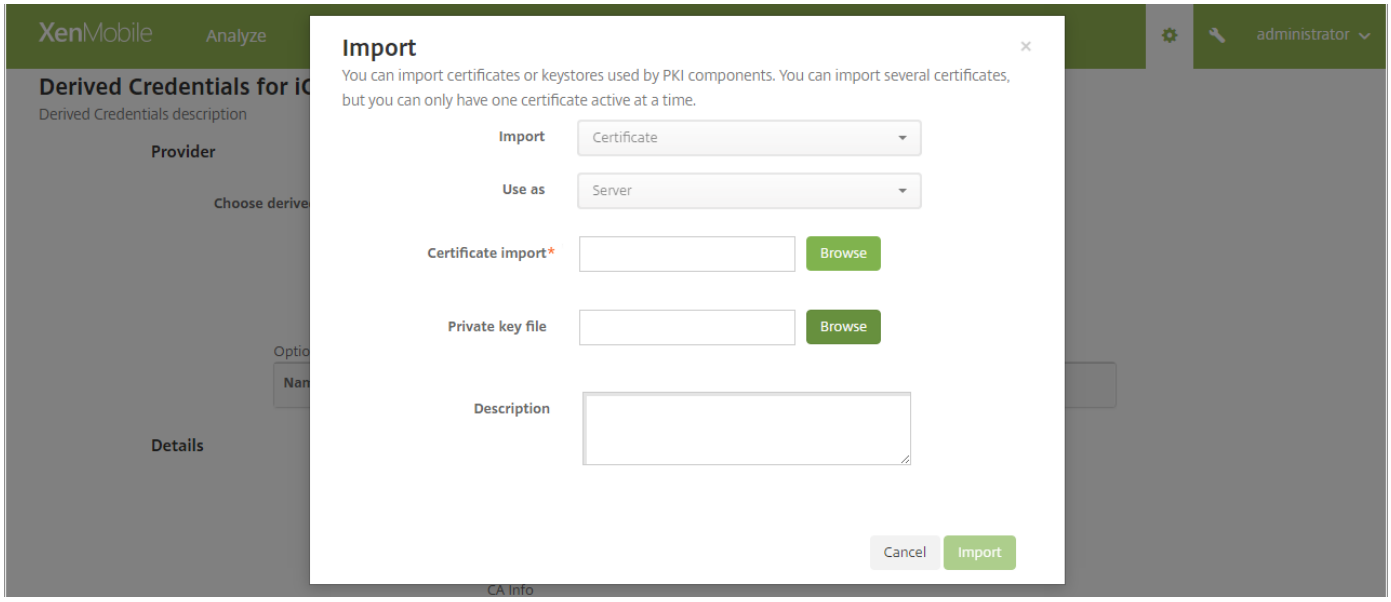
  Nota: se um dispositivo não puder entrar em contato com seu provedor, verifique a URL do aplicativo com o provedor. Talvez seja necessário alterá-la.

- **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.

3. 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.

4. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

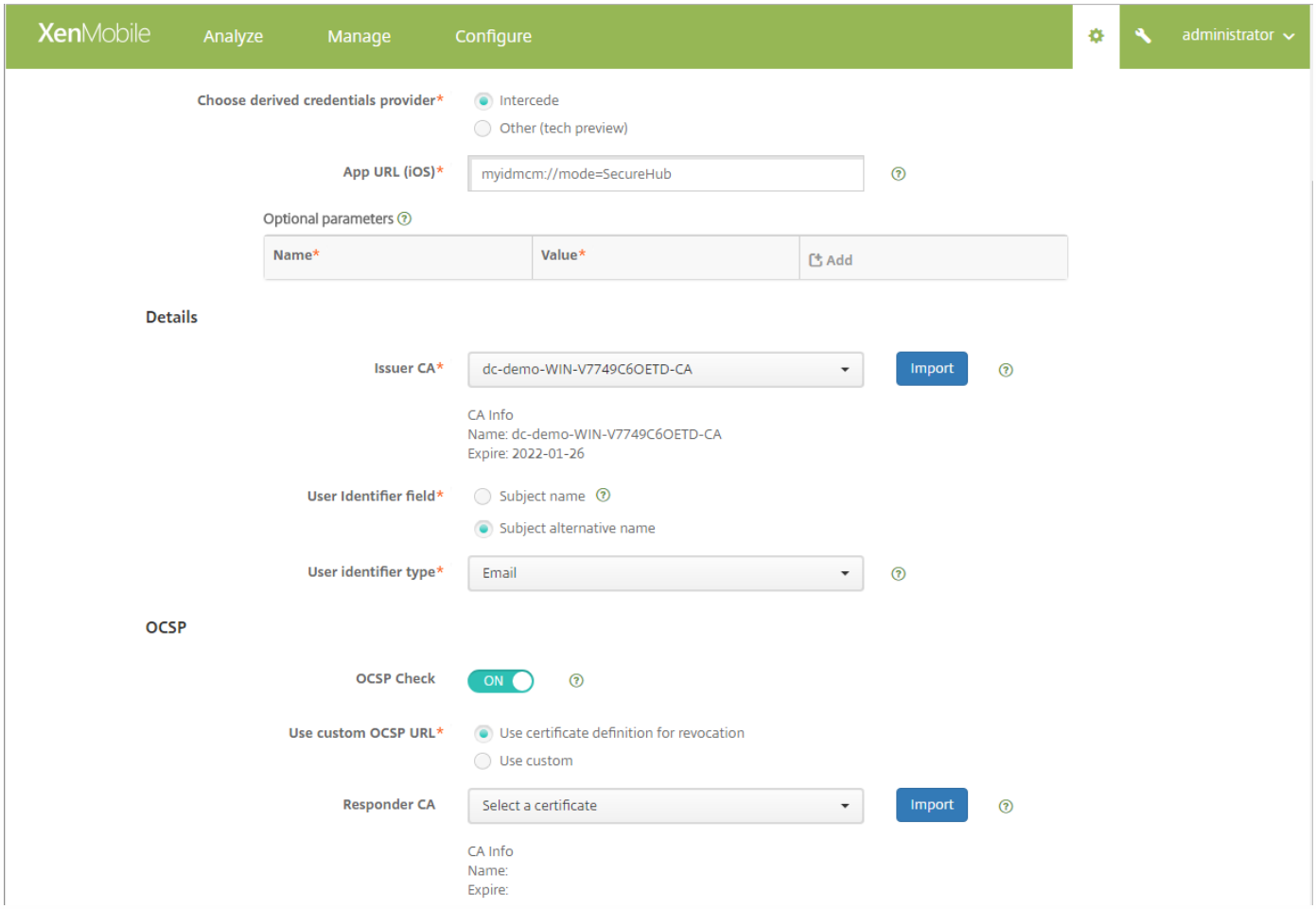


5. Se você escolher **Intercede** como provedor, o XenMobile preencherá o **Campo de identificador do usuário** e o **Tipo de identificador do usuário**. Para Intercede, o **Campo de identificador do usuário** é **Nome de entidade alternativo**, e o **Tipo de identificador do usuário** é **userPrincipalName** . Entre em contato com outros provedores de credenciais derivadas para obter suas informações relacionadas e definir as configurações.

6. Você tem a opção de usar um respondedor OCSP para verificação da revogação de certificados. Por padrão, a verificação OSP está desativada. Para ativar o suporte OCSP para o certificado de CA:

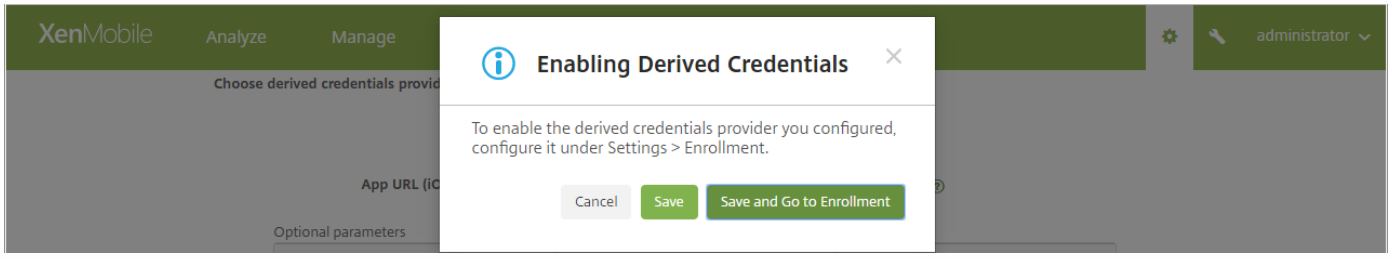
   - Defina **Verificação OCSP** como **I**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- Escolha uma opção para **Use o 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.

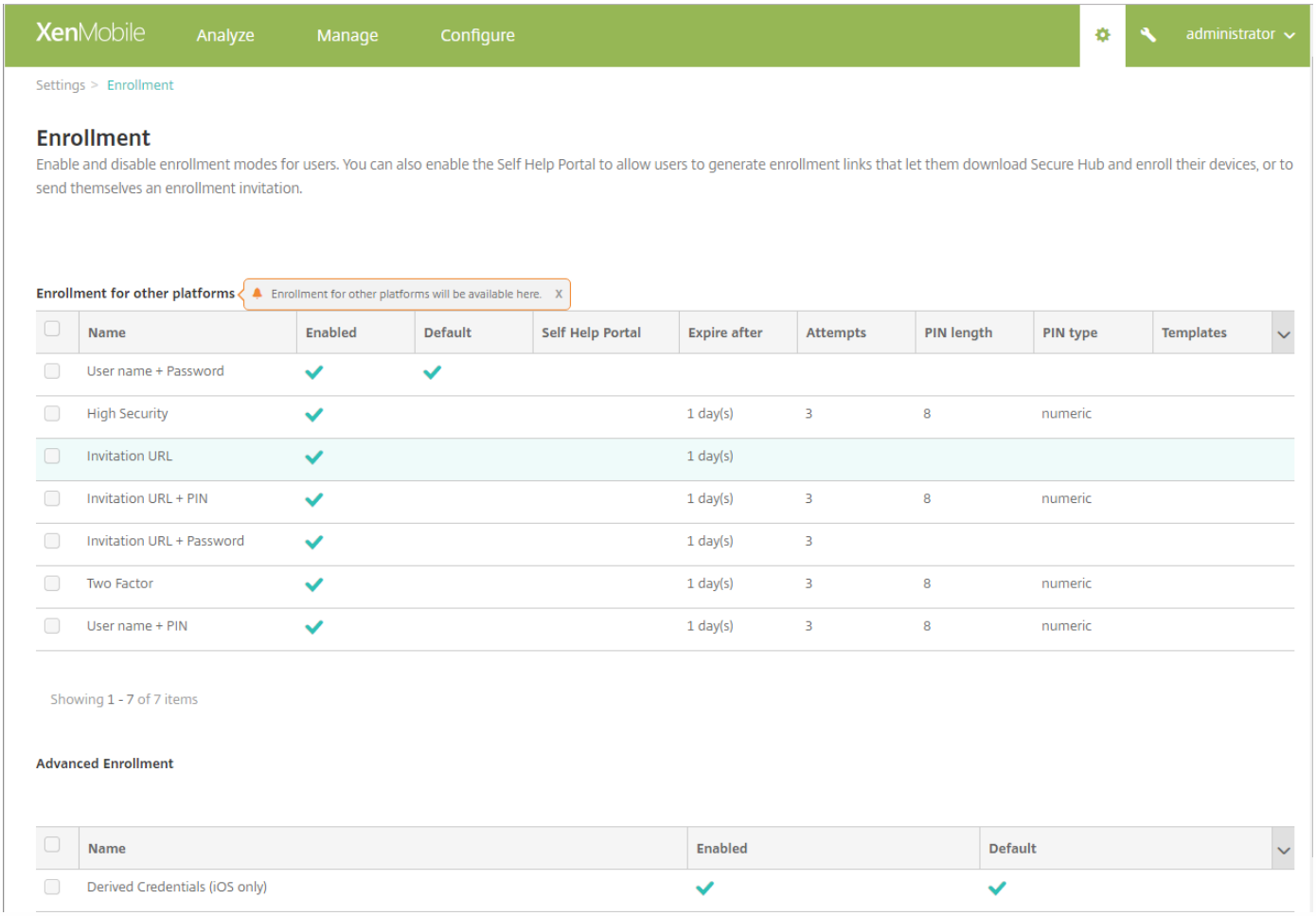
7. Clique em **Salvar**. A caixa de diálogo **Credenciais derivadas** é exibida.



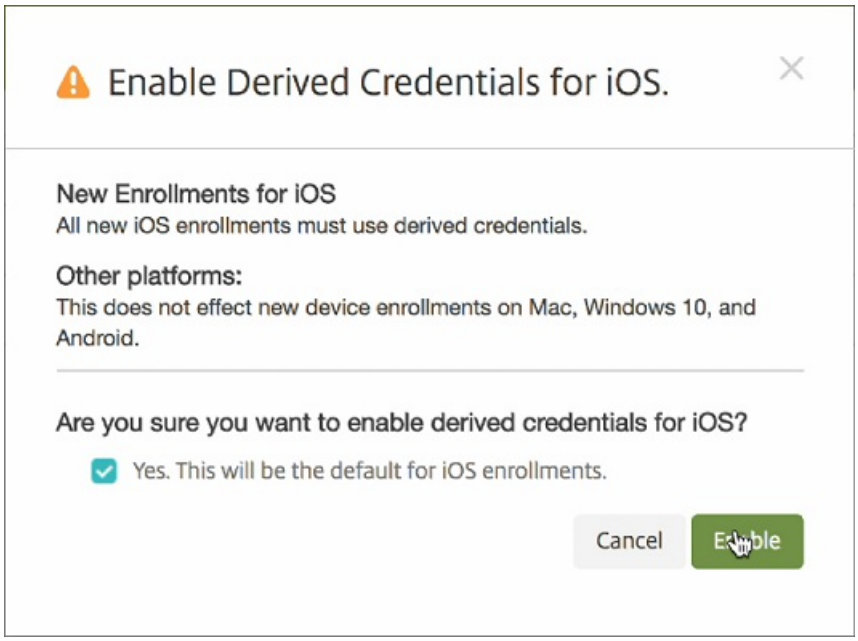
- Para ativar a configuração de credenciais derivadas, clique em **Salvar**. Para usar credenciais derivadas, você também deve definir as configurações de registro.
- Para ativar a configuração de credenciais derivadas e ir imediatamente para **Configurações > Registro**, clique em **Salvas e ir até Registro**.

8. Para ativar credenciais derivadas para registro: na página **Configurações > Registro**, em **Registro avançado**, selecione **Credenciais derivadas (apenas iOS)** e clique em **Ativar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



9. Uma caixa de diálogo de confirmação é exibida. Para ativar credenciais derivadas, marque a caixa de seleção e clique em **Ativar**.



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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

derived_credentials.

Para conhecer as etapas de registro ao usar credenciais derivadas, consulte Dispositivos iOS usando credenciais derivadas.

Mensagens de log para credenciais derivadas

Mensagens de log durante a comunicação do Secure Hub com o XenMobile Server indicam êxito ou falha, da seguinte maneira.

Mensagens do XenMobile Server (SessionCreate SUCCESS)

2017-05-11T23:23:28.537+0000 | D88973753C718B23 | INFO | http-nio-10080-exec-47 | com.sparus.nps.ios.agent.V9AgentUtils | Credencial derivada: usuário extraído do certificado: XXXXXXX@XMTEST.NET

2017-05-11T23:23:28.728+0000 | D88973753C718B23 | INFO | http-nio-10080-exec-47 | com.sparus.nps.ios.agent.V9AgentUtils | Credencial derivada: usando usuário XXXXXX@XMTEST.NET' do certificado e convertido em XXXXXXX com certid 60000001a95b7fecbbbf2821dd0000000001a9

2017-05-11T23:23:28.883+0000 | D88973753C718B23 | INFO | http-nio-10080-exec-47 | com.citrix.cg.bo.spring.impl.InternalUserServiceImpl | Parâmetros de entrada para addUser. Nome de usuário XXXXXXX@auster.ctx' e nome de domínio 'auster.ctx'

2017-05-11T23:23:29.94+0000 | D88973753C718B23 | INFO | http-nio-10080-exec-47 | com.citrix.xms.oca.imil.service.impl.GroupServiceImpl | N° de grupos:0 recuperados por UserID:40

2017-05-11T23:23:29.95+0000 | D88973753C718B23 | WARN | http-nio-10080-exec-47 | com.sparus.nps.ldap.LdapCredentialHandlerImpl | Nenhum grupo encontrado para o usuário XXXXXX@auster.ctx'

2017-05-11T23:23:34.244+0000 | 21829910a6438ef5 | INFO | http-nio-10080-exec-60 | com.sparus.nps.ios.agent.V7ContextBuilder | Nenhuma identidade correspondente encontrada na solicitação de 172.16.1.57 para /zdm/ios/agent;jsessionid=D88973753C718B23ADDEA26B46E5FBB2

2017-05-11T23:23:59.118+0000 | 21829910a6438ef5 | INFO | http-nio-10080-exec-52 | com.sparus.nps.ios.enroll.ProfileServiceServlet | Novo registro iniciado para serialNumber=CCQLQNKPFMJF, imei=null, udid=4a621749b64f7d915849ebcef3ded9cf7f460406, meid=null

Mensagens do XenMobile Server (SessionCreate FAIL)

2017-05-11T23:06:46.168+0000 | 40DA582380D50C72 | INFO | http-nio-10080-exec-42 | com.sparus.nps.ios.agent.V9AgentUtils | Credencial derivada: usuário extraído do certificado: XXXXXXXX@XMTEST.NET

2017-05-11T23:06:46.233+0000 | 40DA582380D50C72 | WARN | http-nio-10080-exec-42 | com.citrix.cg.util.CGUtil | Nenhum domínio padrão encontrado, redirecionando para o domínio 'local'.

2017-05-11T23:06:46.253+0000 | 40DA582380D50C72 | WARN | http-nio-10080-exec-42 | com.citrix.cg.util.CGUtil | domínio local. Serviço de diretório não gerenciado para local IDP

2017-05-11T23:06:46.253+0000 | 40DA582380D50C72 | ERROR | http-nio-10080-exec-42 | com.sparus.nps.ios.agent.V9AgentUtils | dc ecxeption

com.citrix.xms.oca.imil.exception.OperationFailedException: Não foi possível fazer logon. Nome de usuário ou senha

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

incorreto

Mensagens do Secure Hub (SessionCreate SUCCESS)

iniciar solicitação com id 6 e valor (omitido) https://*****/zdm/ios/agent?action=sessioncreate&h=dc

Lidando com o desafio de certificado de cliente para h=dc

O tamanho das credenciais é 3405

Transmitindo as credenciais no desafio do certificado de cliente DC

Credenciais analisadas com êxito

desafio recebido NSURLAuthenticationMethodServerTrust

solicitação com id 6 bem-sucedida com o código httpResponse 200

Mensagens do Secure Hub (SessionCreate FAIL)

iniciar solicitação com id 6 e valor (omitido) https://*****/zdm/ios/agent?action=sessioncreate&h=dc

Lidando com o desafio de certificado de cliente para h=dc

Item encontrado.

O tamanho das credenciais é 3434

Transmitindo as credenciais no desafio do certificado de cliente DC

Credenciais analisadas com êxito

falha na solicitação com id 6 com o código httpResponse 500

Mensagens relacionadas ao NetScaler

O usuário está registrado com credencial derivada e transientCredential NÃO é nulo. //O certificado de credencial derivada é passado para o NetScaler.

O usuário está registrado com credencial derivada e transientCredential é nulo. ////O certificado de credencial derivada não é encontrado e não é passado para o NetScaler.

O usuário está registrado com Credencial Derivada e o certificado expirou. Exibindo a mensagem para o usuário para renovar o certificado.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Atualização

Feb 21, 2018

Important

Antes de atualizar para o XenMobile 10.8 (no local)

1. Atualize o seu Citrix License Server para 11.14.x ou posterior antes de atualizar para a versão mais recente do XenMobile Server 10.8.
   A versão mais recente do XenMobile exige o Citrix License Server 11.14.x (versão mínima). A data da Subscription Advantage (SA) em sua licença Citrix deve ser posterior a 6 de junho de 2016. Você pode ver sua data de SA 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 da as em sua licença, baixe o último arquivo de licença do Portal Citrix e carregue o arquivo para o Servidor de Licenciamento. Para obter mais informações, consulte http://support.citrix.com/article/CTX209580.
2. Para um ambiente em cluster: Para instalar aplicativos da XenMobile Store em dispositivos iOS 11, você deve habilitar a porta 80 no 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.

Após atualizar para o XenMobile 10.8 (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.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.

Você pode atualizar diretamente para o XenMobile 10.8 do XenMobile 10.7.x ou 10.6.x. Para executar a atualização, use o xms_10.8.0.23.bin ou o binário 10.8 mais recente disponível na página de download da Citrix. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console e clique em **Gerenciamento de versão**.

Para atualizar de versões mais antigas do XenMobile, consulte o artigo sobre atualização no PDF do XenMobile Server 10.7.

Este artigo descreve como usar a página **Gerenciamento de versão**, atualizar implantações do XenMobile em cluster e atualizar do MDM para o Enterprise Edition.

Para atualizar usando a página Gerenciamento de versão

Use a página **Gerenciamento de versão** para atualizar do XenMobile 10.7.x ou 10.6.x para a versão mais recente do

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile Server.

Pré-requisitos:

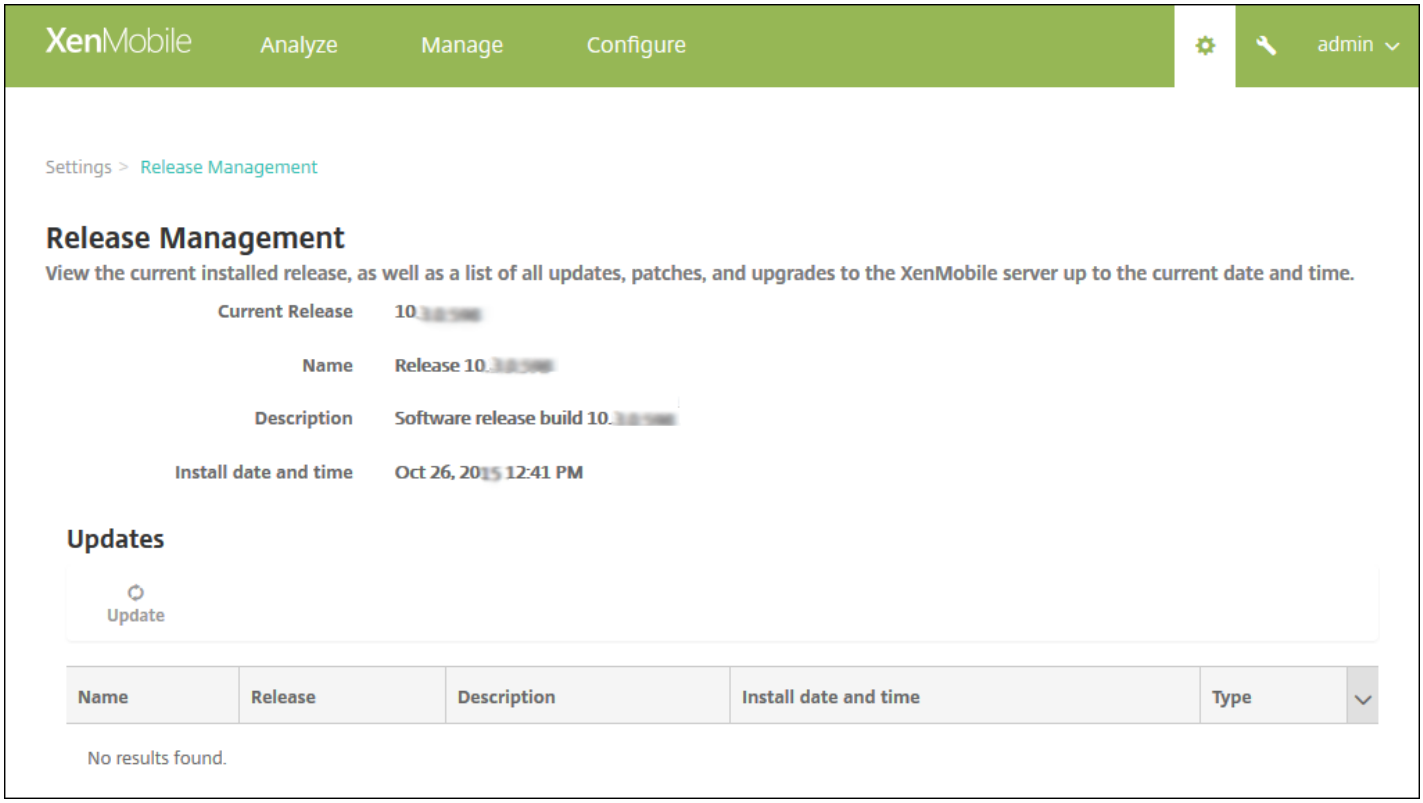
- Reveja os Requisitos do sistema.

Se você tem uma implantação em cluster, consulte as instruções no final deste artigo.

1. Faça logon na sua conta no site da Citrix e vá para a página de Download. Baixe o arquivo de atualização do XenMobile (.bin) para uma localização apropriada.

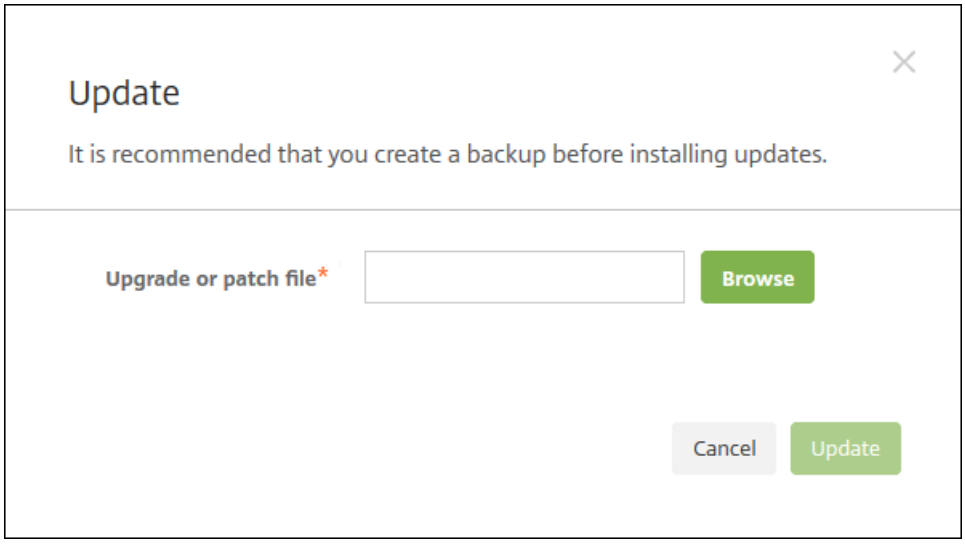
2. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.

Nota: 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.

Para atualizar implantações XenMobile em cluster

> **Important**
>
> 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 10.8 MDM Edition para Enterprise Edition.

Você pode atualizar do XenMobile 10.8 MDM Edition para o XenMobile 10.8 Enterprise Edition para dispositivos iOS e

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Android.

Pré-requisitos:

- A licença Enterprise correta.
- O NetScaler 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 > Netscaler Gateway** e configure os detalhes do NetScaler 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 de 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Contas de usuário, funções e registro

Feb 21, 2018

Configure o seguinte no console XenMobile, na guia **Gerenciar** e na página **Configurações**:

- Contas de usuário e grupos
- Funções para contas de usuário e grupos
- Modo de registro e convites.

Da **guia gerenciar** , você pode fazer o seguinte:

- Clique em **Usuários** para adicionar contas de usuário manualmente ou use um arquivo de provisionamento .csv para importar as contas e gerenciar os grupos locais. Para obter detalhes, consulte:
  - Para adicionar, editar ou excluir contas de usuários
  - Para importar contas de usuário usando um arquivo de provisionamento .csv e Formatos de arquivo de provisionamento
  - Para adicionar ou remover grupos no XenMobile

  Você também pode usar os fluxos de trabalho para gerenciar a criação e a remoção de contas de usuário, como descrito posteriormente neste artigo em Criar e gerenciar fluxos de trabalho.

- Clique em **Registro** para configurar até sete modos e enviar convites para registro. Cada modo de registro tem seu próprio nível de segurança e o número de etapas que os usuários deve seguir para registrar seus dispositivos. Para obter detalhes, consulte:
  - Para configurar os modos de registro e ativar o Portal de Autoajuda
  - Ativar a detecção automática no XenMobile para o registro de usuário

Na página **Configurações**, você pode fazer o seguinte:

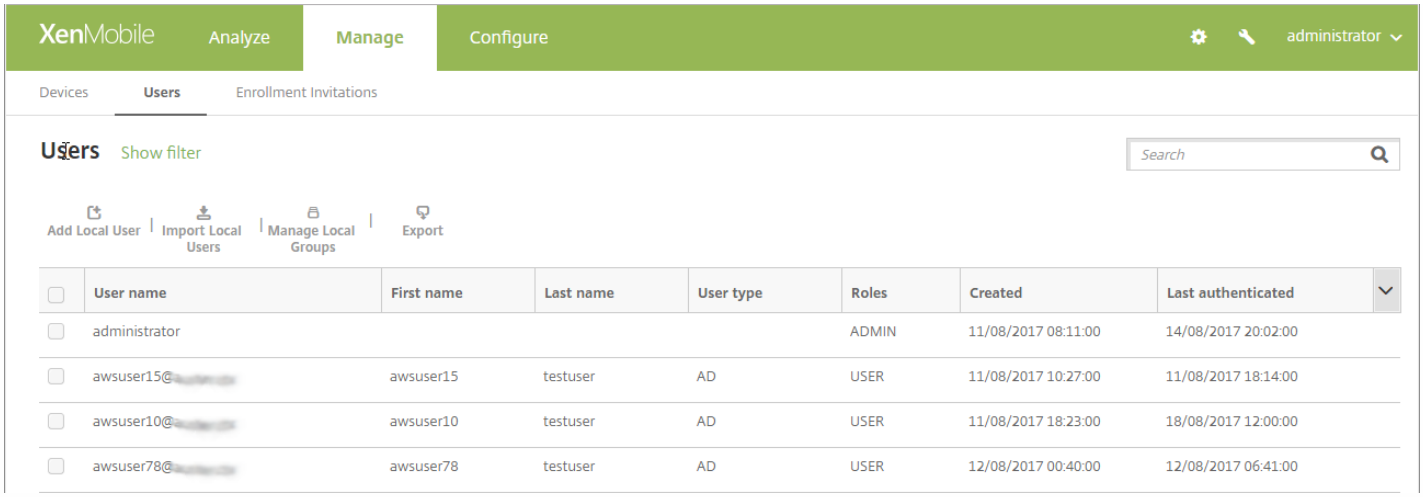
- Clique em **Controle de acesso baseado em função** para atribuir funções predefinidas ou conjuntos de permissões a usuários e grupos. Essas permissões controlam o nível de acesso que os usuários têm às funções do sistema. Para obter detalhes, consulte:
  - Configuração de funções com RBAC
- Clique em **Modelos de notificação** para usá-los nas mensagens de notificação padrão, de ações automatizadas e de registros enviadas para os usuários. Configure os modelos de notificação para enviar mensagens por três canais diferentes: Secure Hub, SMTP ou SMS. Para obter detalhes, consulte:
  - Criando e atualizando modelos de notificação

Para adicionar, editar 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 obter as etapas importar contas de usuário de um arquivo de provisionamento, consulte Para importar contas de usuário usando um arquivo de provisionamento. csv.

1. No console XenMobile, clique em **Gerenciar** > **Usuários**. A página **Usuários** é exibida.

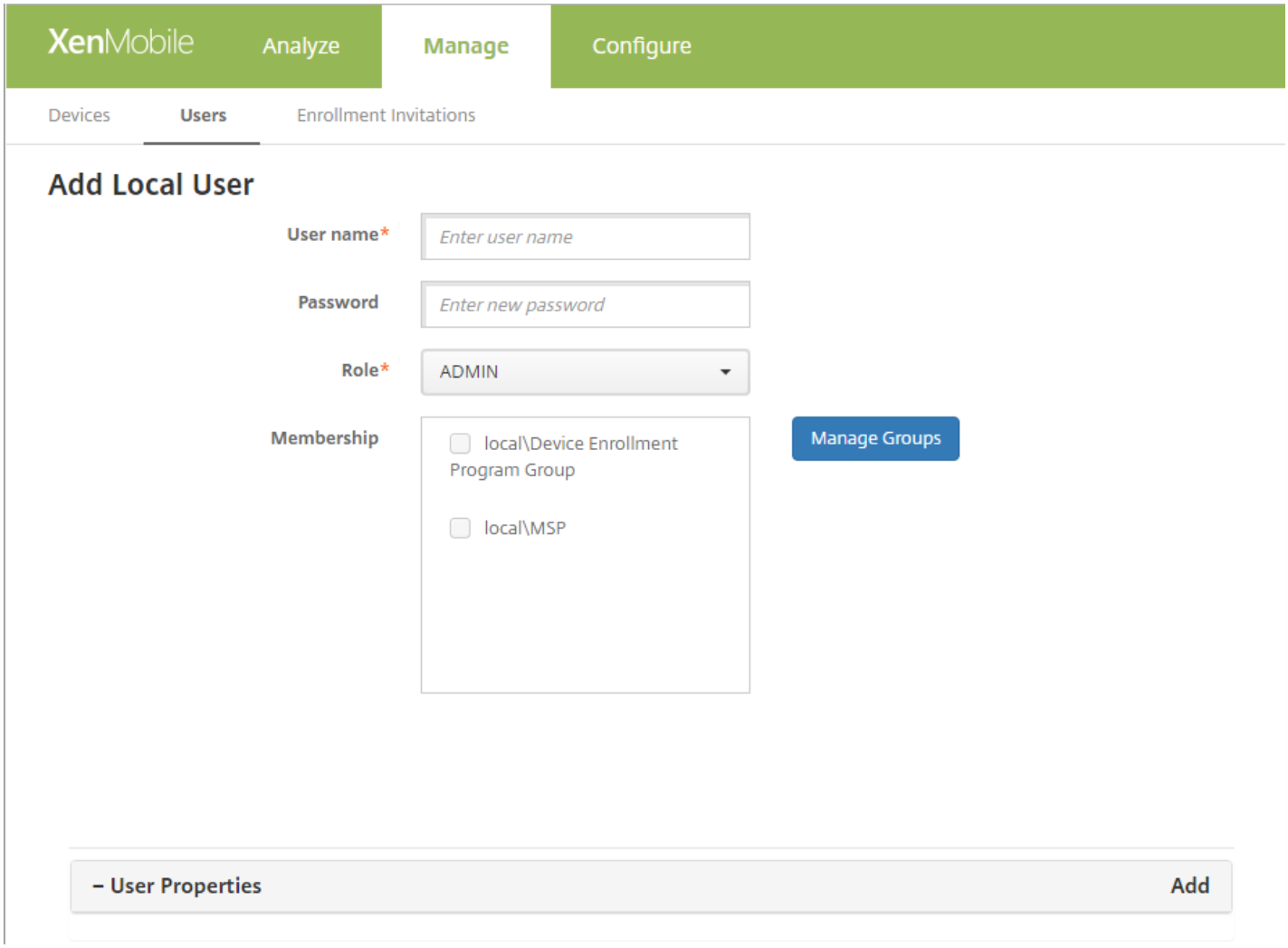
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

maiúsculas e minúsculas.

- **Senha**: digite uma senha de usuário opcional.
- **Função**: Na lista, clique na função do usuário. Para obter mais informações sobre as funções, consulte Configuração de 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 seguintes 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**.

Nota: 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.

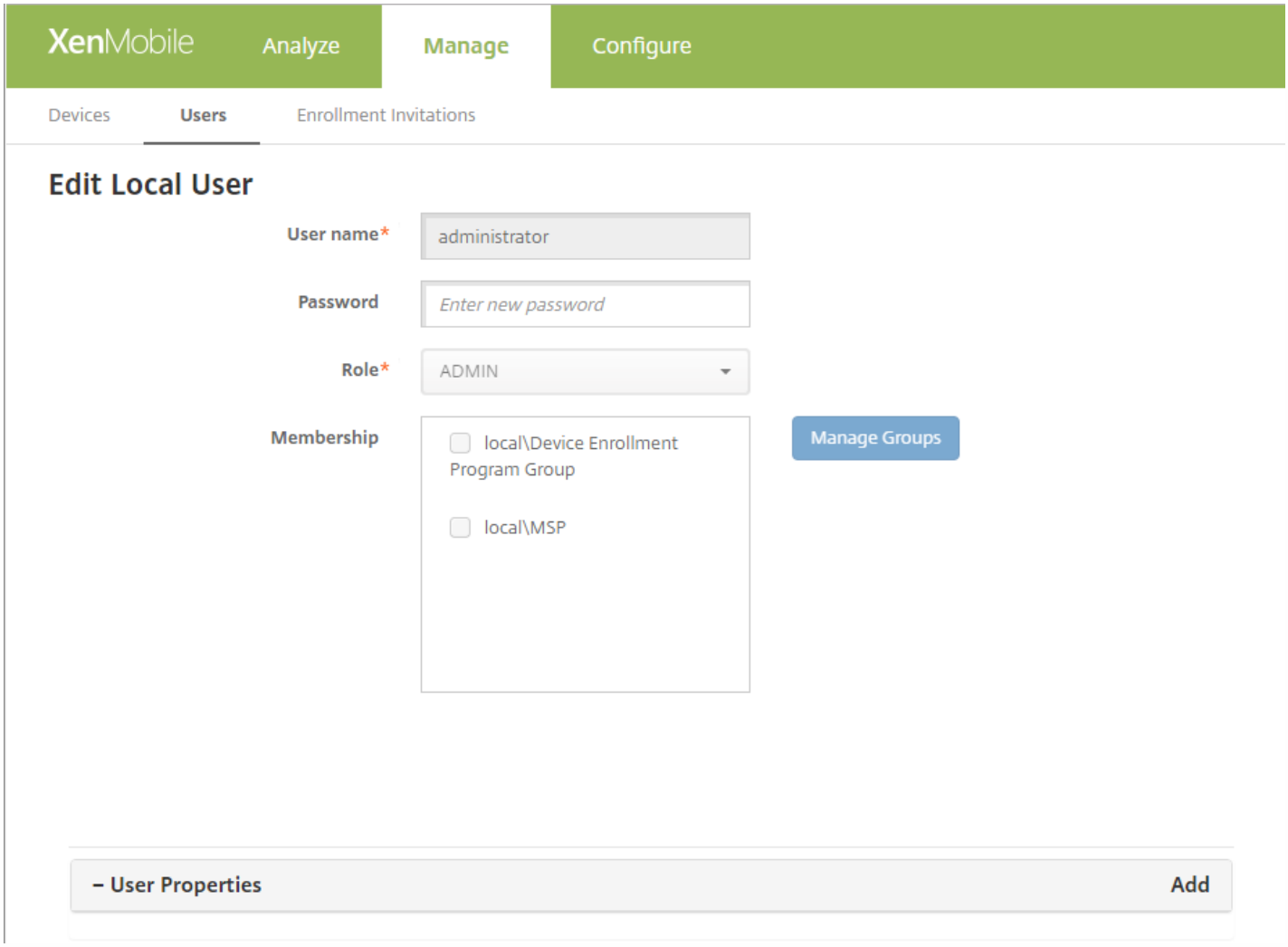
Para editar uma propriedade do usuário existente, clique na propriedade e faça alterações. Clique em **Concluído** para salvar a listagem alterada ou em **Cancelar** para deixar a listagem inalterada.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 seguintes 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 excluir uma conta de usuário local

1. Na página **Usuários**, na lista de contas de usuários, clique para selecionar um usuário.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Observação: você pode selecionar mais de um usuário a ser excluído marcando a caixa de seleção ao lado de cada usuário.

2. Clique em **Excluir**. Uma caixa de diálogo de confirmação é exibida.

3. 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**.

Importação de 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:

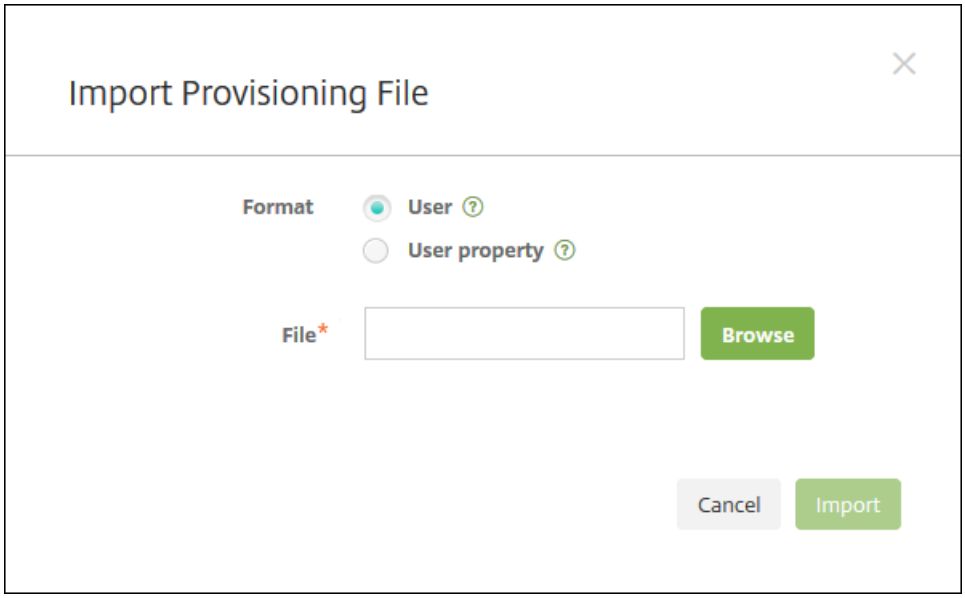
- Para usuários locais, use o nome de domínio junto com o nome do usuário no arquivo de importação. Por exemplo, especifique nome_usuário@domínio. Se o usuário local que você criar ou importar for um domínio gerenciado no XenMobile, o usuário não poderá fazer o registro usando as credenciais LDAP correspondentes.
- 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, você deve reativar o domínio padrão após a conclusão da importação de usuários internos.
- 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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

Um arquivo de provisionamento que você cria manualmente e usa para importar contas de usuário e propriedades para o XenMobile deve estar em um dos seguintes formatos:

- **Campos do arquivo de provisionamento de usuário**: user;password;role;group1;group2
- **Campos do arquivo de provisionamento de atributo de 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 provisionamento de usuário

Esta entrada, user01;pwd\;o1;USER;myGroup.users01;myGroup.users02;myGroup.users.users01, significa:

- **Usuário**: user01
- **Senha**: pwd;01
- **Função**: USER
- **Grupos**:
  - myGroup.users01

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- myGroup.users02
- myGroup.users.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 provisionamento de atributo de usuário

Esta 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 os modos de registro e ativar o Portal de Autoajuda

Configure os modos de registro de dispositivo para permitir que os usuários registrem seus dispositivos no XenMobile. O XenMobile oferece sete modos, cada um com seu próprio nível de segurança e etapas que os usuários devem seguir para registrar os dispositivos. Você pode disponibilizar alguns modos no Portal de Autoajuda. Os usuários podem fazer login no portal e gerar links de registro que lhes permitem registrar os dispositivos ou optar por enviar um convite de registro para si mesmos. Configure modos de registro no console XenMobile dapágina **Configurações** > **Registro**.

Envie convites de registro na página **Gerenciar** > **Convites de registro**. Para obter informações, consulte Enviar um convite para registro.

Observação: se você planejar usar modelos de notificação personalizados, deverá configurar os modelos antes de configurar os modos de registro. Para obter mais informações sobre os modelos de notificação, consulte Criando ou atualizando modelos de notificação.

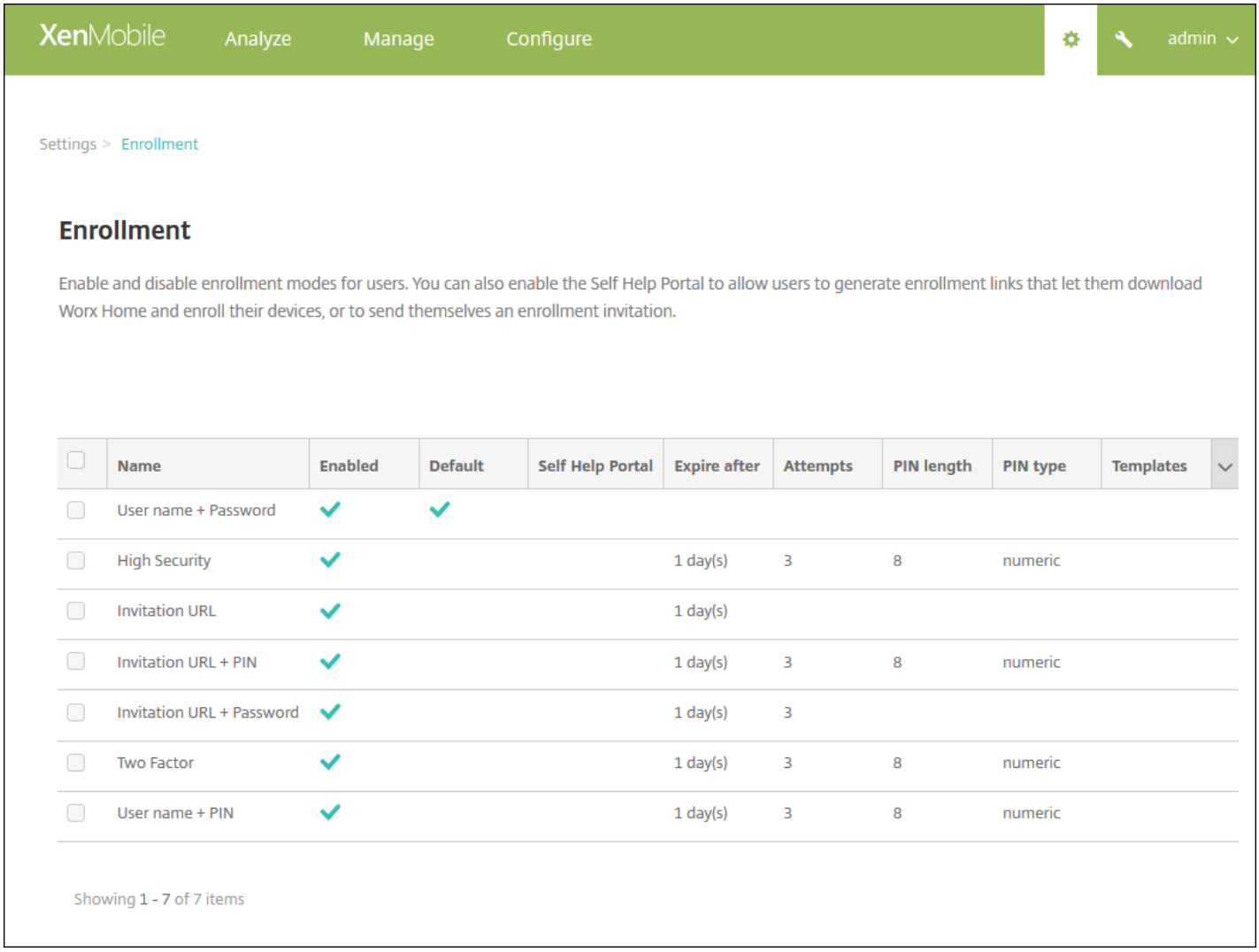
1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.

2. Clique em **Registro**. A página **Registro** é exibida, contendo uma tabela de todos os modos de registro disponíveis. Por padrão, todos os modos de registro estão ativados.

3. Selecione um modo 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 registro, o menu de opções é exibido acima da lista de modos de registro. Quando você clica em qualquer outro lugar da lista, o menu de opções é exibido no lado direito da listagem.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Escolha entre os modos de registro:

- Nome de usuário + Senha
- Alta Segurança
- URL de Convite
- URL de Convite + PIN
- URL de Convite + Senha
- Dois Fatores
- Nome de usuário + PIN

Você pode usar convites de registro para restringir o registro para os usuários com apenas um convite.

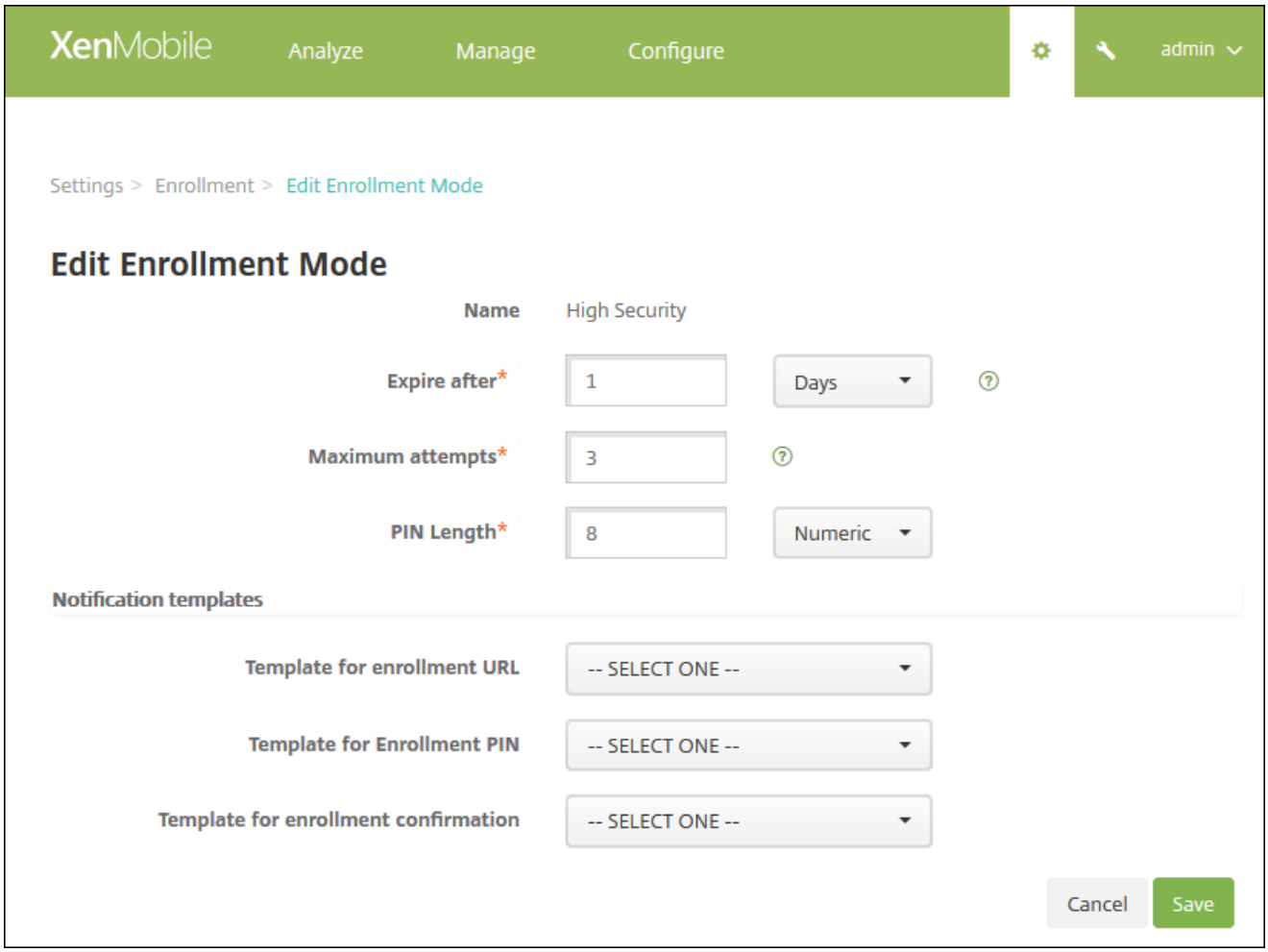
Você pode usar convites de registro de PIN de uso único (OTP) como uma solução de dois fatores. Os convites de registro OTP controlam o número de dispositivos que um usuário pode registrar.

Para ambientes com requisitos de segurança, você pode associar convites de registro a um dispositivo por UDID/SN/EMEI. Uma opção de dois fatores também está disponível para exigir senha do Active Directory e OTP.

Para editar um modo de registro

1. Na lista **Registro**, selecione um modo de registro e clique em **Editar**. A página **Editar modo de registro** é exibida. Dependendo do modo selecionado, você pode ver opções diferentes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.
  Observação: 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.
  Observação: 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 o 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 os 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Clique em **Salvar**.

Para definir um modo de registro como padrão

Quando você define um modo de registro como padrão, o modo é usado para todas as solicitações de registro de dispositivo, a menos que você selecione um modo de registro diferente. Se nenhum modo de registro for definido como padrão, você deverá criar uma solicitação de registro para cada dispositivo.

Nota: Os únicos modos 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 registro, **Nome de usuário + senha**, **Dois fatores** ou **Nome de usuário + PIN**.

Nota: 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 registro tiver sido definido como padrão, o modo não será mais o padrão.

Para desativar um modo de registro

Desativar um modo de registro o torna indisponível para uso nos convites de registro de grupo e no Portal de Autoajuda. Você pode alterar como permite que usuários registrem seus dispositivos desativando um modo de registro e permitindo outro.

1. Selecione um modo de registro.

Observação: você não pode desativar o modo de registro padrão. Se você desejar desativar o modo de registro padrão, deverá primeiro remover o status padrão.

2. Clique em **Desativar**. O modo de registro não está mais ativado.

Para ativar um modo de registro no Portal de Autoajuda

Permitir um modo de registro no Portal de Autoajuda permite que os usuários registrem seus dispositivos no XenMobile individualmente.

Observação:

- O modo 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 registro no Portal de Autoajuda por vez.

1. Selecione um modo de registro.

2. Clique em **Portal de Autoajuda**. O modo 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

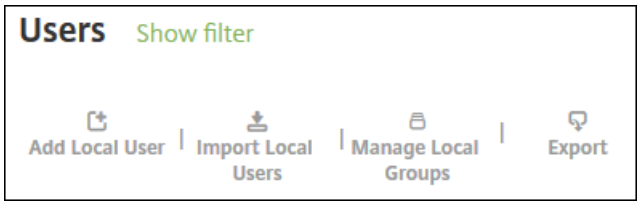
© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

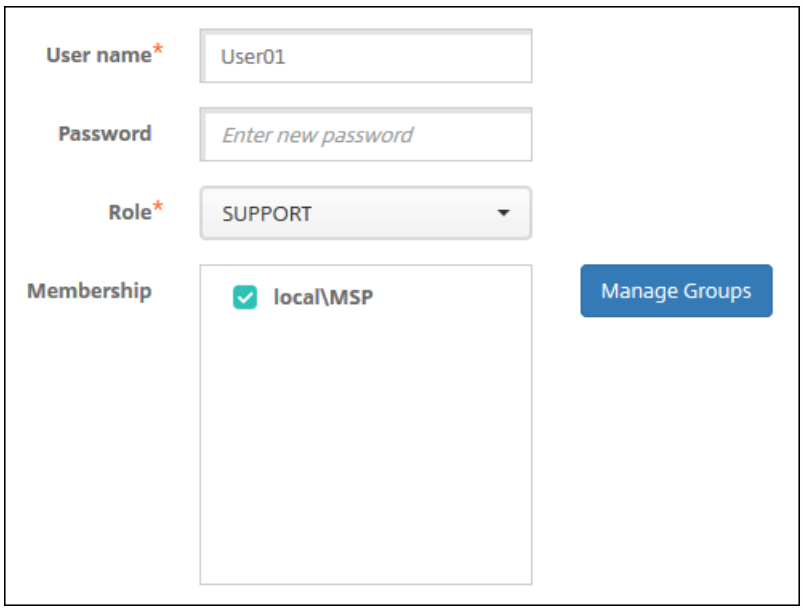
Para adicionar um grupo local

1. Você pode optar por um dos seguintes procedimentos:

- Na página **Usuários**, clique em **Gerenciar grupos locais**.

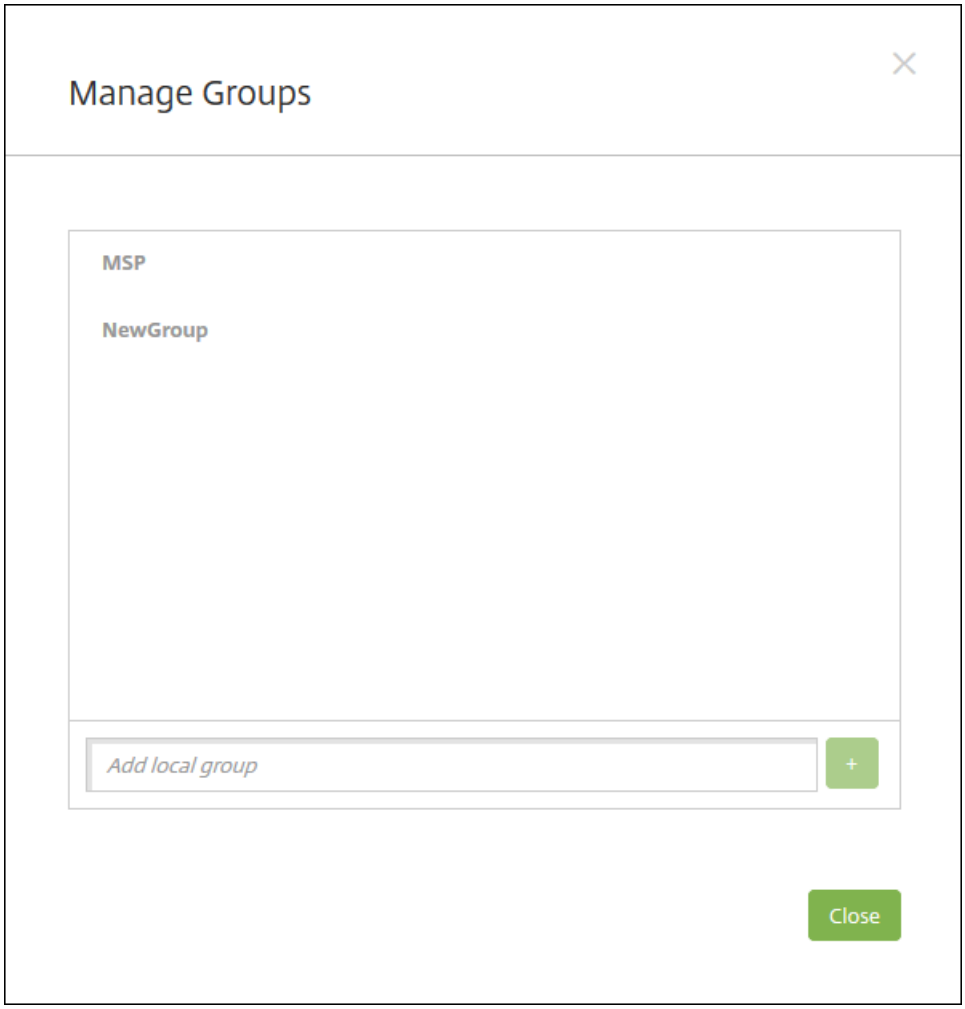


- Na página **Adicionar usuário local** ou na página **Editar usuário local**, clique em **Gerenciar grupos**.



A caixa de diálogo **Gerenciar grupo** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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

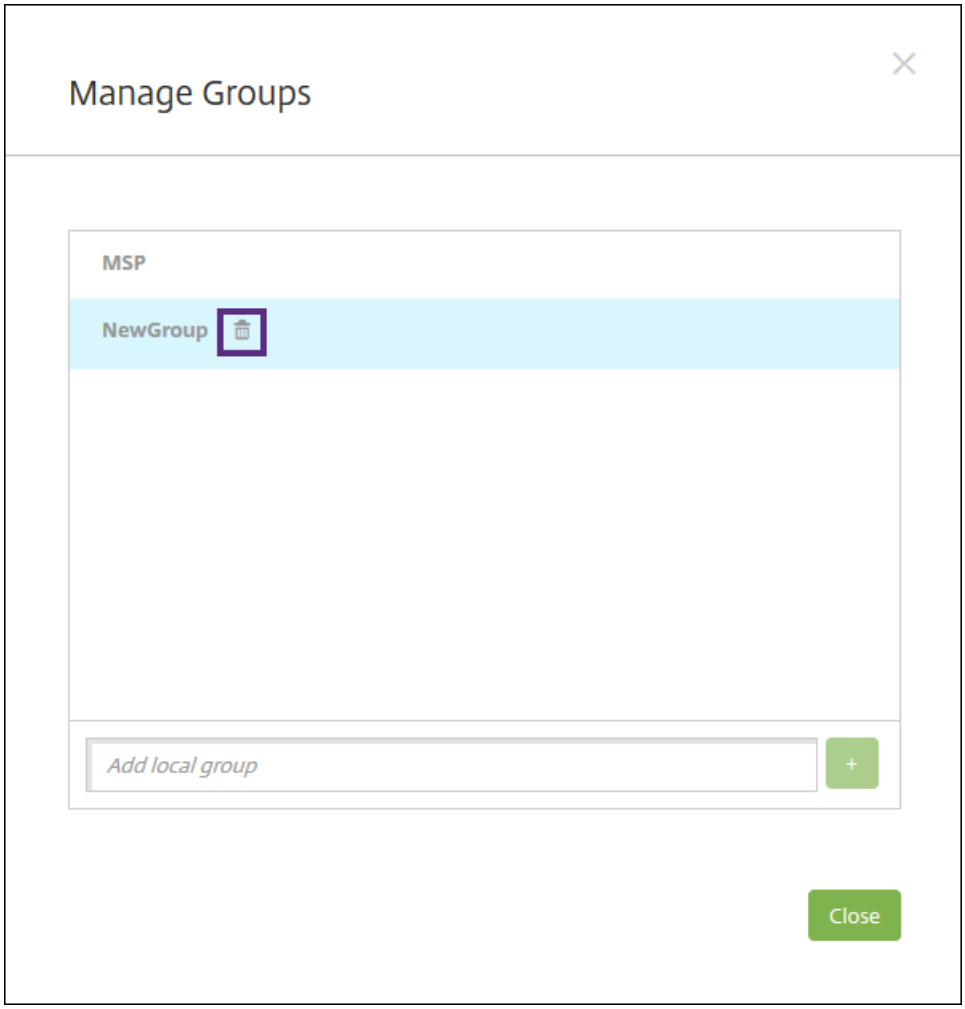
Observação: remover um grupo não afeta as contas de usuário. Remover um grupo simplesmente remove a associação dos usuários àquele grupo. Os usuários também perdem acesso aos aplicativos ou aos perfis fornecidos pelos Grupos de Entrega que são associados a esse grupo; todas as outras associações de grupo, no entanto, permanecem intactas. Se os usuários não estiverem associados a nenhum outro grupo local, eles estarão associados ao nível superior.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Na caixa de diálogo **Gerenciar grupos**, clique no grupo que você desejar 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

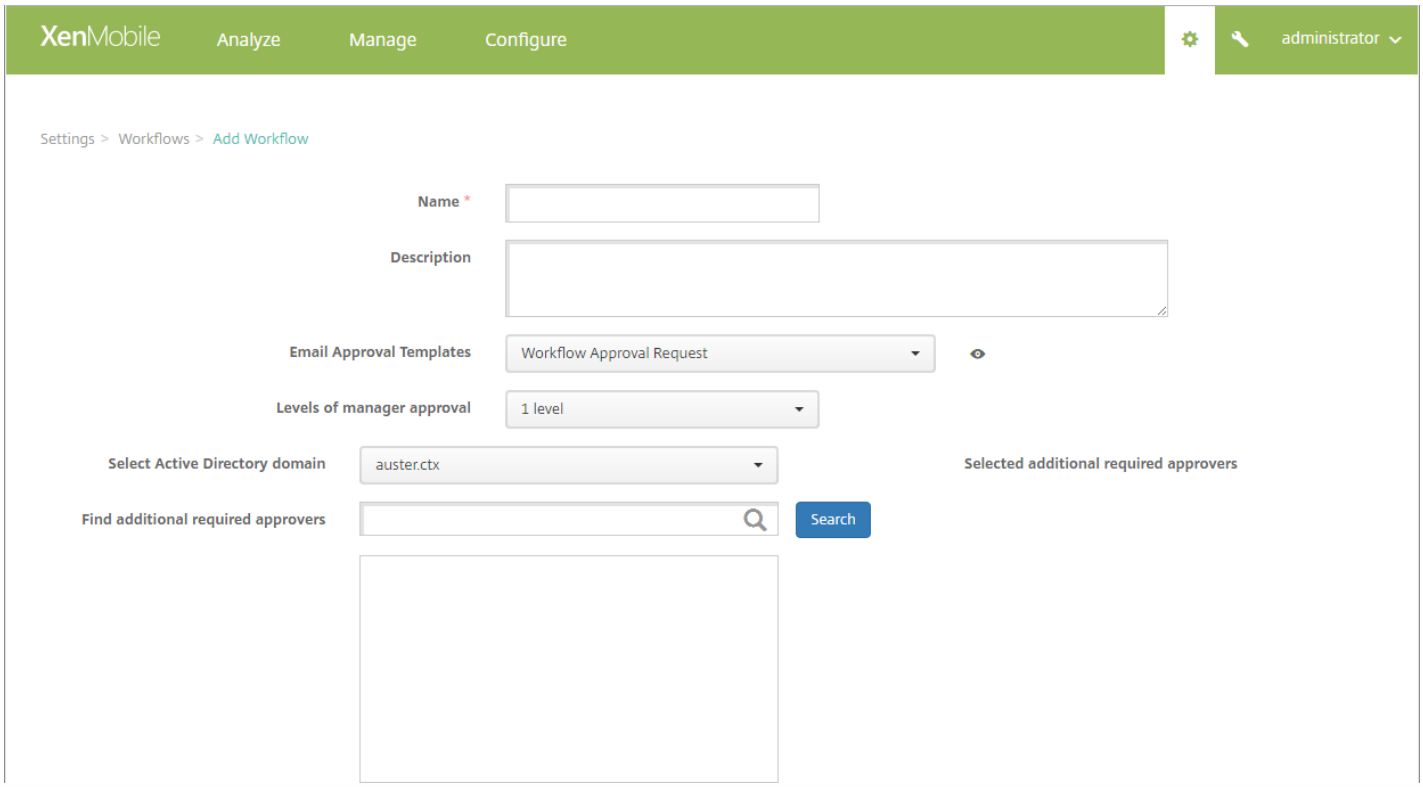
- Ao configurar um conector de aplicativo, forneça um nome de fluxo de trabalho e configure os indivíduos que podem aprovar a solicitação de conta de usuário. Para obter detalhes, consulte Adição de aplicativos ao XenMobile.

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 **Configurações** 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.



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** das **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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

    - 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 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 desejar 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 exibir os 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurar funções com RBAC

Feb 21, 2018

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 *aplicar permissões*, você define os grupos de usuários que a função RBAC tem a permissão para gerenciar. Observe que 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.

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 e Suporte Remoto), **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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

* O suporte remoto não está disponível para os clientes do XenMobile Service. 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.

Recursos do console

Os administradores têm acesso irrestrito ao console XenMobile.

Painel	O **painel** é a primeira página que os administradores veem depois de fazer login no console XenMobile. O **painel** mostra informações básicas sobre as notificações e os dispositivos.
Criação de relatórios	A página **Analisar > Relatórios** fornece relatórios predefinidos que permitem analisar as implantações de aplicativo e dispositivo.
Dispositivos	A página **Gerenciar > Dispositivos** é o local em que você gerencia os dispositivos dos usuários. Você pode adicionar dispositivos individuais na página ou importar um arquivo de provisionamento de dispositivo para adicionar vários dispositivos ao mesmo tempo.
Usuários locais e grupos	A página **Gerenciar > Dispositivos** é o local em que você pode adicionar, editar ou excluir usuários locais e grupos de usuários locais.
Registro	A página **Gerenciar > Convites de Registro** é o local em que você gerencia como os usuários são convidados para registrar seus dispositivos no XenMobile.
Políticas	A página **Configurar > Políticas de dispositivo** é o local em que você gerencia as políticas de dispositivo, como VPN e WiFi.
Aplicativos	A página **Configurar > Aplicativos** é o local em que você gerencia os vários aplicativos que os usuários podem instalar nos seus dispositivos.
Mídia	A página **Configurar > Mídia** é o local em que você gerencia as várias mídias que os usuários podem instalar nos seus dispositivos.
Ação inteligente	A página **Configurar > Ações** é o local em que você gerencia as respostas a eventos de disparo.
Perfis de registro	A página **Configurar > Perfis de registro** é o local em que você configura perfis (modos) de registro para permitir que os usuários registrem seus dispositivos.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Grupos de entrega	A página **Configurar > Grupos de Entrega** é o local em que você gerencia os grupos de entrega e os recursos associados a eles.
Configurações	A página **Configurações** é o local em que você administra as configurações do sistema, como propriedades do cliente e servidor, certificados e provedores de credenciais.
Suporte	A página **Solução de problemas e suporte** é o local em que você executa atividades de solução de problemas, como realizar 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	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 poderão fazer logon para o XenMobile de modo nenhum. No iOS, os usuários poderão continuar a fazer logon, mas elas não poderão acessar aplicativos.
Apagamento de aplicativos	No Android, esta opção exclui a conta do XenMobile. No iOS, essa opção 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	Na página Gerenciar, em dispositivos, você pode colocar um dispositivo

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	supervisionado no modo perdido para bloquear um dispositivo supervisionado na tela de bloqueio e localize o dispositivo quando o dispositivo seja perdido ou roubado.
Desativar o modo perdido	Na página Gerenciar dispositivos, você pode desativar o modo perdido para um dispositivo está configurado para 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/excluir usuários locais
Editar usuários locais
Importar usuários locais
Exportar usuários locais
Grupos de usuários locais

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 de loja de aplicativos pública ou um aplicativo não preparado com o MDX Toolkit.
Editar loja de aplicativos ou aplicativo empresarial	Fazer alterações em um aplicativo de loja de aplicativos pública ou um aplicativo não preparado com o MDX Toolkit.
Adicionar/excluir aplicativo MDX, Web e SaaS	Adicionar ou remover um aplicativo preparado com o MDX Toolkit (aplicativo MDX), um aplicativo da sua rede interna (aplicativo Web) ou um aplicativo de uma rede pública (SaaS) ao XenMobile.
Editar aplicativo MDX, Web e SaaS	Fazer alterações em um aplicativo preparado com o MDX Toolkit (aplicativo MDX), um aplicativo da sua rede interna (aplicativo Web) ou um aplicativo de uma rede pública (SaaS) ao XenMobile.
Adicionar/excluir categoria	Adicionar ou excluir uma categoria na qual os aplicativos podem aparecer no XenMobile Store.
Atribuir aplicativo público/empresarial ao	Atribuir um aplicativo de loja de aplicativos pública ou um aplicativo não

© 1999-2017 Citrix Systems, Inc. All rights reserved.

grupo de entrega	preparado com o MDX Toolkit a um grupo de entrega para implantação.
Atribuir aplicativo MDX/WebLink/SaaS ao grupo de entrega	Atribuir um aplicativo preparado com o MDX Toolkit (aplicativo MDX), um aplicativo que não exige logon único (WebLink) ou um aplicativo de uma rede pública (SaaS) a um grupo de entrega para implantação nos dispositivos do usuário.
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 VPP.

Adicionar/excluir loja de aplicativos ou livros empresariais
Atribuir livros públicos/empresariais ao grupo de entrega
Editar loja de aplicativos ou livros empresariais

Ação inteligente

Adicionar/excluir ação inteligente	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 inteligente	Alterar uma ação definida por um gatilho (evento, propriedade do dispositivo ou usuário, ou nome do aplicativo instalado) e a resposta associada.
Atribuir ação inteligente ao grupo de entrega	Atribuir uma ação a um grupo de entrega para implantação nos dispositivos do usuário.
Exportar ação inteligente	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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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
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 registro dos usuários, bem como 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	Crie 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	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, a expiração e assim por diante.
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 um logotipo personalizado para ser 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.
Credenciais do Google Play	Configurar o nome do usuário, a senha e o ID de dispositivo para permitir o acesso ao Google Play.
Device Enrollment Program (DEP) da Apple	Adicione uma conta do Apple DEP ao XenMobile.
Registro de dispositivo do Apple Configurator	Definir configurações do Apple Configurator no XenMobile.
Configurações iOS/VPP	Adicionar contas do Apple Volume Purchase Program.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.
NetScaler Gateway	Para o XenMobile Server local. Adicionar um NetScaler Gateway. Escolha se deseja ativar a autenticação e se deseja enviar o 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 (syslog) de logs do sistema usando o nome de host ou o endereço IP do servidor.
XenApp/XenDesktop	Permitir que os usuários adicionem XenApp e XenDesktop via Secure Hub.
ShareFile	Ao usar o XenMobile com ShareFile Enterprise: defina configurações para conexão com a conta do ShareFile e a conta de serviço do administrador para gerenciar contas de usuário. Exige um domínio do ShareFile existente e credenciais de administrador. Ao usar o XenMobile com Conectores do StorageZone: configure o XenMobile para apontar para compartilhamentos de rede e SharePoint locais definidos nos Conectores do ShareFile StorageZones.
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 for Work	Definir as configurações de servidor do Android for Work.
Provedor de identidade (IDP)	Configure um provedor de identidade.
Credenciais derivadas	Configure credenciais derivadas para o registro de dispositivo iOS.
XenMobile Tools	Acesse a página do XenMobile Tools.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 NetScaler Gateway	Executar várias verificações de conectividade do NetScaler 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, o Google Plan e assim por diante.
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 NetScaler 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	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 de dispositivo NetScaler Connector	Consulta o XenMobile para obter o status de um dispositivo conforme enviado para o XenMobile NetScaler Connector 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 na página Anonimização e desanonimização e, Suporte, sob 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

> **Important**
>
> A Função de Provisionamento do Dispositivo se aplica somente aos dispositivos Windows CE.

Os usuários com a função de provisionamento do dispositivo predefinida têm acesso limitado aos recursos do console; Por padrão, sua permissão é definida como todos os grupos de usuários e 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Adicionar/excluir dispositivo	Adicionar ou remover dispositivos no XenMobile.

Configurações

Os usuários de provisionamento do dispositivo pode acessar o **configurações** página, mas não tenha os direitos para configurar os recursos.

Função de suporte

Os usuários com a função de suporte têm acesso ao suporte remoto; as permissões se aplicam a todos os usuários por padrão e 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 dispositivo para os dispositivos Windows CE.
- **Suporte**. Concede acesso para suporte remoto.
- **Usuário**. Usado pelos usuários que podem registrar dispositivos e acessar o Portal de Autoajuda.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Você também pode usar as funções padrão como modelos que podem ser personalizados para criar novas funções de usuário com permissões para acessar funções do sistema específicas 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, se os usuários de ADGroupA podem localizar dispositivos de gerente e os usuários de ADGroupB podem apagar dispositivos de funcionário, um usuário que pertence a ambos os grupos pode localizar e apagar os dispositivos de gerentes e funcionários.

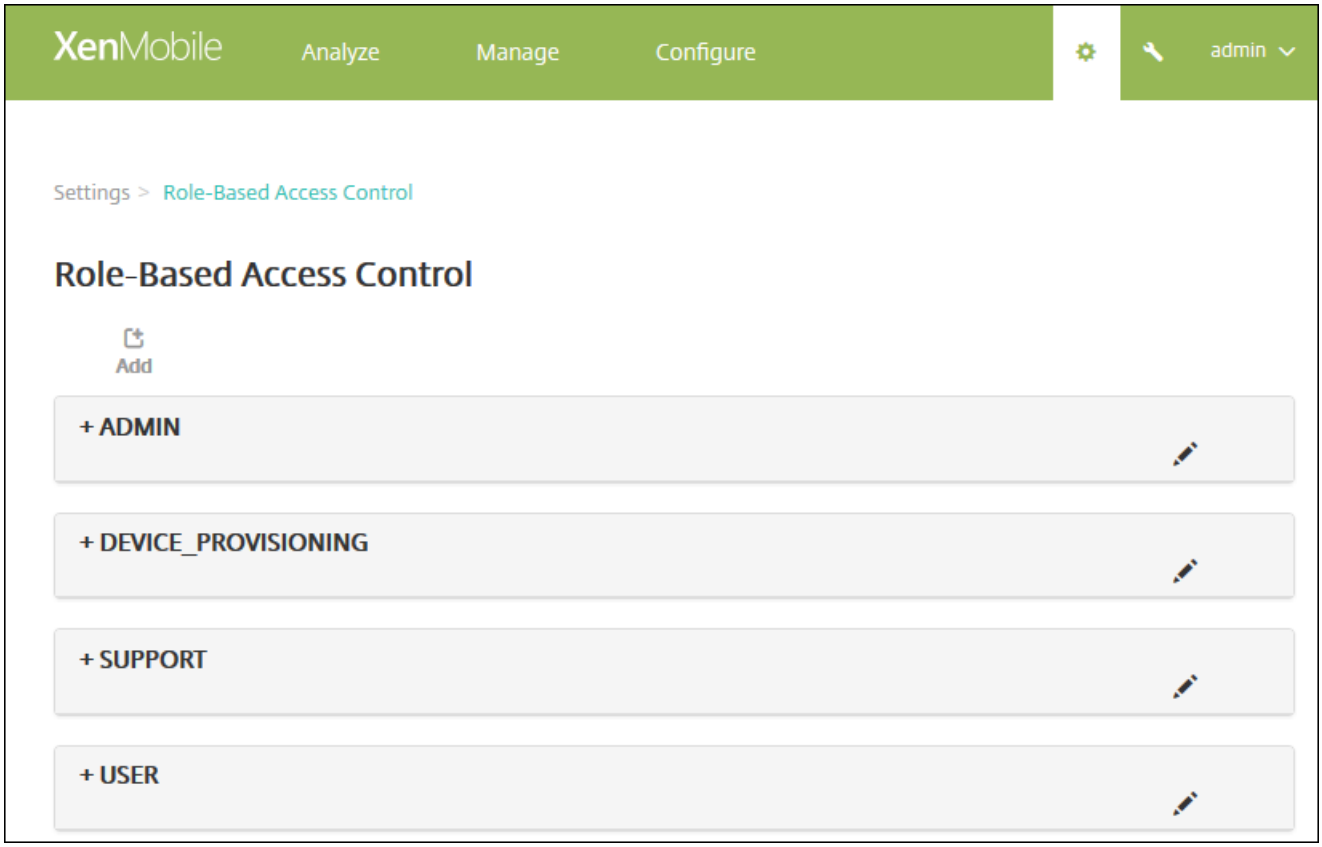
Observação: os usuários locais podem ter somente uma função atribuída a eles.

Você pode usar o recurso RBAC no XenMobile para fazer o seguinte:

- Criar uma nova função.
- Adicionar grupos a uma função.
- Associar os usuários locais a funções.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.

2. Clique em **Controle de acesso baseado em função**. É exibida a página **Controle de acesso baseado em função** que mostra as quatro funções do usuário padrão, além de todas 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

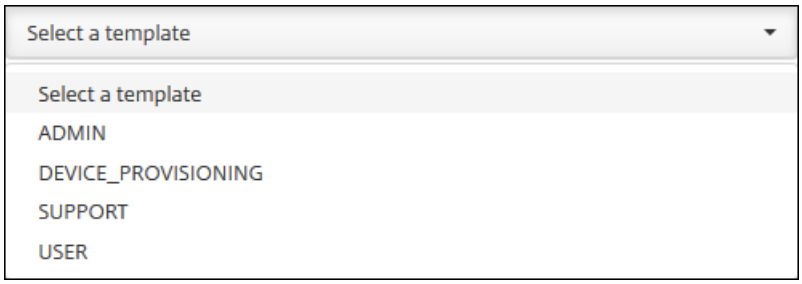
3. Clique em **Adicionar** para adicionar uma nova função do usuário, clique no ícone de caneta à direita de uma função existente para editá-la ou clique no ícone de lixeira à direita de uma função definida anteriormente para excluí-la. Você não pode excluir as funções do usuário padrão.

- 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.

4. Insira as seguintes informações para criar uma nova função do usuário ou para editar uma função do usuário existente:

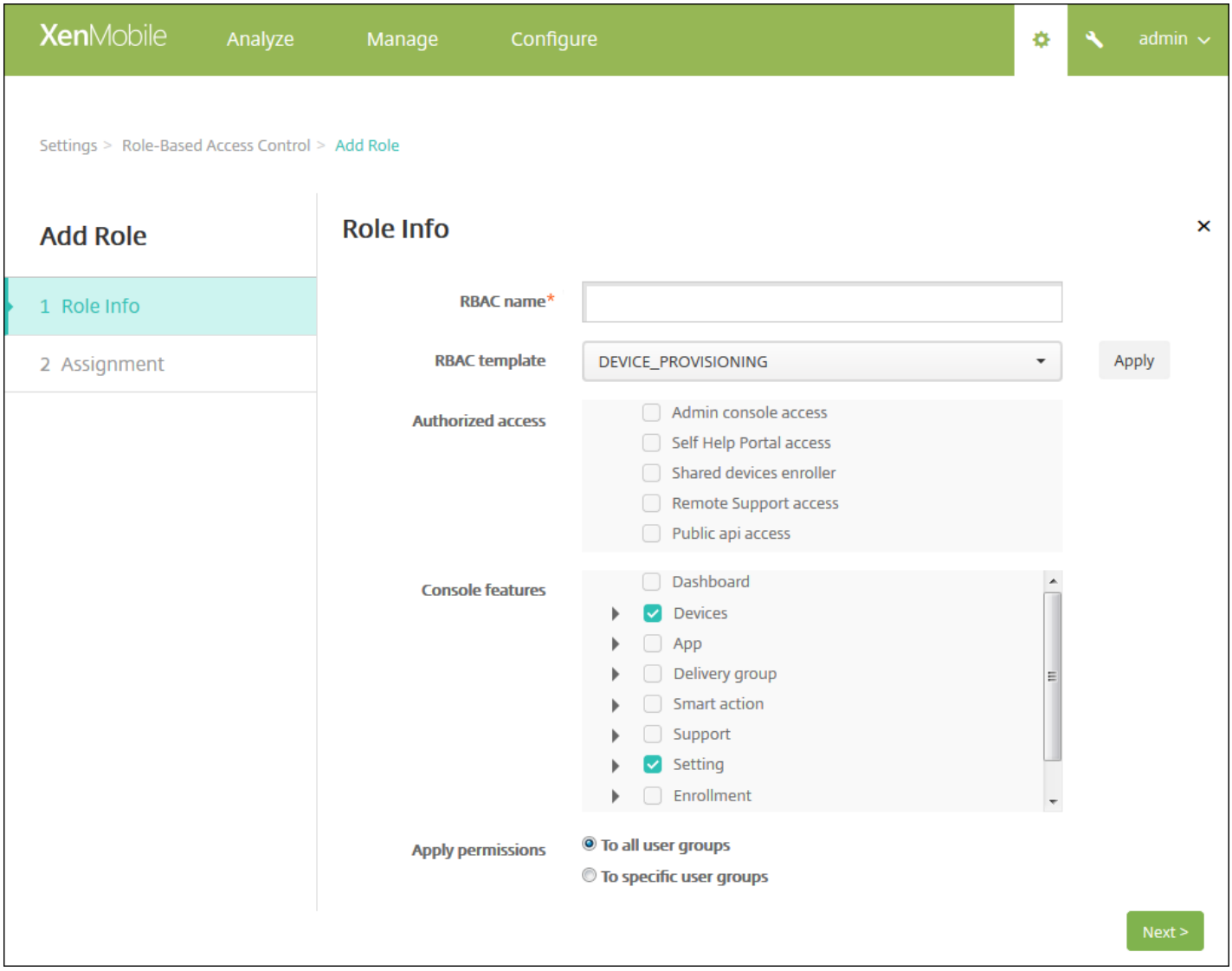
- **Nome RBAC**: digite um nome descritivo para a nova função do usuário. Você não pode alterar o nome de uma função existente.
- **Modelo RBAC**: opcionalmente, clique em um modelo como o ponto de partida para a nova função. Você não poderá selecionar um modelo se estiver editando uma função existente.

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**. Usar um modelo é opcional; você pode selecionar diretamente as opções que desejar atribuir a uma função nos campos **Acesso autorizado** e **Recursos do console**.



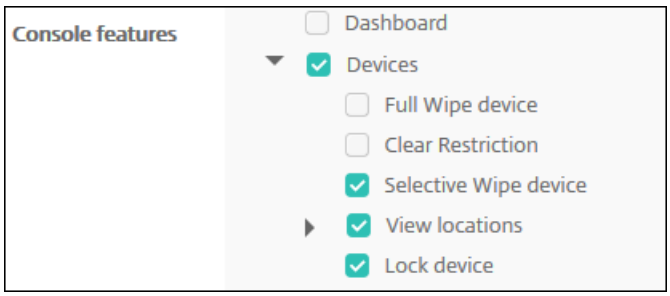
5. Clique em **Aplicar** à direita do campo **Modelo RBAC** para preencher as caixas de seleção **Acesso autorizado** e **Recursos do console** com as permissões de acesso e recurso predefinidas para o modelo selecionado.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



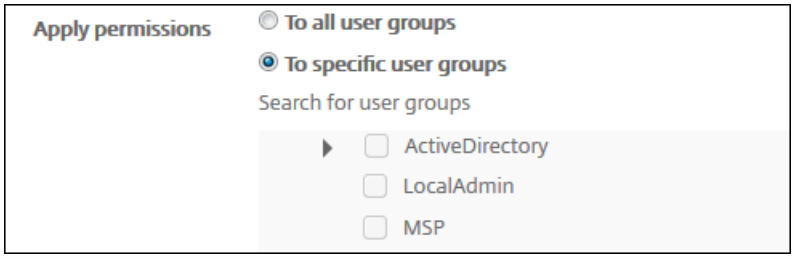
6. Marque e desmarque as caixas de seleção em **Acesso autorizado** e **Recursos do console** para personalizar a função.

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 parte do console; você deve selecionar as opções individuais abaixo do nível superior para ativá-las. Por exemplo, na figura a seguir, as opções **Apagamento completo do dispositivo** e **Limpar restrições** não são exibidas no console para os usuários atribuídos à função, mas as opções marcadas são exibidas.

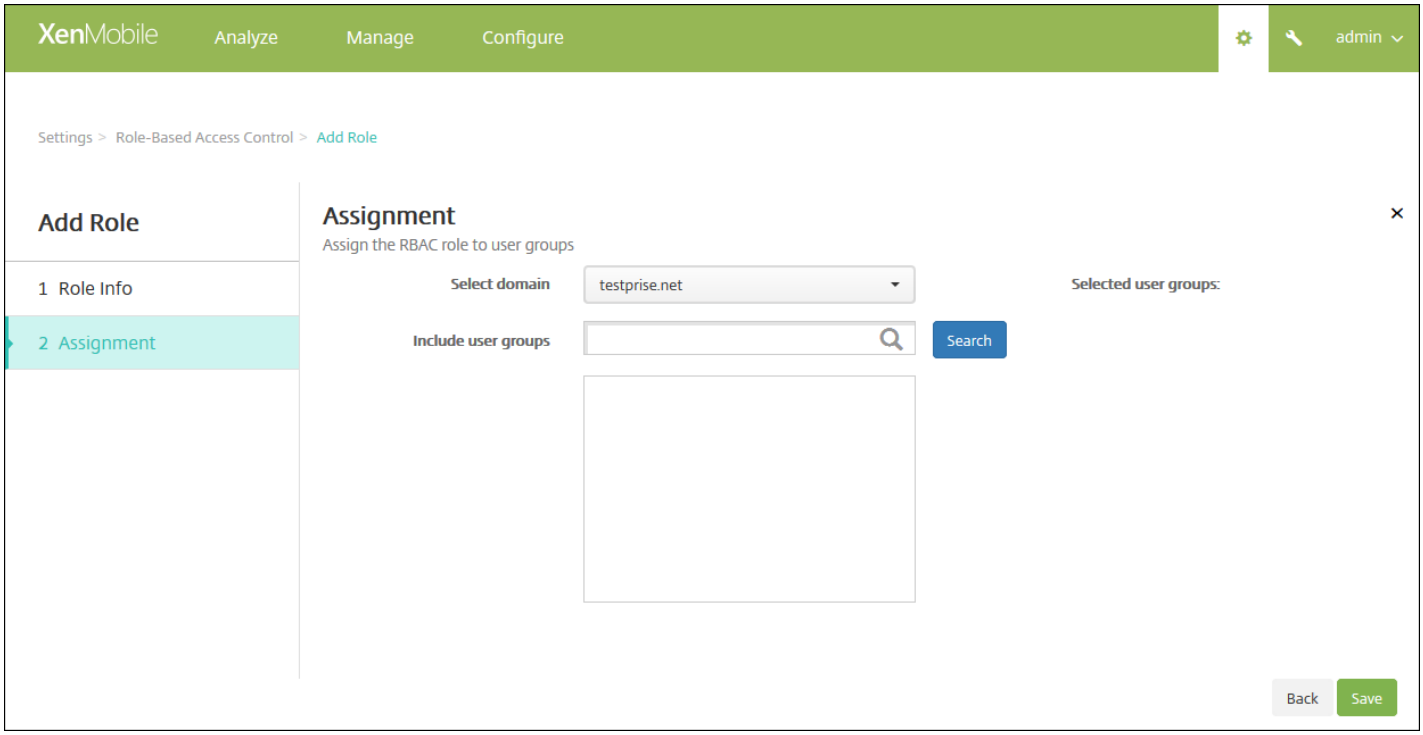


7. **Aplicar permissões**: selecione os grupos aos quais você deseja aplicar as permissões selecionadas. Se você clicar em **Para grupos de usuários específicos**, será exibida uma lista de grupos na qual você pode selecionar um ou mais grupos.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



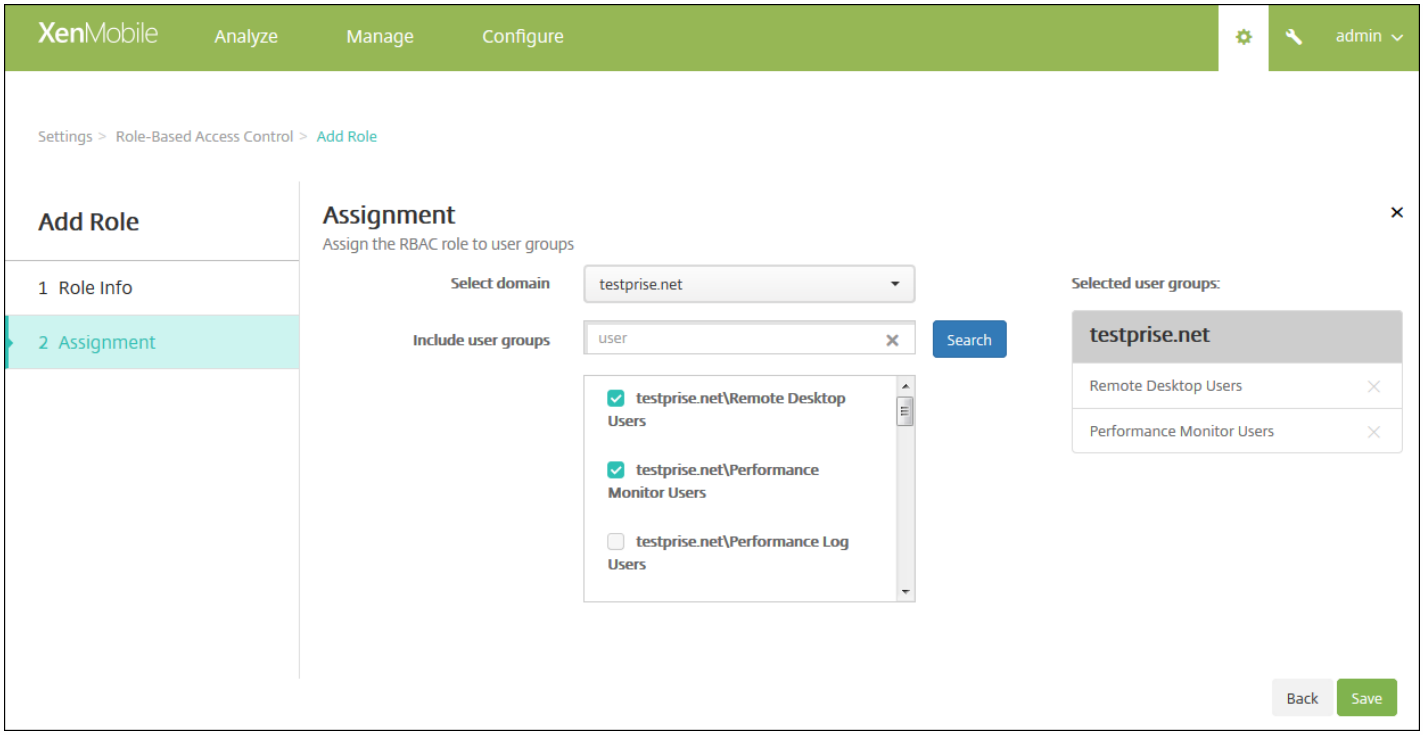
8. Clique em **Avançar**. A página **Atribuições** é exibida.



9. 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, ele é exibido na lista **Grupos de usuários selecionados**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Observação: para remover um grupo de usuários da lista **Grupos de usuários selecionados**, clique no X ao lado do nome do grupo de usuários.

10. Clique em **Salvar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Notificações

Feb 21, 2018

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.

Este artigo explica como:

Adicionar servidor SMTP

Adicionar um gateway SMS

Adicionar um gateway SMS de operadora

Criar e atualizar modelos de notificação

Pré-requisitos

- Antes de configurar o gateway de SMS, consulte o administrador do sistema para determinar as informações do servidor.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

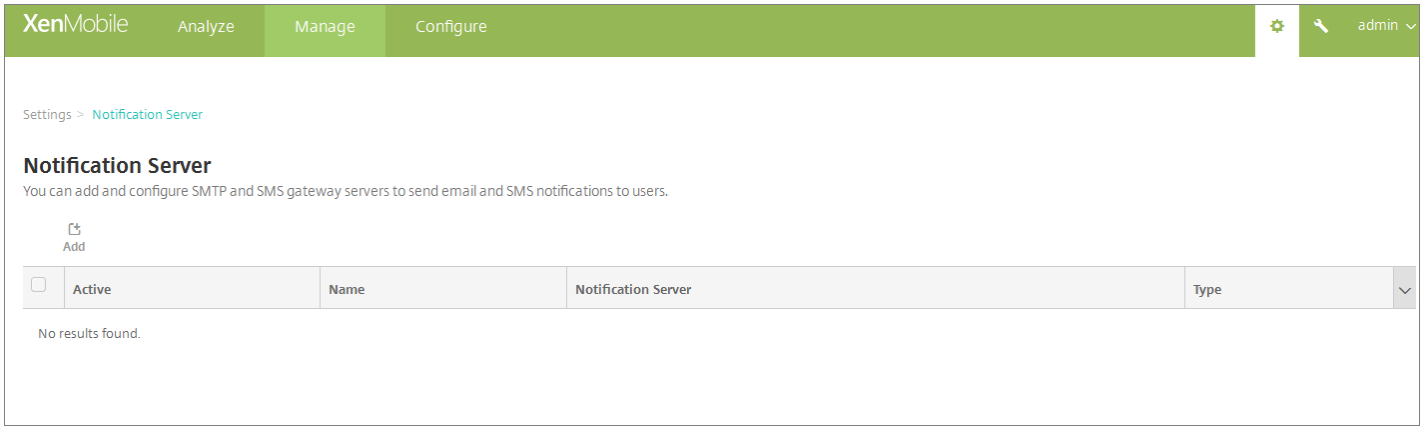
É importante saber se o servidor SMS está hospedado em um servidor corporativo interno ou se ele faz parte de um serviço de email hospedado. Nesse caso, você precisa de informações do site do provedor de serviços.

- 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.
- Somente um servidor SMTP e somente um servidor SMS estão ativos por vez.
- 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 **Configurações** é exibida.

2. Em **Notificações**, clique em **Servidor de notificação**. A página **Servidor de notificação** é exibida.

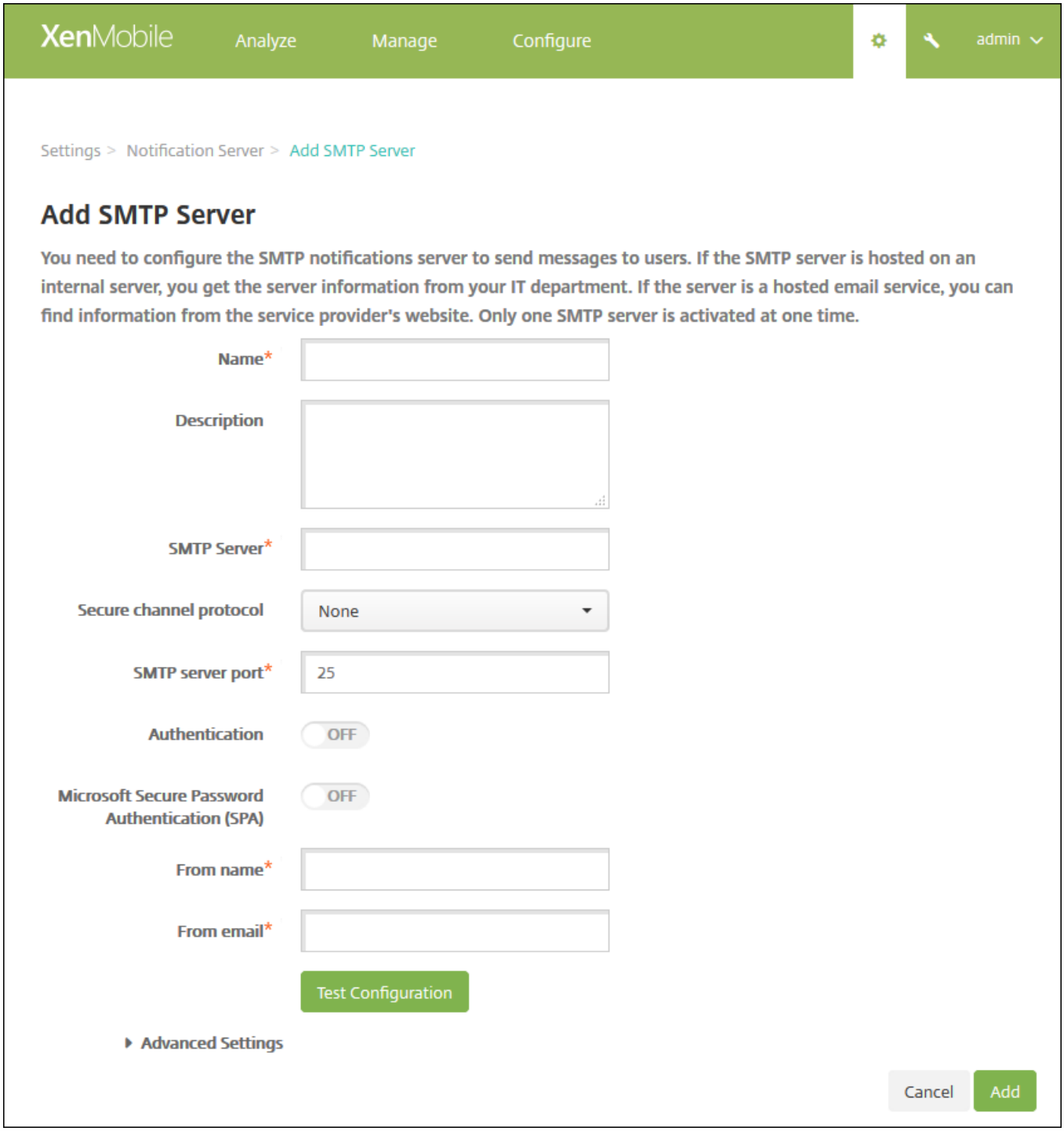


2. Clique em **Adicionar**. Um menu é exibido com as opções para configurar um servidor SMTP ou um gateway de SMS.

- Para adicionar um servidor SMTP, clique em **Servidor SMTP** e, em seguida, consulte Para adicionar um servidor SMTP para obter 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 conhecer as etapas para definir essa configuração.

Adicionar um servidor SMTP

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Se você ativar **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.

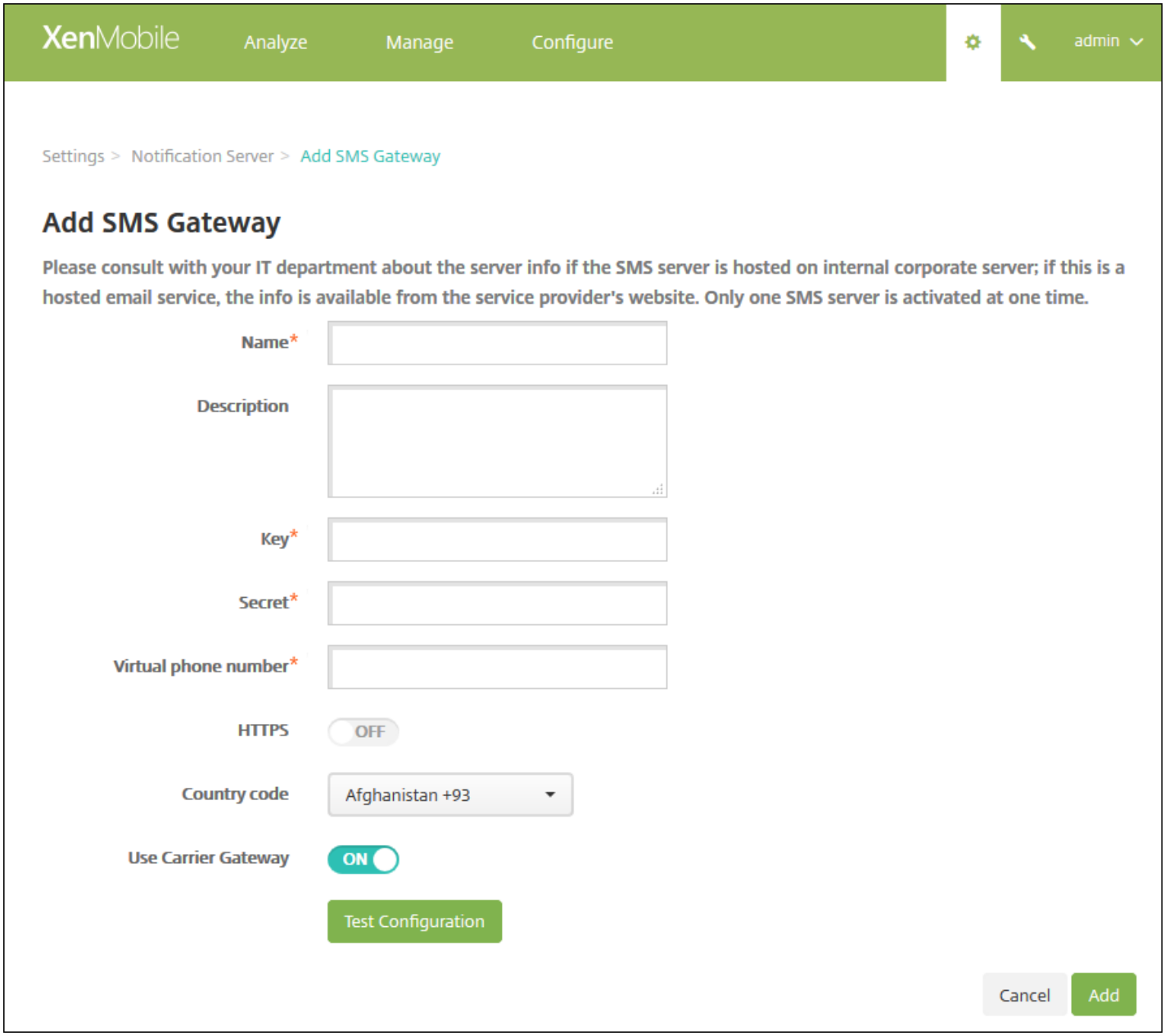
3. Expanda **Configurações avançadas** e defina estas configurações:

- **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

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 da empresa 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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 da 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 **Afeganistão +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.

2. Clique em **Adicionar**.

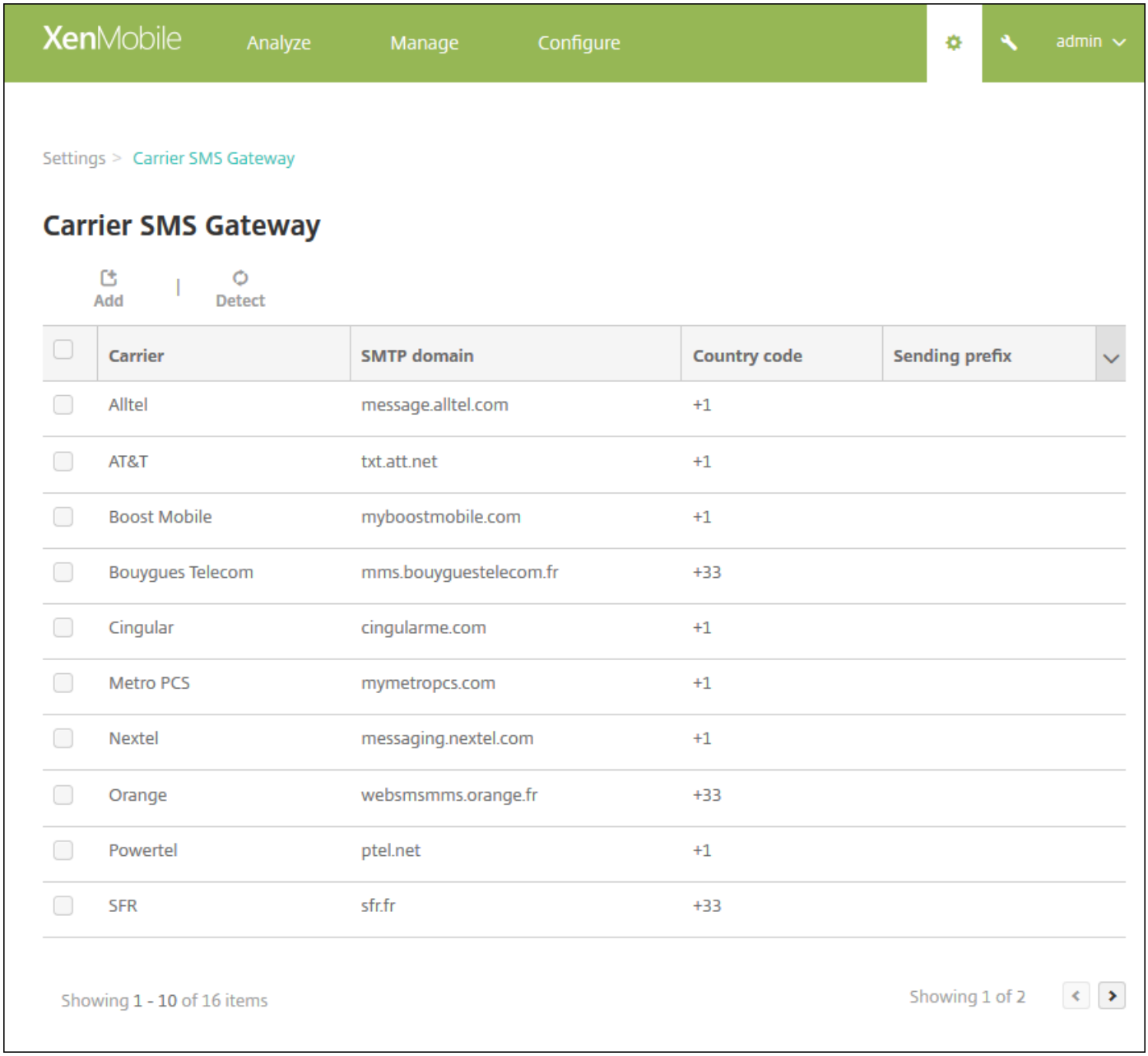
Adicionar um gateway de SMS de operadora

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 **Configurações** é exibida.

2. Em **Notificações**, clique em **Gateway de SMS da operadora**. A página **Gateway de SMS da operadora** é exibida.

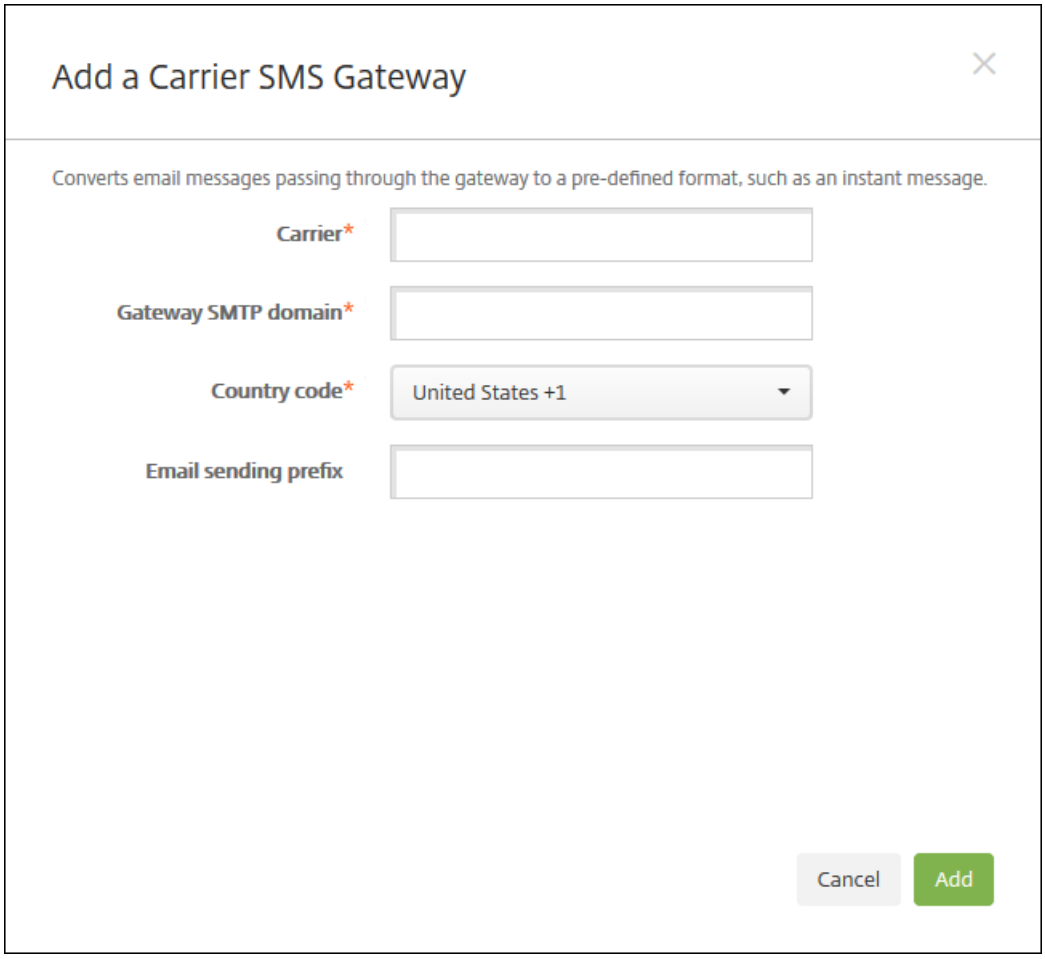
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 SMS de operadora** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 da empresa para criar uma.

4. Defina estas configurações:

- **Operadora**: digite o nome da operadora.
- **Domínio SMTP de gateway**: digite o domínio associado ao gateway 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.

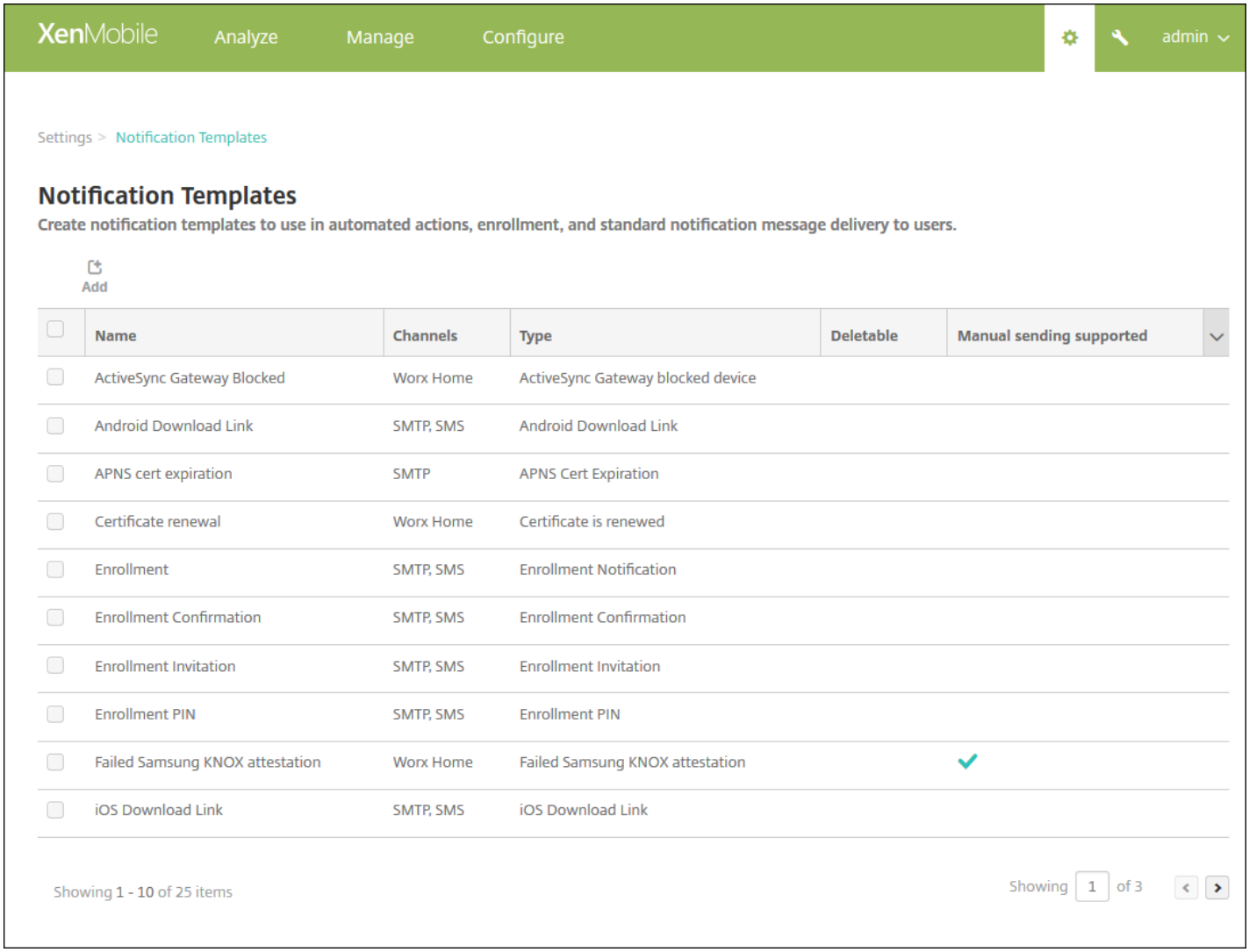
Nota: se planejar usar canais SMTP ou SMS para enviar notificações aos usuários, você deverá configurar os canais antes que possa ativá-los. O XenMobile solicita que você configure os canais ao adicionar modelos de notificação, se eles já não

© 1999-2017 Citrix Systems, Inc. All rights reserved.

estiverem configurados.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.

2. Clique em **Modelos de notificação**. A página **Modelos de notificação** é exibida.



Adicionar um 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.

> ## Important
>
> 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 "Há 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)}
- ${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.

  Importante: Você poderá ativar a notificação SMTP somente se já tiver configurado 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

mensagem, consulte Macros.

SMS :

- **Ativar**: Clique para ativar o canal de notificação.

  Importante: você poderá ativar a notificação SMS somente se já tiver configurado o gateway de SMS.

- **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.

5. Clique em **Adicionar**. Quando todos os canais estiverem corretamente configurados, eles serão exibidos nessa 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

Nota: você pode excluir somente os modelos de notificação que adicionou; não é possível excluir os modelos de notificação predefinidos.

1. Selecione um modelo de notificação existente.

2. Clique em **Excluir**. Uma caixa de diálogo de confirmação é exibida.

2. Clique em **Excluir** para excluir o modelo de notificação ou em **Cancelar** para cancelar a exclusão.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Dispositivos

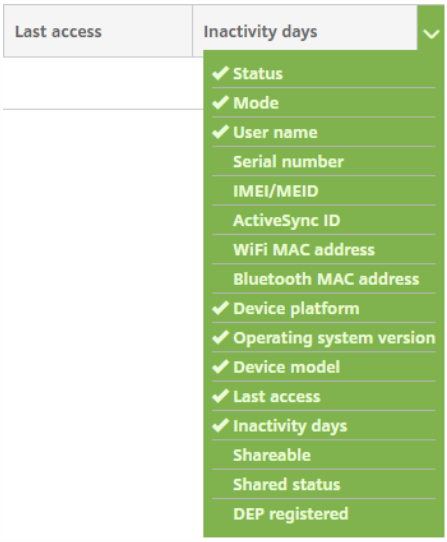
Feb 21, 2018

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. Consulte Formatos de arquivo de provisionamento do dispositivo para obter mais informações sobre os formatos de arquivo de provisionamento de dispositivo.

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.



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.

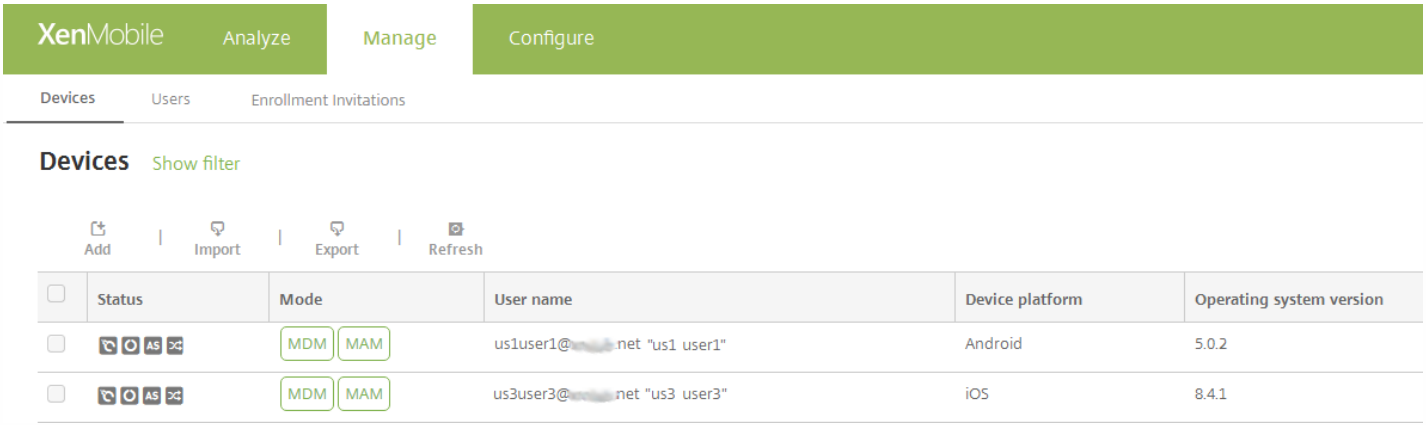
Consulte as seções a seguir para obter detalhes sobre como gerenciar dispositivos:

- Adicionar um dispositivo manualmente
- Importar dispositivos de um arquivo de provisionamento de dispositivo
- Executar ações de segurança
- Enviar uma notificação para dispositivos
- Exportar a tabela Dispositivos
- Marcar os dispositivos de usuário manualmente
- Formatos de arquivo de provisionamento do dispositivo
- Nomes de propriedade do dispositivo e os valores

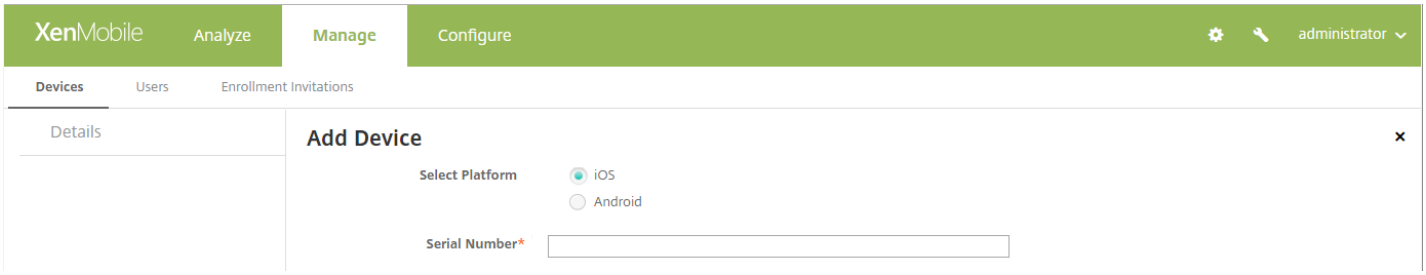
Adicionar um dispositivo manualmente

1. No console XenMobile, clique em **Gerenciar > Dispositivos**. A página **Dispositivos** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Clique em **Adicionar**. A página **Adicionar dispositivo** é exibida.



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.

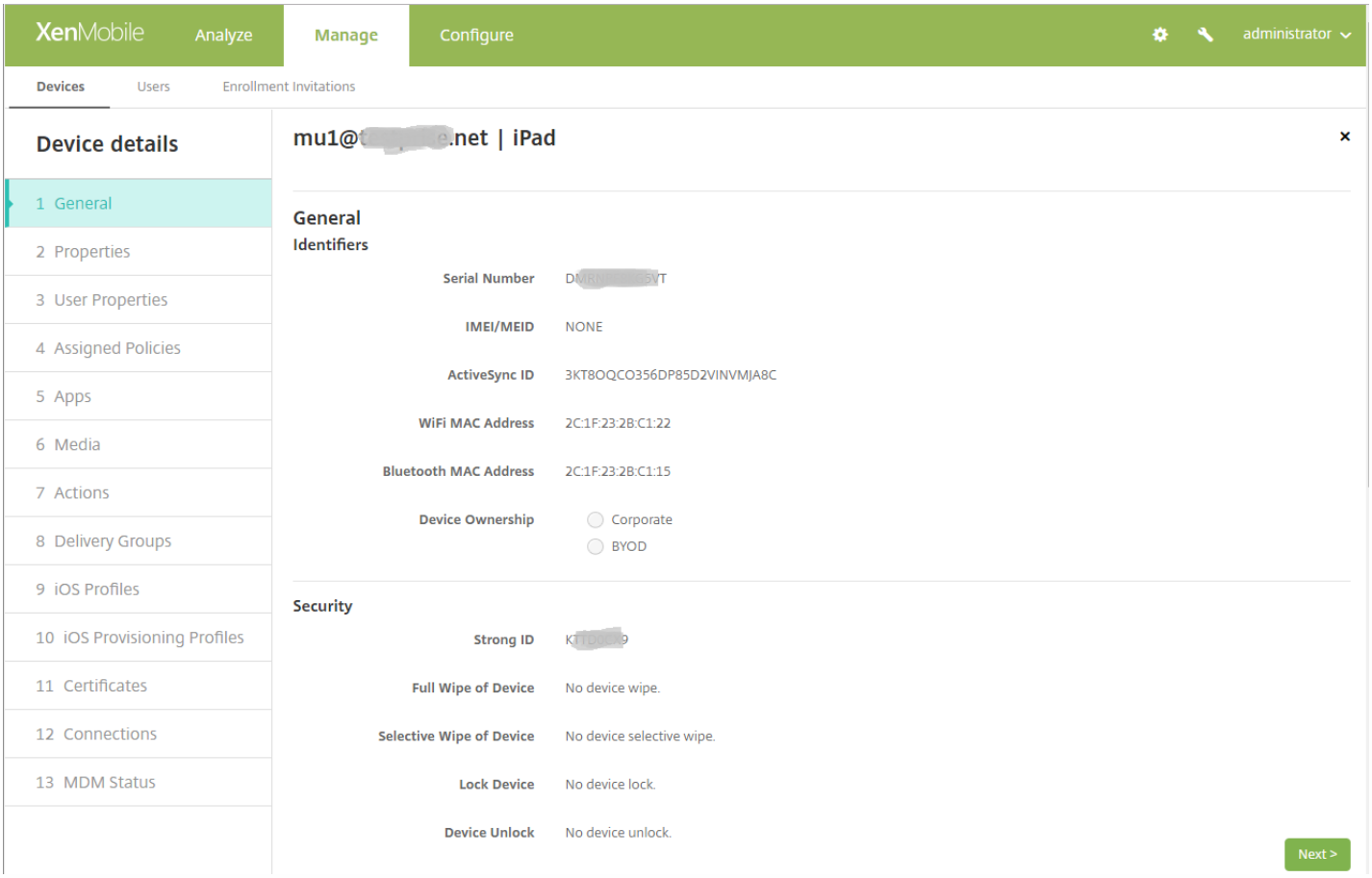
4. Clique em **Adicionar**. A tabela **Dispositivos** é exibida com o dispositivo adicionado à parte inferior da lista. Escolha o dispositivo que você adicionou e, no menu exibido, clique em **Editar** para exibir e confirmar os detalhes do dispositivo.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 os valores válidos para cada propriedade, consulte Nomes de propriedade do dispositivo e os valores neste artigo.

Quando você adicionar uma propriedade, ela inicialmente aparece na categoria em que você adicionou. Depois de clicar em **Avançar** e, em seguida, volte 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. O restante **detalhes do dispositivo** seções contêm informações resumidas para o dispositivo.

- **Propriedades do usuário:** exibe funções RBAC, associações de grupo, contas VPP e propriedades do usuário. Você pode desativar uma conta VPP nessa 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

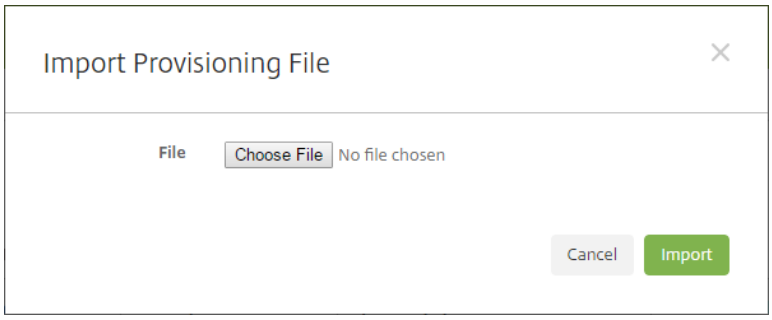
restantes antes da expiração.

- **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.
- **TouchDown** (somente dispositivos Android): Exibe informações sobre a última autenticação de dispositivo e do último usuário autenticado. Fornece o nome de cada política aplicável valor da política.

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 mais informações, consulte Formatos de arquivo de provisionamento de dispositivo neste artigo.

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 **Devices** contém o arquivo importado.

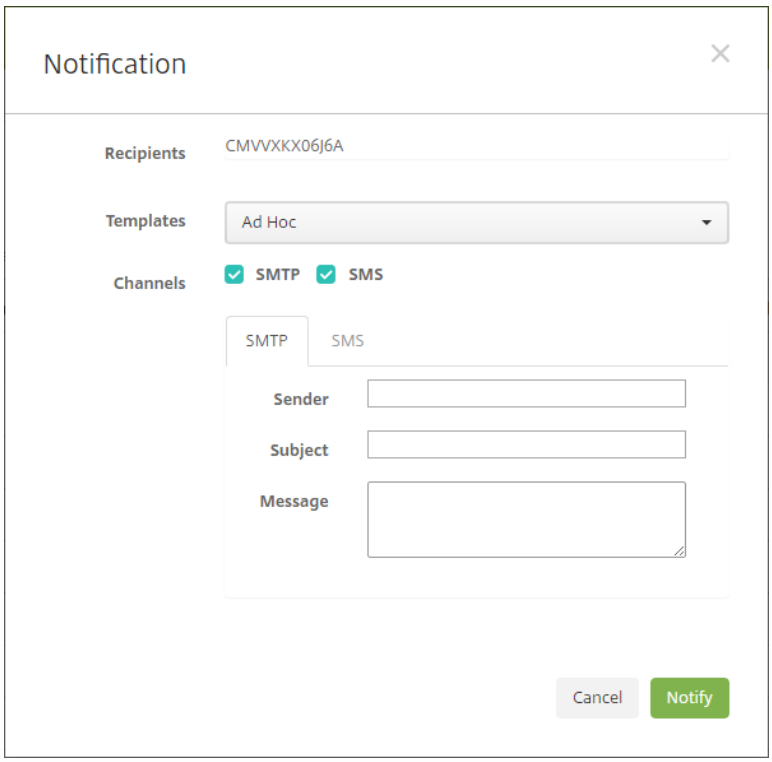
4. Para editar as informações do dispositivo, selecione-o e, em seguida, clique em **Editar** . Para obter informações sobre o **detalhes do dispositivo** páginas, consulte Adicionar um dispositivo manualmente .

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.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

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. Filtro a **dispositivos** tabela de acordo com as quais você deseja exibir no arquivo de exportação.

2. Clique no botão **Exportar** acima da tabela **Dispositivos**. O XenMobile extrai as informações na tabela **Dispositivos** e converte-as em um arquivo .csv.

3. Quando avisado, abra ou salve o arquivo .csv.

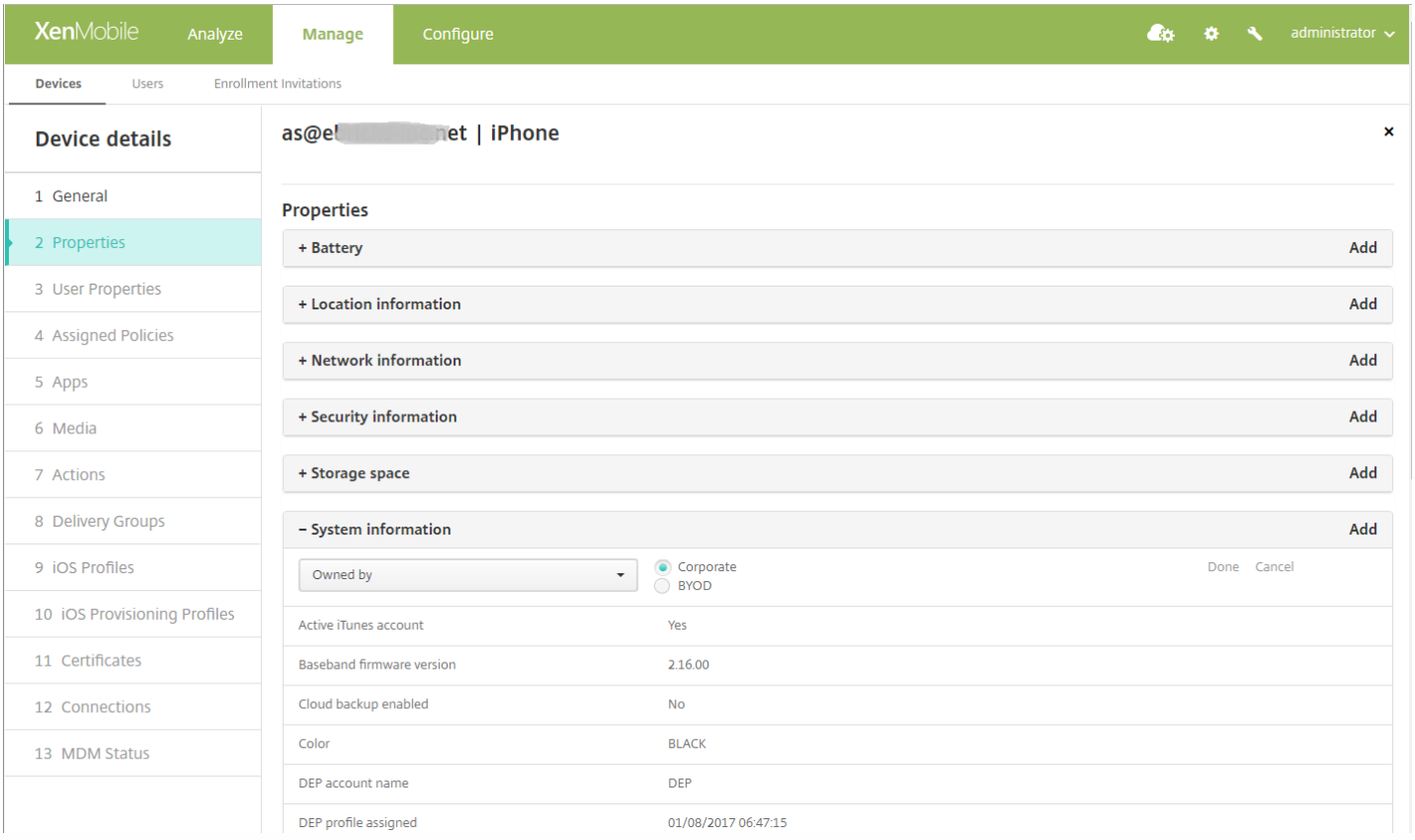
Marcar os dispositivos de usuário manualmente

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 na guia **Dispositivos** no console XenMobile.
2. Adicione a propriedade chamada **Pertencentes a** e escolha **Corporativo** ou **BYOD** (propriedade do funcionário).



Formatos de arquivo de provisionamento do dispositivo

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

Observações:

- Para nomes e valores, consulte "nomes de propriedade do dispositivo e os valores" na próxima seção.
- 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

  Utilize barras invertidas 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 COPIAR

```
1050BF3F5173010816100655105903 91;15244201625379901;WINDOWS;propertyN;propertyV\;test\;1\;2;prop 2

2050BF3F5173010816100655105903 92;25244201625379902;ANDROID;propertyN;propertyV$*&&éééétest

3050BF3F5173010816100655105903 93;35244201625379903;iOS;test;

4050BF3F5173010816100655105903 93;;iOS;test;

;55244201625379903;ANDROID;test.testé;value;
```

Cada linha no arquivo descreve um dispositivo. A primeira entrada no exemplo acima significa o seguinte:

- SerialNumber: 1050BF3F51730108161006551059039 1
- IMEI: 15244201625379901
- OperatingSystemFamily: WINDOWS
- PropertyName: propertyN
- PropertyValue: propertyV\;test\;1\;2;prop 2

Nomes de propriedade do dispositivo e os valores

Nome da propriedade na página Gerenciar > Dispositivos	Nome e valores para o arquivo de provisionamento do dispositivo	Valores (significado)	Tipo de valor
AIK presente?	WINDOWS_HAS_AIK_PRESENT		Cadeia de caracteres
Conta suspensa?	GOOGLE_AW_DIRECTORY_SUSPENDED		Cadeia de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

			caracteres
Código de desvio do bloqueio de ativação	ACTIVATION_LOCK_BYPASS_CODE		Cadeia de caracteres
Bloqueio de ativação ativado	ACTIVATION_LOCK_ENABLED	1 (Sim), 0 (Não)	Booliana
Conta do iTunes Active	ACTIVE_ITUNES	1 (Sim), 0 (Não)	Booliana
ID do ActiveSync	EXCHANGE_ACTIVESYNC_ID		Cadeia de caracteres
Dispositivo ActiveSync conhecido por MSP	AS_DEVICE_KNOWN_BY_ZMSP	1 (Verdadeiro), 0 (Falso)	Booliana
Administrador desativado	ADMIN_DISABLED	1 (Sim), 0 (Não)	Booliana
API do MDM Amazon disponível	AMAZON_MDM	1 (Verdadeiro), 0 (Falso)	Booliana
ID de dispositivo do Android for Work	GOOGLE_AW_DEVICE_ID		Cadeia de caracteres
Dispositivo Android for Work ativado?	GOOGLE_AW_ENABLED_DEVICE		Cadeia de caracteres
Android para o tipo de instalação de trabalho	GOOGLE_AW_INSTALL_TYPE	DeviceAdministrator (proprietário do dispositivo), AvengerManagedProfile (dispositivo gerenciado de trabalho), ManagedProfile (perfil de trabalho)	Cadeia de caracteres
Status da assinatura antispyware (Windows 10)	ANTI_SPYWARE_SIGNATURE_STATUS		Booliana
Status do antispyware (Windows 10)	ANTI_SPYWARE_STATUS		Booliana
Status da assinatura antivírus (Windows 10)	ANTI_VIRUS_SIGNATURE_STATUS	Not recent version, Most recent version. N/D	Cadeia de caracteres
Status do antivírus (Windows 10)	ANTI_VIRUS_STATUS	ON and monitoring, Disabled, OFF or not monitoring, Temporarily not monitoring, N/A	Cadeia de caracteres
Marca do recurso	ASSET_TAG		Cadeia de caracteres

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Status de atualização automática	AUTOUPDATE_STATUS		Cadeia de caracteres
RAM disponível	MEMORY_AVAILABLE		Inteiro
Espaço de armazenamento disponível	TOTAL_DISK_SPACE		Inteiro
Informações de BIOS	BIOS_INFO		Cadeia de caracteres
Bateria de backup	BACKUP_BATTERY_PERCENT		Inteiro
Versão de firmware banda básica	MODEM_FIRMWARE_VERSION		Cadeia de caracteres
Status da bateria	BATTERY_STATUS		Cadeia de caracteres
Bateria carregando (telefone Windows 8.1)	BATTERY_CHARGING	1 (Verdadeiro), 0 (Falso)	Booliana
Bateria carregando (Windows 10)	BATTERY_CHARGING_STATUS	1 (Verdadeiro), 0 (Falso)	Booliana
Bateria restante (Windows 10)	BATTERY_ESTIMATED_CHARGE_REMAINING		Inteiro
Dispositivo de BES conhecido por MSP	BES_DEVICE_KNOWN_BY_ZMSP	1 (Verdadeiro), 0 (Falso)	Booliana
PIN DO BES	BES_PIN		Cadeia de caracteres
ID do BES servidor agente	ENROLLMENT_AGENT_ID		Cadeia de caracteres
Nome do servidor BES	BES_SERVER		Cadeia de caracteres
Versão do servidor BES	BES_VERSION		Cadeia de caracteres
Status de Bit Locker	WINDOWS_HAS_BIT_LOCKER_STATUS		Cadeia de caracteres
Endereço MAC Bluetooth	BLUETOOTH_MAC		Cadeia de caracteres
Depuração de inicialização ativada?	WINDOWS_HAS_BOOT_DEBUGGING_ENABLED		Cadeia de caracteres

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Versão da lista de revisões do Gerenciador de inicialização	WINDOWS_HAS_BOOT_MGR_REV_LIST_VERSION		Cadeia de caracteres
Código da operadora	CARRIER_CODE		Cadeia de caracteres
Versão de configurações de operadora	CARRIER_SETTINGS_VERSION		Cadeia de caracteres
Latitude celular	GPS_LATITUDE_FROM_CELLULAR		Cadeia de caracteres
Longitude da rede celular	GPS_LONGITUDE_FROM_CELLULAR		Cadeia de caracteres
Tecnologia celular	CELLULAR_TECHNOLOGY		Inteiro
Timestamp celular	GPS_TIMESTAMP_FROM_CELLULAR		Data
Alterar a senha no próximo Login?	GOOGLE_AW_DIRECTORY_CHANGE_PASSWORD_NEXT_LOGIN		Cadeia de caracteres
ID de dispositivo de cliente	CLIENT_DEVICE_ID		Cadeia de caracteres
Backup de nuvem ativado	CLOUD_BACKUP_ENABLED	1 (Sim), 0 (Não)	Booliana
Integridade do código ativada?	WINDOWS_HAS_CODE_INTEGRITY_ENABLED		Cadeia de caracteres
Versão da lista de revisões de integridade do código	WINDOWS_HAS_CODE_INTGTY_REV_LIST_VERSION		Cadeia de caracteres
Cor	COR		Cadeia de caracteres
Velocidade de CPU	CPU_CLOCK_SPEED		Inteiro
Tipo de CPU	CPU_TYPE		Cadeia de caracteres
Criação de regras	GOOGLE_AW_DIRECTORY_CREATION_TIME		Cadeia de caracteres
Rede da operadora atual	CURRENT_CARRIER_NETWORK		Cadeia de caracteres
Código do país móvel atual	CURRENT_MCC		Inteiro
Código de rede móvel atual	CURRENT_MNC		Cadeia de caracteres

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nome da conta DEP	BULK_ENROLLMENT_DEP_ACCOUNT_NAME		Cadeia de caracteres
Política DEP	WINDOWS_HAS_DEP_POLICY		Cadeia de caracteres
Dados roaming permitido	DATA_ROAMING_ENABLED	1 (Sim), 0 (Não)	Booliana
Data do último backup iCloud	LAST_CLOUD_BACKUP_DATE		Data
Descrição	DESCRIÇÃO		Cadeia de caracteres
Perfil do programa de registro de dispositivo atribuído	PROFILE_ASSIGN_TIME		Data
Perfil do Programa de Registro de Dispositivo enviado	PROFILE_PUSH_TIME		Data
Perfil do Programa de Registro de Dispositivo removido	PROFILE_REMOVE_TIME		Data
Registro do programa de registro de dispositivos por	DEVICE_ASSIGNED_BY		Cadeia de caracteres
Data de registro no Device Enrollment Program	DEVICE_ASSIGNED_DATE		Data
Tipo de dispositivo	DEVICE_TYPE		Cadeia de caracteres
Modelo do dispositivo	MODEL_ID		Cadeia de caracteres
Nome do dispositivo	NOME DO DISPOSITIVO		Cadeia de caracteres
Você pode optar por não perturbe ativado	DO_NOT_DISTURB	1 (Sim), 0 (Não)	Booliana
Driver ELAM carregado?	WINDOWS_HAS_ELAM_DRIVER_LOADED		Cadeia de caracteres
Conformidade de criptografia (Windows 10)	ENCRYPTION_COMPLIANCE	Encrypted, Not Encrypted	Cadeia de caracteres
ENROLLMENT_KEY_GENERATION_DATE	ENROLLMENT_KEY_GENERATION_DATE		Data
ID da empresa	ENTERPRISE_ID		Cadeia de caracteres

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Armazenamento externo 1: espaço disponível	EXTERNAL_STORAGE1_FREE_SPACE		Inteiro
Armazenamento externo 1: nome	EXTERNAL_STORAGE1_NAME		Cadeia de caracteres
Armazenamento externo 1: espaço total	EXTERNAL_STORAGE1_TOTAL_SPACE		Inteiro
Armazenamento externo 2: espaço disponível	EXTERNAL_STORAGE2_FREE_SPACE		Inteiro
Armazenamento externo 2: nome	EXTERNAL_STORAGE2_NAME		Cadeia de caracteres
Armazenamento externo 2: espaço total	EXTERNAL_STORAGE2_TOTAL_SPACE		Inteiro
Armazenamento externo criptografado	EXTERNAL_ENCRYPTION	1 (Sim), 0 (Não)	Booliana
Status do firewall (telefone Windows 8.1)	FIREWALL_STATUS		Cadeia de caracteres
Status do firewall (Windows 10)	DEVICE_FIREWALL_STATUS	On and monitoring, Disabled, Off or not monitoring, Temporarily not monitoring, N/A	Cadeia de caracteres
Versão de firmware	FIRMWARE_VERSION		Cadeia de caracteres
Primeira sincronização	ZMSP_FIRST_SYNC		Data
Altitude GPS	GPS_ALTITUDE_FROM_GPS		Cadeia de caracteres
Latitude de GPS	GPS_LATITUDE_FROM_GPS		Cadeia de caracteres
Longitude do GPS	GPS_LONGITUDE_FROM_GPS		Cadeia de caracteres
Timestamp GPS	GPS_TIMESTAMP_FROM_GPS		Data
Alias do diretório do Google	GOOGLE_AW_DIRECTORY_GOOGLE_ALIAS		Cadeia de caracteres
Nome de família do Google diretório	GOOGLE_AW_DIRECTORY_FAMILY_NAME		Cadeia de caracteres
Nome do Google Directory	GOOGLE_AW_DIRECTORY_NAME		Cadeia de caracteres

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Email principal do Google diretório	GOOGLE_AW_DIRECTORY_PRIMARY		Cadeia de caracteres
ID de usuário do Google diretório	GOOGLE_AW_DIRECTORY_USER_ID		Cadeia de caracteres
HAS_CONTAINER	HAS_CONTAINER	1 (Sim), 0 (Não)	Booliana
Versão de API HTC	HTC_MDM_VERSION		Cadeia de caracteres
API MDM de HTC disponível	HTC_MDM	1 (Sim), 0 (Não)	Booliana
Recursos de criptografia de hardware	HARDWARE_ENCRYPTION_CAPS		Inteiro
Hash do iTunes armazenar fez logon de conta	ITUNES_STORE_ACCOUNT_HASH		Cadeia de caracteres
Rede da operadora inicial	SIM_CARRIER_NETWORK		Cadeia de caracteres
Código do país móvel local	SIM_MCC		Inteiro
Código de rede móvel local	SIM_MNC		Cadeia de caracteres
ICCID	ICCID		Cadeia de caracteres
Número IMEI/MEID	IMEI		Cadeia de caracteres
IMSI	IMSI		Cadeia de caracteres
Localização de IP	IP_LOCATION		Cadeia de caracteres
Identidade	AS_DEVICE_IDENTITY		Cadeia de caracteres
Armazenamento interno criptografado	LOCAL_ENCRYPTION	1 (Verdadeiro), 0 (Falso)	Booliana
Endereço IPv4 (Windows 10)	IP_ADDRESSV4		Cadeia de caracteres
Endereço IPv6 (Windows 10)	IP_ADDRESSV6		Cadeia de caracteres

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Emitido em	WINDOWS_HAS_ISSUED_AT		Cadeia de caracteres
Jailbroken/com raiz	ROOT_ACCESS	1 (Sim), 0 (Não)	Booliana
Depuração de kernel ativada?	WINDOWS_HAS_OS_KERNEL_DEBUGGING_ENABLED		Cadeia de caracteres
Modo de quiosque	IS_KIOSK	1 (Verdadeiro), 0 (Falso)	Booliana
Último endereço IP conhecido	LAST_IP_ADDR		Cadeia de caracteres
Última vez de atualização de política	LAST_POLICY_UPDATE_TIME		Data
Última sincronização	ZMSP_LAST_SYNC		Data
Serviço de localização ativado	DEVICE_LOCATOR	1 (Sim), 0 (Não)	Booliana
Conexão de rede do endereço MAC (Windows 10)	MAC_NETWORK_CONNECTION	1 (Sim), 0 (Não)	Booliana
Tipo de endereço MAC (Windows 10)	MAC_ADDRESS_TYPE	Unknown, LAN, WLAN	Cadeia de caracteres
MDX_SHARED_ENCRYPTION_KEY	MDX_SHARED_ENCRYPTION_KEY		Cadeia de caracteres
MEID	MEID		Cadeia de caracteres
Configuração de caixa de correio	GOOGLE_AW_DIRECTORY_MAILBOX_SETUP		Cadeia de caracteres
Bateria principal	MAIN_BATTERY_PERCENT		Inteiro
Número de telefone celular	TEL_NUMBER		Cadeia de caracteres
ID do modelo	SYSTEM_OEM		Cadeia de caracteres
Número do modelo	MODEL_NUMBER		Cadeia de caracteres
Tipo de adaptador de rede	NETWORK_ADAPTER_TYPE		Cadeia de caracteres
NitroDesk TouchDown instalado	TOUCHDOWN_FIND	1 (Verdadeiro), 0 (Falso)	Booliana

© 1999-2017 Citrix Systems, Inc. All rights reserved.

NitroDesk TouchDown licenciados por meio do MDM	TOUCHDOWN_LICENSED_VIA_MDM	1 (Verdadeiro), 0 (Falso)	Booliana
Compilação do sistema operacional	SYSTEM_OS_BUILD		Cadeia de caracteres
Edição do sistema operacional (Windows 10)	OS_EDITION		Cadeia de caracteres
Idioma do sistema operacional (local)	SYSTEM_LANGUAGE		Cadeia de caracteres
Versão do sistema operacional	SYSTEM_OS_VERSION		Cadeia de caracteres
Endereço da organização	ORGANIZATION_ADDRESS		Cadeia de caracteres
Email da organização	ORGANIZATION_EMAIL		Cadeia de caracteres
Magic da organização	ORGANIZATION_MAGIC		Cadeia de caracteres
Nome da organização	ORGANIZATION_NAME		Cadeia de caracteres
Número de telefone da organização	ORGANIZATION_PHONE		Cadeia de caracteres
Outros	OTHER		Cadeia de caracteres
Fora de conformidade	OUT_OF_COMPLIANCE	1 (Verdadeiro), 0 (Falso)	Booliana
Propriedade	CORPORATE_OWNED	1 (Corporativo), 0 (BYOD)	Booliana
PCR0	WINDOWS_HAS_PCR0		Cadeia de caracteres
Código PIN para geocerca	PIN_CODE_FOR_GEO_FENCE		Cadeia de caracteres
Código secreto em conformidade	PASSCODE_IS_COMPLIANT	1 (Sim), 0 (Não)	Booliana
Código secreto em conformidade com a configuração	PASSCODE_IS_COMPLIANT_WITH_CFG	1 (Sim), 0 (Não)	Booliana
Código secreto presente	PASSCODE_PRESENT	1 (Sim), 0 (Não)	Booliana

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Violação do perímetro	GPS_PERIMETER_BREACH	1 (Sim), 0 (Não)	Booliana
Ponto de acesso pessoal ativado	PERSONAL_HOTSPOT_ENABLED	1 (Sim), 0 (Não)	Booliana
Plataforma	SYSTEM_PLATFORM		Cadeia de caracteres
Nível de plataforma API	API_LEVEL		Inteiro
Nome da política	NOME_DA_DIRETIVA		Cadeia de caracteres
Número de telefone principal	IDENTITY1_PHONENUMBER		Cadeia de caracteres
Operadora da portadora SIM principal (Windows 10)	IDENTITY1_CARRIER_NETWORK_OPERATOR		Cadeia de caracteres
ICCID SIM primário (Windows 10)	IDENTITY1_ICCID		Cadeia de caracteres
Principal IMEI SIM	IDENTITY1_IMEI		Cadeia de caracteres
IMSI de SIM principal	IDENTITY1_IMSI		Cadeia de caracteres
SIM principal em Roaming	IDENTITY1_ROAMING	1 (Verdadeiro), 0 (Falso)	Booliana
Conformidade com roaming de SIM principal (Windows 10)	IDENTITY1_ROAMING_COMPLIANCE	1 (Verdadeiro), 0 (Falso)	Booliana
Nome do produto	PRODUCT_NAME		Cadeia de caracteres
ID de dispositivo de fornecedor	PUBLISHER_DEVICE_ID		Cadeia de caracteres
Redefinir contagem	WINDOWS_HAS_RESET_COUNT		Cadeia de caracteres
Reiniciar contagem	WINDOWS_HAS_RESTART_COUNT		Cadeia de caracteres
Hash SBCP	WINDOWS_HAS_SBCP_HASH		Cadeia de caracteres
Com capacidade de SMS	IS_SMS_CAPABLE	1 (Verdadeiro), 0 (Falso)	Booliana

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Modo de segurança ativado?	WINDOWS_HAS_SAFE_MODE		Cadeia de caracteres
API do Samsung KNOX disponível	SAMSUNG_KNOX	1 (Verdadeiro), 0 (Falso)	Booliana
Versão de API do Samsung KNOX	SAMSUNG_KNOX_VERSION		Cadeia de caracteres
Atestado do Samsung KNOX	SAMSUNG_KNOX_ATTESTED	1 (Aprovado), 0 (Falha)	Booliana
Data de atualização do atestado do Samsung KNOX	SAMSUNG_KNOX_ATT_UPDATED_TIME		Data
API Samsung SAFE disponível	SAMSUNG_MDM	1 (Verdadeiro), 0 (Falso)	Booliana
Versão da API do Samsung SAFE	SAMSUNG_MDM_VERSION		Cadeia de caracteres
Tela: Resolução de eixo x	SCREEN_XDPI		Inteiro (PPI)
Tela: Resolução do eixo Y	SCREEN_YDPI		Inteiro (PPI)
Tela: altura	SCREEN_HEIGHT		Inteiro (pixels)
Tela: número de cores	SCREEN_NB_COLORS		Inteiro
Tela: tamanho	SCREEN_SIZE		Decimal (polegadas)
Tela: largura	SCREEN_WIDTH		Inteiro (pixels)
Número de telefone secundário	IDENTITY2_PHONENUMBER		Cadeia de caracteres
Secundário IMEI SIM	IDENTITY2_IMEI		Cadeia de caracteres
IMSI de SIM secundário	IDENTITY2_IMSI		Cadeia de caracteres
SIM secundário Roaming	IDENTITY2_ROAMING	1 (Verdadeiro), 0 (Falso)	Booliana
Inicialização segura ativada? (Windows 8.1 Phone)	WINDOWS_HAS_SECURE_BOOT_ENABLED		Cadeia de caracteres
Status de inicialização segura	SECURE_BOOT_STATE	Not supported,	Cadeia de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

(Windows 10)		Enabled, Disabled	caracteres
SecureContainer ativado	WINDOWS_HAS_BIT_LOCKER_STATUS		Cadeia de caracteres
Número de série	NÚM_SÉRIE		Cadeia de caracteres
API de Enterprise Sony disponível	SONY_MDM	1 (Verdadeiro), 0 (Falso)	Booliana
Versão da API de Enterprise Sony	SONY_MDM_VERSION		Cadeia de caracteres
Supervisionado	Supervisionado	1 (Sim), 0 (Não)	Booliana
Motivo da suspensão	GOOGLE_AW_DIRECTORY_SUSPENTION_REASON		Cadeia de caracteres
Status alterado	TAMPERED_STATUS		Cadeia de caracteres
Termos e Condições	TERMS_AND_CONDITIONS		Cadeia de caracteres
Termos e contrato aceitos?	GOOGLE_AW_DIRECTORY_AGREED_TO_TERMS		Cadeia de caracteres
Sinalização de teste ativada?	WINDOWS_HAS_TEST_SIGNING_ENABLED		Cadeia de caracteres
Total de RAM	MEMORY		Inteiro
Espaço de armazenamento total	FREEDISK		Inteiro
Versão do TPM (Windows 10)	TPM_VERSION		Cadeia de caracteres
UDID	UDID		Cadeia de caracteres
Status do controle de conta de usuário (Windows 10)	UAC_STATUS	Not supported, Enabled, Disabled	Cadeia de caracteres
Agente de usuário	USER_AGENT		Cadeia de caracteres
Definida pelo usuário #1	USER_DEFINED_1		Cadeia de caracteres
Definida pelo usuário #2	USER_DEFINED_2		Cadeia de

© 1999-2017 Citrix Systems, Inc. All rights reserved.

			caracteres
Definida pelo usuário #3	USER_DEFINED_3		Cadeia de caracteres
Idioma do usuário (local)	USER_LANGUAGE		Cadeia de caracteres
VSM ativado?	WINDOWS_HAS_VSM_ENABLED		Cadeia de caracteres
Fornecedor	VENDOR		Cadeia de caracteres
Com capacidade de voz	IS_VOICE_CAPABLE	1 (Verdadeiro), 0 (Falso)	Booliana
Roaming de voz permitido	VOICE_ROAMING_ENABLED	1 (Sim), 0 (Não)	Booliana
WINDOWS_ENROLLMENT_KEY	WINDOWS_ENROLLMENT_KEY		Cadeia de caracteres
Status de notificação WNS	WNS_PUSH_STATUS		Cadeia de caracteres
URL de notificação WNS	PROPERTY_WNS_PUSH_URL		Cadeia de caracteres
Data de expiração da URL de notificação WNS	PROPERTY_WNS_PUSH_URL_EXPIRY		Cadeia de caracteres
Endereço MAC WiFi	WIFI_MAC		Cadeia de caracteres
WinPE ativado?	WINDOWS_HAS_WINPE		Cadeia de caracteres
ID de agente do XenMobile	AGENT_ID		Cadeia de caracteres
Revisão de agente do XenMobile	EW_REVISION		Cadeia de caracteres
Versão do agente XenMobile	EW_VERSION		Cadeia de caracteres

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ActiveSync Gateway

Feb 21, 2018

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**. O padrão é **Permitir**.

Para obter mais informações sobre a política de dispositivo de Acesso aos aplicativos, consulte Políticas 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Dispositivos Android com raiz e iOS com jailbreak: Verifica se um dispositivo Android ou iOS tem jailbreak.

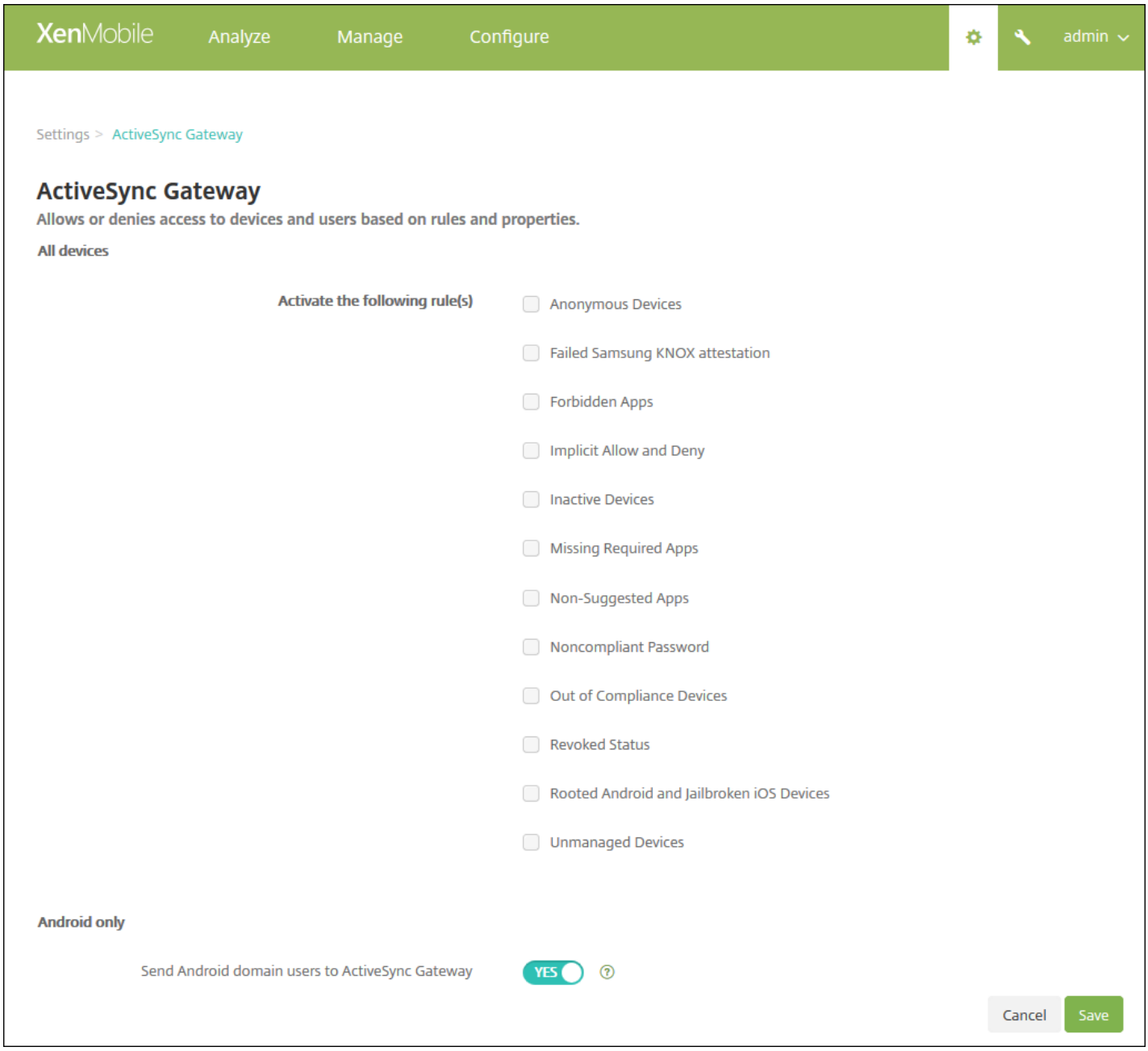
Dispositivos não gerenciados: Verifica se um dispositivo ainda está em um estado gerenciado, sob o controle do XenMobile. Por exemplo, um dispositivo que está em execução no modo MAM ou um dispositivo não registrado não é gerenciado.

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 **Configurações** 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 desejar ativar.

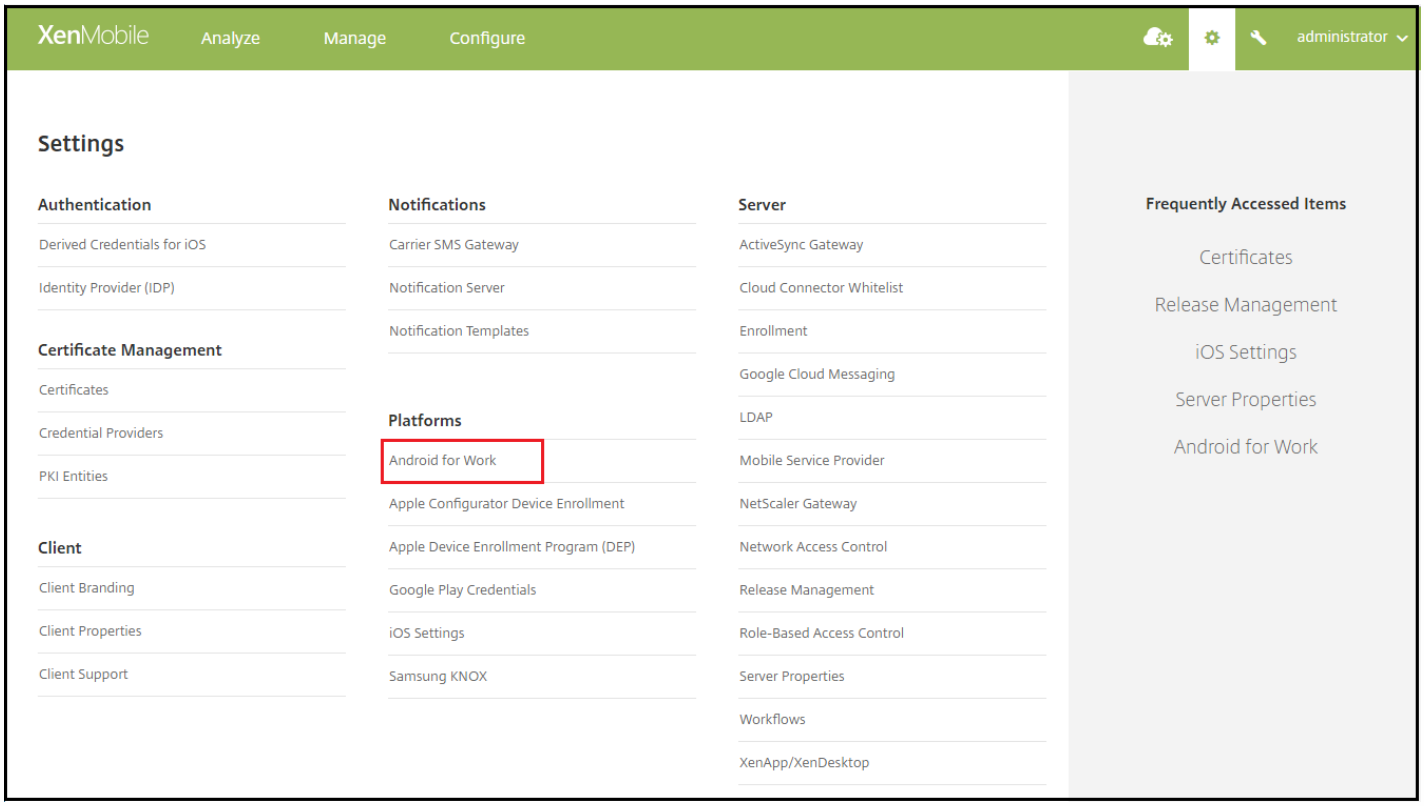
© 1999-2017 Citrix Systems, Inc. All rights reserved.

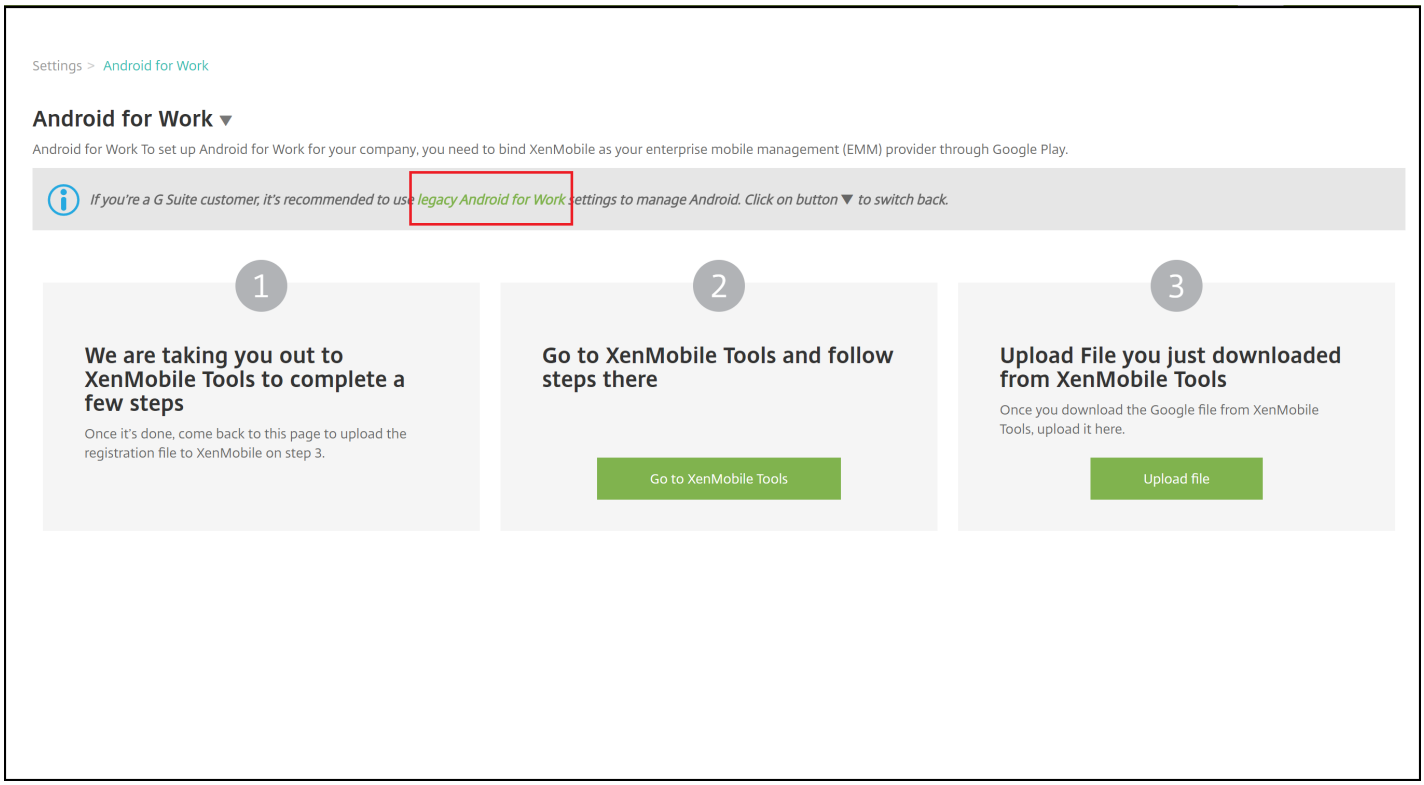
4. Em **Somente Android**, em **Enviar usuários de domínio do Android para o ActiveSync Gateway**, clique em **SIM** para garantir que o XenMobile envie as informações do dispositivo Android para o ActiveSync Gateway.

5. Clique em **Salvar**.

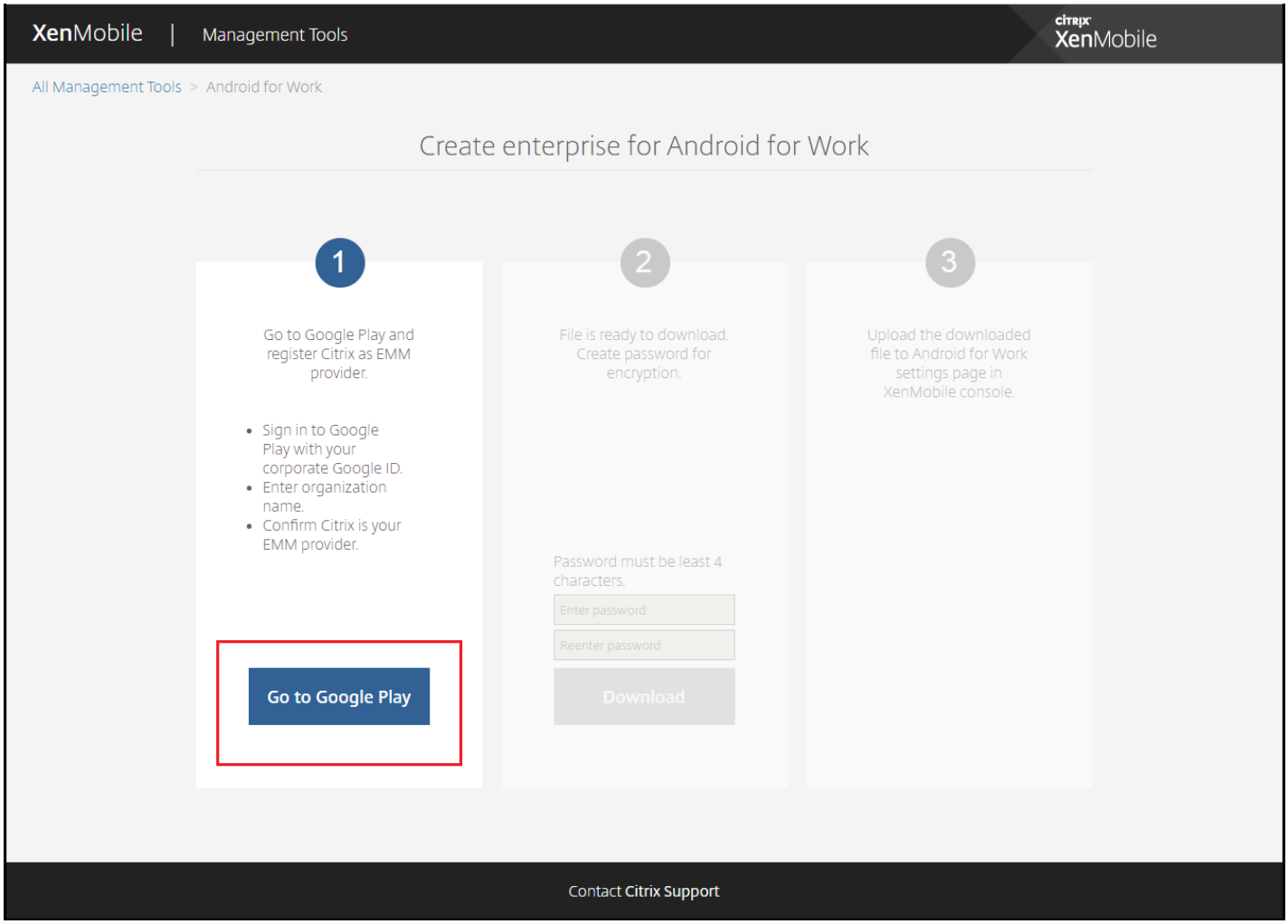
© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

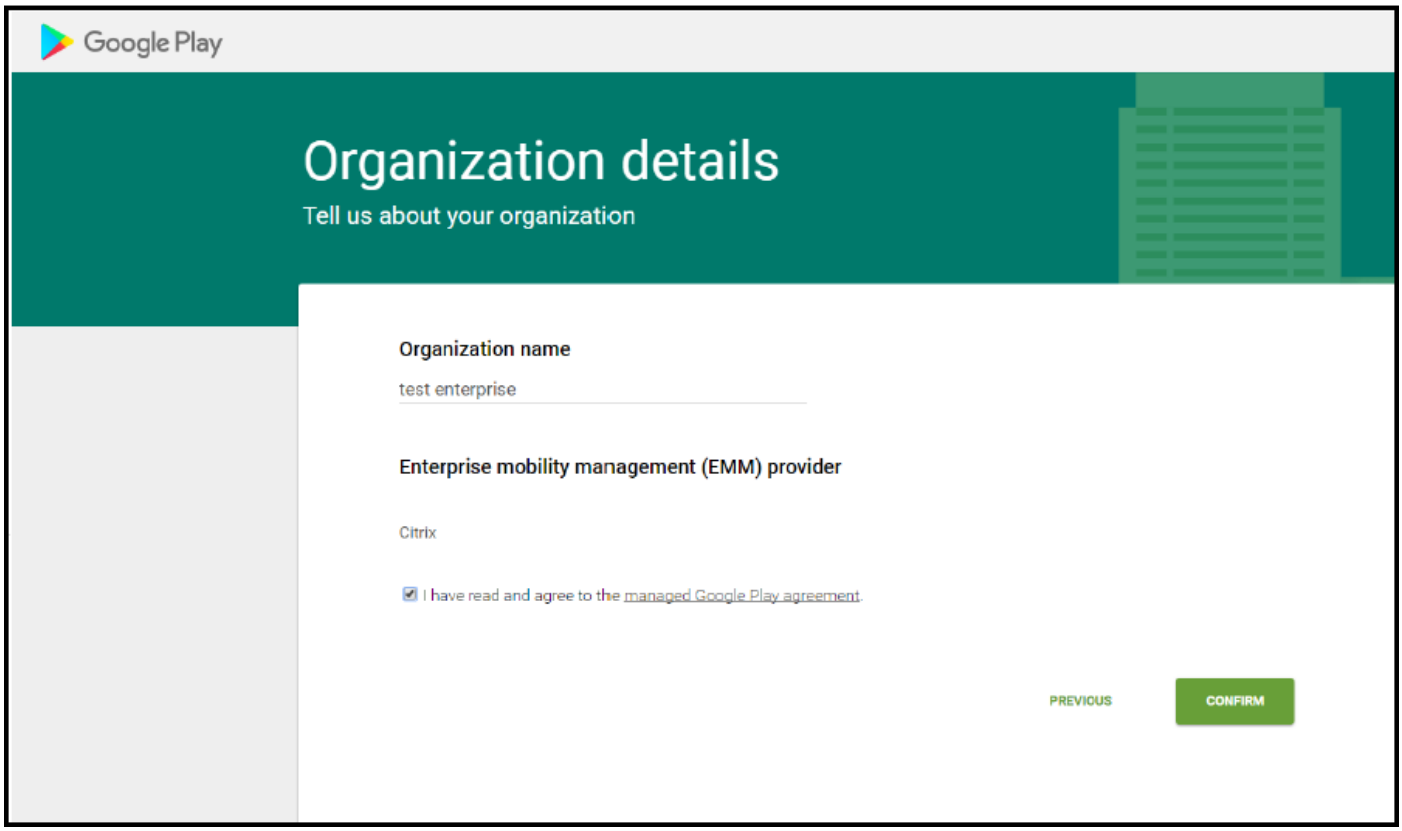




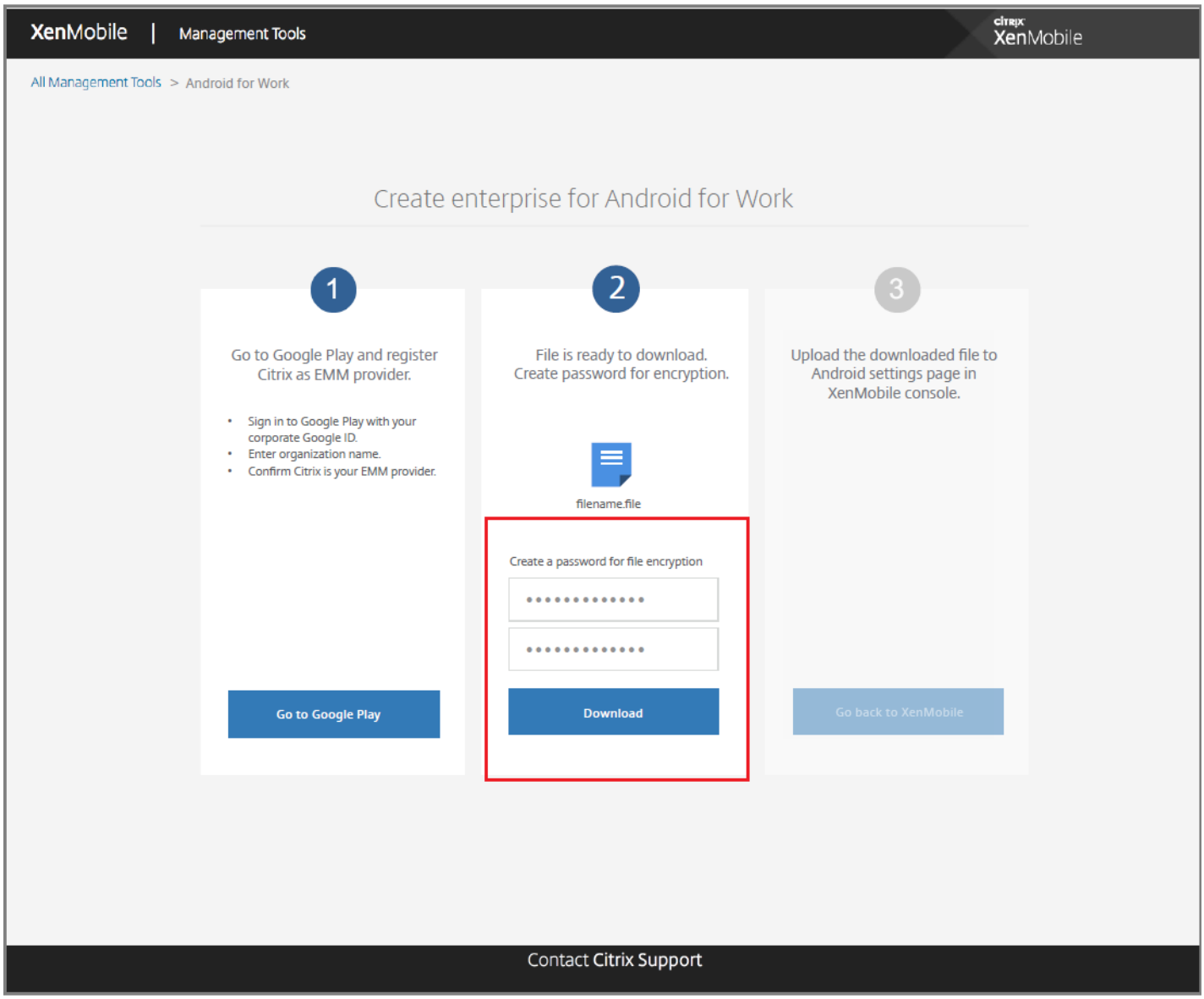
© 1999-2017 Citrix Systems, Inc. All rights reserved.



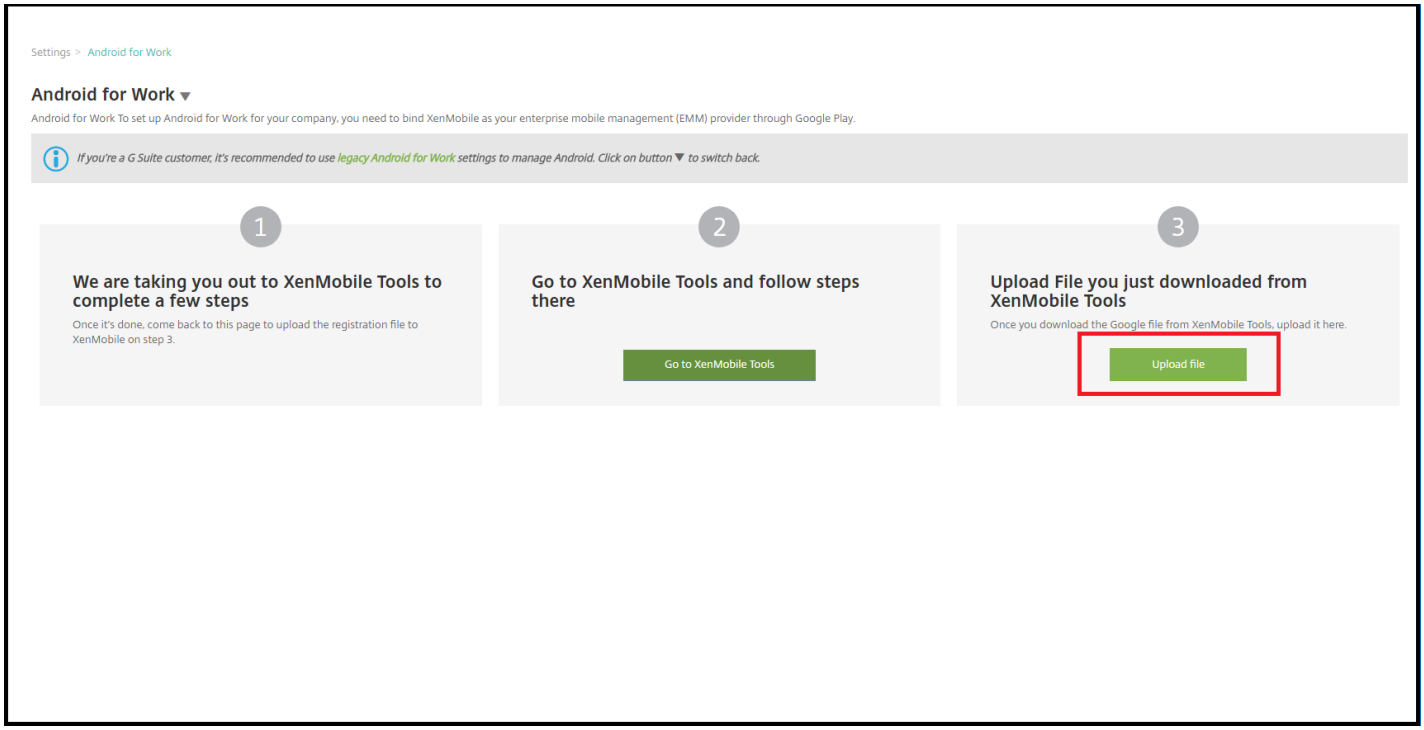
© 1999-2017 Citrix Systems, Inc. All rights reserved.

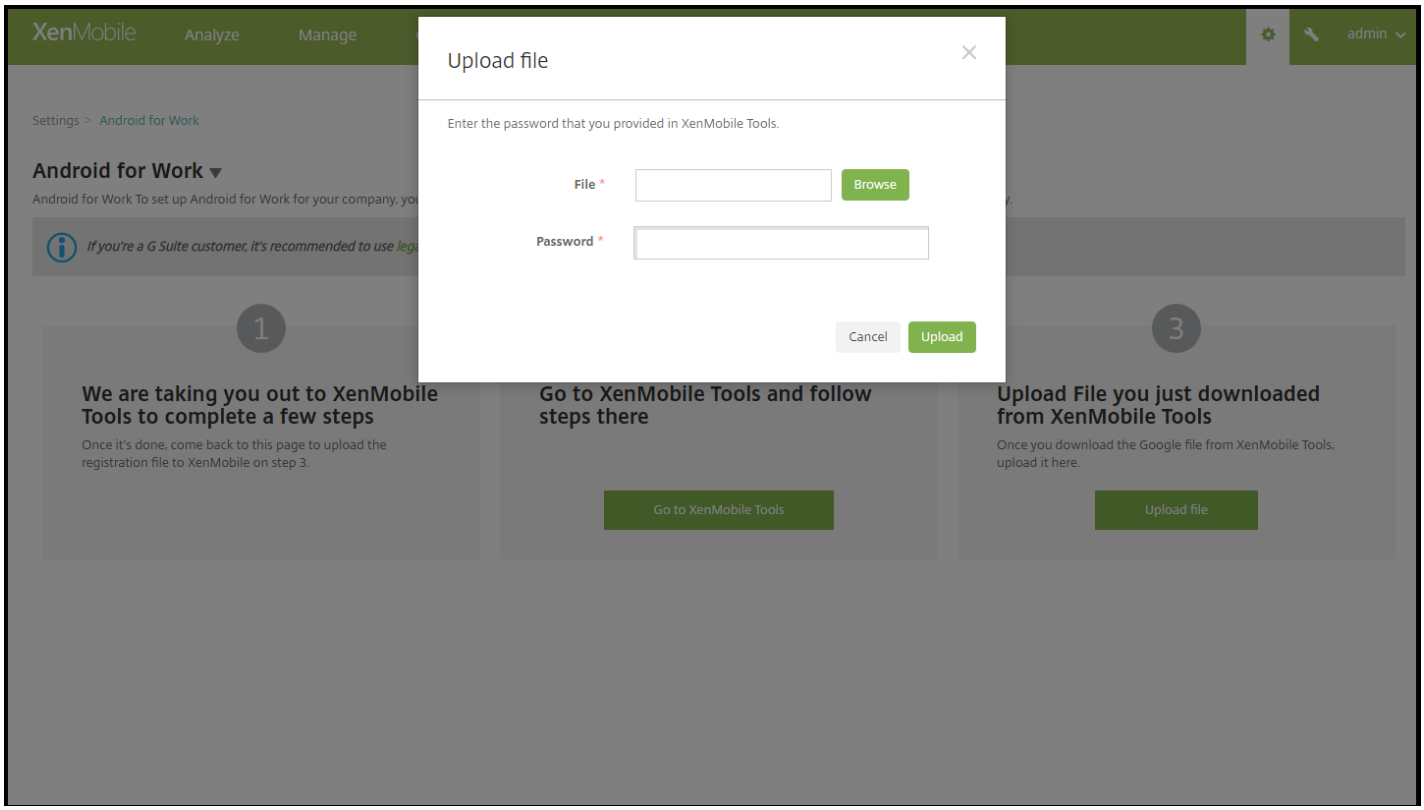


© 1999-2017 Citrix Systems, Inc. All rights reserved.

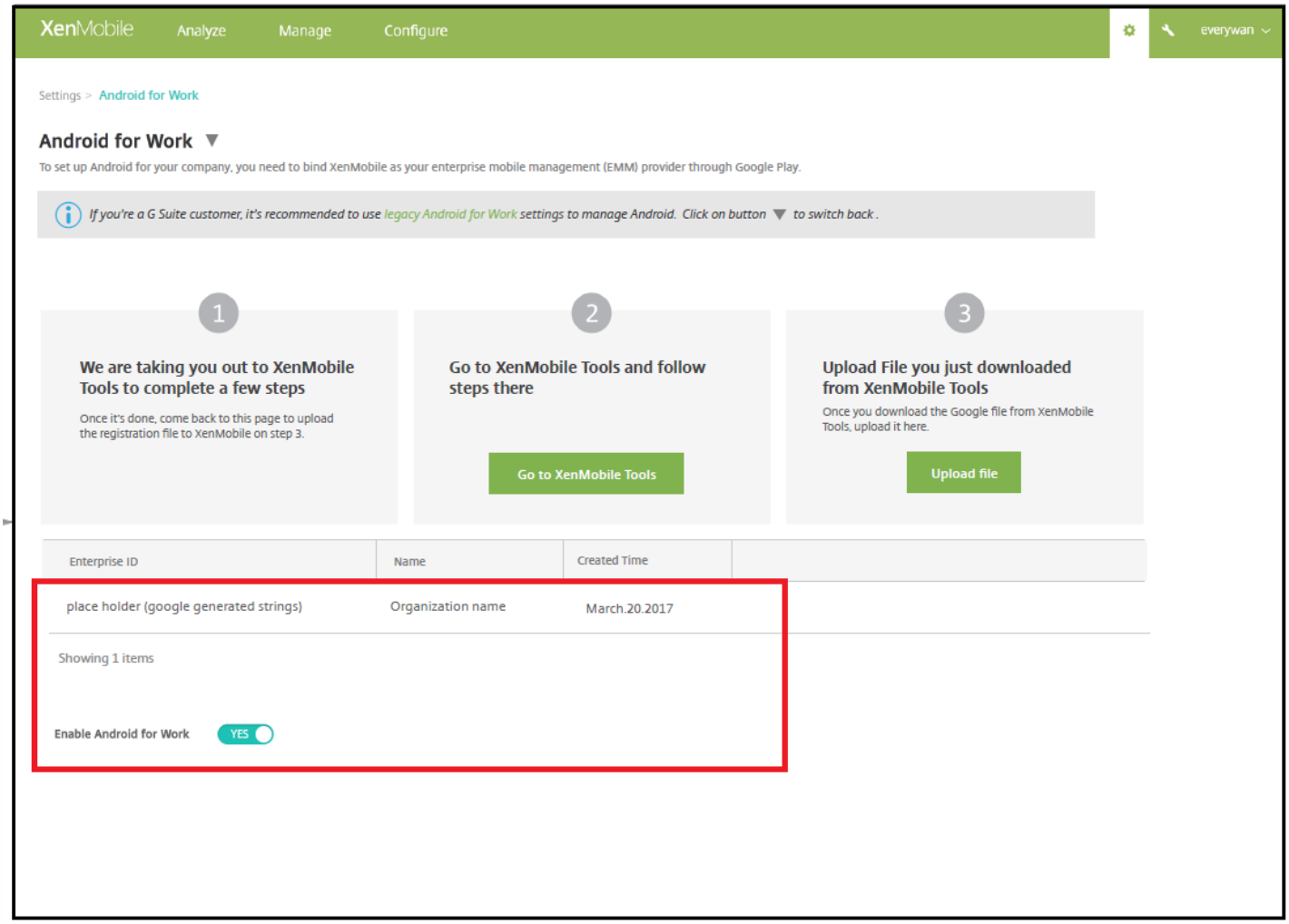


© 1999-2017 Citrix Systems, Inc. All rights reserved.



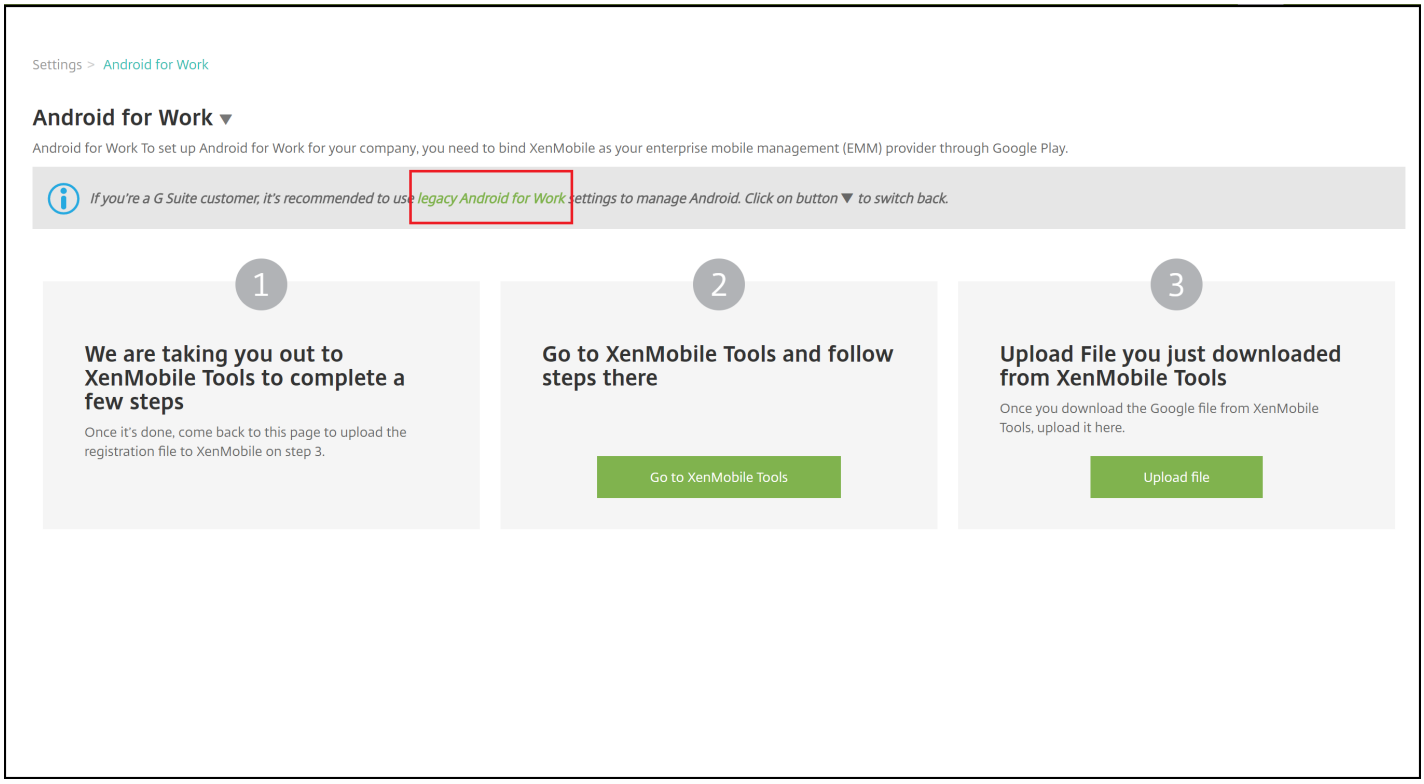


© 1999-2017 Citrix Systems, Inc. All rights reserved.



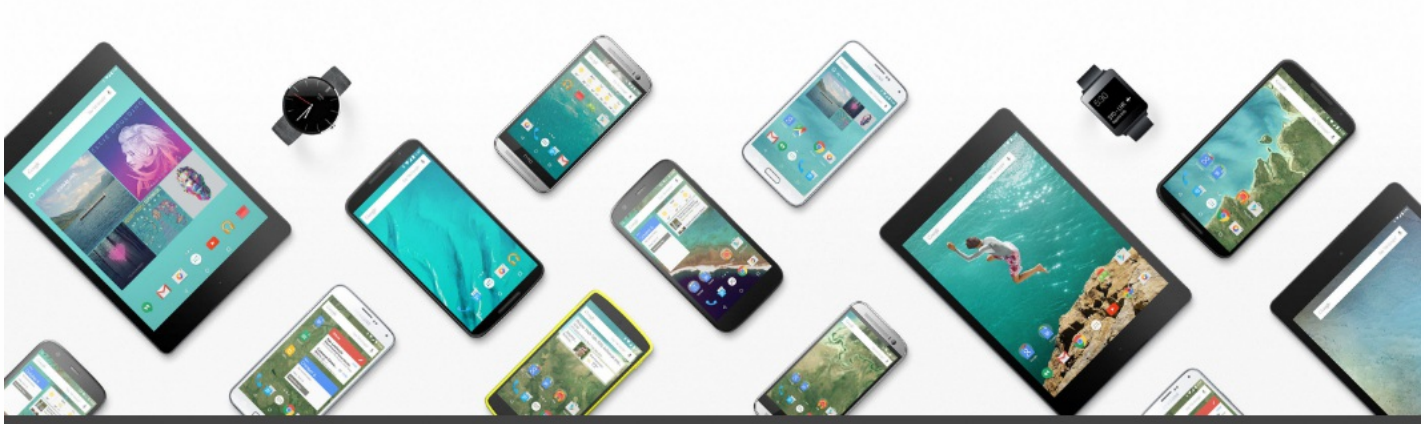
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

G Suite



Bring Android to your office

Sign up to use Android devices at your company.

1 About you

Name

First Name

Last Name

Current work email

Doesn't have to be an official business email.

e.g. john@mydomain.com

Phone

+1

1 About you

Name

Justa

User

Current work email

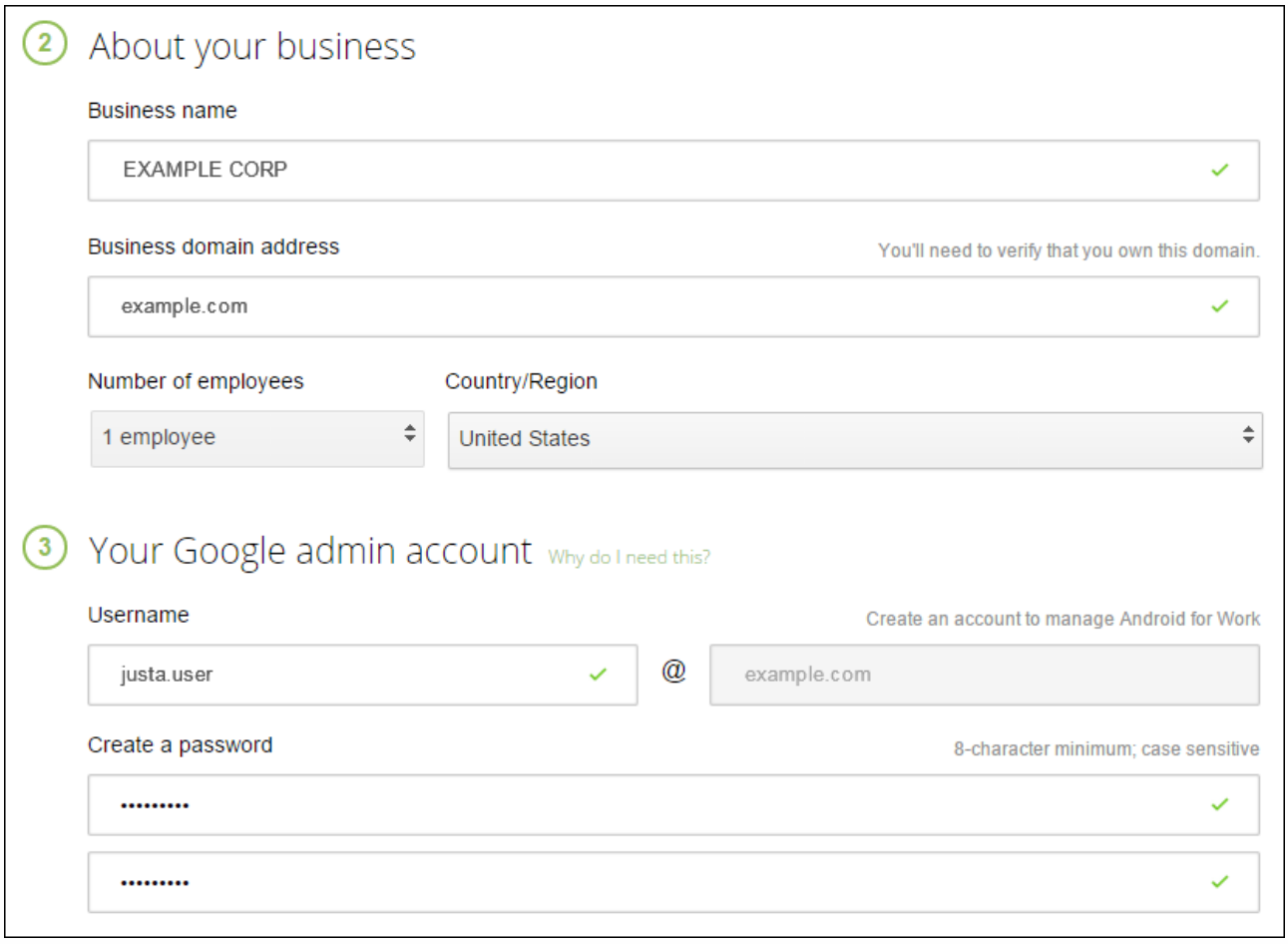
Doesn't have to be an official business email.

justa.user@gmail.com

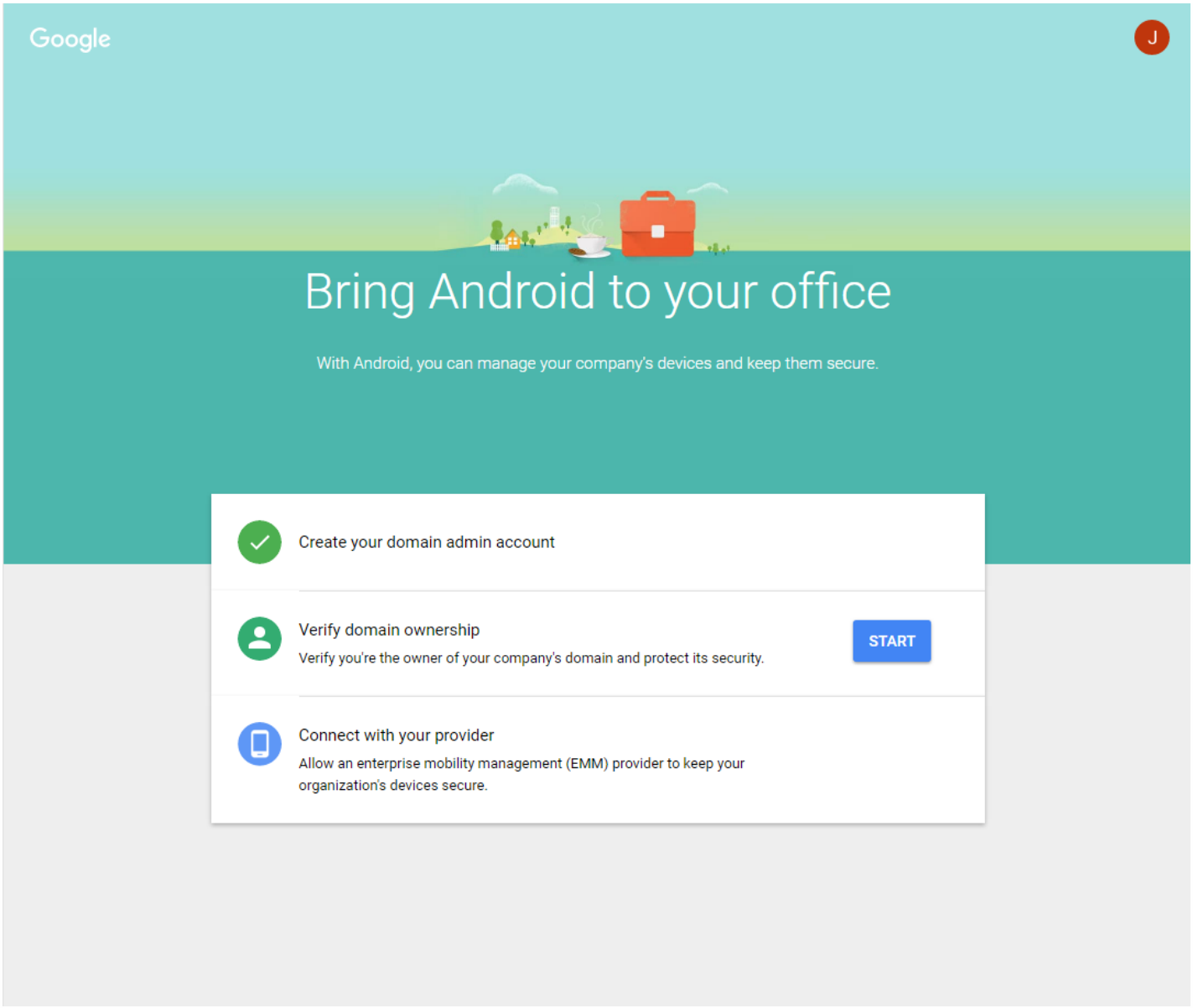
Phone

+15551234567

© 1999-2017 Citrix Systems, Inc. All rights reserved.

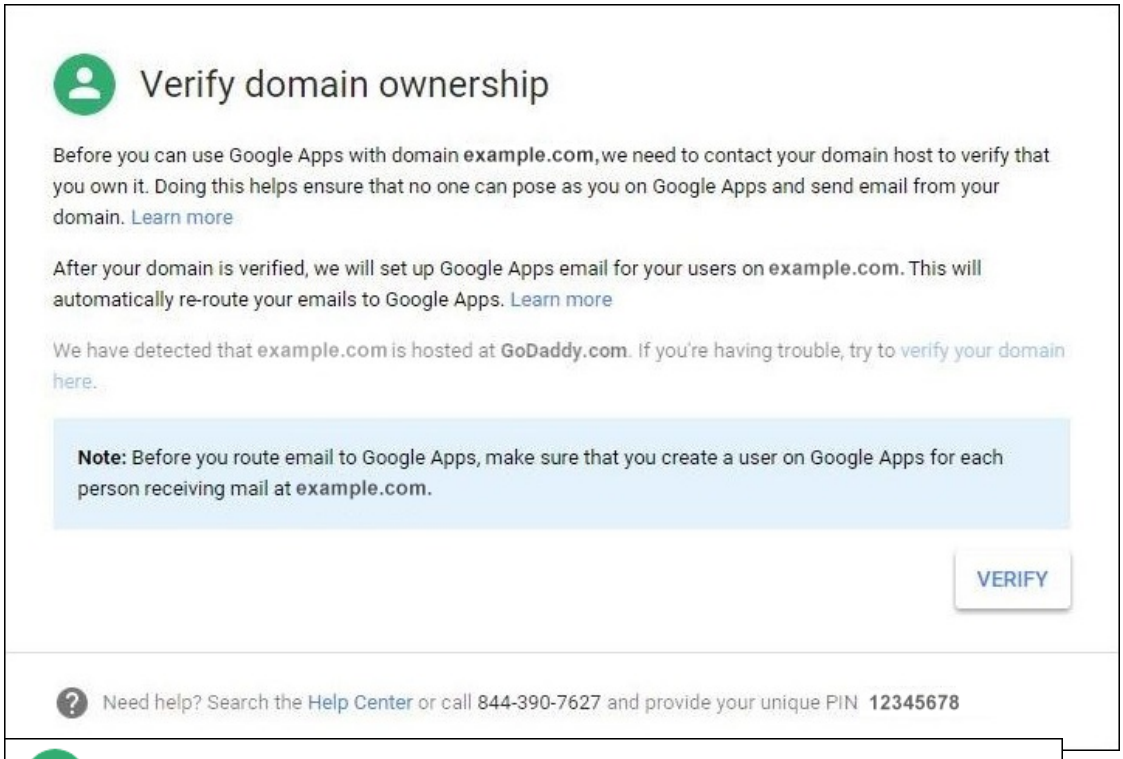


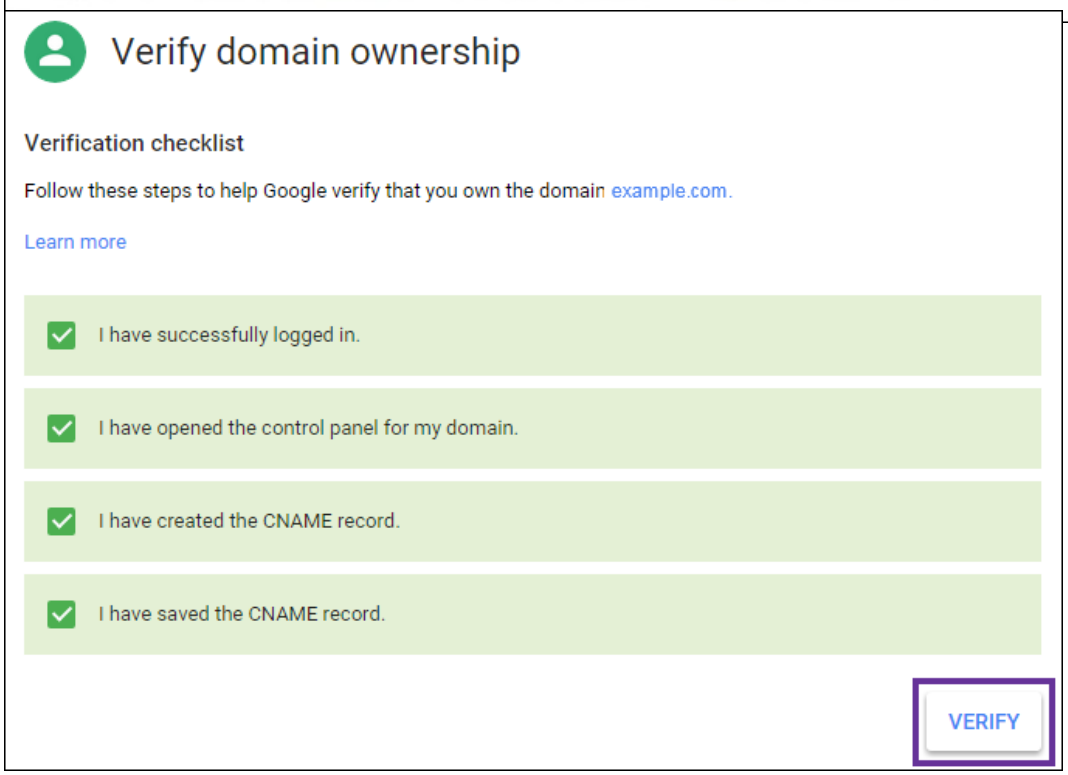
© 1999-2017 Citrix Systems, Inc. All rights reserved.



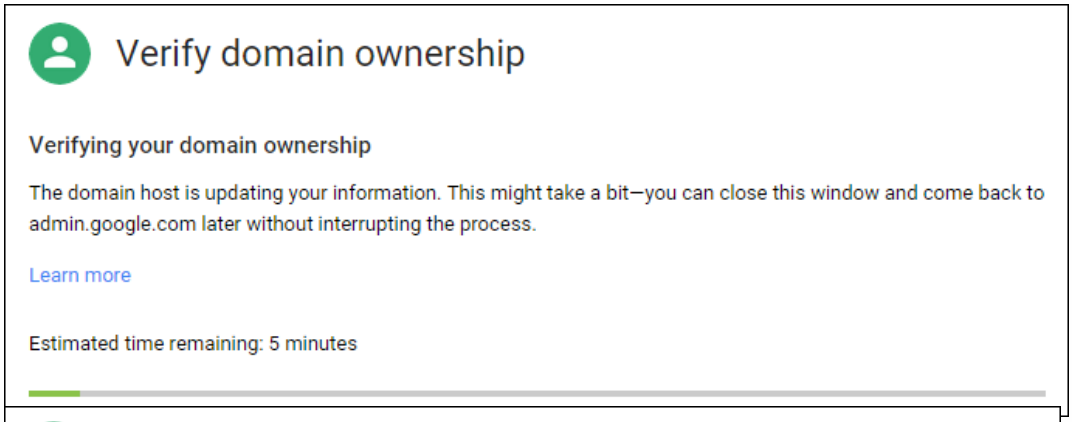
-
-
-

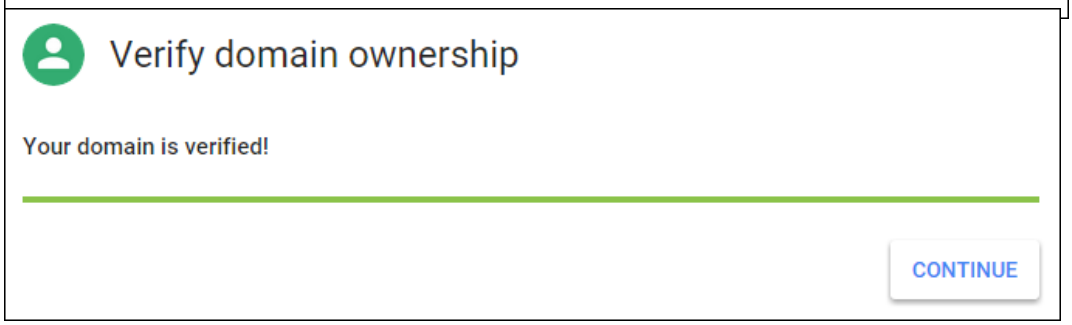
© 1999-2017 Citrix Systems, Inc. All rights reserved.

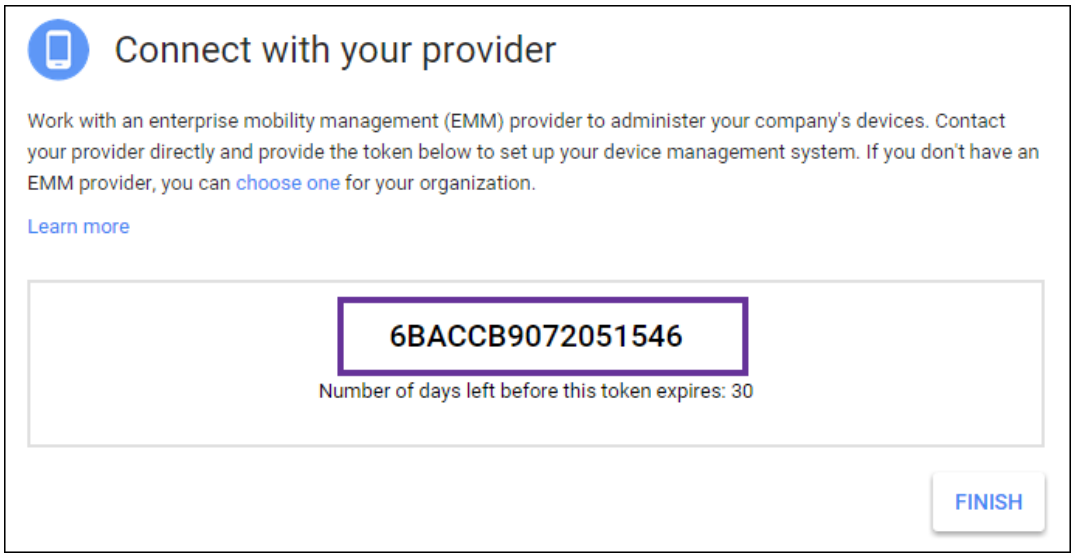




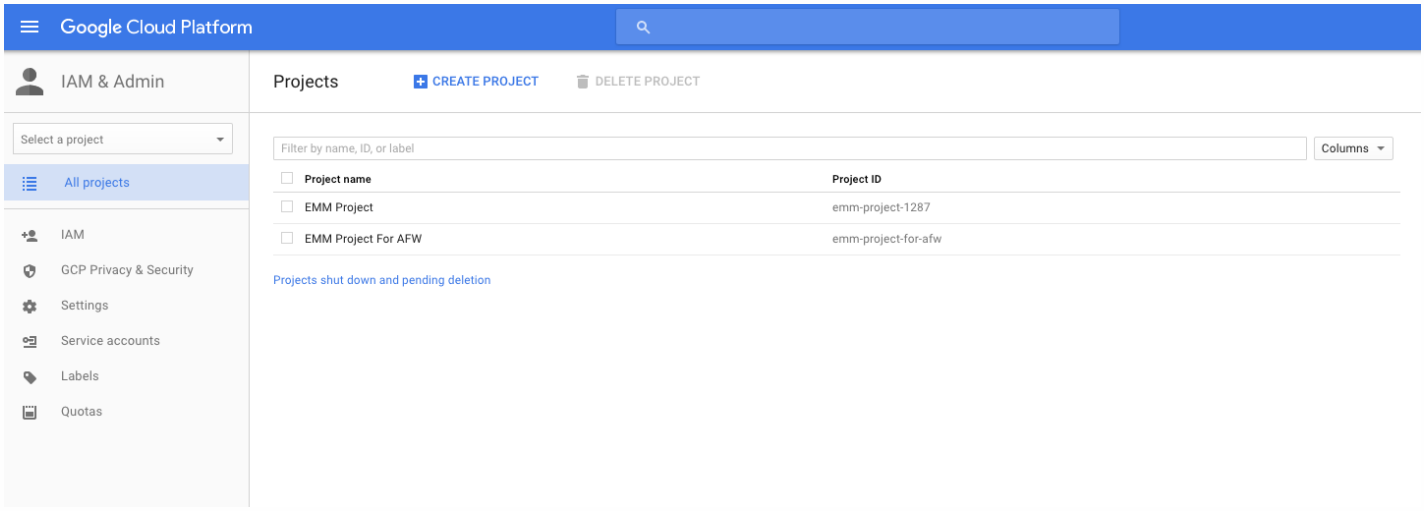
© 1999-2017 Citrix Systems, Inc. All rights reserved.

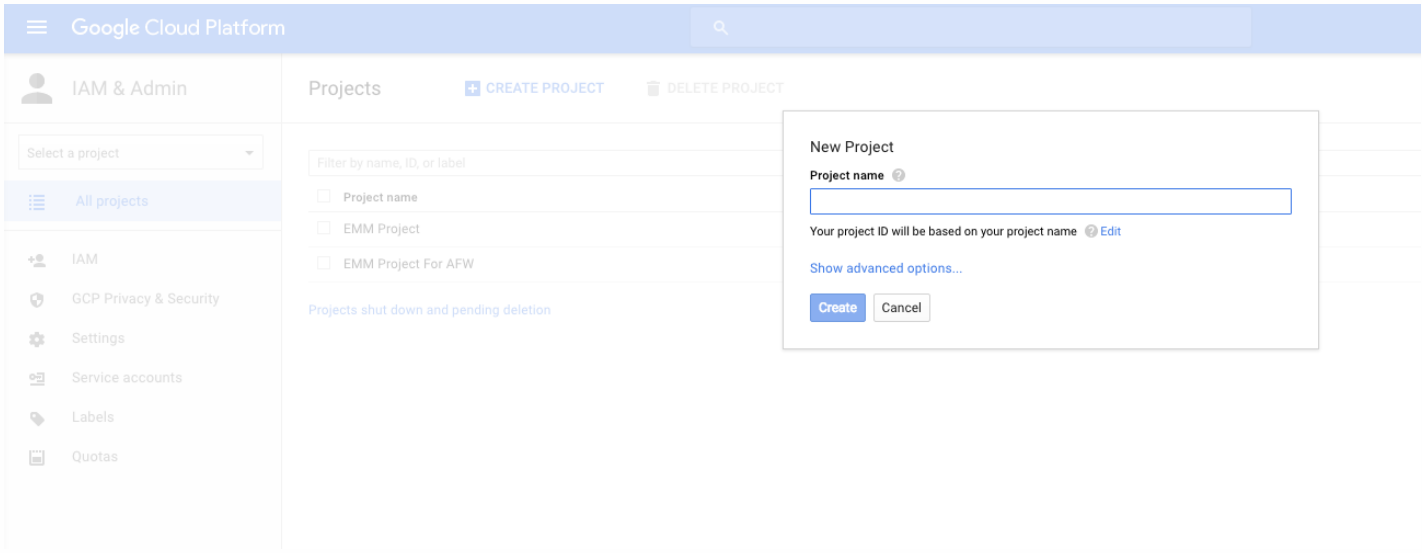




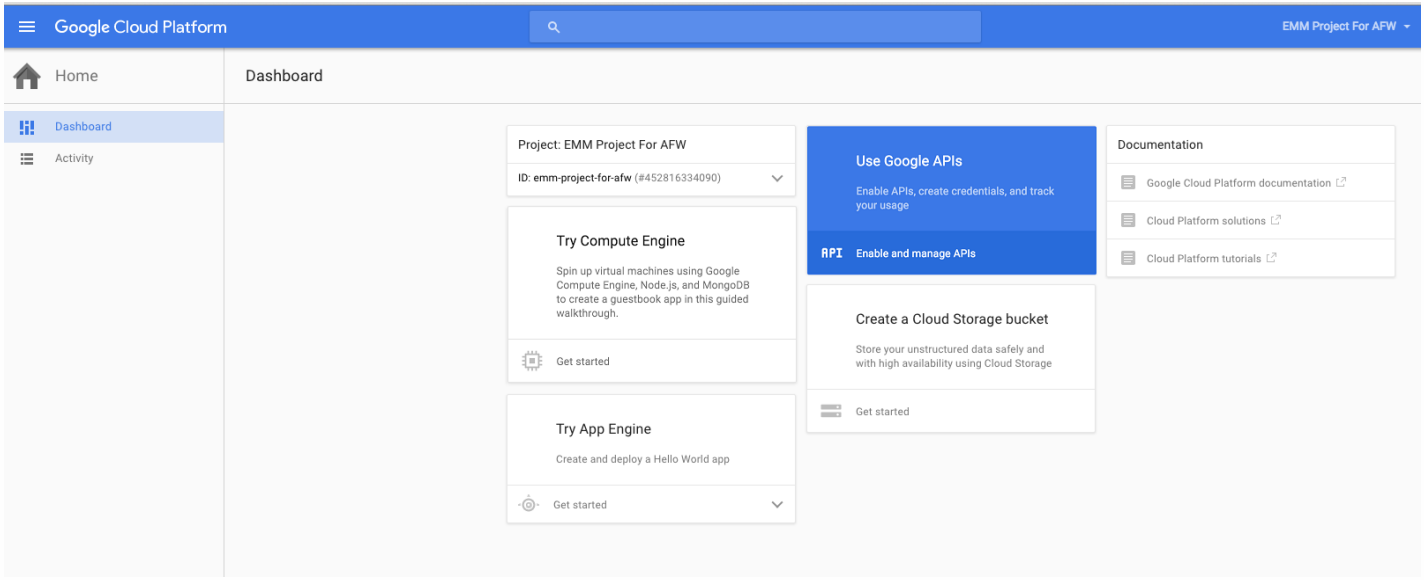


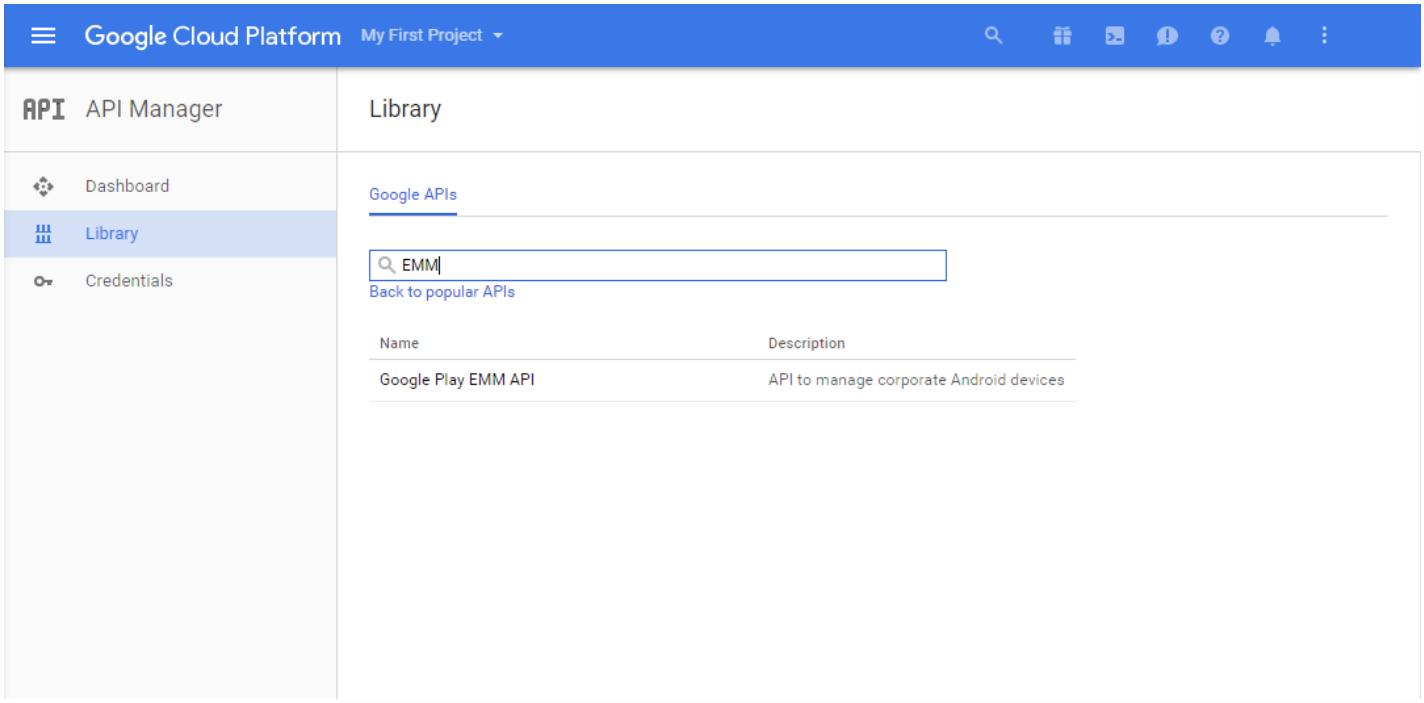
© 1999-2017 Citrix Systems, Inc. All rights reserved.



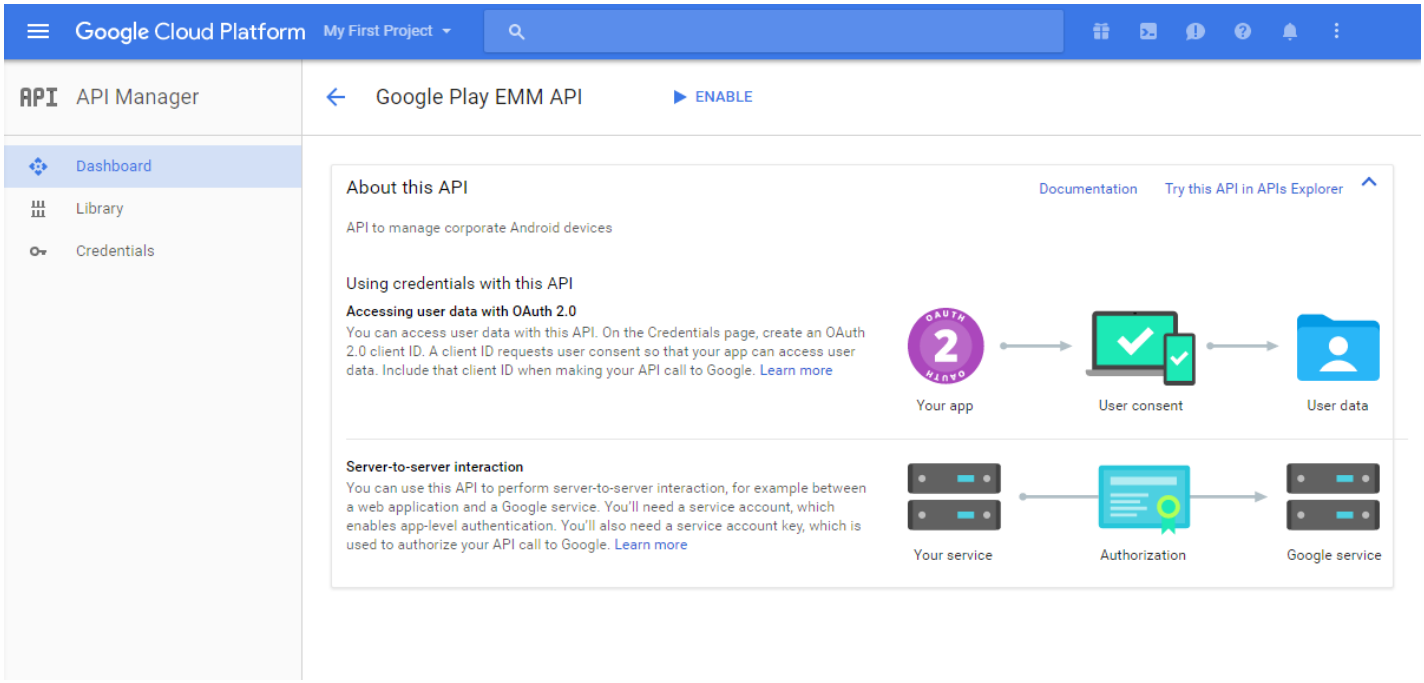


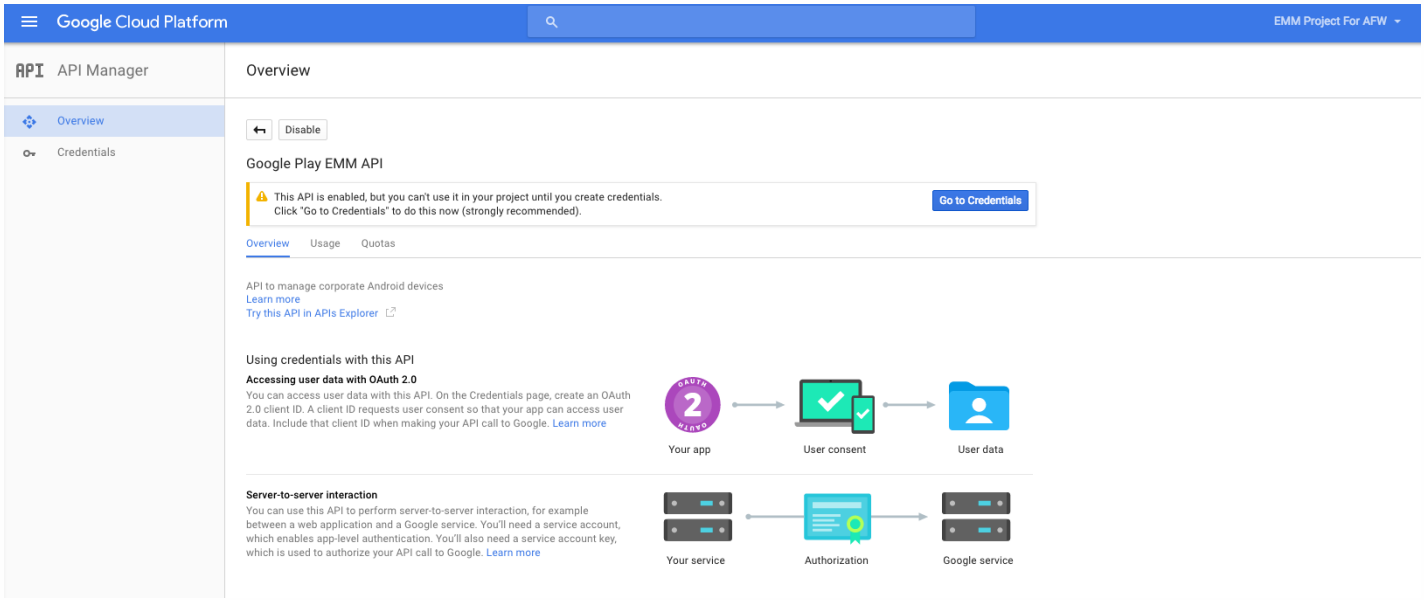
© 1999-2017 Citrix Systems, Inc. All rights reserved.



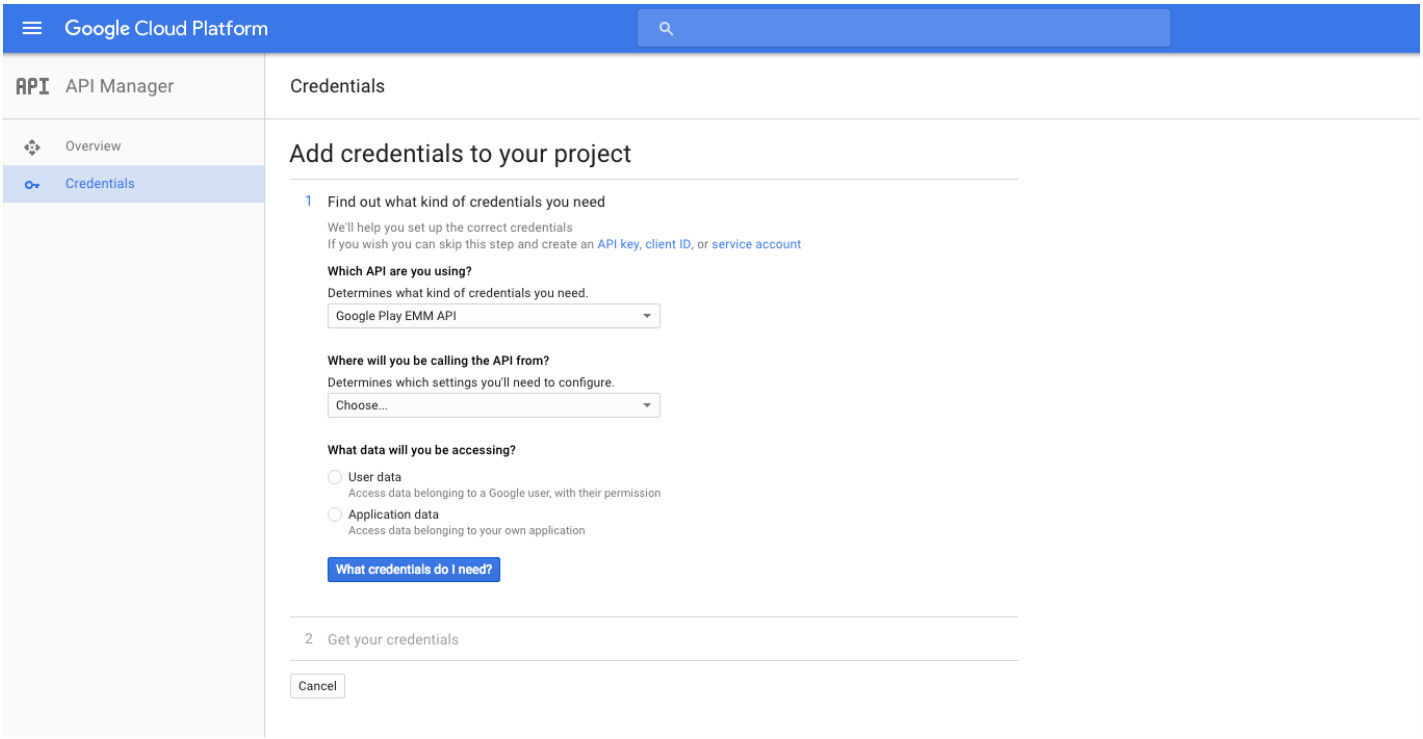


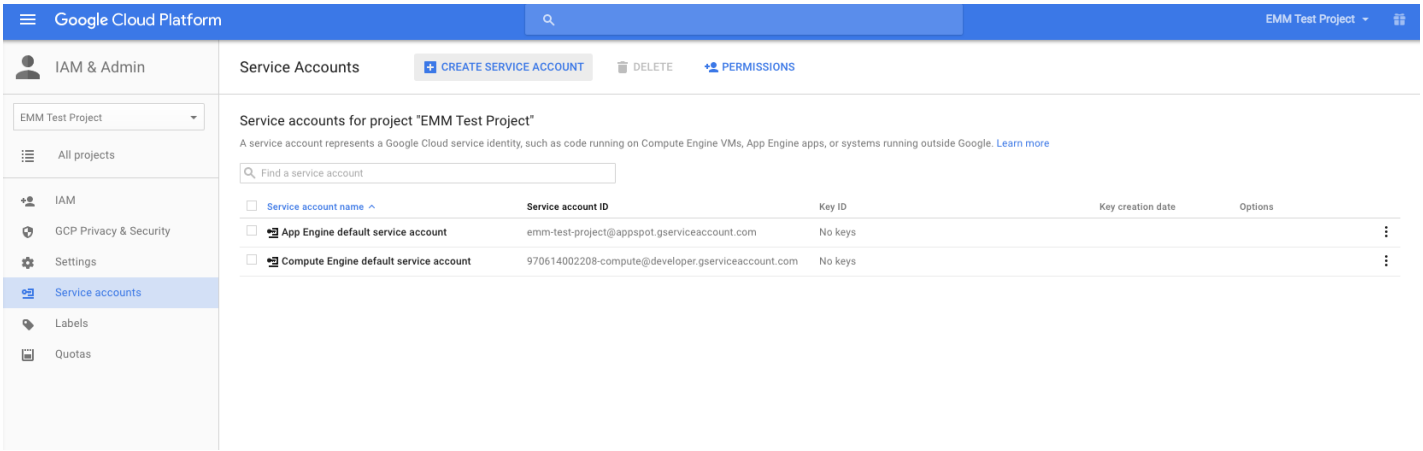
© 1999-2017 Citrix Systems, Inc. All rights reserved.



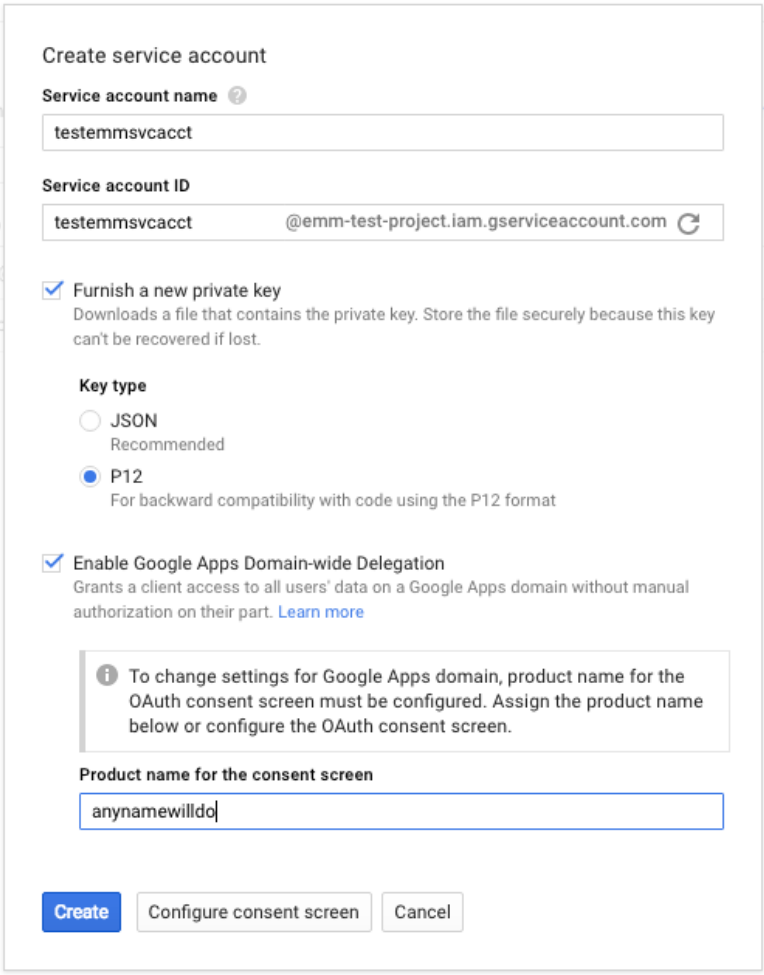


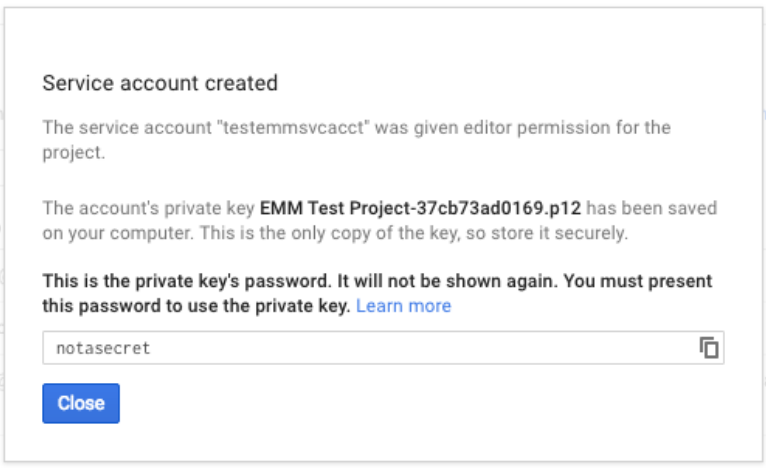
© 1999-2017 Citrix Systems, Inc. All rights reserved.



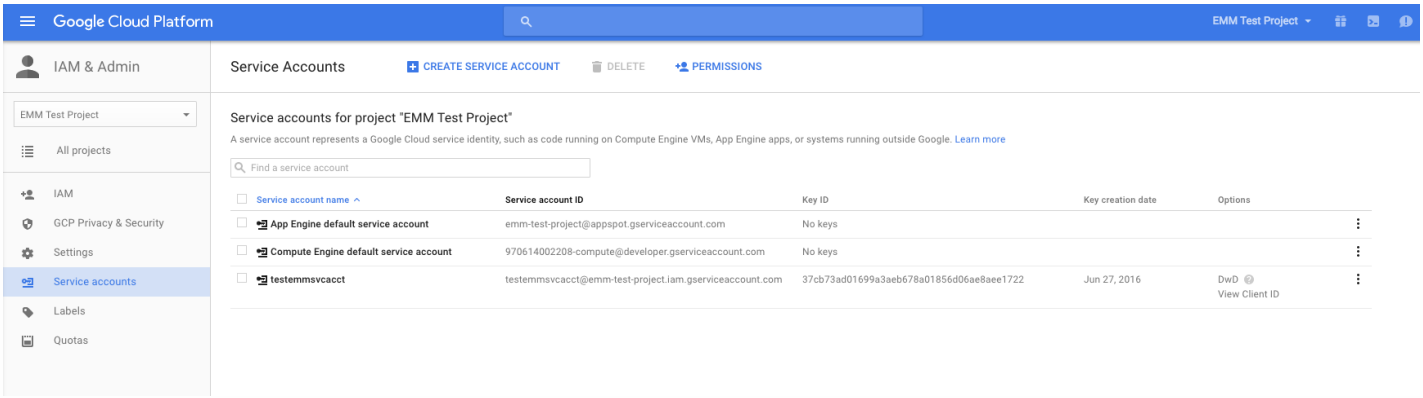


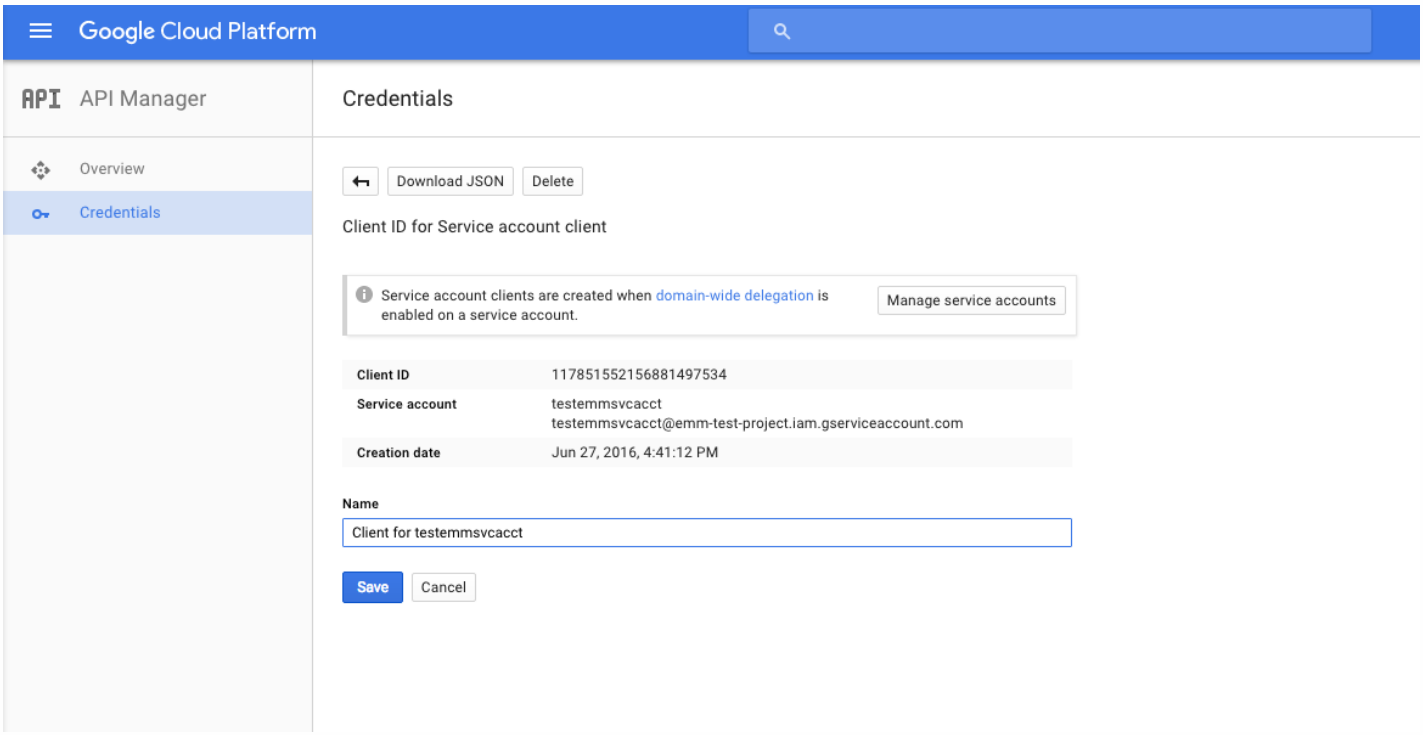
© 1999-2017 Citrix Systems, Inc. All rights reserved.



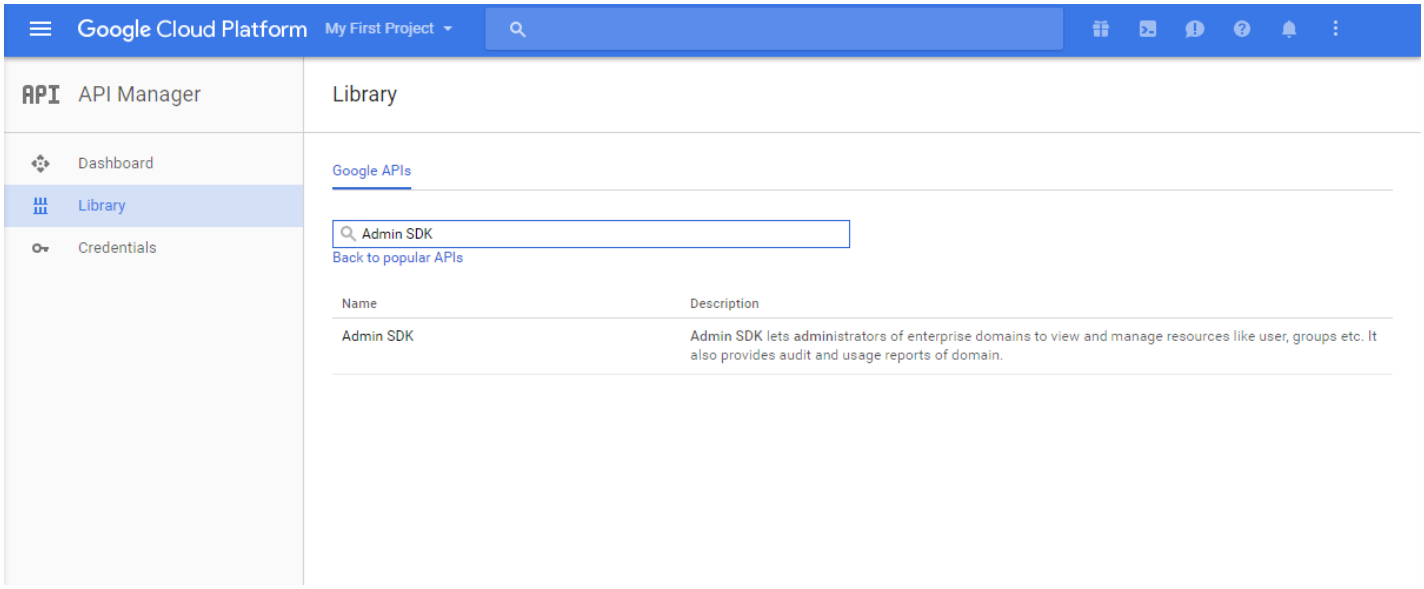


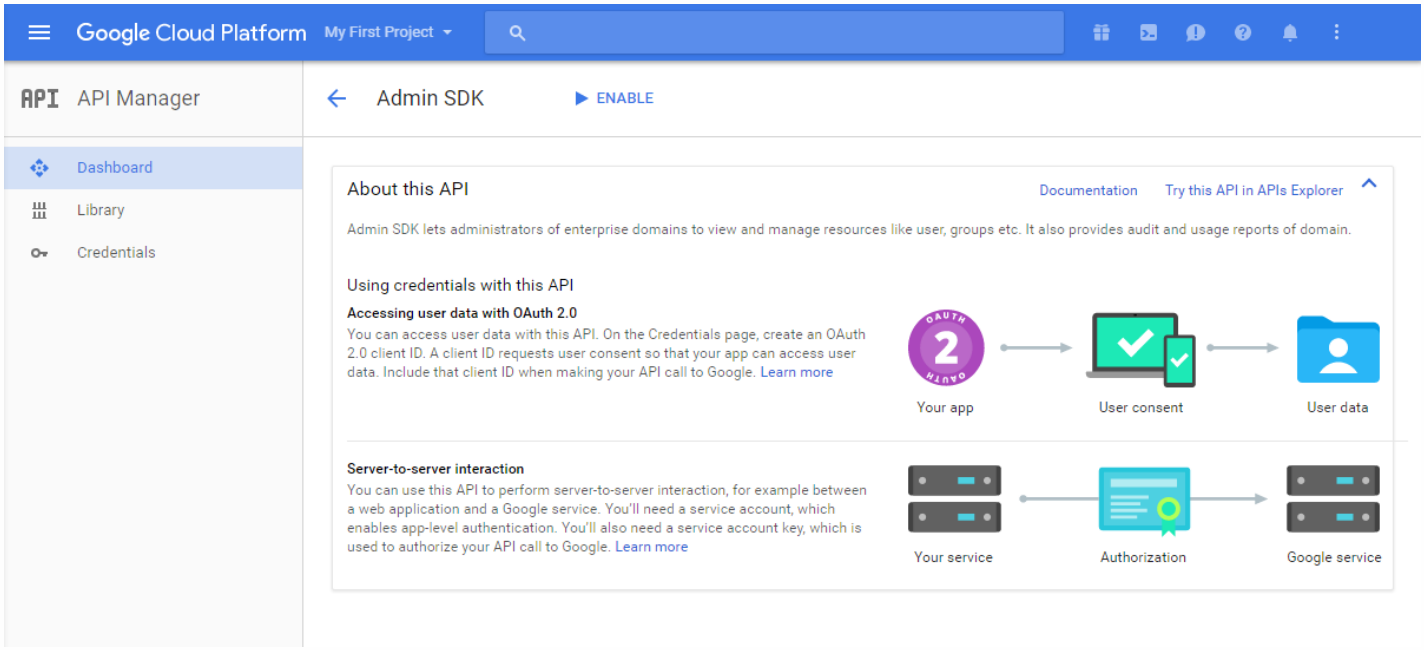
© 1999-2017 Citrix Systems, Inc. All rights reserved.

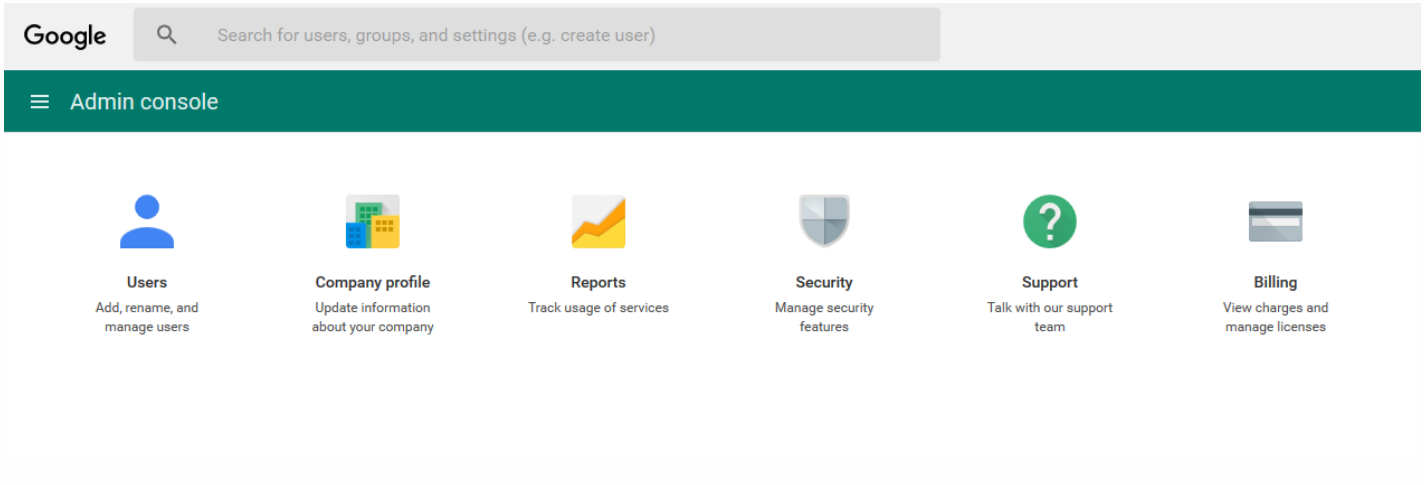




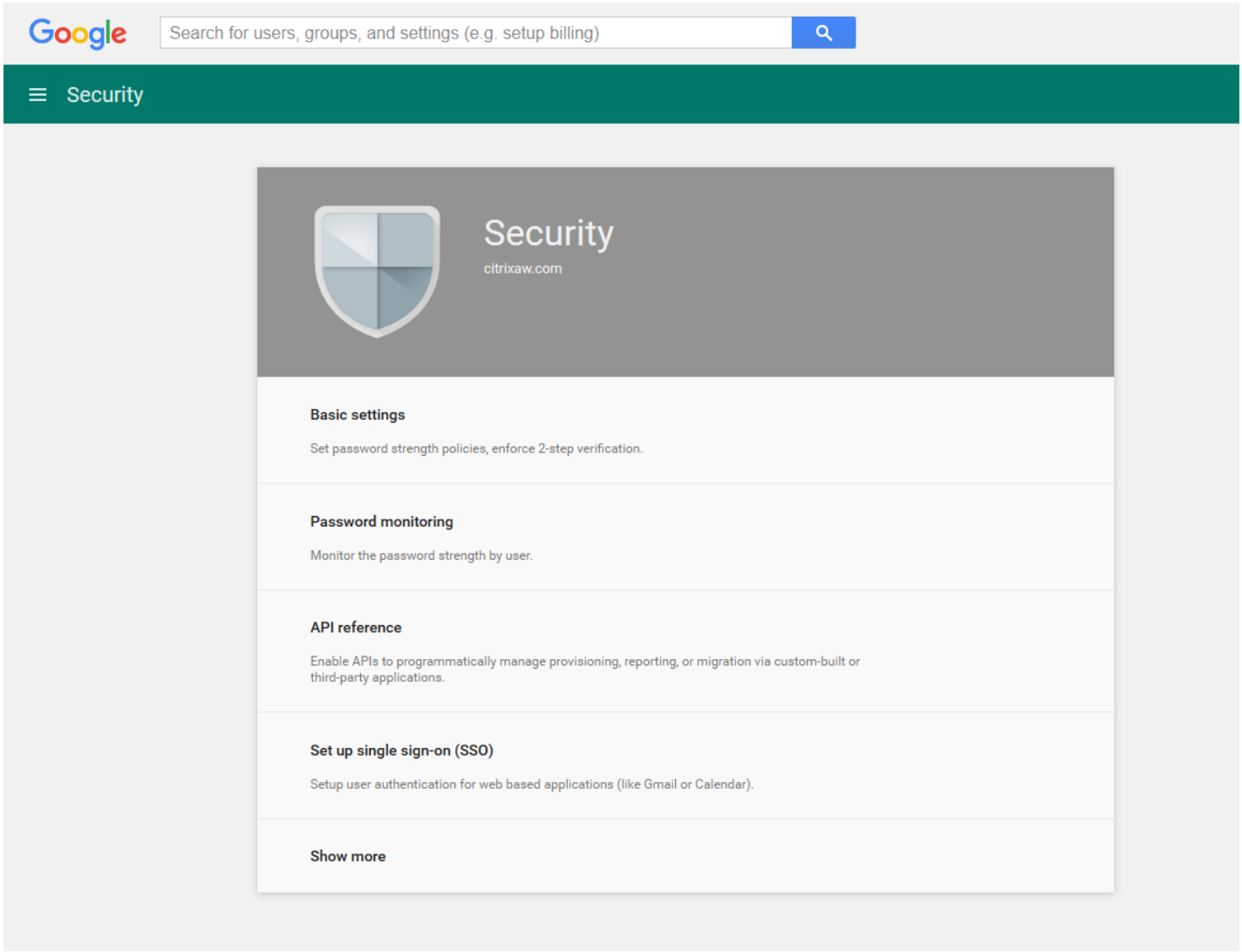
© 1999-2017 Citrix Systems, Inc. All rights reserved.



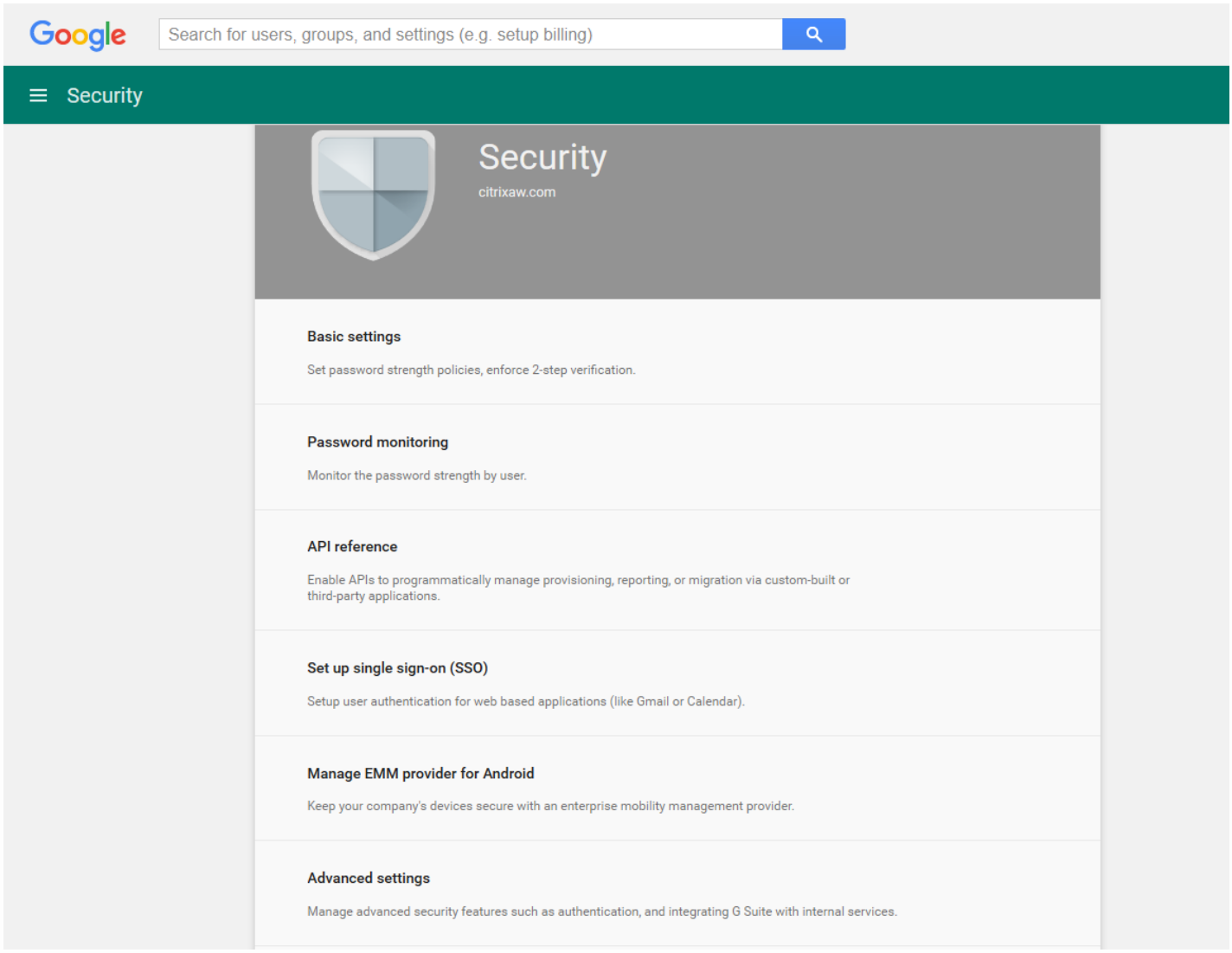




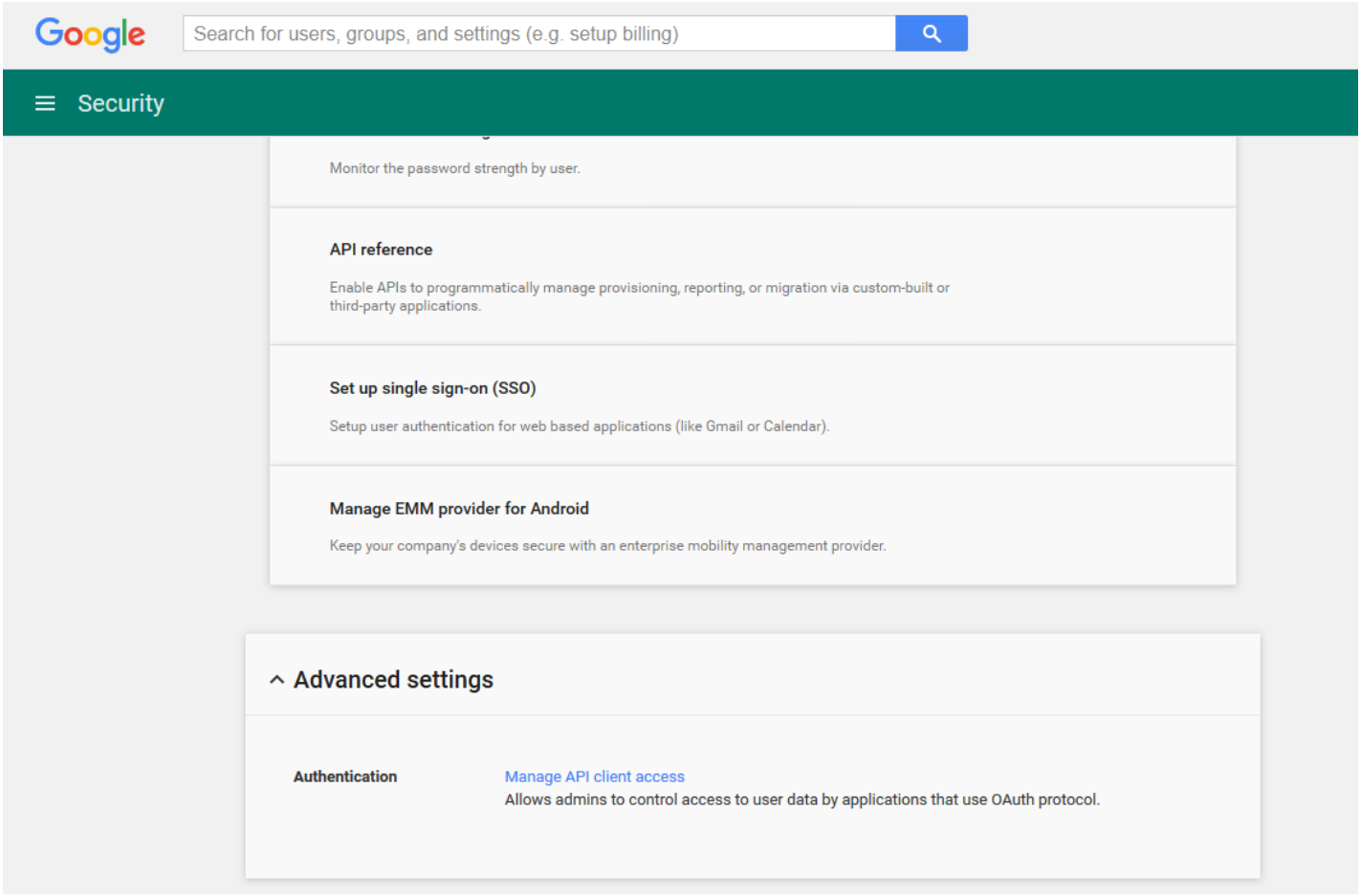
© 1999-2017 Citrix Systems, Inc. All rights reserved.

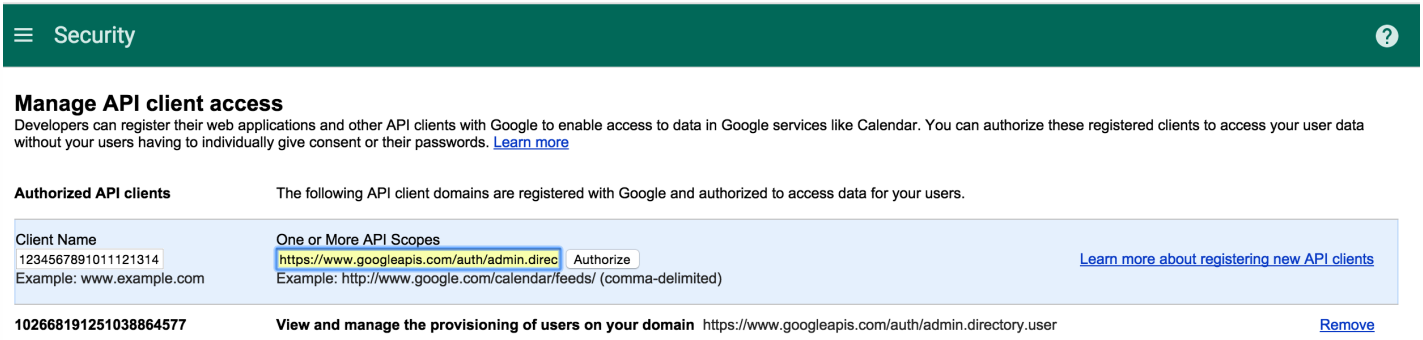


© 1999-2017 Citrix Systems, Inc. All rights reserved.



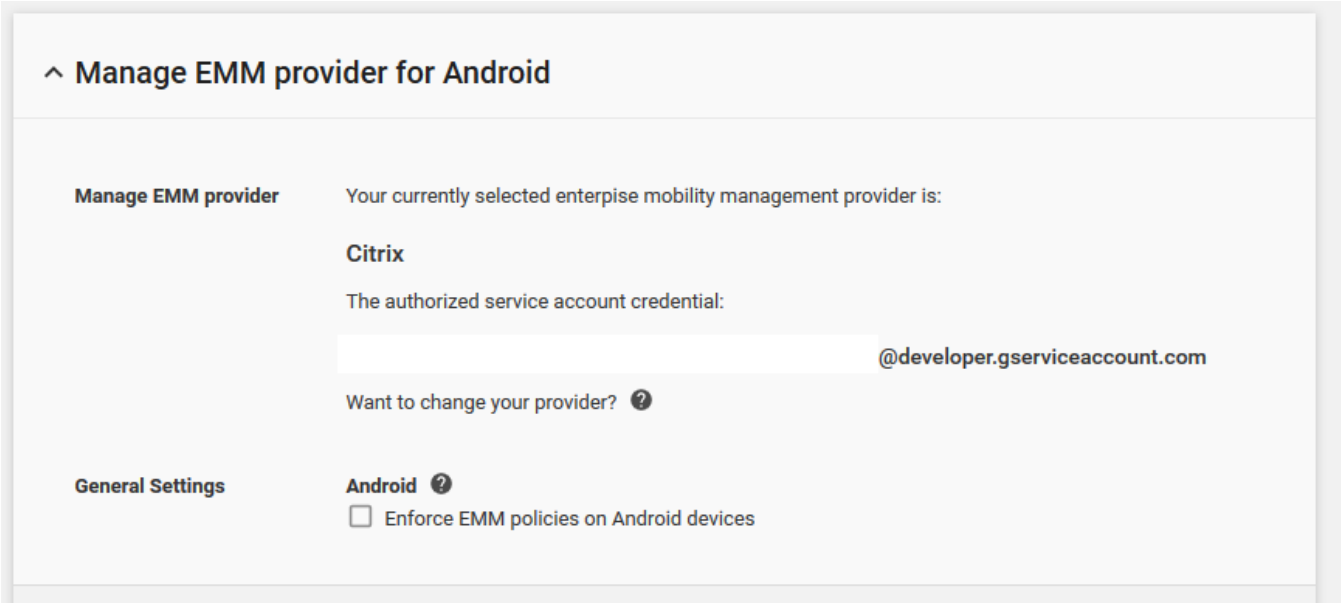
© 1999-2017 Citrix Systems, Inc. All rights reserved.



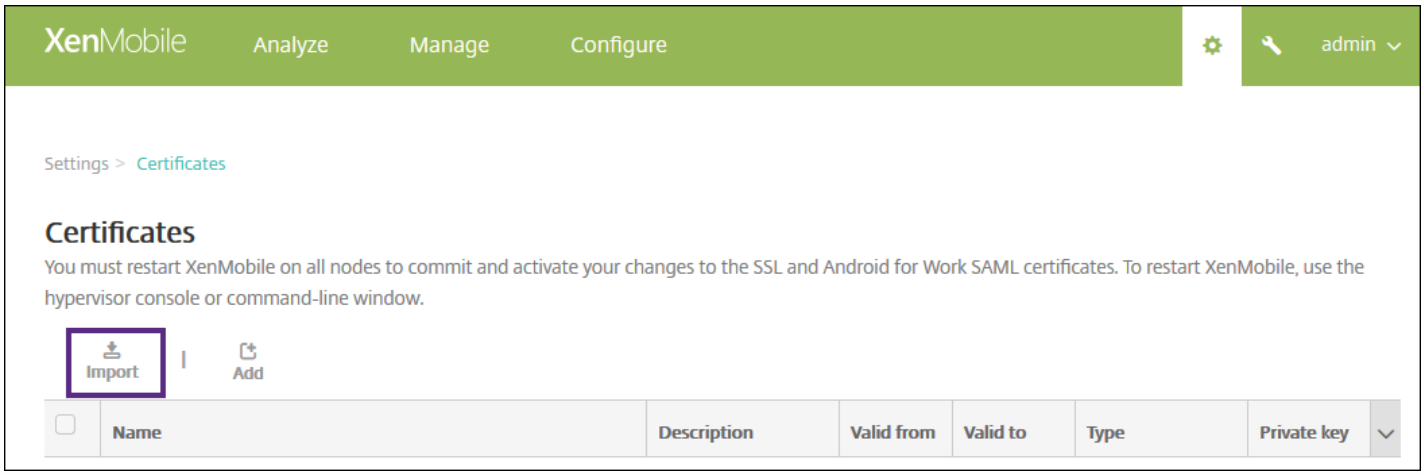


Vinculando ao EMM

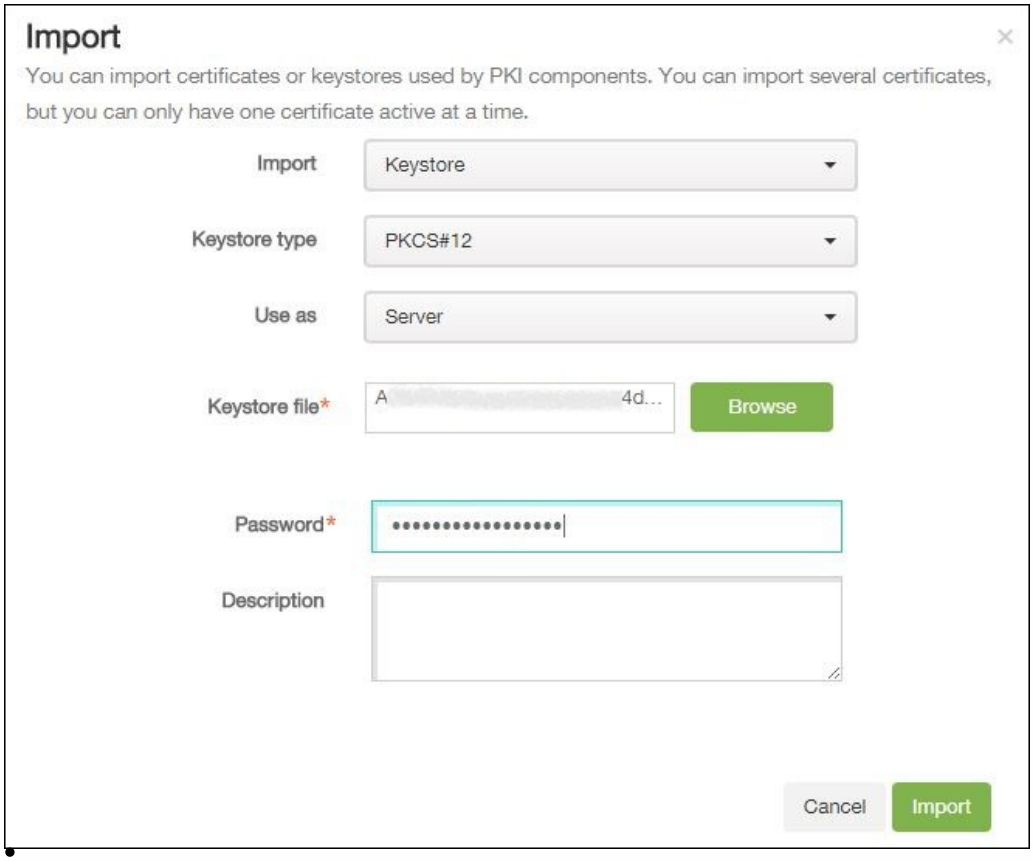
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Importe o certificado P12



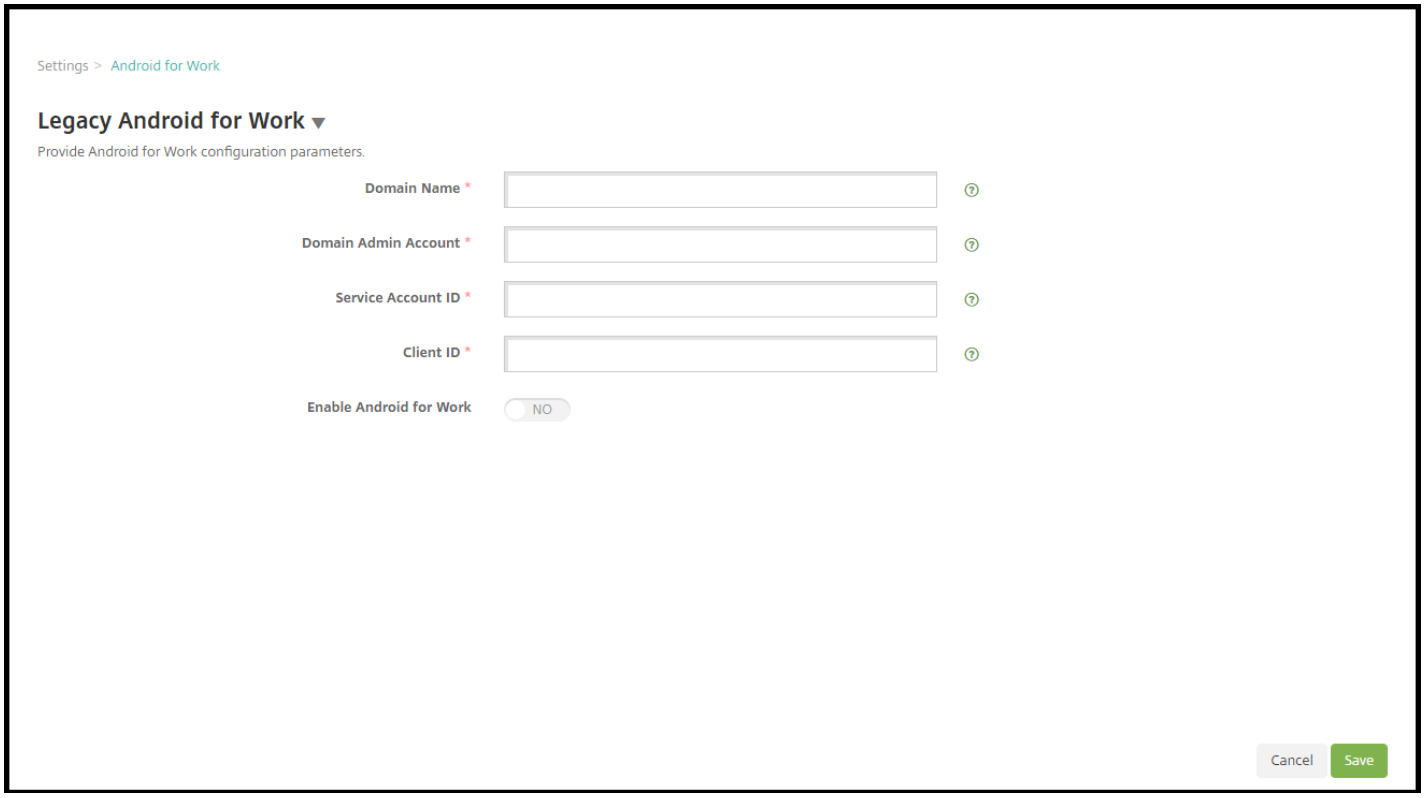
© 1999-2017 Citrix Systems, Inc. All rights reserved.



-
-
-
-
-
-

Definir as configurações de servidor do Android for Work

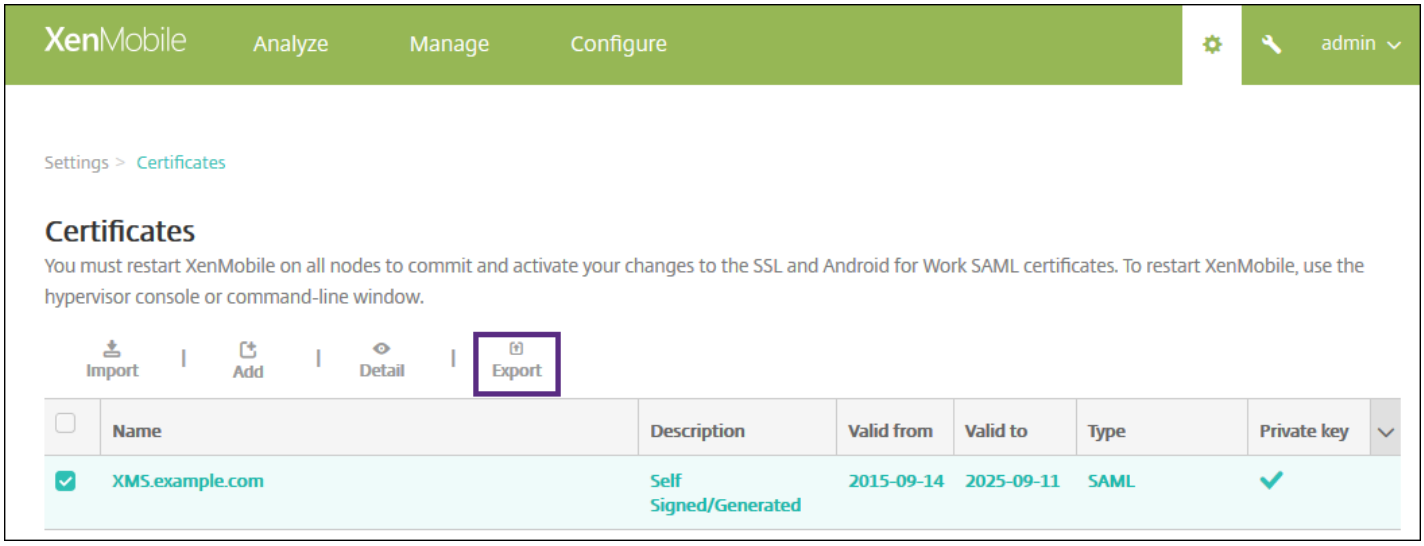
© 1999-2017 Citrix Systems, Inc. All rights reserved.

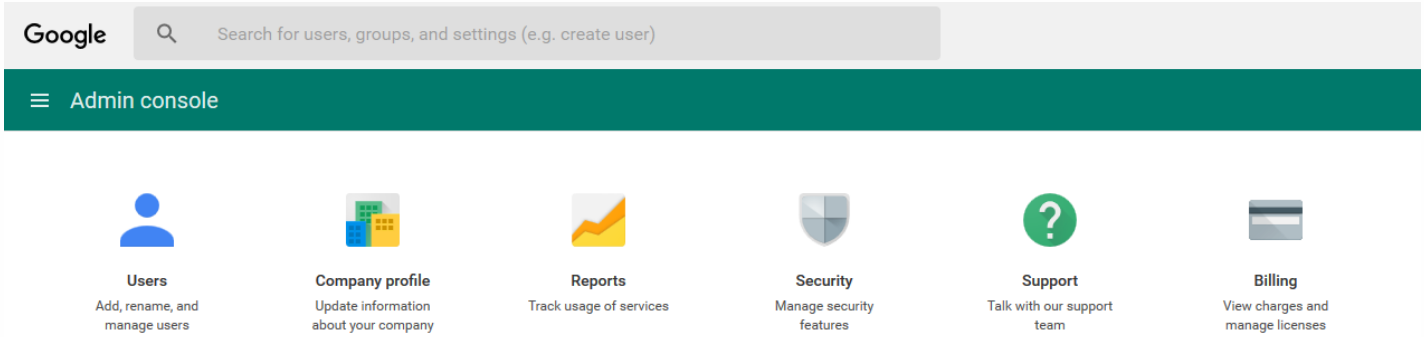


-
-
-
-
-

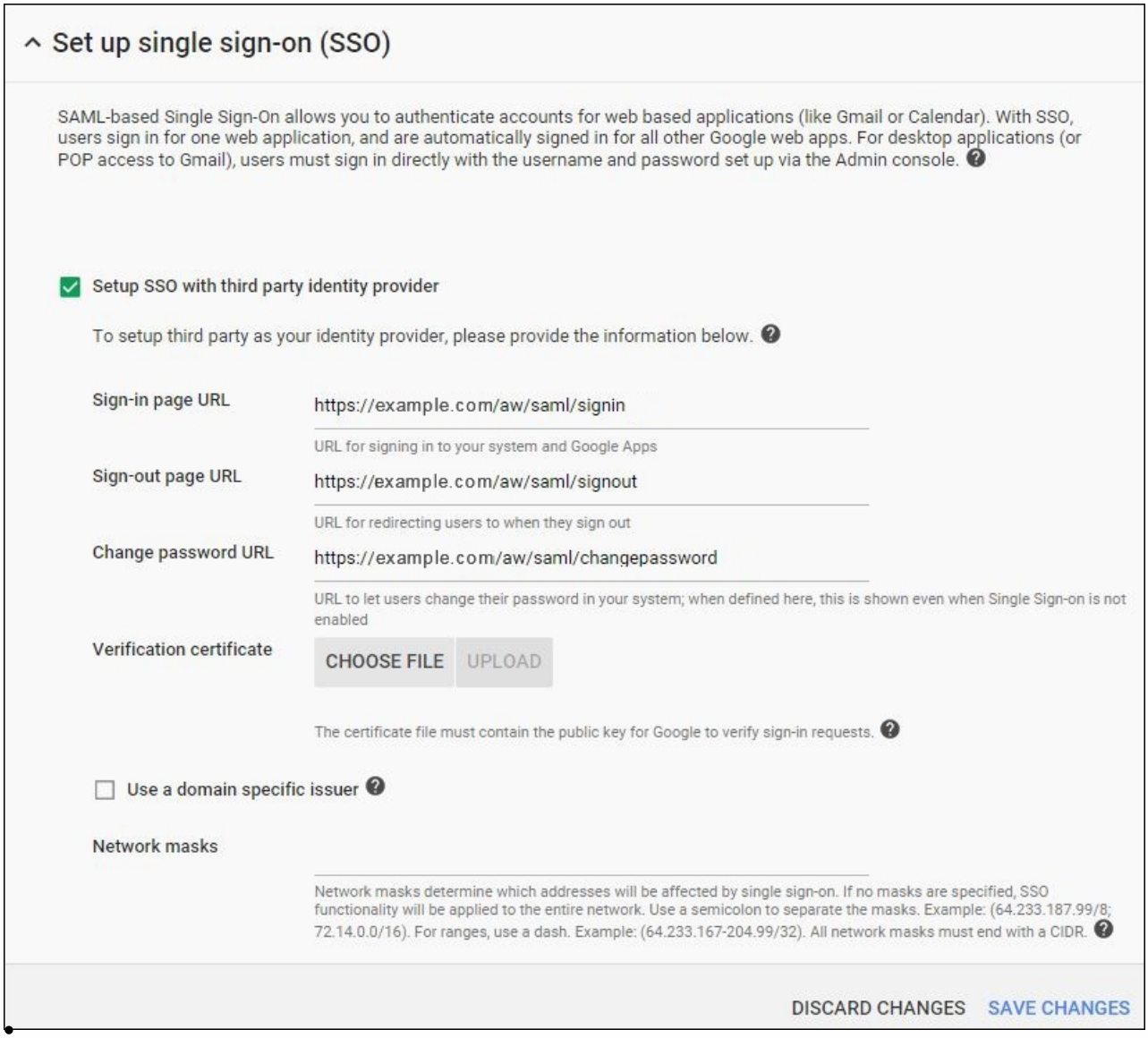
Ativar o logon único baseado em SAML

© 1999-2017 Citrix Systems, Inc. All rights reserved.





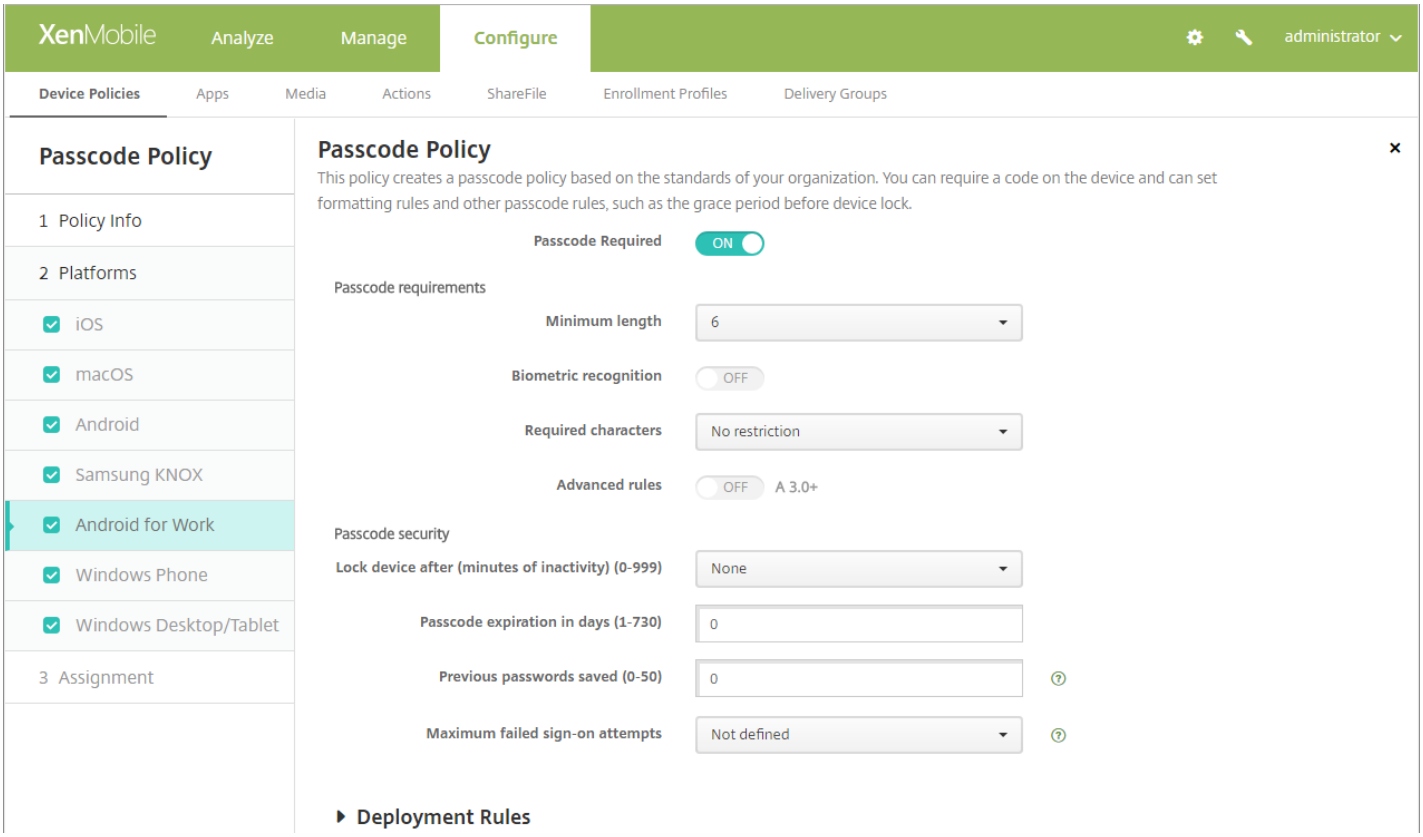
© 1999-2017 Citrix Systems, Inc. All rights reserved.



-
-
-
-

Configurar uma política de dispositivo do Android for Work

© 1999-2017 Citrix Systems, Inc. All rights reserved.



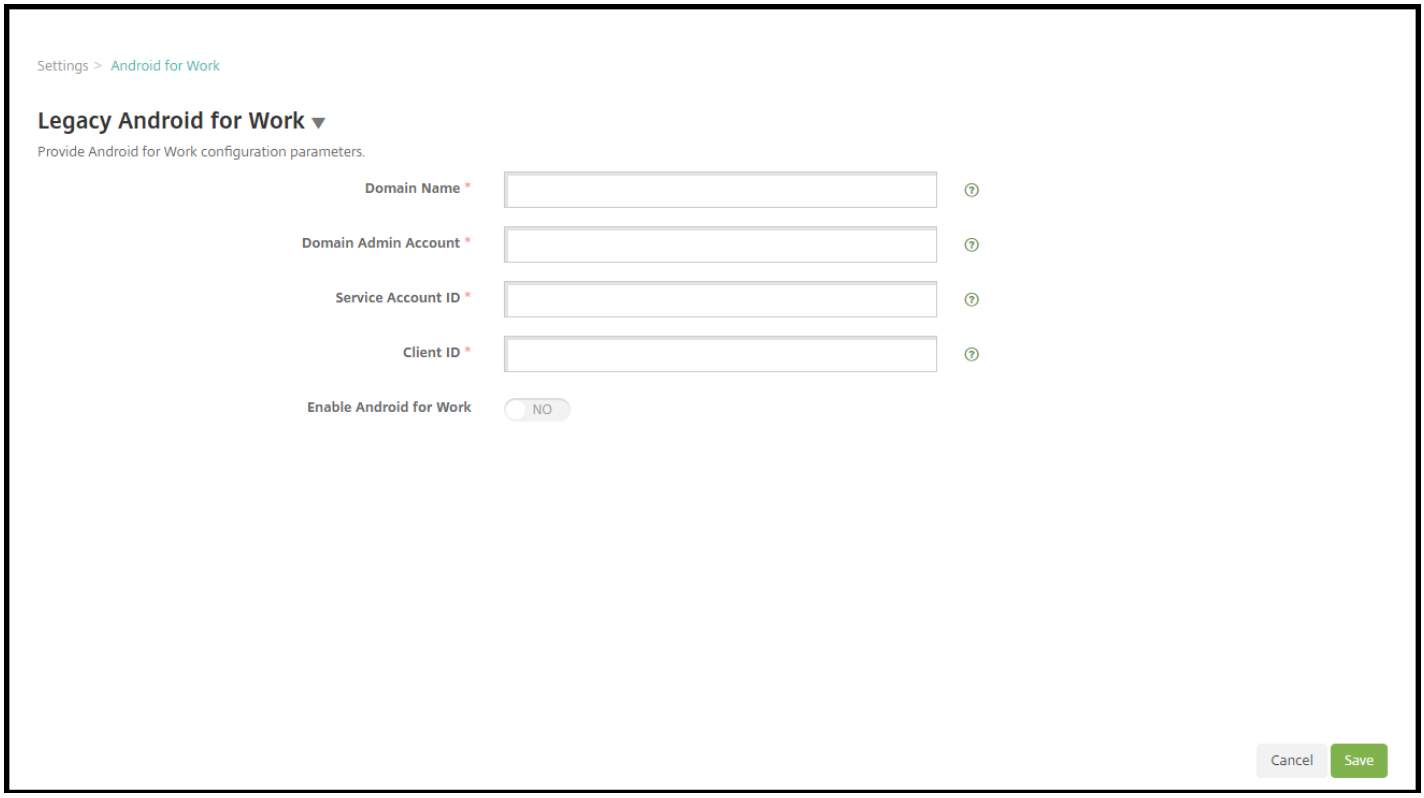
Políticas MDX e as políticas de dispositivo com suporte

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Definir as configurações de conta do Android for Work

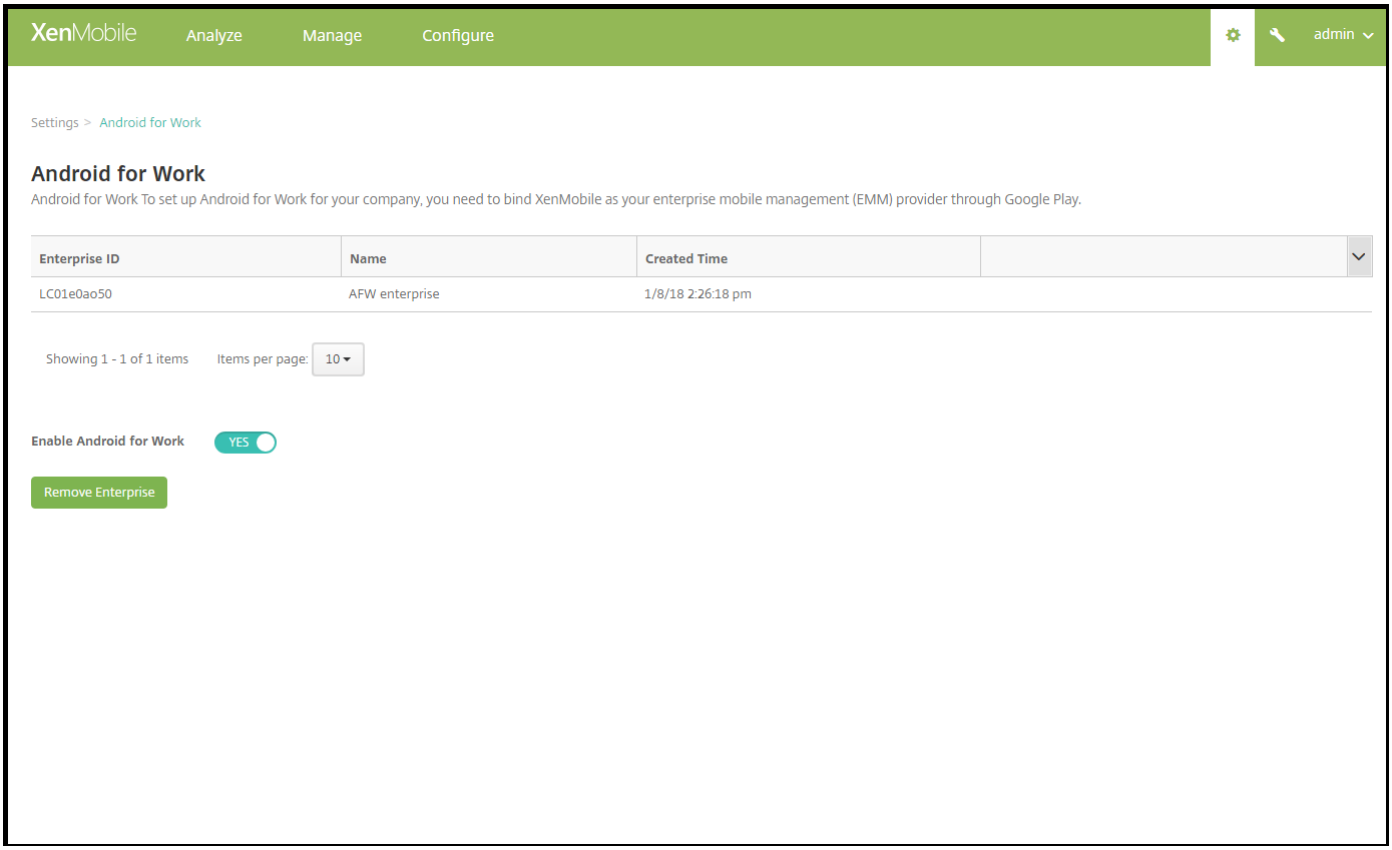
© 1999-2017 Citrix Systems, Inc. All rights reserved.



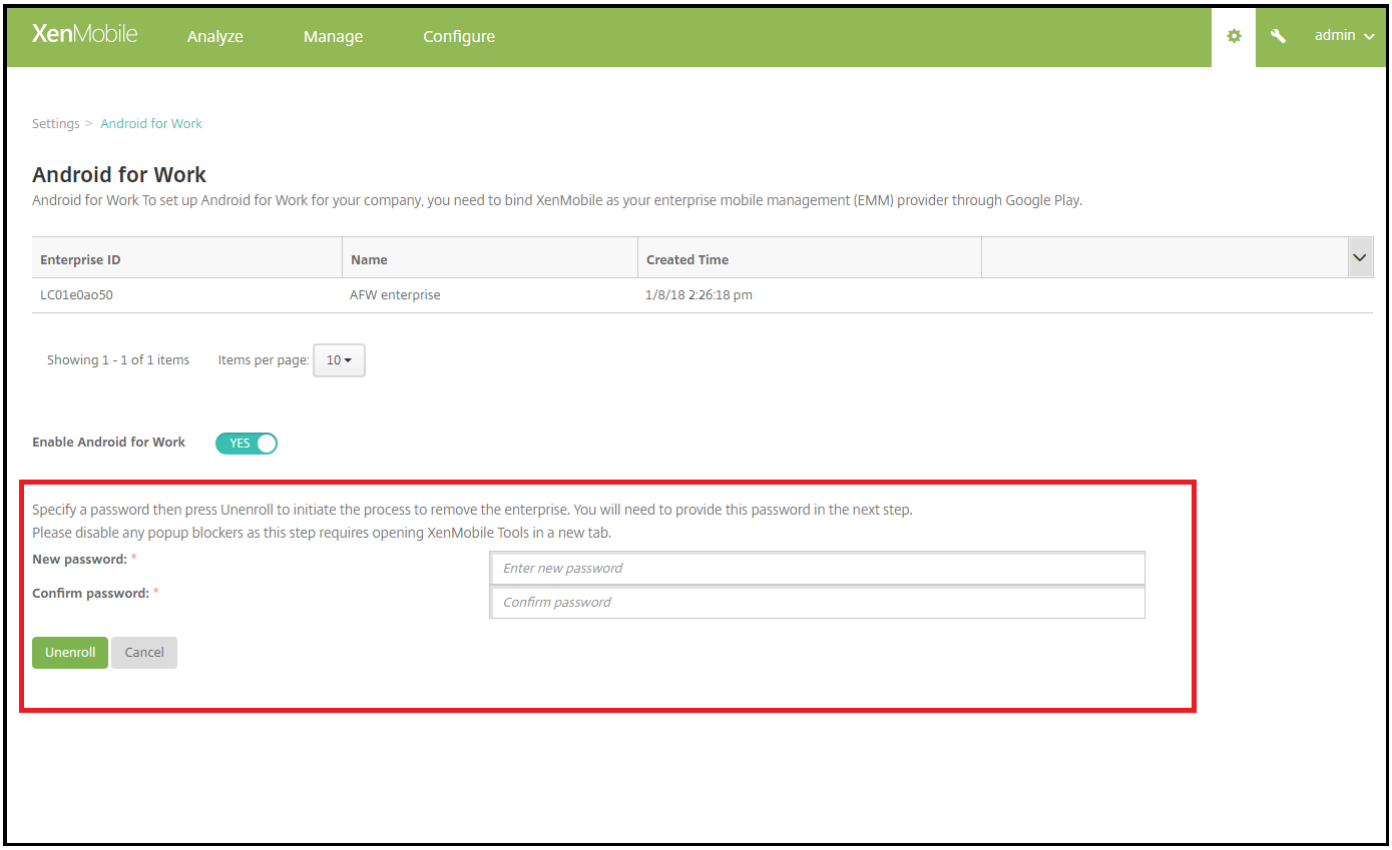
-
-
-
-
-

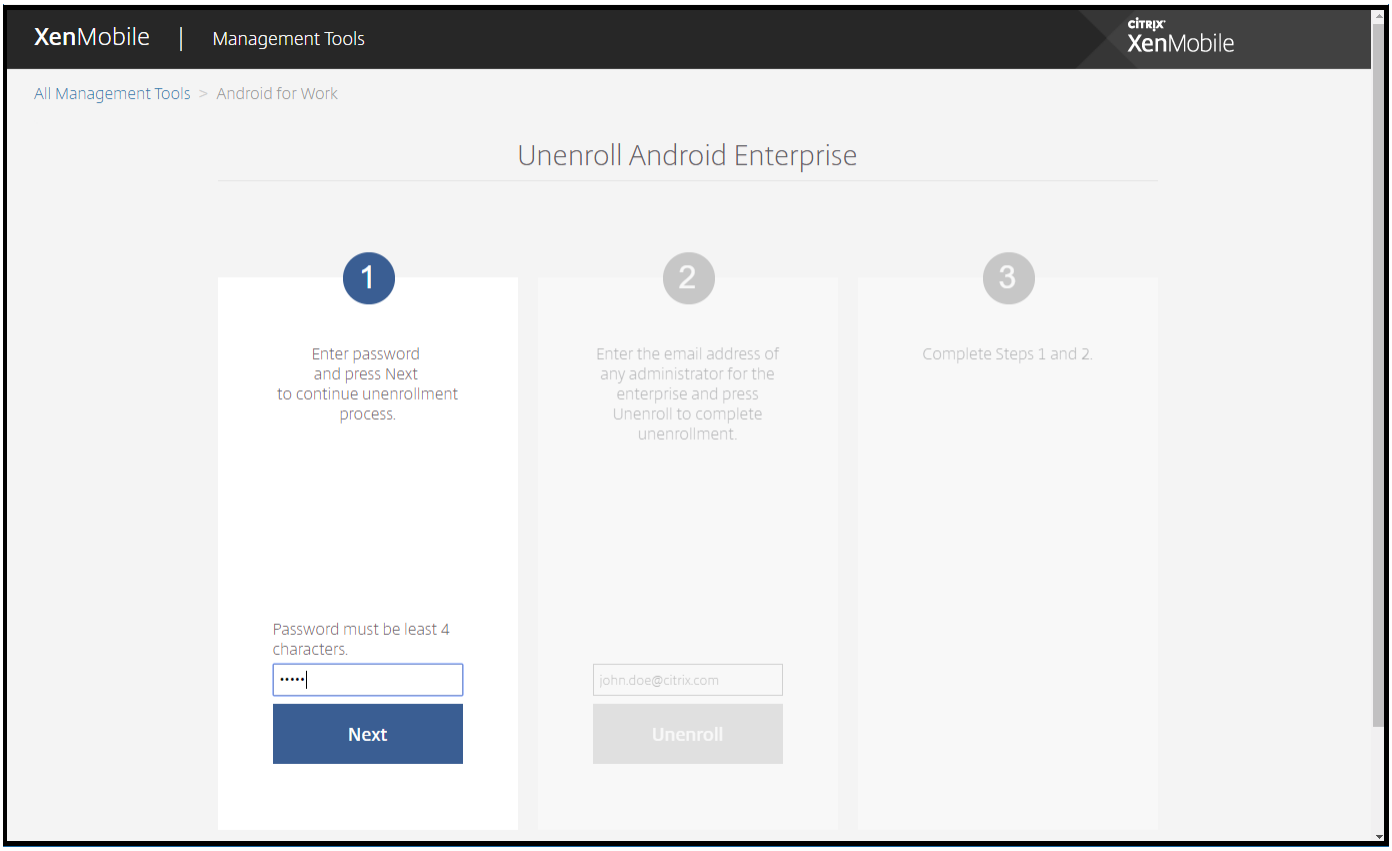
© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-

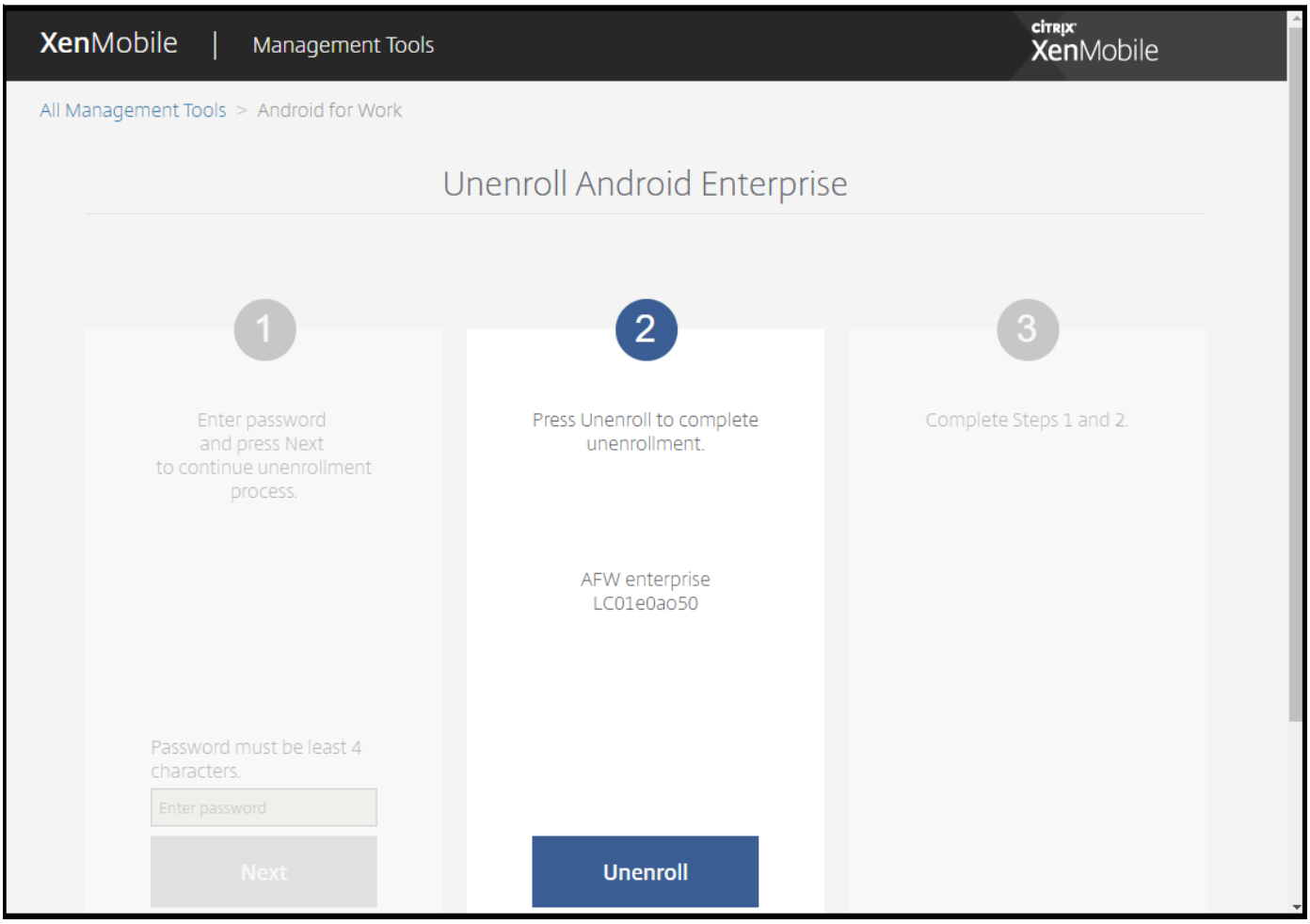


© 1999-2017 Citrix Systems, Inc. All rights reserved.





© 1999-2017 Citrix Systems, Inc. All rights reserved.



-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-

afw#xenmobile

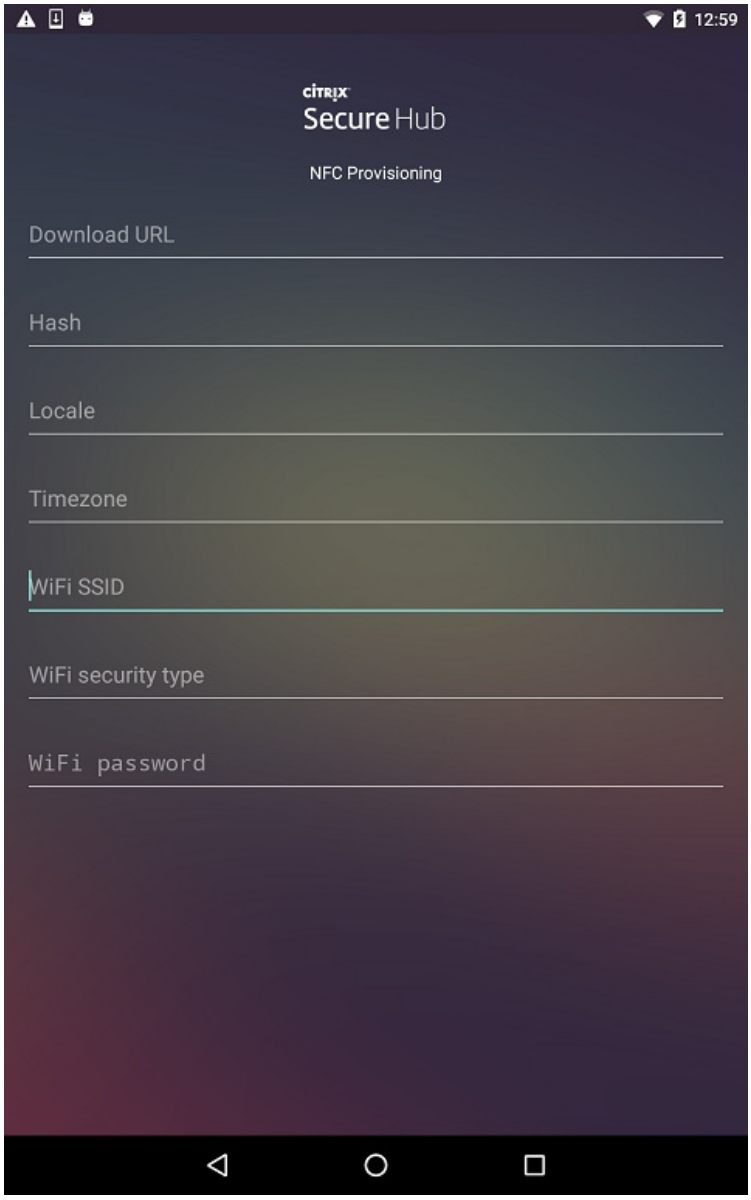
Compartilhamento por NFC

-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-

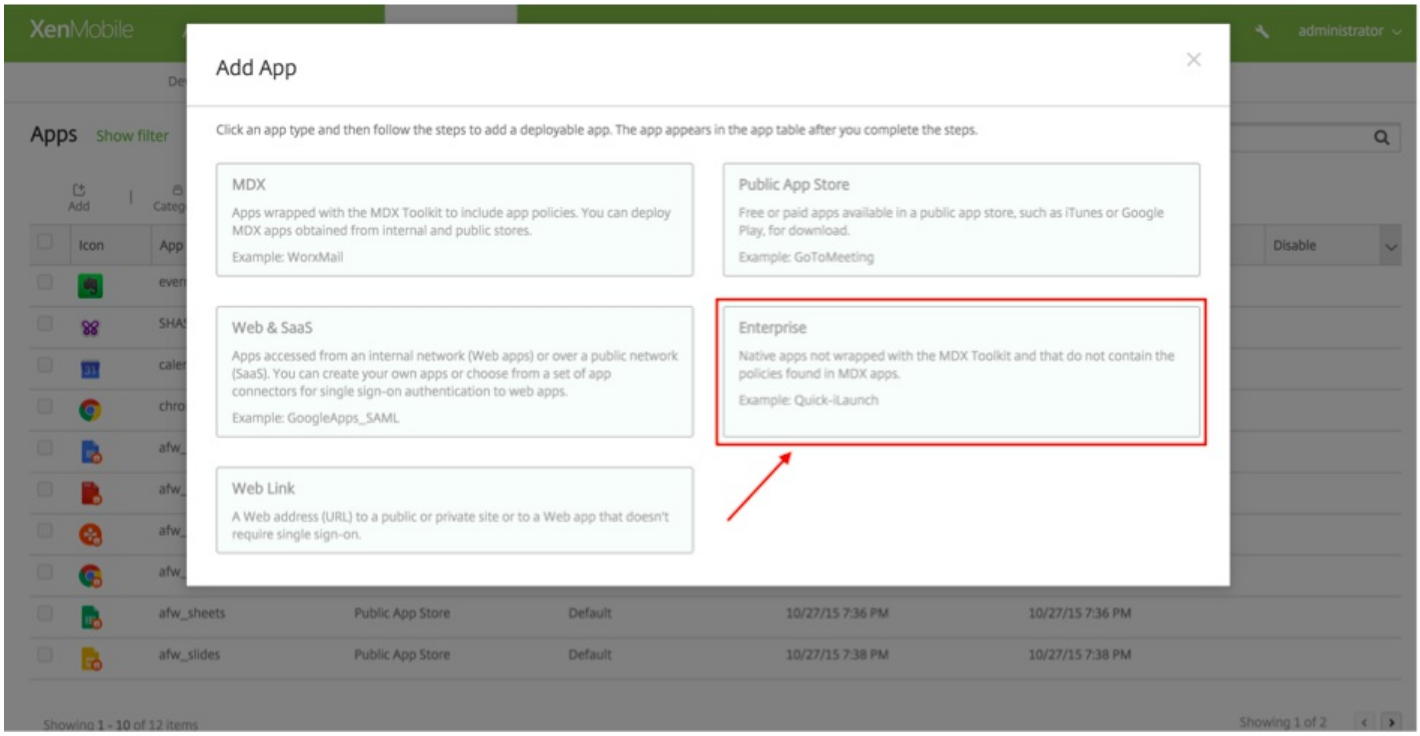
-
-

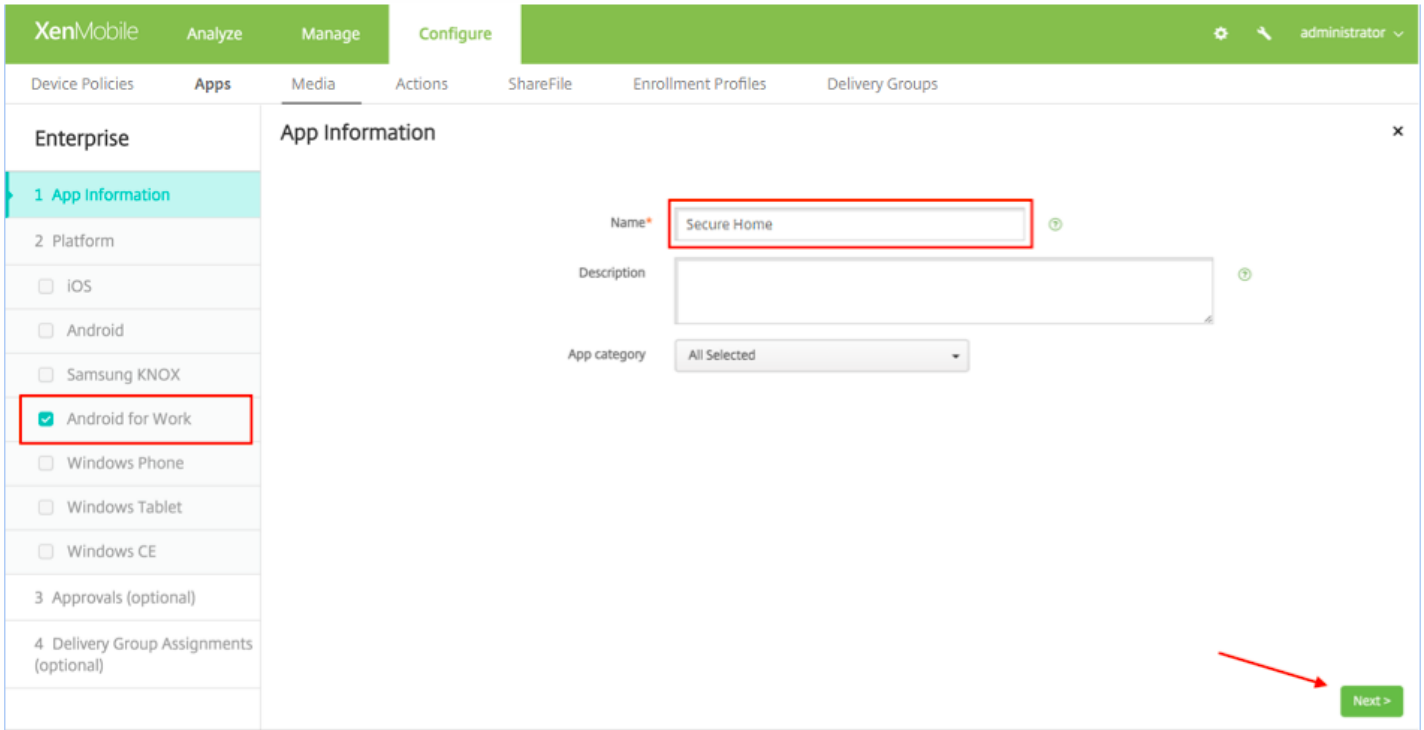


© 1999-2017 Citrix Systems, Inc. All rights reserved.

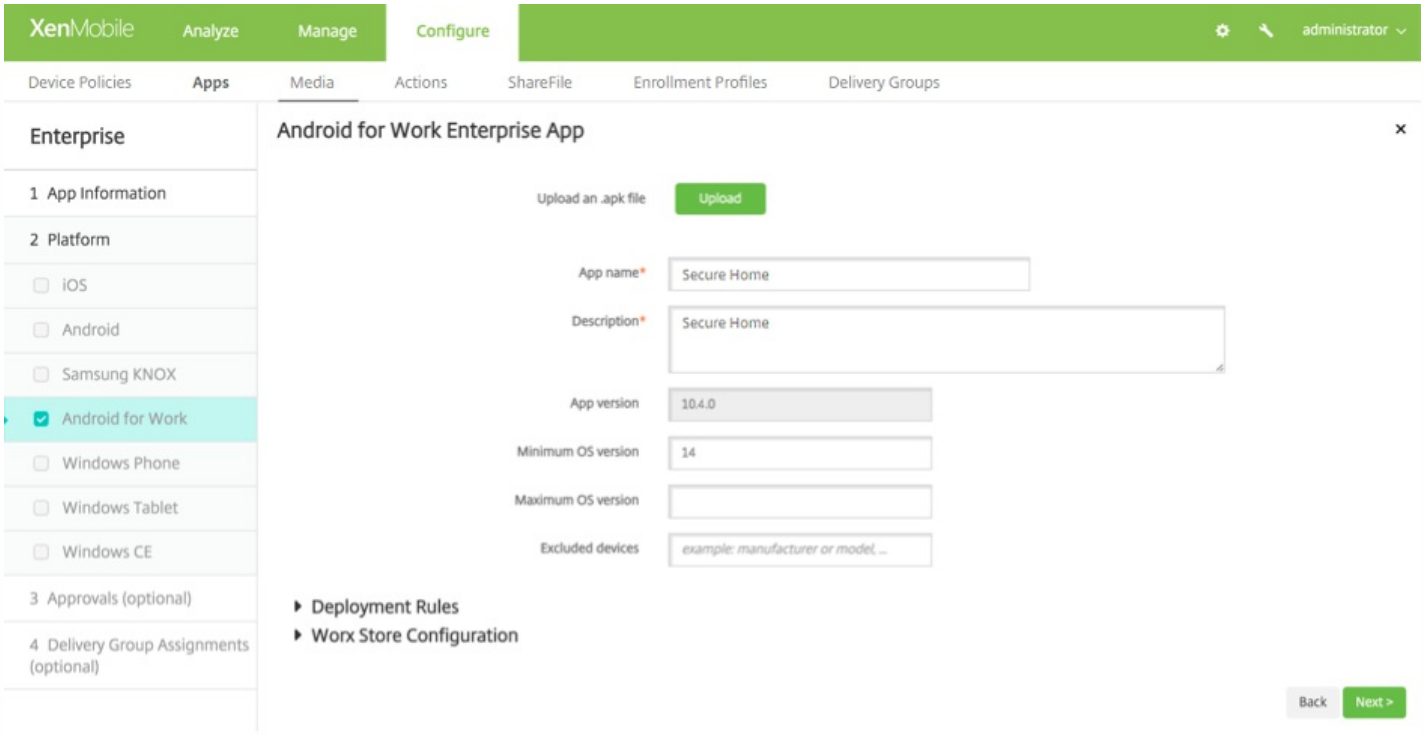
© 1999-2017 Citrix Systems, Inc. All rights reserved.

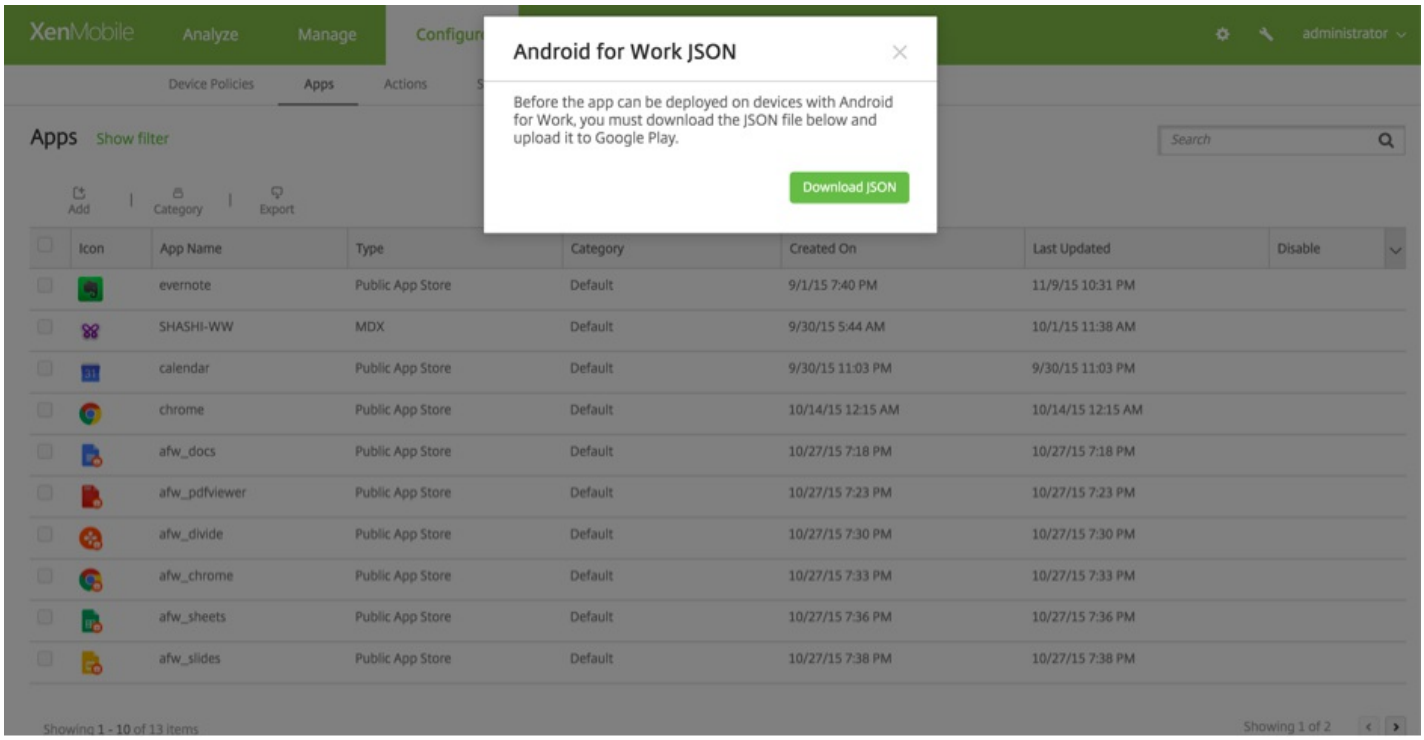
© 1999-2017 Citrix Systems, Inc. All rights reserved.

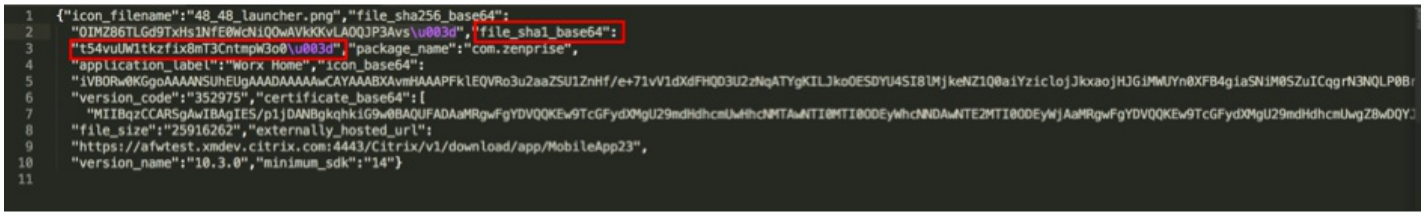




© 1999-2017 Citrix Systems, Inc. All rights reserved.







© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-

-
-
-
-

Código QR

-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
{
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME": "com.zenprise/com.zenprise.configuration.AdminFunction",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM": "qn7oZUtheu3JBAinzZRrrjCQv6LOO6Ll1OjcxT3-yKM",
  "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION": "https://www.example.com/securehub.apk",
  "android.app.extra.PROVISIONING_LOCALE": "en_US",
  "android.app.extra.PROVISIONING_TIME_ZONE": "America/Los_Angeles",
  "android.app.extra.PROVISIONING_LOCAL_TIME": 1507852861778,
  "android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false
}
```

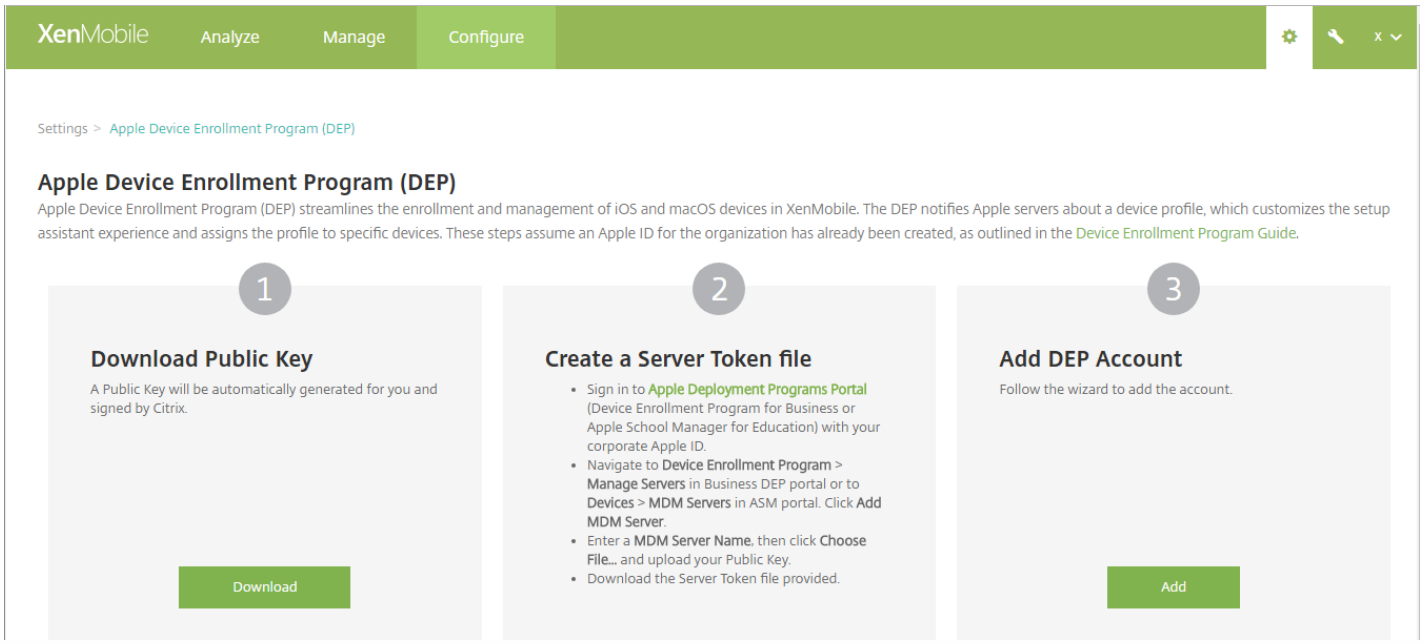

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

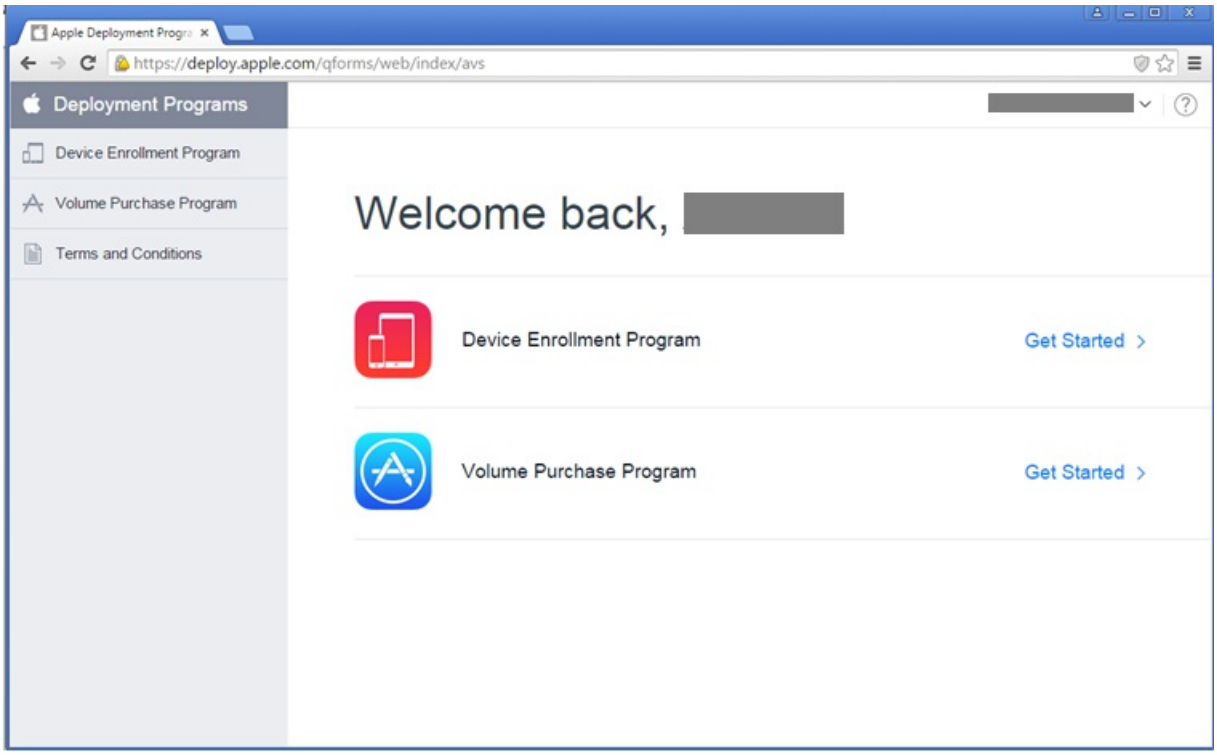
-
-

Etapa 1: baixe uma chave pública do XenMobile Server

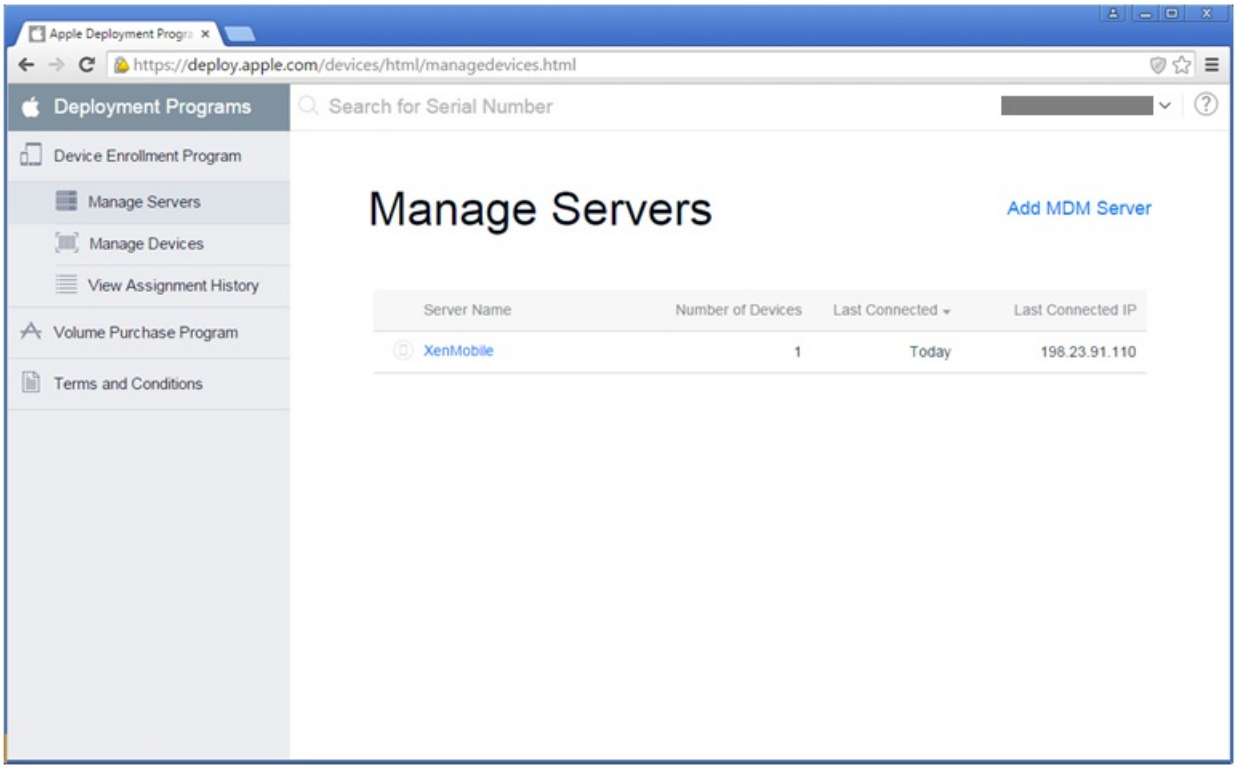
© 1999-2017 Citrix Systems, Inc. All rights reserved.

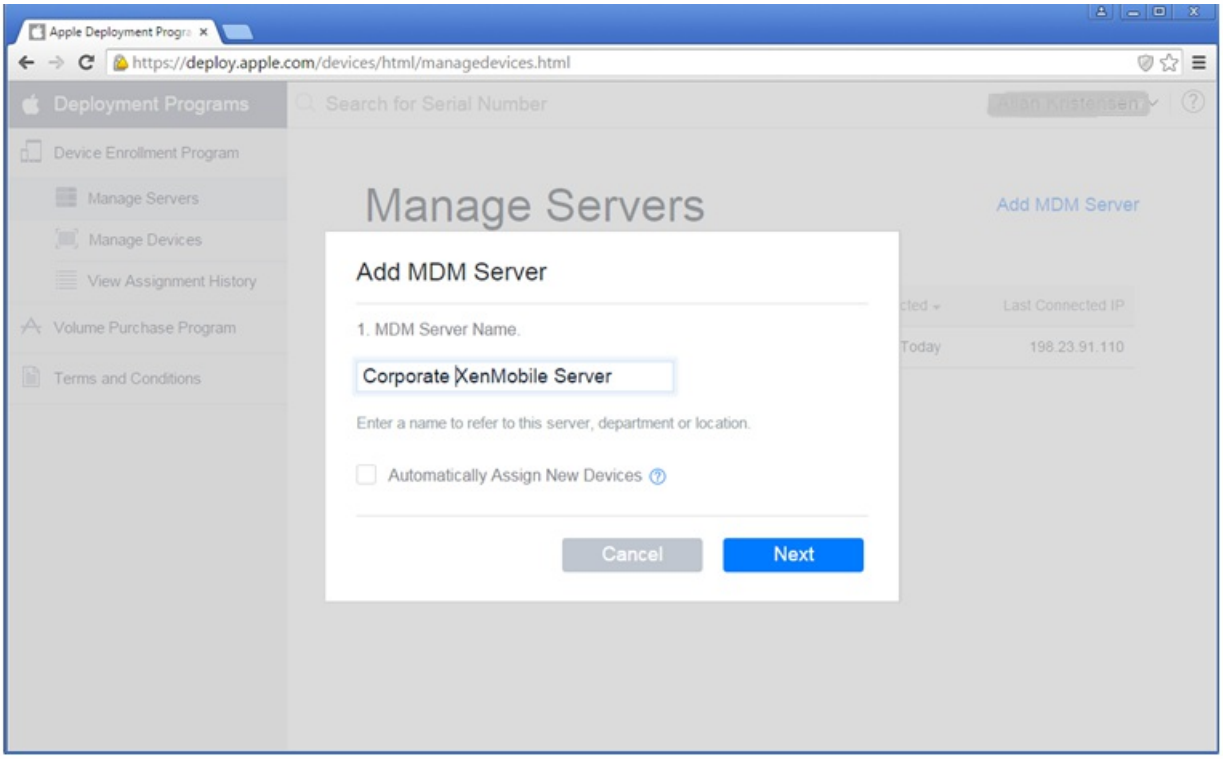


Etapa 2: crie e baixe um arquivo de token de servidor da sua conta da Apple

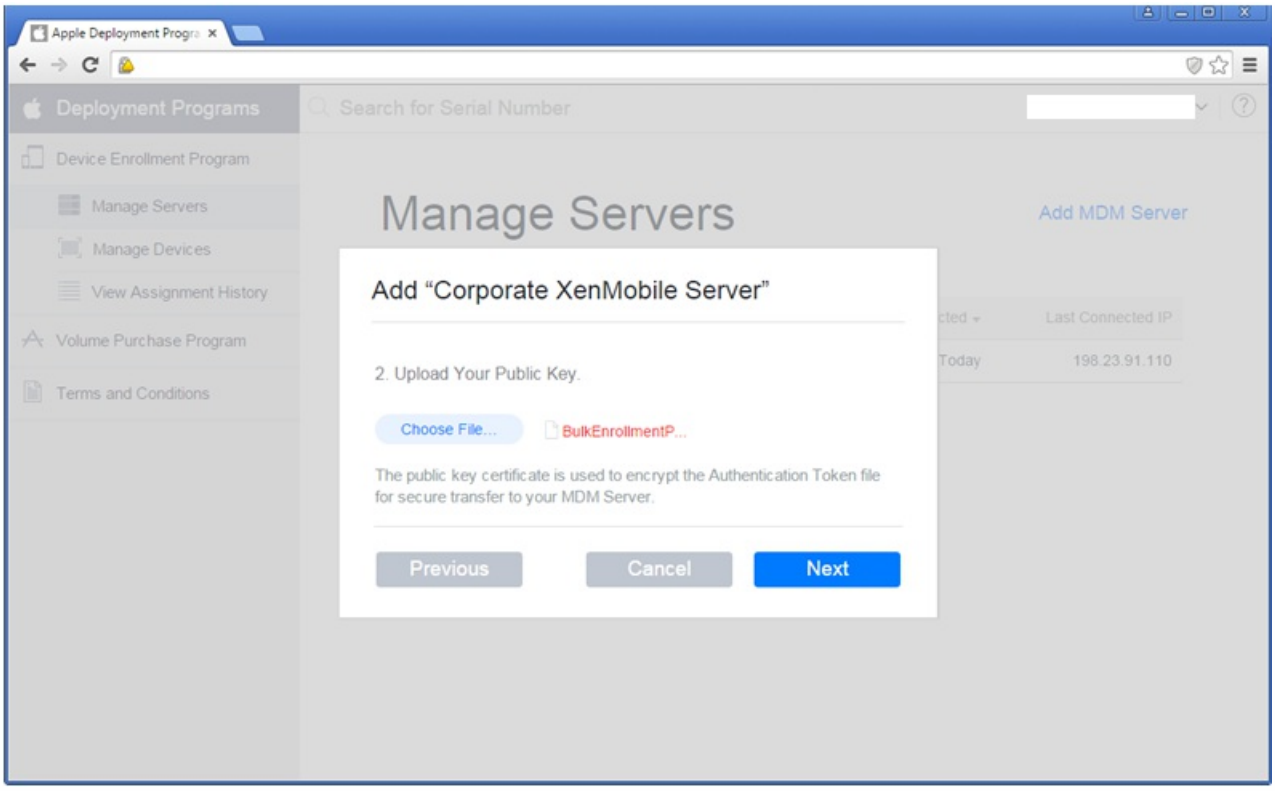


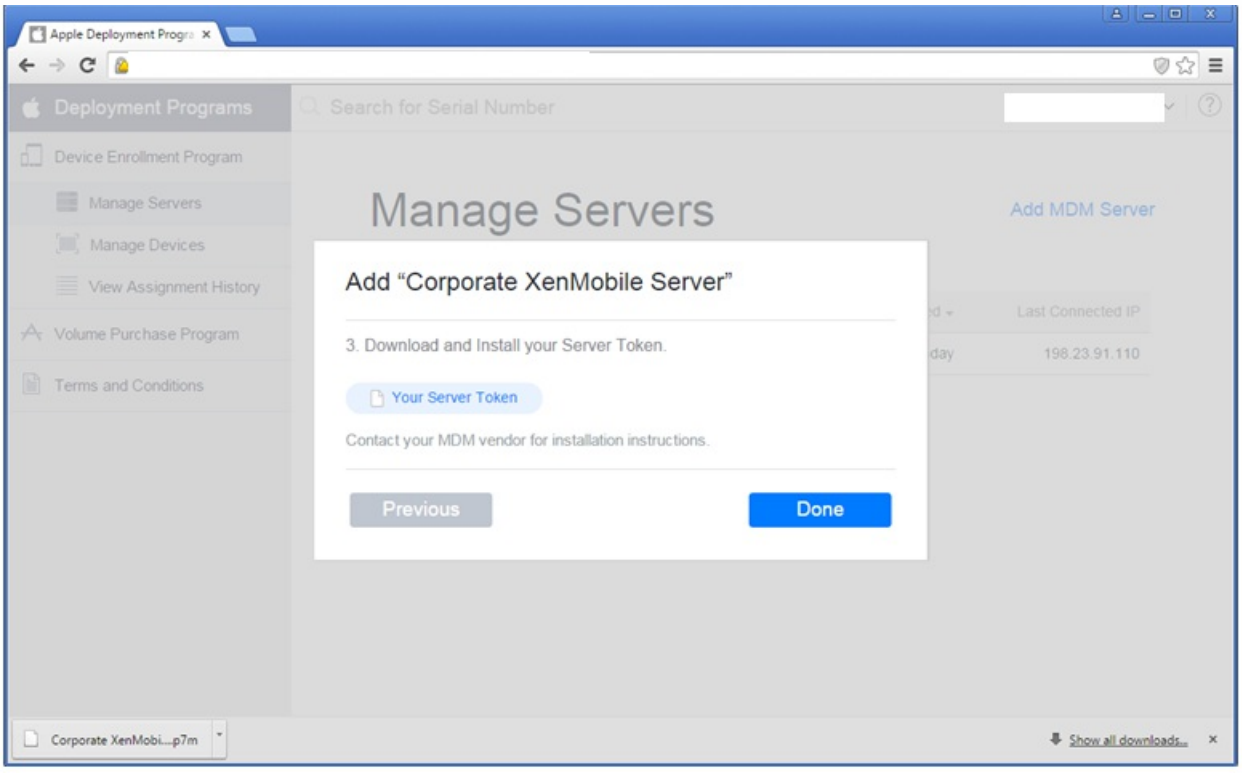
© 1999-2017 Citrix Systems, Inc. All rights reserved.





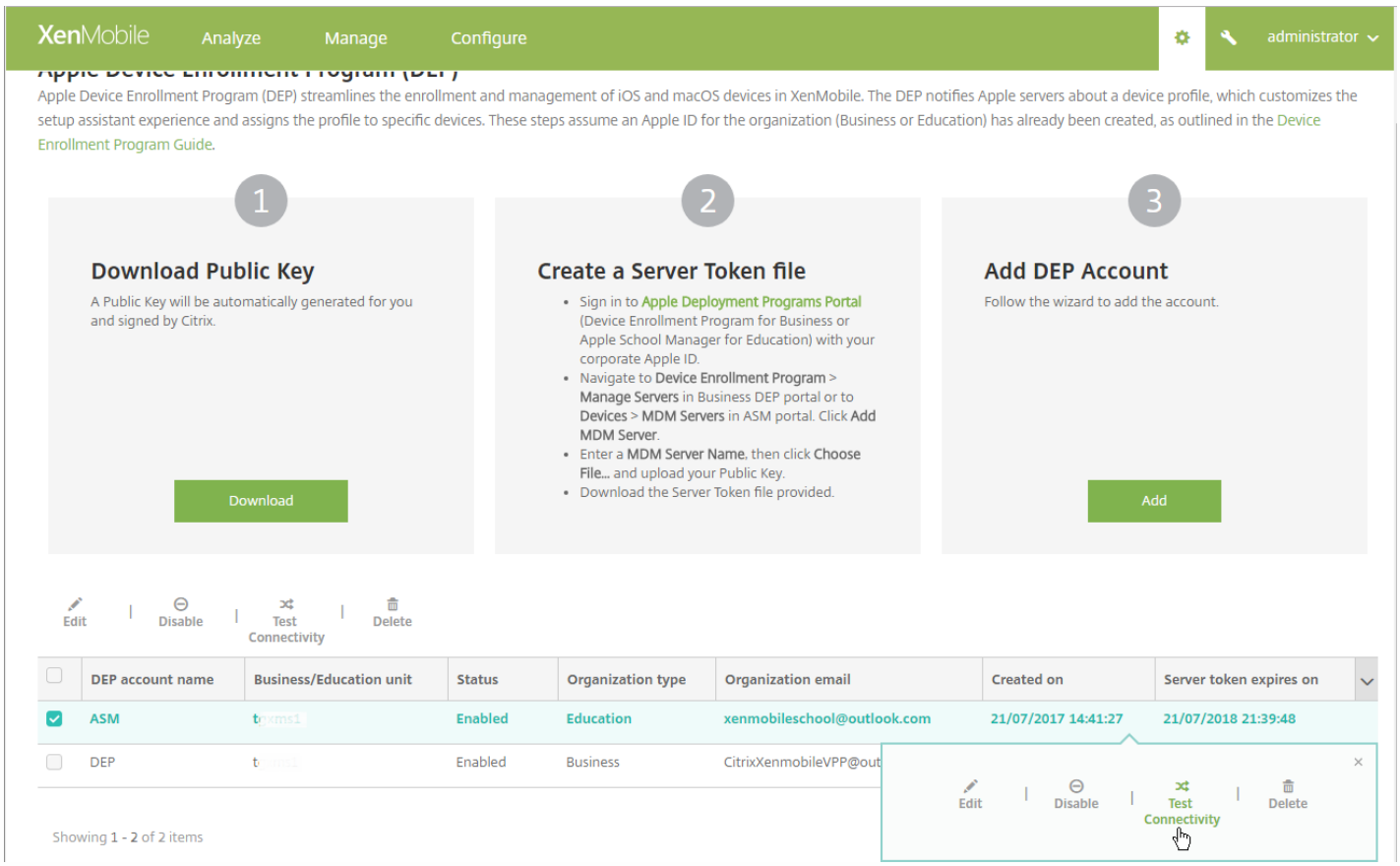
© 1999-2017 Citrix Systems, Inc. All rights reserved.

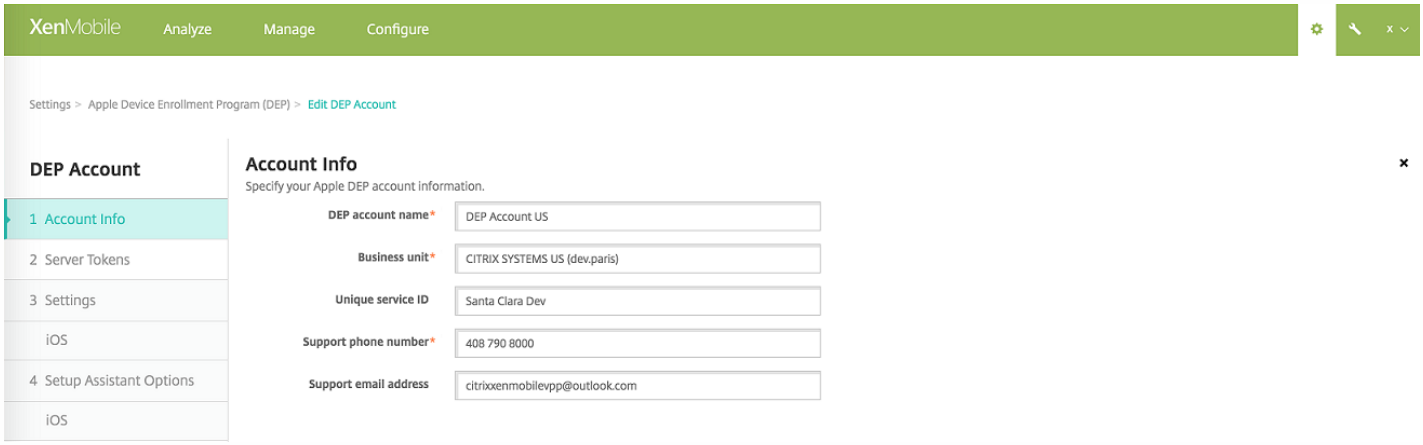




Etapa 3: adicione uma conta do DEP ao XenMobile

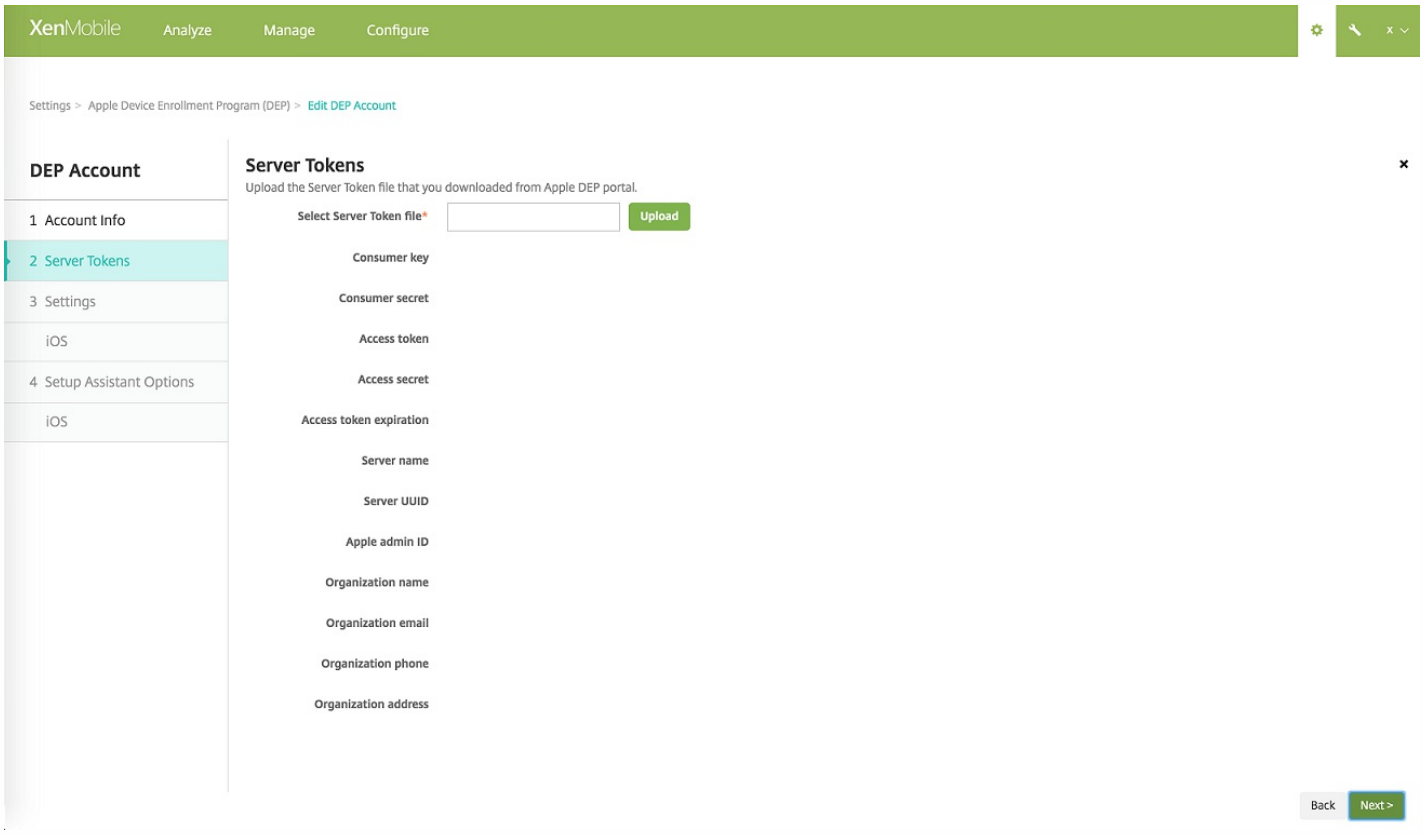
© 1999-2017 Citrix Systems, Inc. All rights reserved.



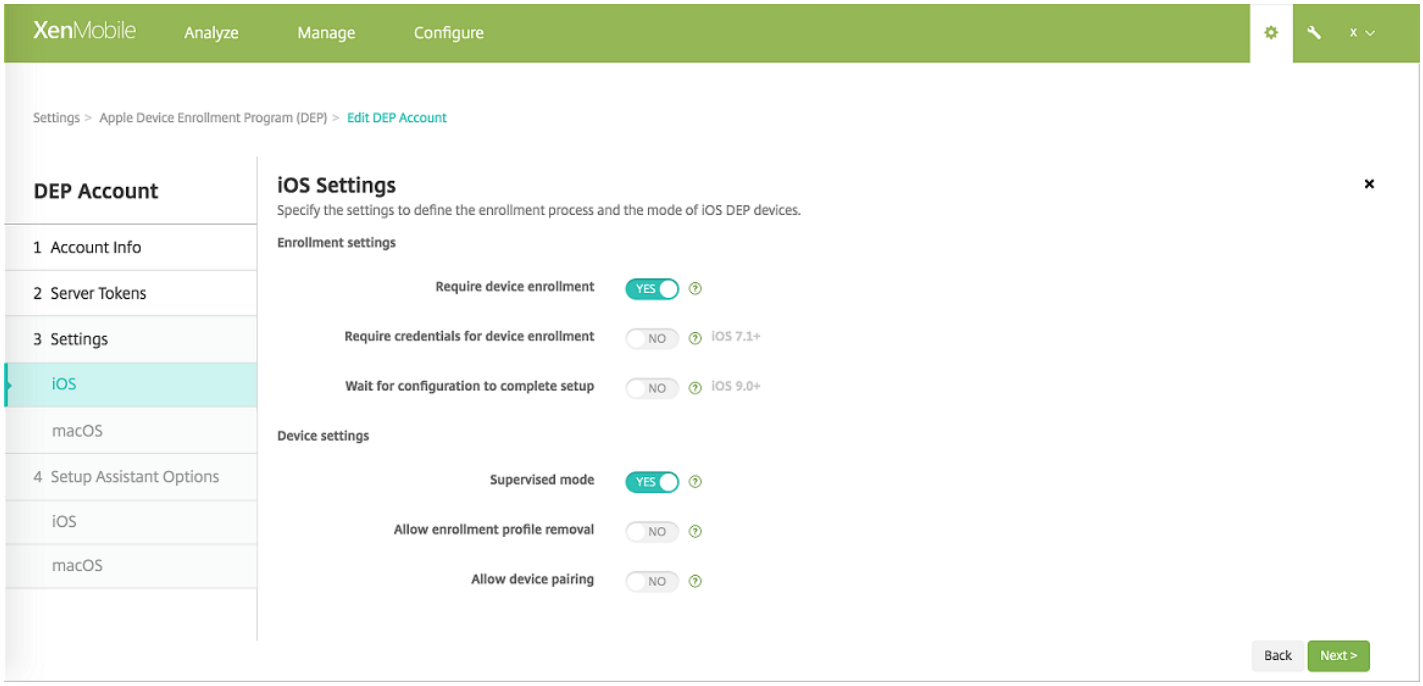


© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-



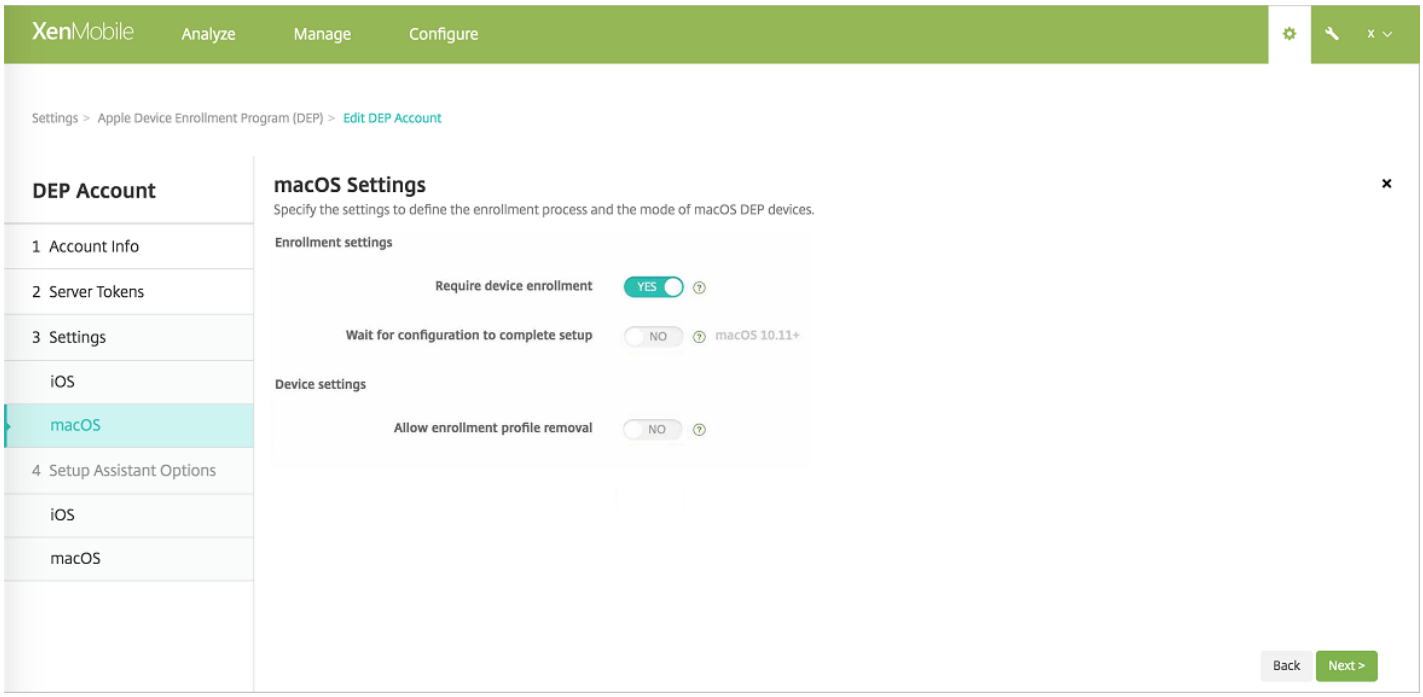
© 1999-2017 Citrix Systems, Inc. All rights reserved.



-
-
-
  -
    -
    -
    -
    -
    -
    -
    -
-

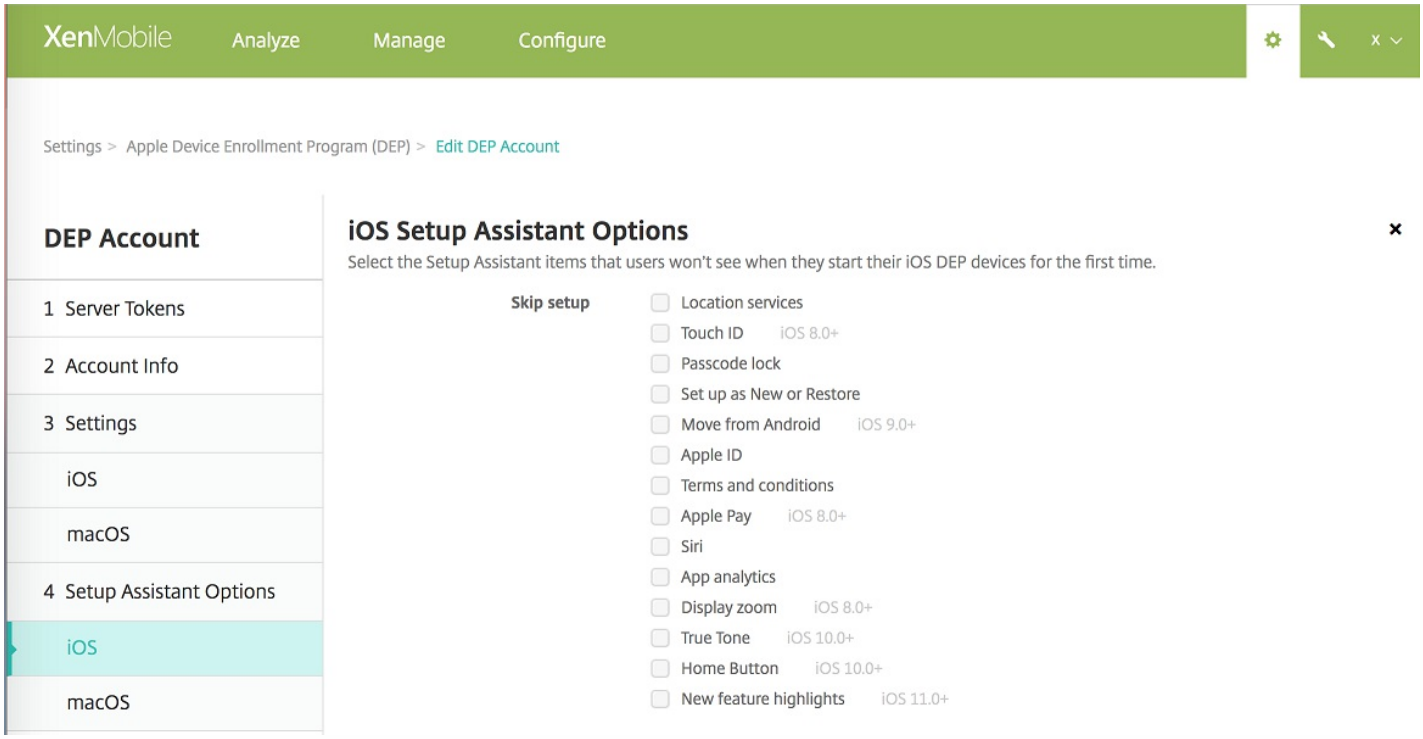
© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-

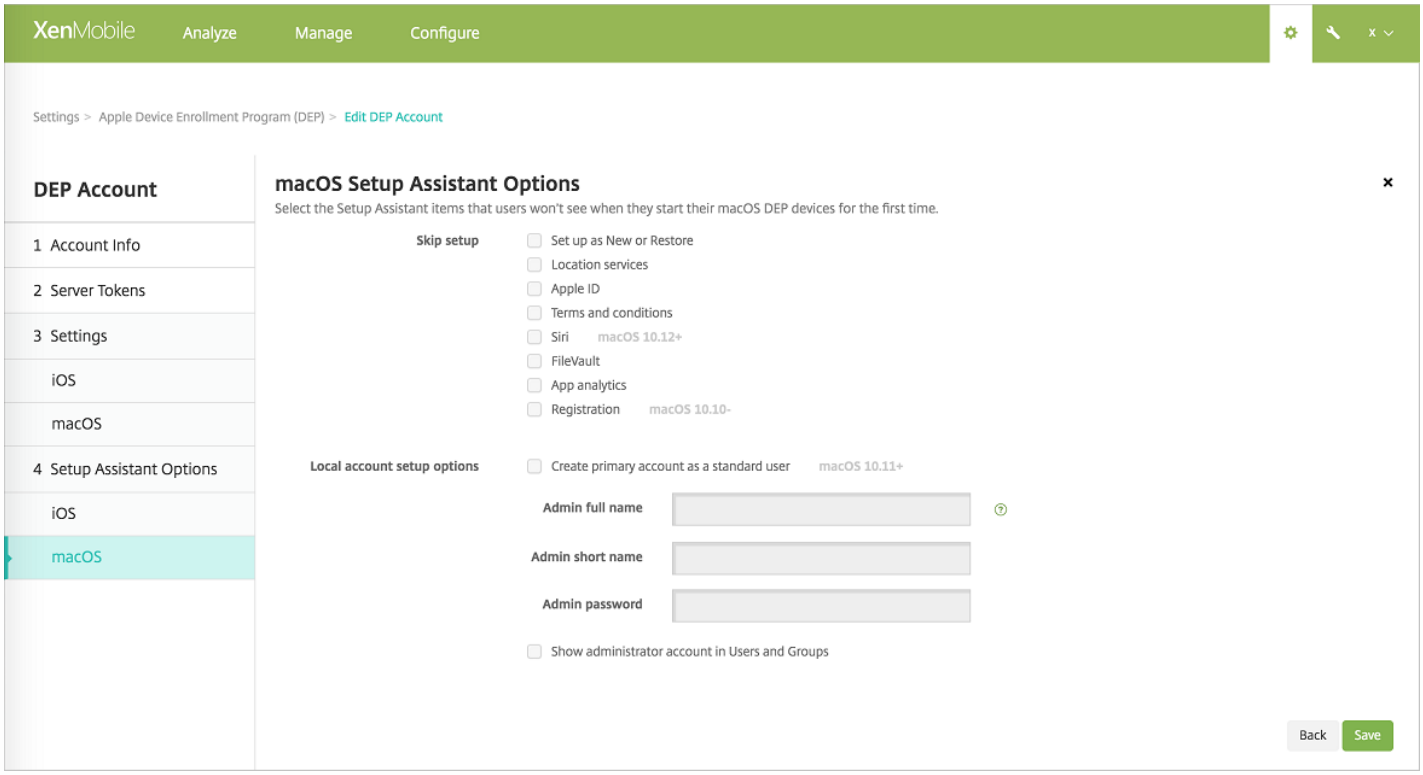


-
-
-

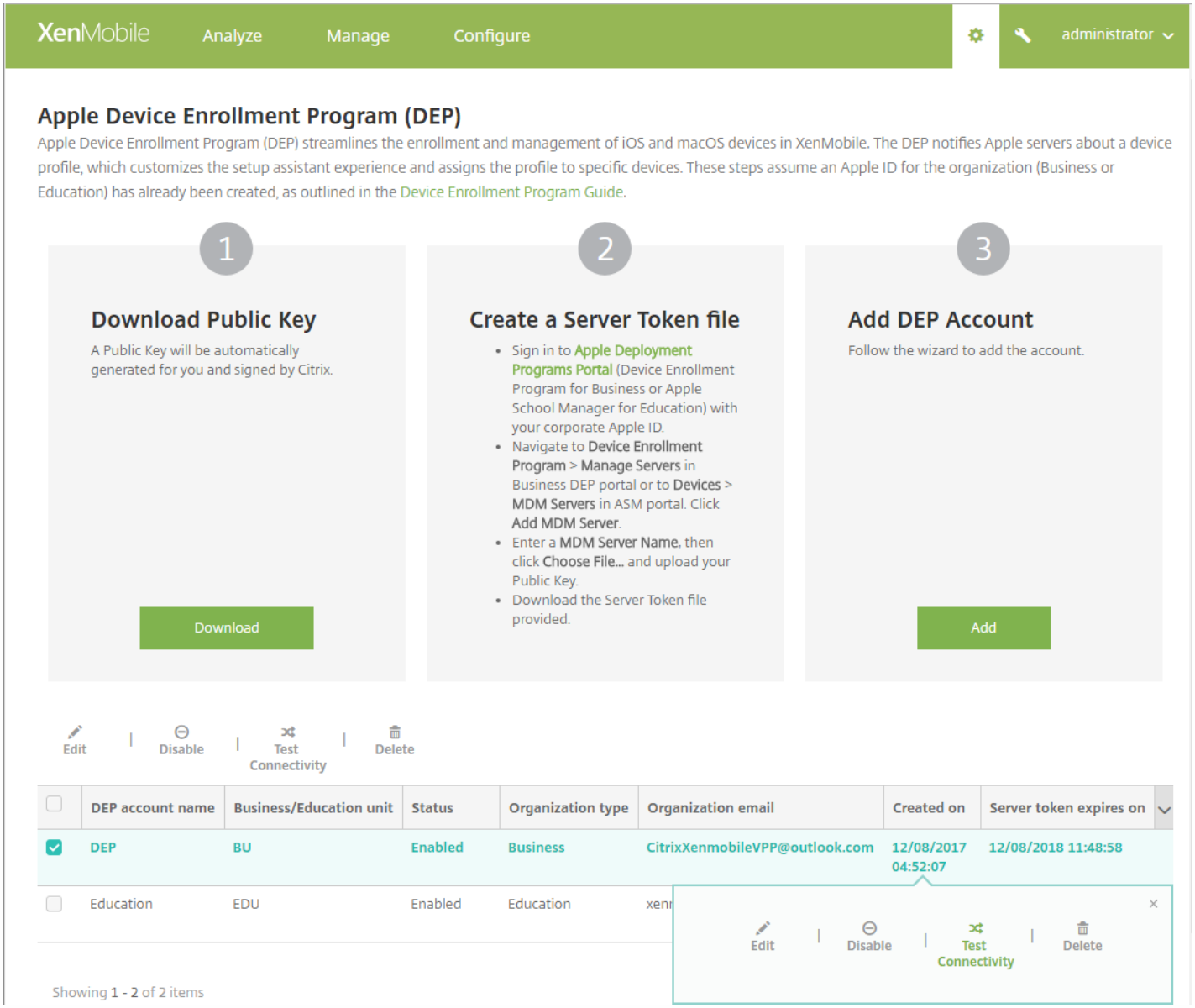
© 1999-2017 Citrix Systems, Inc. All rights reserved.

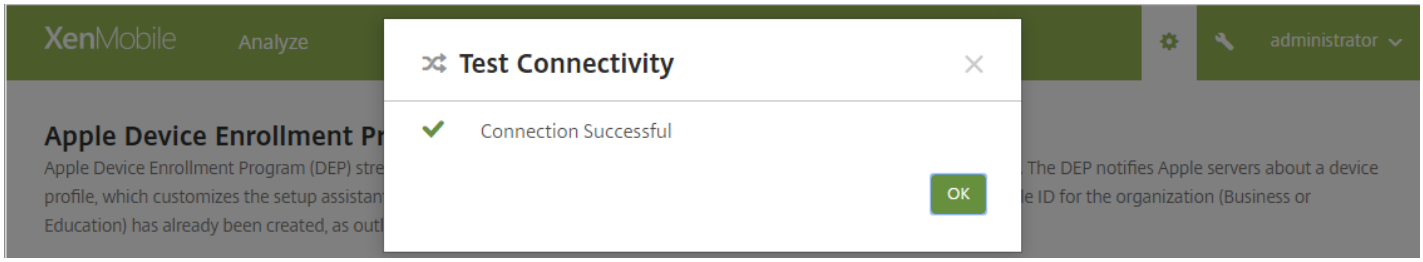


© 1999-2017 Citrix Systems, Inc. All rights reserved.



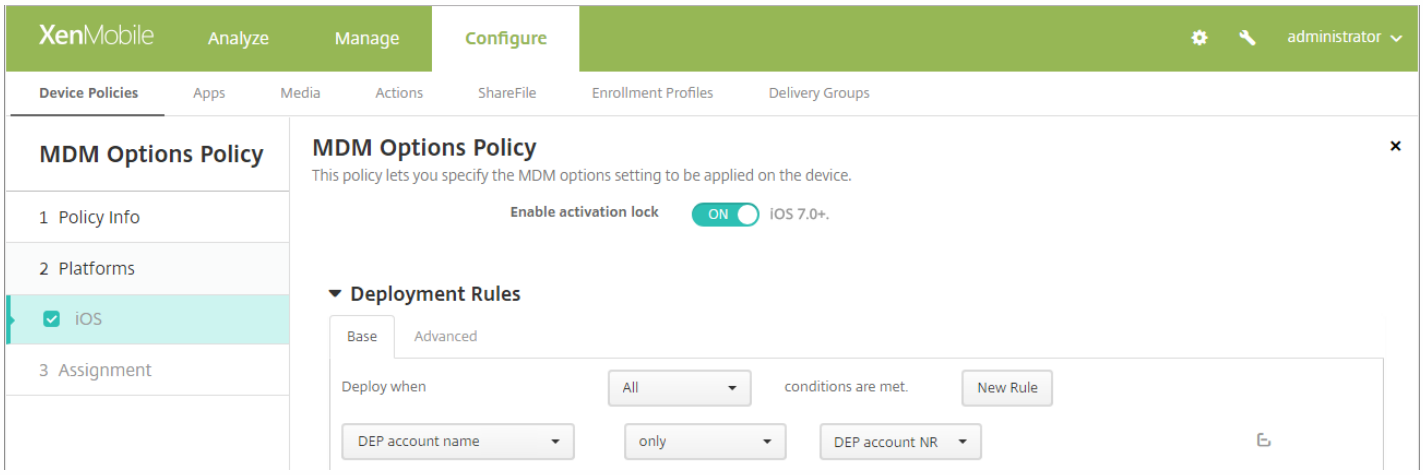
© 1999-2017 Citrix Systems, Inc. All rights reserved.

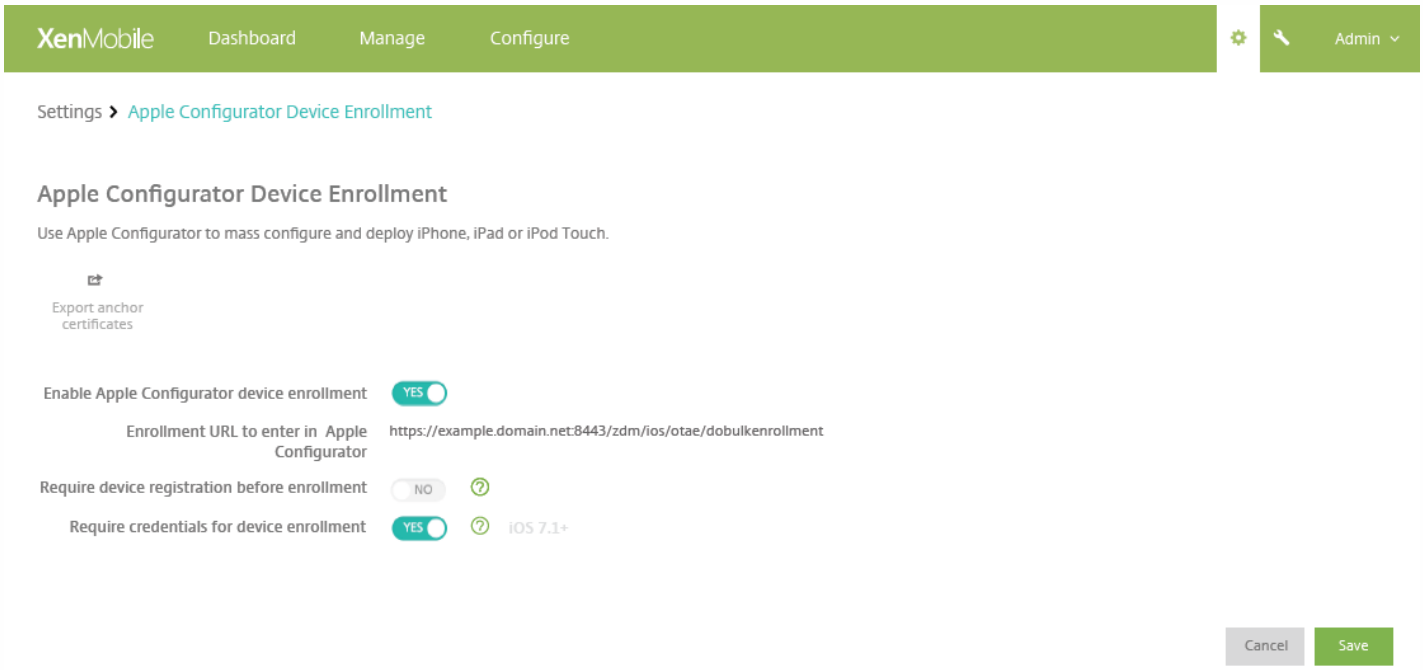




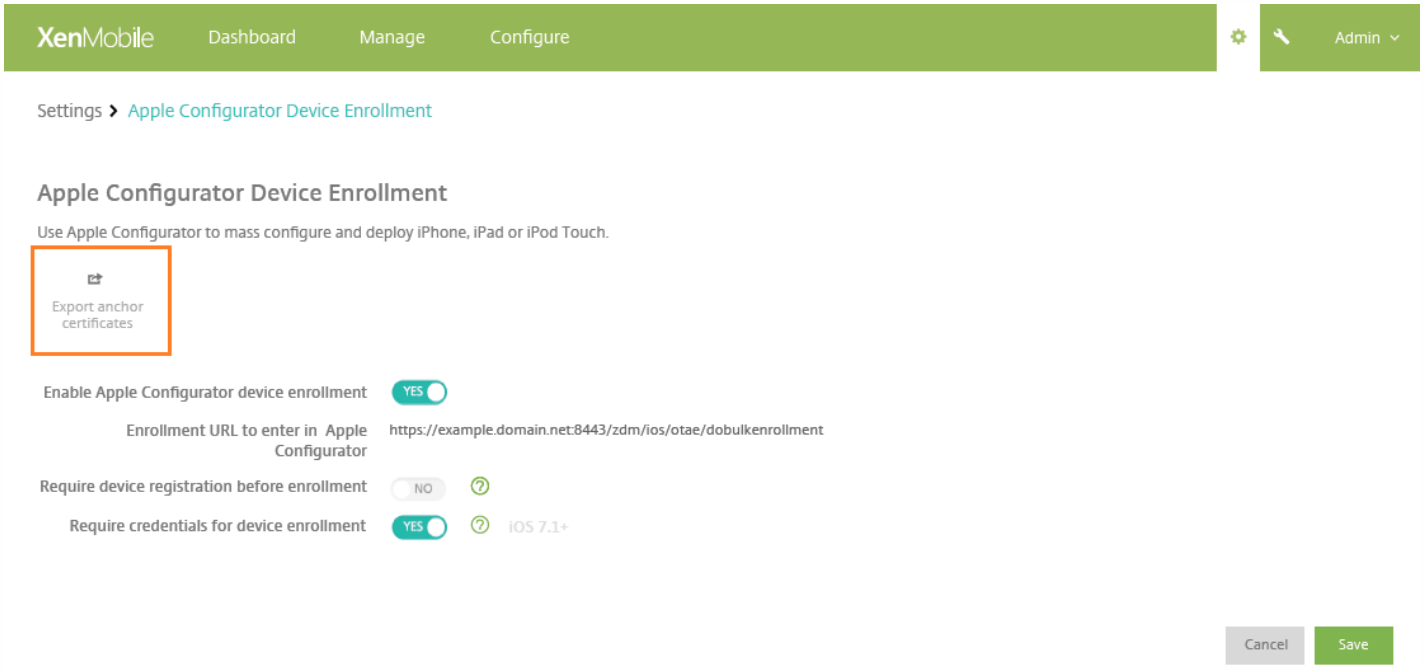
© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-



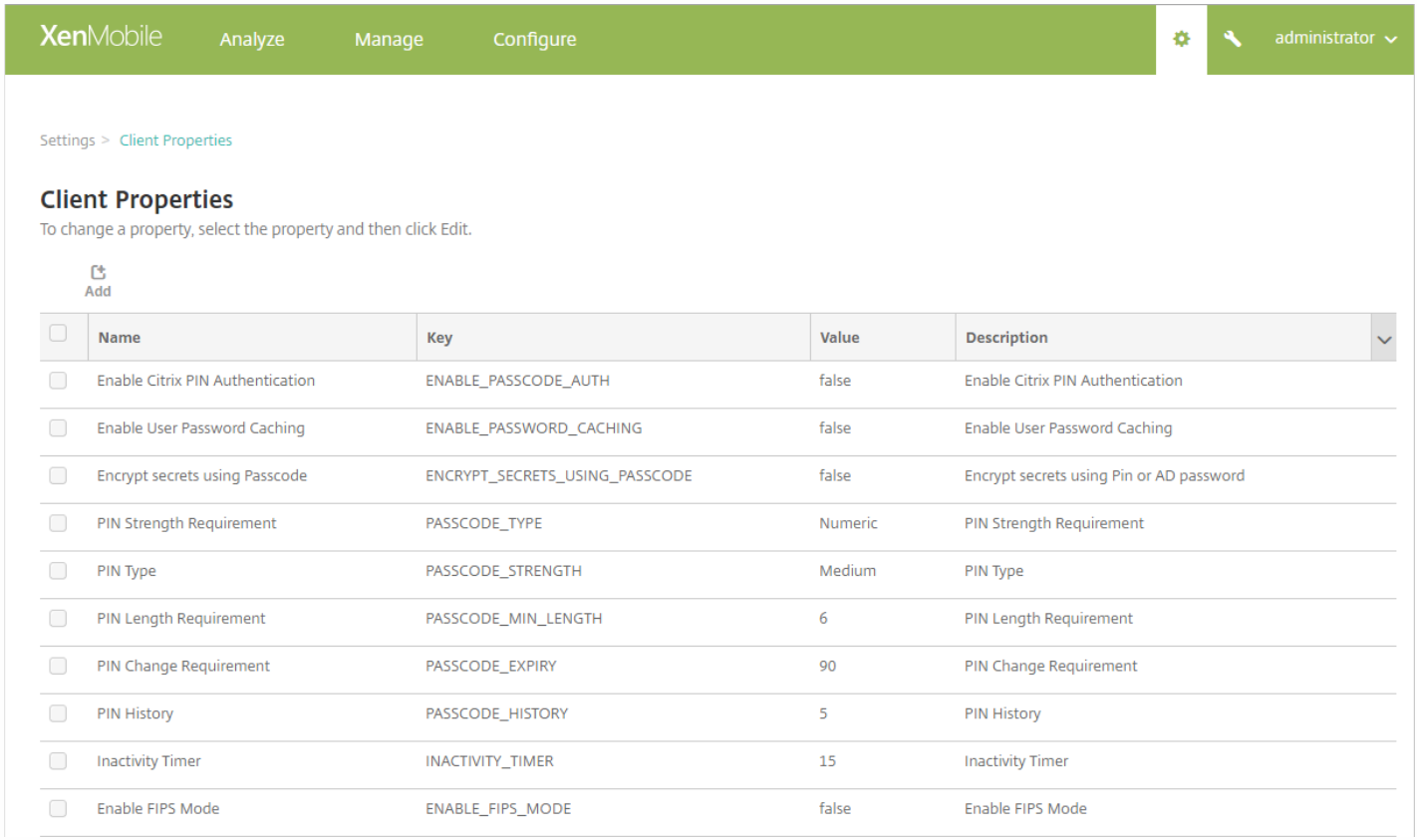


© 1999-2017 Citrix Systems, Inc. All rights reserved.



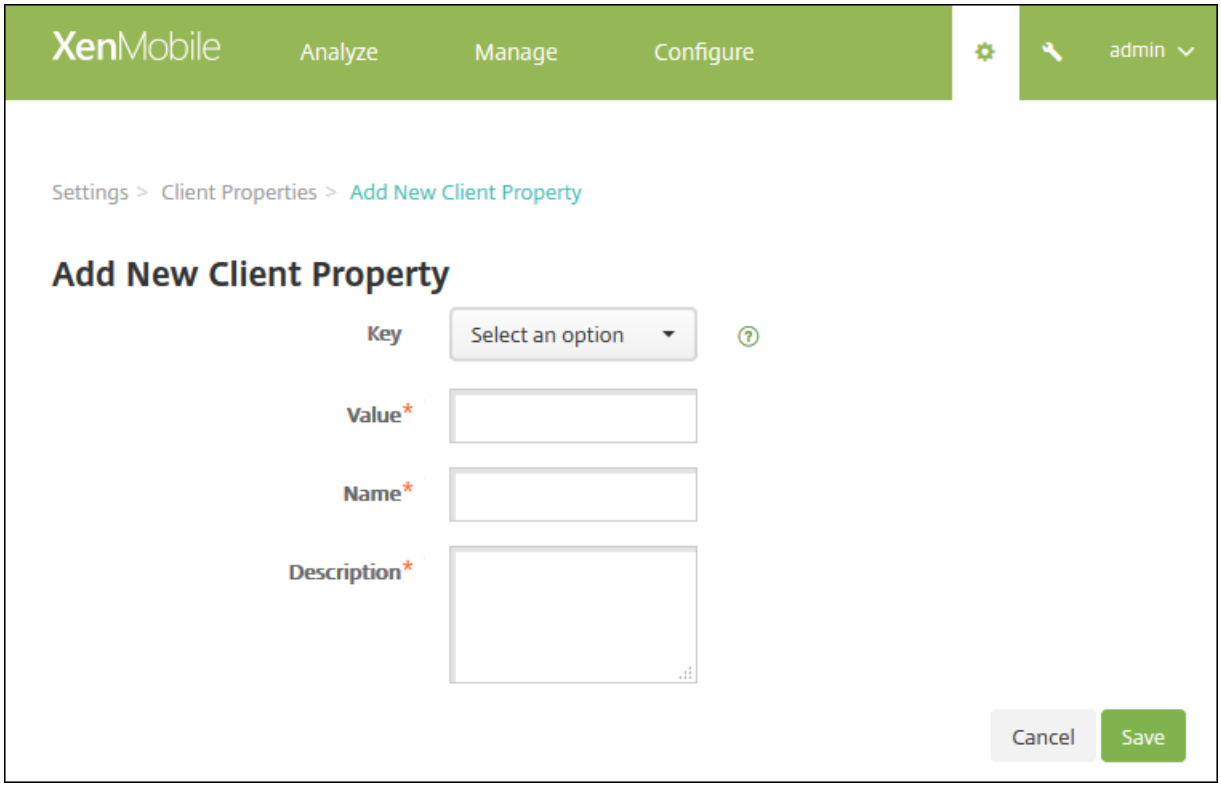
© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Para adicionar uma propriedade do cliente

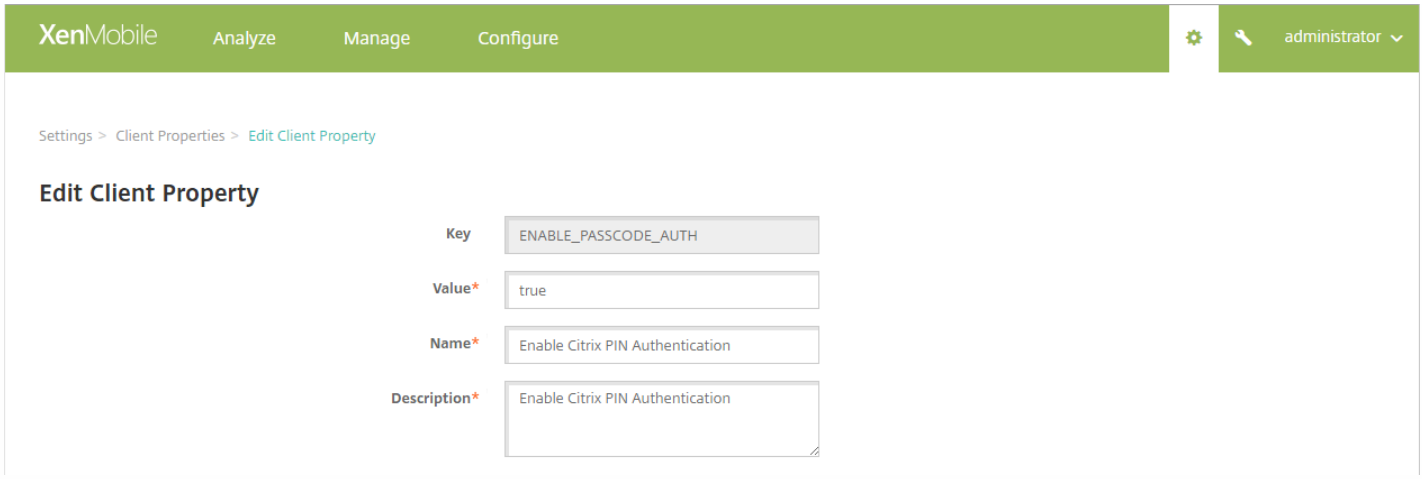
© 1999-2017 Citrix Systems, Inc. All rights reserved.



-
-
-
-

Para editar uma propriedade do cliente

© 1999-2017 Citrix Systems, Inc. All rights reserved.



-
-
-
-

Para excluir uma propriedade do cliente

-
-

-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

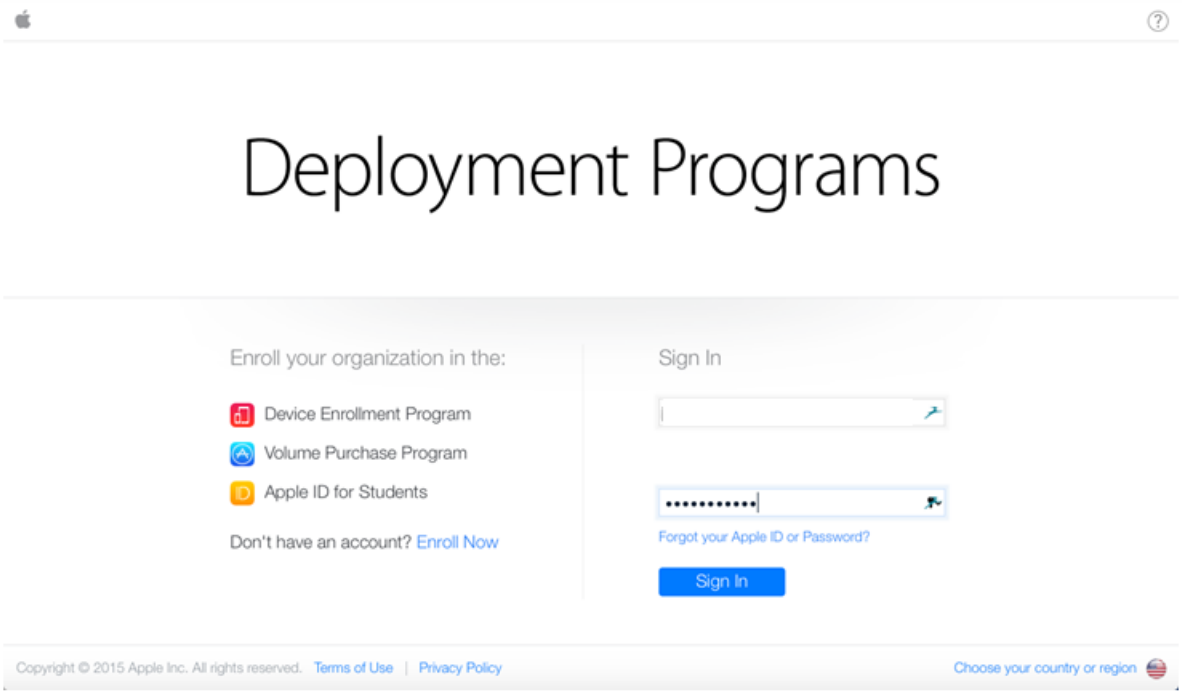
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

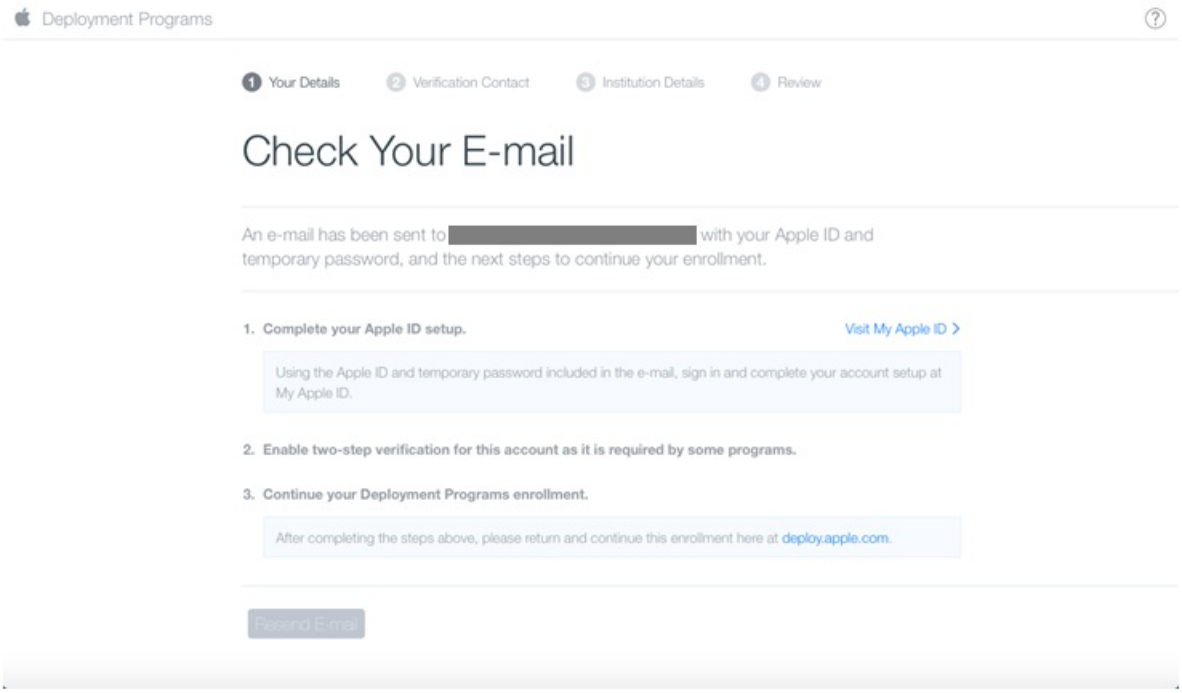
-
-
-
-

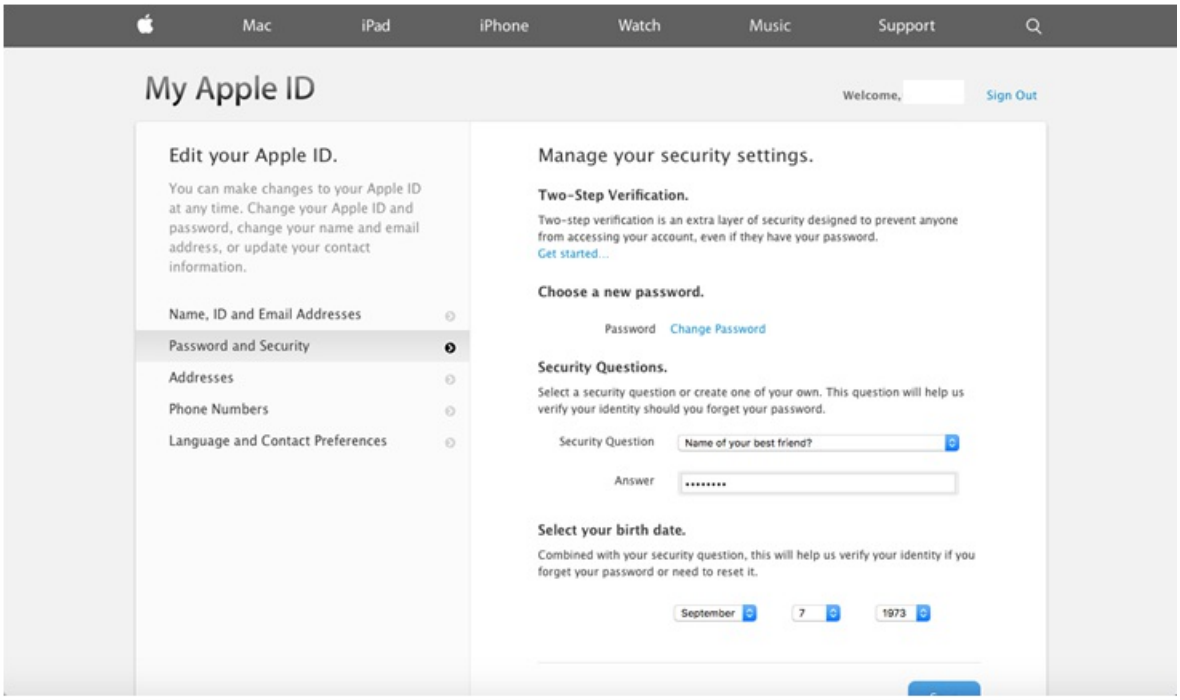
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Cadastrar-se no Apple Deployment Program

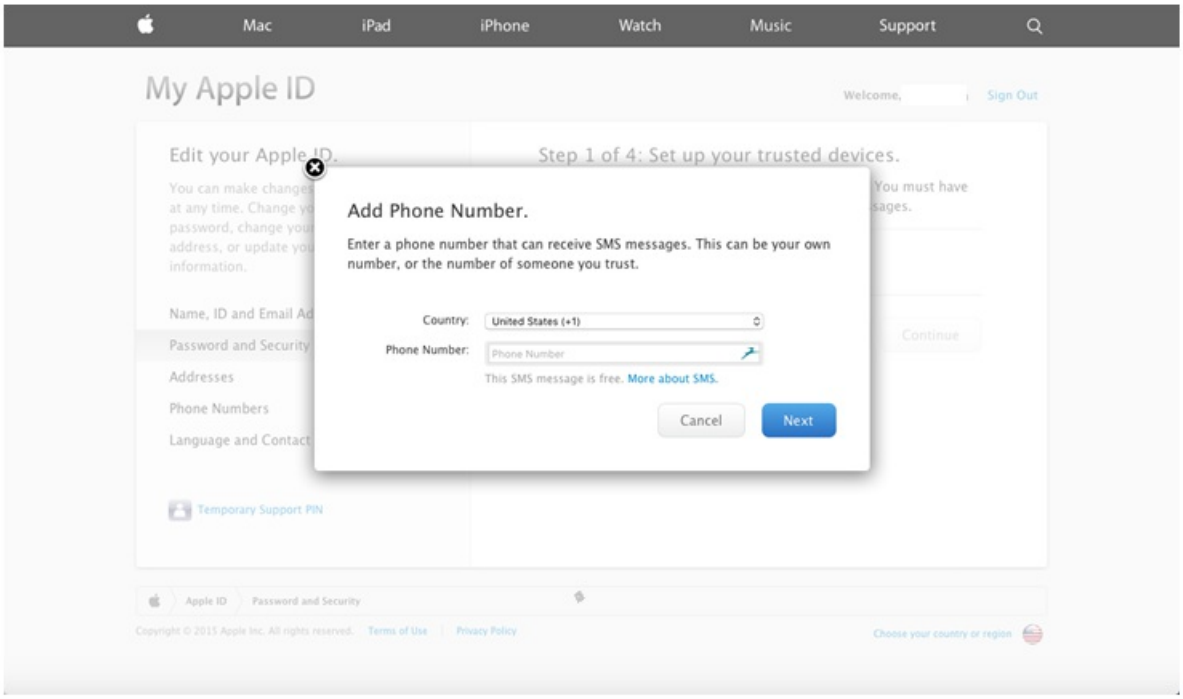


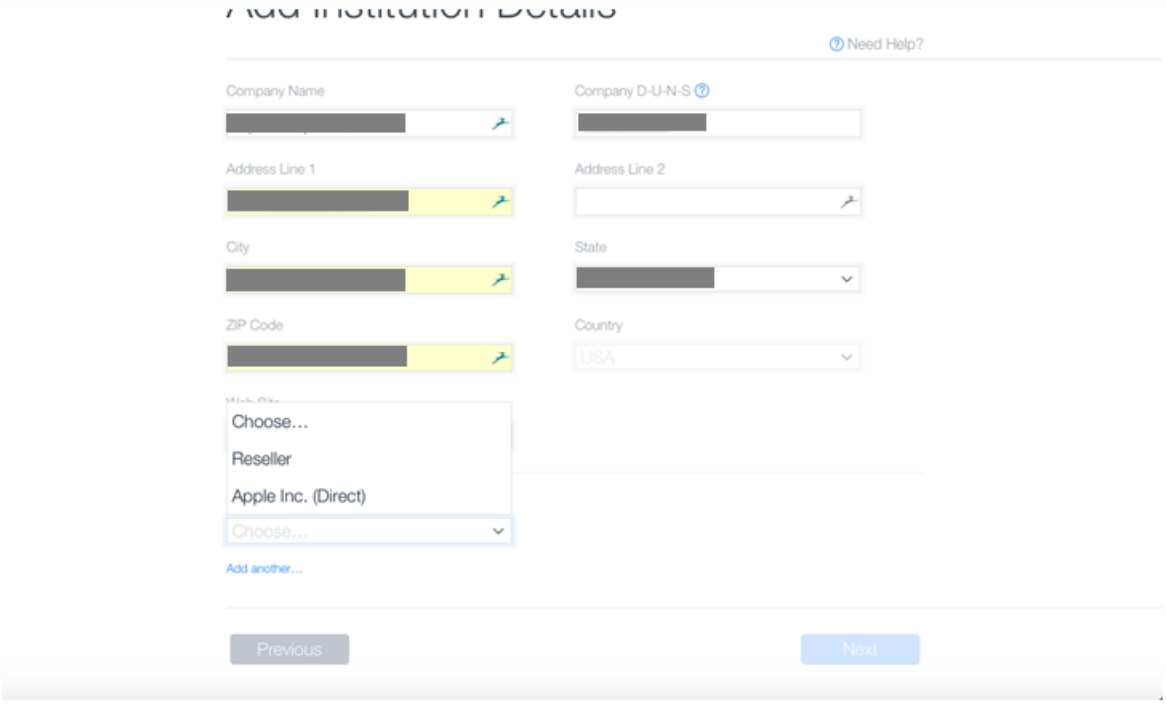
© 1999-2017 Citrix Systems, Inc. All rights reserved.



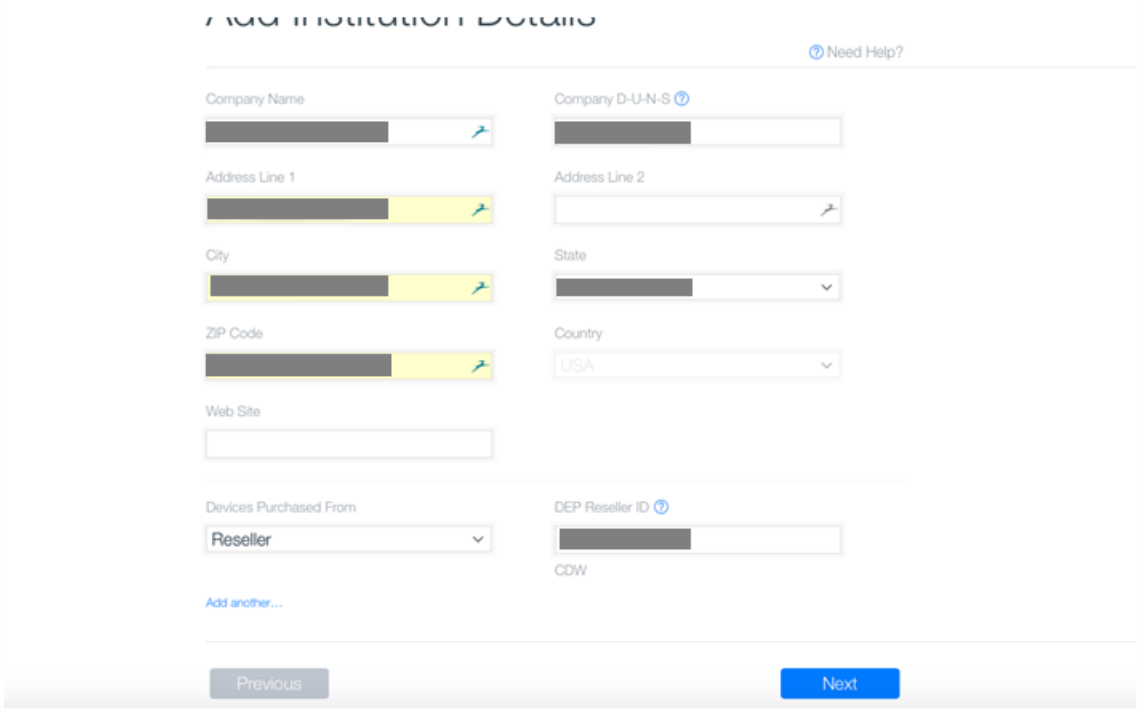


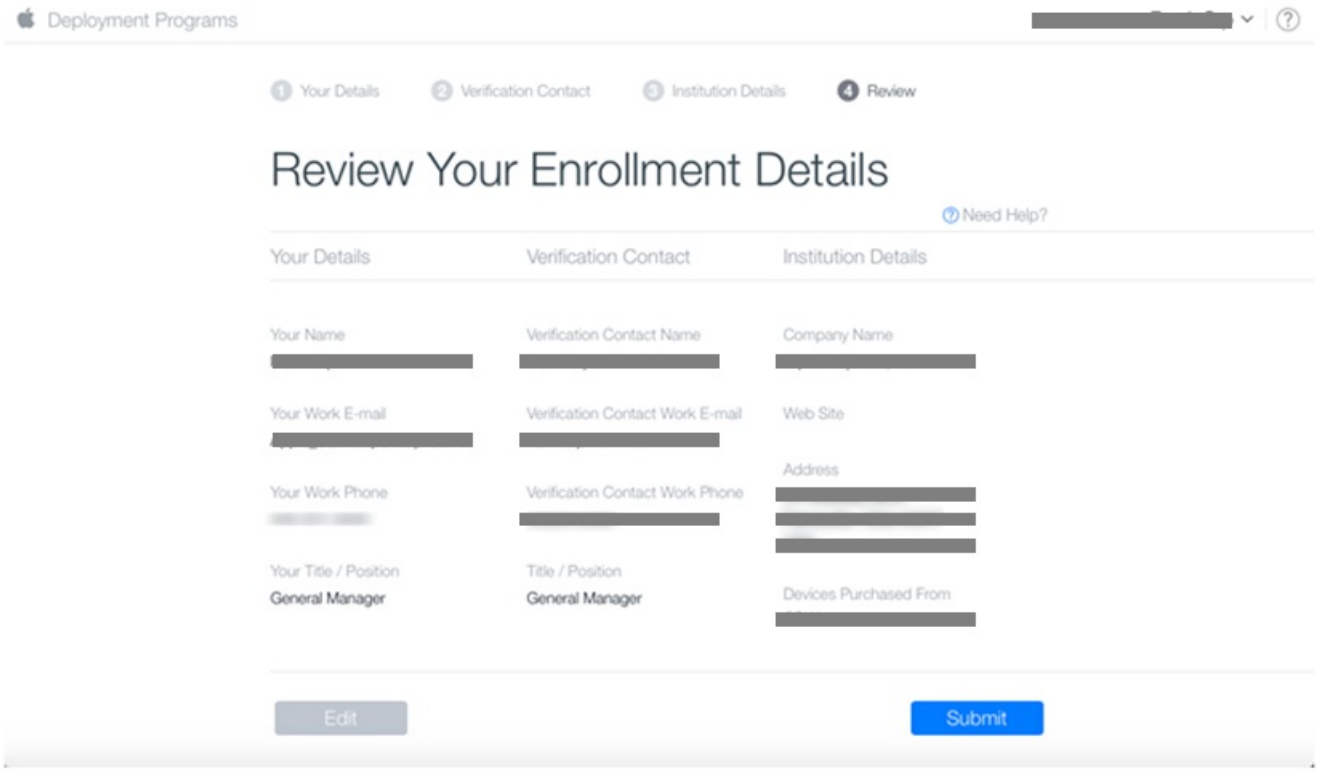
© 1999-2017 Citrix Systems, Inc. All rights reserved.



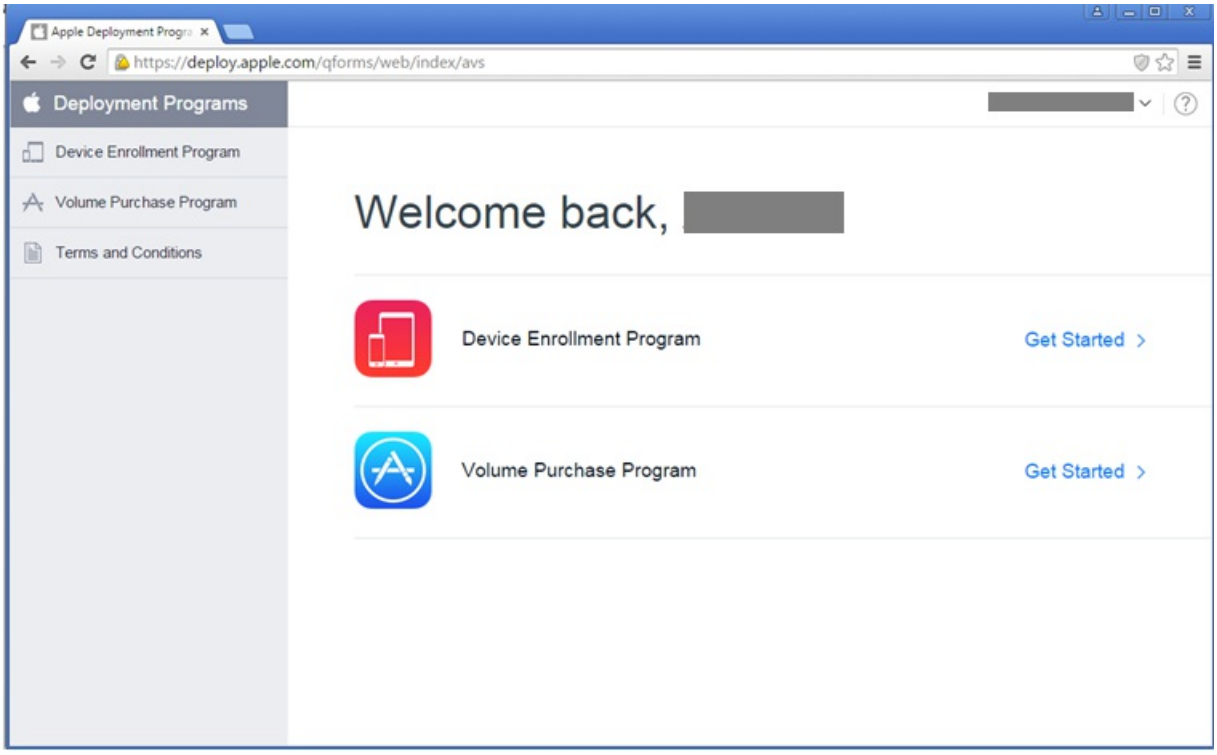


© 1999-2017 Citrix Systems, Inc. All rights reserved.





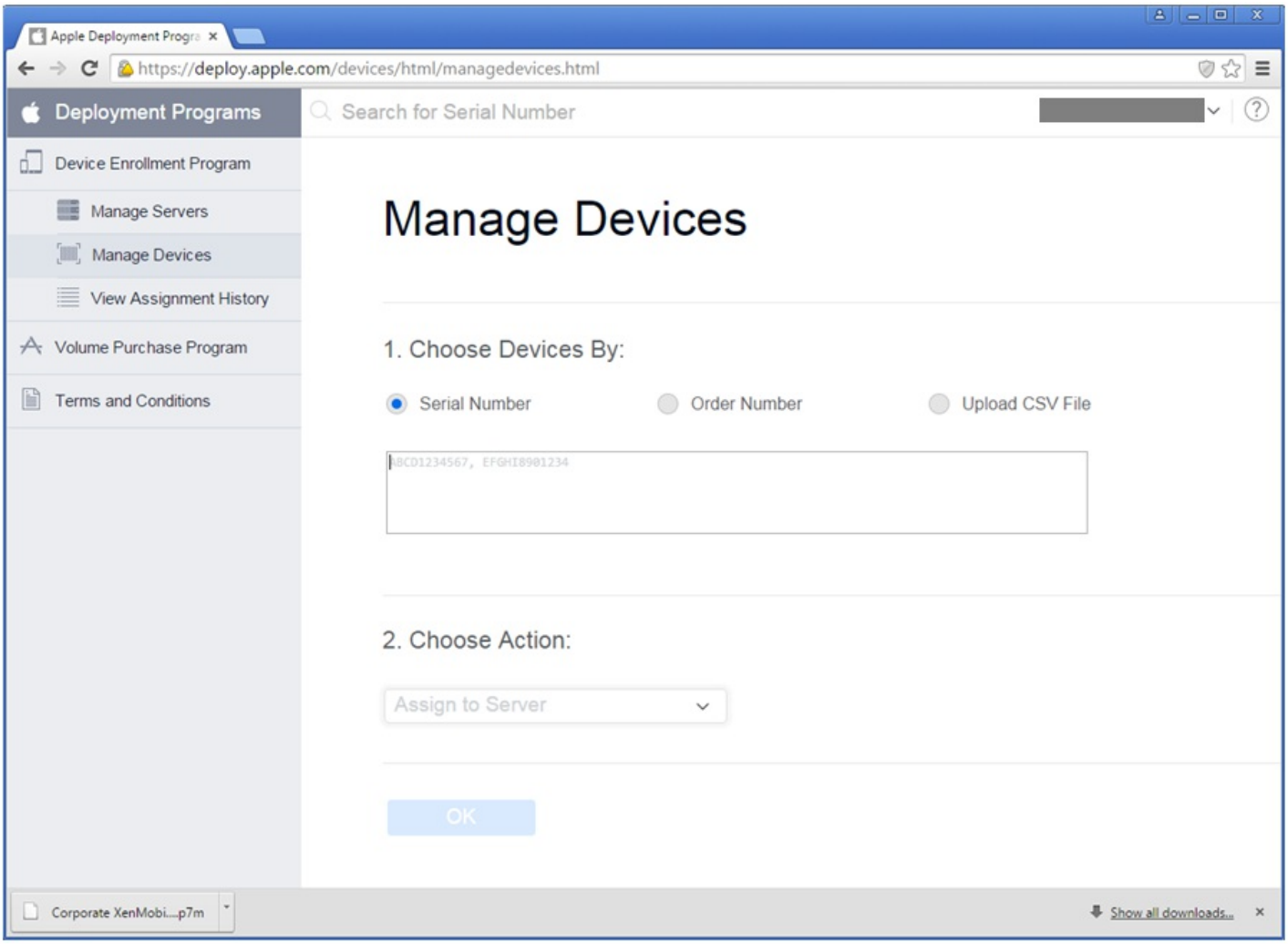
© 1999-2017 Citrix Systems, Inc. All rights reserved.



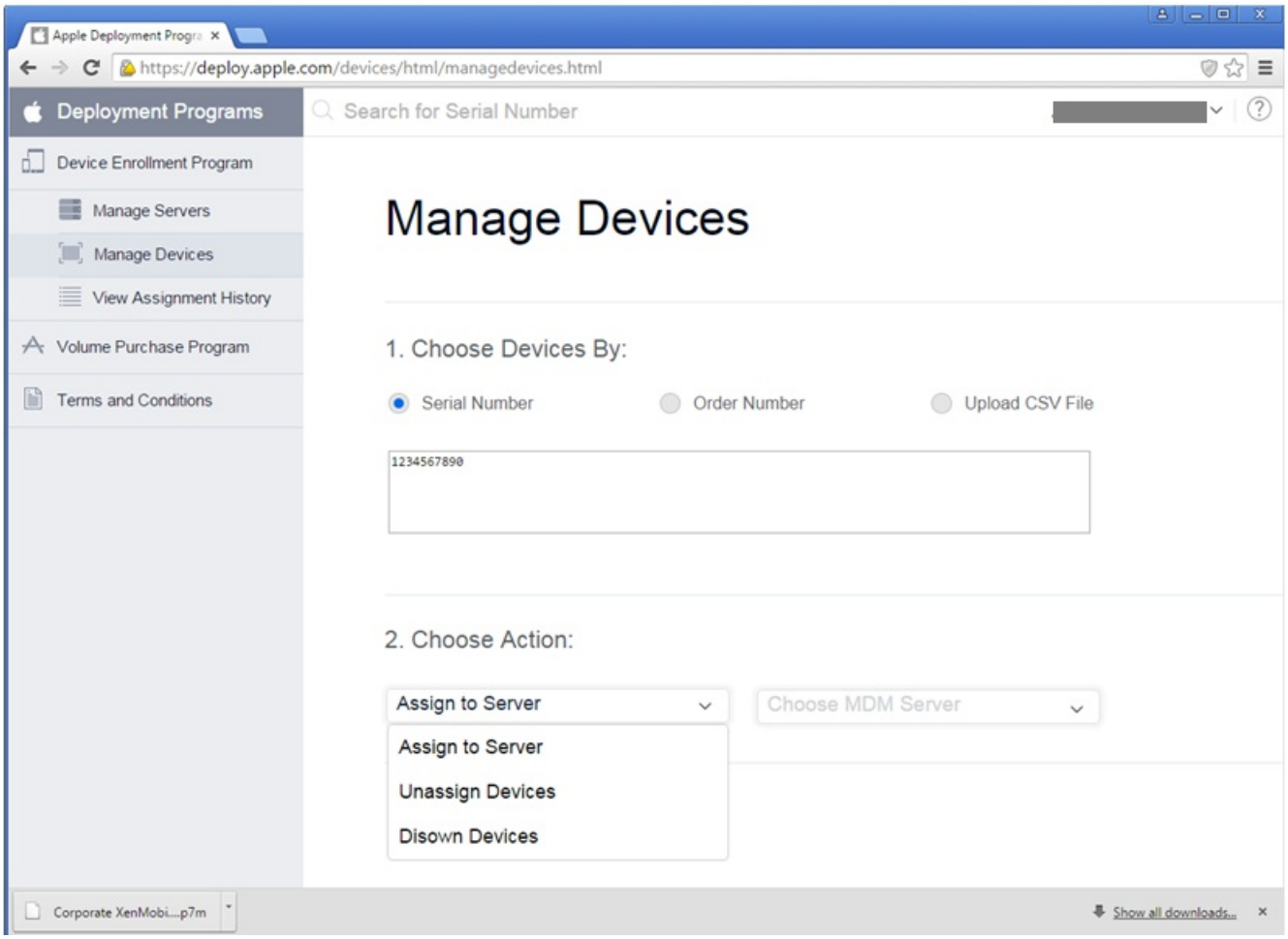
Solicitar dispositivos ativados para o DEP

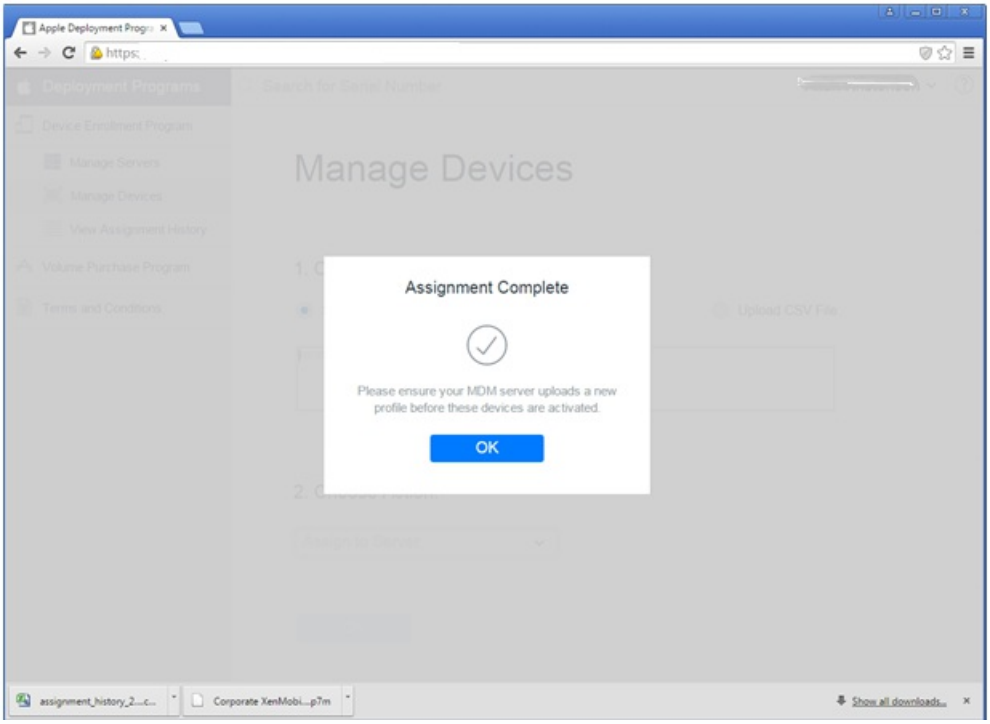
Gerenciar dispositivos ativados para DEP

© 1999-2017 Citrix Systems, Inc. All rights reserved.

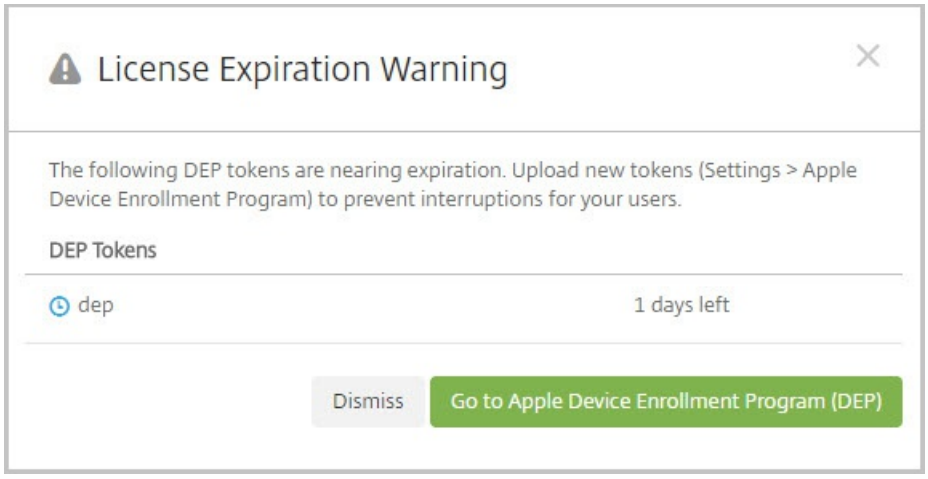


© 1999-2017 Citrix Systems, Inc. All rights reserved.



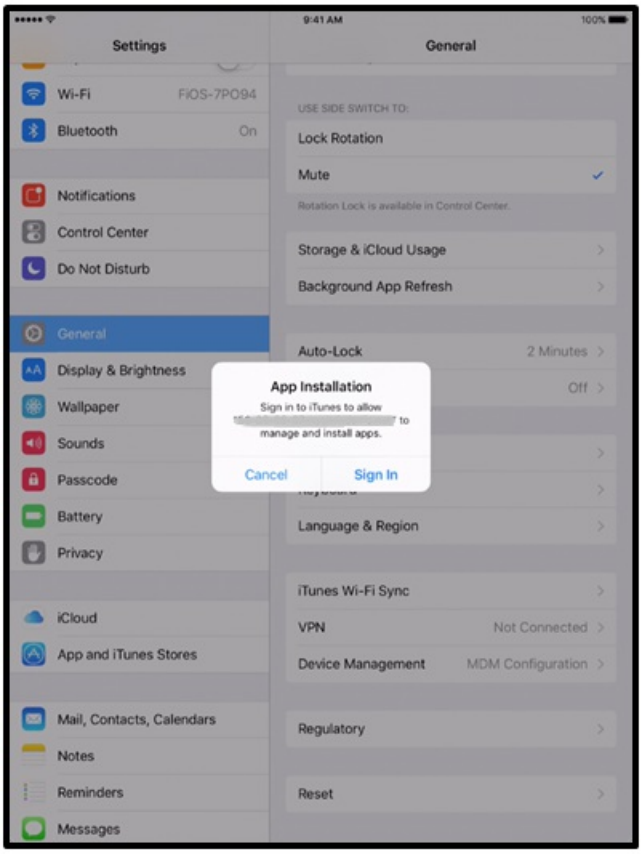


© 1999-2017 Citrix Systems, Inc. All rights reserved.

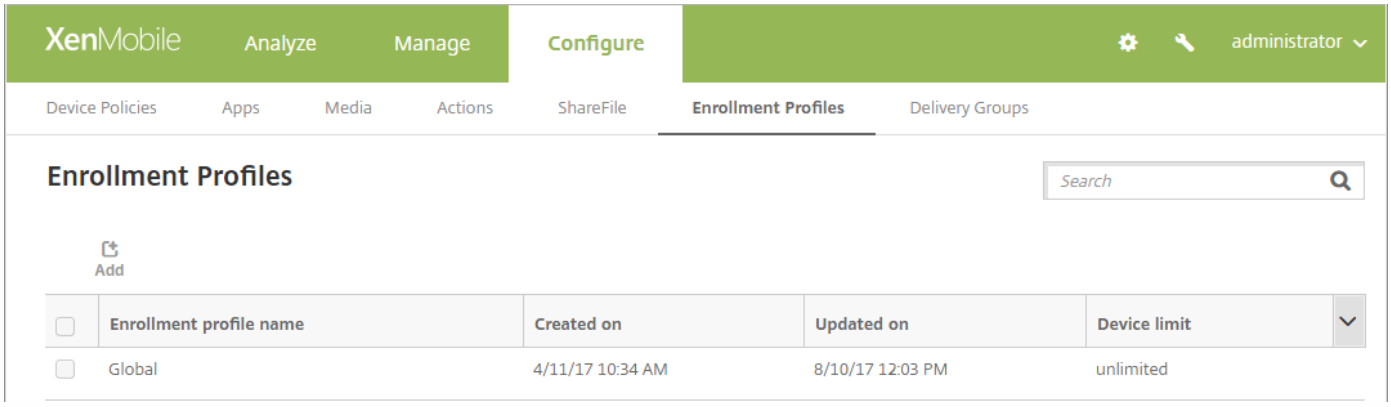


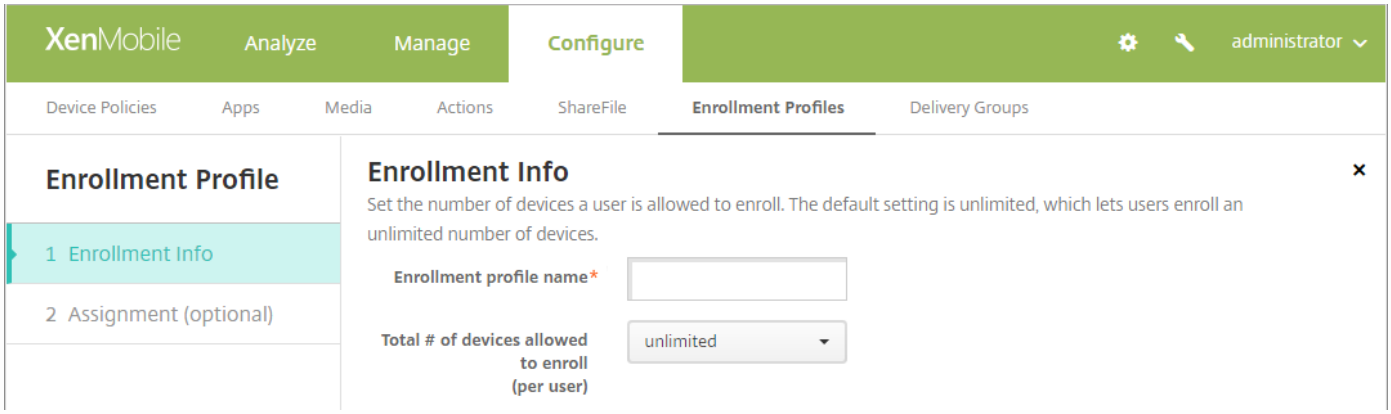
Experiência do usuário ao registrar um dispositivo ativado para o Apple DEP

© 1999-2017 Citrix Systems, Inc. All rights reserved.

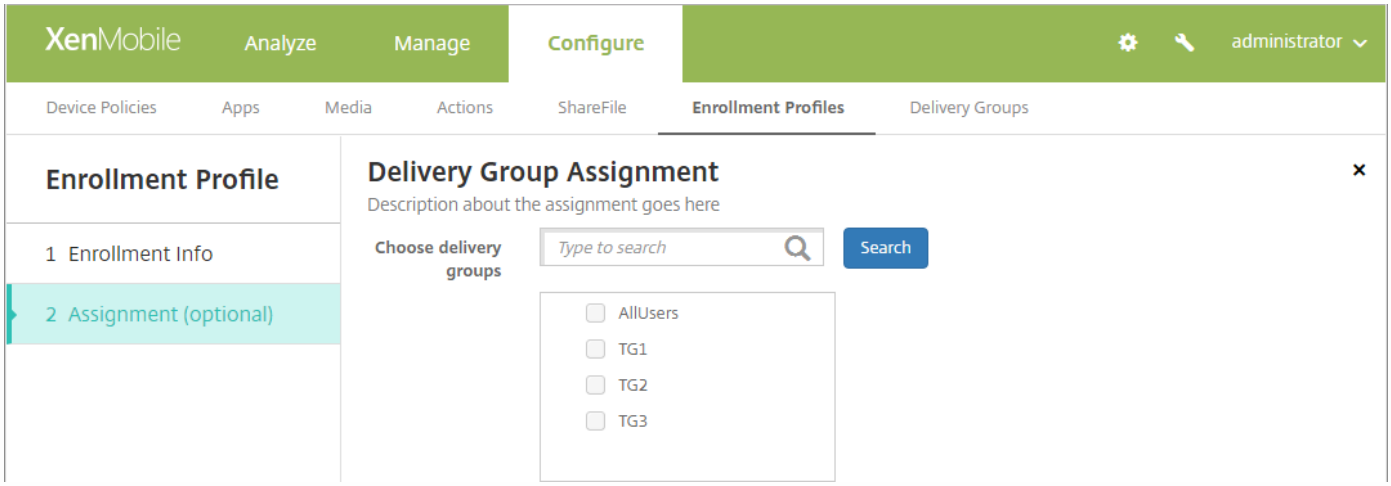


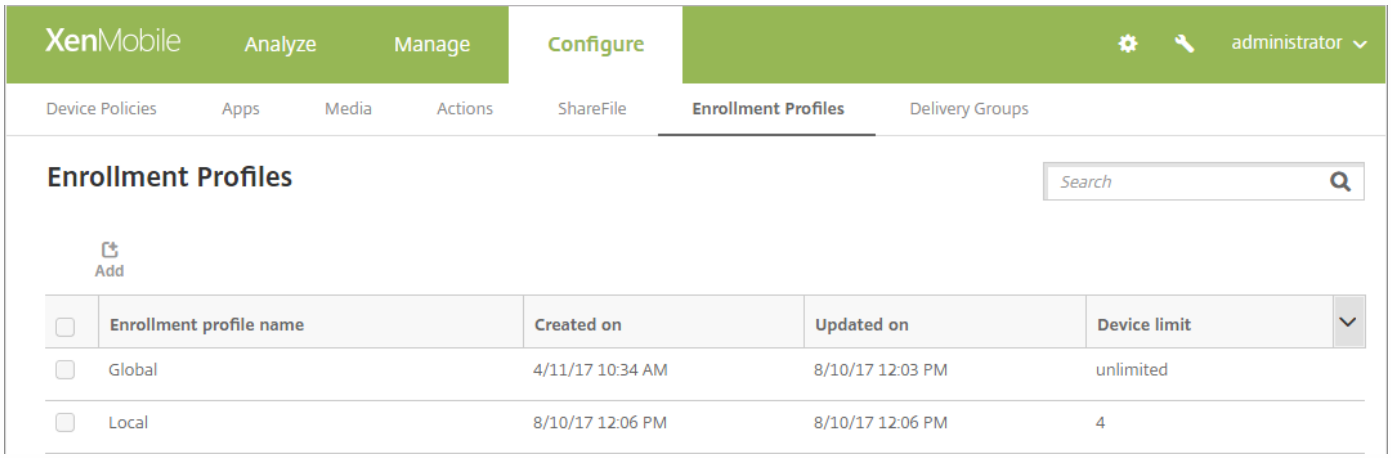
© 1999-2017 Citrix Systems, Inc. All rights reserved.



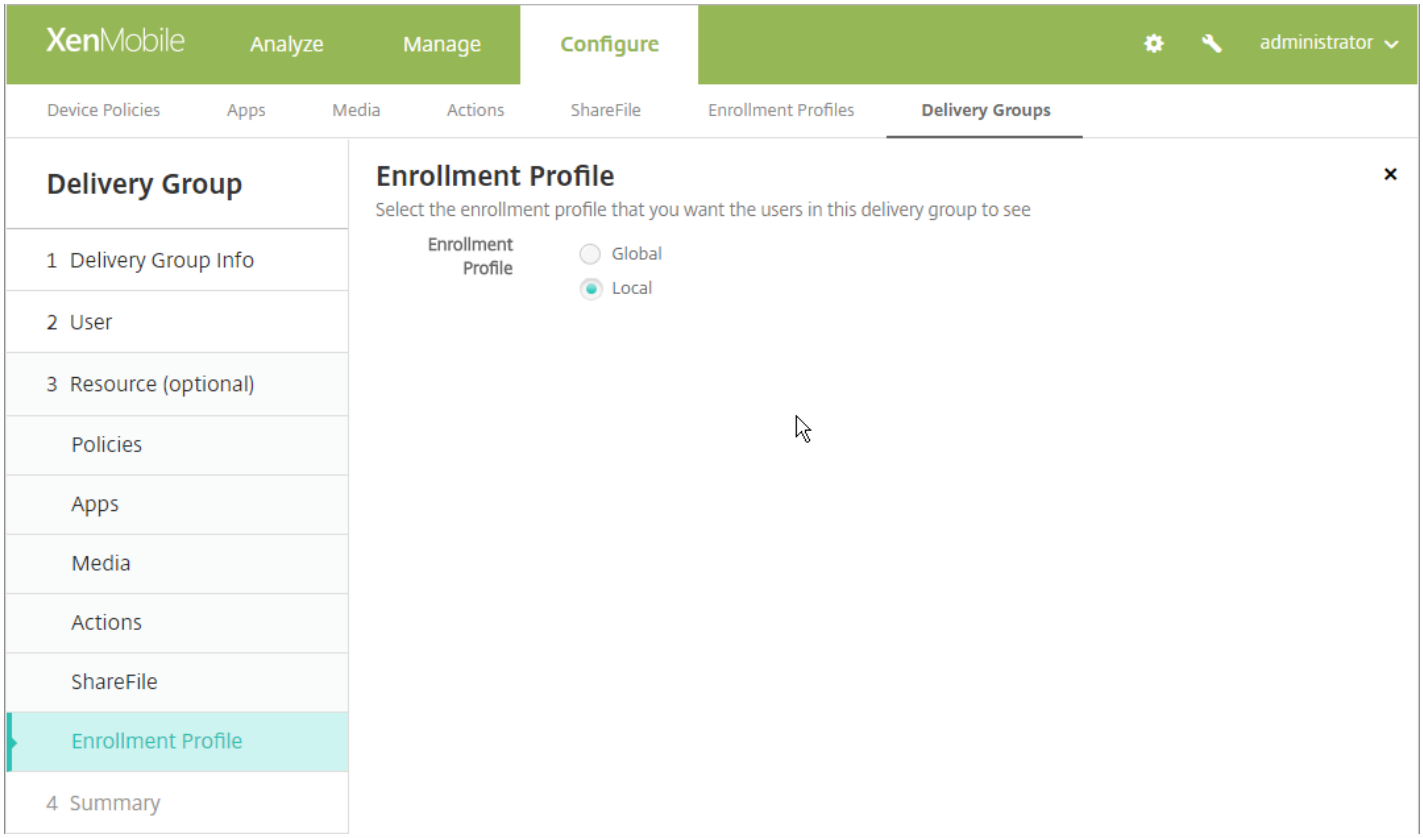


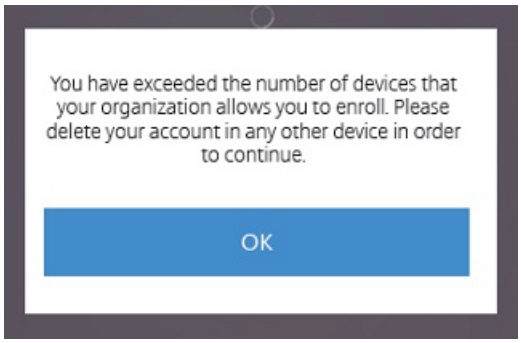
© 1999-2017 Citrix Systems, Inc. All rights reserved.





© 1999-2017 Citrix Systems, Inc. All rights reserved.

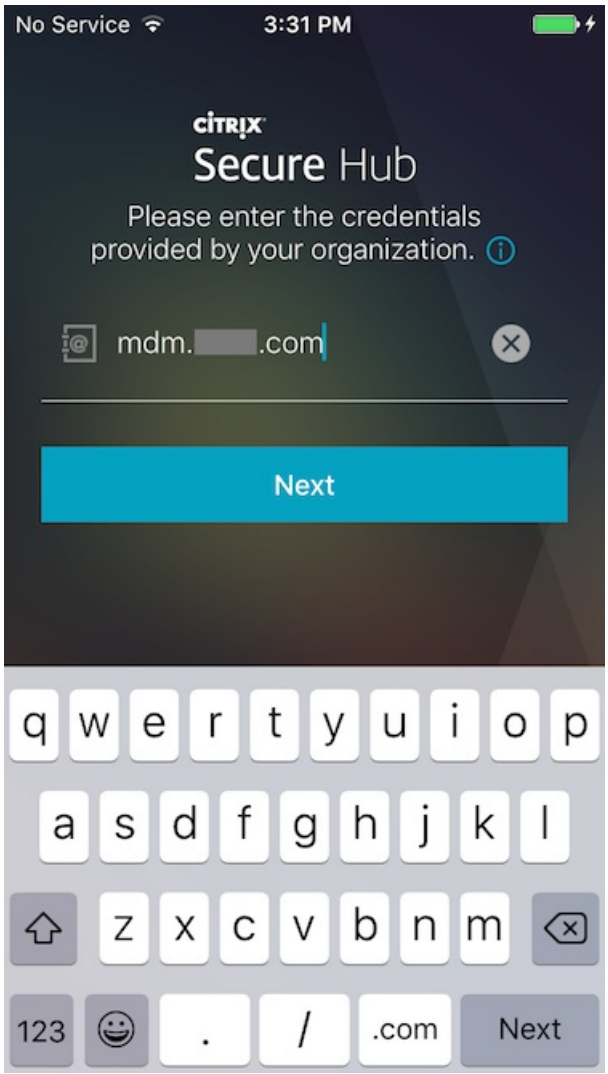




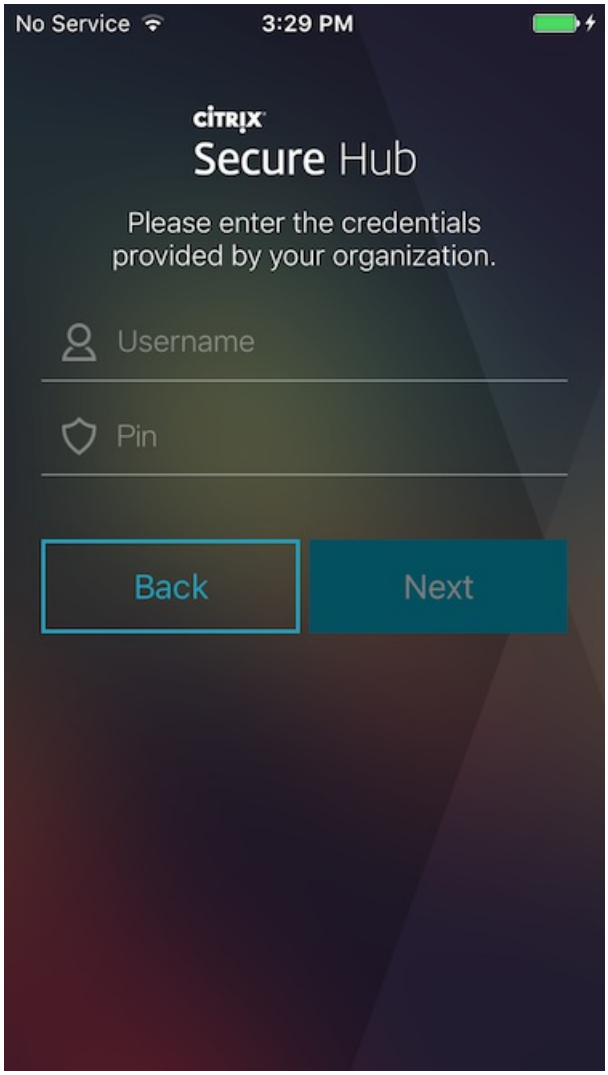
© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

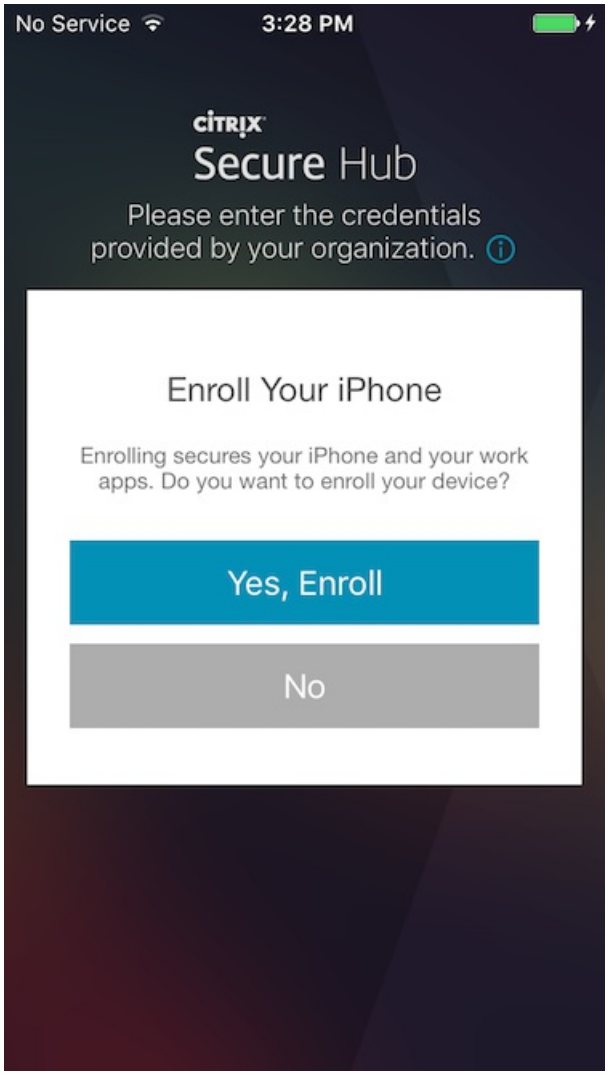
© 1999-2017 Citrix Systems, Inc. All rights reserved.



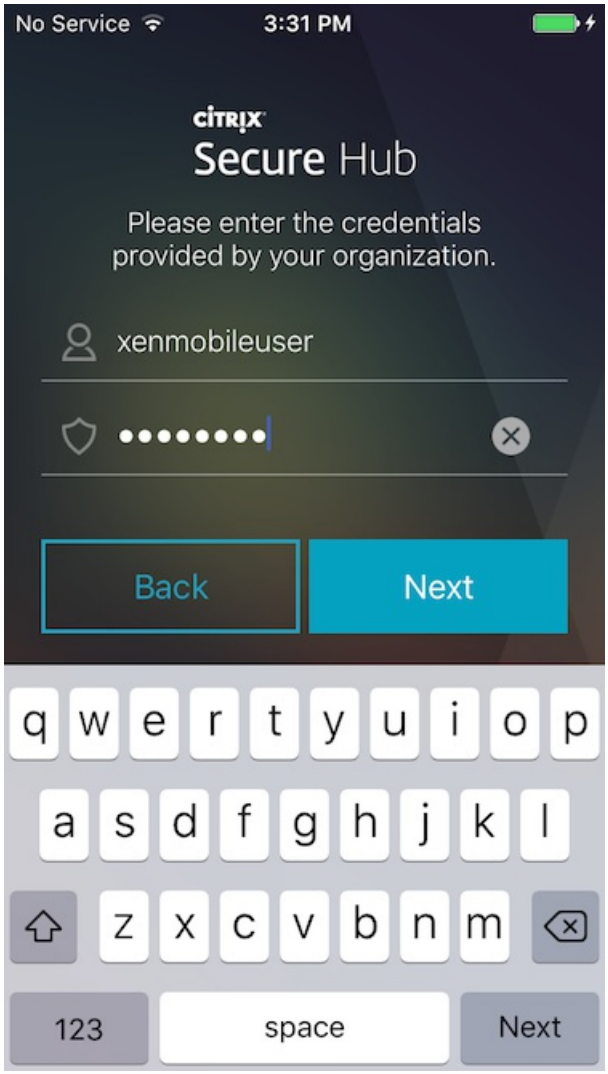
© 1999-2017 Citrix Systems, Inc. All rights reserved.



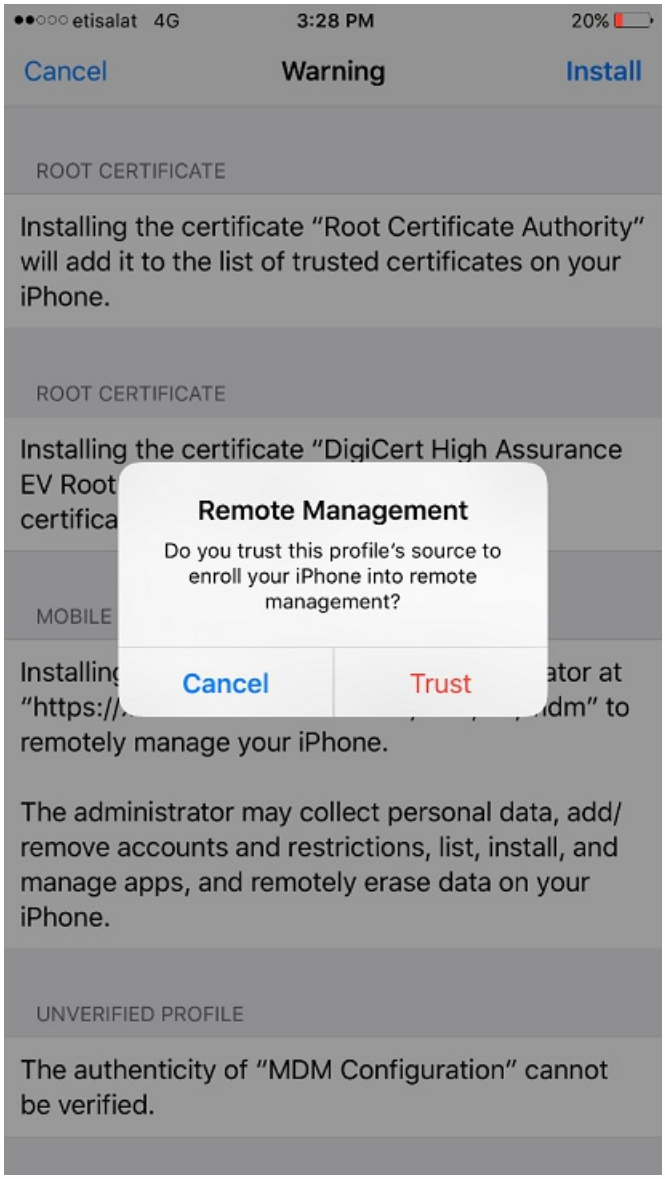
© 1999-2017 Citrix Systems, Inc. All rights reserved.



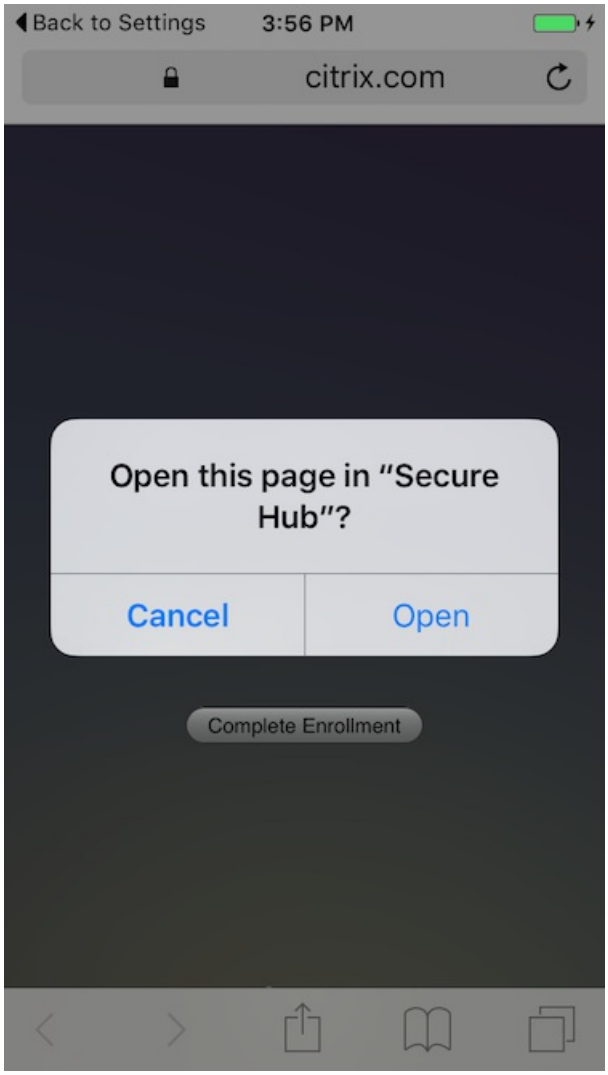
© 1999-2017 Citrix Systems, Inc. All rights reserved.



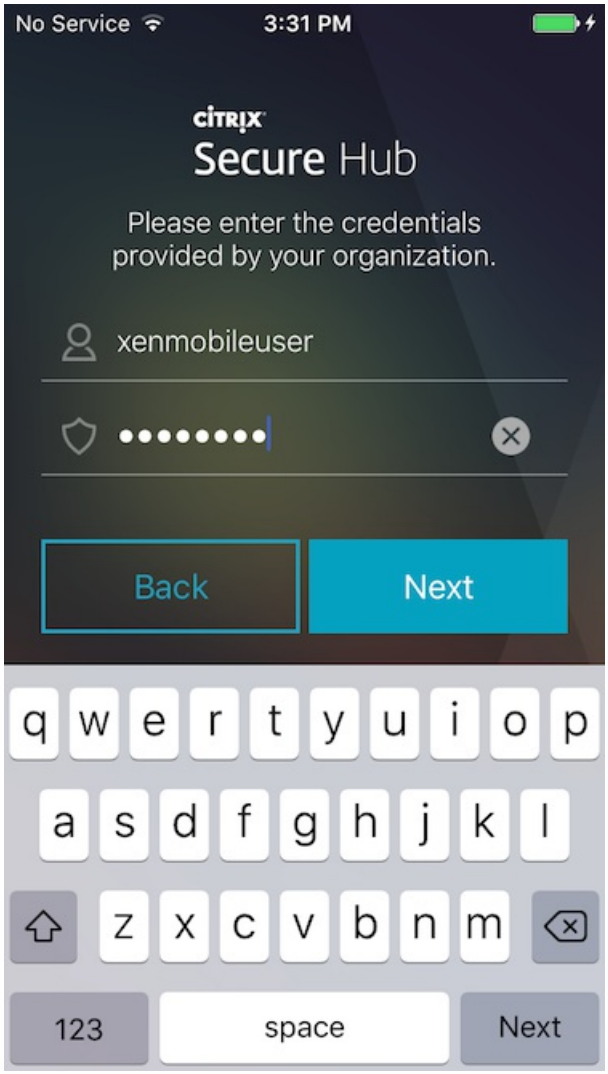
© 1999-2017 Citrix Systems, Inc. All rights reserved.



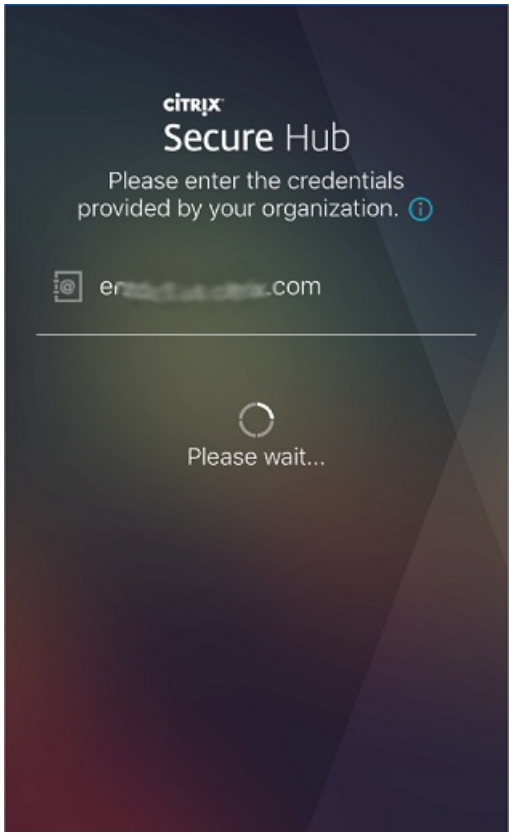
© 1999-2017 Citrix Systems, Inc. All rights reserved.

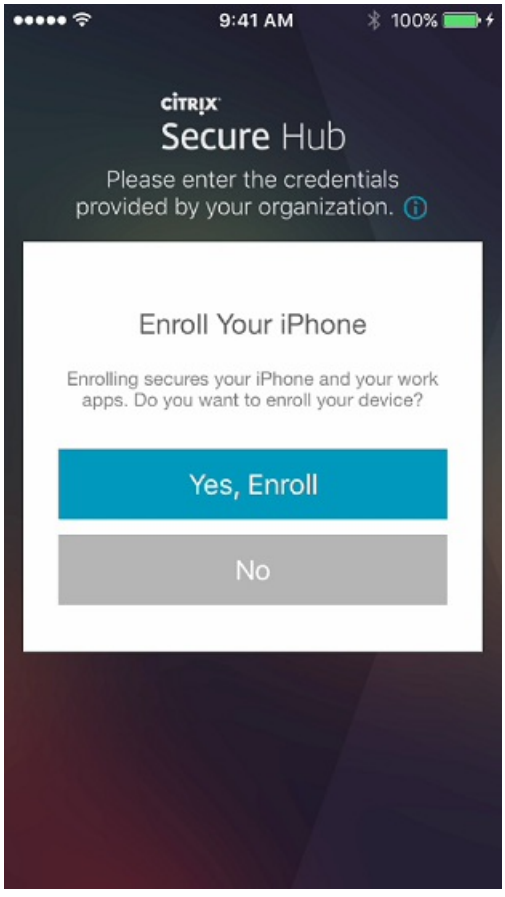


© 1999-2017 Citrix Systems, Inc. All rights reserved.

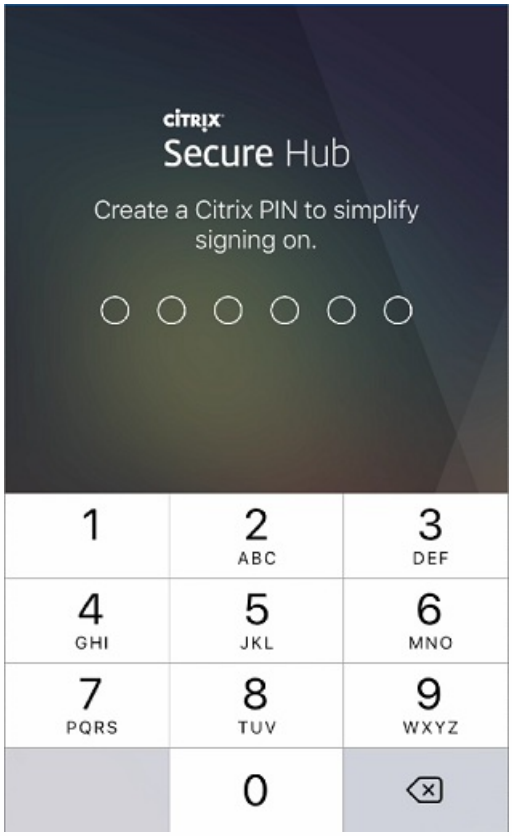


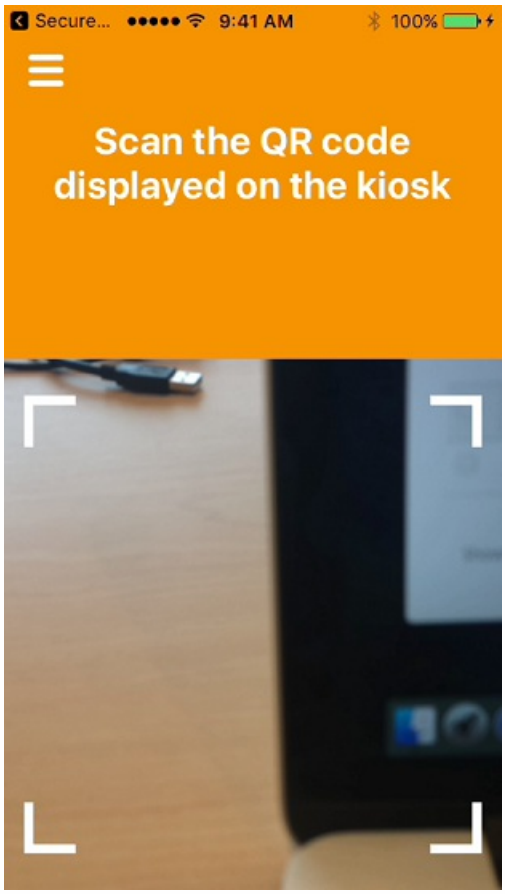
© 1999-2017 Citrix Systems, Inc. All rights reserved.



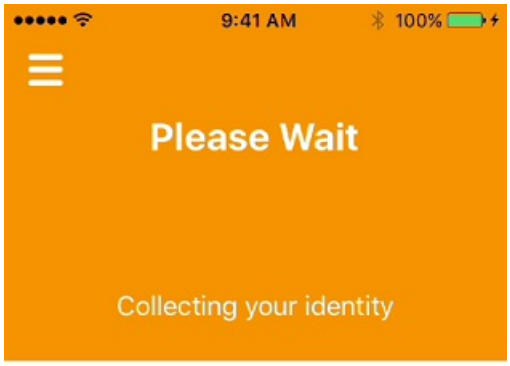


© 1999-2017 Citrix Systems, Inc. All rights reserved.

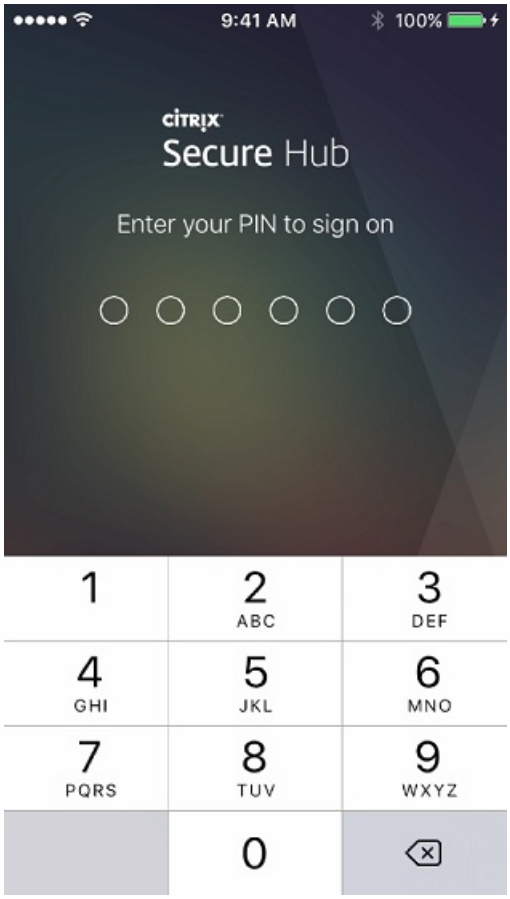




© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

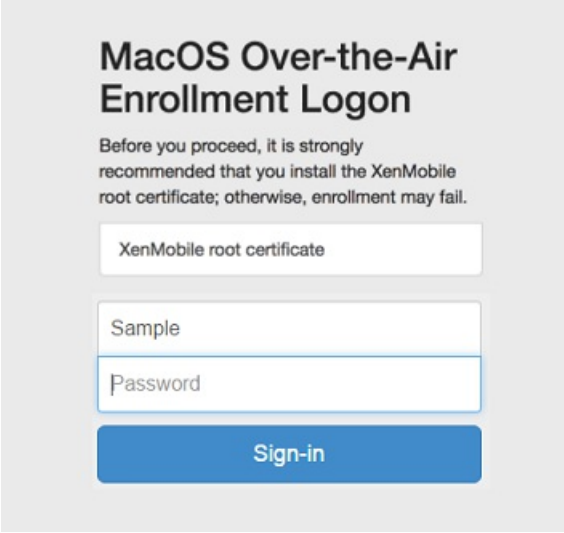


-
-
-
  -
  -
  -

© 1999-2017 Citrix Systems, Inc. All rights reserved.

•

Enviar aos usuários um convite para registro



Enviar um link de instalação para os usuários

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-

-
-

-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

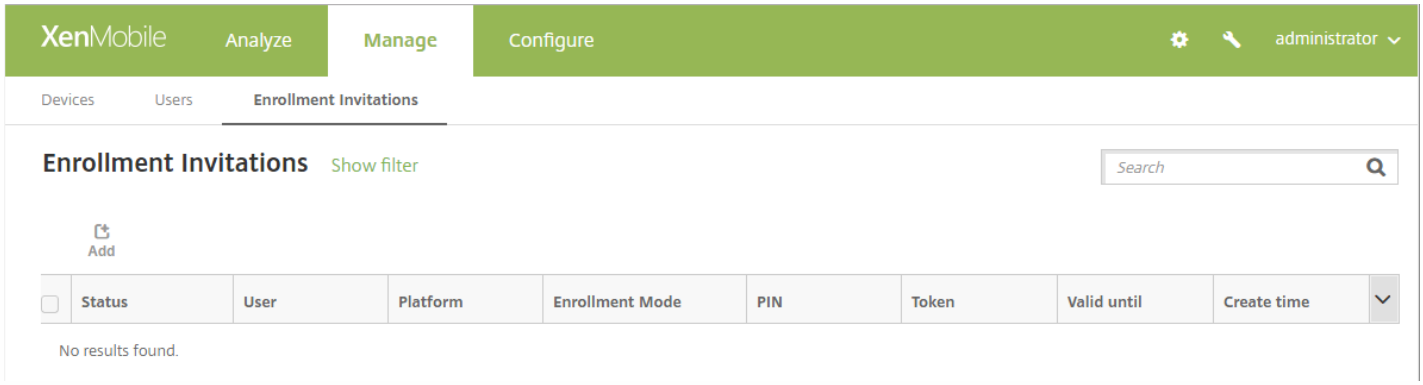
-
-

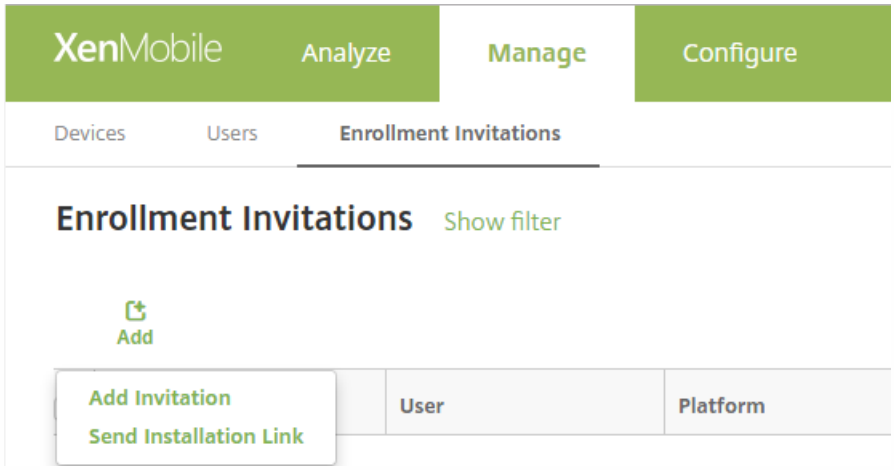
Pré-requisitos

-
-
-
  -
  -
  -
-
  -

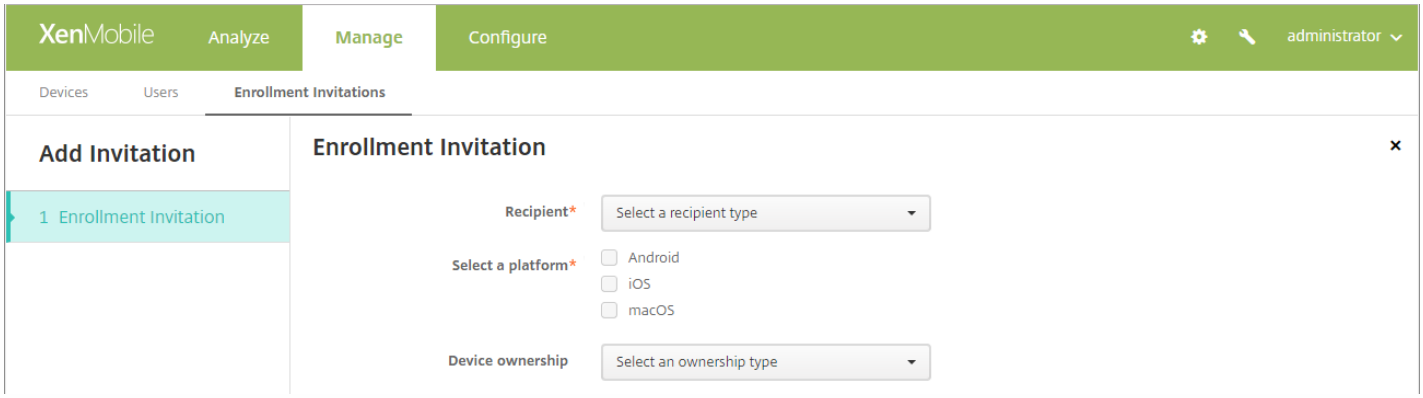
Criar um convite para registro

 © 1999-2017 Citrix Systems, Inc. All rights reserved.



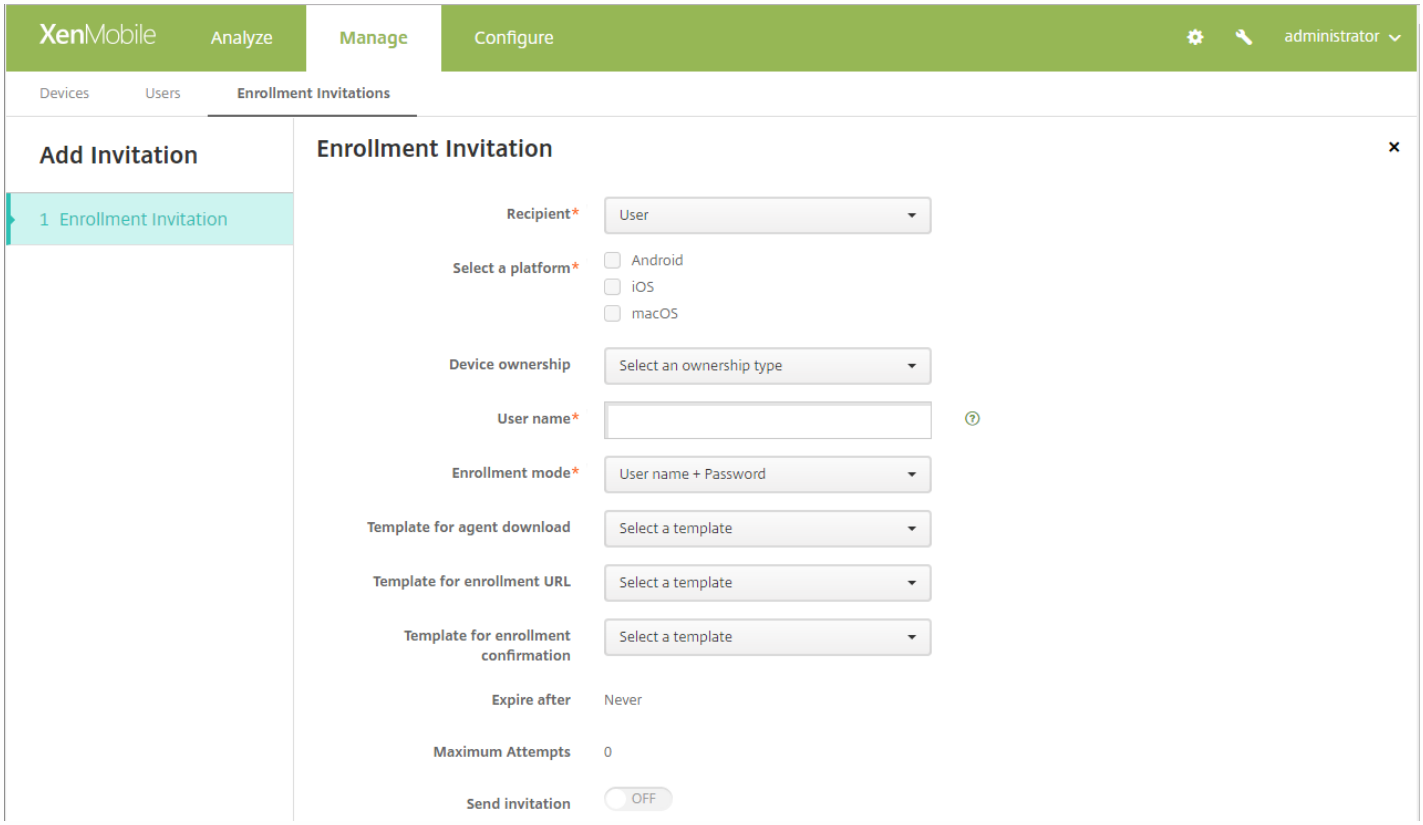


-
-



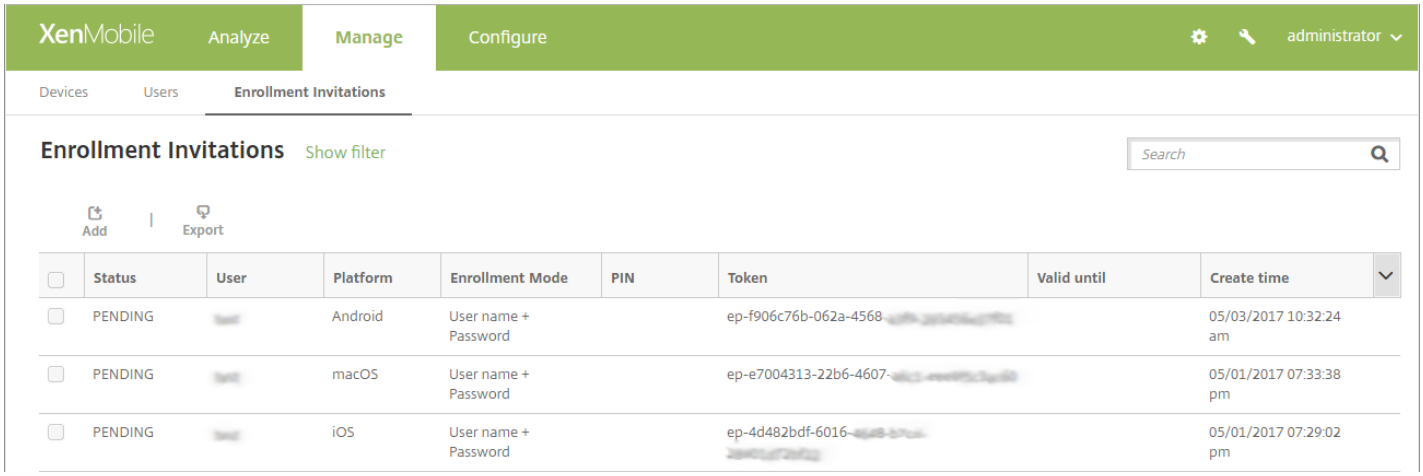
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

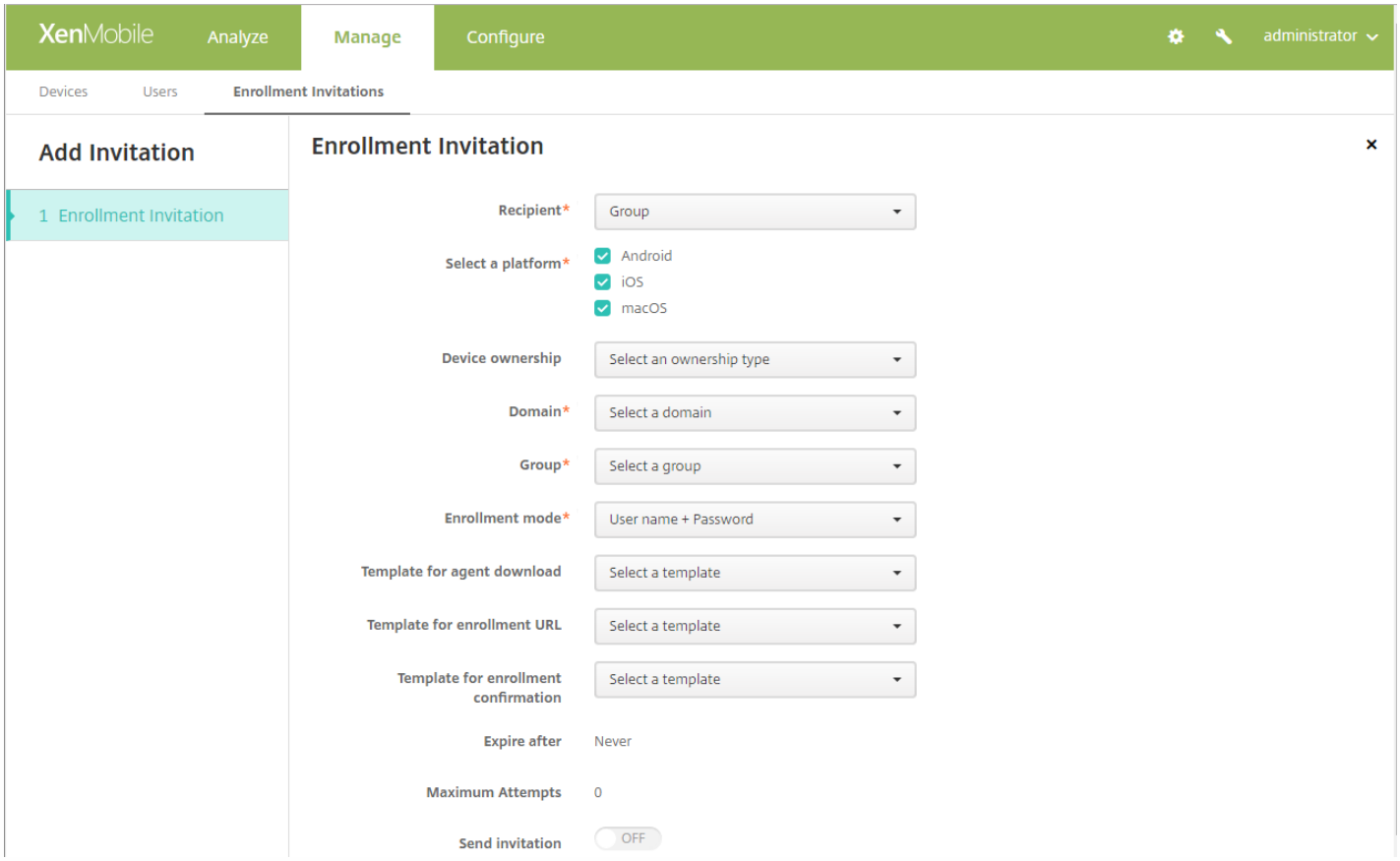


© 1999-2017 Citrix Systems, Inc. All rights reserved.

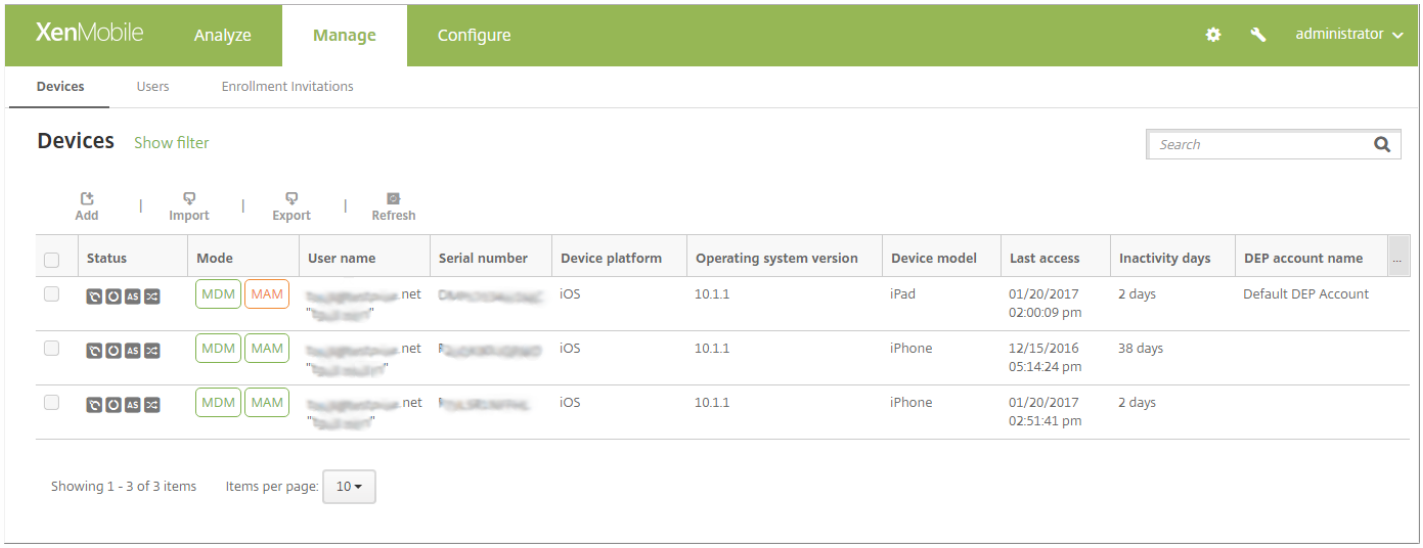
-
-
-
-
-
-

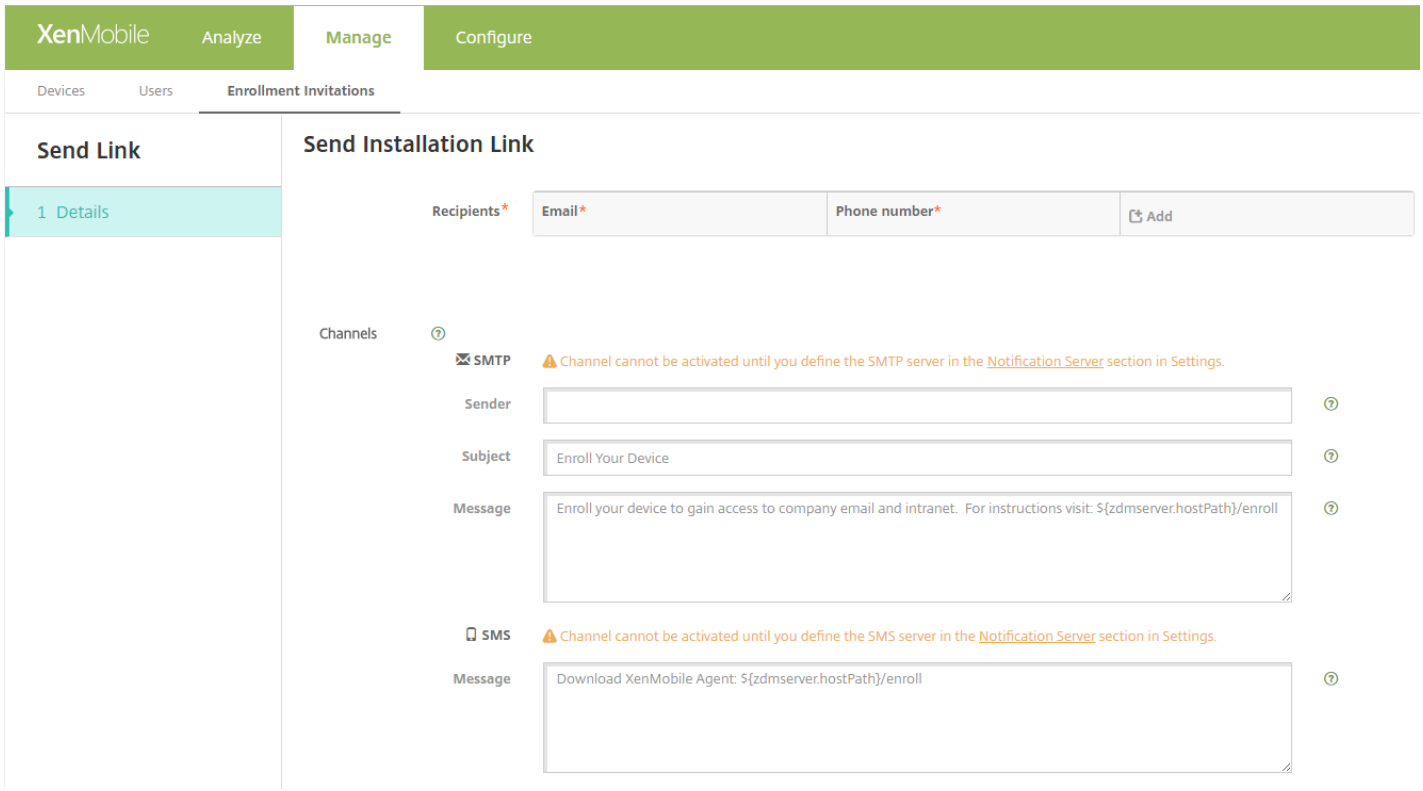


© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.



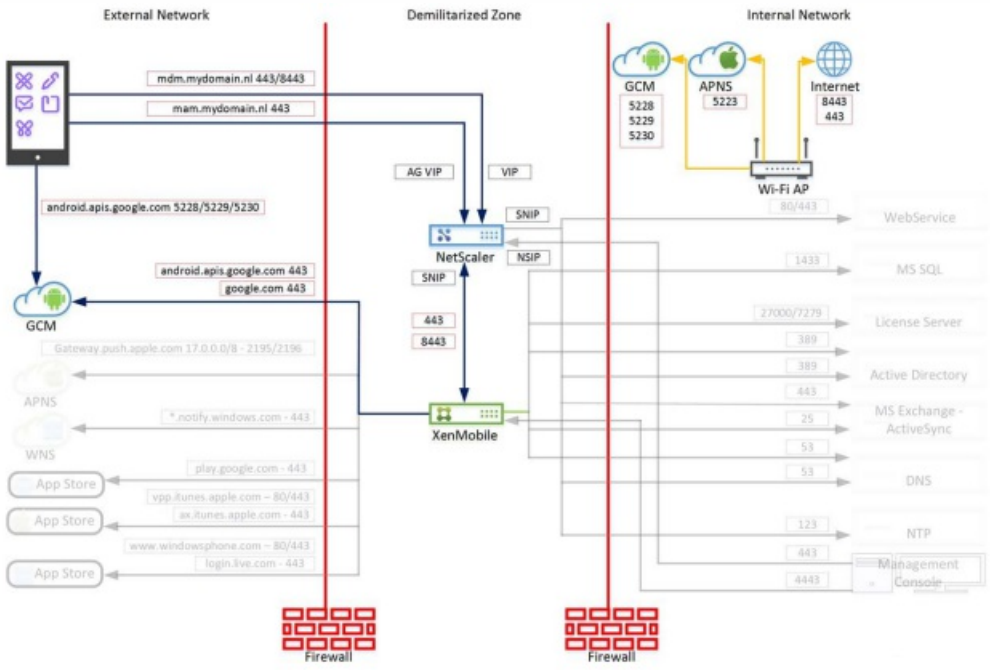


© 1999-2017 Citrix Systems, Inc. All rights reserved.

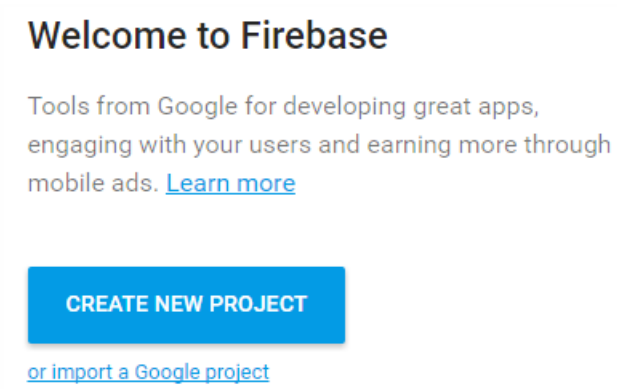
-
  -
  -
  -
-
  -
    -
    -
    -
  -
    -

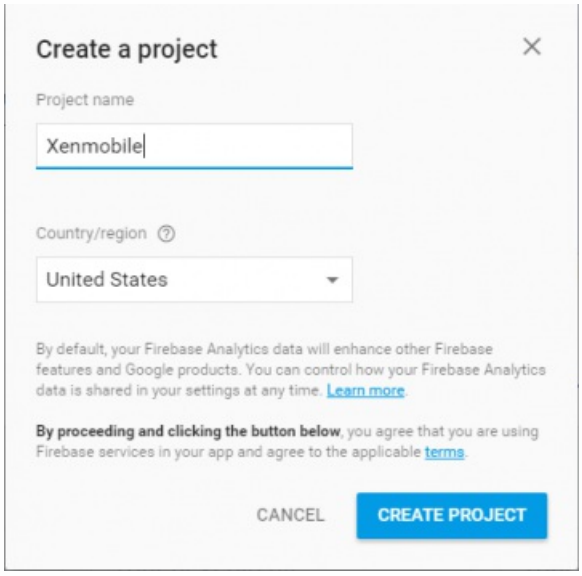
© 1999-2017 Citrix Systems, Inc. All rights reserved.

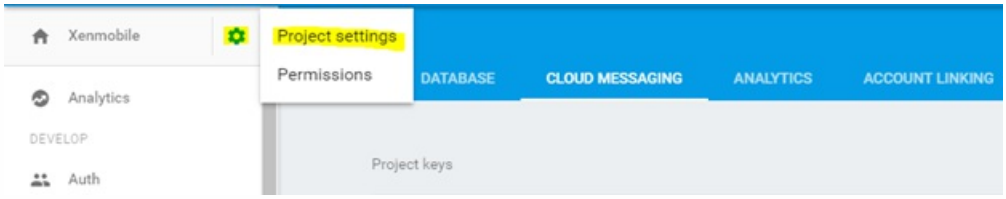
-
-
-
-

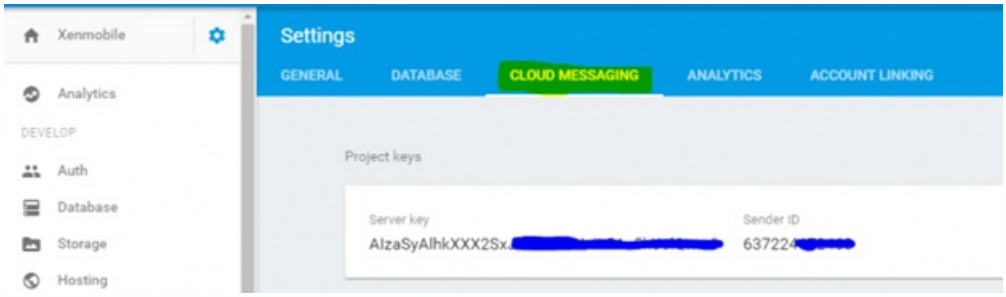


© 1999-2017 Citrix Systems, Inc. All rights reserved.

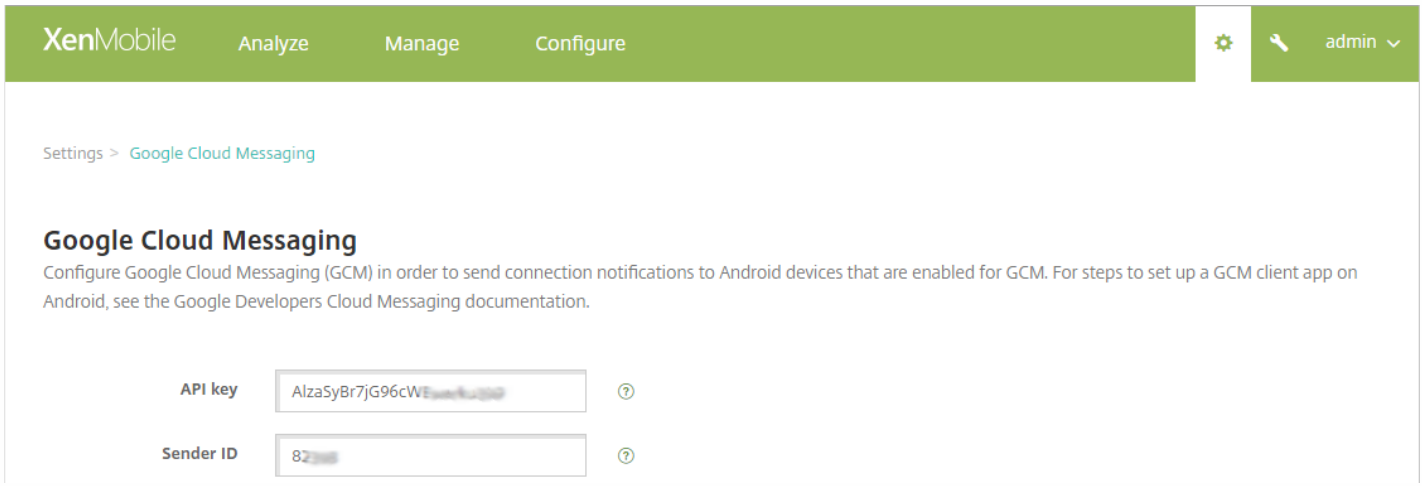


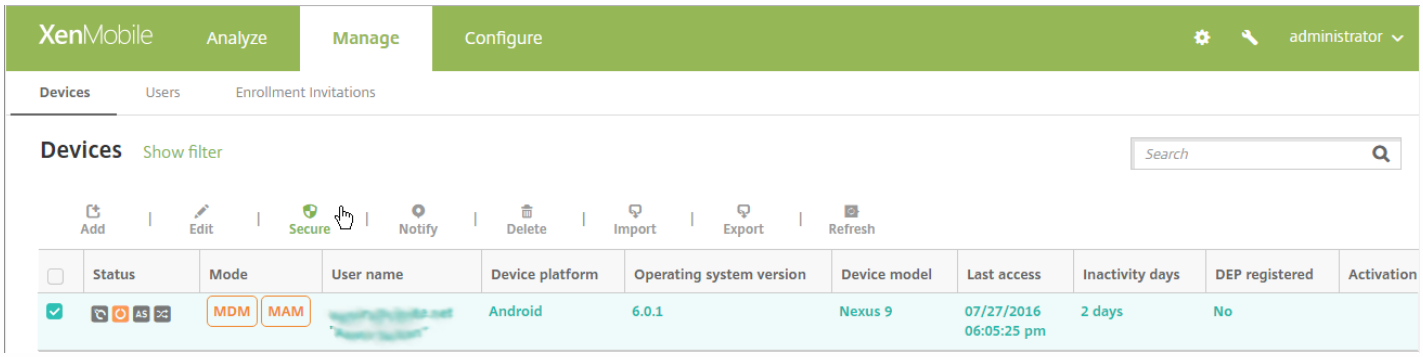




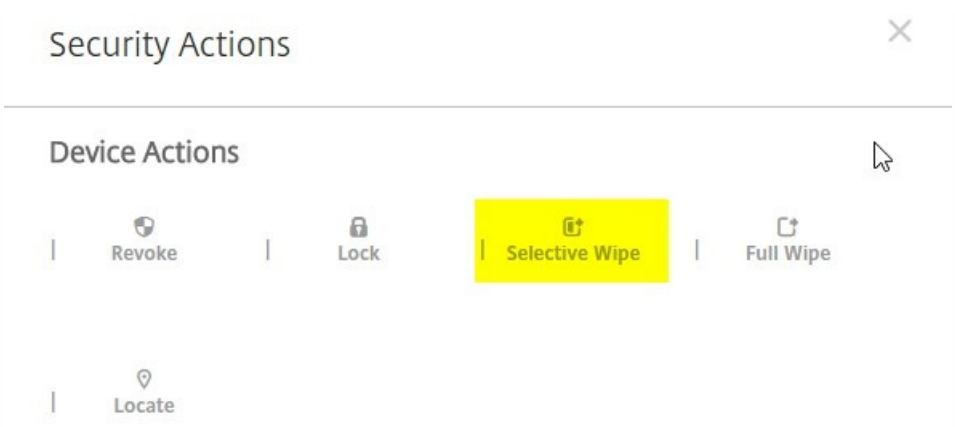


© 1999-2017 Citrix Systems, Inc. All rights reserved.

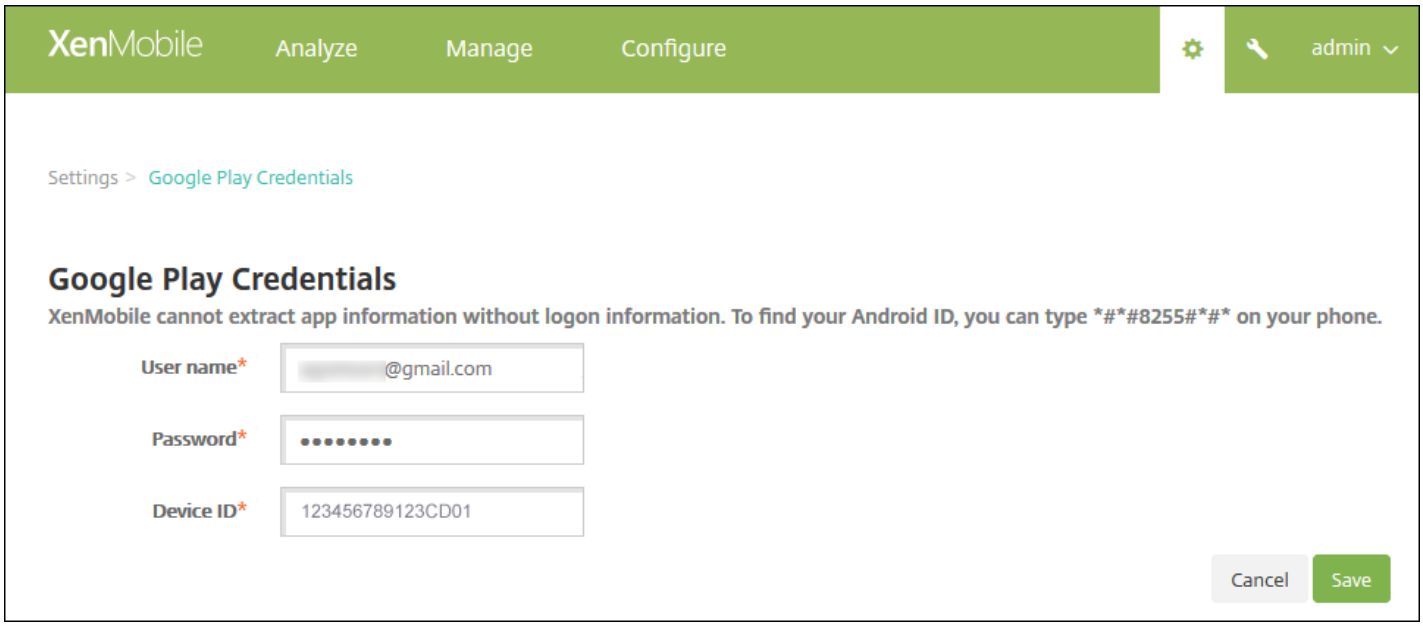




© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-
-
-
-
-

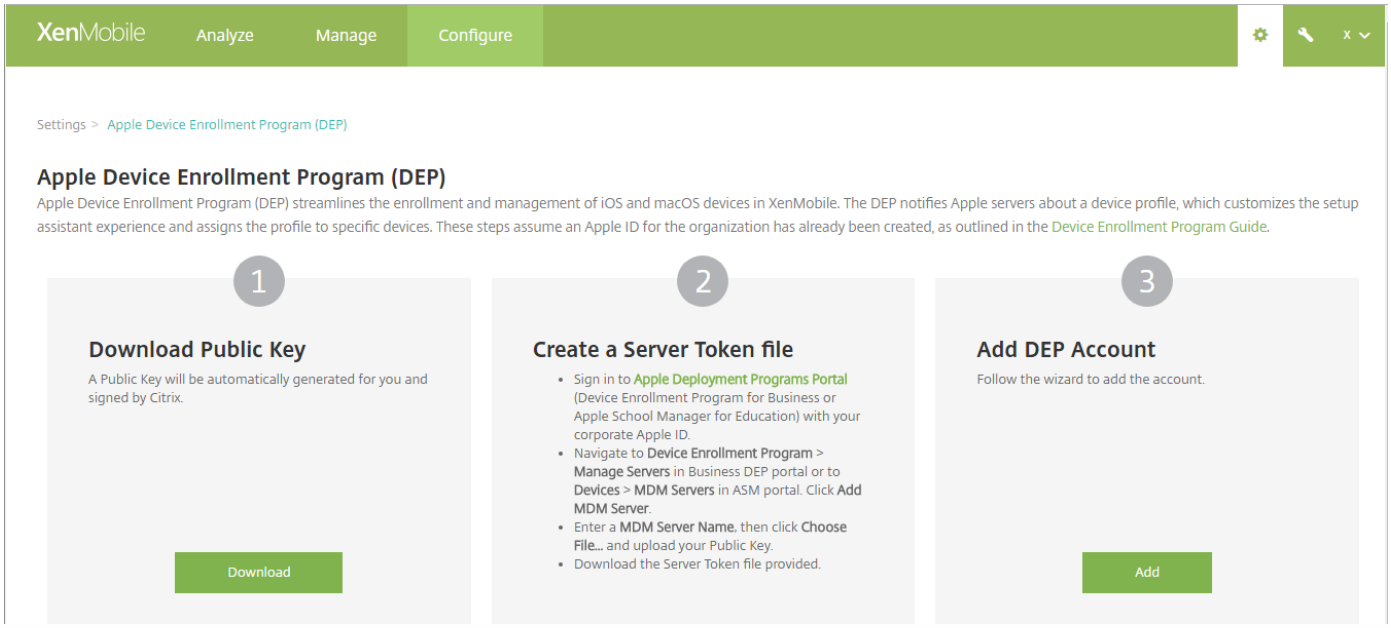
© 1999-2017 Citrix Systems, Inc. All rights reserved.

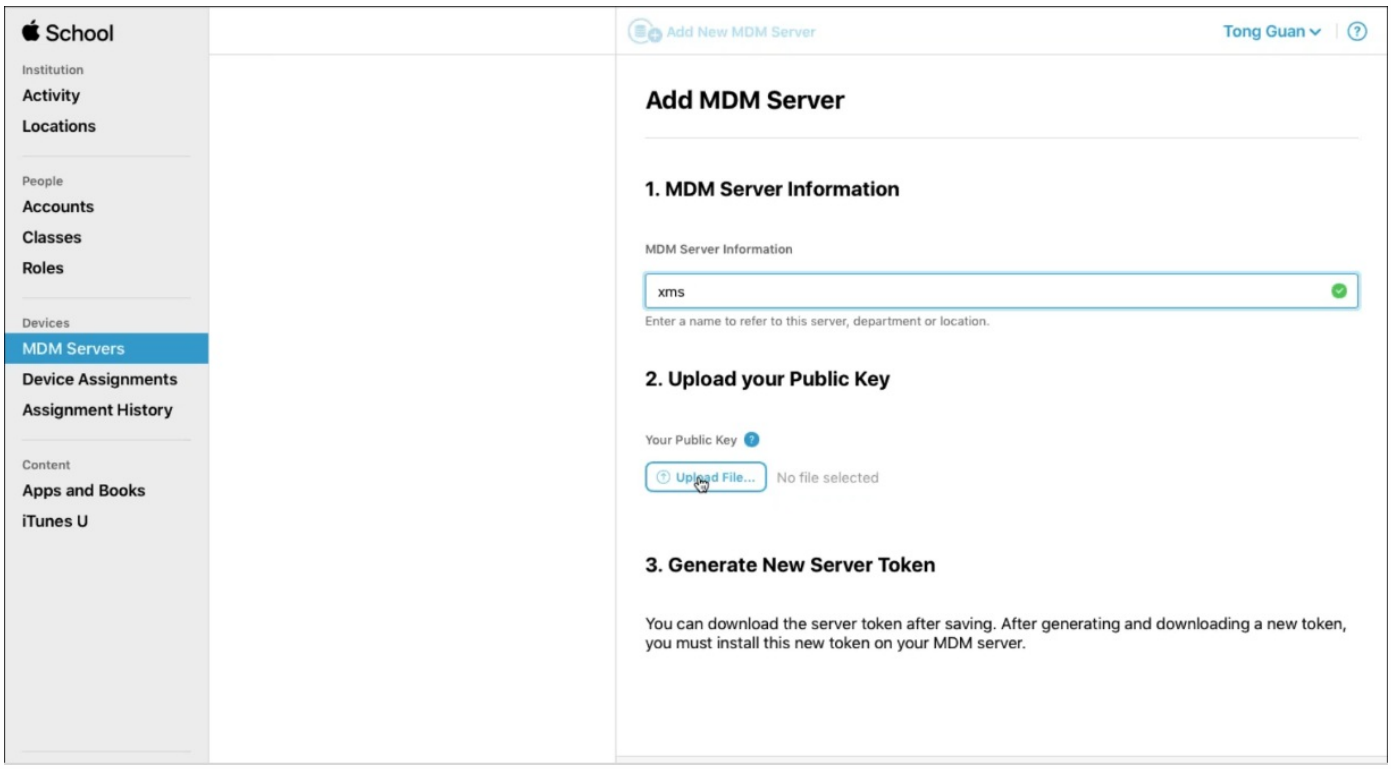
Etapa 1: Crie sua conta do Apple School Manager e siga o Assistente de Configuração

-
-
-
-
-

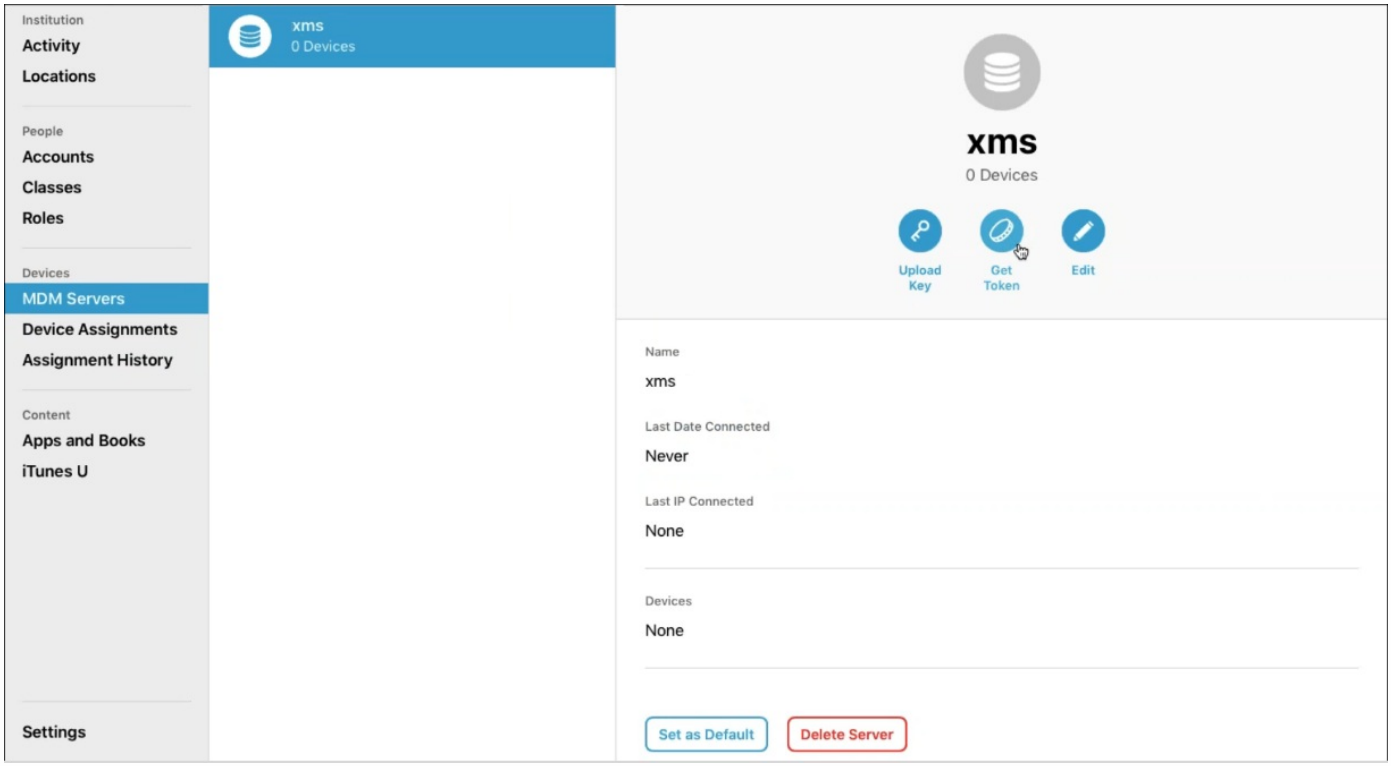
Etapa 2: Configure o XenMobile Server como o servidor MDM para o Apple School Manager e configure as atribuições do dispositivo

© 1999-2017 Citrix Systems, Inc. All rights reserved.

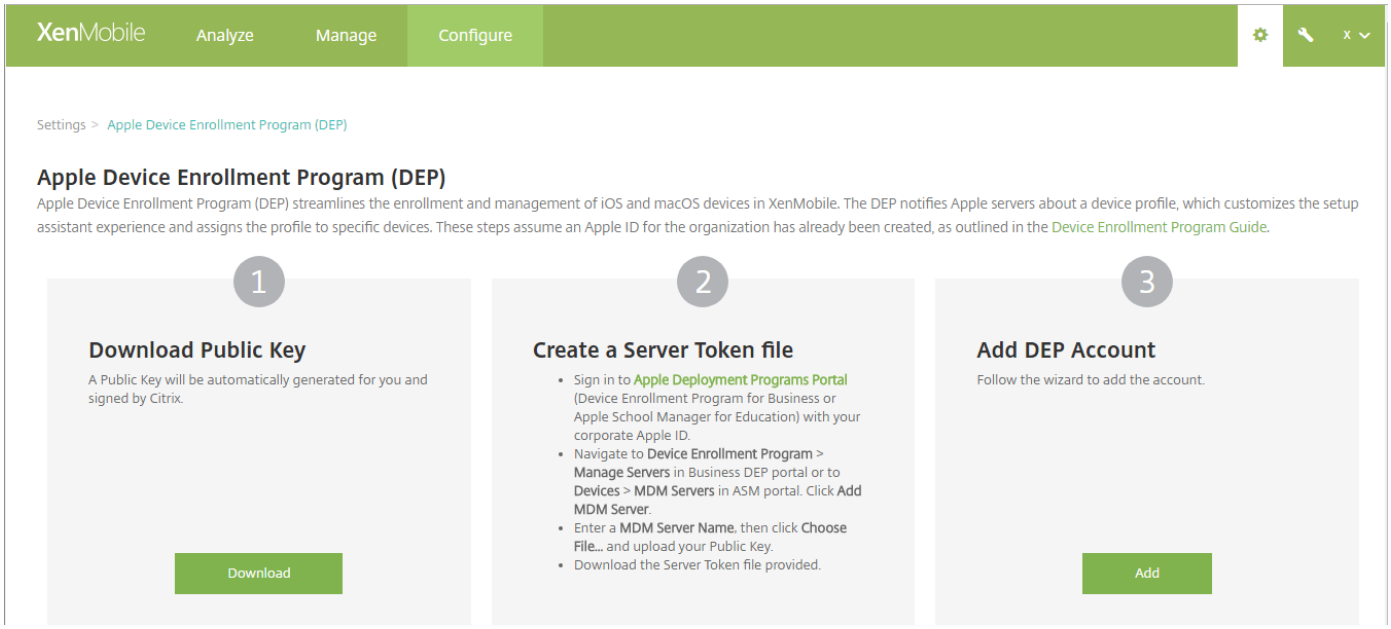




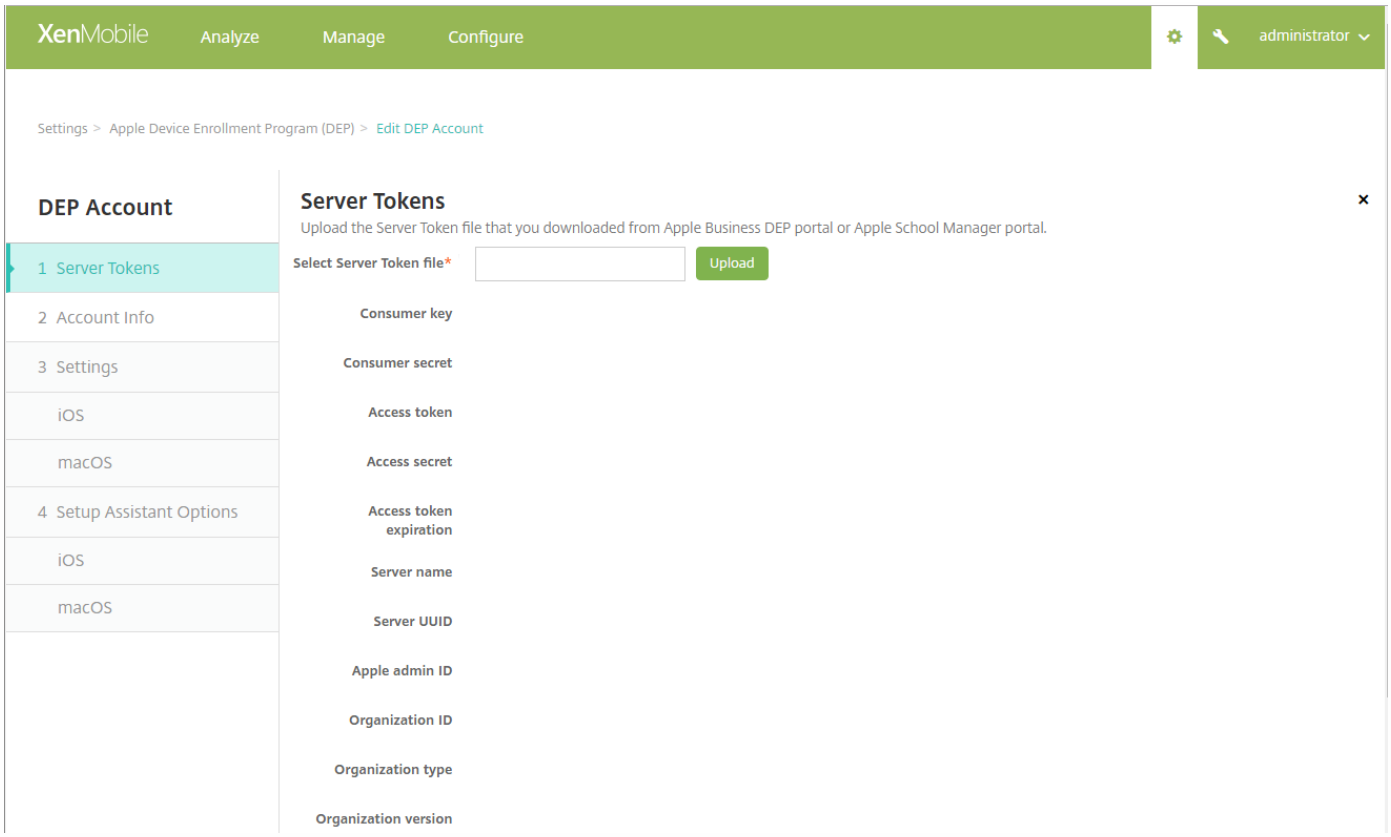
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Etapa 3: Adicione a conta do Apple School Manager ao XenMobile Server

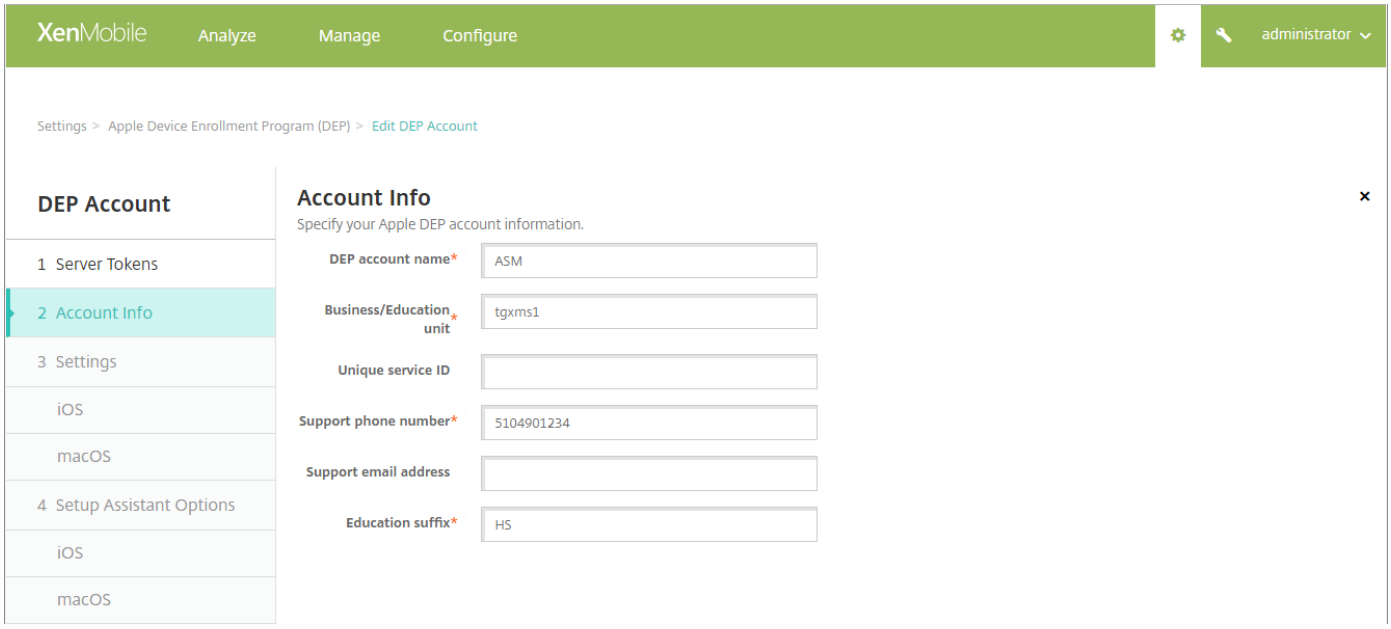


© 1999-2017 Citrix Systems, Inc. All rights reserved.



-

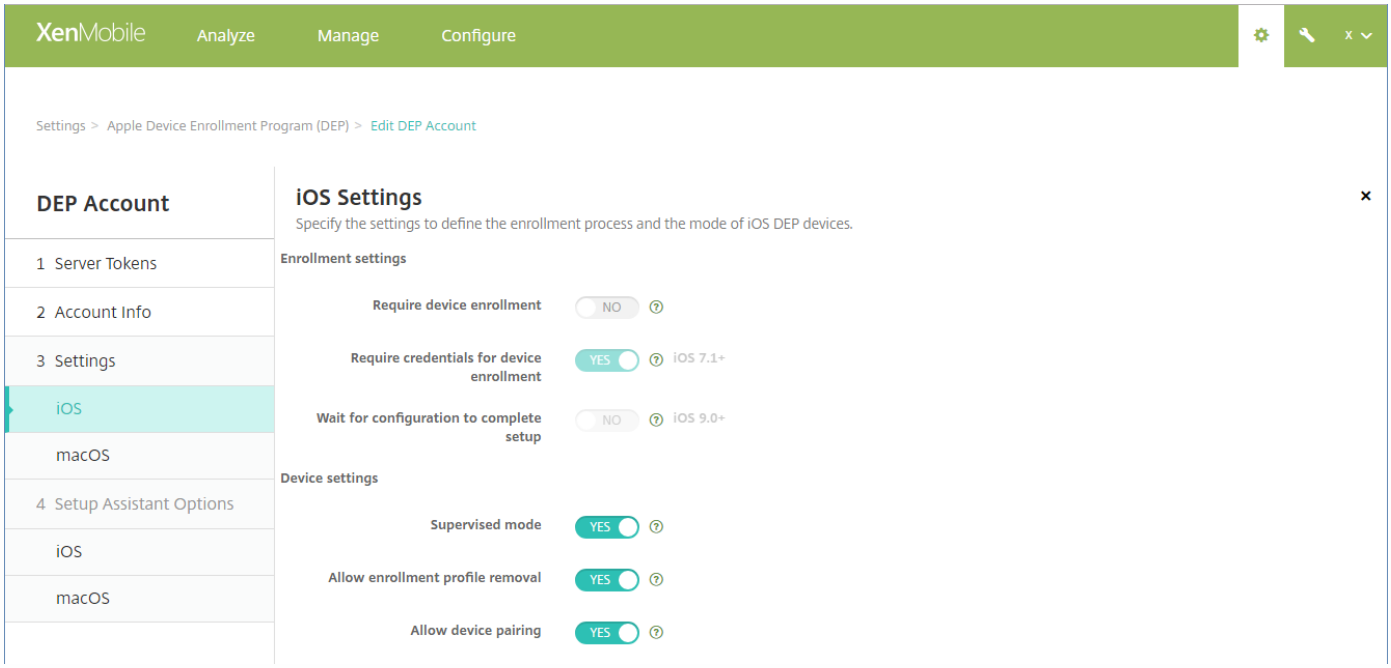
-



-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

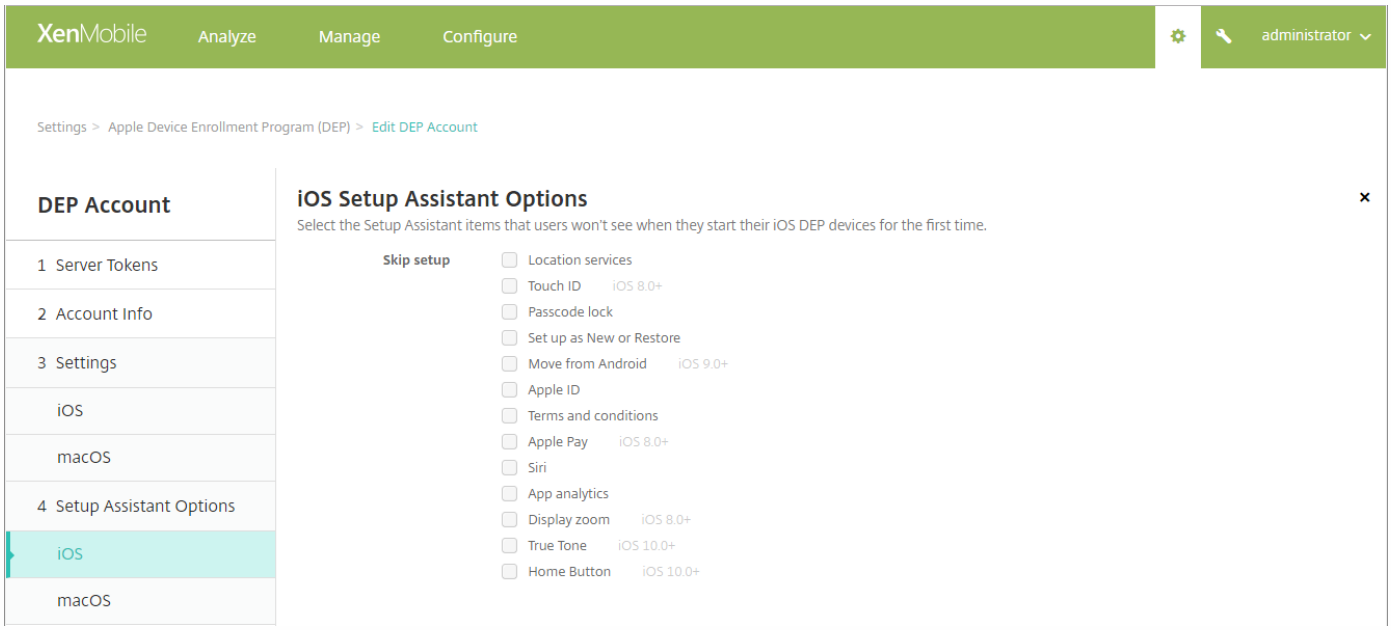
-
-
-
-
-



-
-
-
-
-
-
-

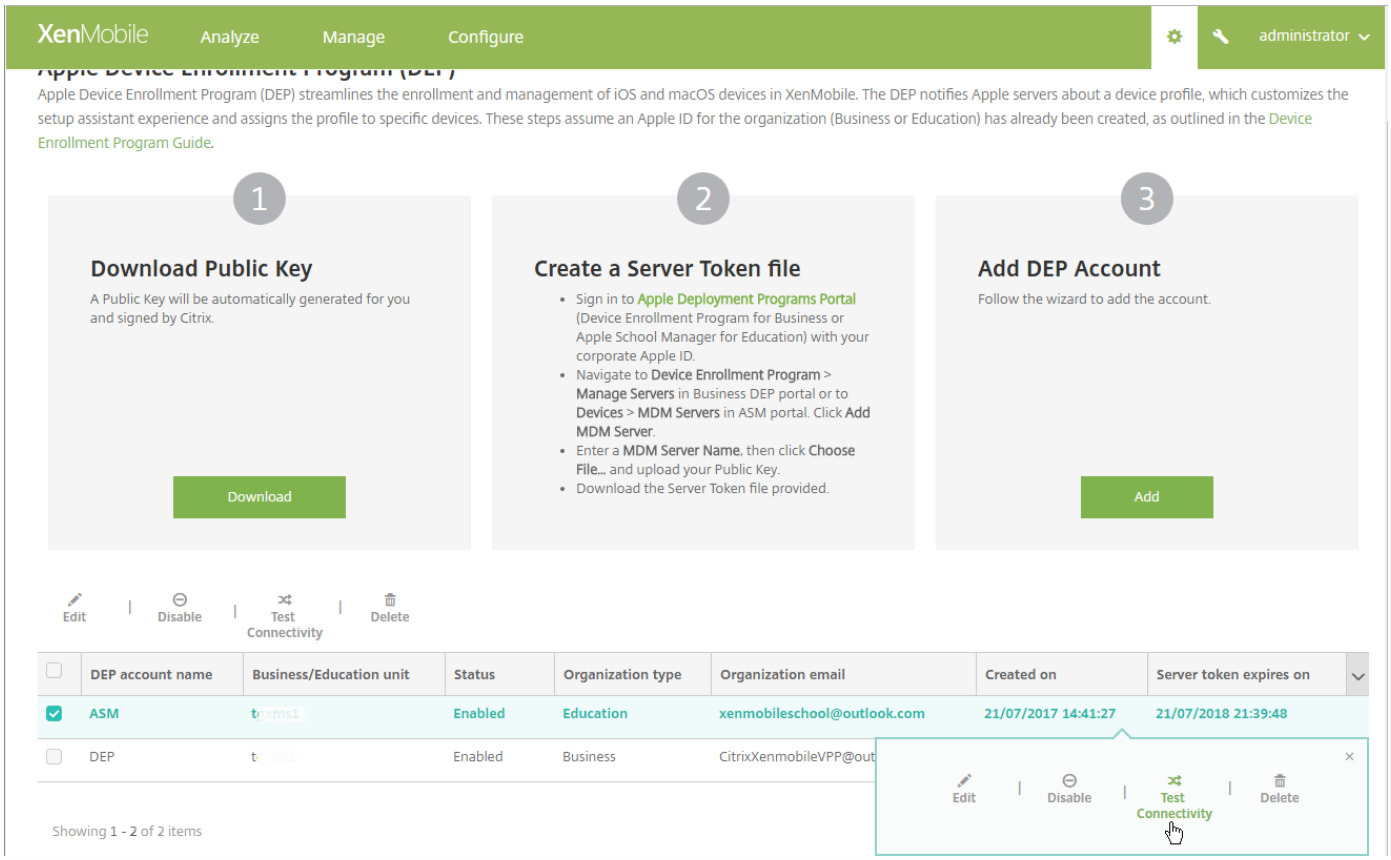
© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-

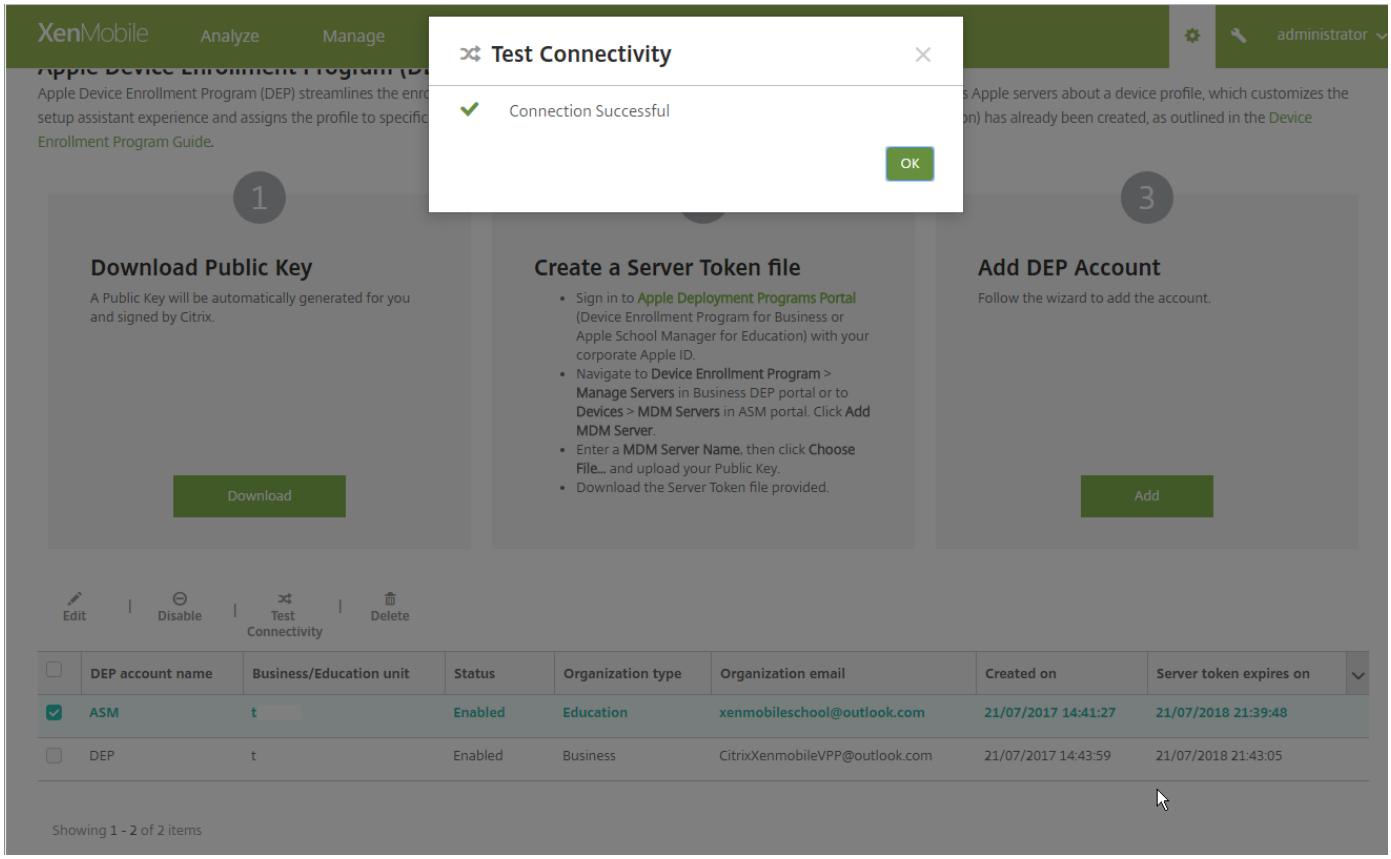


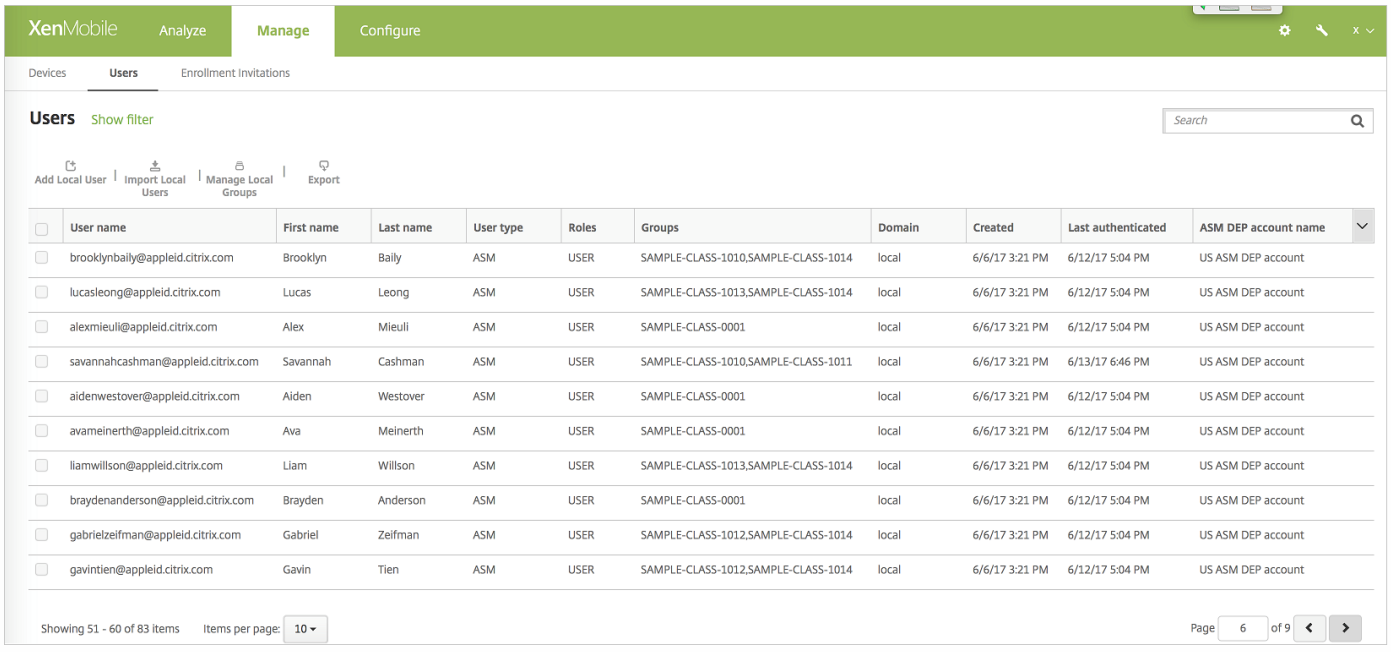
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.



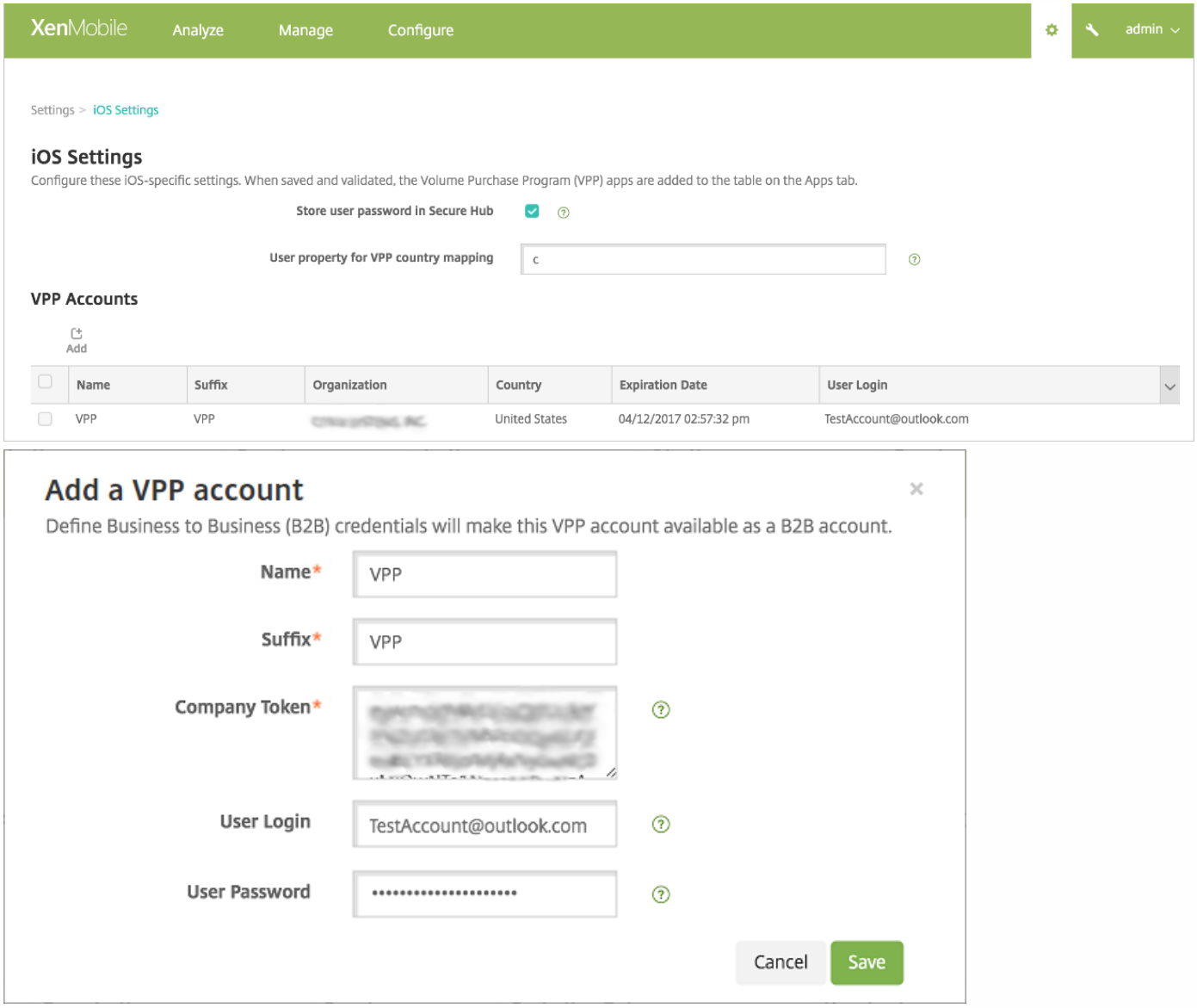
© 1999-2017 Citrix Systems, Inc. All rights reserved.





Etapa 4: Configure uma conta VPP de Educação para o Apple School Manager

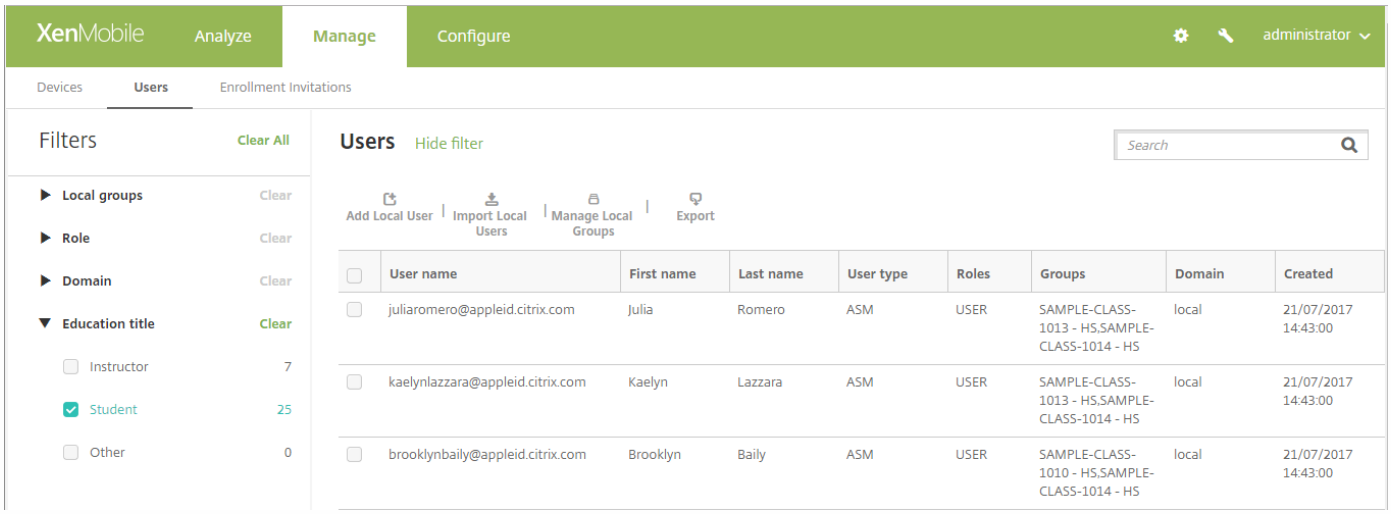
© 1999-2017 Citrix Systems, Inc. All rights reserved.



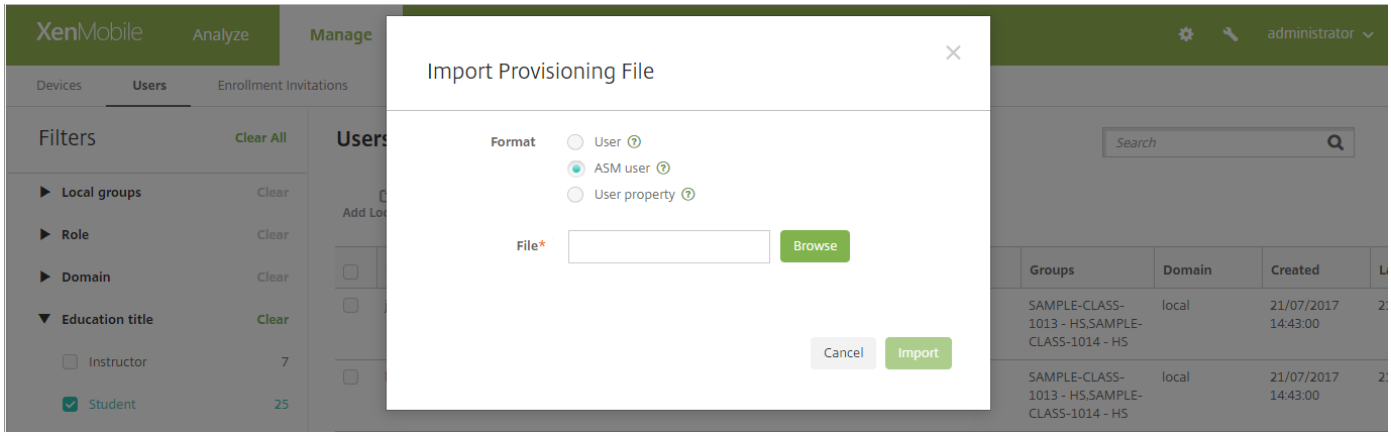
Etapa 5: Adicione senhas para usuários do Apple School Manager

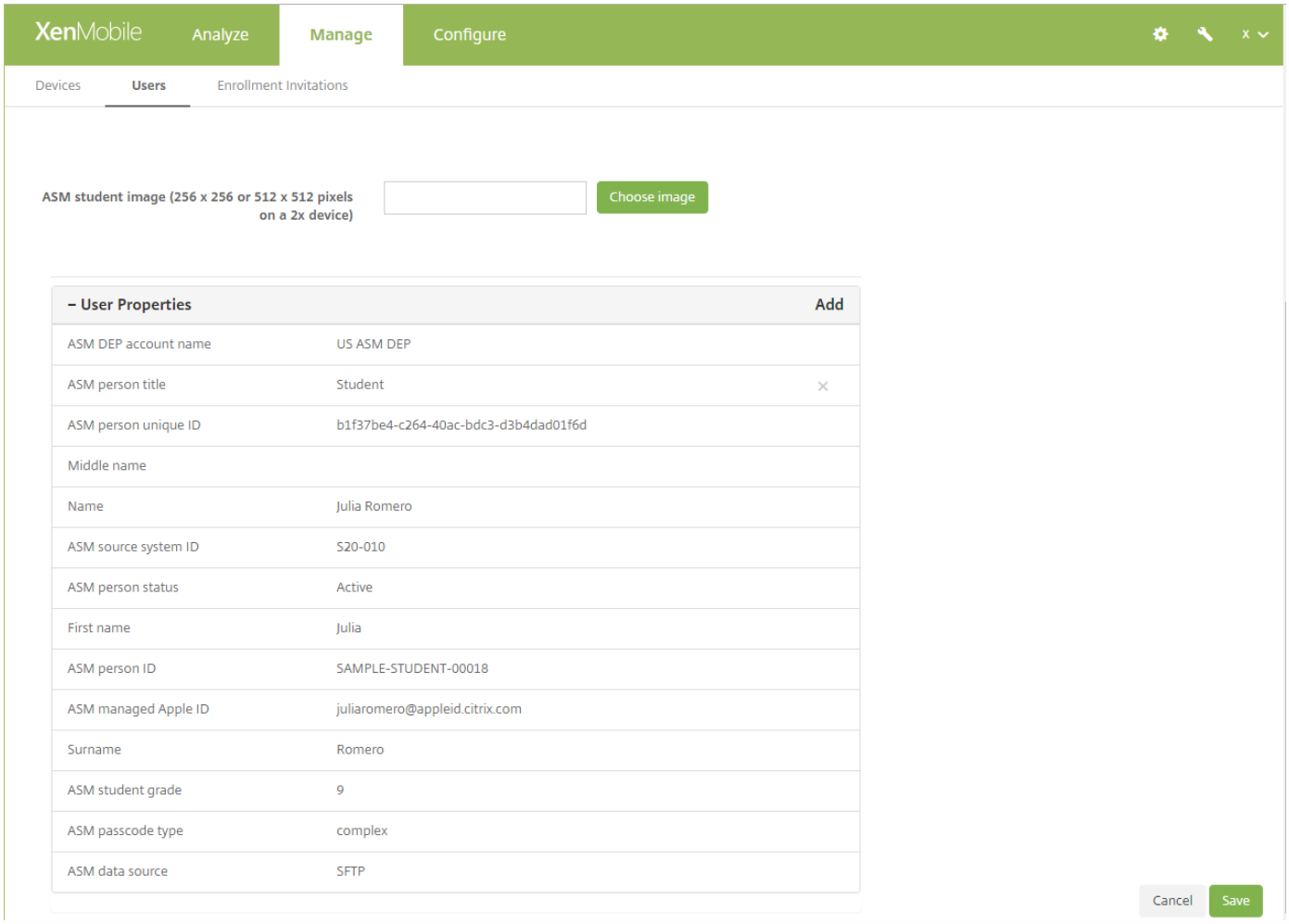
© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-



© 1999-2017 Citrix Systems, Inc. All rights reserved.





-
-
-
-
-

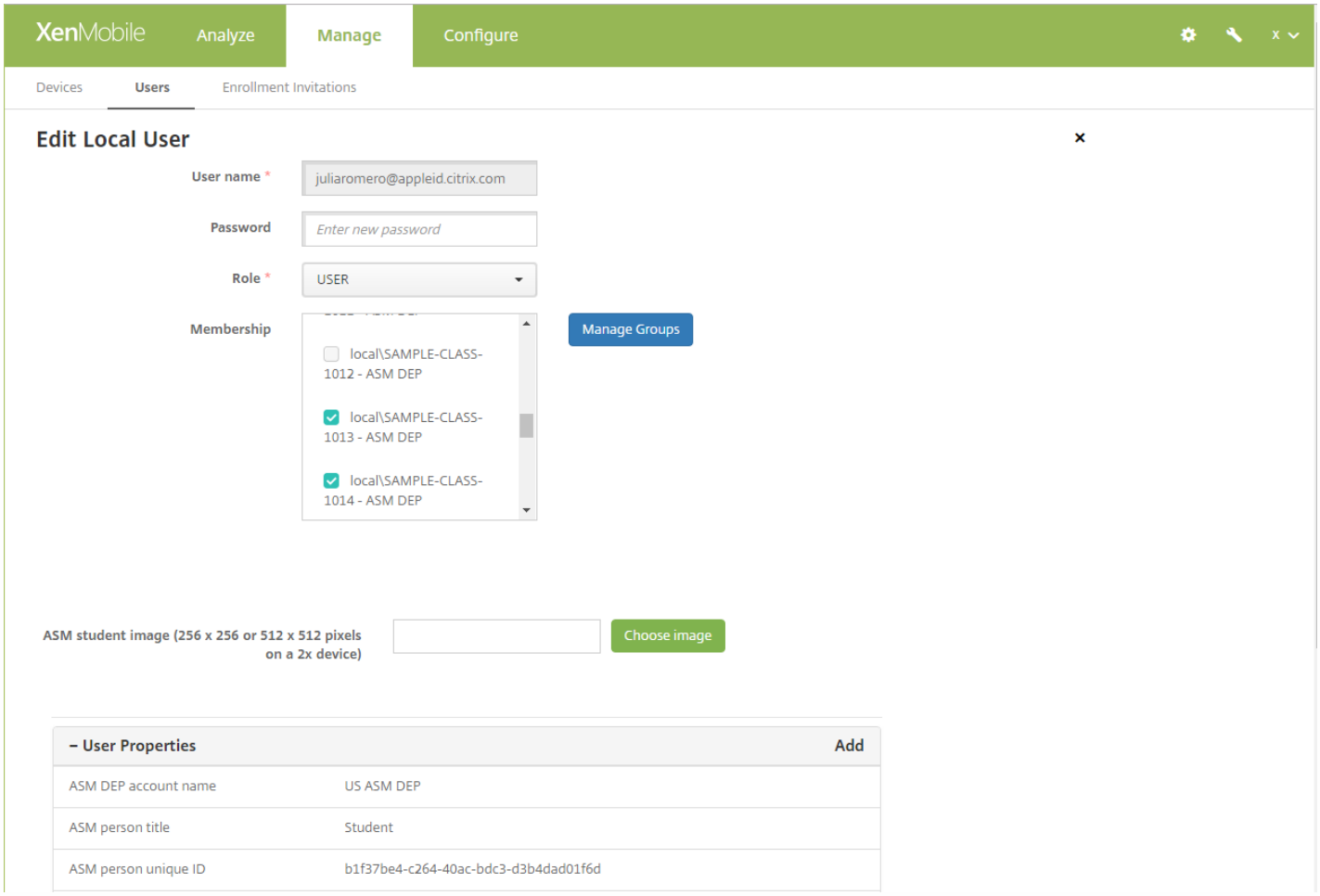
© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-

Etapa 6: Opcionalmente, adicione fotos de alunos

-
-

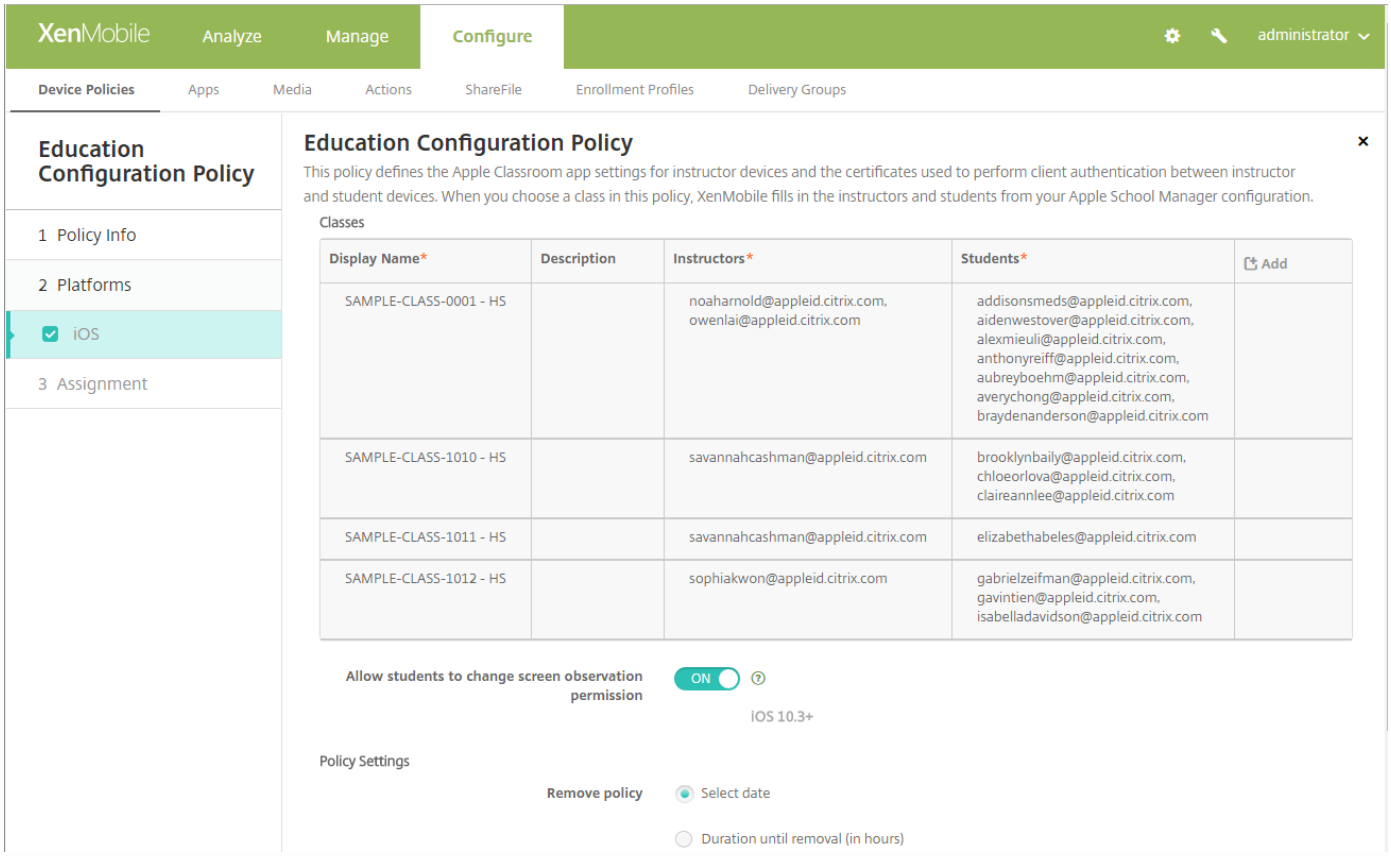
© 1999-2017 Citrix Systems, Inc. All rights reserved.



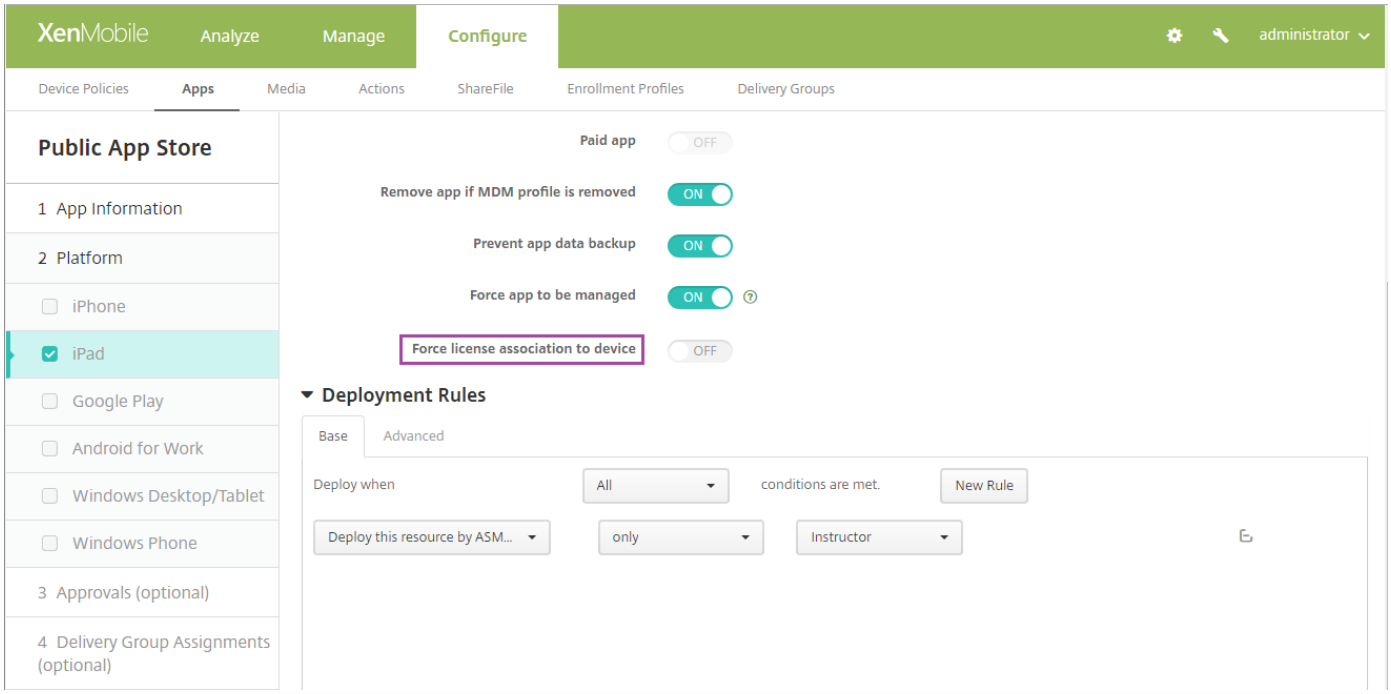
Etapa 7: Planeje e adicione recursos e grupos de entrega ao XenMobile Server

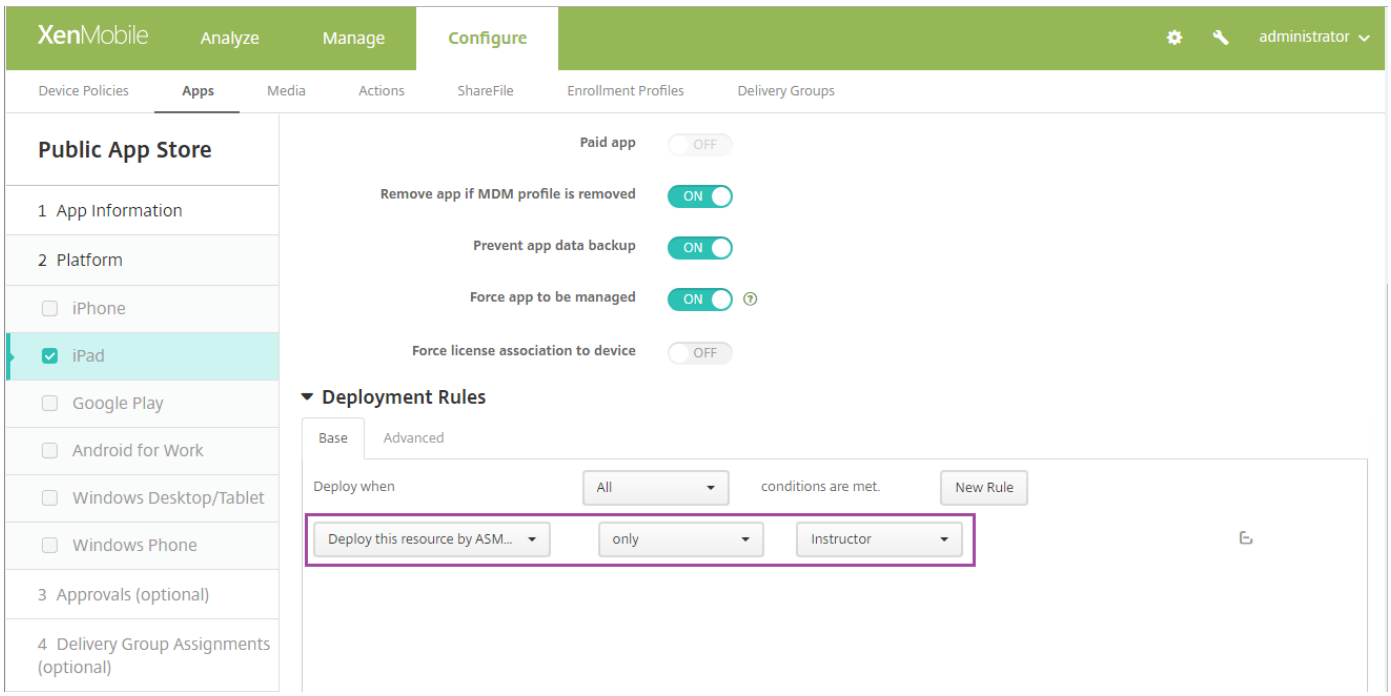
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

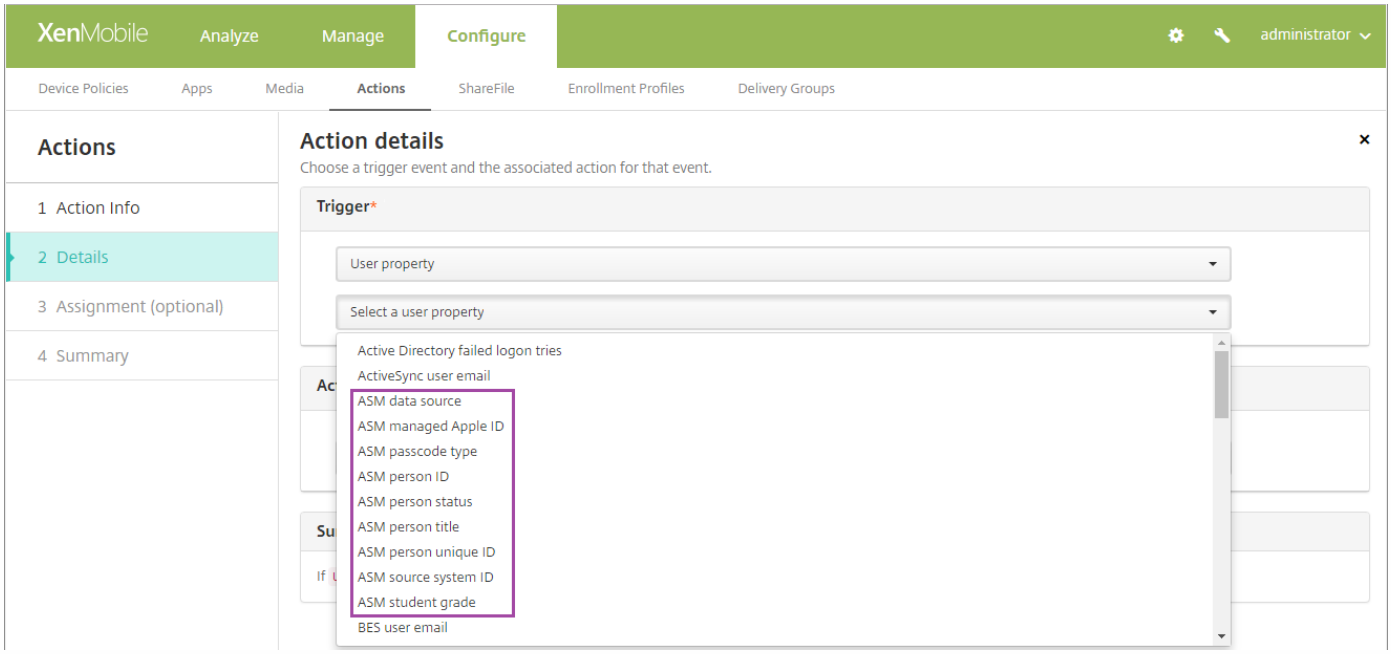


© 1999-2017 Citrix Systems, Inc. All rights reserved.

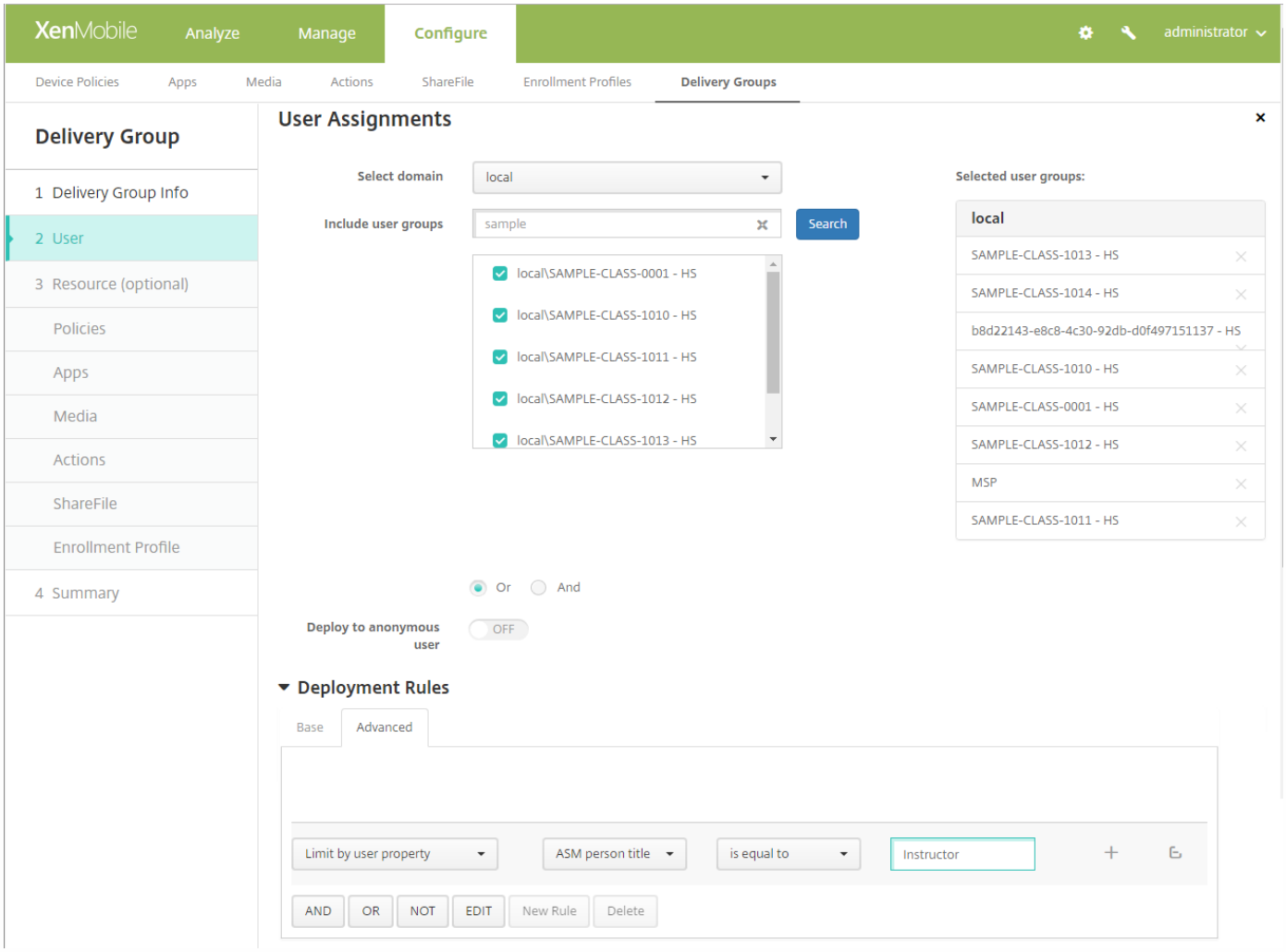




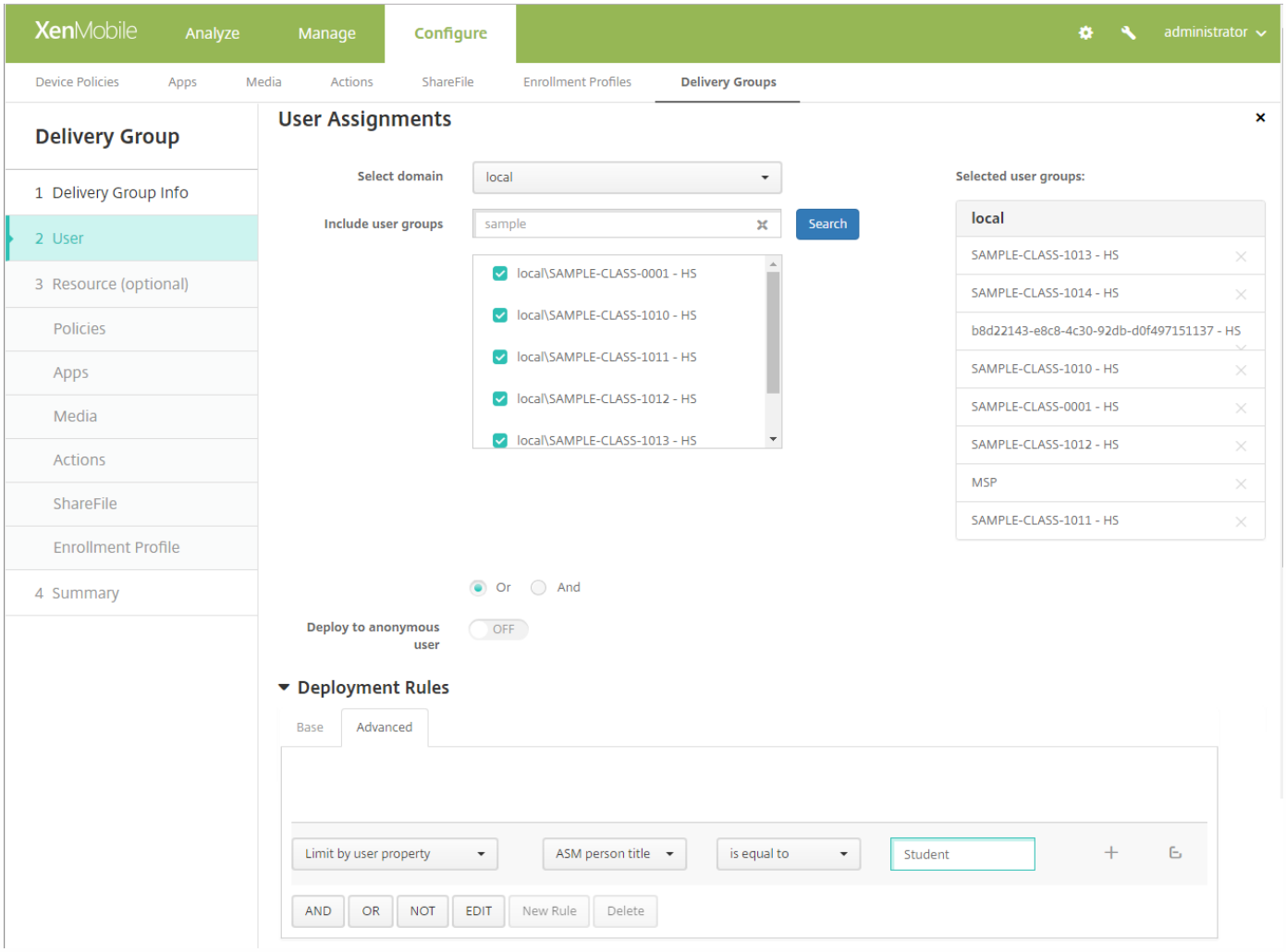
© 1999-2017 Citrix Systems, Inc. All rights reserved.

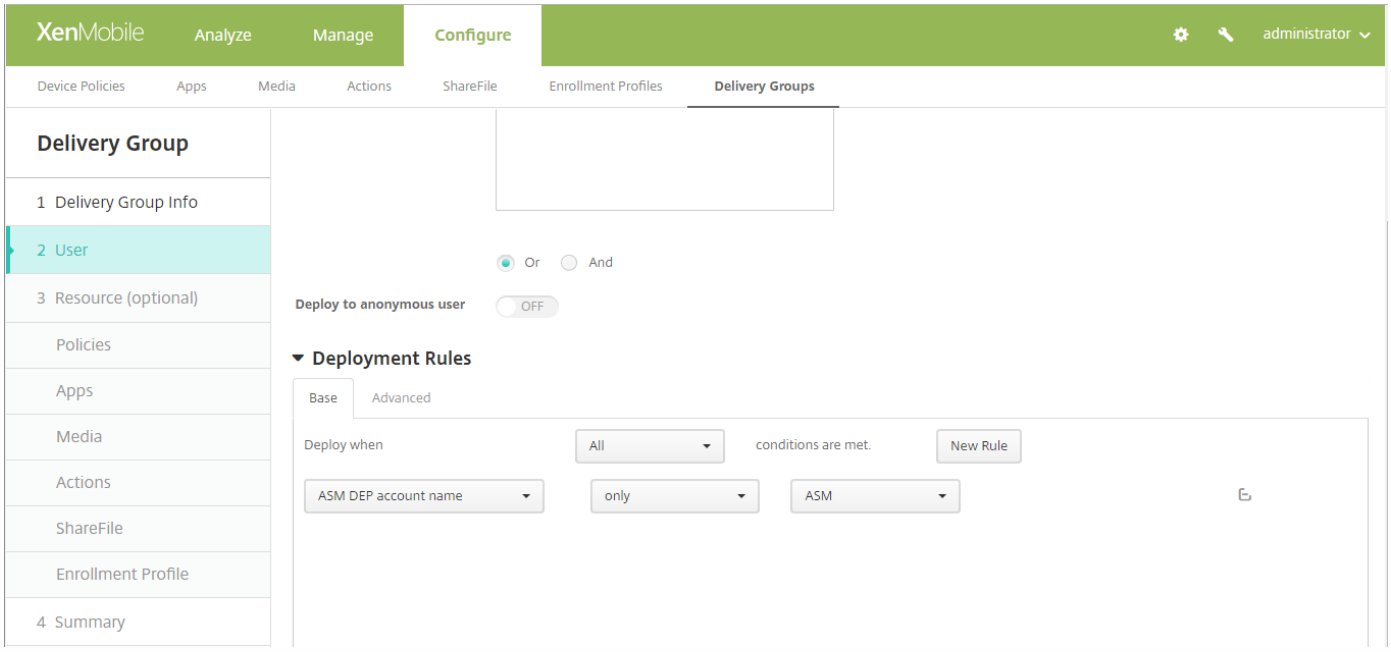


© 1999-2017 Citrix Systems, Inc. All rights reserved.

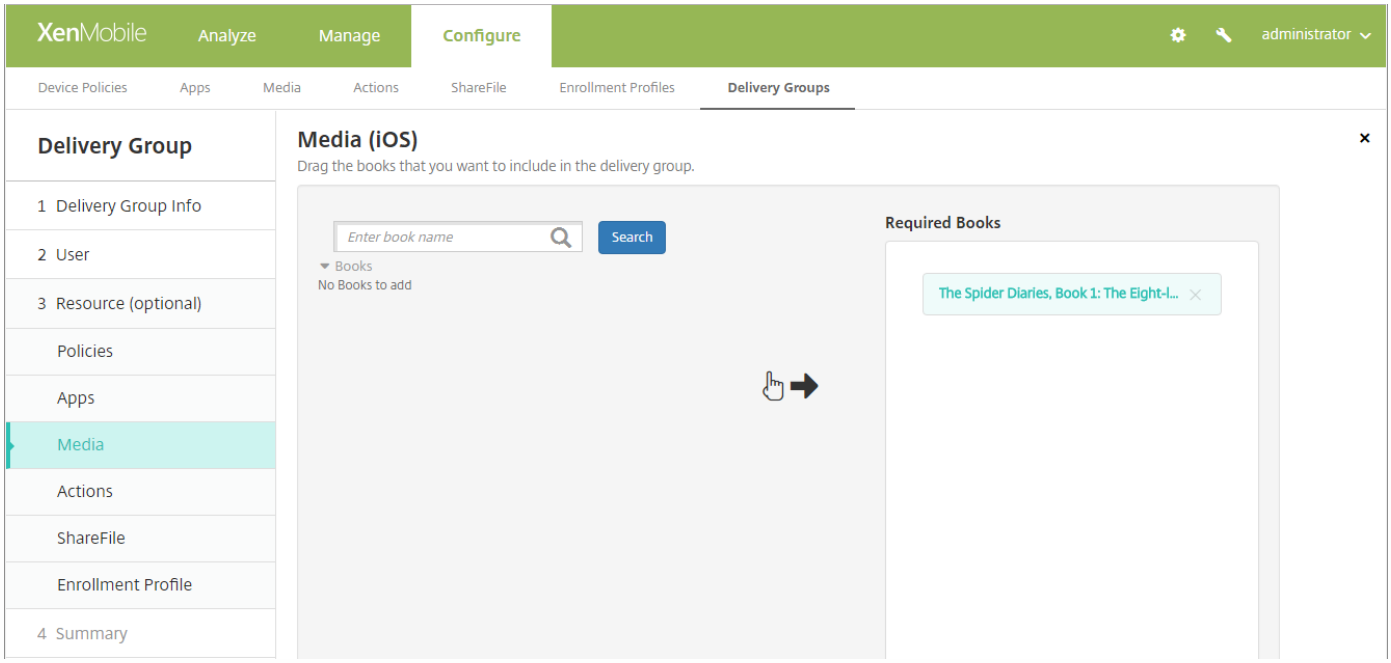


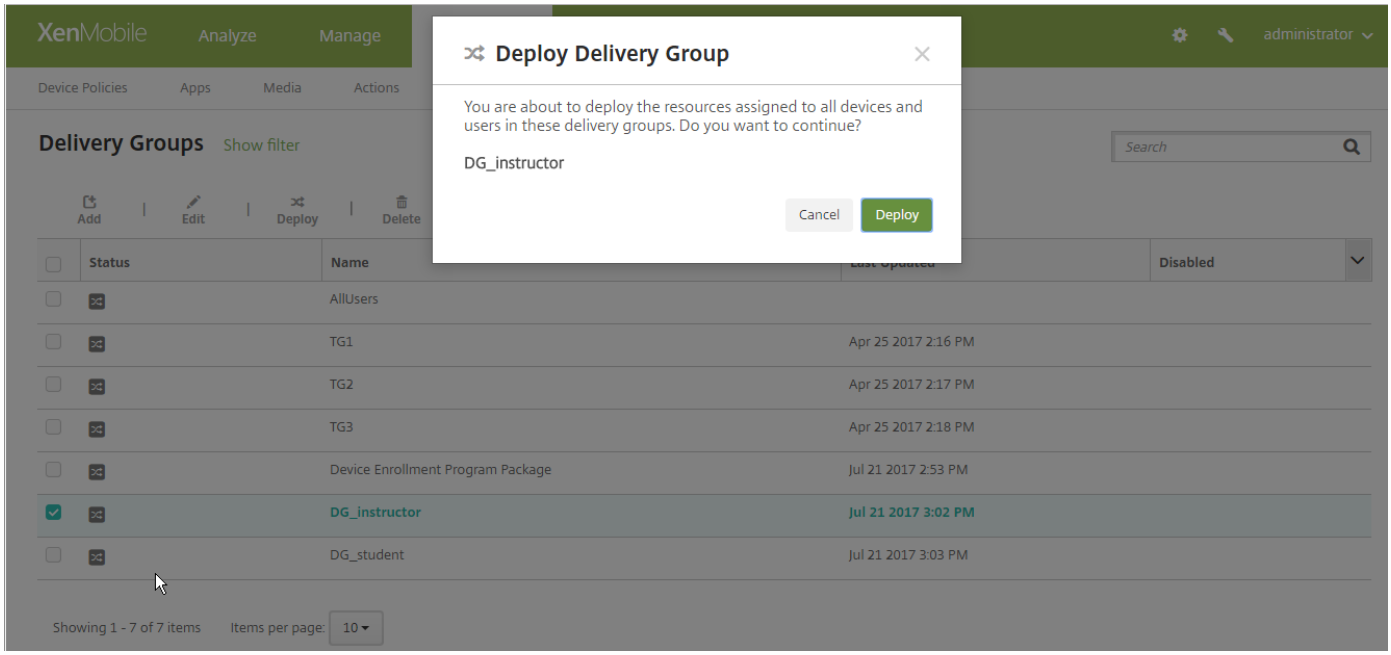
© 1999-2017 Citrix Systems, Inc. All rights reserved.





© 1999-2017 Citrix Systems, Inc. All rights reserved.

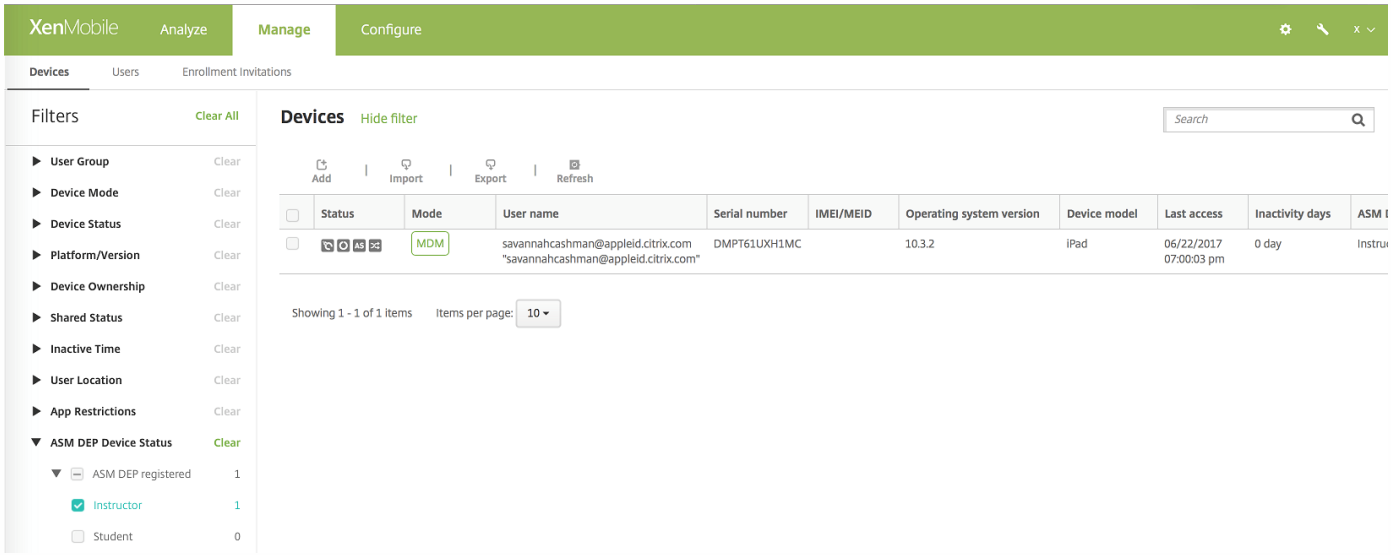




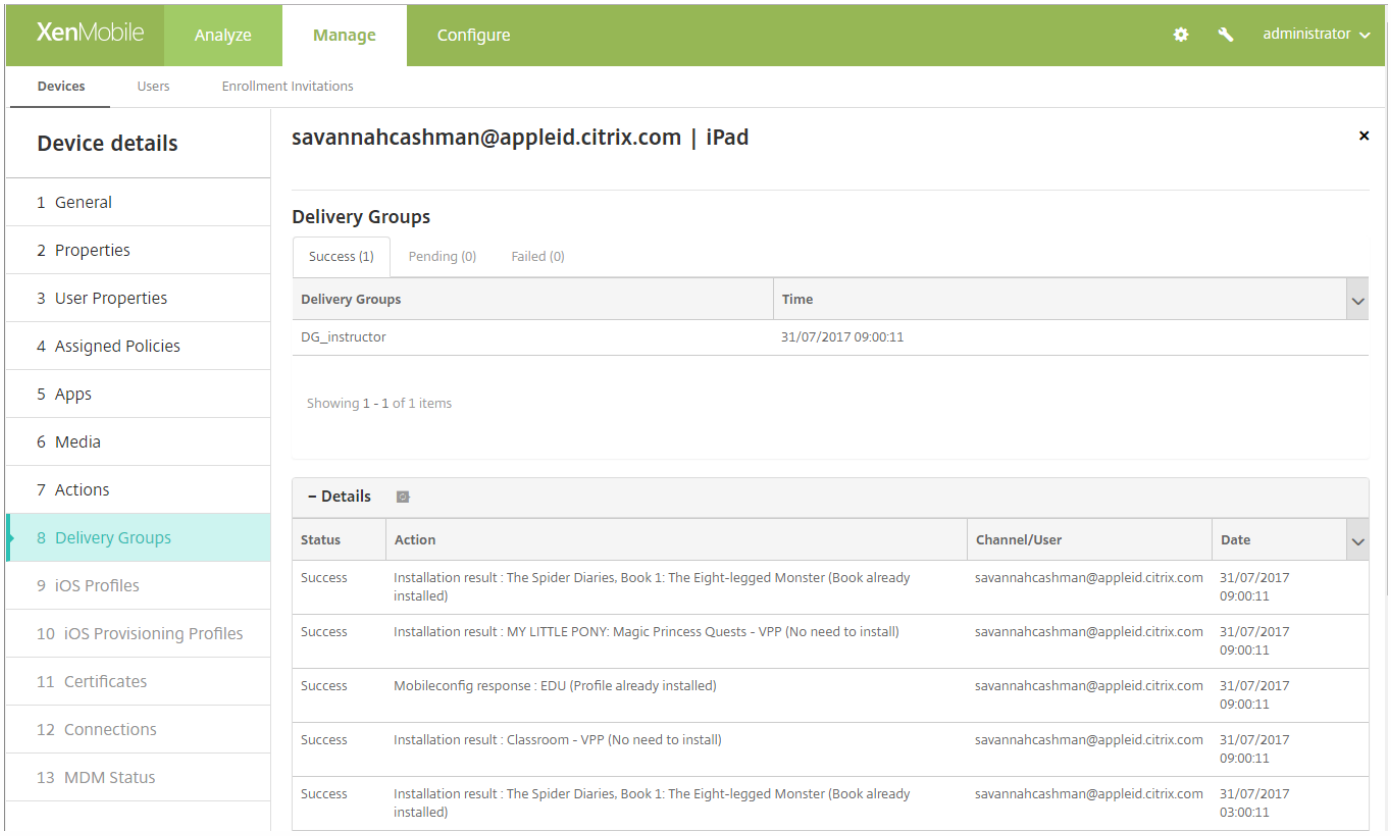
Etapa 8: Teste o registro do dispositivo do instrutor e aluno

-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.



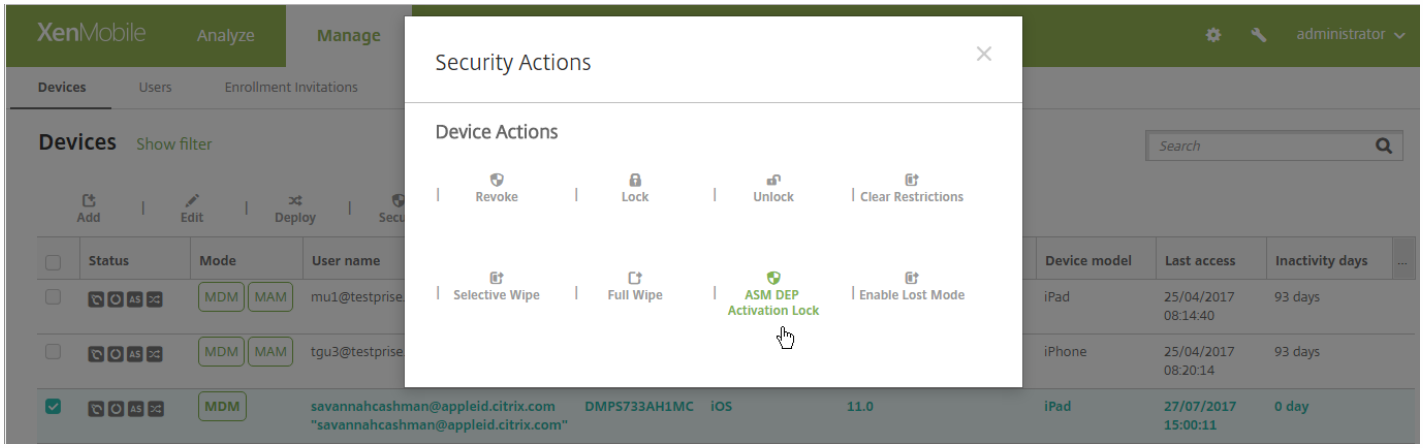
Etapa 9: Distribua os dispositivos

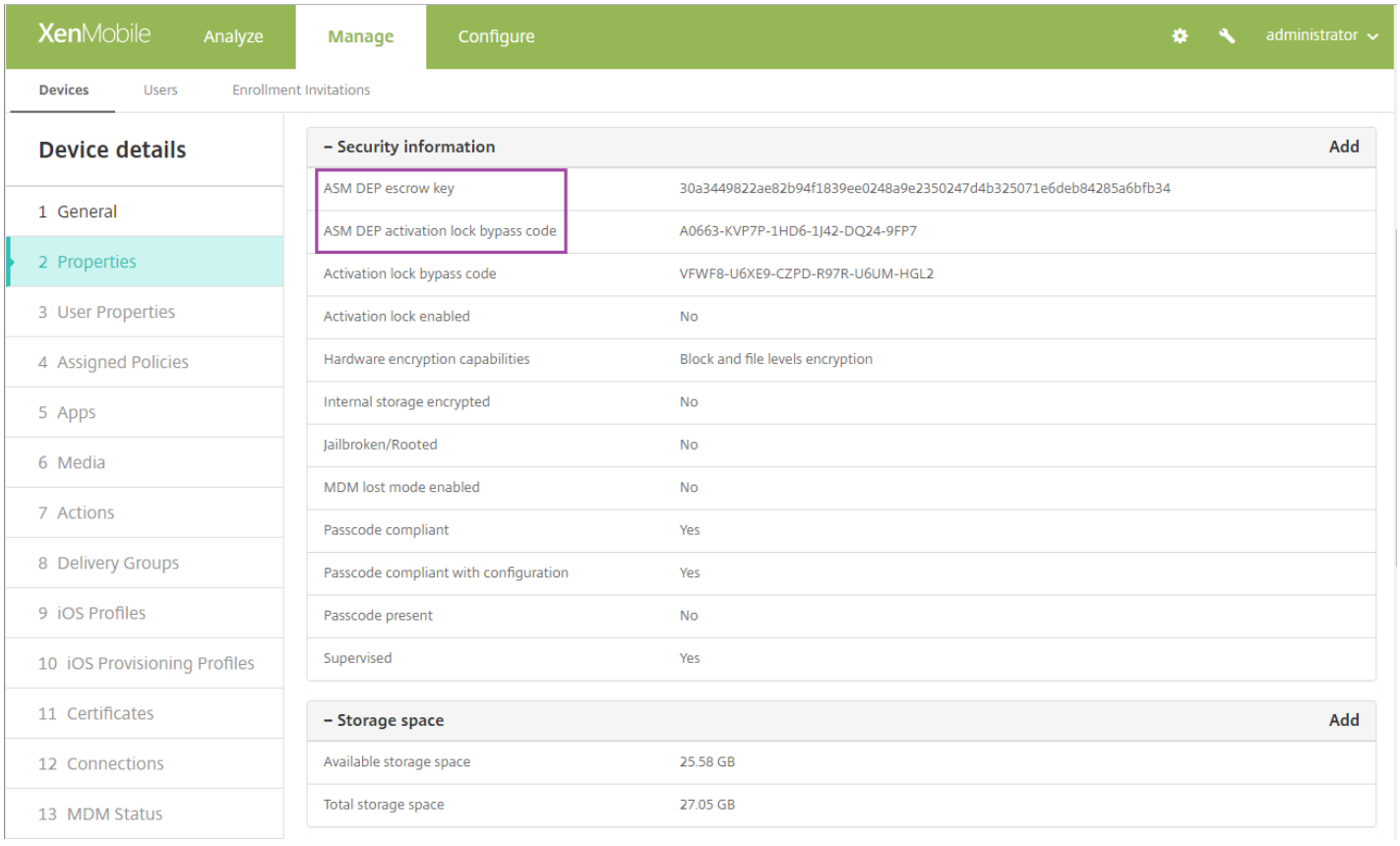
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

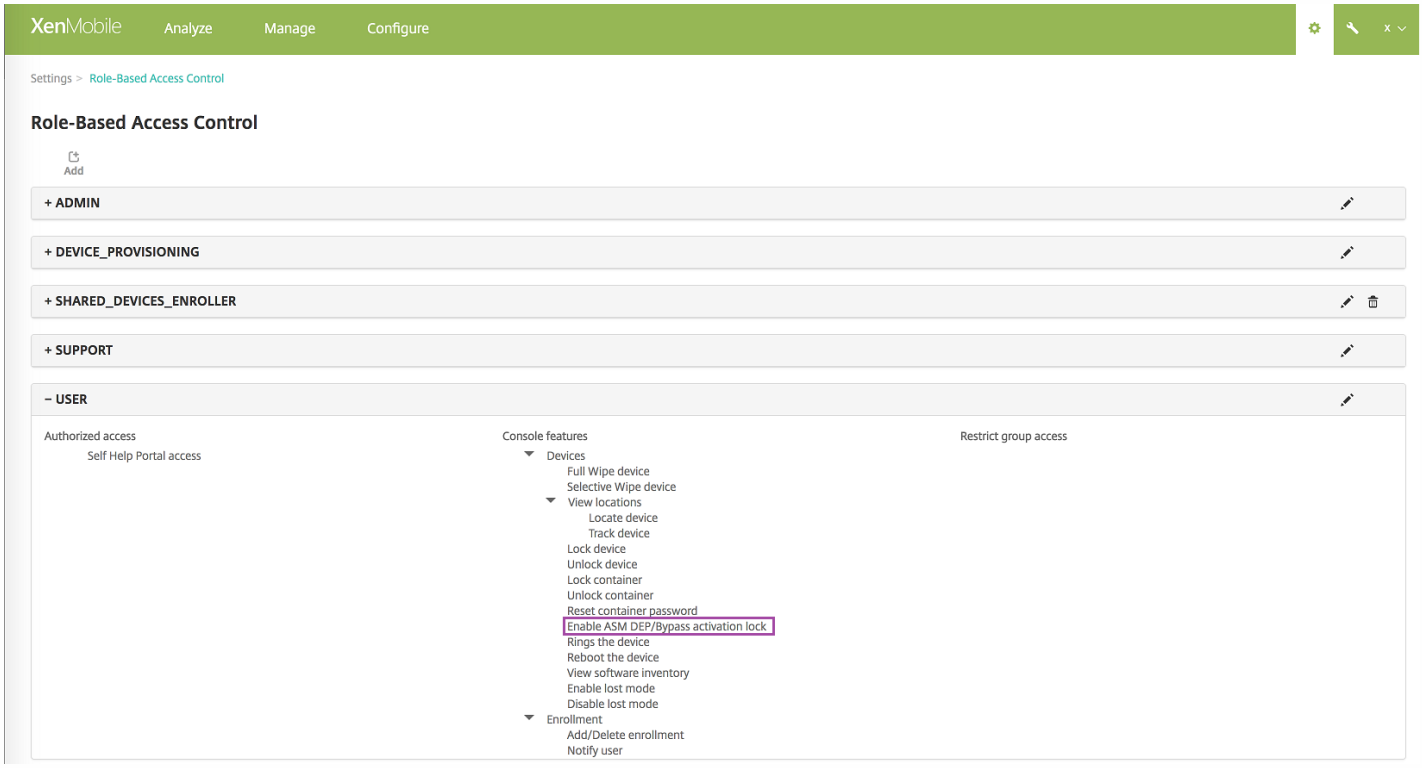
-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.



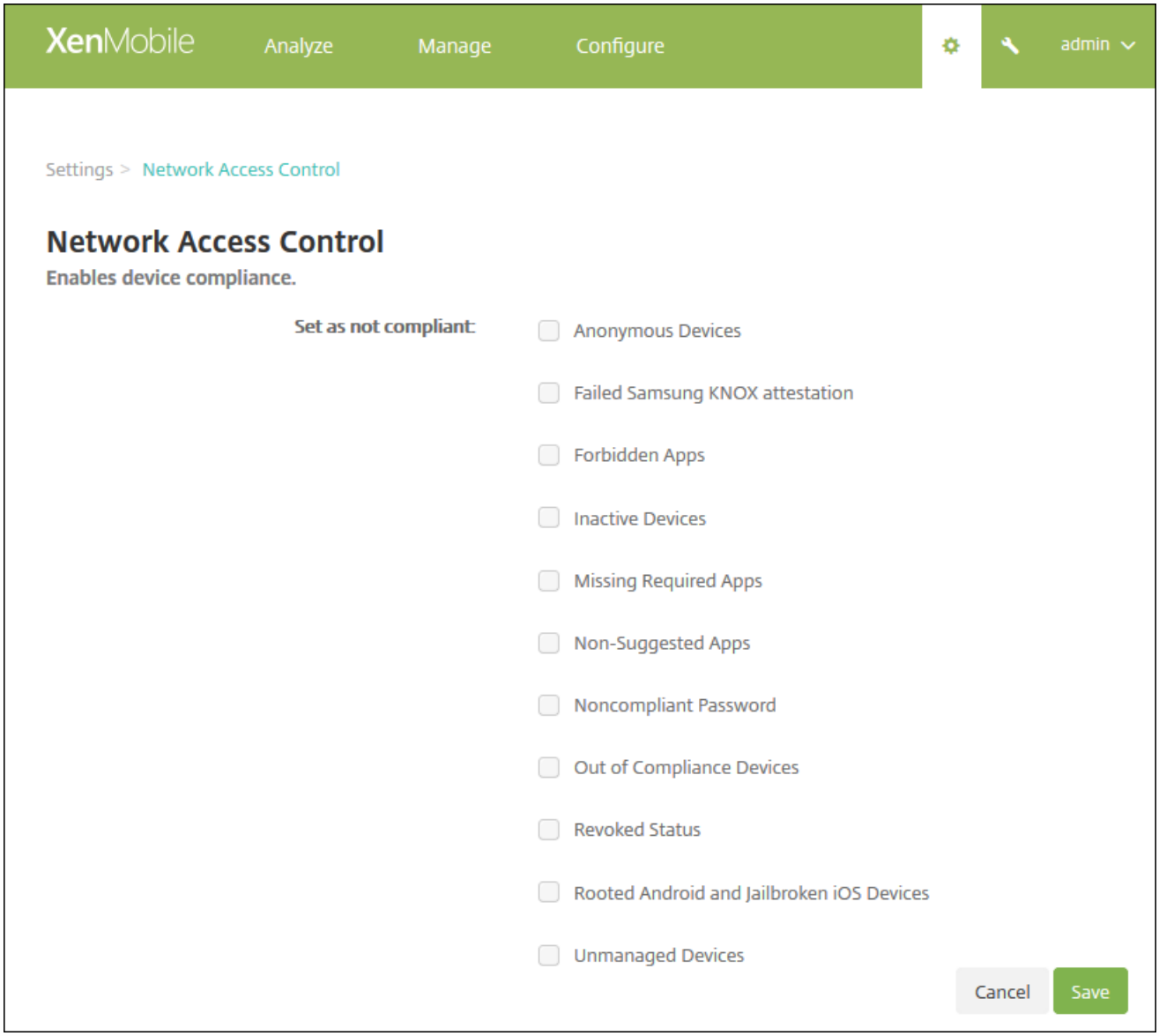


© 1999-2017 Citrix Systems, Inc. All rights reserved.



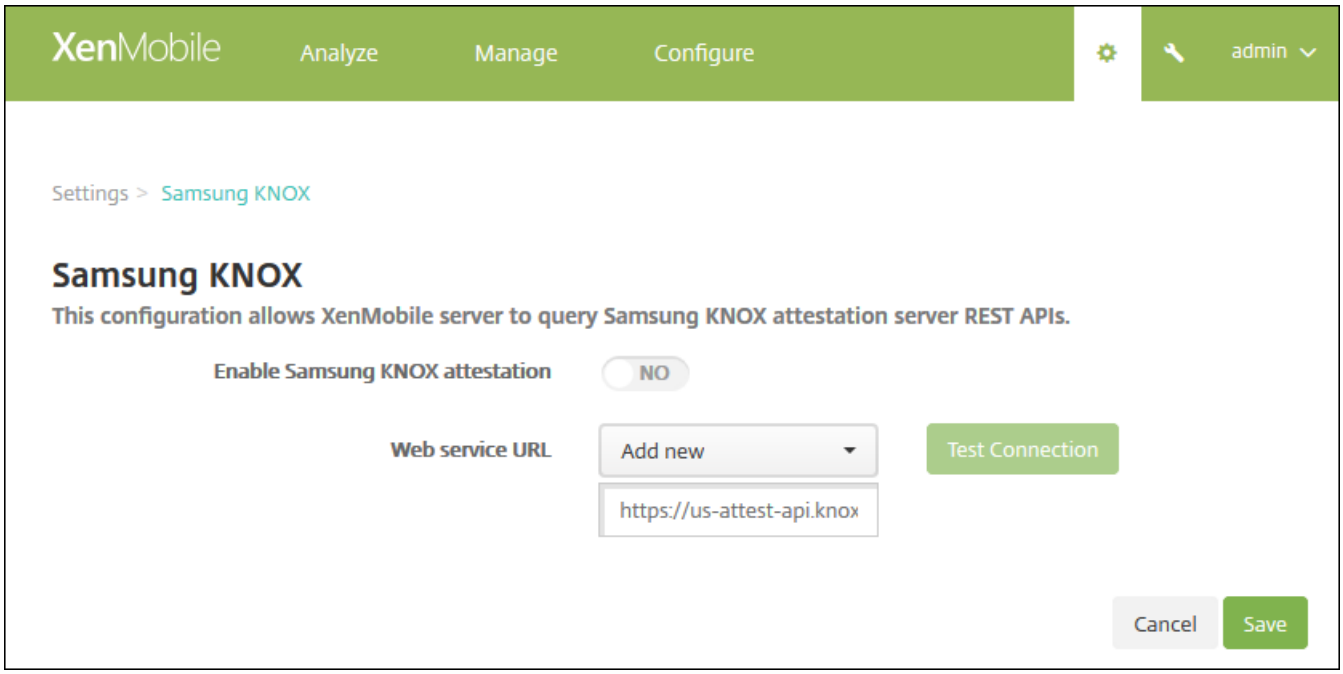
© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-
-
  -
  -
  -
  -
  -
  -
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-
-
-
-
-
-
  -
  -
  -
  -
  -
-

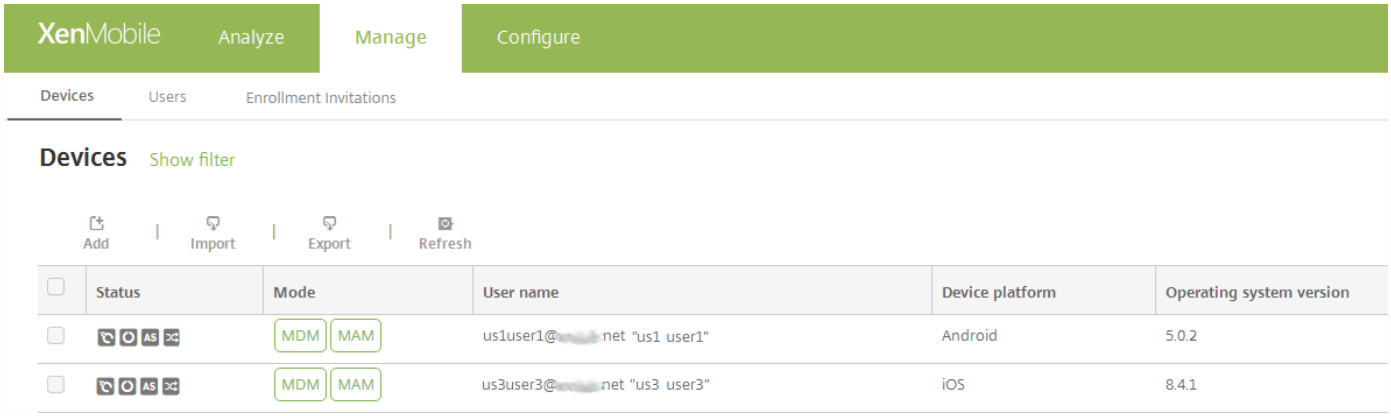
© 1999-2017 Citrix Systems, Inc. All rights reserved.

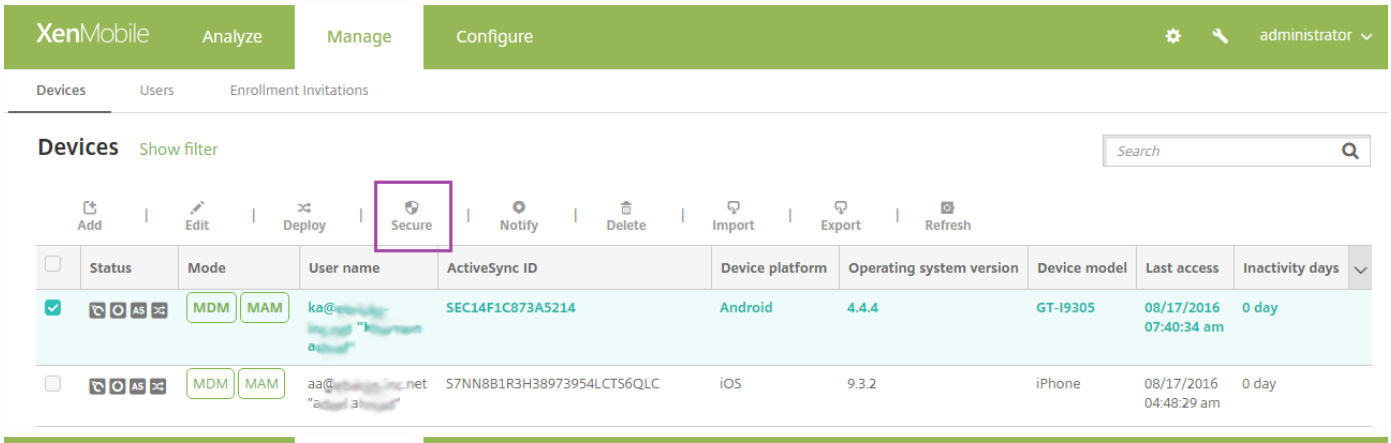
-
-
-
-
-
-
-
-
-
-

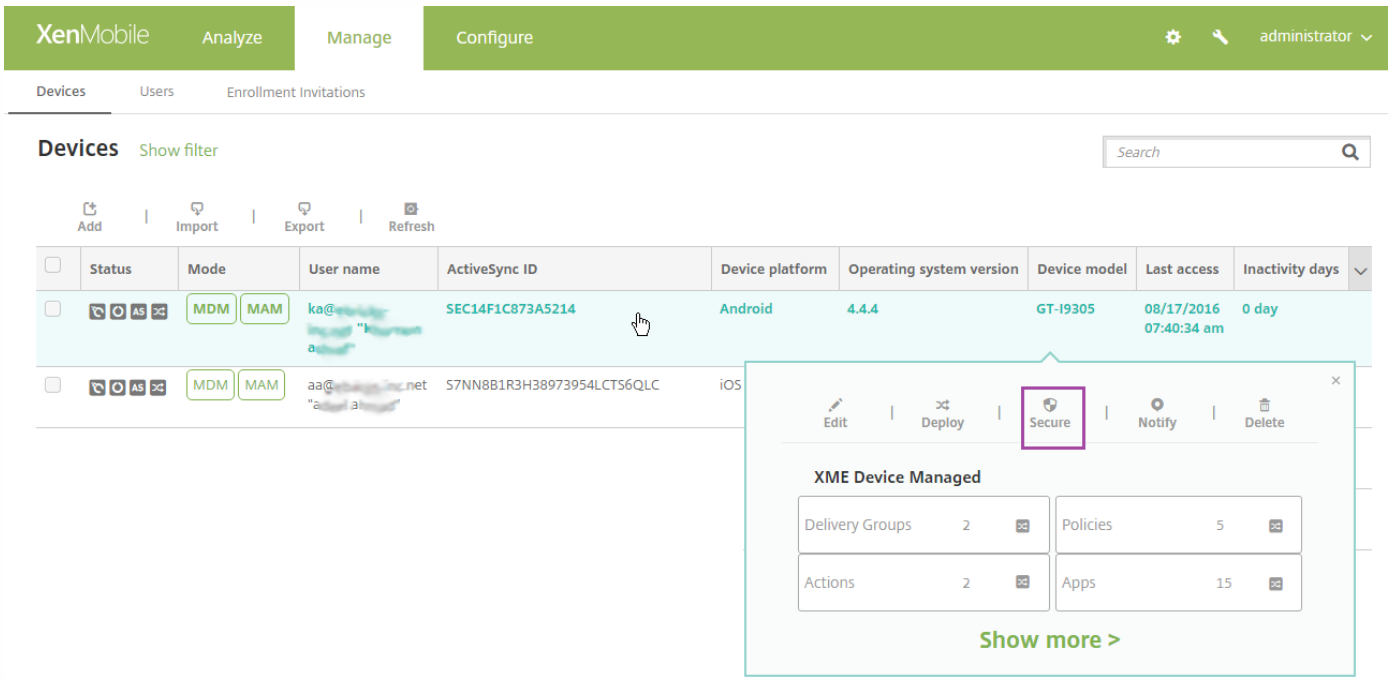
© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

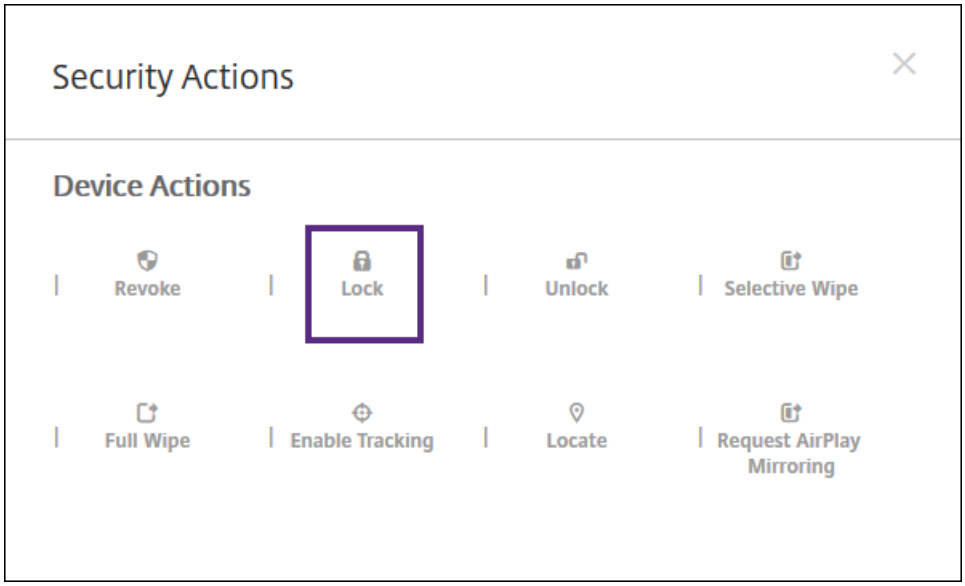
© 1999-2017 Citrix Systems, Inc. All rights reserved.

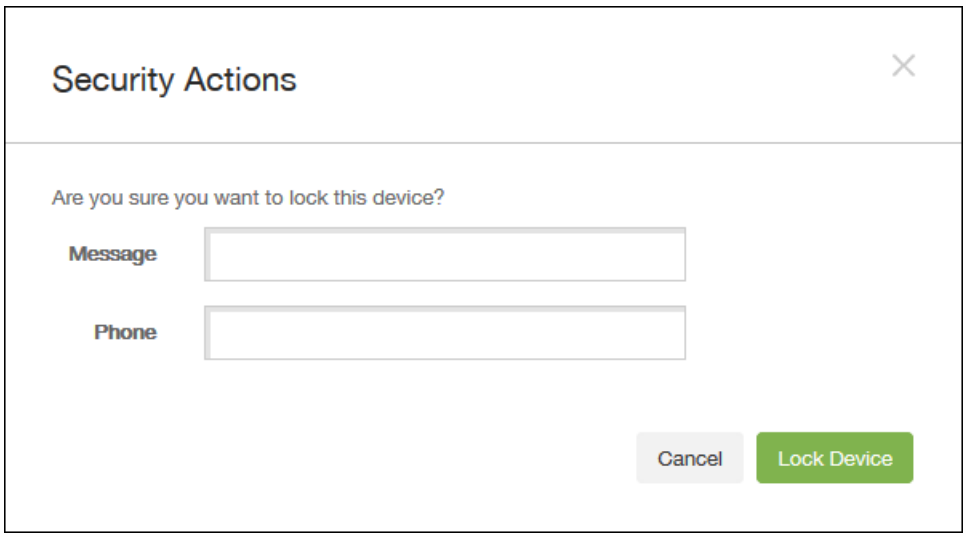




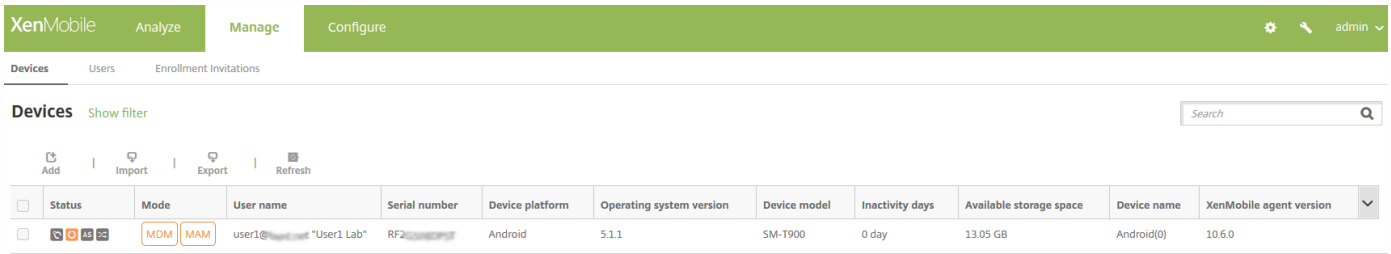


© 1999-2017 Citrix Systems, Inc. All rights reserved.

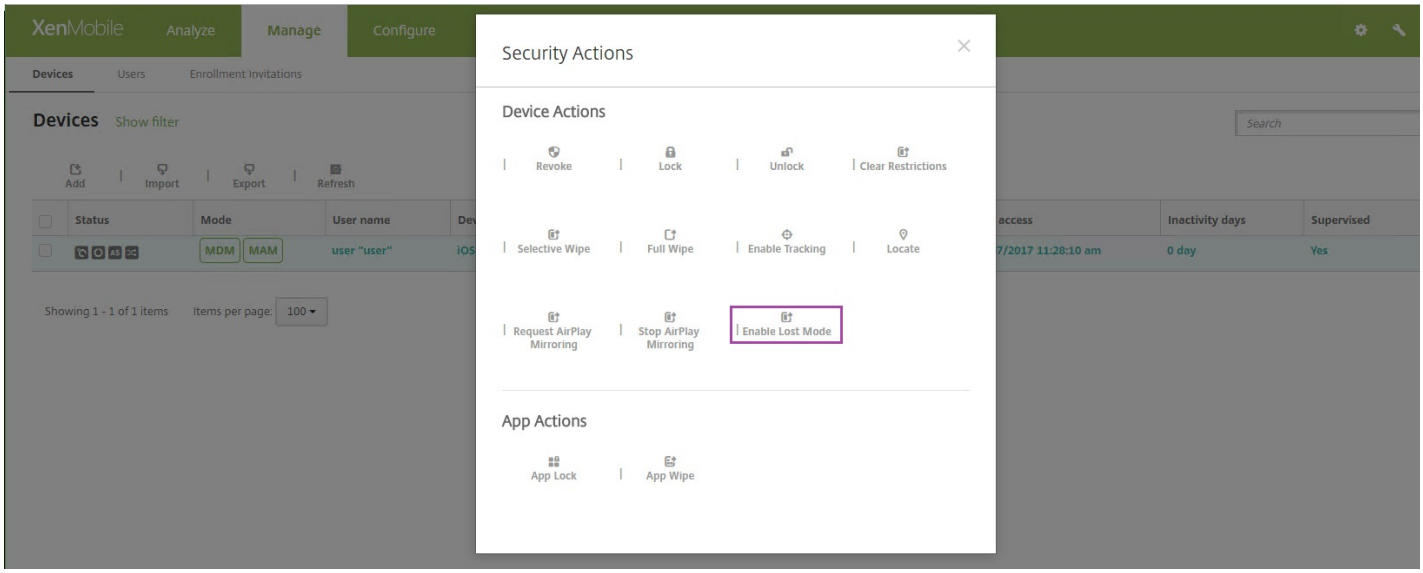




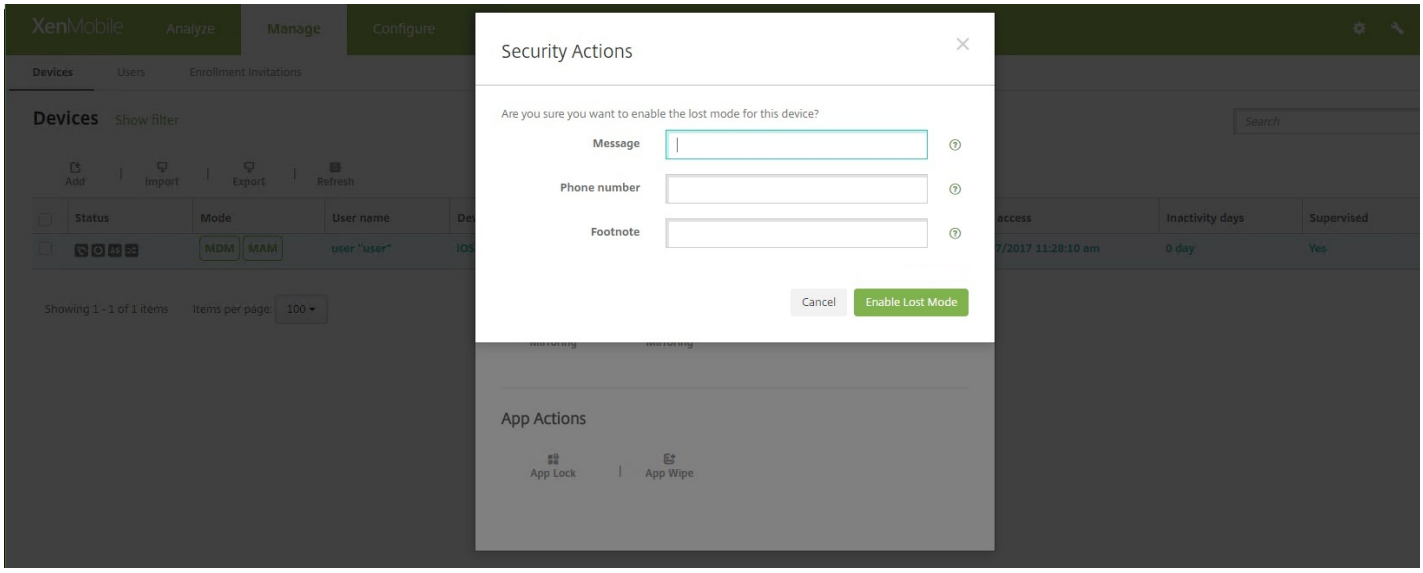
© 1999-2017 Citrix Systems, Inc. All rights reserved.



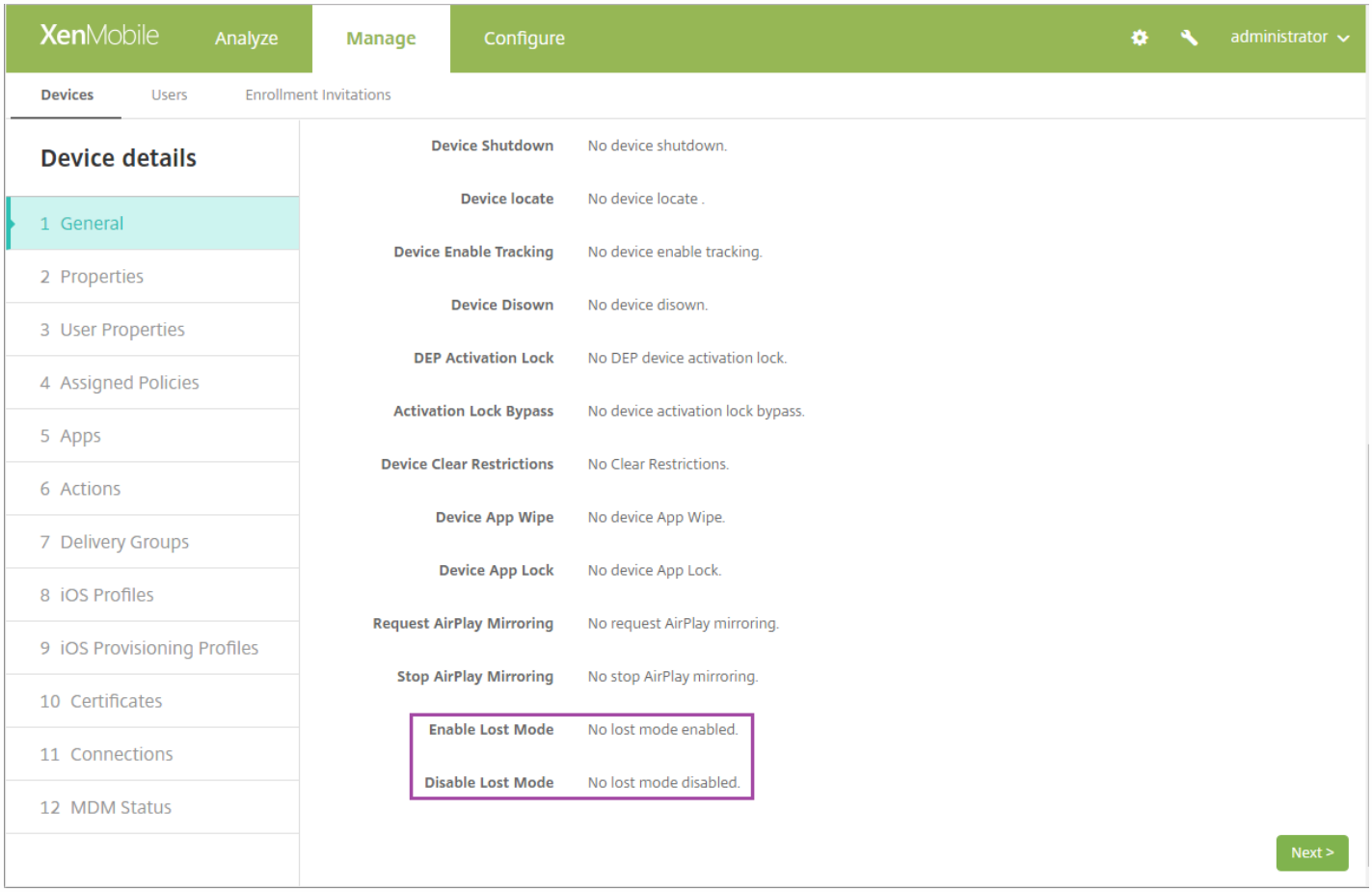
© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

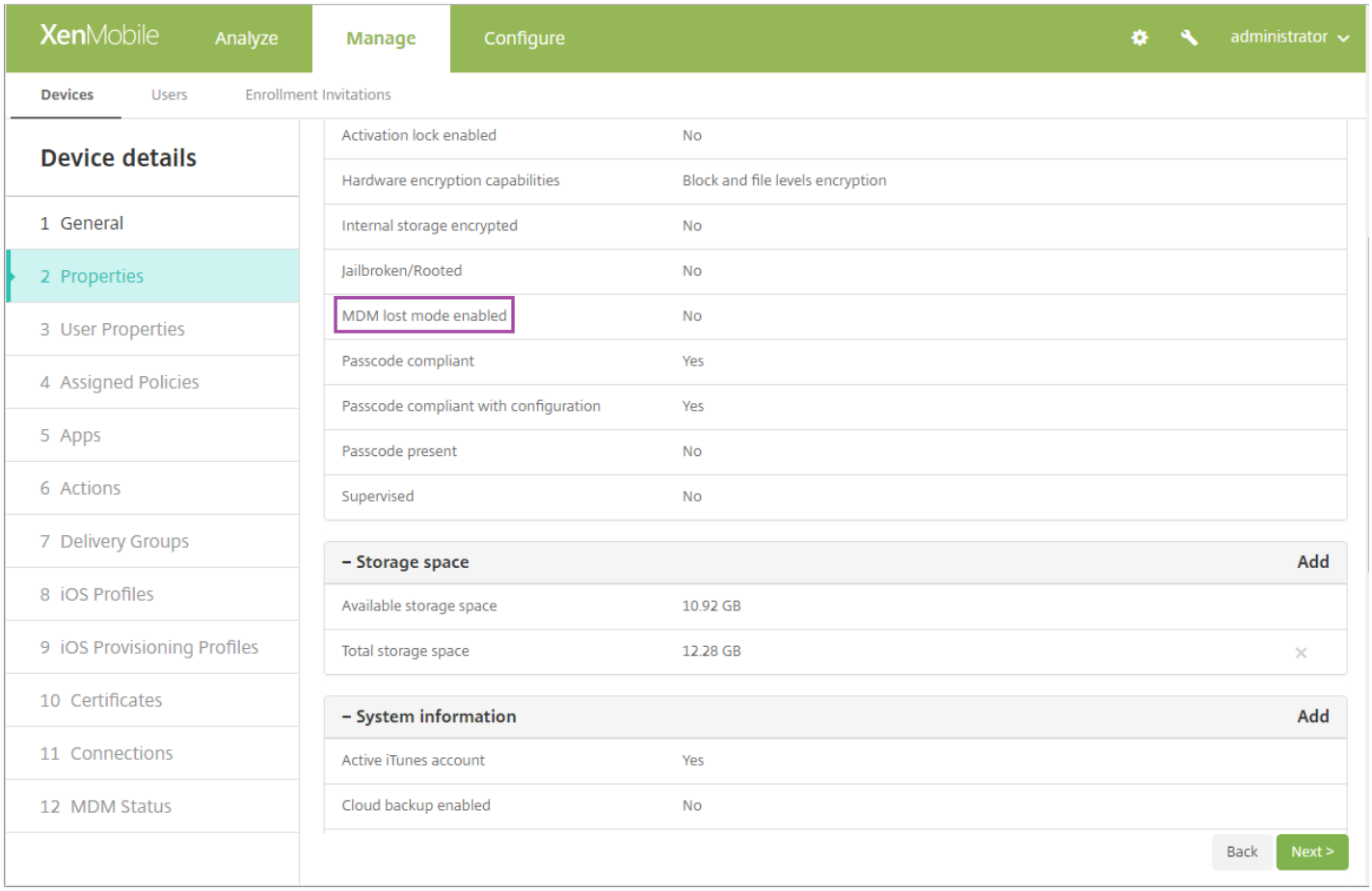


-
-



-

© 1999-2017 Citrix Systems, Inc. All rights reserved.



-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-

-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-
-

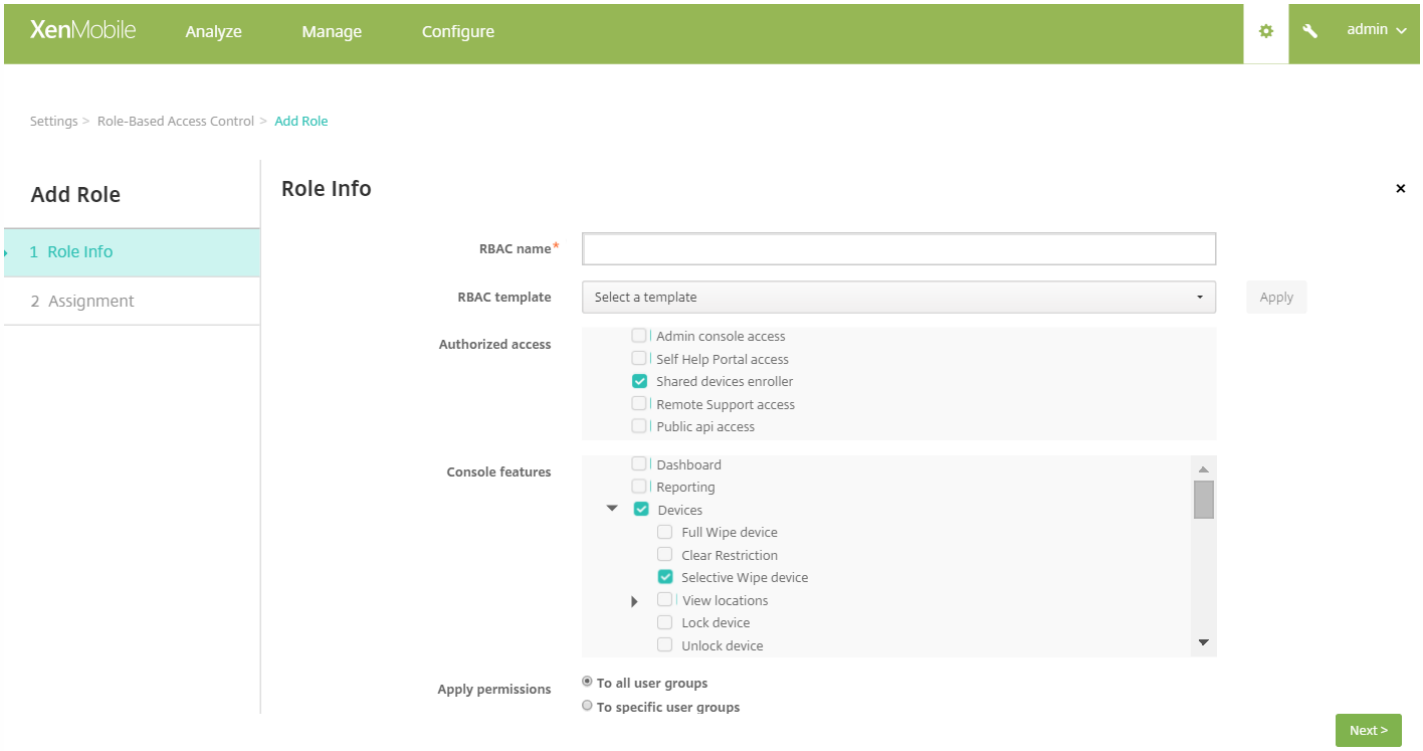
© 1999-2017 Citrix Systems, Inc. All rights reserved.

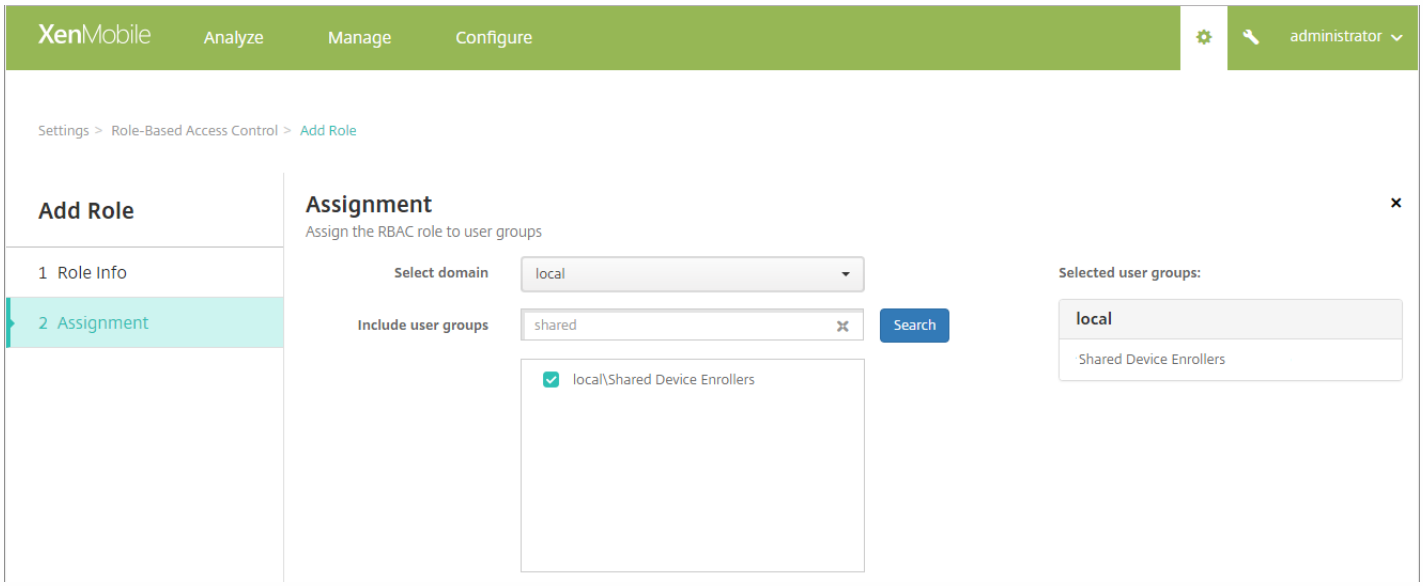
-
-
-

Pré-requisitos do modo MDM+MAM

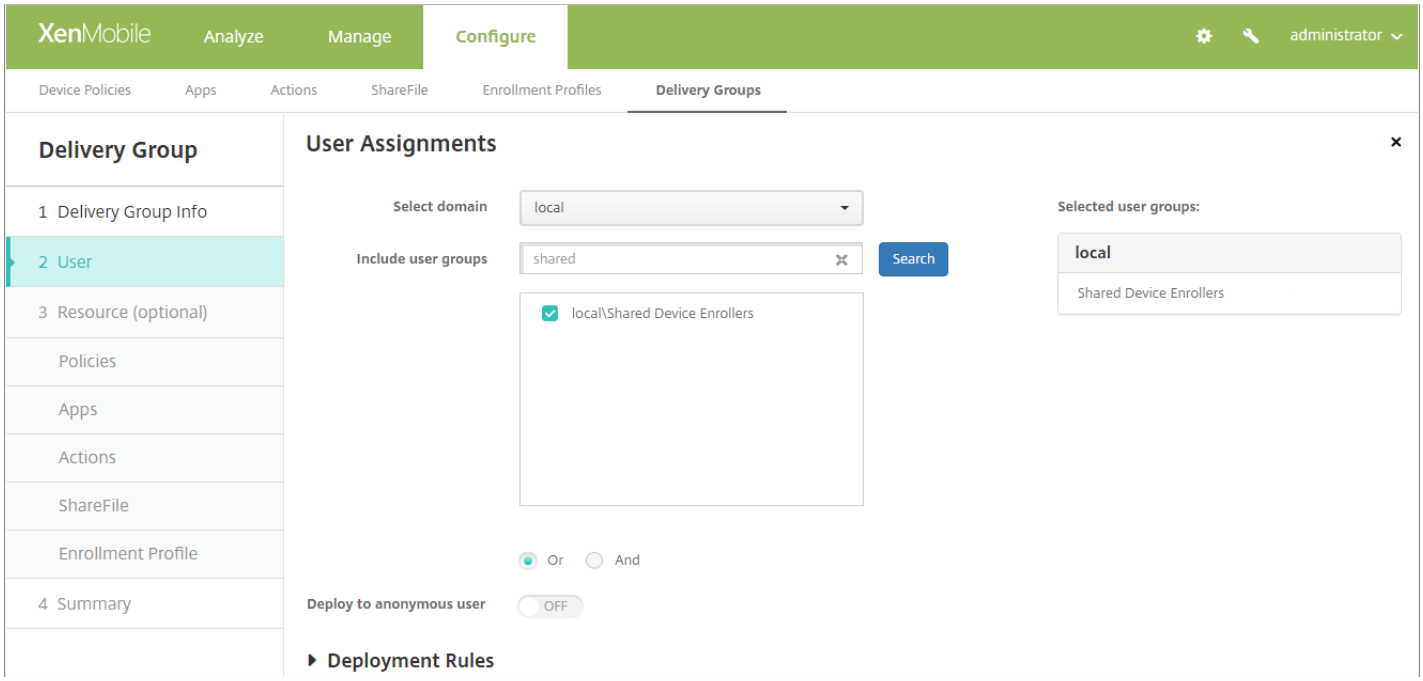
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.





© 1999-2017 Citrix Systems, Inc. All rights reserved.



Modo MDM

Modo MDM+MAM

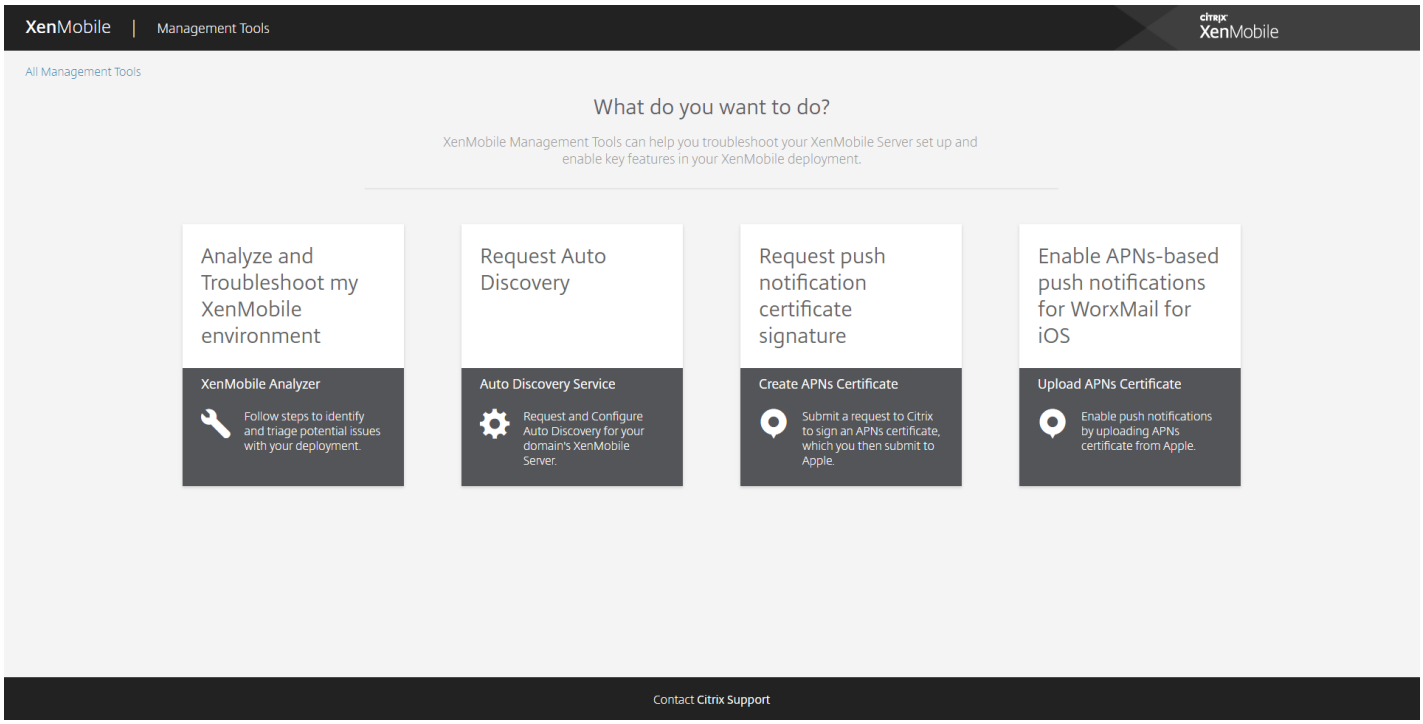
© 1999-2017 Citrix Systems, Inc. All rights reserved.

-

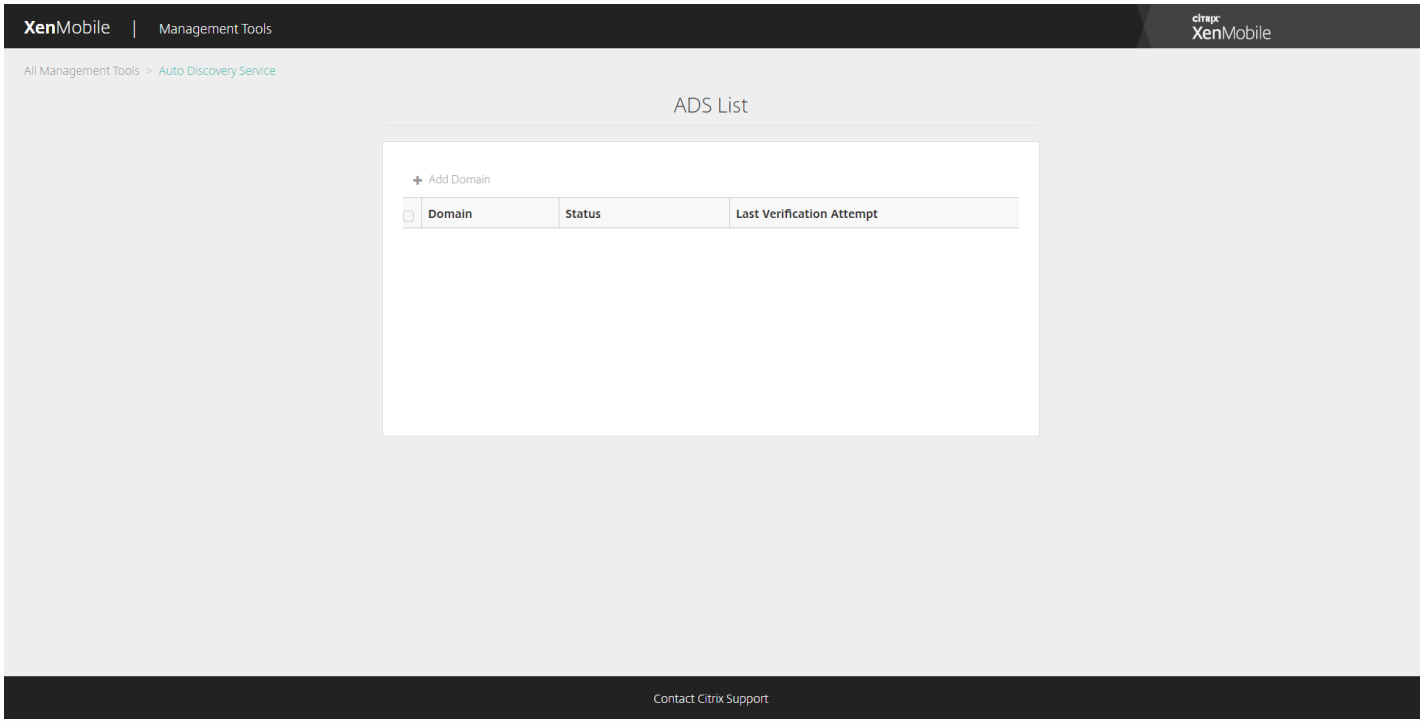
-

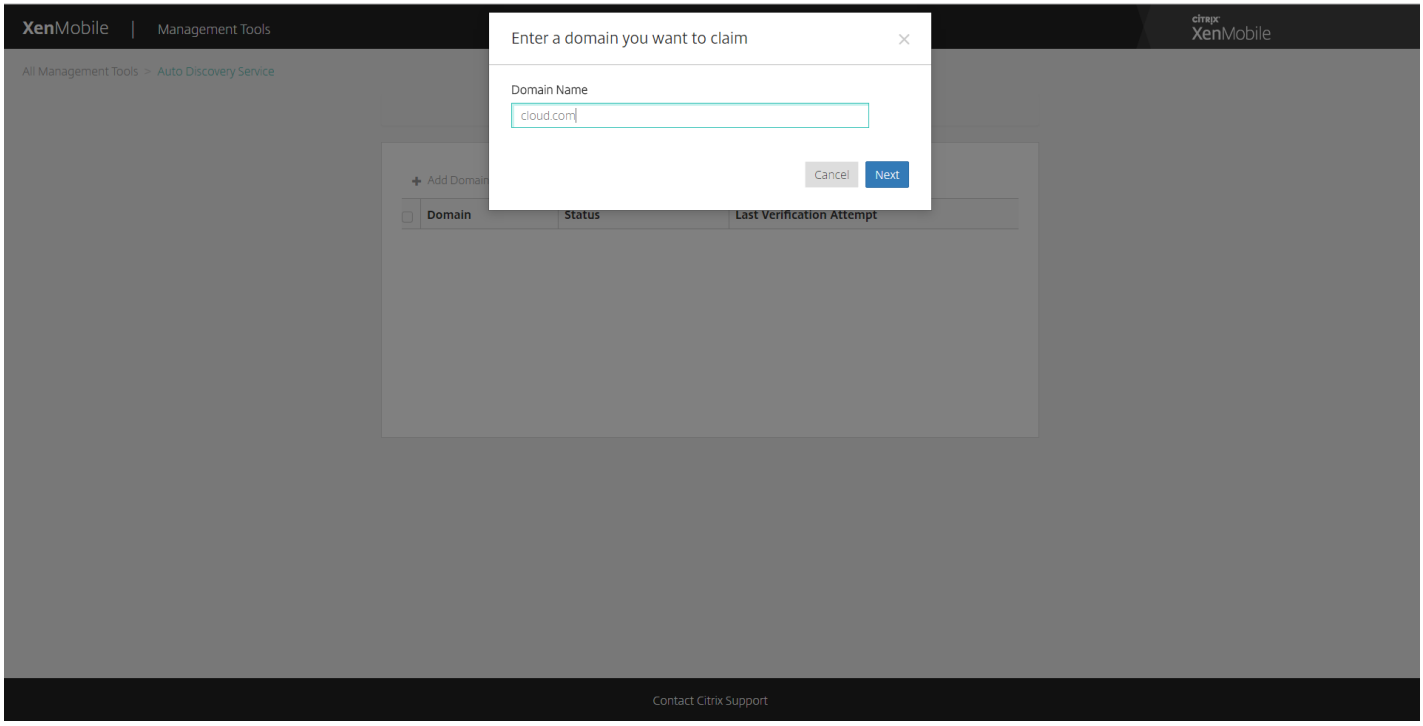
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

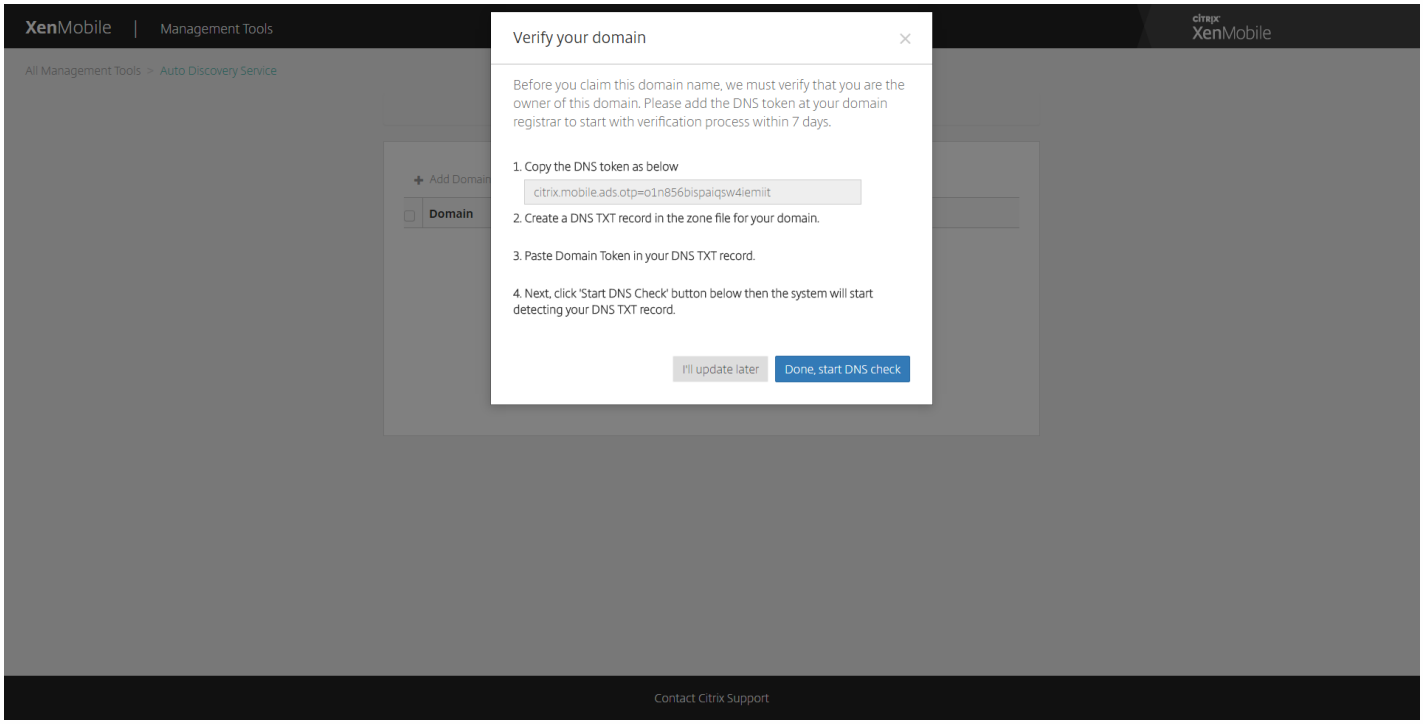


© 1999-2017 Citrix Systems, Inc. All rights reserved.

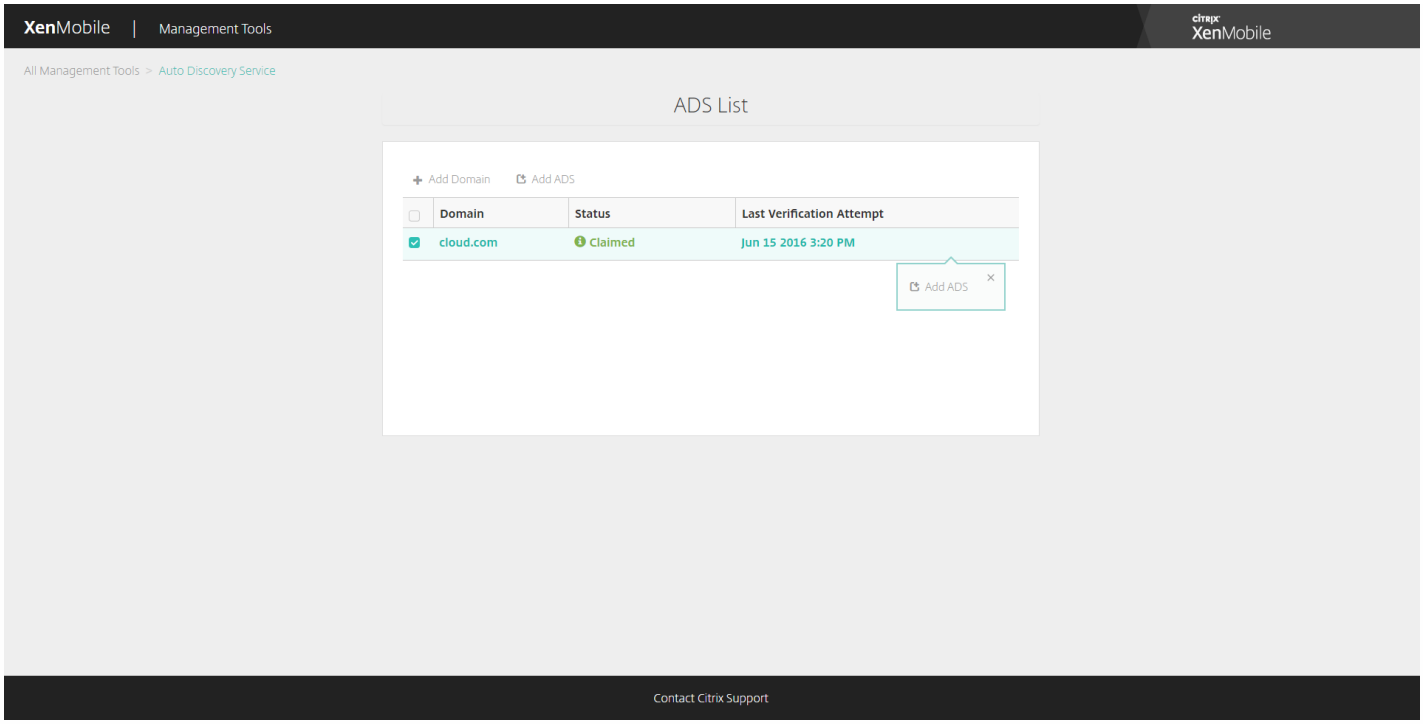


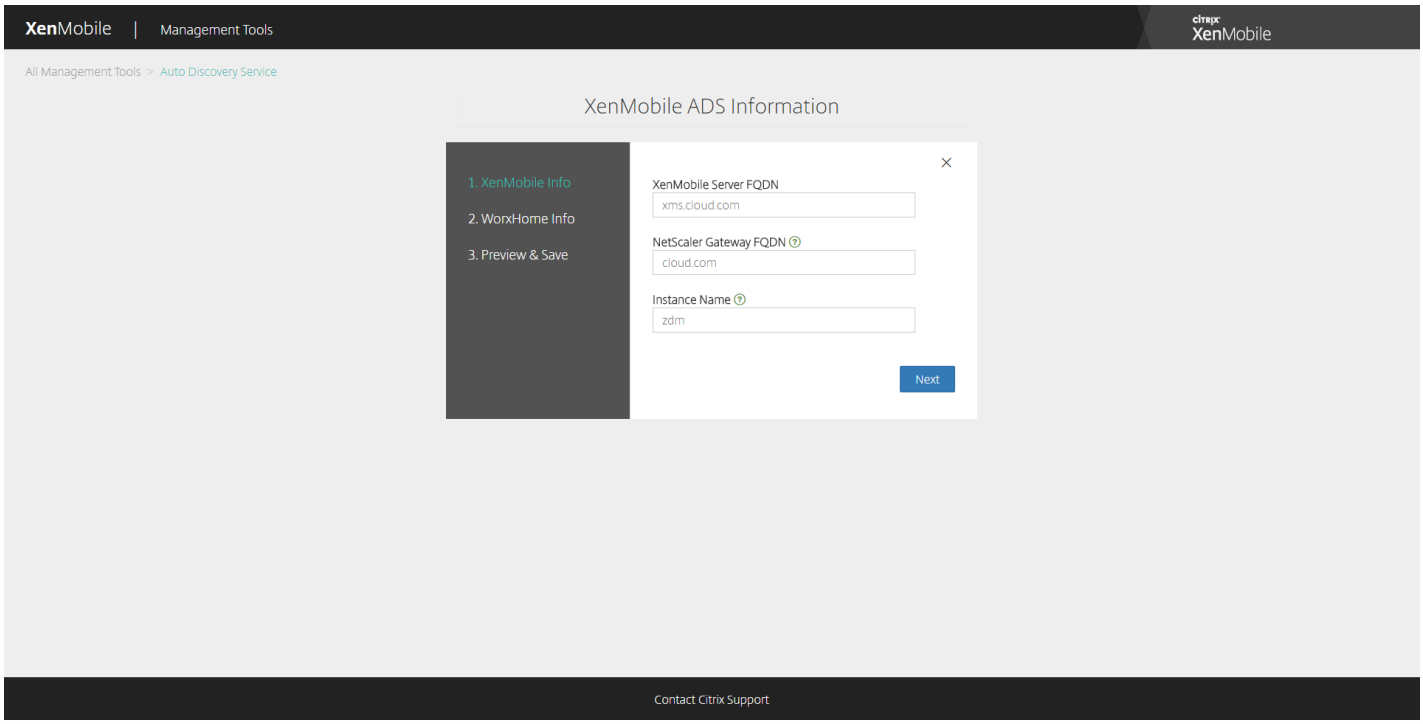


© 1999-2017 Citrix Systems, Inc. All rights reserved.

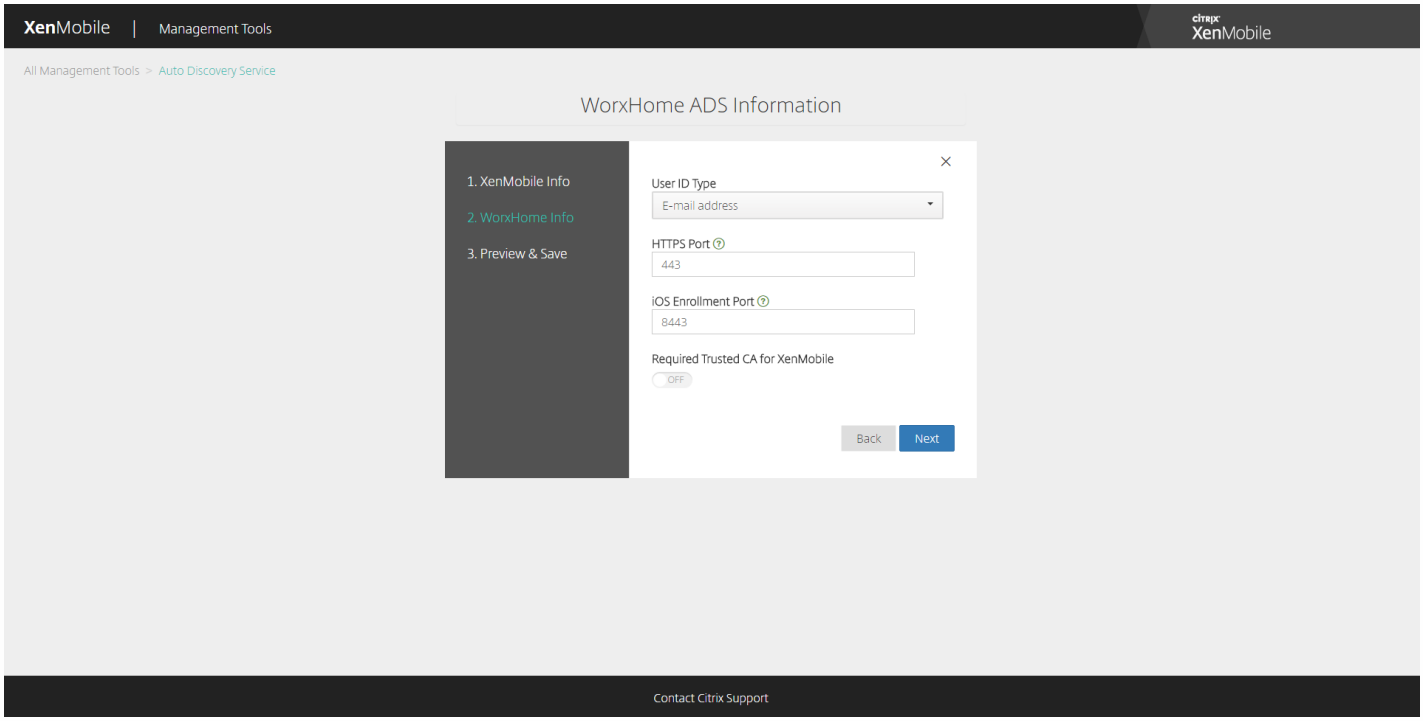


© 1999-2017 Citrix Systems, Inc. All rights reserved.

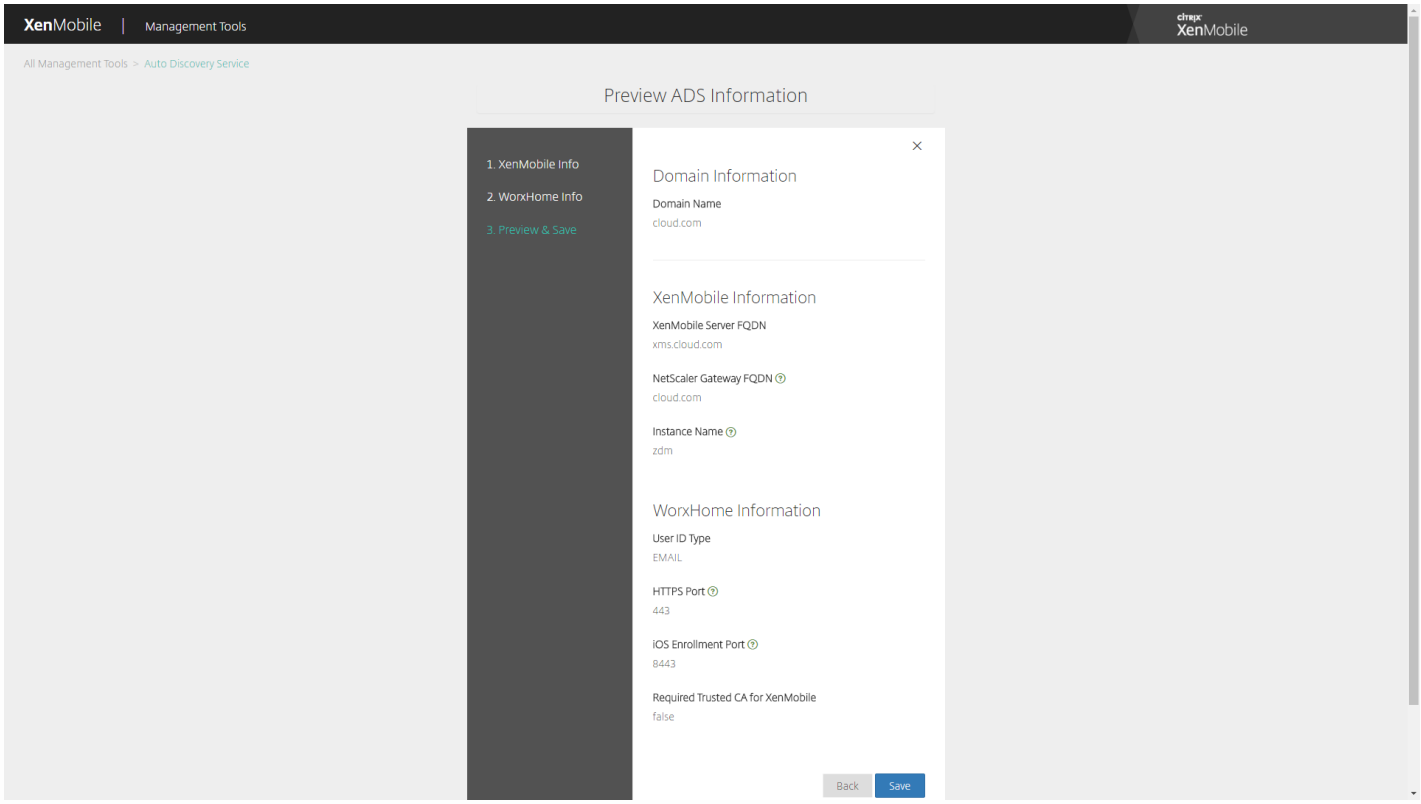




© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.



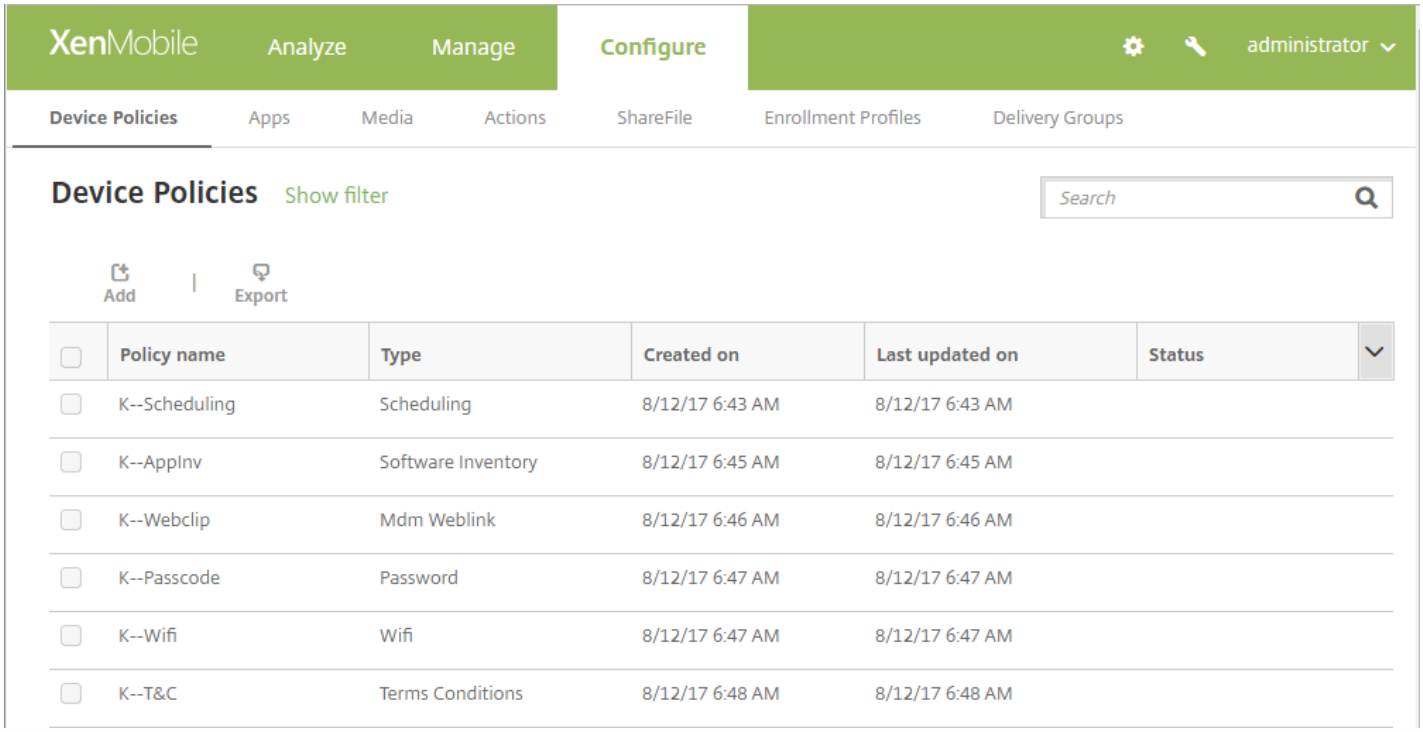
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

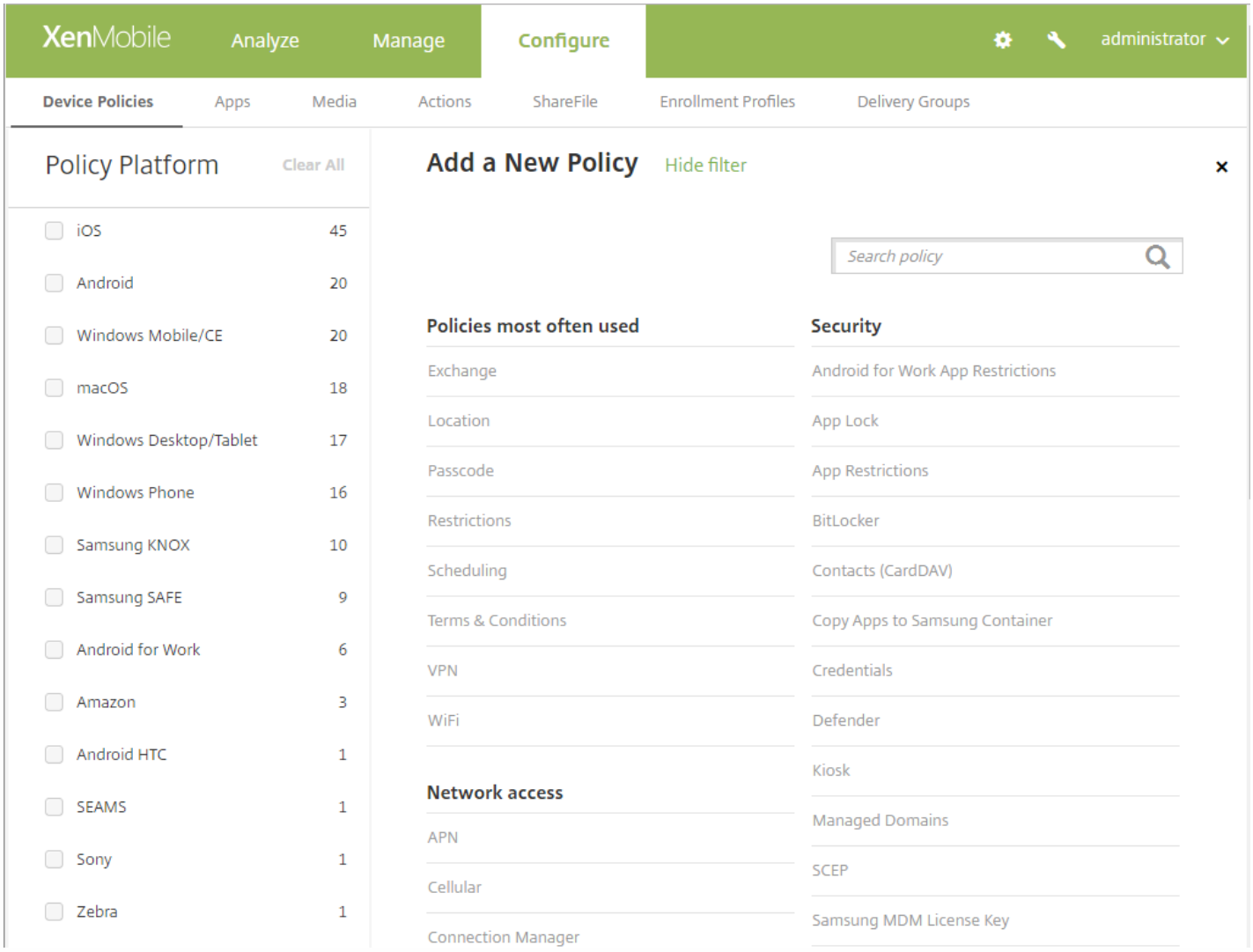
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

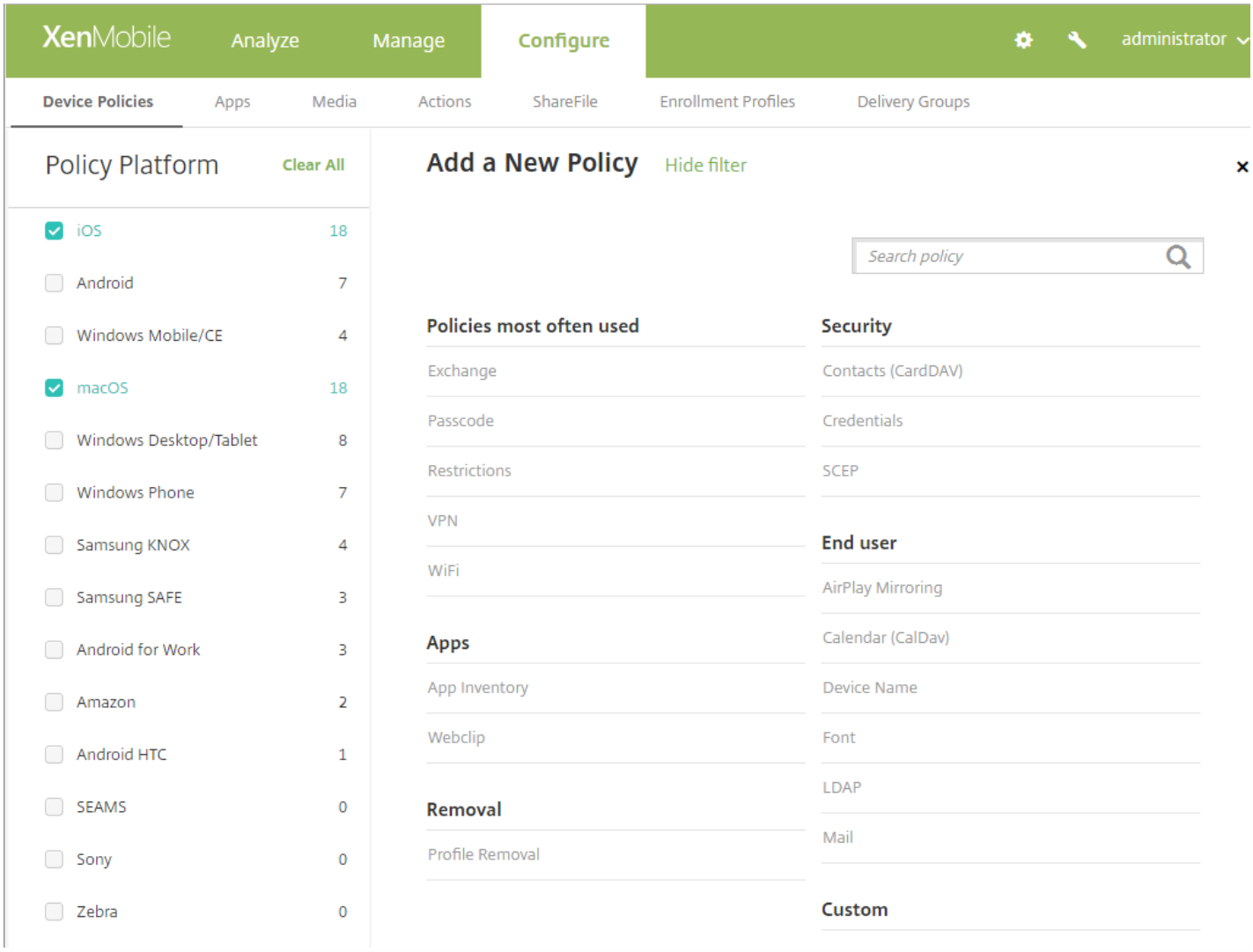
© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

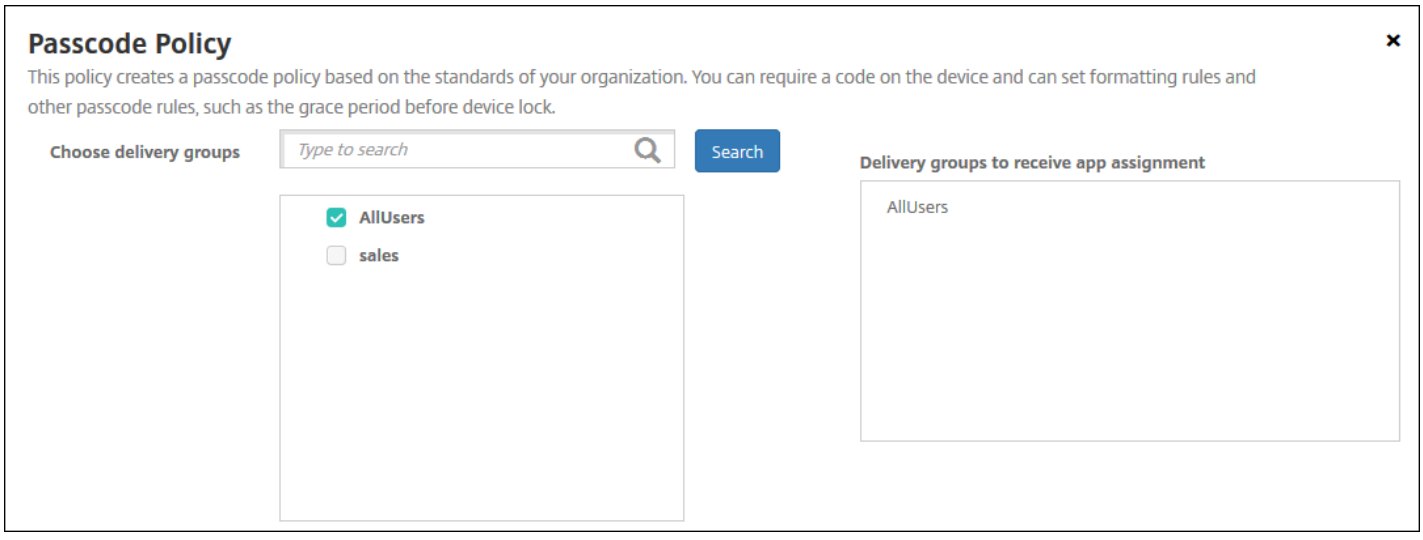


© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

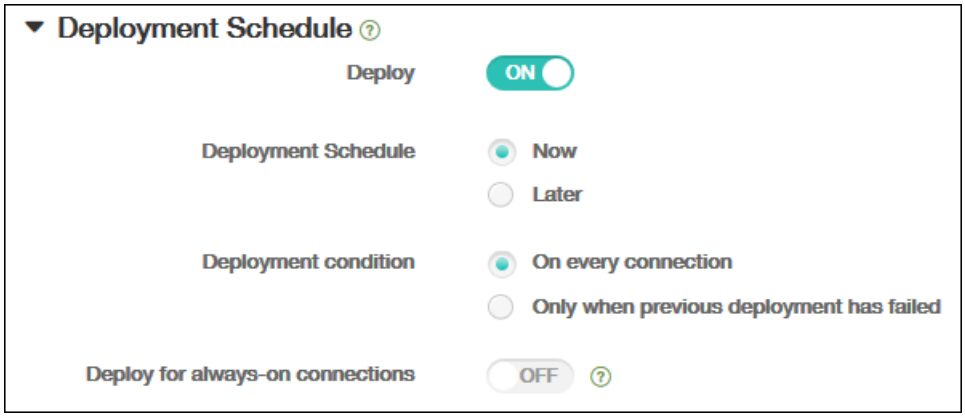
-
-
-
-
-
-
-

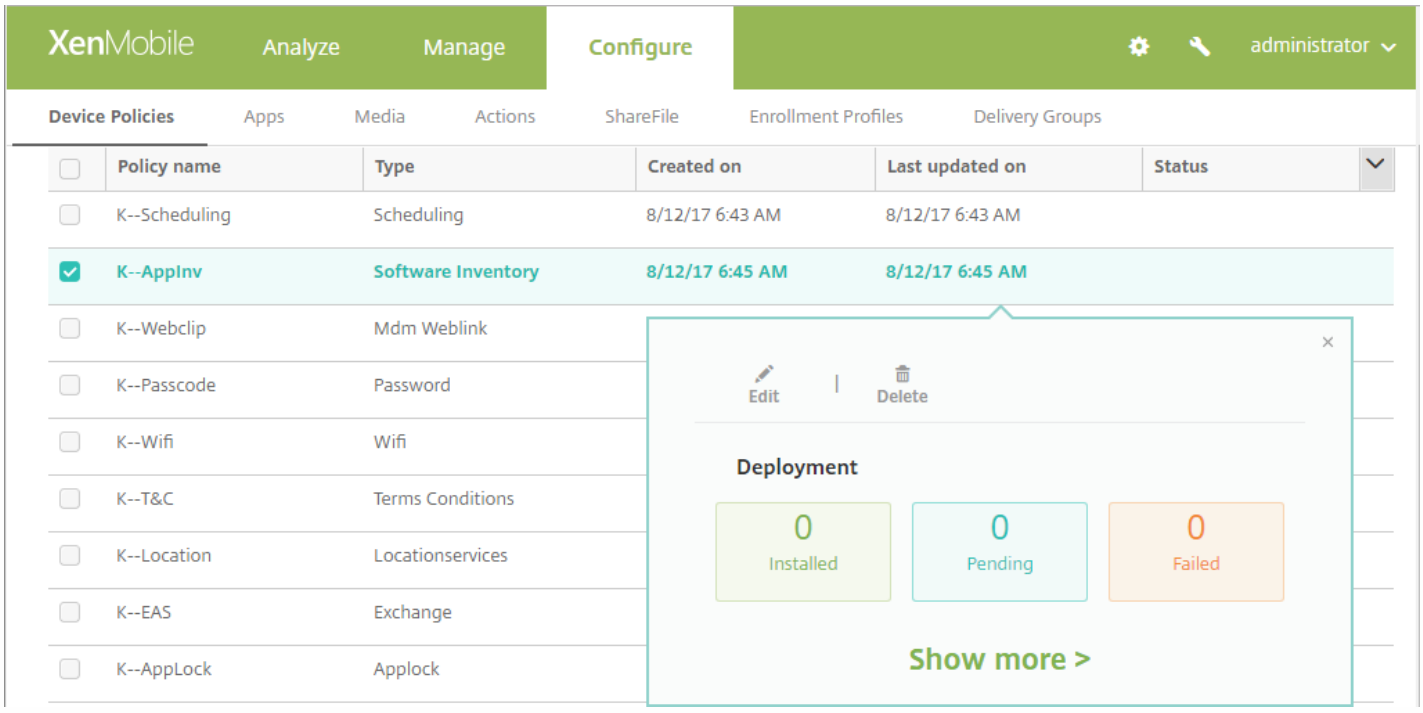


-
-
-
-

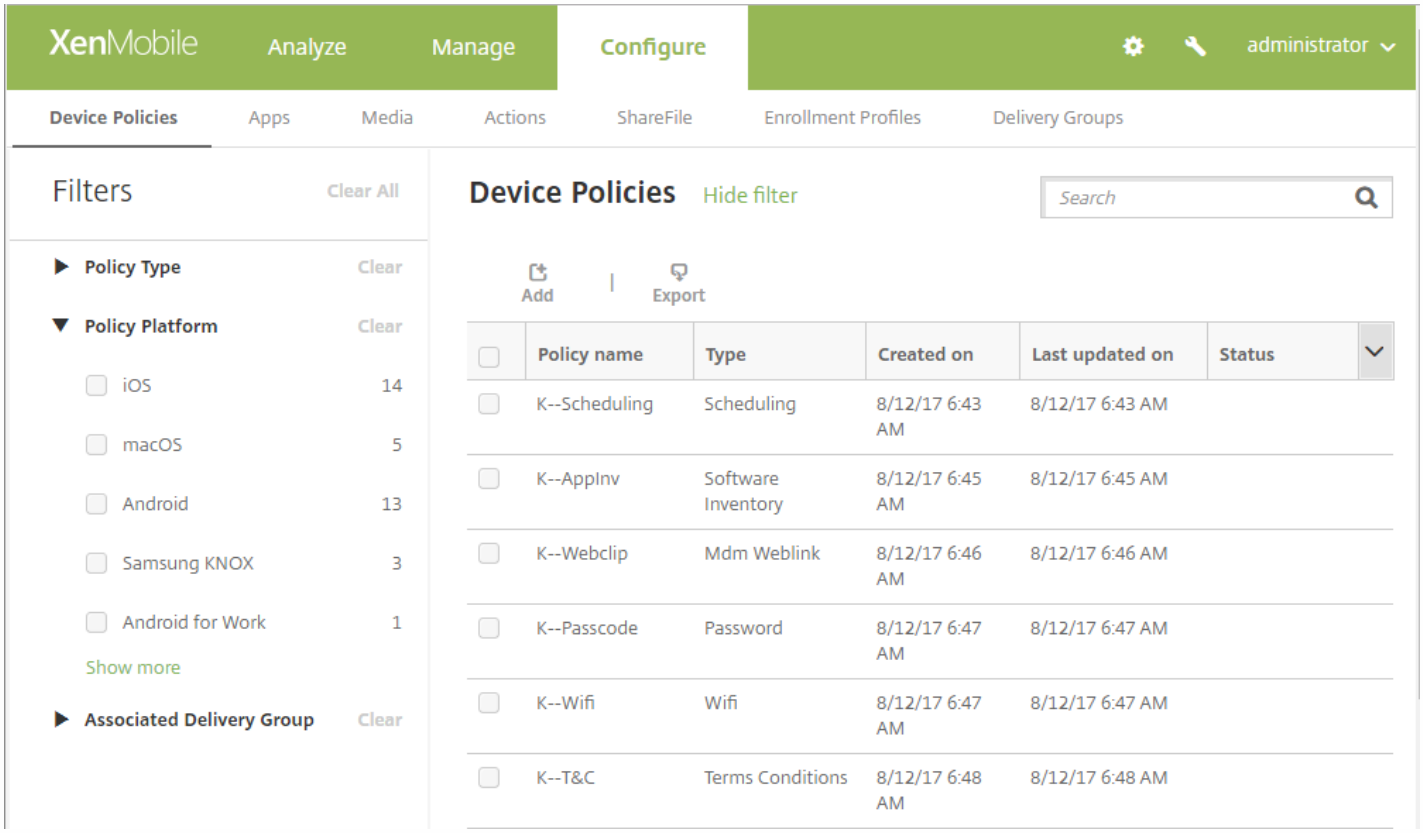
© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-





© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

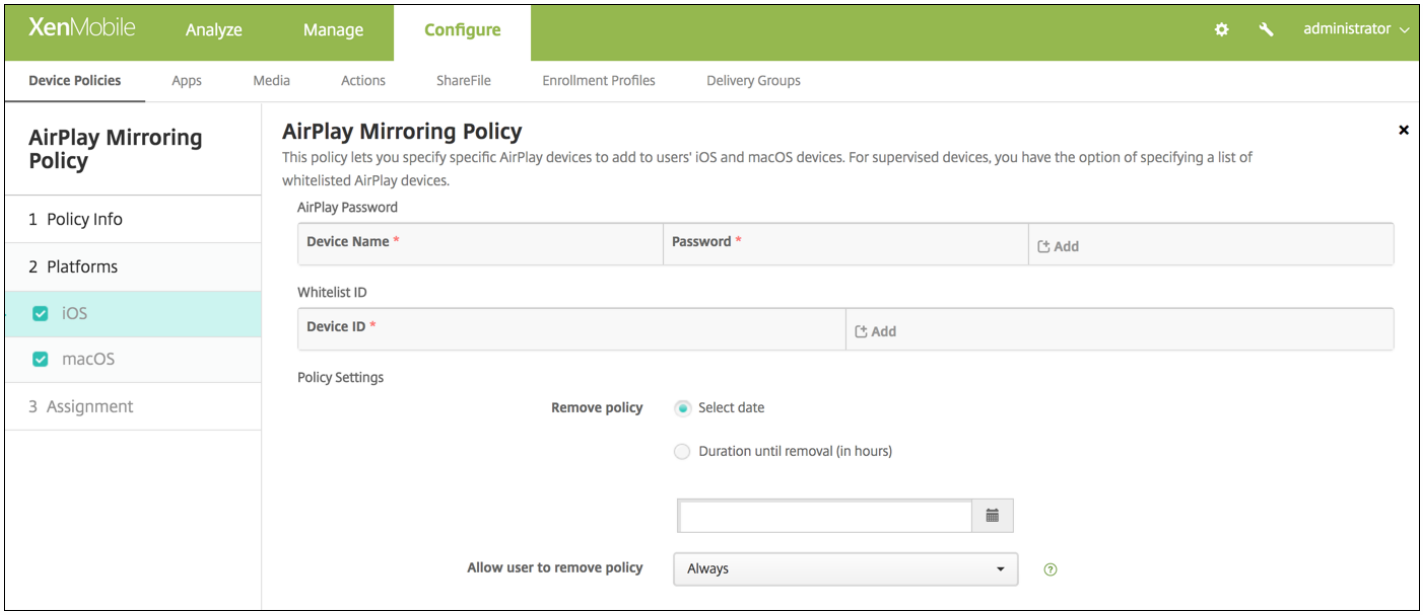
-
-
-
-
-
-
-
-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-

Definir as configurações do iOS

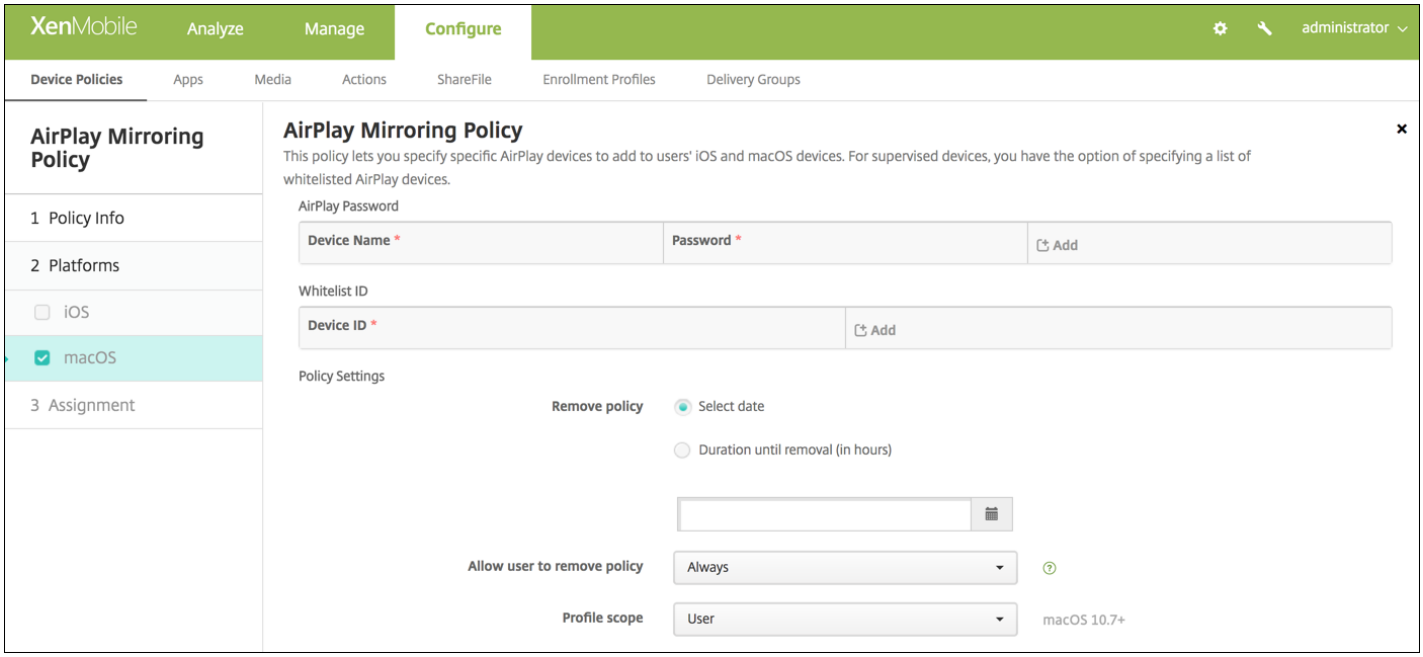
© 1999-2017 Citrix Systems, Inc. All rights reserved.



-
  -
  -
  -
-
  -
  -
-
  -
  -
  -
  -

Defina as configurações do macOS

© 1999-2017 Citrix Systems, Inc. All rights reserved.



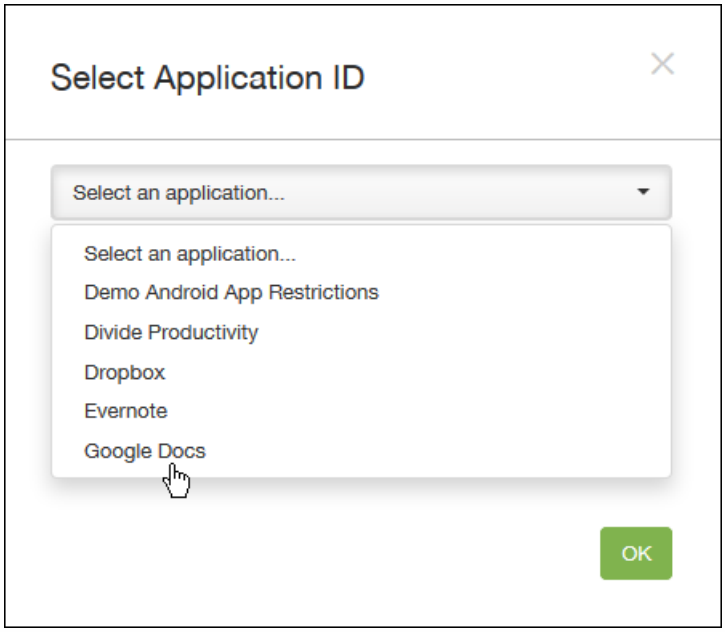
-
  -
  -
  -
-
  -
  -
-
  -
  -
  -
  -
  -

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
  -
  -
  -
-
  -
  -
  -
  -
  -
  -

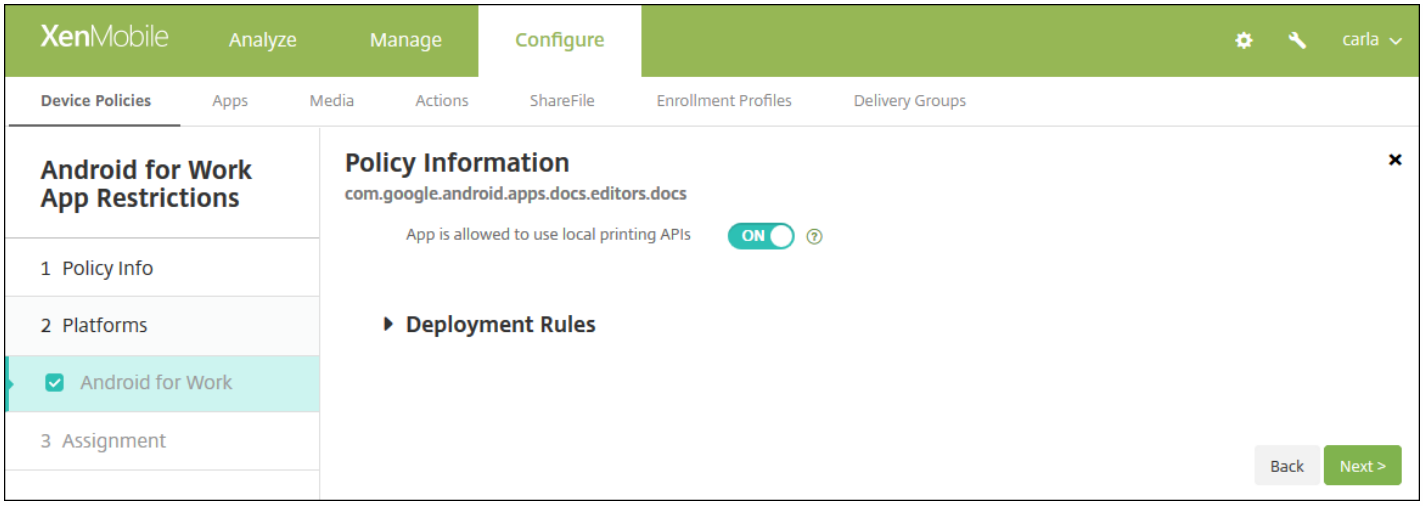
© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-

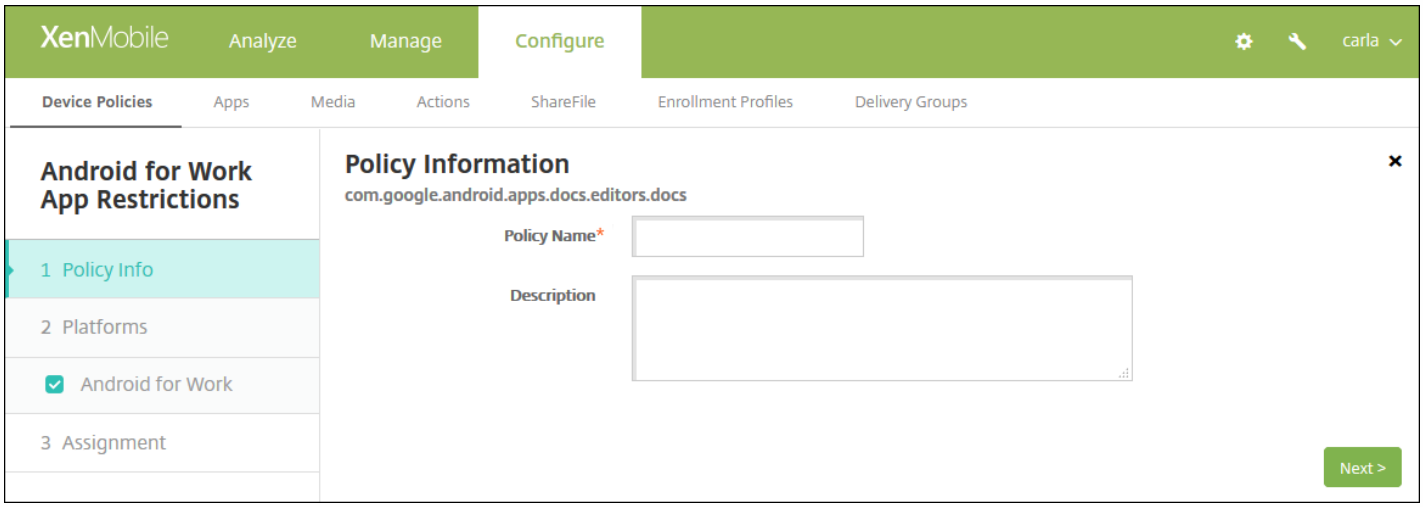


-
-
-

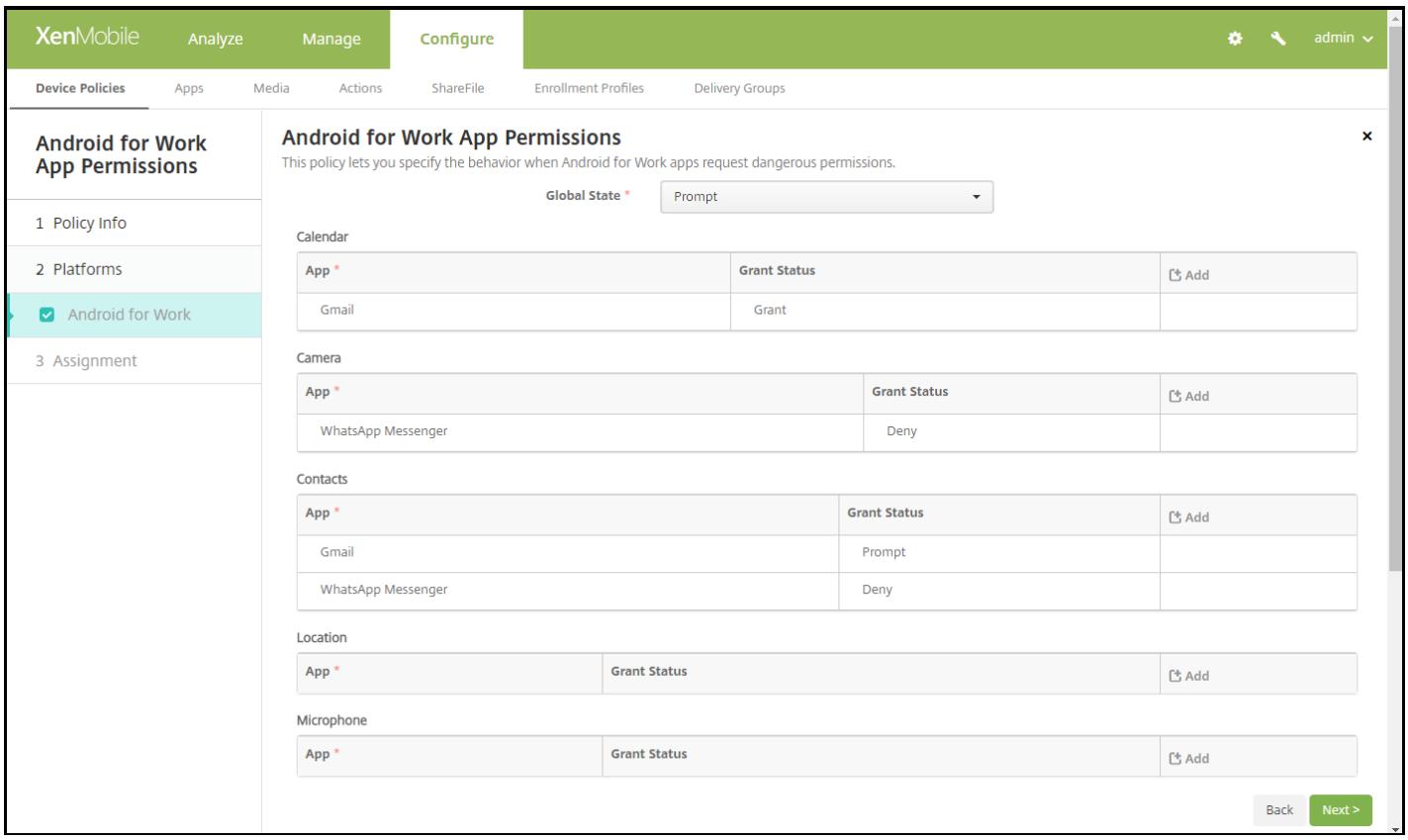
© 1999-2017 Citrix Systems, Inc. All rights reserved.



-
-



© 1999-2017 Citrix Systems, Inc. All rights reserved.



-
  -

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-
-
-
-
-
-
-
-
-
-
-
-
-

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo do APN

Feb 21, 2018

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.

Configurações do iOS

Configurações do Android

Configurações do Windows Mobile/CE

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Clique em **Mais** e, em **Acesso à rede**, clique em **APN**. A página de informações **Política de APN** é exibida.

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.

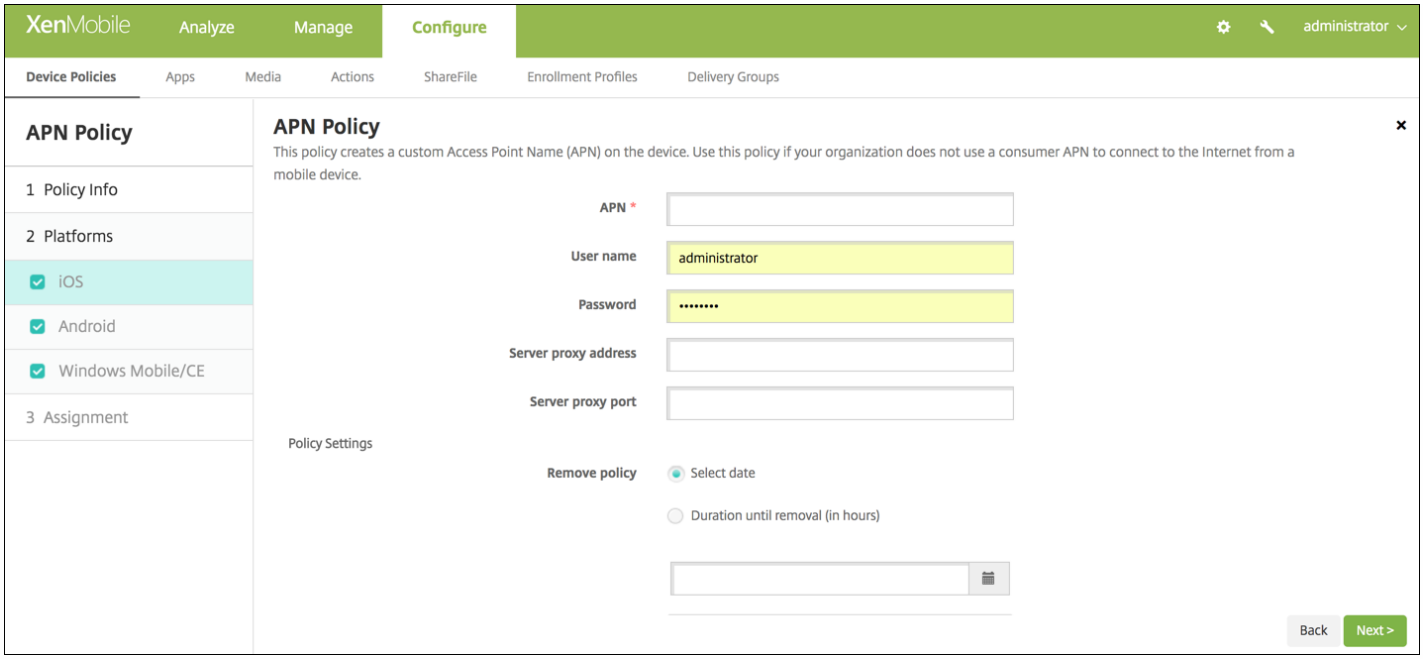
5. Clique em **Avançar**. A página **Plataforma de política** é exibida.

Nota: quando a página **Plataforma de política** é exibida, todas as plataformas estão selecionadas e você vê a plataforma iOS primeiro.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

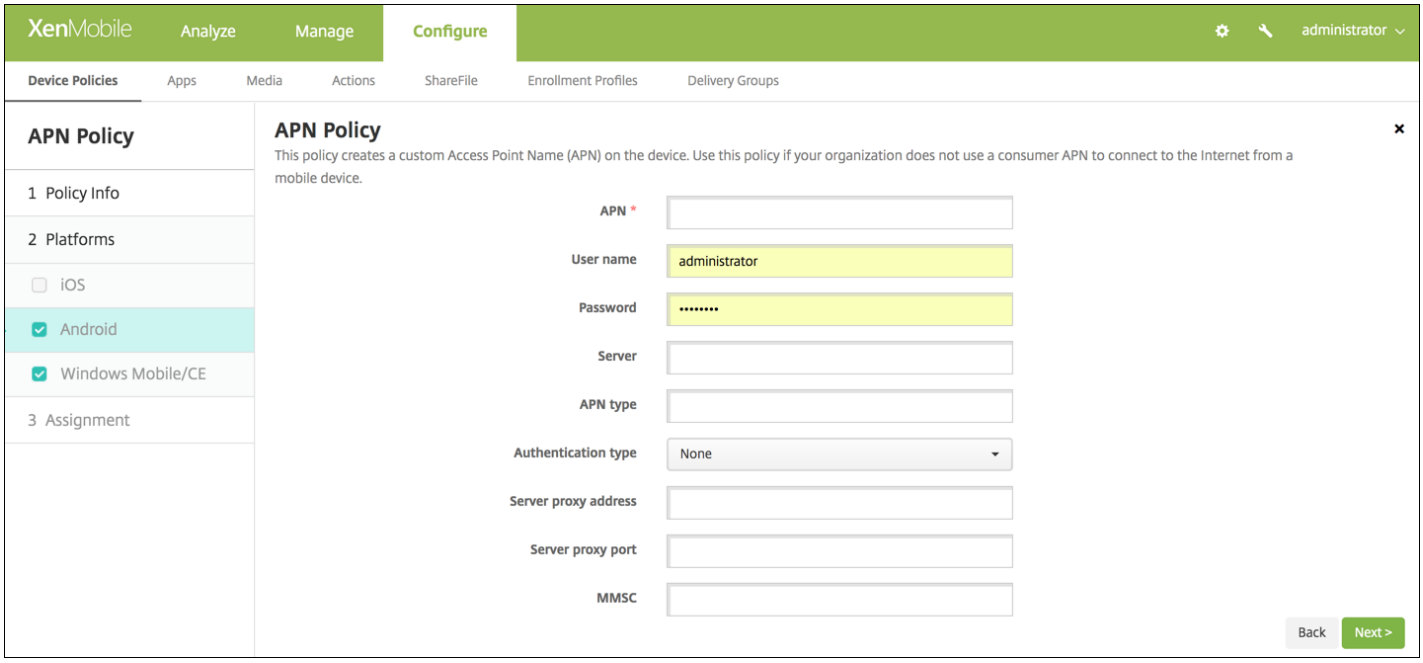
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Defina estas configurações:

- **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 de usuário desse 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 de perfil**, digite a senha necessária.

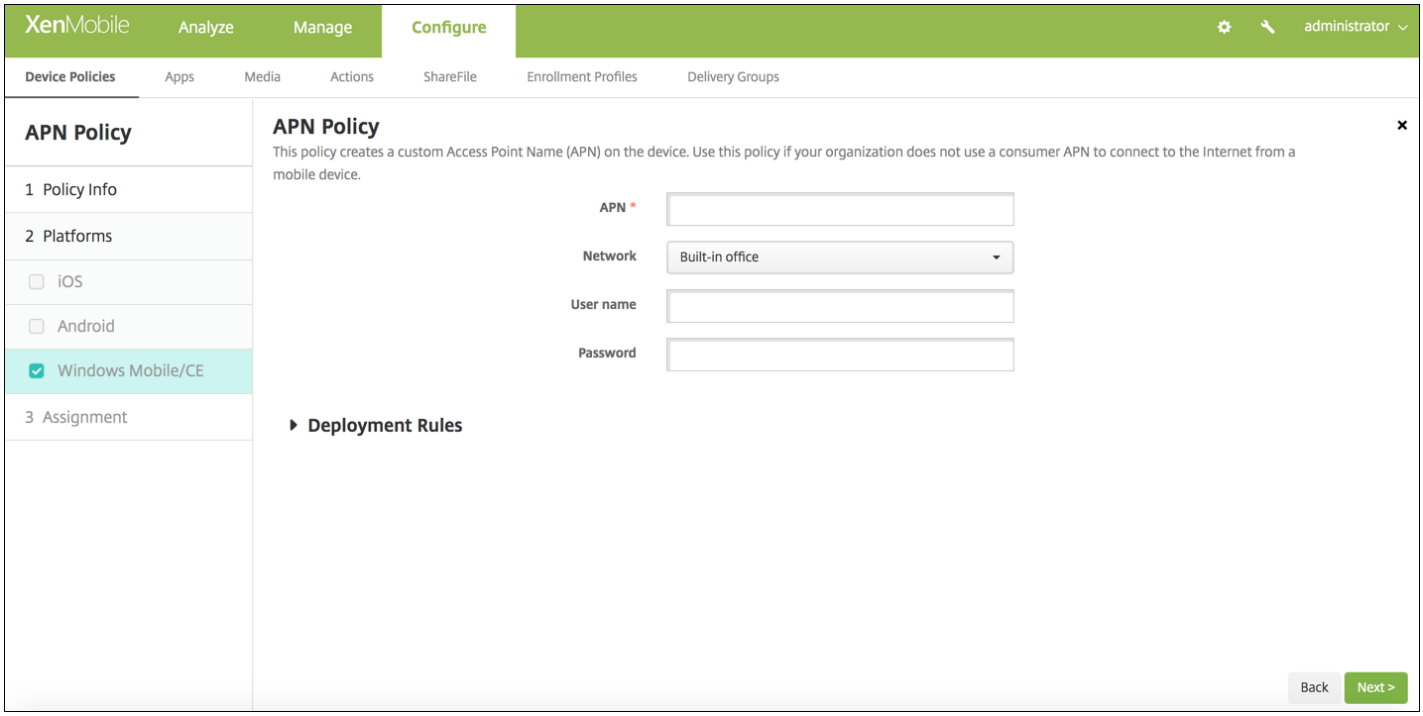
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Defina estas configurações:

- **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 de usuário desse 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 de protocolo WAP para telefones que não conseguiam acessar ou processar sites padrão.
- **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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Faça as seguintes configurações:

- **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 de usuário estiver ausente, o dispositivo solicitará a cadeia de caracteres durante a instalação do perfil.
- **Senha**: a senha de usuário desse 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.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de acesso aos aplicativos

Feb 21, 2018

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, é recomendável que você nomeie cada política cuidadosamente, para que saiba qual política no XenMobile se aplica à qual lista de aplicativos.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Expanda **Mais** e, em **Aplicativos**, clique em **Acesso aos aplicativos**. A página de informações **Política de acesso aos aplicativos** é exibida.

4. No painel **Informações sobre a política**, insira as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma de política** é exibida.

Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

6. Defina as configurações a seguir para cada plataforma selecionada.

- **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 desejar adicionar.

    Nota: para excluir um aplicativo 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 aplicativo existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de atributos de aplicativo

Feb 21, 2018

A política de dispositivos de atributos de aplicativo permite especificar atributos, como um aplicativo gerenciado ID do pacote ou um identificador de VPN por aplicativo, para dispositivos iOS.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

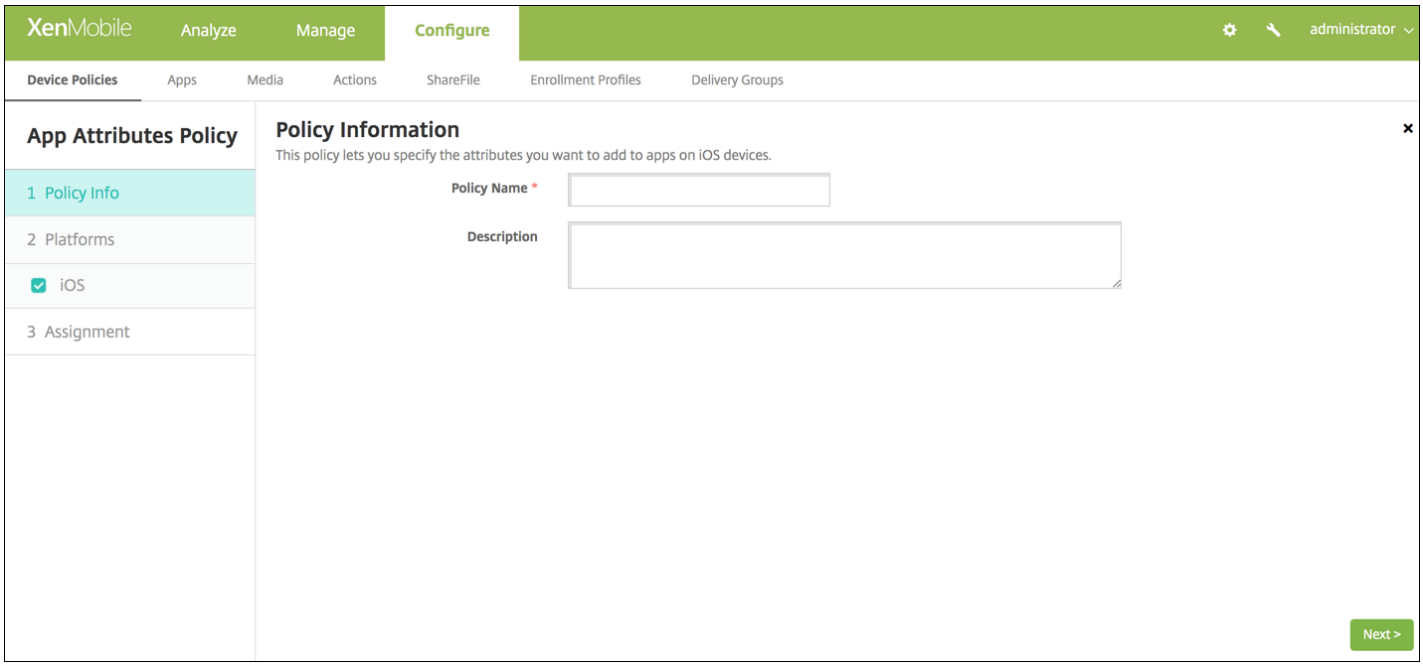
2. Clique em **Adicionar**. A página **Adicionar uma nova política** é exibida.

3. Expanda **Mais** e, em **Aplicativos**, clique em **Atributos de aplicativo**. A página de informações sobre **Política de atributos de aplicativo** é exibida.

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 de informações sobre a plataforma de **Atributos de aplicativo** é exibida.



6. Defina estas configurações:

- **ID de pacote de aplicativos gerenciados**: na lista, clique em uma ID de pacote de aplicativos ou em **Adicionar novo**.
  - Se você clicar em **Adicionar novo**, digite a ID de pacote de aplicativos no campo exibido.
- **Identificador VPN por aplicativo**: na lista, clique em identificador VPN por aplicativo.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de configuração de aplicativo

Feb 21, 2018

Você pode configurar remotamente aplicativos que dão suporte à configuração gerenciada por meio da implantação de um arquivode configuração XML (chamado de lista de propriedade, ou plist) para os dispositivos iOS dos usuários ou pares de chave/valor para dispositivos Windows 10 phone, tablet ou desktop. 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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. A página **Adicionar uma nova política** é exibida.

3. Expanda **Mais** e, em **Aplicativos**, clique em **Configuração do aplicativo**. A página de informações **Política de configuração de aplicativo** é exibida.

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 **Plataforma de política** é exibida.

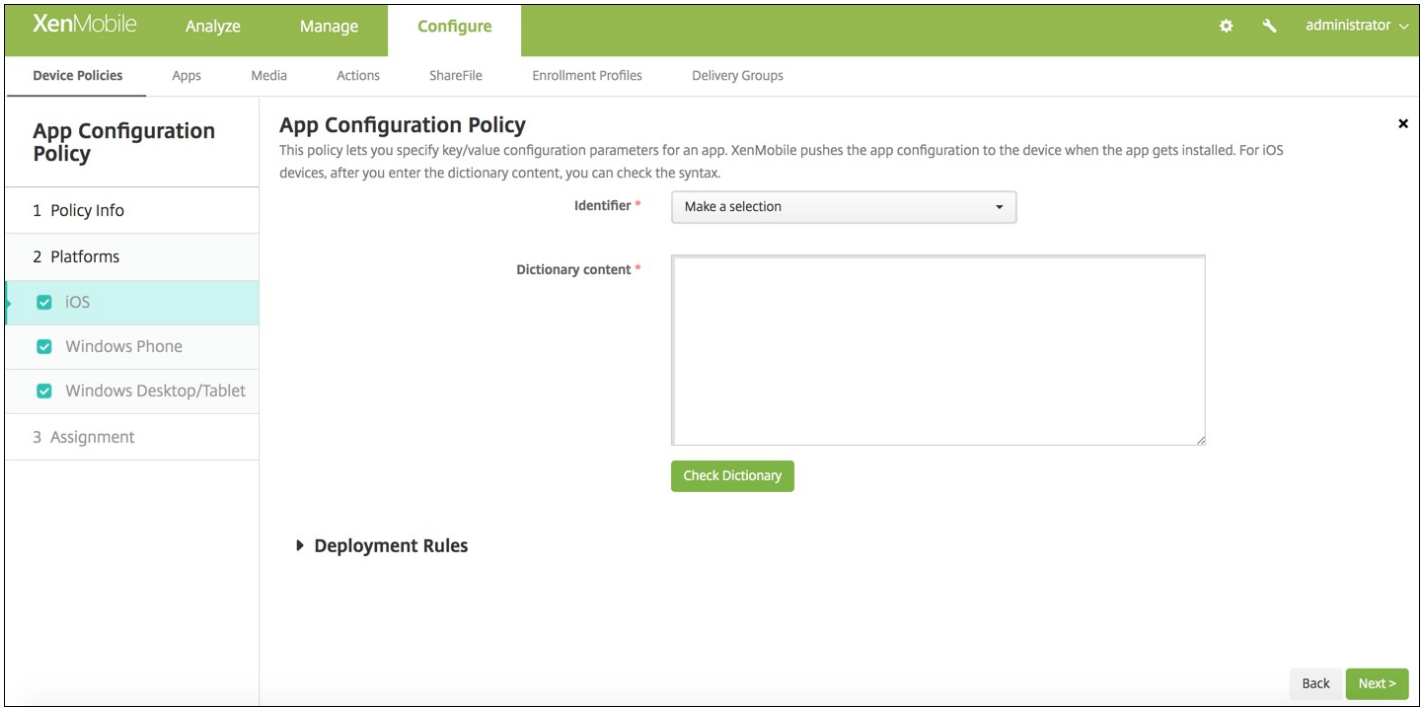
   Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

   Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 6 para saber como definir as regras de implantação dessa plataforma.

Definir as configurações do iOS

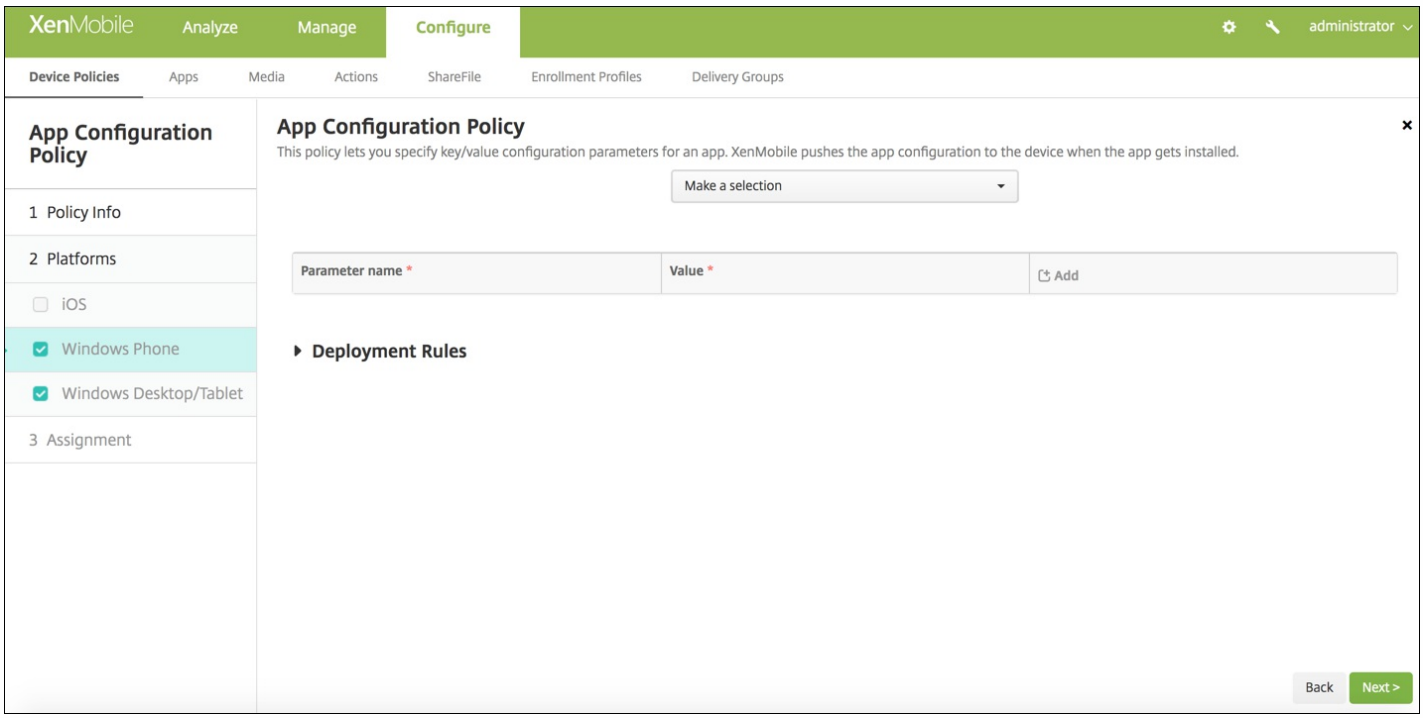
- **Identificador**: na lista, clique no aplicativo que você desejar configurar ou em **Adicionar novo** para adicionar um novo aplicativo à lista.
  - Se você clicar em **Adicionar novo**, digite o identificador do aplicativo no campo exibido.
- **Conteúdo do dicionário**: digite ou copie e cole as 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

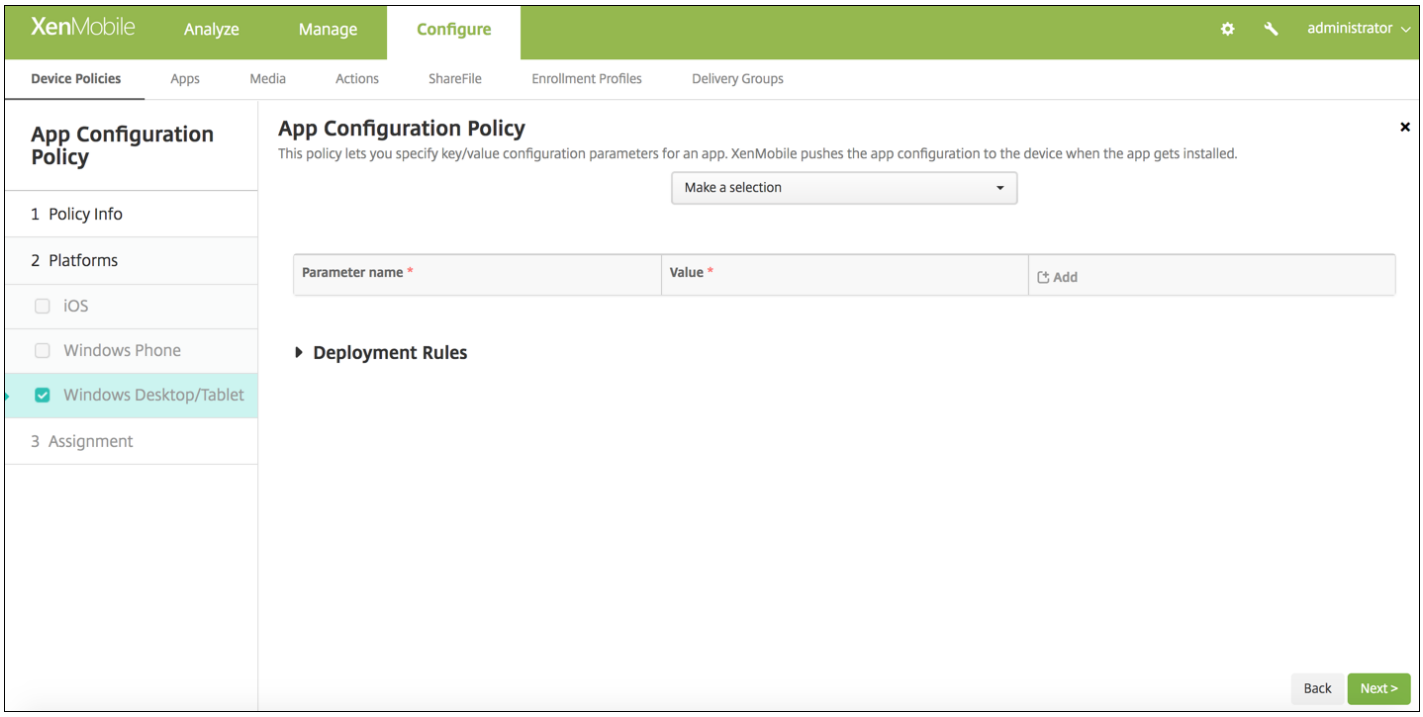


Definir as configurações do Windows Phone ou Desktop/Tablet

- Na lista **Faça uma seleção**, clique no aplicativo que você desejar configurar ou em **Adicionar novo** para adicionar um novo aplicativo à lista.
  - Se você clicar em **Adicionar novo**, digite o nome da família no campo exibido.
- Para cada parâmetro de configuração que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
  - **Nome do parâmetro**: insira 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**: insira o valor do parâmetro especificado.
  - Clique em **Adicionar** para adicionar o parâmetro ou em **Cancelar** para cancelar a adição do URL.



© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de inventário de aplicativos

Feb 21, 2018

Uma política de inventário de aplicativos no XenMobile permite coletar um inventário dos aplicativos nos dispositivos gerenciados e, em seguida, esse inventário é comparado a qualquer política de acesso aos aplicativos implantada nesses dispositivos. Dessa forma, você pode detectar aplicativos que são exibidos em uma lista negra de aplicativos (proibidos em uma política de acesso aos aplicativos) ou lista branca (obrigatórios em uma política de acesso aos aplicativos) e tomar uma ação apropriada. Você pode criar as políticas de acesso a aplicativos para iOS, macOS X e Android (inclusive para dispositivos para Android for Work), dispositivos Windows desktop/tablet, Windows Phone ou Windows Mobile/CE.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

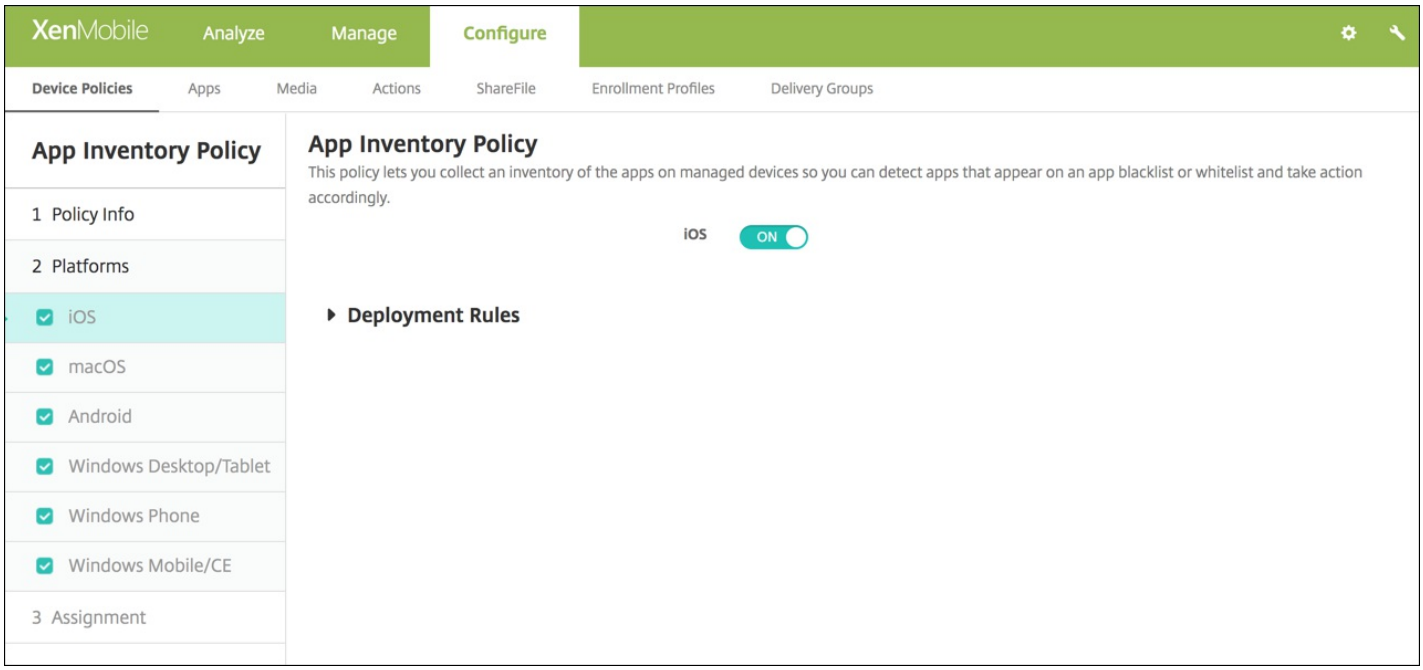
2. Clique em **Adicionar**. É exibida a página **Adicionar uma nova política**.

3. Expanda **Mais** e, em **Aplicativos**, clique em **Inventário de aplicativos**. A página **Política de inventário de aplicativos** é exibida.

4. No painel **Informações sobre a política**, digite as seguintes informações:

- **Nome da política**: digite um nome para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma de política** é exibida.



Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

6. Para cada plataforma que você selecionar, mantenha a configuração padrão ou altere a configuração para **O**. O padrão é **I**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de bloqueio de aplicativo

Feb 21, 2018

Você pode criar uma política no XenMobile para definir uma lista de aplicativos que podem ser executados em um dispositivo ou uma lista de aplicativos que têm a execução 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.

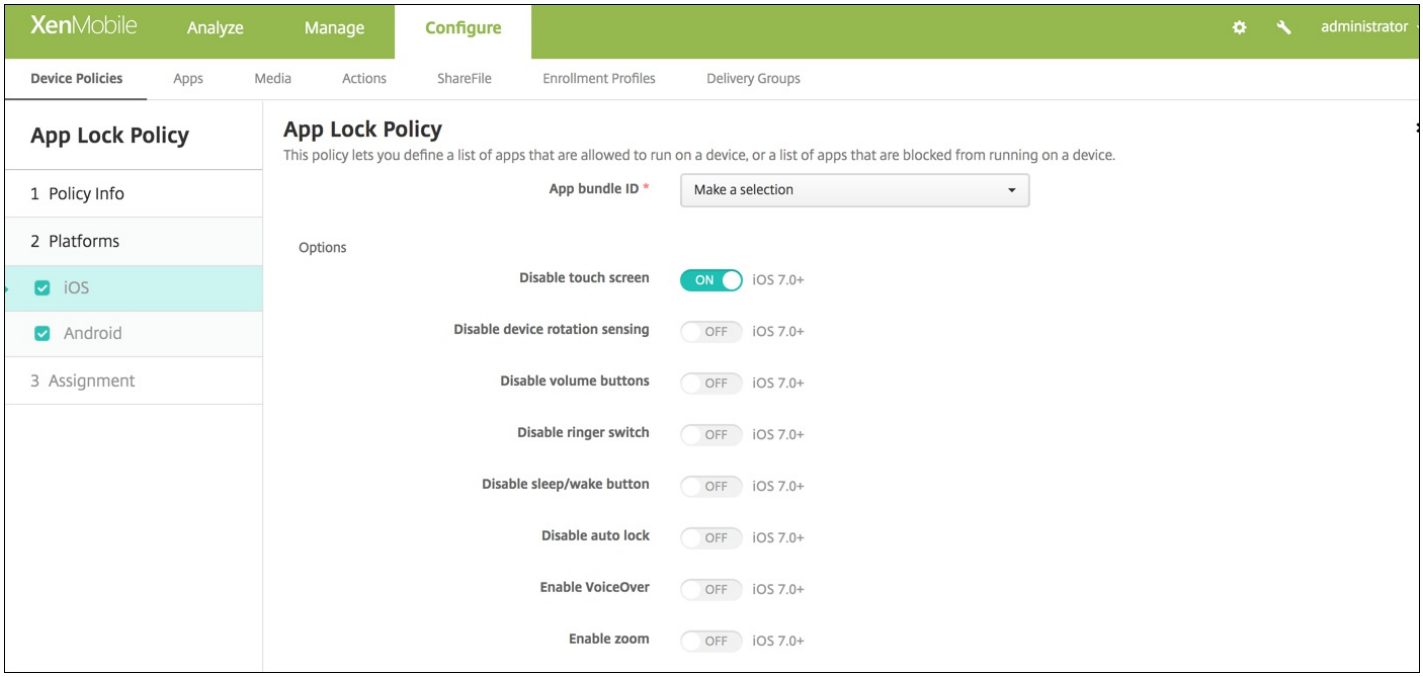
Da mesma forma, em dispositivos iOS, você pode selecionar apenas um aplicativo iOS por política. Isso significa que os usuários só são capazes de usar o dispositivo para executar um único aplicativo. Eles não podem realizar outras atividades no dispositivo. exceto as opções permitidas especificamente 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 a API necessária do Google não é mais utilizada.

Configurações do iOS

Configurações do Android



Defina estas configurações:

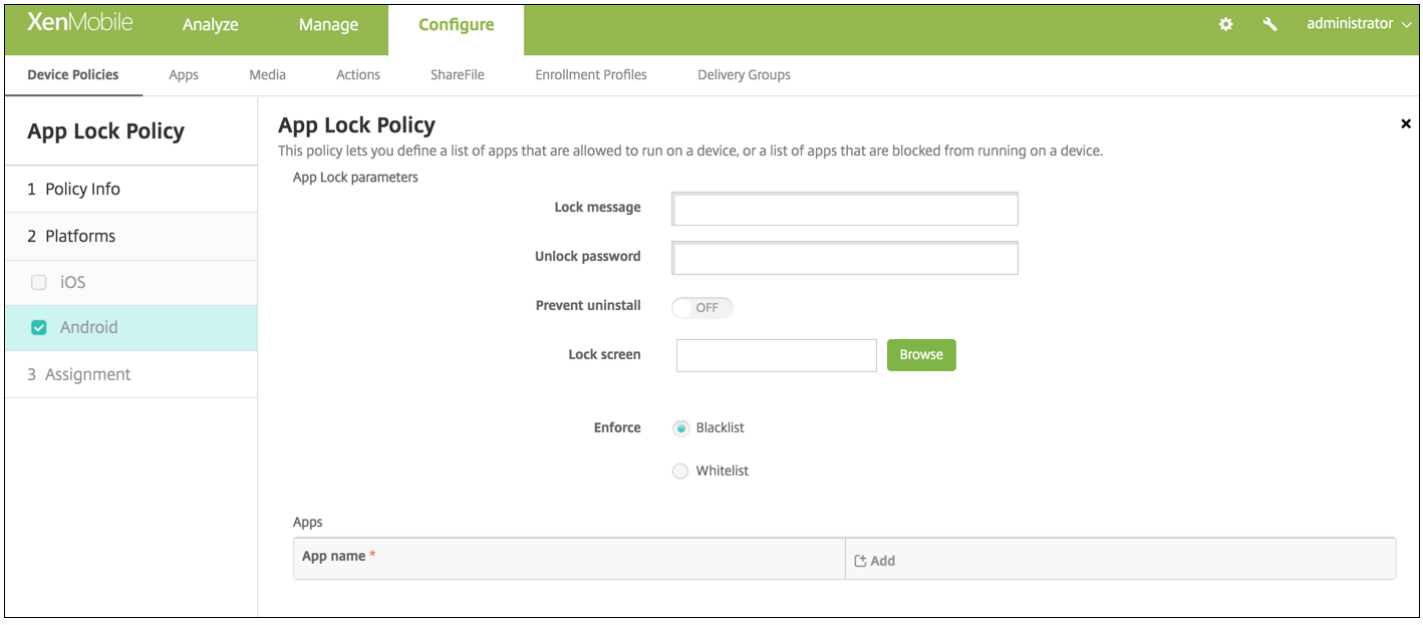
- **ID do pacote de aplicativos**: na lista, clique no aplicativo ao qual esta política se aplica ou clique em **Adicionar novo** para adicionar um novo aplicativo à lista. Se você selecionar **Adicionar novo**, digite o nome do aplicativo no campo exibido.
- **Opções**: cada uma das opções a seguir 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Desativar botões de volume
- Desativar botão de toque - **Nota**: quando essa opção está desativada, 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**
  - o Ao lado de **Remover política**, clique em **Selecionar data** ou em **Duração até remoção (em horas)**.
  - o Se você clicar em **Selecionar data**, clique no calendário para selecionar a data específica para a remoção.
  - o Na lista **Permitir que o usuário remova a política**, clique em **Sempre**, **Senha obrigatória** ou **Nunca**.
  - o Se você clicar em **Senha obrigatória**, ao lado de **Senha de remoção**, digite a senha necessária.

> ## Nota
>
> Você não pode bloquear o aplicativo de configurações do Android usando a política de dispositivo de bloqueio de aplicativo.



Defina estas configurações:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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 **O**.
  - **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.
- **Aplicativos**: clique em **Adicionar** e faça o seguinte:
  - **Nome do aplicativo**: na lista, clique no nome do aplicativo para adicioná-lo à lista branca ou negra, 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 à lista branca ou negra.

    Nota: para excluir um aplicativo 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 aplicativo existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de uso de rede de aplicativos

Feb 21, 2018

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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Expanda **Mais** e, em **Aplicativos**, clique em **Uso de rede de aplicativos**. A página de informações **Política de uso de rede de aplicativos** é exibida.

4. No painel **Informações sobre a política**, insira as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma de política** é exibida.

6. Defina estas configurações.

- **Permitir dados celulares de roaming**: selecione se os aplicativos especificados podem usar uma conexão de dados celulares enquanto estiverem em roaming. O padrão é **O**.
- **Permitir dados celulares**: selecione se os aplicativos especificados podem usar uma conexão de dados celulares. O padrão é **O**.
- **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.

    Observação: para excluir um aplicativo 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 aplicativo existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

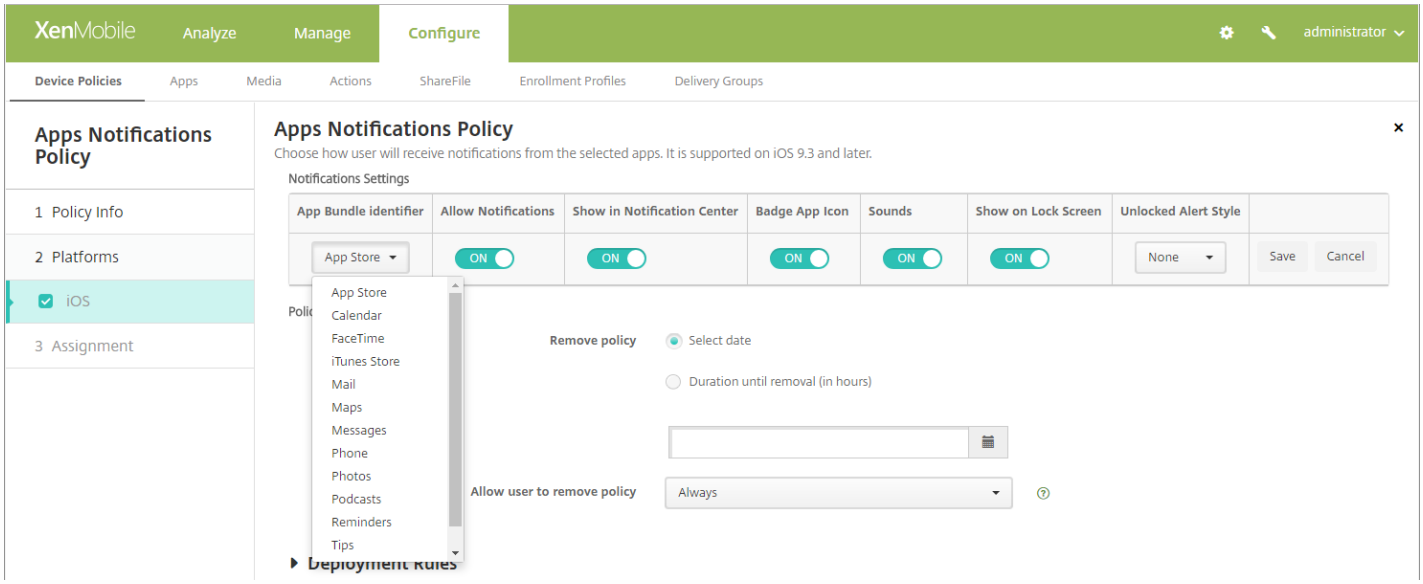
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de notificações de aplicativo

Feb 21, 2018

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.

Defina estas configurações:



- **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.
- **Estilo de alerta desbloqueado**: na lista, selecione **Nenhum**, **Banner** ou **Alertas** para configurar a aparência dos alertas desbloqueados.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de restrições de aplicativo

Feb 21, 2018

Você pode criar listas negras para os aplicativos que deseja impedir que os usuários instalem nos dispositivos Samsung KNOX, bem como listas brancas para os aplicativos que deseja permitir que os usuários instalem.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

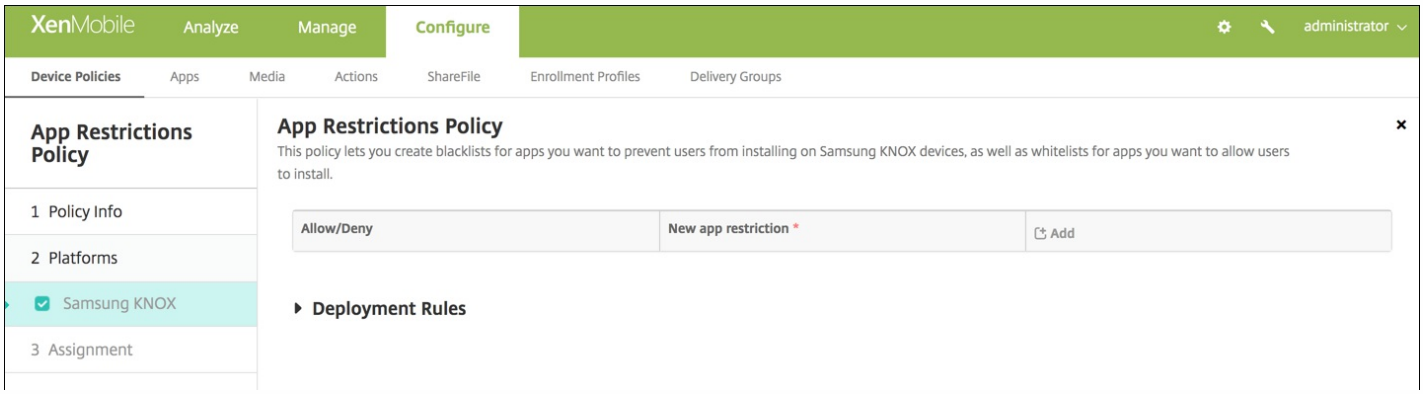
2. Clique em **Adicionar**. A caixa de diálogo **Adicionar uma nova política** é exibida.

3. Expanda **Mais** e, em **Segurança**, clique em **Restrições de aplicativo**. A página de informações **Política de restrições de aplicativo** é exibida.

4. No painel **Informações sobre a política**, digite as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma Samsung KNOX** é exibida.



6. 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.

  Observação: para excluir um aplicativo 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 aplicativo existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de encapsulamento de aplicativo

Feb 21, 2018

> **Nota**
>
> A política de encapsulamento de aplicativo é usado somente para suporte remoto.Para obter informações sobre suporte remoto, consulte Opções de suporte e suporte remoto.

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.

Nota: qualquer tráfego de aplicativo enviado por meio de um túnel definido nessa política passa pelo XenMobile antes de ser redirecionado para o servidor que executa o aplicativo.

Configurações do Android

Configurações do Windows Mobile/CE

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Clique em **Mais** e, em **Acesso à rede**, clique em **Túnel**. A página **Política de túnel** é exibida.

4. No painel **Informações sobre a política**, insira as seguintes informações:

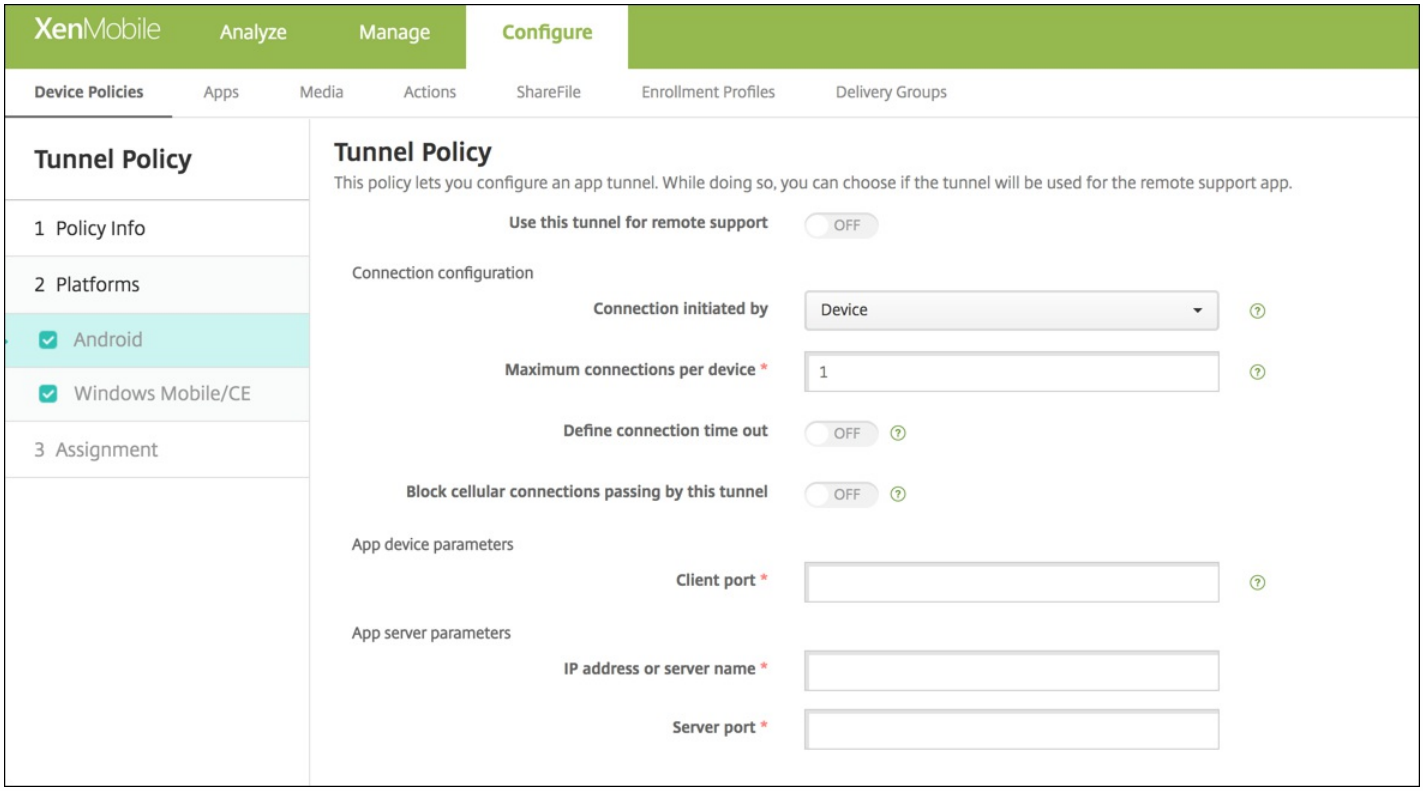
- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: opcionalmente, digite uma descrição para a política.

5. Clique em **Avançar**. A página **Plataforma de política** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Defina estas configurações:

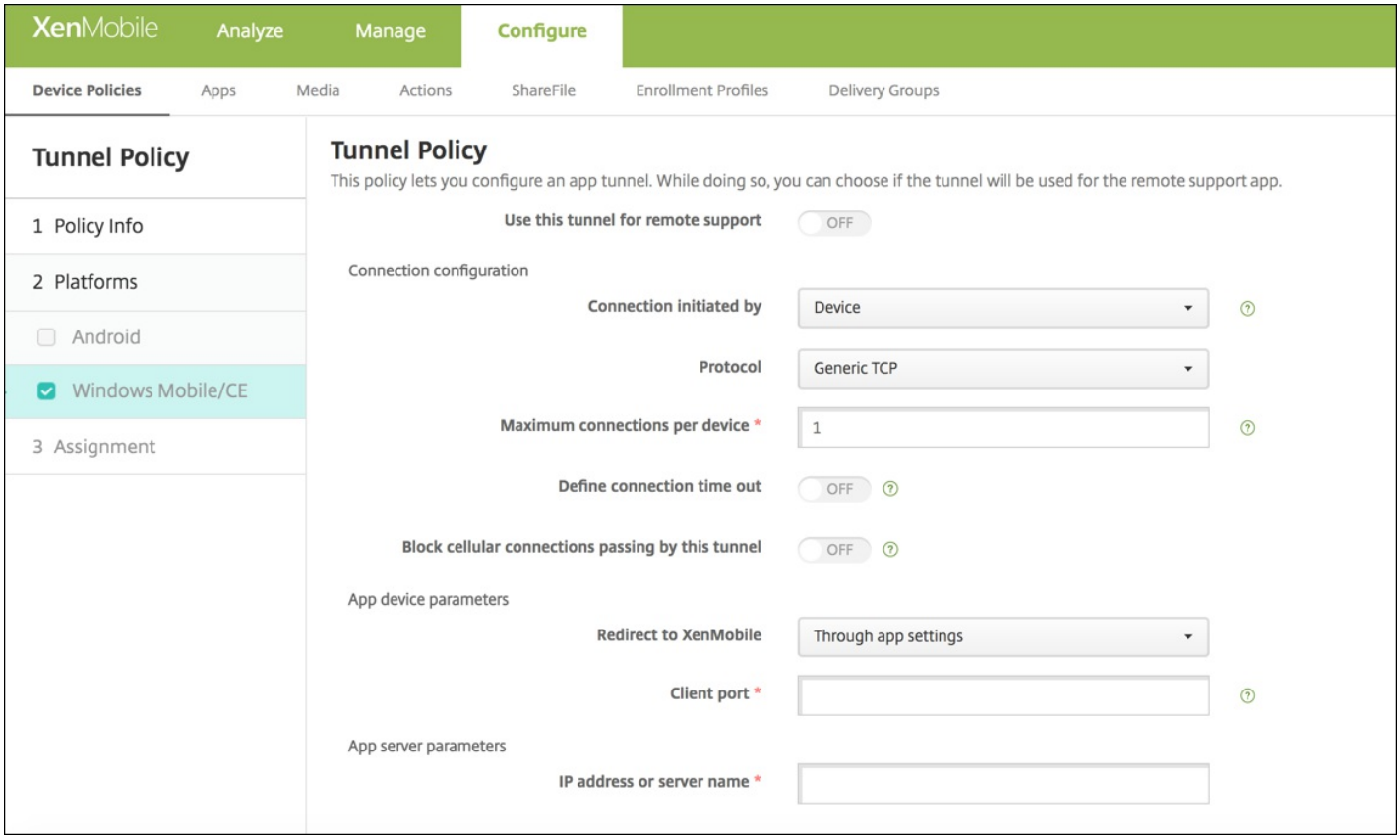
- **Usar este túnel para suporte remoto**: selecione se o túnel será usado para suporte remoto.

  Observações: 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 definir **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 WiFi e USB não serão bloqueadas.
  - **Porta do cliente**: digite o número da porta do cliente. 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 definir **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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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. **Nota**: conexões WiFi e USB não serão bloqueadas.



Defina estas configurações:

- **Usar este túnel para suporte remoto**: selecione se o túnel será usado para suporte remoto.

  Observações: 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 **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 definir **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 WiFi 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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

    - 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 do cliente. 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. **Nota**: conexões WiFi e USB não serão bloqueadas.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de desinstalação de aplicativo

Feb 21, 2018

Você pode criar uma política de desinstalação de aplicativo para as plataformas iOS, Android, Samsung KNOX, Android for Work, Windows Desktop/Tablet e Windows Mobile/CE. Uma política de desinstalação de aplicativo permite que você remova aplicativos dos dispositivos dos usuários 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 seus 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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. A caixa de diálogo **Adicionar uma nova política** é exibida.

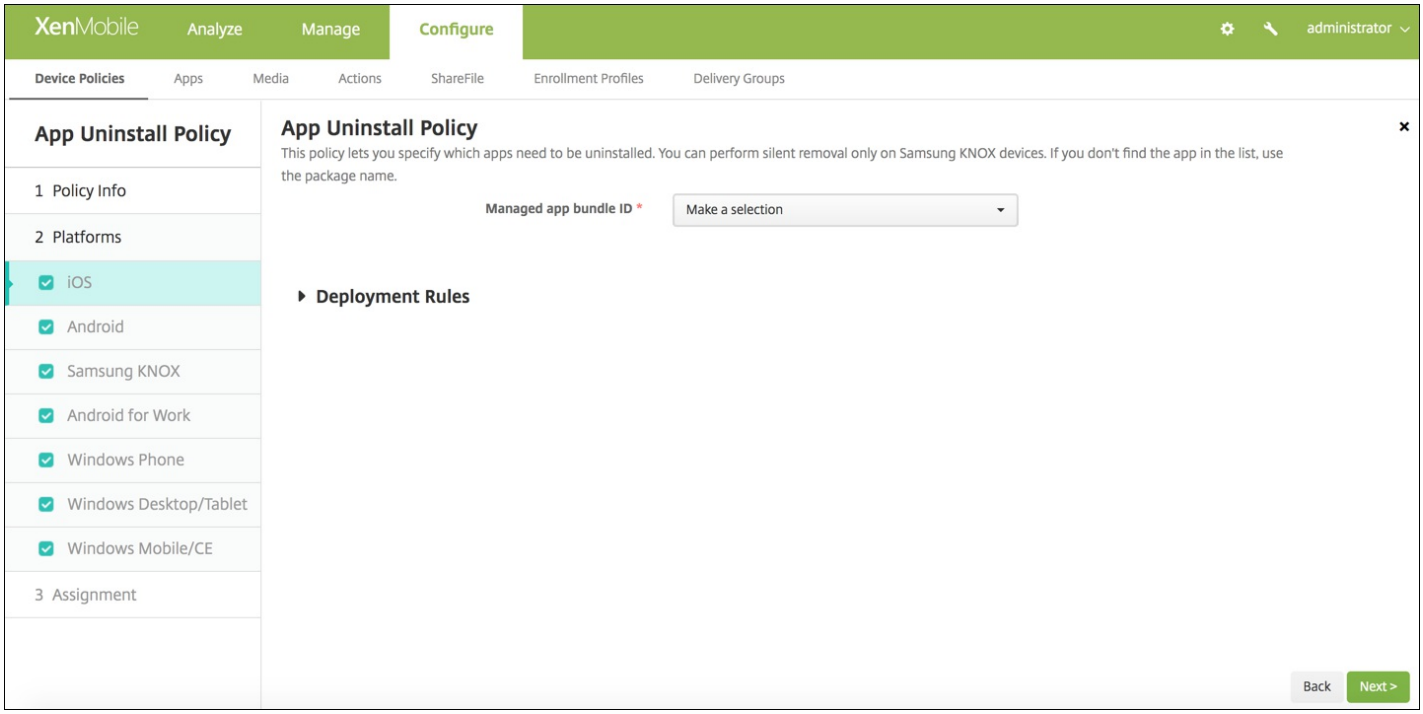
3. Expanda **Mais** e, em **Aplicativos**, clique em **Desinstalação de aplicativo**. A página **Política de desinstalação de aplicativo** é exibida.

4. No painel **Informações sobre a política**, insira as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma de política** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.



Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configure esta definição:

- **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**, é exibido um campo no qual é possível digitar um nome do aplicativo.

Configure esta definição:

- **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.

    Nota: para excluir um aplicativo existente da política de desinstalação, 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 aplicativo existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

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).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de restrições de desinstalação de aplicativo

Feb 21, 2018

Você pode especificar os aplicativos que os usuários podem ou não podem desinstalar em um dispositivo Samsung SAFE ou Amazon.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Expanda **Mais** e, em **Aplicativos**, clique em **Restrições de desinstalação de aplicativo**. A página de informações **Política de restrições de desinstalação de aplicativo** é exibida.

4. No painel **Informações sobre a política**, insira as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma de política** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

7. Defina as seguintes configurações para cada plataforma selecionada:

- **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**.

    Nota: para excluir um aplicativo 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 aplicativo existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

8.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo BitLocker

Feb 21, 2018

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 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.

Requisitos

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.

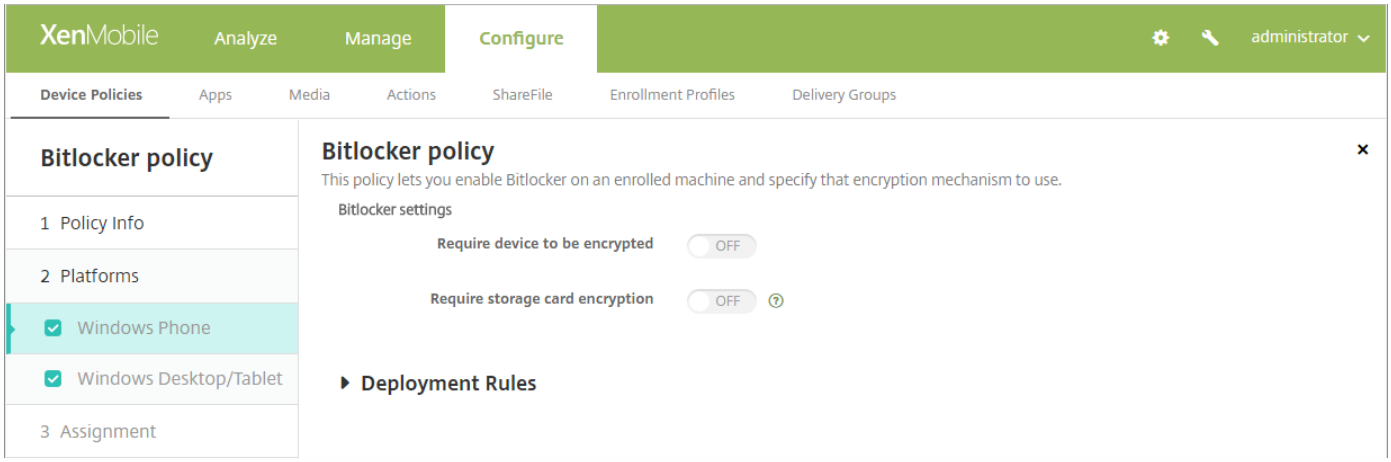
Definir as configurações do Windows 10

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 de política.

1. Clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.
2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.
3. Comece a digitar **BitLocker** e, em seguida, clique nesse nome nos resultados da pesquisa. A página **Informações sobre a Política** de BitLocker é exibida.
4. Na página **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** e defina essas configurações para cada plataforma escolhida.

   Configurações do Windows Phone

© 1999-2017 Citrix Systems, Inc. All rights reserved.

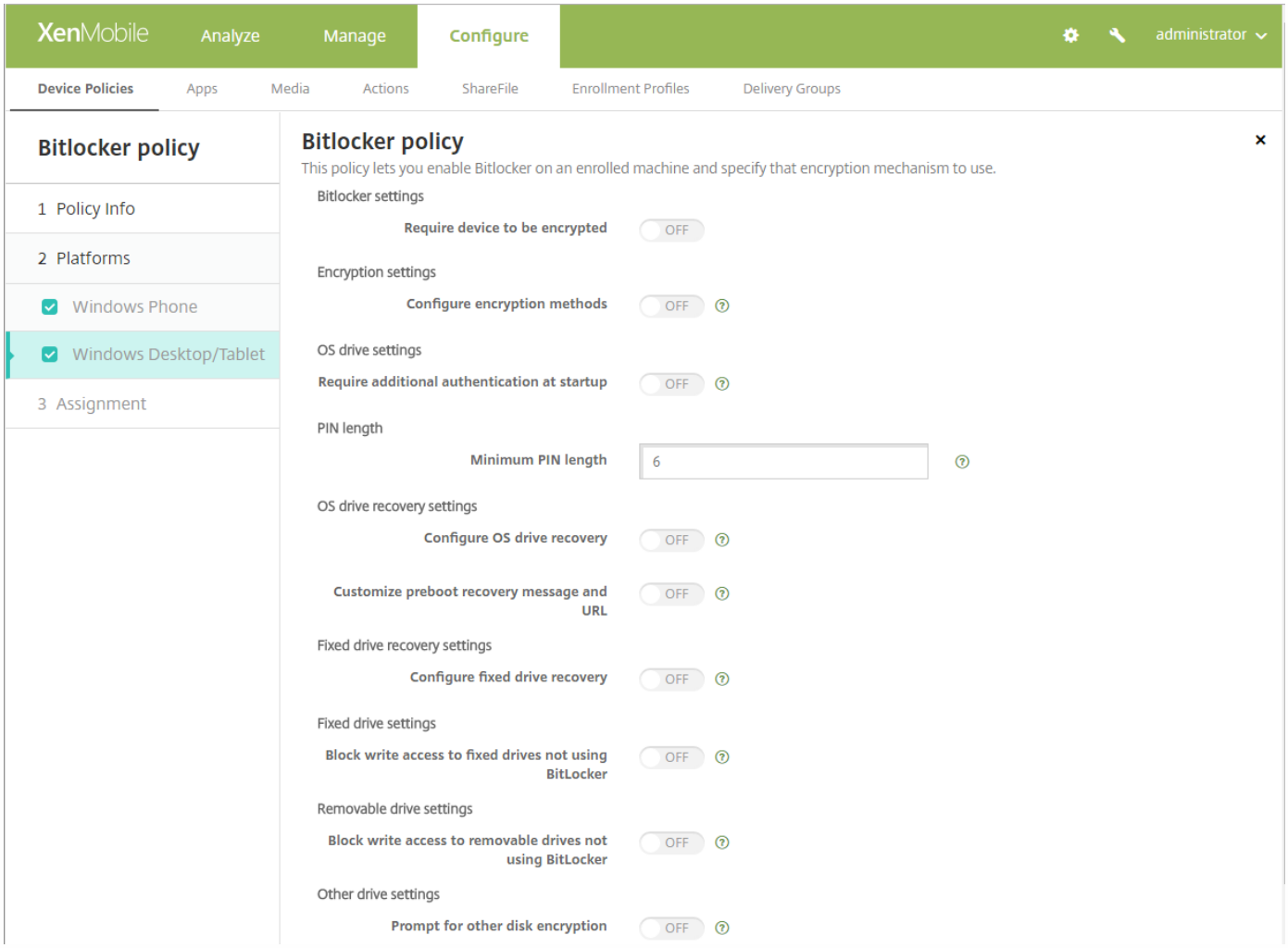


- **Exigir que o dispositivo seja criptografado**: determina se os usuários devem para ativar a criptografia de BitLocker em um cartão de sistema do Windows Phone. Se o valor for **Ativado**, os dispositivos mostram uma mensagem após a conclusão do registro, indicando que a empresa requer criptografia 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 **O**.

- **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 **O**.

Configurações do Windows Desktop e Tablet

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- **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 **O**.

- **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 **O**.

- **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 Trusted Platform Module Technology Overview. Se o valor for **Ativado**, as seguintes configurações adicionais são exibidas. O padrão é **O**.

  - **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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

um mínimo de oito caracteres. O padrão é **O**.

- **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 valor 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 BitLocker Basic Deployment. O valor padrão é **Desativado**.
  - **Criar senha de recuperação de 48 dígitos 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 dígitos**: 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 valor 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 valor padrão é **Desativado**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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 valor 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 valor 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 valor 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 valor 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 valor 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 **O**.

6. Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

> ## 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de navegador

Feb 21, 2018

Você pode criar políticas de dispositivo de navegador para dispositivos Samsung SAFE ou Samsung KNOX para definir se os dispositivos dos usuários podem usar o navegador ou para limitar as funções do navegador que os dispositivos dos usuários 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.

Configurações do Samsung SAFE e do Samsung KNOX

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar** para adicionar uma nova política. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Clique em **Mais** e, em **Aplicativos**, clique em **Navegador**. A página de informações **Política de Navegador** é exibida.

4. No painel **Informações sobre a política**, insira as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma de política** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

Defina estas configurações:

- **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.

8. Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de calendário (CalDav)

Feb 21, 2018

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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Expanda **Mais** e, em **Usuário final**, clique em **Calendário (CalDav)**. A página **Política de calendário (CalDAV)** é exibida.

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 as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

Faça as seguintes configurações:

- **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 **I**.
- **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 de perfil**, digite a senha necessária.

Faça as seguintes configurações:

- **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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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 **I**.
- **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 de perfil**, digite a senha necessária.
  - Ao lado de **Escopo do perfil**, clique em **Usuário** ou **Sistema**. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo celular

Feb 21, 2018

Essa política permite que você defina as configurações da rede celular em um dispositivo iOS.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. A página **Adicionar uma nova política** é exibida.

3. Expanda **Mais** e, em **Acesso à rede**, clique em **Celular**. A página de informações **Política de rede celular** é exibida.

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 de informações **Plataforma iOS** é exibida.

6. Defina estas configurações:

- **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**
  - 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 de perfil**, digite a senha necessária.

8. Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo do gerenciador de conexões

Feb 21, 2018

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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. A caixa de diálogo **Adicionar uma nova política** é exibida.

3. Clique em **Mais** e, em **Acesso à rede**, clique em **Gerenciador de conexões**. A página de informações de política **Gerenciador de conexões** é exibida.

4. No painel **Informações sobre a política**, insira as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma Windows Mobile/CE** é exibida.

6. Defina estas configurações.

Observação: **Escritório interno** significa que todas as conexões são estabelecidas com a intranet da sua empresa e **Internet interna** significa que todas as conexões são estabelecidas com a Internet.

- **Aplicativos que se conectam a uma rede privada usam automaticamente**: na lista, clique em **Escritório interno** ou **Internet interna**. O padrão é **Escritório interno**.
- **Aplicativos que se conectam à Internet automaticamente usam**: na lista, clique em **Escritório interno** ou **Internet interna**. O padrão é **Escritório interno**.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de agendamento de conexão

Feb 21, 2018

Crie políticas de agendamento de conexão para controlar como e quando os dispositivos dos usuários se conectam ao XenMobile. Observe que você pode configurar essa política também para dispositivos ativados para Android for Work.

Você pode especificar que os usuários conectem os dispositivos deles manualmente, que os dispositivos se mantenham conectados permanentemente ou que os dispositivos se conectem em um período de tempo definido.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. A caixa de diálogo **Adicionar uma nova política** é exibida.

3. Clique em **Agendamento**. A página de informações **Política de agendamento de conexão** é exibida.

4. No painel **Informações sobre a política**, insira as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma de política** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 8 para saber como definir as regras de implantação dessa plataforma.

7. Defina as seguintes configurações para cada uma das plataformas selecionadas:

- **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 escolhe **Sempre**, use também para a **Política de túnel** do dispositivo a configuração **Definir o tempo limite de conexão** para garantir que a conexão não drene 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 de **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 para saber como definir um período de tempo de conexão.

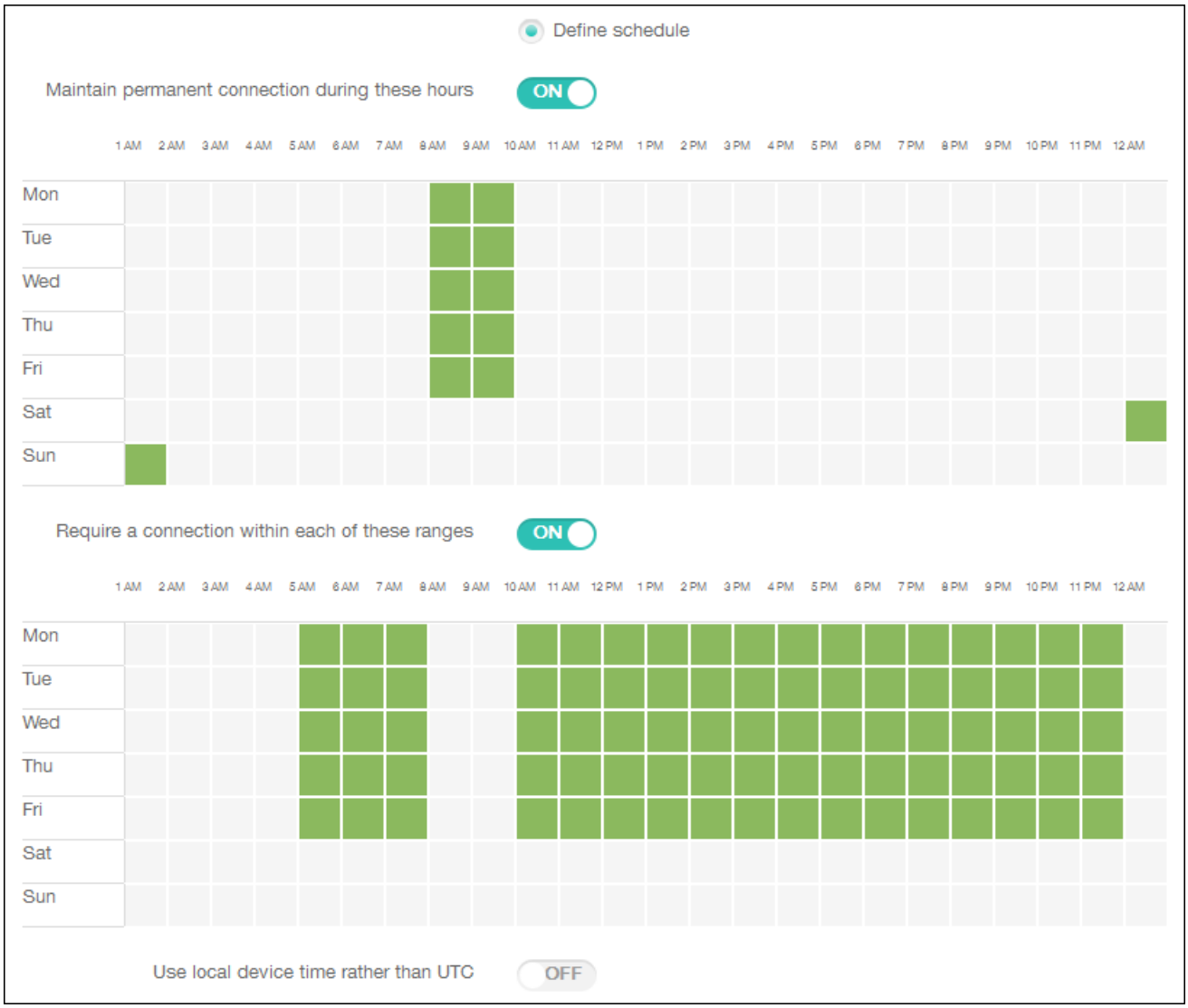
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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.



8.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma

© 1999-2017 Citrix Systems, Inc. All rights reserved.

política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de contatos (CardDAV)

Feb 21, 2018

Você pode adicionar uma política de dispositivo no XenMobile para adicionar uma conta de contatos do iOS (CardDAV) aos dispositivos iOS ou macOS dos usuários para permitir que eles sincronizem dados de contato com qualquer servidor compatível com CardDAV.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. A caixa de diálogo **Adicionar uma nova política** é exibida.

3. Expanda **Mais** e, em **Segurança**, clique em **Contatos (CardDAV)**. A página **Política de CardDAV** é exibida.

4. No painel **Informações sobre a política**, digite 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 as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

Defina estas configurações:

- **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 **I**.
- **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 de perfil, digite a senha necessária.

Defina estas configurações:

- **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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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 **I**.
- **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 de perfil, digite a senha necessária.
  - Ao lado de **Escopo do perfil**, clique em **Usuário** ou **Sistema**. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Control OS Updates device policy

Feb 21, 2018

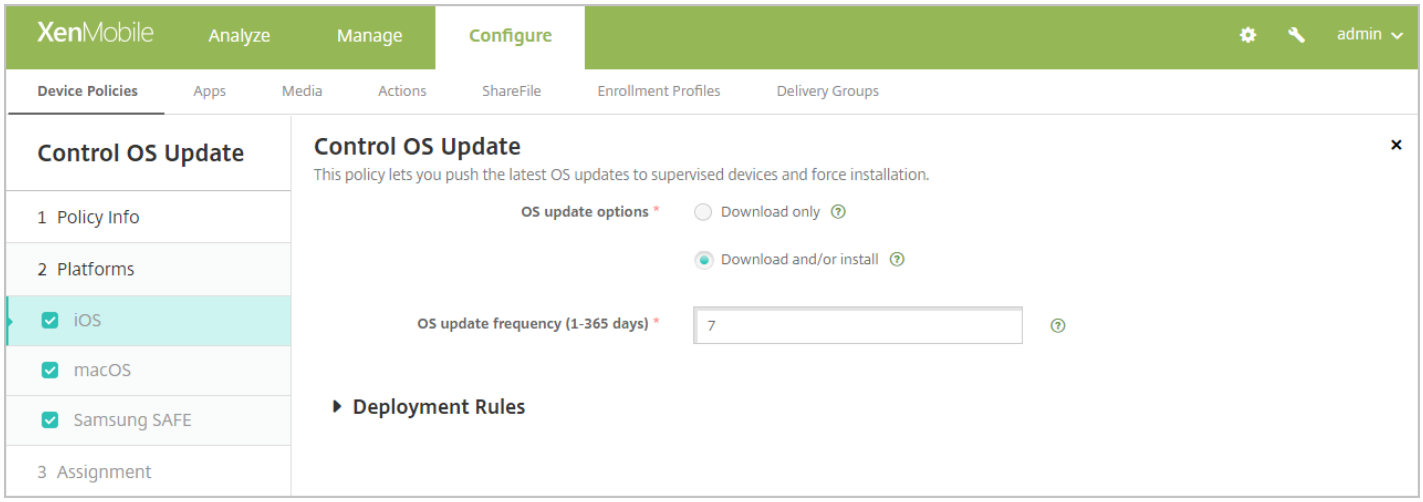
A política de dispositivo de controle de atualização do sistema operacional permite que você implante:

- As atualizações do sistema operacional mais recentes a dispositivos iOS com supervisão e Samsung SAFE.

  Para dispositivos que executam o iOS 10.3 e versões posteriores, o Controle de atualizações do sistema operacional funciona em dispositivos supervisionados. Para dispositivos que executam uma versão anterior ao iOS 10.3, o Controle de atualizações do sistema operacional funciona em dispositivos supervisionados e registrados no DEP.

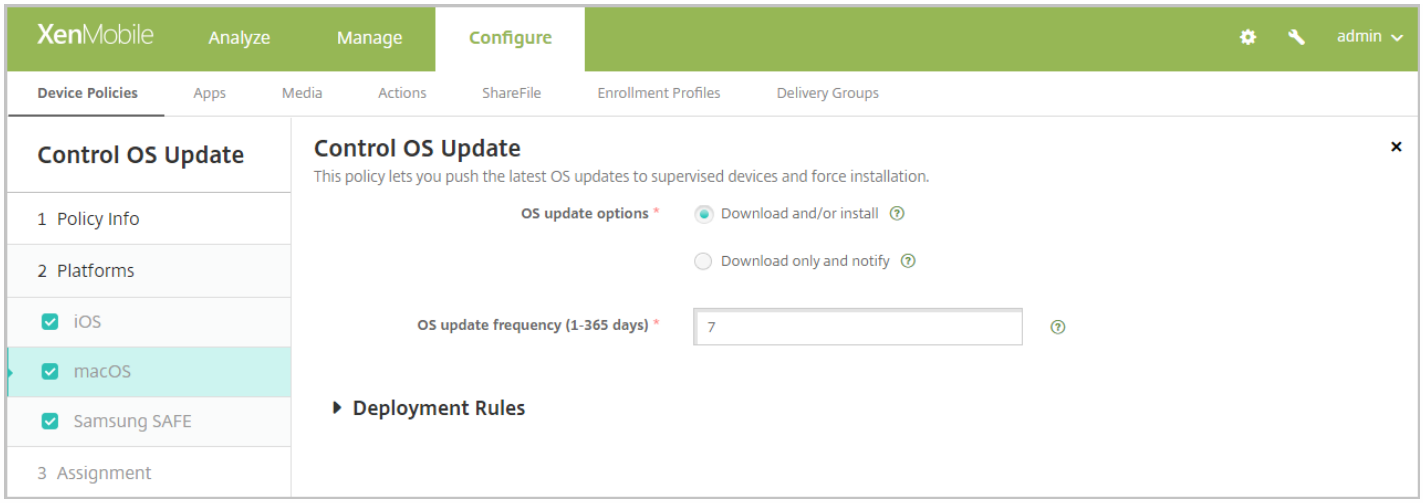
- As atualizações mais recentes de sistema operacional e aplicativo para dispositivos macOS registrados em DEP com macOS 10.11.5 e versões posteriores.

Nos dispositivos Samsung SAFE, o XenMobile envia a política de controle de atualização 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.



- **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 sistema operacional**. O dispositivo solicita que os usuários instalem atualizações. O aviso é visível depois que o usuário desbloqueia o dispositivo.
- **Frequência de atualização de SO**: determina com que frequência o XenMobile verifica e atualiza o sistema operacional do dispositivo. O padrão é **7** dias.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



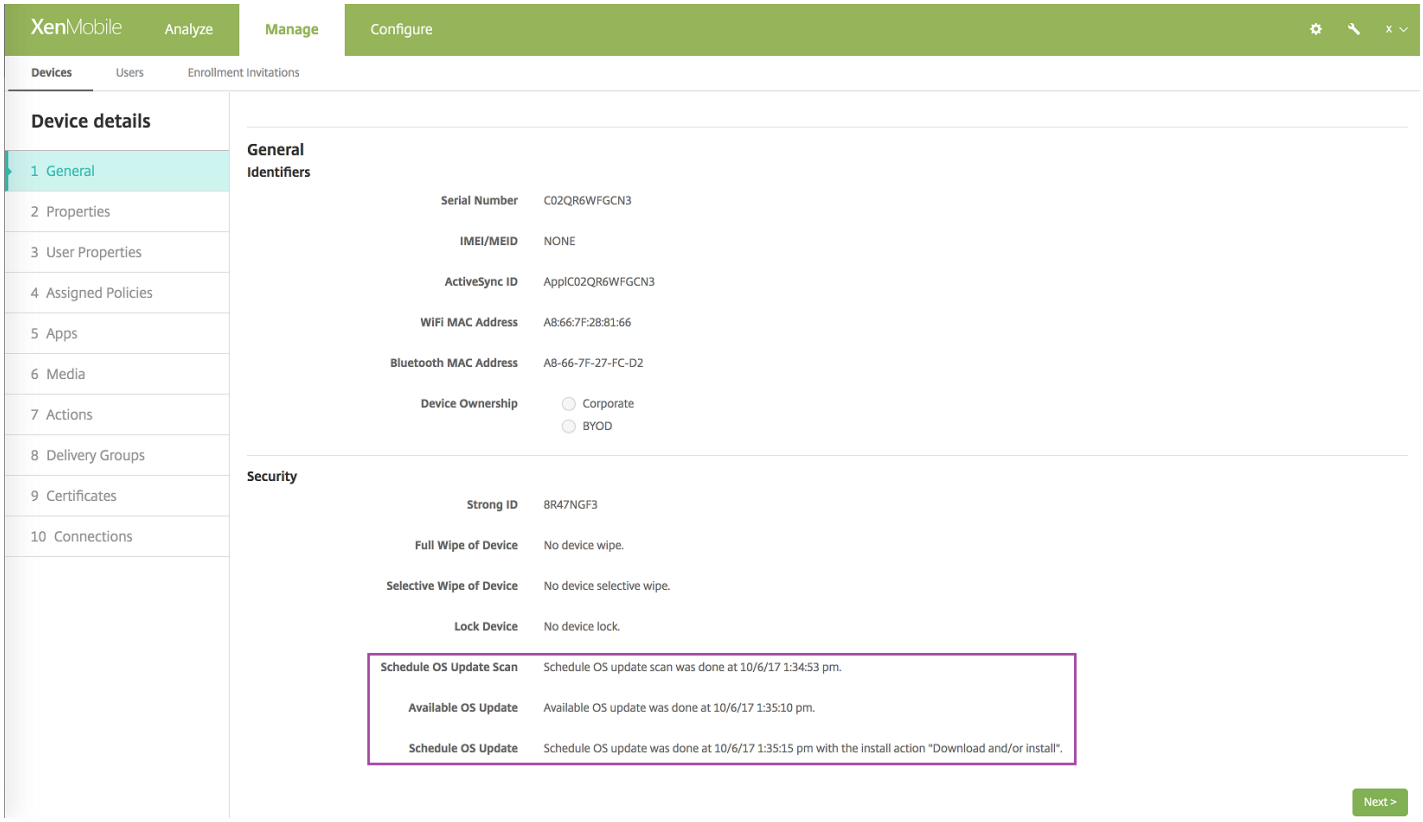
- **Opções de atualização do sistema operacional**: ambas as opções baixam as mais recentes atualizações de sistema operacional para macOS de acordo com a **frequência de atualização do sistema operacional**. Você pode optar por instalar as atualizações ou notificar o usuário por meio da loja de aplicativos que as atualizações estão disponíveis.
- **Frequência de atualização de SO**: determina com que frequência o XenMobile verifica e atualiza o sistema operacional do dispositivo. O padrão é **7** dias.

No iOS e macOS, o XenMobile não implementa a política de controle de atualização do sistema operacional nos dispositivos. Em vez disso, o XenMobile usa a política para enviar esses comandos do MDM para dispositivos:

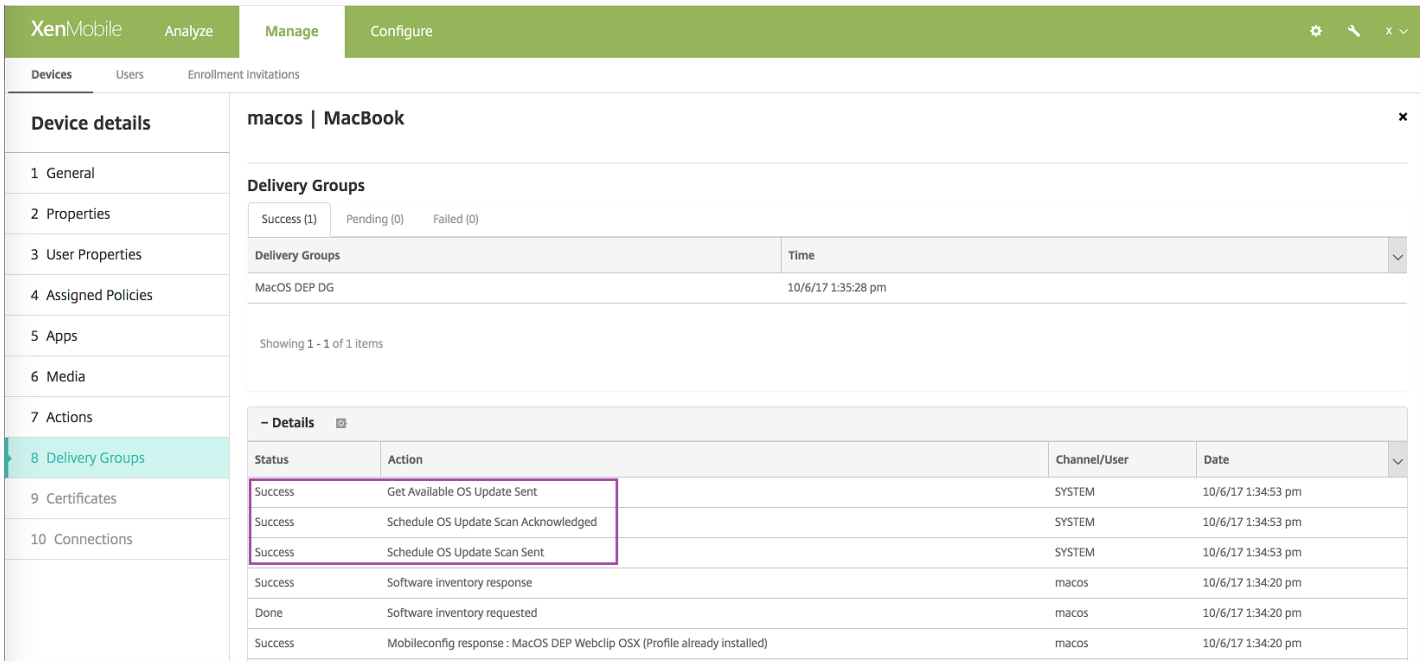
- Cronograma de verificação de atualização do SO: solicita que o dispositivo execute uma verificação em segundo plano de atualizações do sistema operacional. (opcional para iOS)
- Atualização de SO disponível: consulta o dispositivo para obter uma lista de atualizações do sistema operacional disponíveis.
- 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 agendadas de atualizações do sistema operacional, atualizações do sistema operacional disponíveis e atualizações agendadas do macOS e do aplicativo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

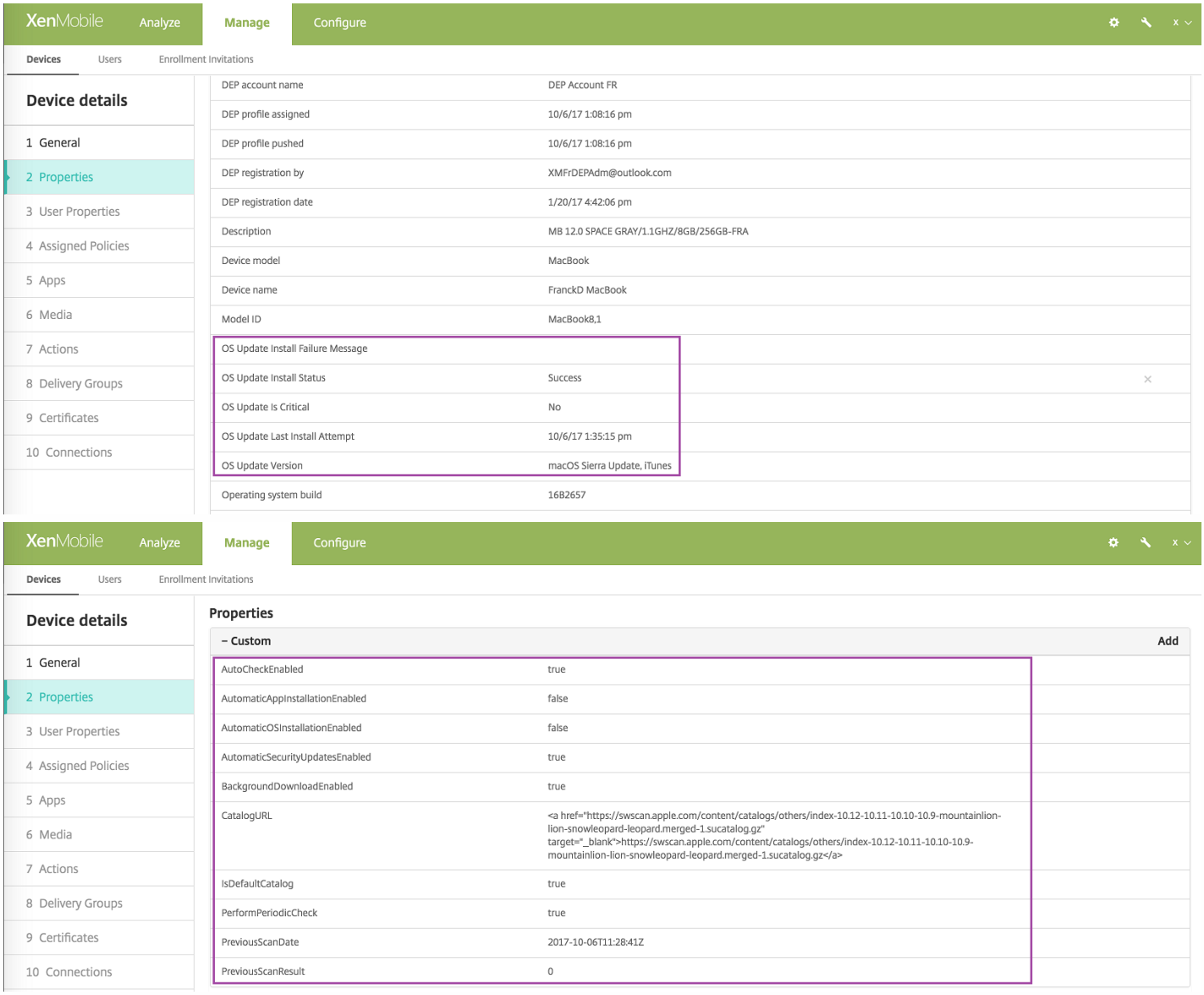


Para obter mais detalhes sobre o status das ações de atualização, vá para a página **Gerenciar > Dispositivos > Detalhes do dispositivo (Grupos de entrega)**.



Para obter detalhes como a lista de atualizações disponíveis do sistema operacional e a última tentativa de instalação, vá para a página **Gerenciar > Dispositivos > Detalhes do dispositivo (Propriedades)**.

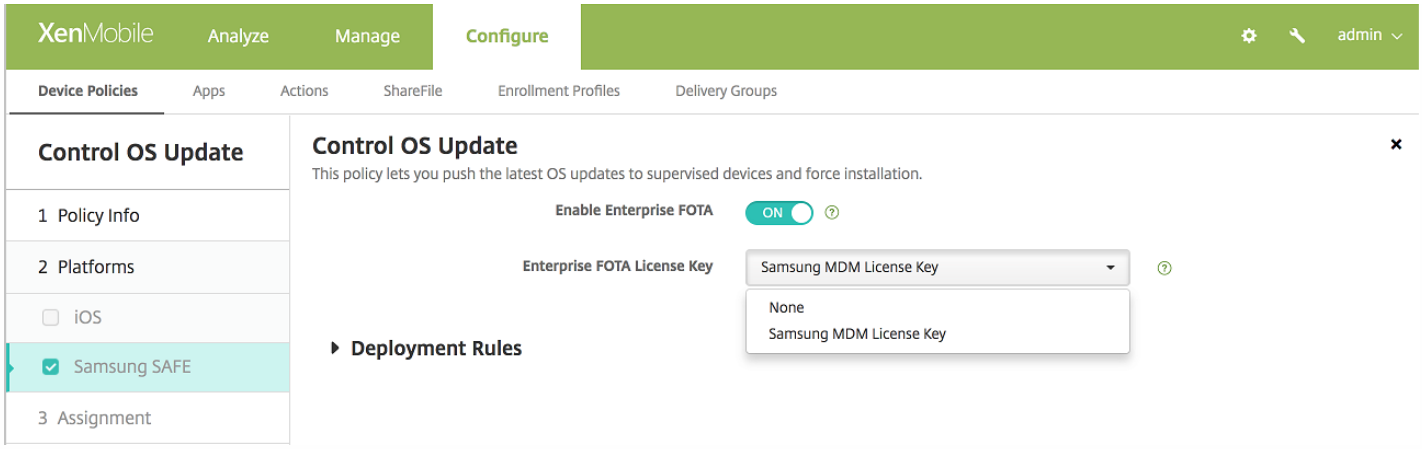
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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. Papara obter mais informações, consulte a Política de dispositivo de chave de licença MDM Samsung.
2. Crie uma política de dispositivo de controle de atualização do sistema operacional para habilitar o Enterprise FOTA.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- **Ativar Enterprise FOTA**: defina como **Ativado**.
- **Chave de licença Enterprise FOTA**: selecione o nome da política de dispositivo de chave de licença Samsung MDM.

Nota

Para obter informações gerais sobre como configurar políticas, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo Copiar aplicativos para o contêiner da Samsung

Feb 21, 2018

Você pode especificar os aplicativos que já estão instalados em um dispositivo a ser copiado para um contêiner do SEAMS ou para um contêiner do KNOX em dispositivos Samsung com suporte. Para obter informações sobre os dispositivos com suporte, consulte a página Dispositivos Samsung KNOX com suporte da Samsung. Os aplicativos copiados para o contêiner do SEAMS estão disponíveis nas telas iniciais dos usuários; os aplicativos copiados para o contêiner do KNOX estão disponíveis somente quando os usuários fazem login no contêiner do KNOX.

Pré-requisitos:

- O dispositivo deve estar registrado no XenMobile.
- As chaves de MDM Samsung (ELM e KLM) devem ser implantadas. Para saber como fazer isso, consulte as políticas de dispositivo Chave de Licença MDM Samsung.
- Os aplicativos já estão instalados no dispositivo
- Inicialize o KNOX no dispositivo para copiar os aplicativos para o contêiner do KNOX.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Expanda **Mais** e, em **Segurança**, clique em **Copiar aplicativos para o contêiner da Samsung**. A página de informações **Política de copiar aplicativos para o contêiner da Samsung** é exibida.

4. No painel **Informações sobre a política**, insira as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma de política** é exibida.

6. Em Plataformas, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 8 para saber como definir as regras de implantação dessa plataforma.

7. Defina a configuração a seguir para cada plataforma selecionada.

- **Novo aplicativo**: para cada aplicativo que você desejar adicionar à lista, clique em **Adicionar** e faça o seguinte:
  - Digite um ID de pacote; por exemplo, com.mobiwolf.lacingart para o aplicativo LacingArt.
  - Clique em **Salvar** ou em **Cancelar**.

    Nota: para excluir um aplicativo 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 aplicativo existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à

© 1999-2017 Citrix Systems, Inc. All rights reserved.

direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

8.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de credenciais

Feb 21, 2018

Você pode criar políticas de dispositivo de credenciais no XenMobile para ativar a autenticação integrada com sua configuração de PKI no XenMobile, como uma entidade PKI, um keystore, um provedor de credenciais ou um certificado de servidor. Para obter mais informações sobre as credenciais, consulte Certificados.

Você pode criar as políticas de credenciais para dispositivos com iOS, macOS, Android, Android for Work, desktop/tablet Windows, Windows Mobile/CE e Windows Phone. Cada plataforma exige um conjunto diferente de valores, que são descritos neste artigo.

Configurações do iOS

Configurações do macOS

Configurações do Android e do Android for Work

Configurações do Windows Desktop/Tablet

Configurações do Windows Mobile/CE

Configurações do Windows Phone

Antes de criar esta política, você precisa ter as informações de credencial que planeja usar para cada plataforma, além de quaisquer certificados e senhas.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. A caixa de diálogo **Adicionar uma nova política** é exibida.

3. Expanda **Mais** e, em **Segurança**, clique em **Credenciais**. A página de informações sobre a **Política de credenciais** é exibida.

4. No painel **Informações sobre a política**, digite as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

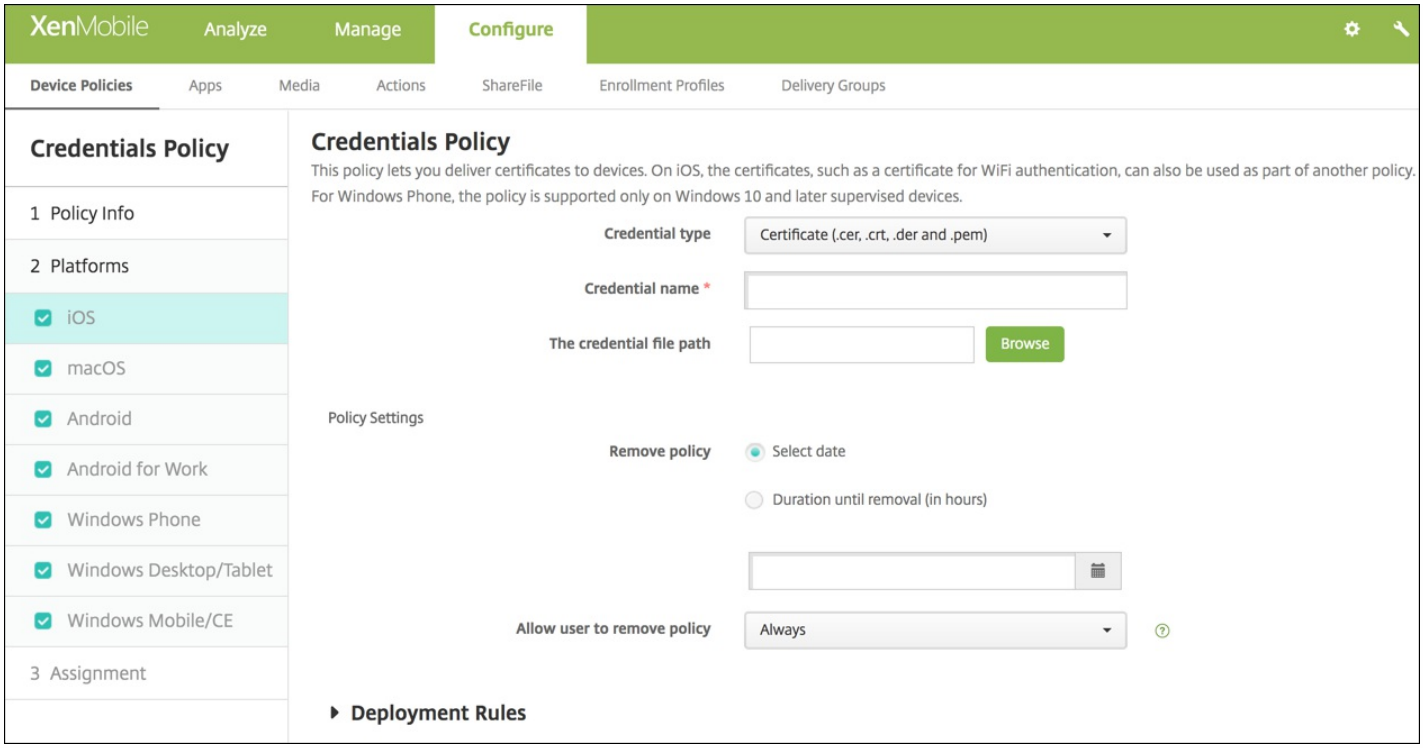
5. Clique em **Avançar**. A página **Plataforma de política** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

Definir as configurações do iOS

© 1999-2017 Citrix Systems, Inc. All rights reserved.

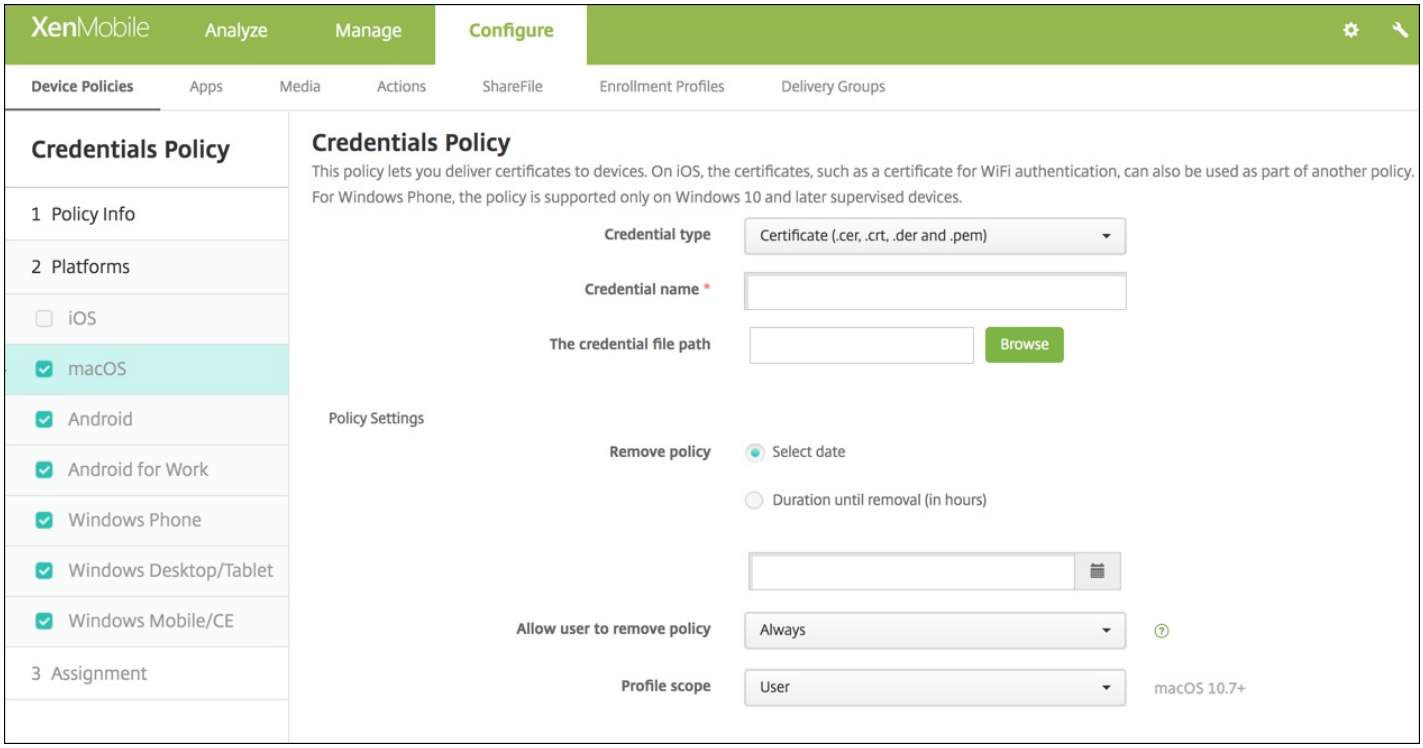


Faça as seguintes configurações:

- **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**
  - 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 de perfil**, digite a senha necessária.

Defina as configurações do macOS

© 1999-2017 Citrix Systems, Inc. All rights reserved.

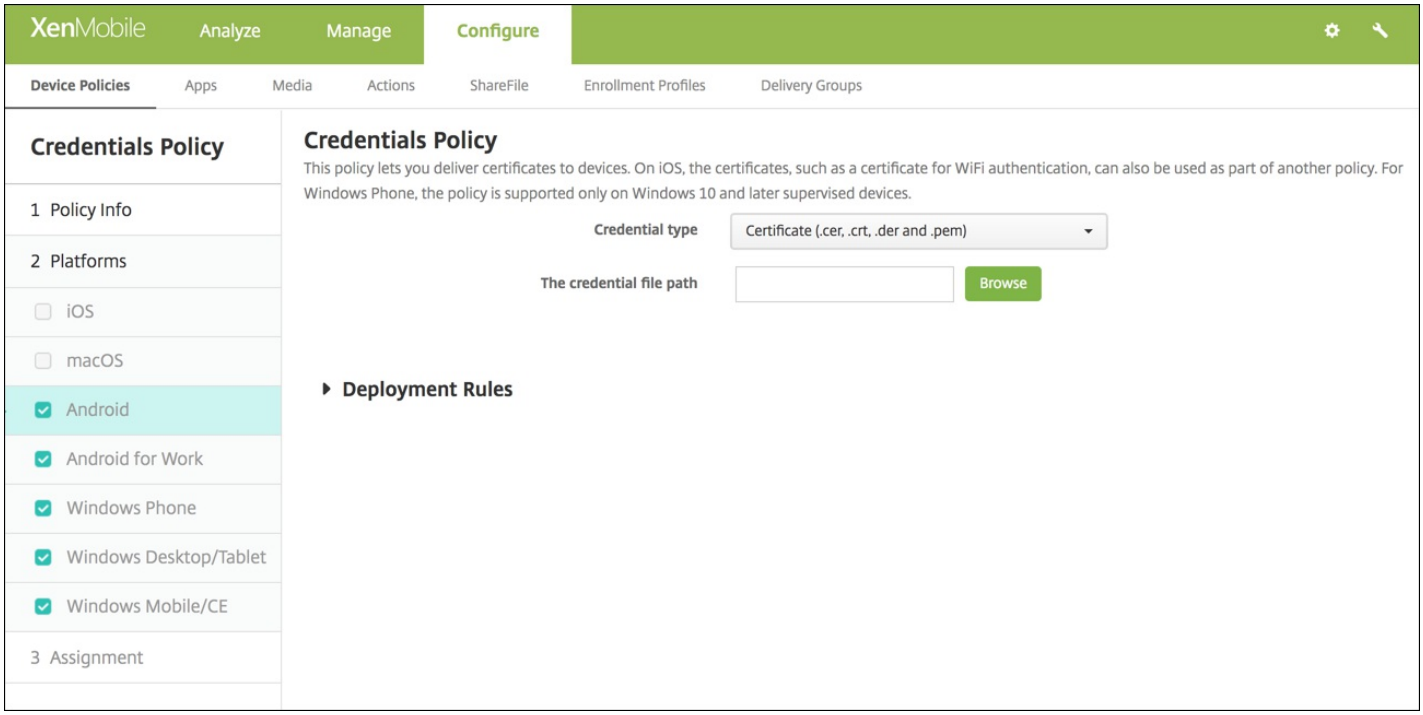


Faça as seguintes configurações:

- **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 até 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 até 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**
  - 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 de perfil**, digite a senha necessária.
  - Ao lado de **Escopo do perfil**, clique em **Usuário** ou **Sistema**. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

Definir as configurações do Android e do Android for Work

© 1999-2017 Citrix Systems, Inc. All rights reserved.

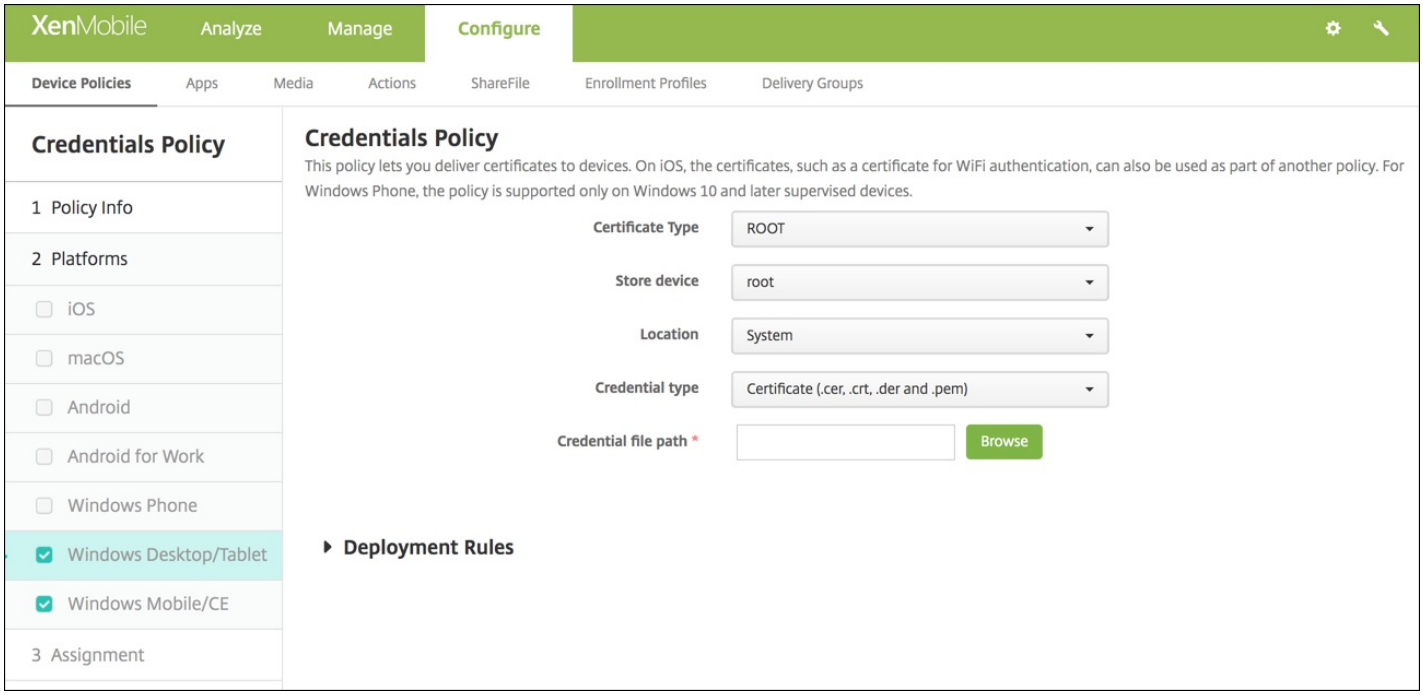


Faça as seguintes configurações:

- **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.

Definir as configurações do Windows Desktop/Tablet

© 1999-2017 Citrix Systems, Inc. All rights reserved.

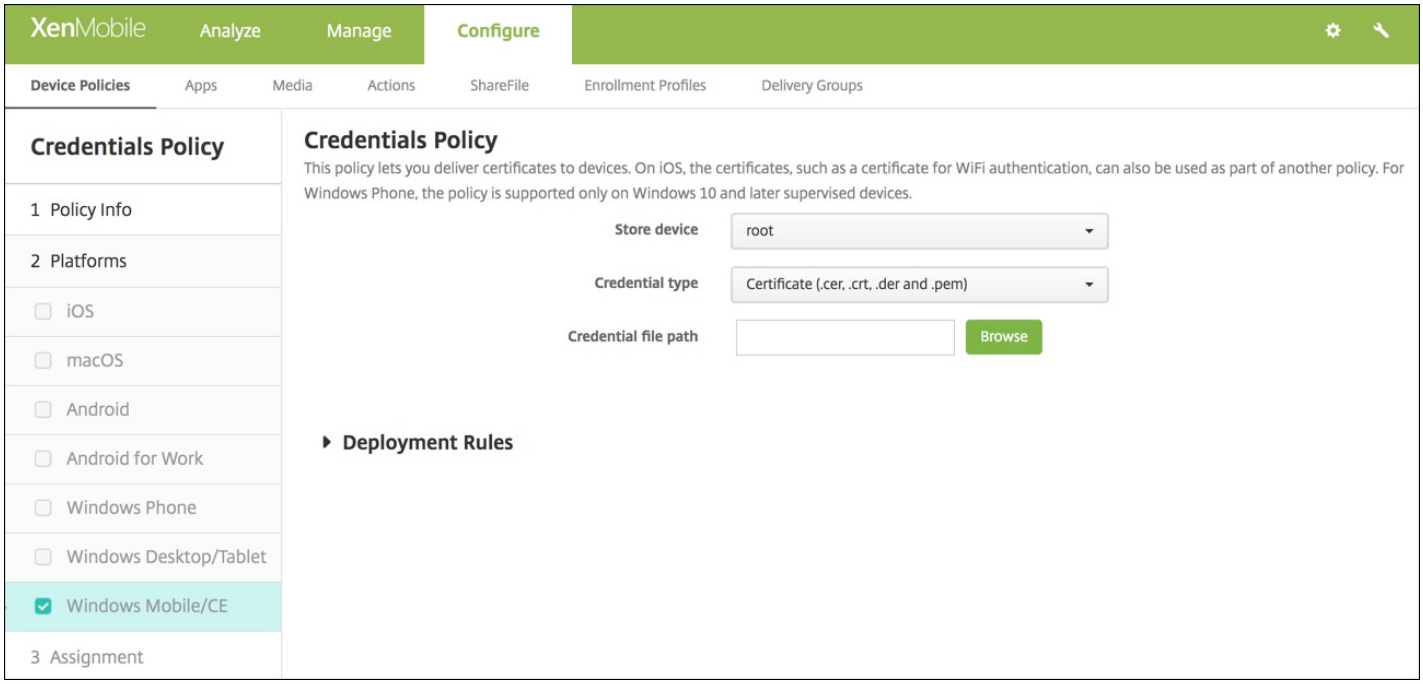


Faça as seguintes configurações:

- **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**: **Sistema** é a única localização dos tablets Windows 10.
  - **Tipo de credencial**: **Certificado** é o único tipo de credencial dos tablets Windows 10.
  - **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**: **Sistema** é a única localização dos tablets Windows 10.
- **Tipo de credencial**: **Keystore** é o único tipo de credencial dos tablets Windows 10.
- **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.

Definir as configurações do Windows Mobile/CE

© 1999-2017 Citrix Systems, Inc. All rights reserved.

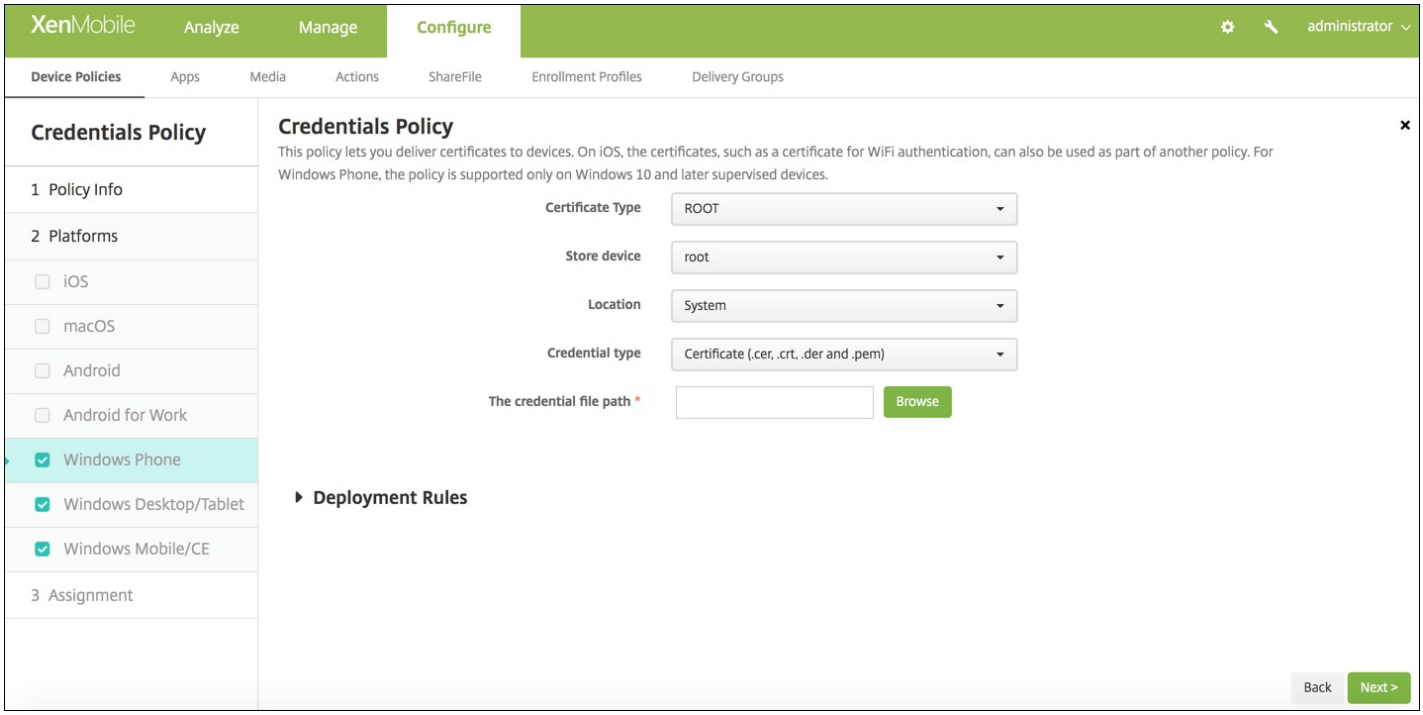


Faça as seguintes configurações:

- **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 essa loja serão executados com nível de confiança normal.
  - **SPC (Certificado de Editor de Software)** — é usado para assinar arquivos .cab.
  - **raiz** — um repositório de certificados que contém certificados raiz ou autoassinados.
  - **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.

Definir as configurações do Windows Phone

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Faça as seguintes configurações:

- **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**: Sistema é a única localização no caso de telefones Windows.
  - **Tipo de credencial**: Certificado é o único tipo de credencial dos telefones Windows.
  - **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**: **Sistema** é a única localização no caso de telefones Windows.
  - **Tipo de credencial**: **Keystore** é o único tipo de credencial dos telefones Windows.
  - **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.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de XML personalizado

Feb 21, 2018

Você pode criar políticas de XML personalizado no XenMobile para personalizar os seguintes recursos em dispositivos Windows e Android Zebra com suporte:

- 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

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 da Microsoft Developer Network.

Para dispositivos Android Zebra, 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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. A caixa de diálogo **Adicionar uma nova política** é exibida.

3. Expanda **Mais** e, em **Personalizado**, clique em **XML personalizado**. A página de informações **Política de XML personalizado** é exibida.

4. No painel **Informações sobre a política**, insira as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma de política** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

7. Defina a seguinte configuração para cada plataforma selecionada:

- **Conteúdo XML**: digite ou recorte e cole o código XML personalizado que você desejar adicionar à política.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

8. Configure as regras de implantação Para obter mais informações, consulte Adicionar uma política de dispositivo.

9. Clique 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.

10. Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega. Ou selecione um ou mais grupos na lista para os quais deseja atribuir a política. 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:

- Ao lado de **Implantar**, clique em **I** para agendar a implantação ou em **O** para impedi-la. A opção padrão é **I**.
- Ao lado de **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 se aplicará 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.

12. Clique em **Salvar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo do Defender

Feb 21, 2018

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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

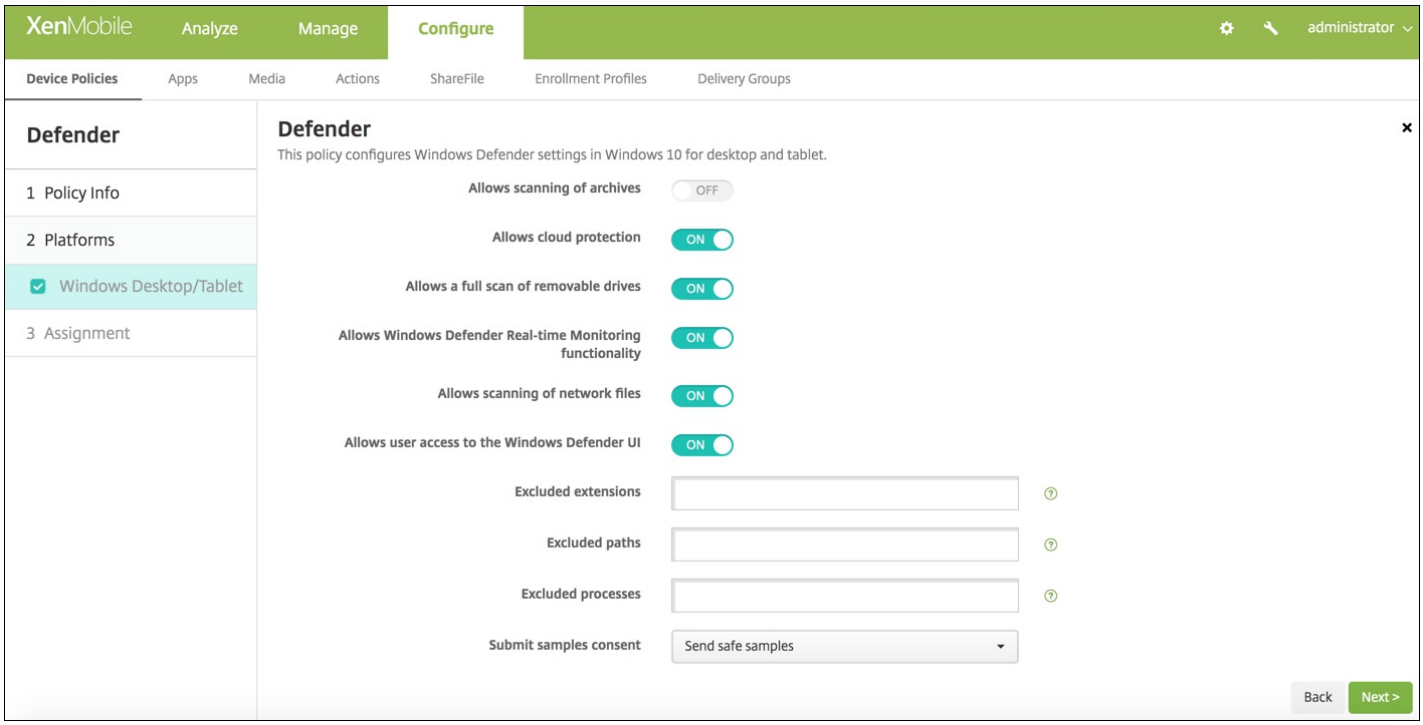
2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Comece a digitar **Defender** e, em seguida, clique nesse nome nos resultados da pesquisa. A página de informações **Política do Defender** é exibida.

4. No painel **Informações sobre a política**, digite 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 **Plataforma de política** é exibida.



Defina estas configurações:

- **Permite exame de arquivos**: permite ou proíbe que o Defender examine arquivos armazenados. O padrão é **O**.
- **Permite proteção da nuvem**: permite ou proíbe que o Defender envie informações à Microsoft sobre atividades de malware. O padrão é **I**.
- **Permite exame completo de unidades removíveis**: permite ou proíbe que o Defender examine unidades removíveis, como pen drives. O padrão é **I**.
- **Permite funcionalidade de monitoramento em tempo real do Windows Defender**: o padrão é **I**.
- **Permite exame de arquivos de rede**: permite ou proíbe que o Defender examine arquivos de rede. O padrão é **I**.
- **Permite o acesso do usuário à interface de usuário do Windows Defender**: especifica se os usuários podem

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 **O**, os usuários não receberão notificações do Windows Defender. O padrão é **I**.

- **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**.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de excluir arquivos e pastas

Feb 21, 2018

Você pode criar uma política no XenMobile para excluir arquivos e pastas específicos dos dispositivos Windows Mobile/CE.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. A caixa de diálogo **Adicionar uma nova política** é exibida.

3. Expanda **Mais** e, em **Aplicativos**, clique em **Excluir arquivos e pastas**. A página de informações **Política de Excluir arquivos e pastas** é exibida.

4. No painel **Informações sobre a política**, digite as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma Windows Mobile/CE** é exibida.

6. Defina estas configurações:

- **Arquivos e pastas a serem excluídos**: para cada arquivo ou pasta que você desejar 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.

    Observação: para excluir uma listagem 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 uma listagem existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo Excluir chaves e valores do Registro

Feb 21, 2018

Você pode criar uma política no XenMobile para excluir chaves e valores específicos do Registro dos dispositivos Windows Mobile/CE.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. A caixa de diálogo **Adicionar uma nova política** é exibida.

3. Expanda **Mais** e, em **Aplicativos**, clique em **Excluir chaves e valores do registro**. A página de informações **Política de excluir chaves e valores do registro** é exibida.

4. No painel **Informações sobre a política**, digite as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma Windows Mobile/CE** é exibida.

6. Defina estas configurações:

- **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.

    Observação: para excluir uma listagem 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 uma listagem existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de Atestado de Integridade de Dispositivo

Feb 21, 2018

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 DEP
- Driver ELAM carregado
- Emitido em
- Depuração de kernel ativada
- PCR
- Redefinir contagem
- Reiniciar contagem
- Modo de segurança ativado
- Hash SBCP
- Inicialização segura ativada
- Sinalização de teste ativada
- VSM ativado
- WinPE ativado

Para obter mais informações, consulte a página HealthAttestation CSP da Microsoft.

Para configurar DHA usando o Microsoft Cloud

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar** para adicionar uma nova política. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Clique em **Mais** e, em **Personalizado**, clique em **Política de atestado de integridade de dispositivo**. A página de informações sobre a **Política de atestado de integridade de dispositivo** é exibida.

4. No painel **Informações sobre a política**, insira as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma de política** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

Configure esta definição para cada plataforma selecionada:

- **Ativar atestado de integridade de dispositivo**: selecione se pretende exigir o Atestado de integridade de dispositivo. O padrão é **O**.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

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.

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.

Para configurar o DHA usando um servidor DHA do Windows no local:

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página Políticas de dispositivo é exibida.

2. Se você já criou uma política para habilitar o DHA através do Microsoft Cloud, vá para a etapa 8.

3. Clique em **Adicionar** para adicionar uma nova política. É exibida a caixa de diálogo **Adicionar uma nova política**.

4. Clique em **Mais** e, em **Personalizado**, clique em **Política de atestado de integridade de dispositivo**. A página de informações sobre a **Política de atestado de integridade de dispositivo** é exibida.

5. No painel Informações sobre a política, insira as seguintes informações:

   Nome da política: digite um nome descritivo para a política.

   Descrição: digite uma descrição opcional para a política.

6. Clique em **Avançar**. A página **Plataforma de política** é exibida.

7. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

8. Para cada plataforma escolhida:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

a. Defina **Ativar atestado de integridade do dispositivo** como **Ativar**.

b. Defina **Configurar o serviço de atestado de integridade local** como **Ativar**.

c. Em **FQDN do Serviço DHA no local**, insira o nome de domínio totalmente qualificado do servidor DHA que você configurou.

d. Em **Versão da API DHA local**, escolha a versão do serviço DHA instalado no servidor DHA.

9. Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de nome do dispositivo

Feb 21, 2018

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 mais informações sobre macros, consulte Macros no XenMobile.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. A página **Adicionar uma nova política** é exibida.

3. Expanda **Mais** e, em **Usuário final**, clique em **Nome do dispositivo**. A página de informações **Política de nome de dispositivo** é exibida.

4. No painel **Informações sobre a política**, digite as seguintes informações:

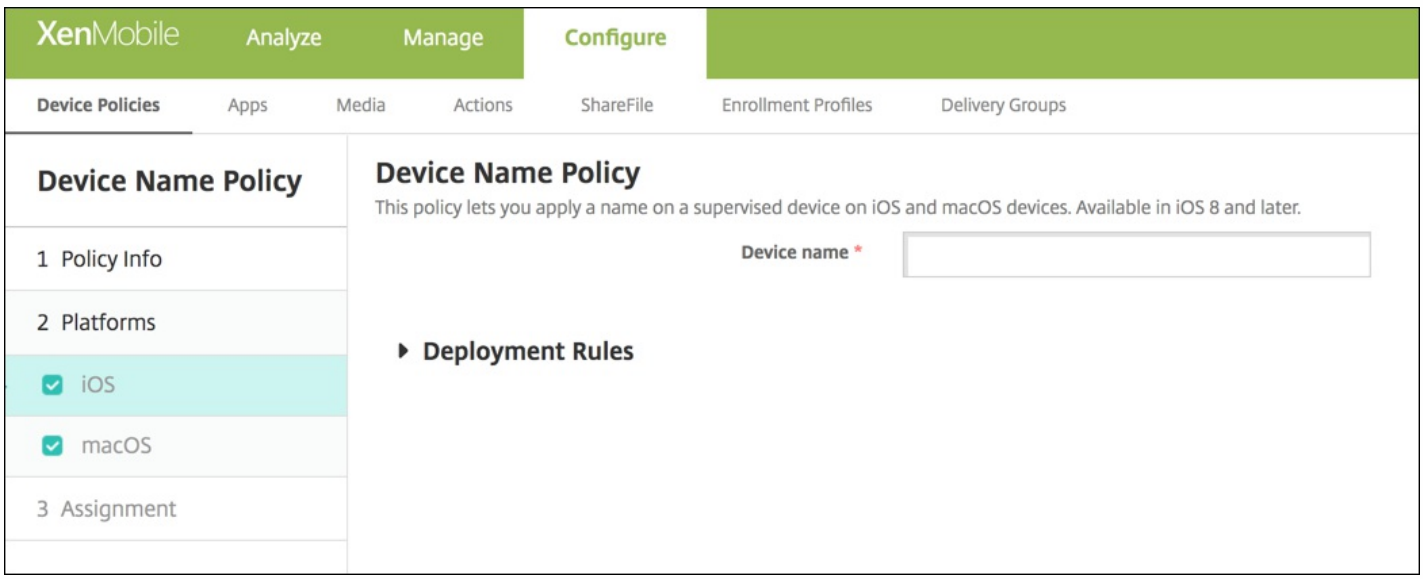
- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma de política** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

Definir as configurações do macOS e do iOS



Defina esta configuração para as plataformas que você escolher:

- **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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

número de série de cada dispositivo ou use ${device.serialnumber} ${user.username} para incluir o nome do usuário no nome do dispositivo.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo Configuração de Educação

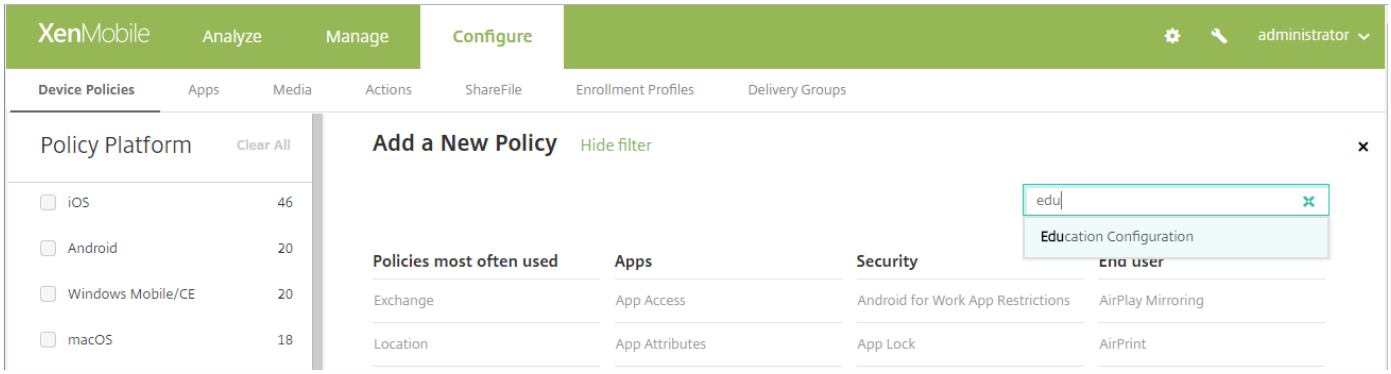
Feb 21, 2018

A Política de dispositivo Configuração de Educação define:

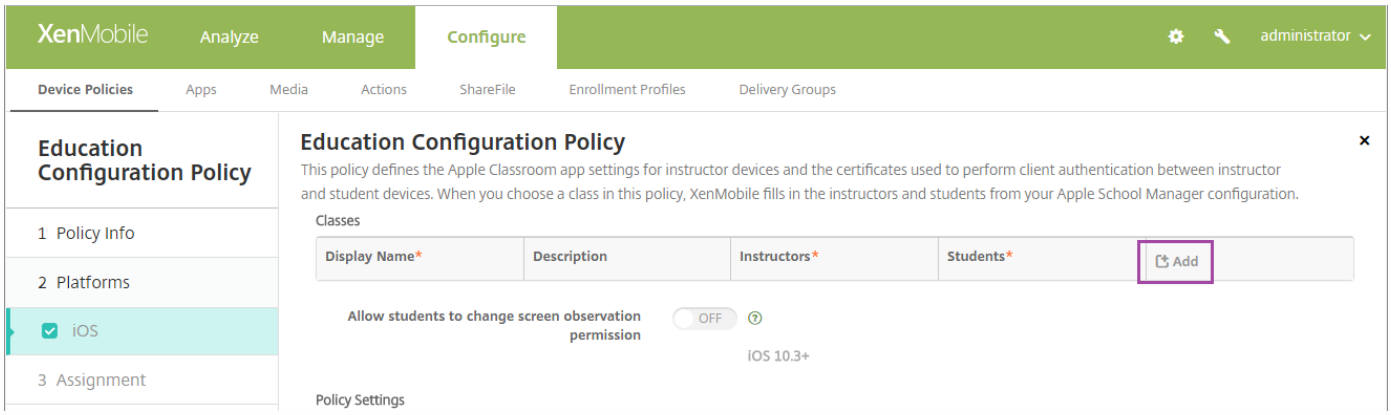
- As configurações de aplicativo Sala de Aula da Apple para dispositivos de instrutores.
- Os certificados usados para realizar a autenticação de cliente entre os dispositivos do instrutor e do aluno.

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.

1. No console XenMobile, vá para **Configurar > Políticas de dispositivo** e clique em **Adicionar**.
2. Na caixa de pesquisa, comece a digitar **educação** e clique em **Configuração de Educação**.

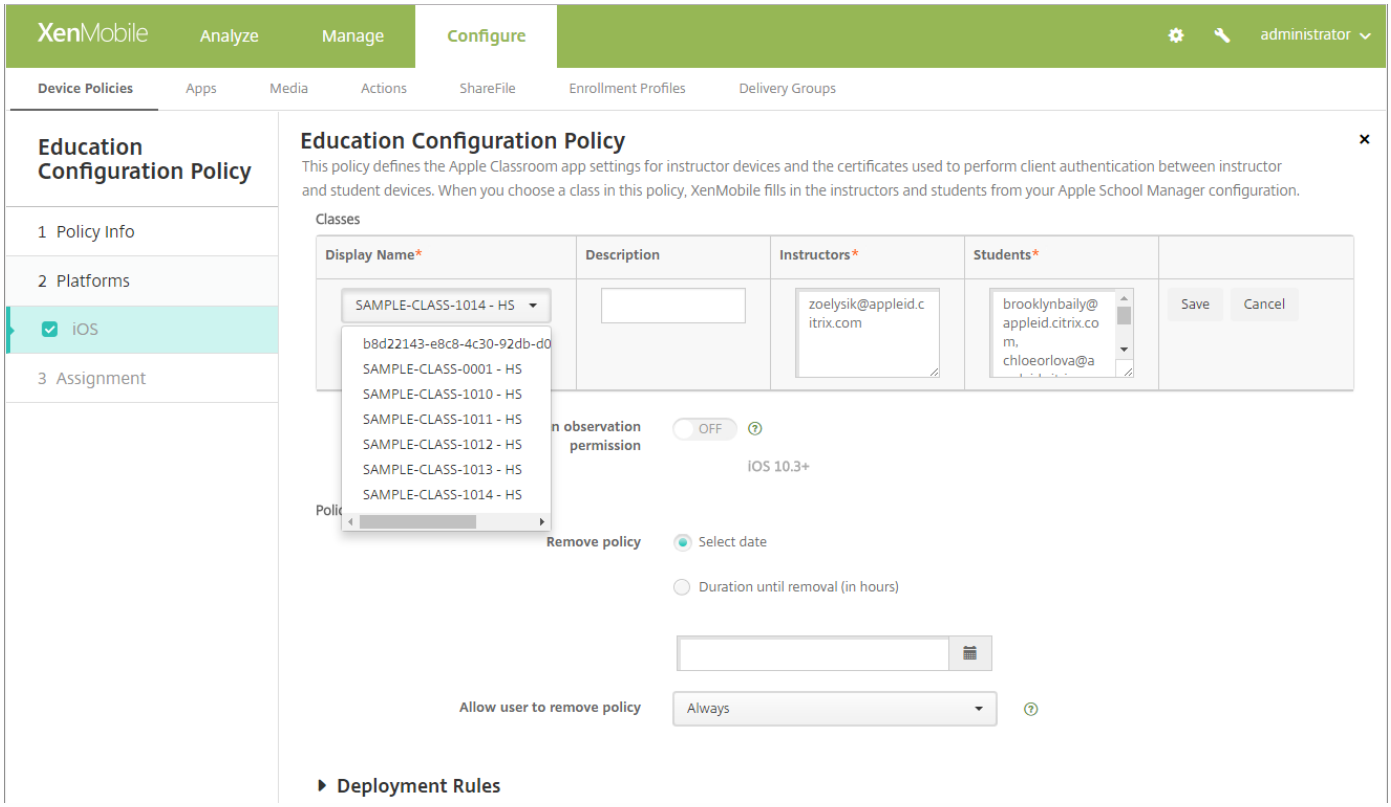


3. Na página **Informações sobre a Política**, digite um **Nome da Política** para identificar a política no XenMobile.
4. Na página **Política de Configuração de Educação**, clique em **Adicionar**.

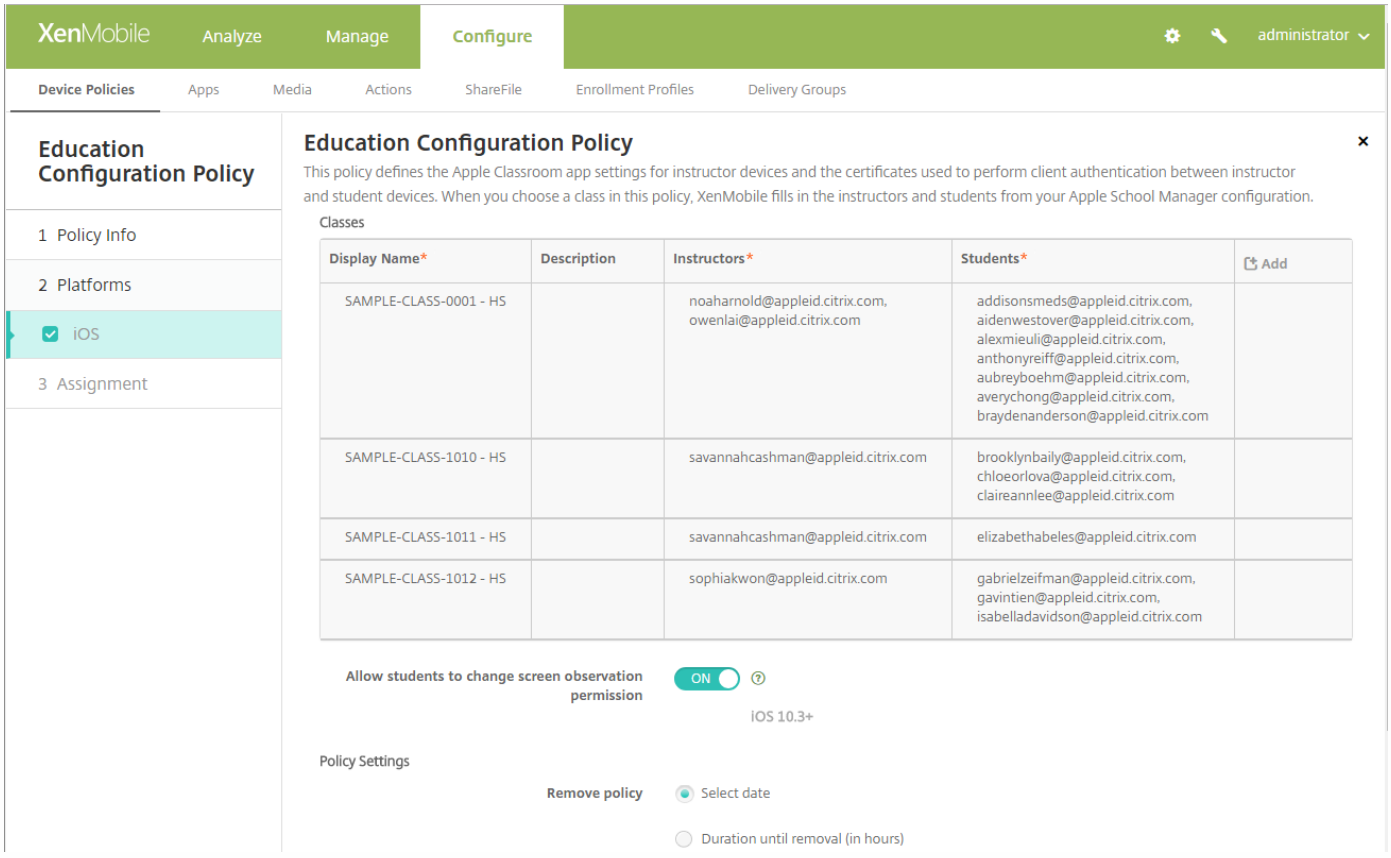


5. Clique na lista **Nome de Exibição**. É exibida uma lista de classes obtidas da sua conta do Apple School Manager conectada.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Quando você escolhe uma classe de **nome de exibição**, o XenMobile preenche as informações de instrutores e alunos. Continue adicionando classes.

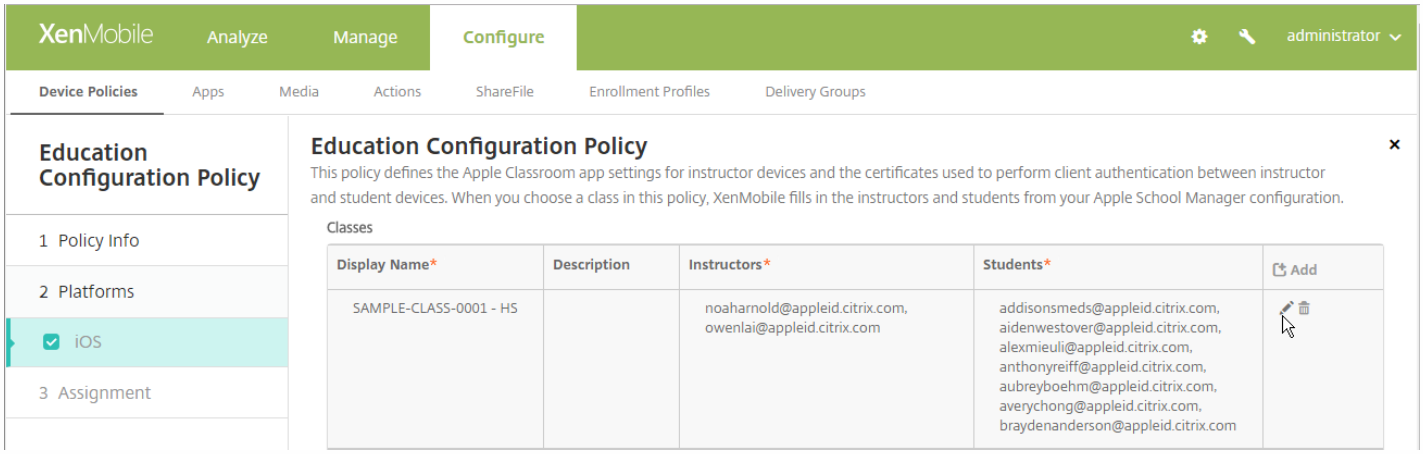


Para editar as informações de classe na política

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 Server 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 da Apple Educação.

Passe o mouse sobre a coluna **Adicionar** da classe que deseja editar e, em seguida, clique no ícone de lápis.



Para excluir uma classe da política, passe o mouse sobre a coluna **Adicionar** da classe que deseja excluir e clique no ícone de lixeira.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo do Hub Empresarial

Feb 21, 2018

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 Symantec
- O aplicativo Citrix Company Hub assinado usando a ferramenta de assinatura de aplicativos da Microsoft (XapSignTool.exe)

Observação: 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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

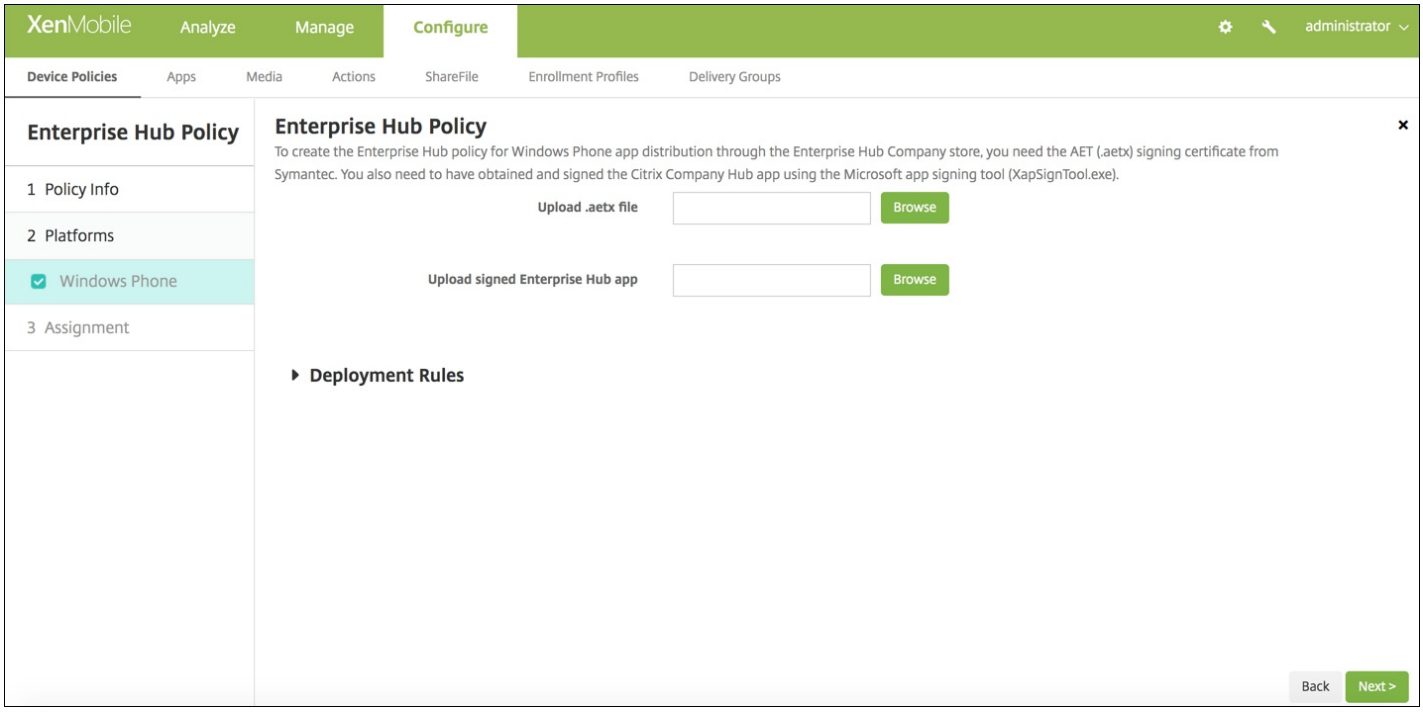
2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Expanda **Mais** e, em **Agente XenMobile**, clique em **Hub Empresarial**. A página **Política de hub empresarial** é exibida.

4. No painel **Informações sobre a política**, digite as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página da plataforma **Windows Phone** é exibida.



6. Defina estas configurações:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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 arquivo.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo do Microsoft Exchange ActiveSync

Feb 21, 2018

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 HTC, Android TouchDown, Android for Work, 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.

iOS

macOS

Android HTC

Android TouchDown

Android for Work

Samsung SAFE e Samsung KNOX

Windows Phone e Windows Desktop/Tablet

Para criar essa política, você precisa saber o nome de host ou endereço IP do Exchange Server. Para obter informações sobre as configurações do ActiveSync, consulte o artigo da Microsoft ActiveSync CSP.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Clique em **Exchange**. A página de informações **Política do Exchange** é exibida.

4. No painel **Informações sobre a política**, digite as seguintes informações:

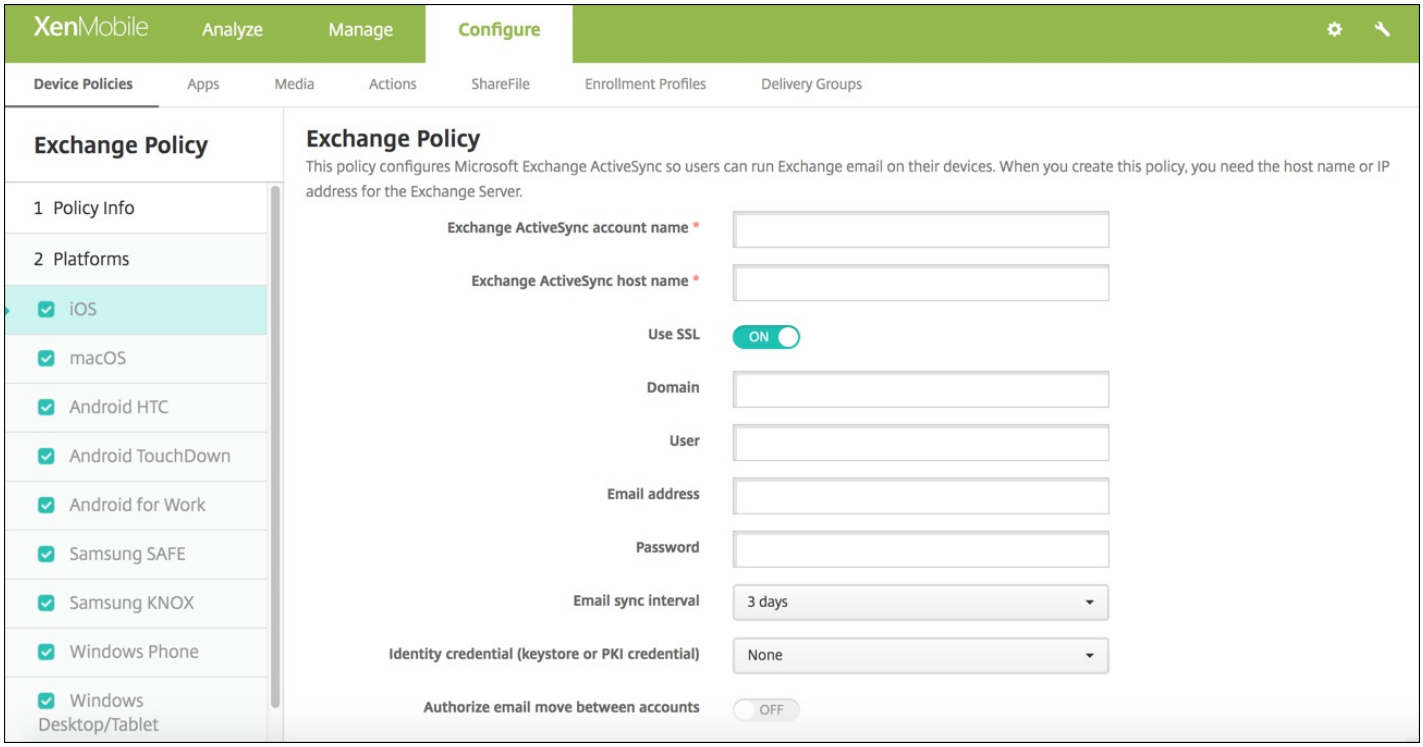
- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação.

Definir as configurações do iOS

© 1999-2017 Citrix Systems, Inc. All rights reserved.



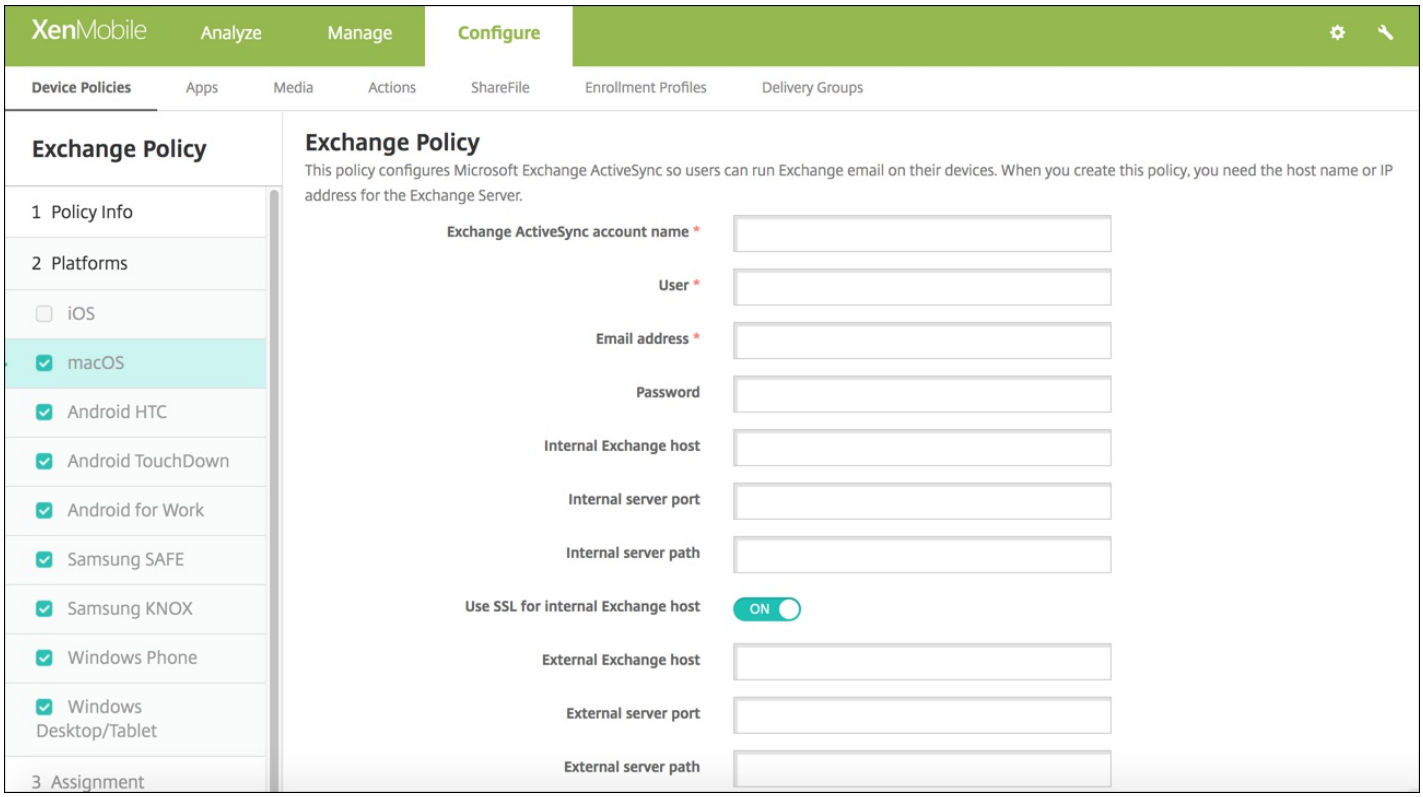
Defina estas configurações:

- **Nome de conta do Exchange ActiveSync**: digite a descrição da conta de email exibida nos dispositivos dos usuários.
- **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 **I**.
- **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.
- **Senha**: digite uma senha opcional para a conta de usuário do Exchange.
- **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 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 **O**.
- **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 **O**.
- **Desativar a sincronização de emails recentes**: selecione se os usuários devem ser impedidos de sincronizar endereços recentes. O padrão é **O**. Essa opção se aplica somente ao iOS 6.0 e versões posteriores.
- **Ativar S/MIME**: selecione se essa conta é compatível com a autenticação e a criptografia S/MIME. O padrão é **O**. Quando definido como **I**, os dois campos abaixo são exibidos.
  - **Credencial de identidade de assinatura**. O padrão é **Nenhum**.
  - **Credencial de identidade de criptografia**. O padrão é **Nenhum**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Ativar comutador de S/MIME por mensagem**: selecione se os usuários têm permissão para criptografar emails enviados a cada mensagem. O padrão é **O**.

Defina as configurações do macOS



Defina estas configurações:

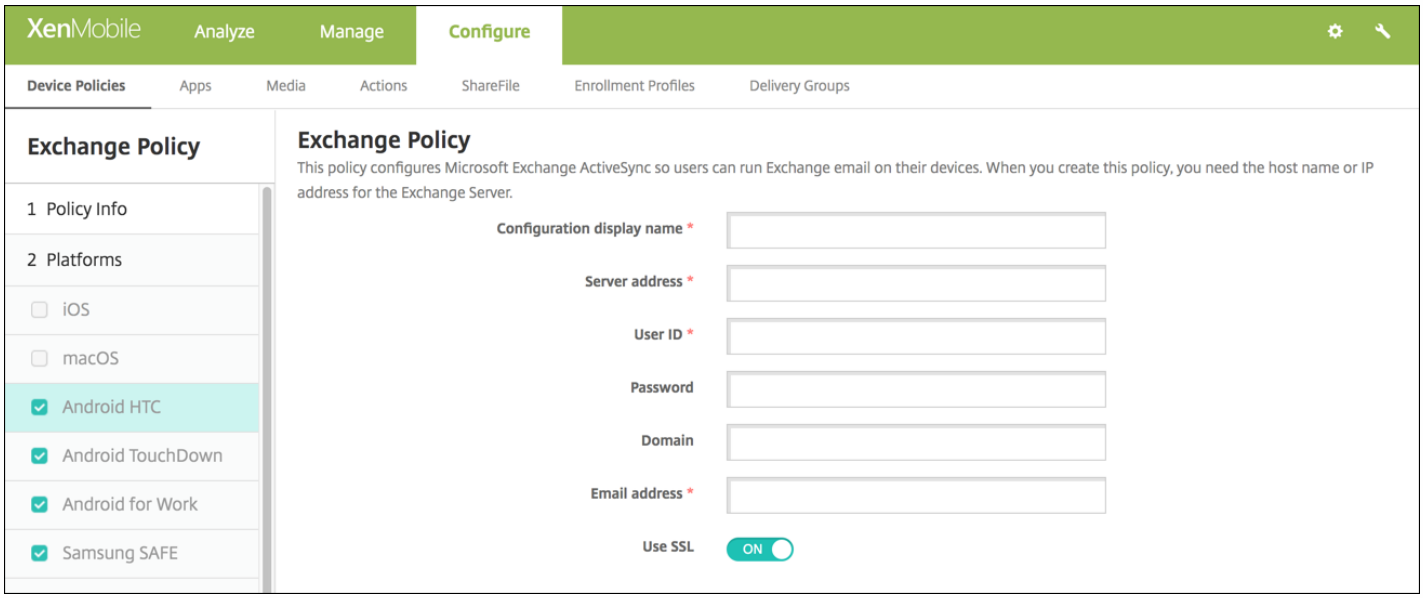
- **Nome de conta do Exchange ActiveSync**: digite a descrição da conta de email exibida nos dispositivos dos usuários.
- **Usuário**: especifique o nome do usuário da conta de usuário do Exchange. Você pode usar a macro de sistema $user.username nesse campo para procurar automaticamente os nomes dos 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.
- **Senha**: digite uma senha opcional para a conta de usuário do Exchange.
- **Host interno do Exchange**: se desejar que os nomes de host internos e externos 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 internas e externas do Exchange sejam diferentes, digite um número de porta de servidor interna do Exchange opcional.
- **Caminho de servidor interno**: se você desejar que os caminhos de servidor internos e externos 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 **I**.
- **Host externo do Exchange**: se você desejar que os nomes de host internos e externos do Exchange sejam diferentes, digite um nome de host externo do Exchange opcional.
- **Porta do servidor externo**: se você desejar que as portas de servidor internas e externas do Exchange sejam diferentes, digite um número de porta opcional do servidor externo do Exchange.
- **Caminho de servidor externo**: se você desejar que os caminhos de servidor internos e externos 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

do Exchange devem ser protegidas. O padrão é **I**.

- **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 **O**.

Definir as configurações do Android HTC

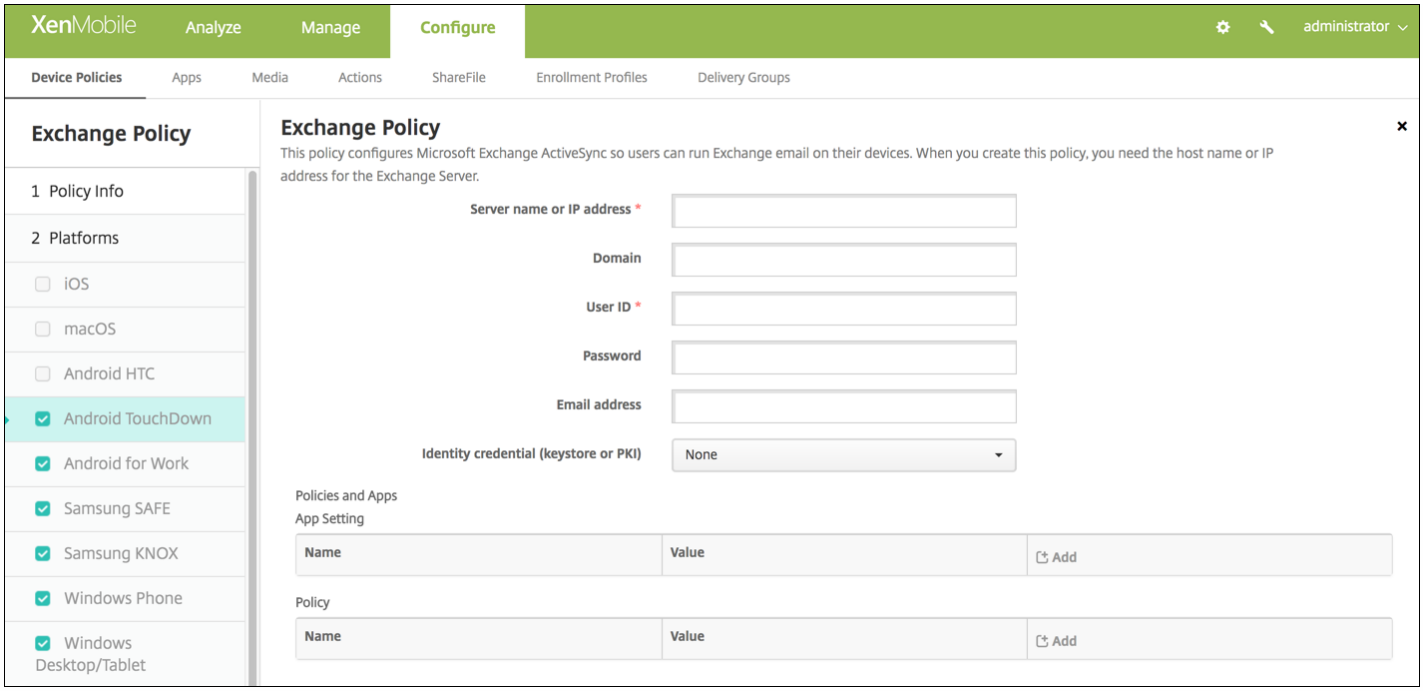


Defina estas configurações:

- **Nome para exibição da configuração**: digite o nome dessa política que aparece nos dispositivos dos usuários.
- **Endereço de servidor**: digite o nome de host ou o endereço IP do Exchange Server.
- **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.
- **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.
- **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 SSL**: selecione se as conexões entre os dispositivos dos usuários e o Exchange Server devem ser protegidas. O padrão é **I**.

Definir as configurações do Android TouchDown

© 1999-2017 Citrix Systems, Inc. All rights reserved.

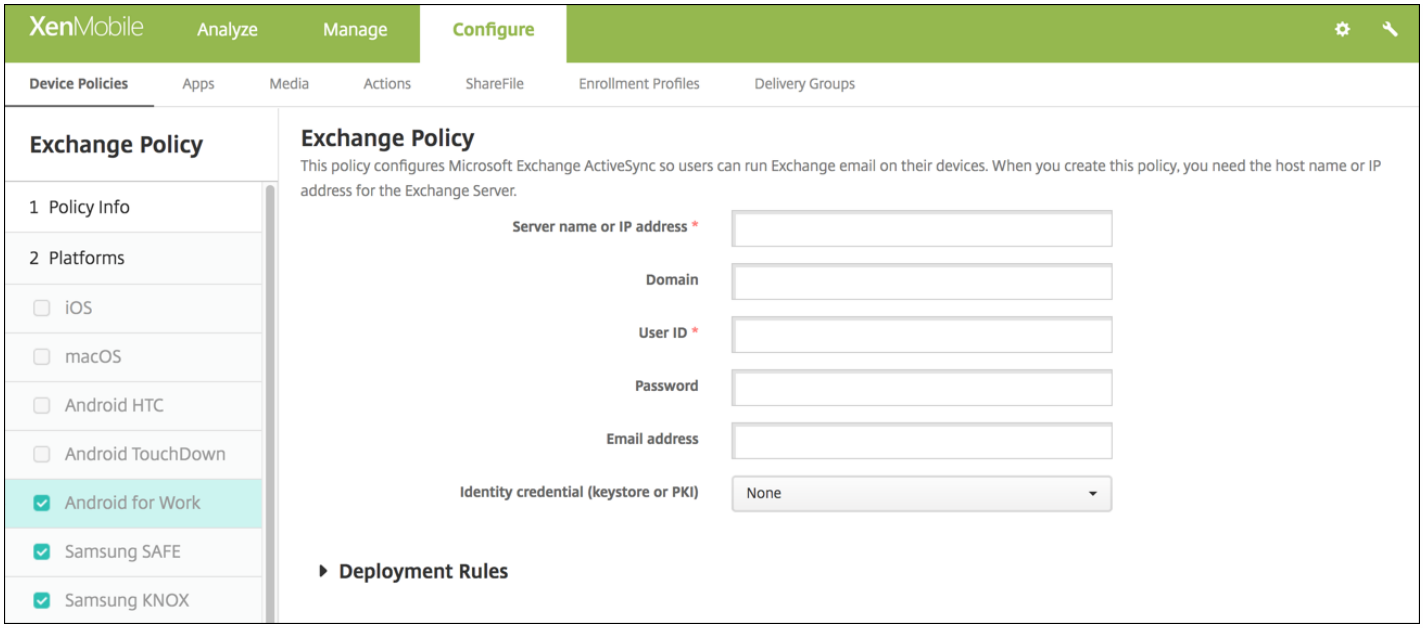


Defina estas configurações:

- **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**: insira 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 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**.
- **Configuração do aplicativo**: opcionalmente, adicione configurações de aplicativo TouchDown para essa política.
- **Política**: opcionalmente, adicione políticas do TouchDown para essa política.

Configurar o Android for Work

© 1999-2017 Citrix Systems, Inc. All rights reserved.

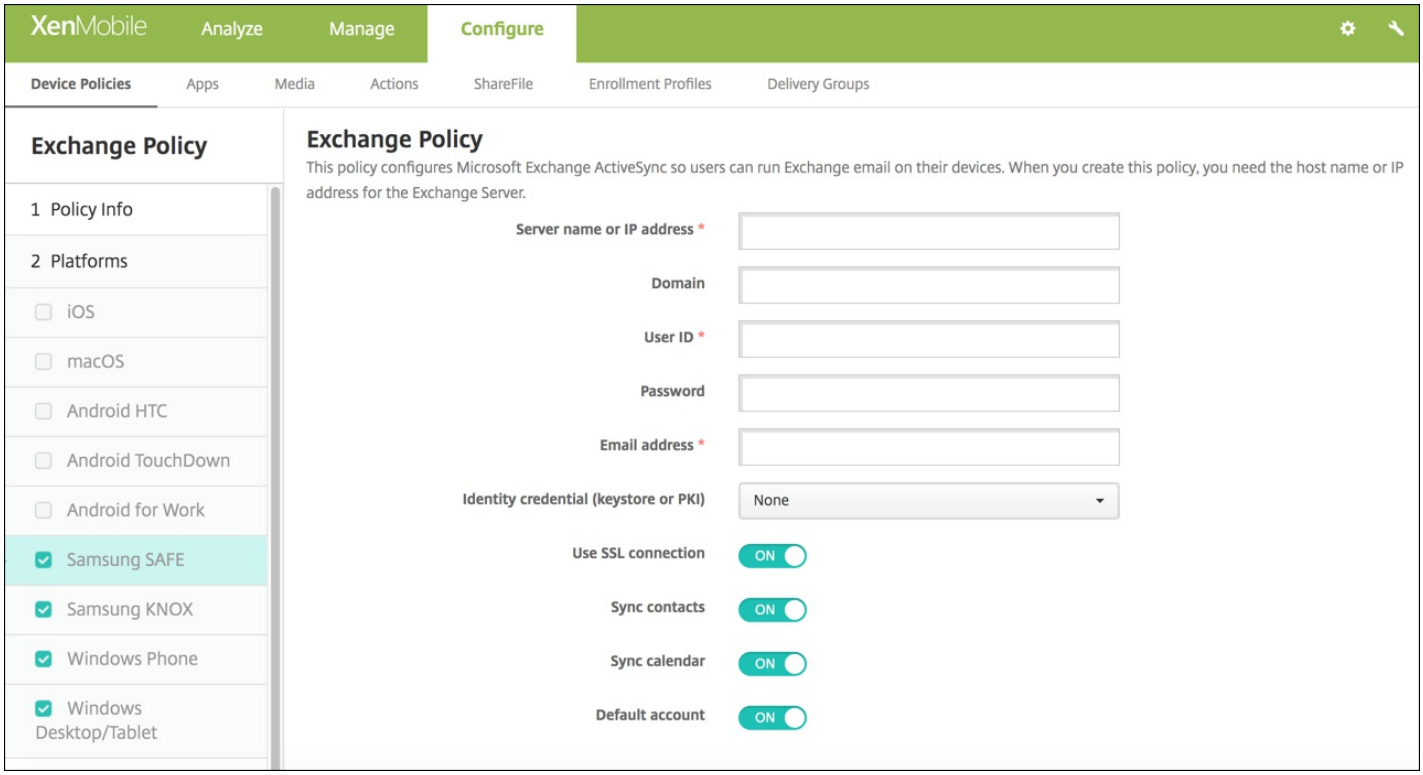


Defina estas configurações:

- **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**: insira 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**.

Definir as configurações do Samsung SAFE e do Samsung KNOX

© 1999-2017 Citrix Systems, Inc. All rights reserved.

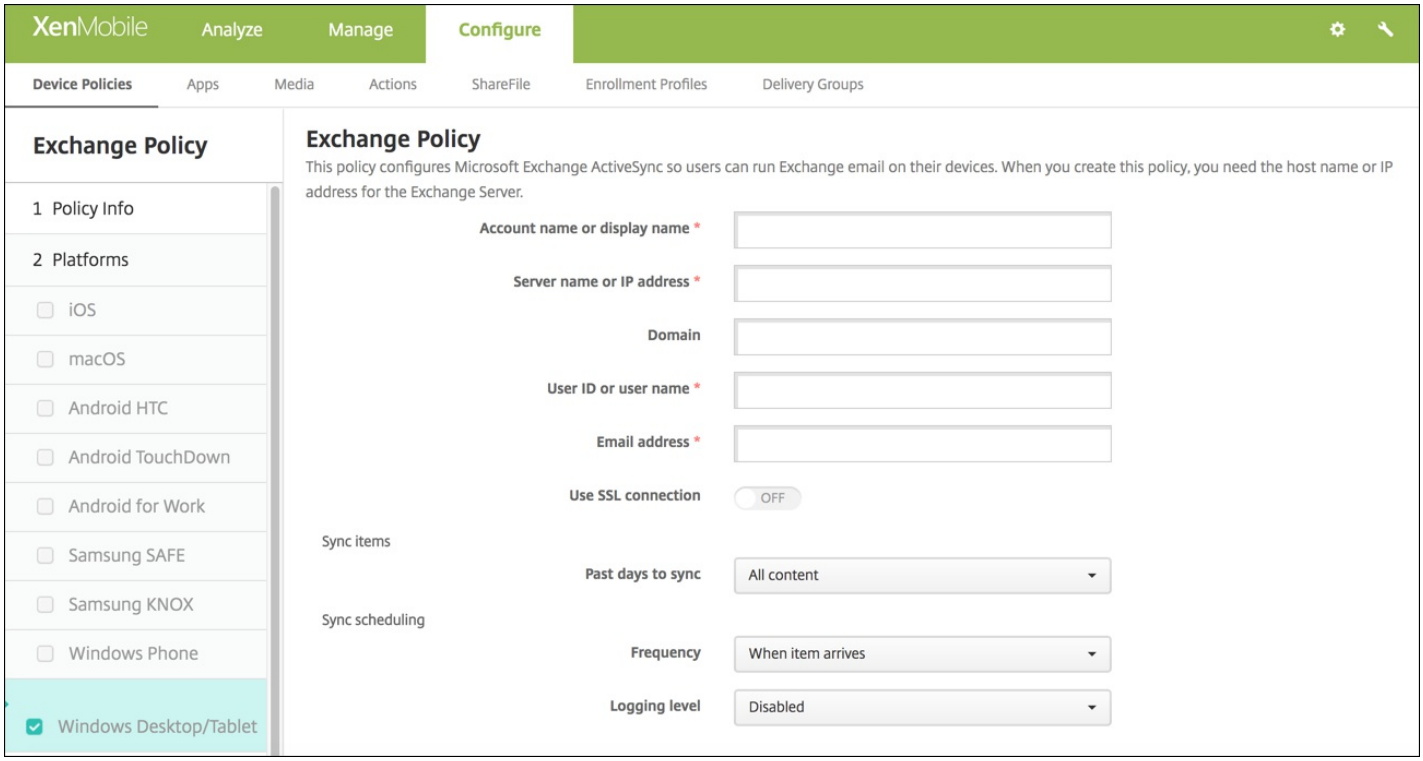


Defina estas configurações:

- **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**: insira 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 **l**.
- **Sincronizar os contatos**: selecione se a sincronização dos contatos dos usuários entre os dispositivos e o Exchange Server deve ser ativada. O padrão é **l**.
- **Sincronizar o calendário**: selecione se a sincronização do calendário dos usuários entre os dispositivos e o Exchange Server deve ser ativada. O padrão é **l**.
- **Conta padrão**: selecione se as contas do Exchange dos usuários devem ser o padrão para envio de email dos respectivos dispositivos. O padrão é **l**.

Definir as configurações do Windows Phone e do Windows Desktop/Tablet

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Defina estas configurações:

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 **O**.
- **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 o item**.
- **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**.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de arquivo

Feb 21, 2018

Você pode adicionar arquivos de script ao XenMobile para realizar determinadas funções para os usuários, ou pode adicionar arquivos de documento que você deseja que os usuários de dispositivos Android consigam acessar nos dispositivos deles. Quando você adiciona o arquivo, pode também especificar o diretório no qual deseja que o arquivo seja armazenado no dispositivo. Por exemplo, se você desejar que os usuários Android recebam um arquivo de documento ou .pdf da empresa, poderá implantar o arquivo no dispositivo e avisar aos usuários onde o arquivo está localizado.

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

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Expanda **Mais** e, em **Aplicativos**, clique em **Arquivos**. A página de informações **Política de navegador** é exibida.

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 **Plataforma de política** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

Definir as configurações do Android

Faça as seguintes configurações:

- **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**. Quando você seleciona **Script**, **Executar imediatamente** é exibido. Selecione se o script deve ser executado quando o arquivo é carregado. O padrão é **O**.
- **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 **O**.
- **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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Definir as configurações do Windows Mobile/CE

Faça as seguintes configurações:

- **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**. Quando você seleciona **Script**, **Executar imediatamente** é exibido. Selecione se o script deve ser executado quando o arquivo é carregado. O padrão é **O**.
- **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 **O**.
- **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 **O**.
- **Arquivo oculto**: selecione se o arquivo não deve ser mostrado na lista de arquivos. O padrão é **O**.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo FileVault

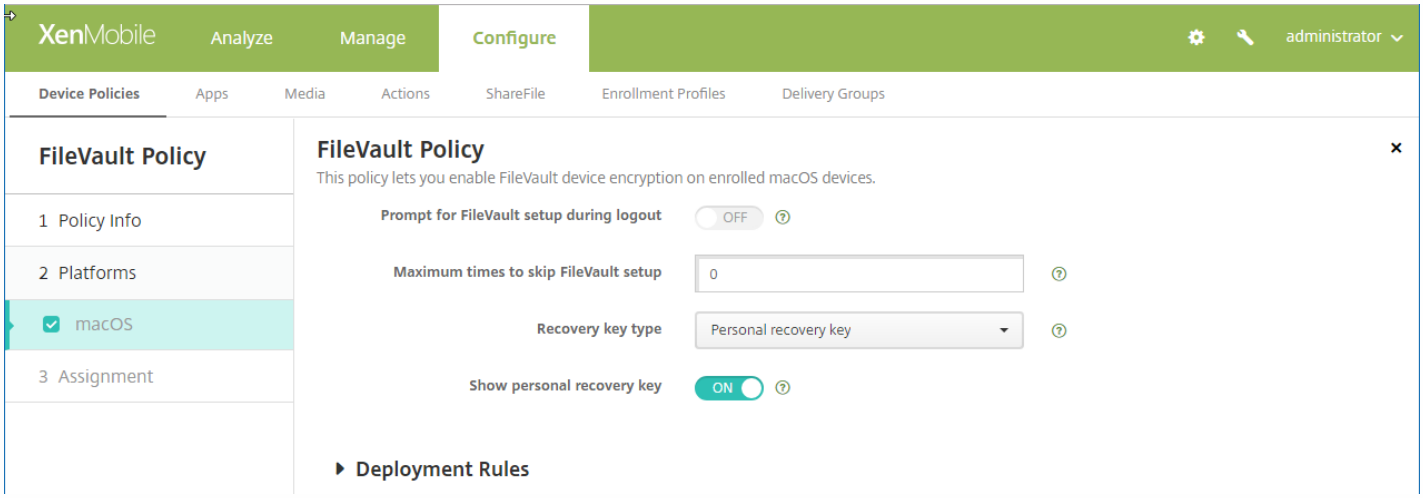
Feb 21, 2018

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 artigo de suporte da Apple, https://support.apple.com/en-us/HT 204837.

Para adicionar a política FileVault, acesse **Configurar > Políticas de dispositivo**.

Configurações do macOS

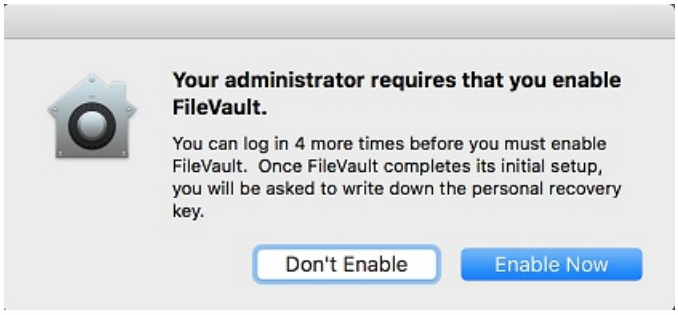


- **Solicitar a configuração do FileVault durante o logout**: se estiver **i**, solicita que o usuário ative o FileVault durante os próximos N logouts, conforme especificado pela opção **Número máximo de vezes para ignorar a configuração do FileVault**. Se o valor for **o**, o aviso de senha do FileVault não aparecerá.

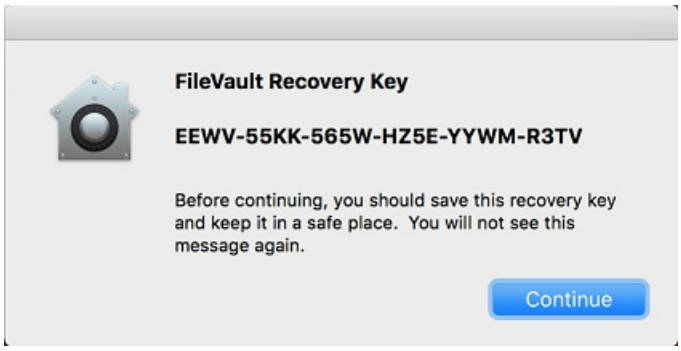
  Depois de implantar a política FileVault com essa configuração ativada, a seguinte tela aparece quando um usuário faz o logoff do dispositivo. A tela dá ao usuário a opção de ativar o FileVault antes de logoff.

  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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.



Nota

Para obter informações gerais sobre como configurar políticas, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de fonte

Feb 21, 2018

Você pode adicionar uma política de dispositivo no XenMobile para adicionar mais fontes aos dispositivos iOS e macOS dos usuários. As fontes devem ser TrueType (.ttf) ou OpenType (.oft). Coleções de fontes (.ttc ou .otc) não são compatíveis.

Nota: No caso do iOS, essa política se aplica somente ao iOS 7.0 e versões posteriores.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Expanda **Mais** e, em **Usuário final**, clique em **Fonte**. A página **Política de fonte** é exibida.

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 as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

Definir as configurações do iOS

Faça as seguintes configurações:

- **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**
  - 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 de perfil**, digite a senha necessária.

Defina as configurações do macOS

Faça as seguintes configurações:

- **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**
  - 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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Se você clicar em **Senha obrigatória**, ao lado de **Senha de remoção de perfil**, digite a senha necessária.
- Ao lado de **Escopo do perfil**, clique em **Usuário** ou **Sistema**. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de layout de tela inicial

Feb 21, 2018

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.

> ## Nota
>
> 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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

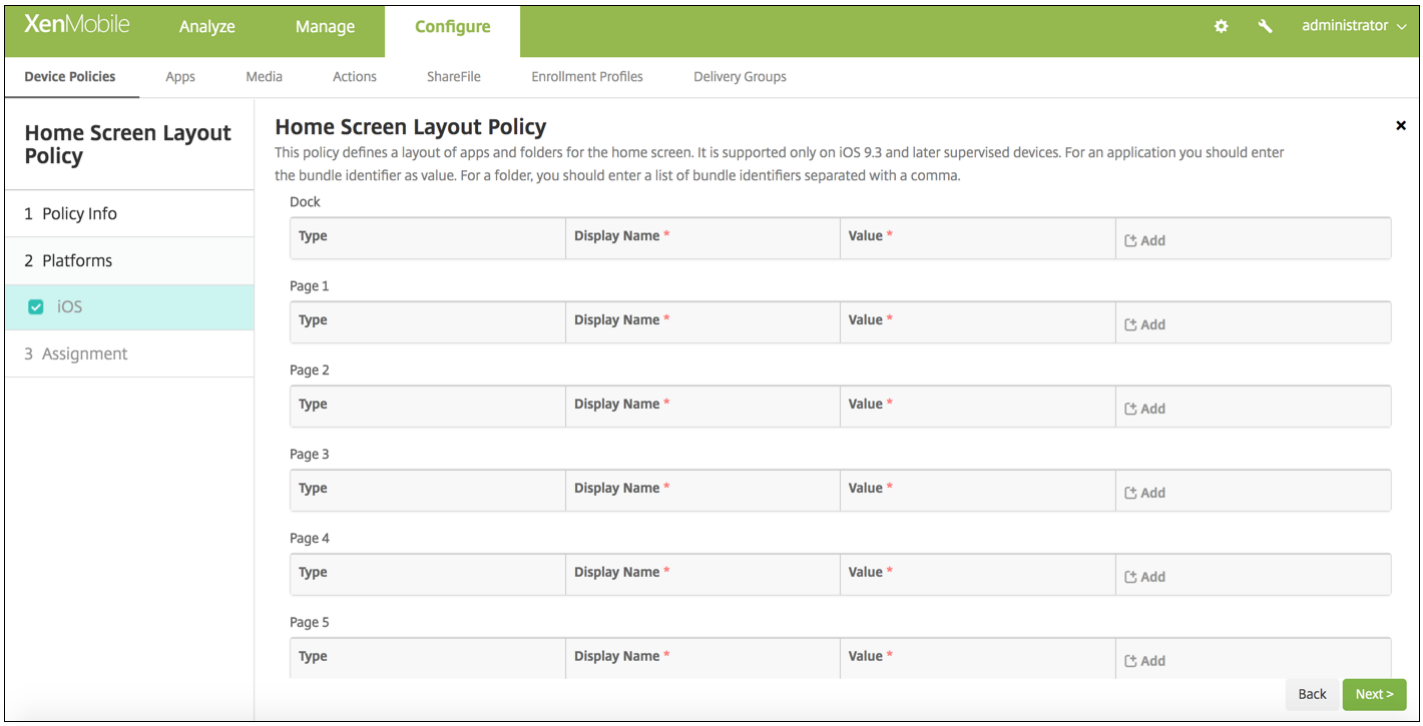
2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Comece a digitar **Layout da tela inicial** e, em seguida, clique nesse nome nos resultados da pesquisa. A página de informações **Política de layout da tela inicial** é exibida.

4. No painel **Informações sobre a política**, digite 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**. O painel **iOS** é exibido.

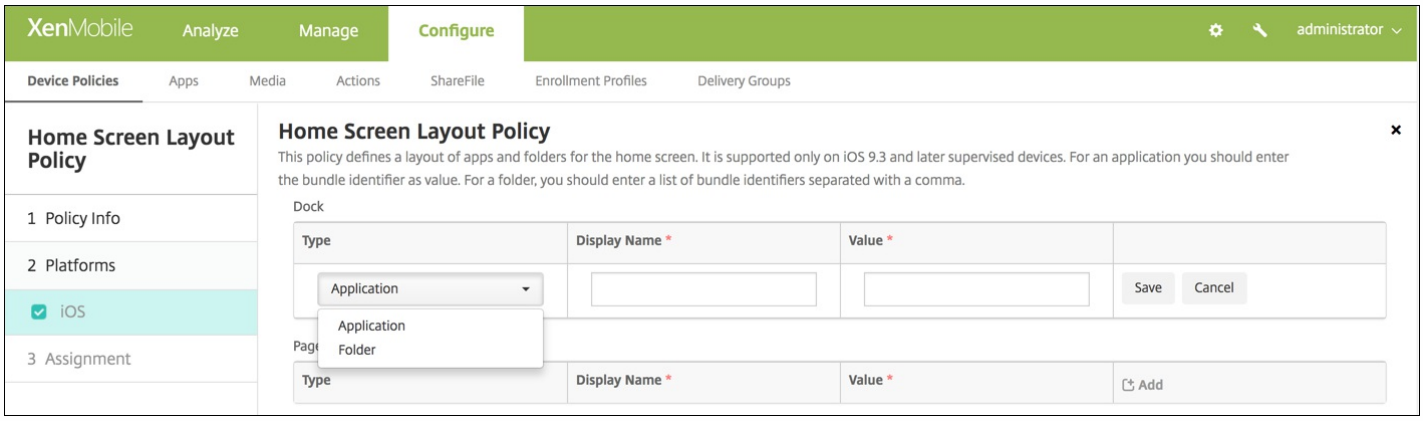


6. Defina as configurações:

- Para cada uma das áreas da tela que você deseja configurar (como **Dock** ou **Página 1**), clique em **Adicionar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Tipo**: escolha **Aplicativo** ou **Pasta**.



- **Nome para exibição**: o nome que aparece na tela inicial do aplicativo ou pasta.
- **Valor**: para aplicativos, o identificador do pacote. Para pastas, uma lista de identificadores de pacote separados por vírgulas.

Configurações de política

- **Remover política**: escolha **Selecionar data** e escolha uma data do calendário ou escolha **Duração até remoção** e especifique o número de dias.
- **Permitir que o usuário remova a política**: especifique quando permitir que o usuário remova a definição da tela inicial: **Sempre**, **Código secreto obrigatório** (somente se um código secreto for fornecido) ou **Nunca**.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de importação do perfil de iOS e Mac OS X

Feb 21, 2018

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 Help da Apple.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**.

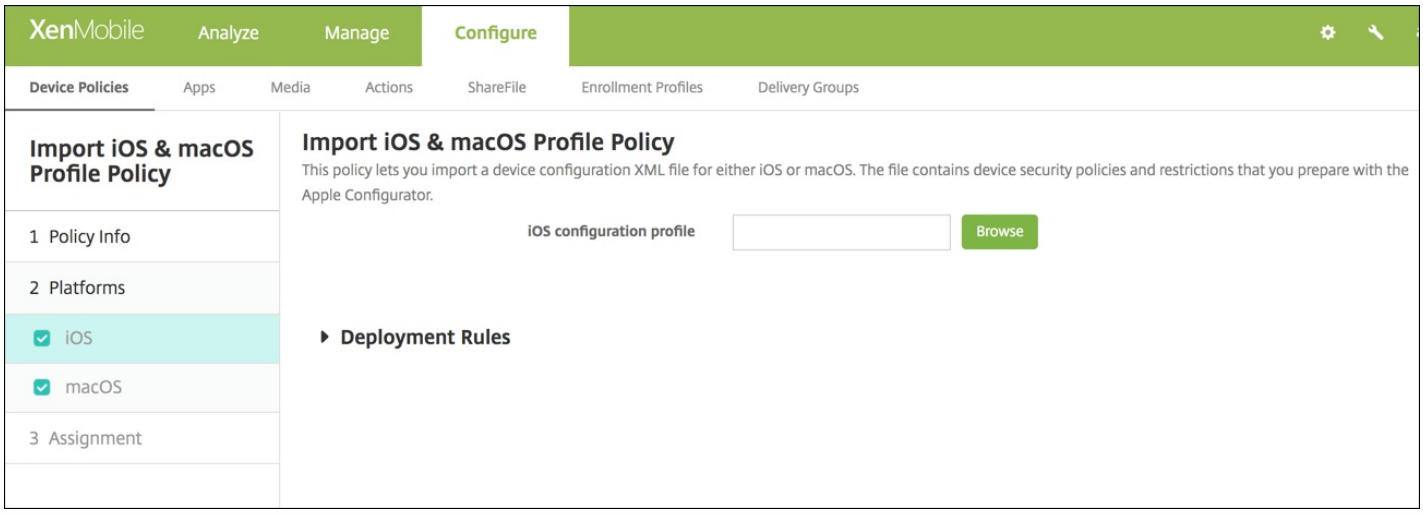
2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Expanda **Mais** e, em **Personalizado**, clique em **Importação do perfil de iOS e macOS**. A página de informações **Importação do perfil de iOS e macOS** é exibida.

4. No painel **Informações sobre a política**, insira as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma de política** é exibida.



6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 8 para saber como definir as regras de implantação dessa plataforma.

7. Defina a seguinte configuração para cada plataforma selecionada:

- **Perfil de configuração do iOS** ou **Perfil de configuração do macOS**: selecione o arquivo de configuração a ser importado clicando em **Procurar** e navegando até a localização do arquivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

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.

> **Important**
>
> Colocar um dispositivo no modo supervisionado instalará 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. Altere o controle **Supervision** para **On**. A Citrix recomenda que você escolha essa configuração se pretender manter o controle contínuo do dispositivo reaplicando uma configuração regularmente.

c. Opcionalmente, forneça um nome para o dispositivo.

c. No iOS, clique em **Latest** para obter a versão mais recente do iOS que você desejar instalar.

5. Quando você estiver pronto para preparar o dispositivo para supervisão, clique em **Prepare**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo do quiosque para Samsung SAFE

Feb 21, 2018

Crie uma política de Quiosque no XenMobile para permitir que você especifique que somente um ou mais aplicativos específicos podem ser usados em dispositivos Samsung SAFE. 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.

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 habilitar as políticas em dispositivos Samsung SAFE.

2. Habilite a Política de agendamento de conexão para dispositivos Android, conforme descrito em Políticas de dispositivo de agendamento de conexão. 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 de quiosque

Nota:

- 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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. 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. No painel **Informações sobre a política**, digite as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página de informações da **Plataforma Samsung SAFE** é exibida.

6. Defina estas configurações:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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 **I**.
- **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 **I**.
- **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 **I**.
- **Permitir barra de sistema**: selecione se deseja permitir que os usuários visualizem a barra de sistema no Modo de quiosque. O padrão é **I**.
- **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 **I**.
- **Alterar código secreto SAFE comum** : essa configuração ajuda a proteger contra alterações inadvertidas no campo Código secreto SAFE comum. Quando essa configuração é **O**, não é possível alterar o campo Código secreto SAFE comum. O padrão é **O**.
- **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 **O**.
    - **Imagem da home pahe**: ao ativar a opção **Definir um papel de parede para a home page**, 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 **O**. 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 adicionar**: 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 clique em **Cancelar** para cancelar a adição do aplicativo.

    Nota: para excluir um aplicativo existente, passe o mouse sobre a linha que contém a listagem e depois 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 aplicativo 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**. Ou clique em **Cancelar** para deixar a listagem inalterada.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivos de configuração de Launcher para Android

Feb 21, 2018

O Citrix Launcher permite que você personalize a experiência do usuário para dispositivos Android implantados pelo XenMobile. 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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

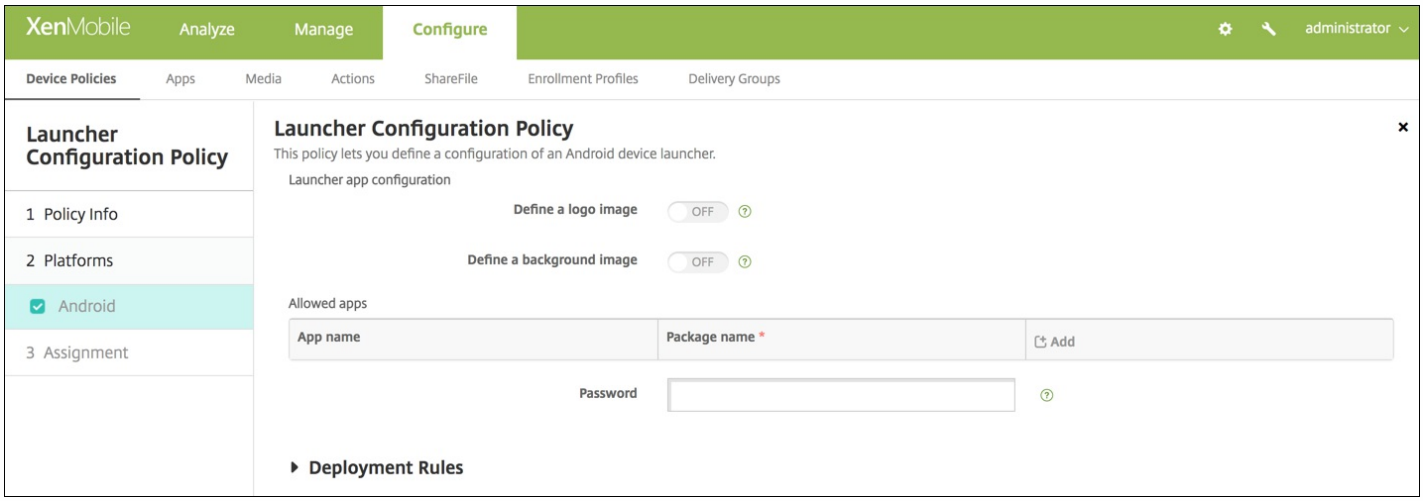
2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Comece a digitar **Launcher** e selecione **Configuração do Launcher** na lista. A página de atribuição **Política de configuração do Launcher** é exibida.

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 de informações **Plataforma Android** é exibida.



6. Defina estas configurações:

- **Definir uma imagem de logotipo**: selecione se deve ser usada uma imagem de logotipo personalizada para o ícone do

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix Launcher. O padrão é **O**.

- **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 **O**.
- **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 clique em **Cancelar** para cancelar a adição do aplicativo.

    Observação: para excluir um aplicativo 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 aplicativo existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.
- **Senha**: a senha que um usuário deve digitar para sair do Citrix Launcher.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo do LDAP

Feb 21, 2018

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.

Configurações do iOS

Configurações do macOS

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar** para adicionar uma política. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Expanda **Mais** e, em **Usuário final**, clique em **LDAP**. A página **Política de LDAP** é exibida.

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 de informações **Plataforma de política** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação.

Definir as configurações do iOS

Faça as seguintes configurações:

- **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 **I**.
- **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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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.

  Nota: para excluir a configuração de pesquisa, 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 uma configuração de pesquisa, 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**. Ou clique em **Cancelar** para deixar a listagem inalterada.

- 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 de perfil**, digite a senha necessária.

Defina as configurações do macOS

Faça as seguintes configurações:

- **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 **I**.
- **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 desejar adicionar.

    Nota: para excluir uma configuração de pesquisa 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 uma configuração de pesquisa já existente, passe o mouse sobre a linha que contém a listagem e

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

clique no ícone de caneta à direita. Atualize a listagem e clique em **Salvar** para salvar a alteração ou em **Cancelar** para deixar a listagem inalterada.

- 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 de perfil**, digite a senha necessária.
- Em **Escopo do perfil**, clique em **Usuário** ou **Sistema**. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de localização

Feb 21, 2018

Crie local 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, por exemplo, ativar o rastreamento e a localização de um dispositivo, consulte a seção Executar ações de segurança em Dispositivos.

Você pode criar políticas de dispositivo de localização para o iOS e o Android. Cada plataforma exige um conjunto diferente de valores, que são descritos neste artigo.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Clique em **Localização**. A página de informações **Política de localização** é exibida.

4. No painel **Informações sobre a política**, insira as seguintes informações:

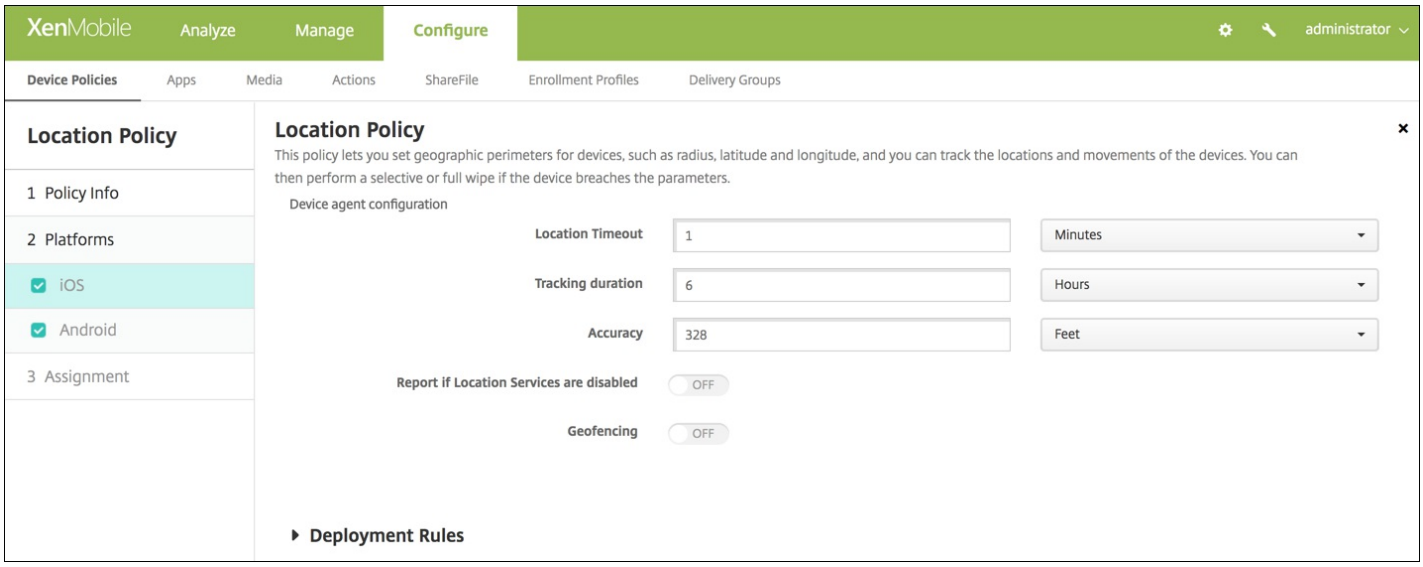
- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataformas** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

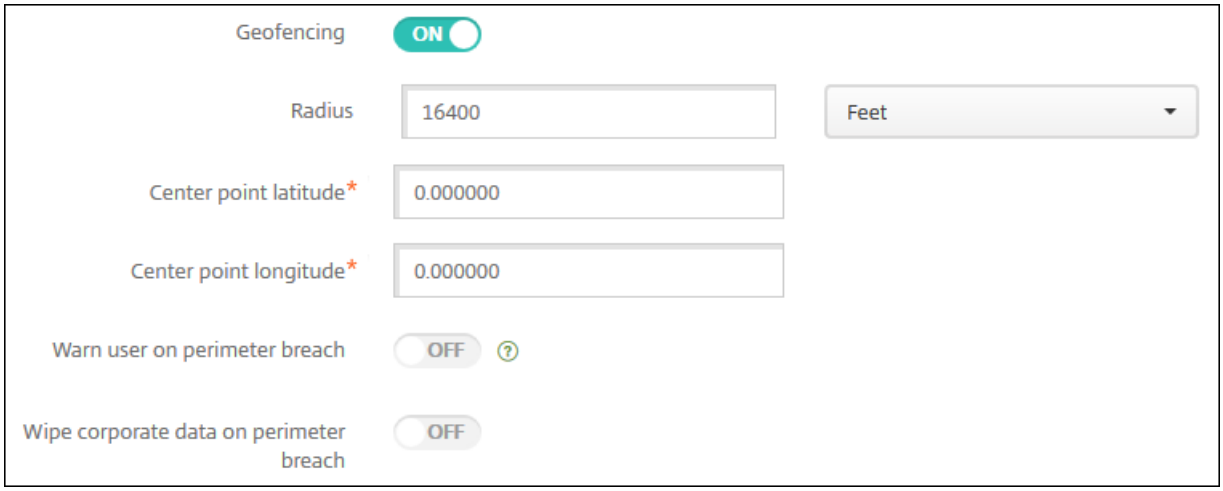
Definir as configurações do iOS



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Defina estas configurações:

- **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 fixar 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 **O**.
- **Geocerca**

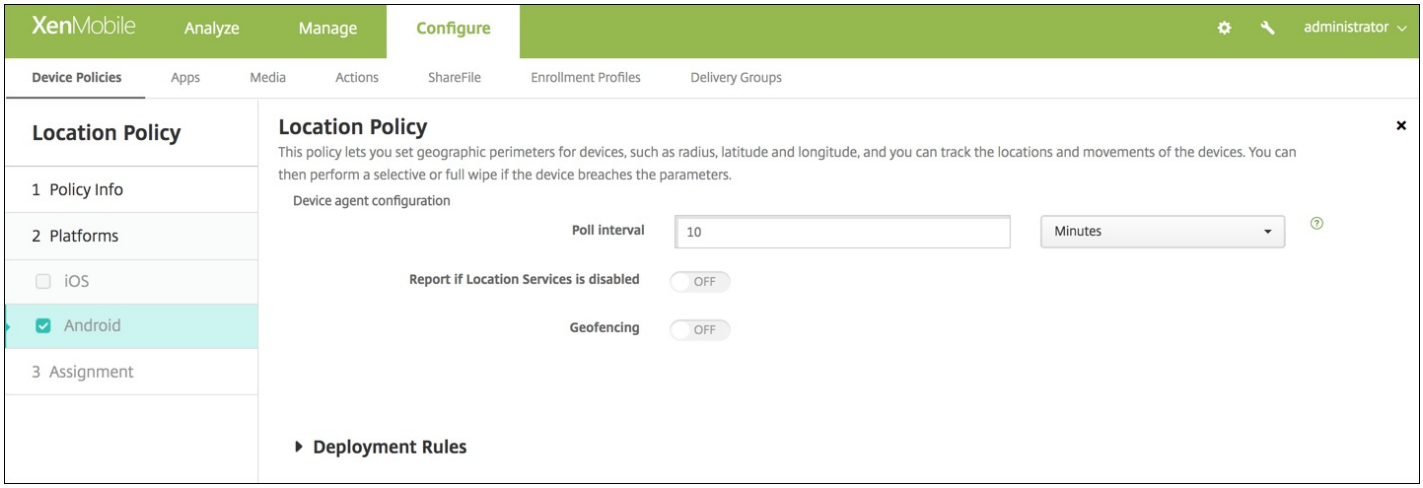


Quando você ativar a Geocerca, defina estas configurações:

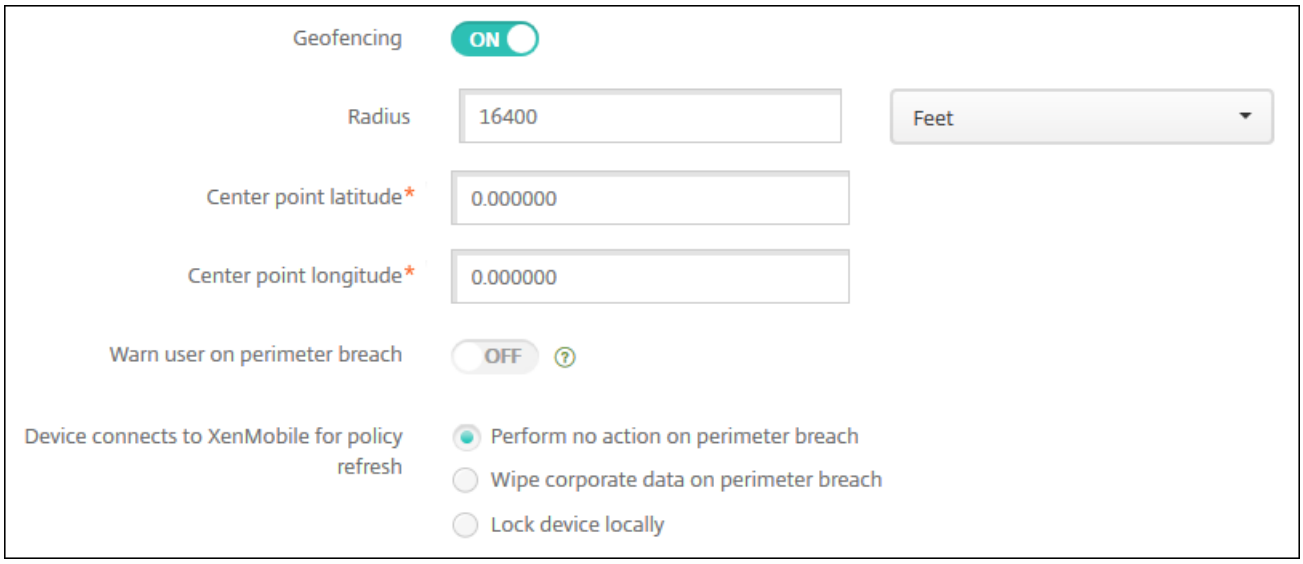
- **Raio**: digite um numeral e, na lista, clique nas unidades a serem usadas para medir o raio. O padrão é 16.400 pés. Valores válidos para o raio são:
  - 164 a 164000 pés
  - 50 a 50000 metros
  - 54 a 54680 jardas
  - 1 a 31 milhas
- **Latitude do ponto central**: digite uma latitude, como 37.787454, 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 **O**. 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 **O**. Quando você ativa essa opção, é exibido o campo **Atraso no apagamento local**.
  - 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 segundos.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Definir as configurações do Android



- **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 **O**.
- **Geocerca**



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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 **O**. 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 corporativo em caso de violação de perímetro**: apagar os dados corporativos depois de um período de tempo especificado. Quando você ativa essa opção é exibido, o campo **Atraso no apagamento local**.
    - 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 segundos.
  - **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 segundos.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de email

Feb 21, 2018

Você pode adicionar uma política de dispositivo de email ao XenMobile para configurar uma conta de email em dispositivos iOS ou macOS.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar** para adicionar uma política. É exibida a caixa de diálogo **Adicionar uma nova política**.

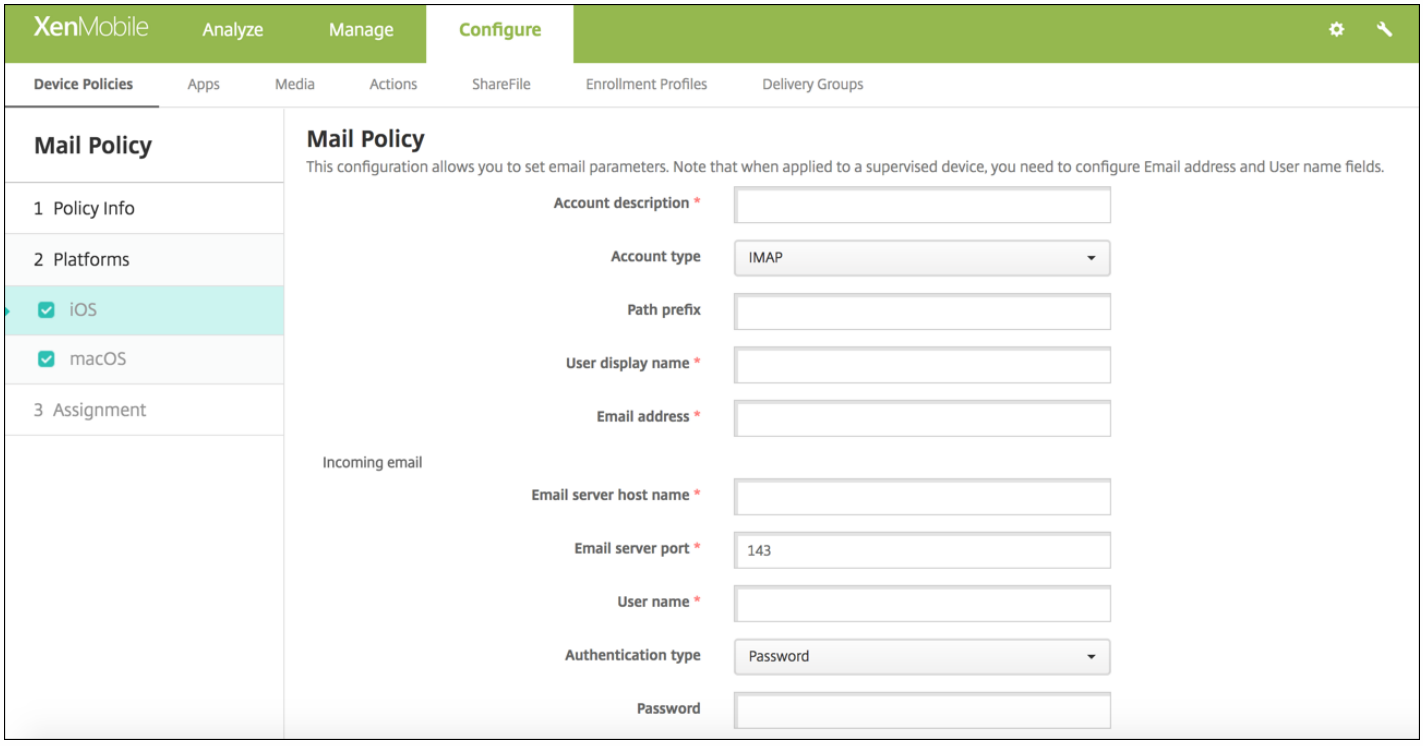
3. Clique em **Mais** e, em **Usuário final**, clique em **Email**. A página **Política de email** é exibida.

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 de política de email** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque a outra.



Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 8 para saber como definir as regras de implantação dessa plataforma.

7. Defina as configurações a seguir para as plataformas selecionadas.

- **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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Quando você seleciona **POP**, a opção de prefixo de **Caminho** a seguir desaparece.

- **Prefixo de caminho**: digite **INBOX** ou o prefixo de caminho de 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 **O**.
- **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 que deve ser usado. 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 **O**, 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 **O**.
- **Política**
  - **Nota**: para configurações do iOS, essas opções se aplicam somente ao iOS 5.0 e versões posteriores. Não há restrições para o macOS.
  - **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 **O**.
  - **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 **O**. 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 dispositivos que executam o iOS 9.2 e versões posteriores. O padrão é **O**.
  - **Ativar S/MIME**: selecione se essa conta é compatível com a autenticação e a criptografia S/MIME. O padrão é **O**. Quando definido como I, os dois campos abaixo são exibidos.
    - **Credencial de identidade de assinatura**: escolha a credencial de assinatura a ser usada.
    - **Credencial de identidade de criptografia**: escolha a credencial de criptografia a ser usada.
- **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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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 de perfil**, digite a senha.
- Ao lado de **Escopo do perfil**, escolha **Usuário** ou **Sistema**. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

8.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de domínios gerenciados

Feb 21, 2018

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 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.

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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. A caixa de diálogo **Adicionar uma nova política** é exibida.

3. Expanda **Mais** e, em **Segurança**, clique em **Domínios Gerenciados** A página de informações **Política de domínios gerenciados** é exibida.

4. No painel **Informações sobre a política**, digite as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma iOS** é exibida.

Como especificar domínios

6. Defina estas configurações:

- **Domínios Gerenciados**
  - **Domínios de email não marcados**: para cada domínio de email que você desejar 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Domínios Web Safari gerenciados**: para cada domínio Web que você desejar 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 desejar 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.

    Nota: para excluir um domínio 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 domínio existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou clique em **Cancelar**.

- **Configurações de política**
  - 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 de perfil**, digite a senha necessária.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Políticas de dispositivo das opções de MDM

Feb 21, 2018

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 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.

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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

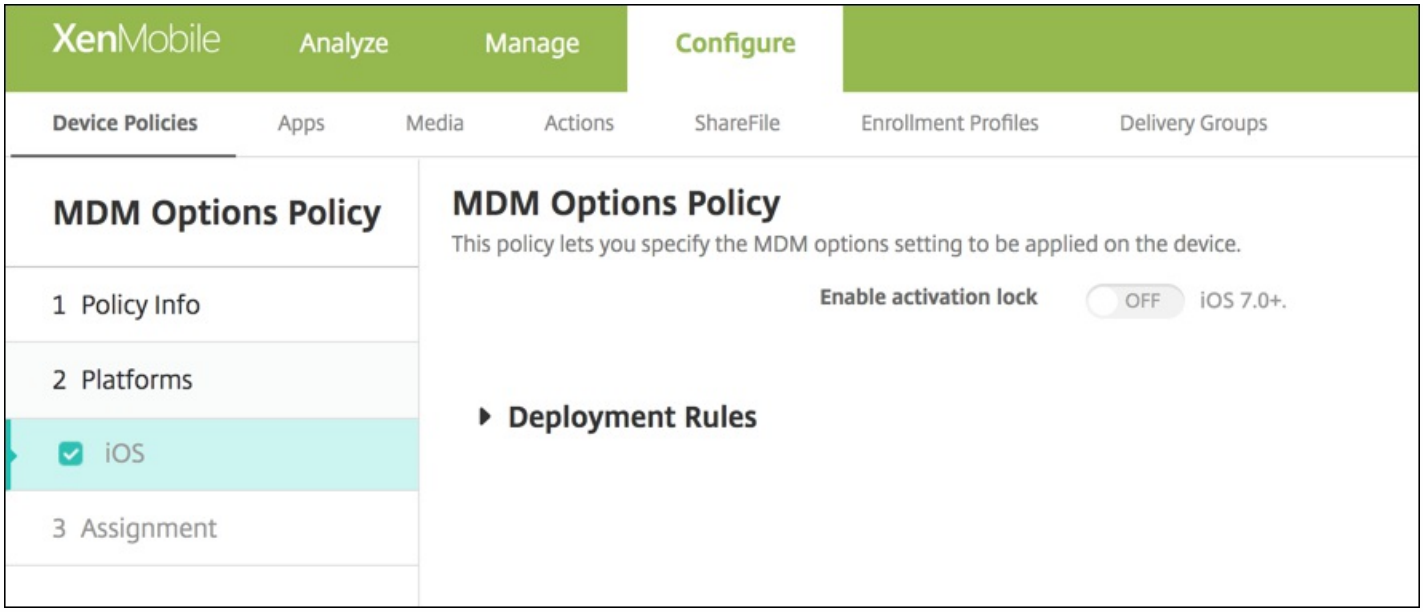
3. Expanda **Mais** e, em **Usuário final**, clique em **Opções de MDM**. A página de informações **Política de opções de MDM** é exibida.

4. No painel **Informações sobre a política**, digite as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma da política de MDM do iOS** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. Configure esta definição:

- **Ativar bloqueio de ativação**: selecione se o bloqueio de ativação deve ser ativado nos dispositivos nos quais você implantar essa política. O padrão é **O**.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

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 um bloqueio de ativação iOS no artigo de ações de segurança.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de informação da organização

Feb 21, 2018

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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Clique em **Mais** e, em **Usuário final**, clique em **Informações sobre a organização**. A página **Política de informações sobre a organização** é exibida.

4. No painel **Informações sobre a política**, insira as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: se desejar, digite uma descrição para a política.

5. Clique em **Avançar**. A página **Informações da plataforma iOS** é exibida.

Defina estas configurações:

- **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.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de código secreto

Feb 21, 2018

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 for Work, Windows Phone e Windows Desktop/Tablet. Cada plataforma exige um conjunto diferente de valores, que são descritos neste artigo.

Configurações do iOS

Configurações do macOS

Configurações do Android

Configurações do Samsung KNOX

Configurações do Android for Work

Configurações do Windows Phone

Configurações do Windows Desktop/Tablet

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**. A página de informações Política de Código Secreto é exibida.

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.

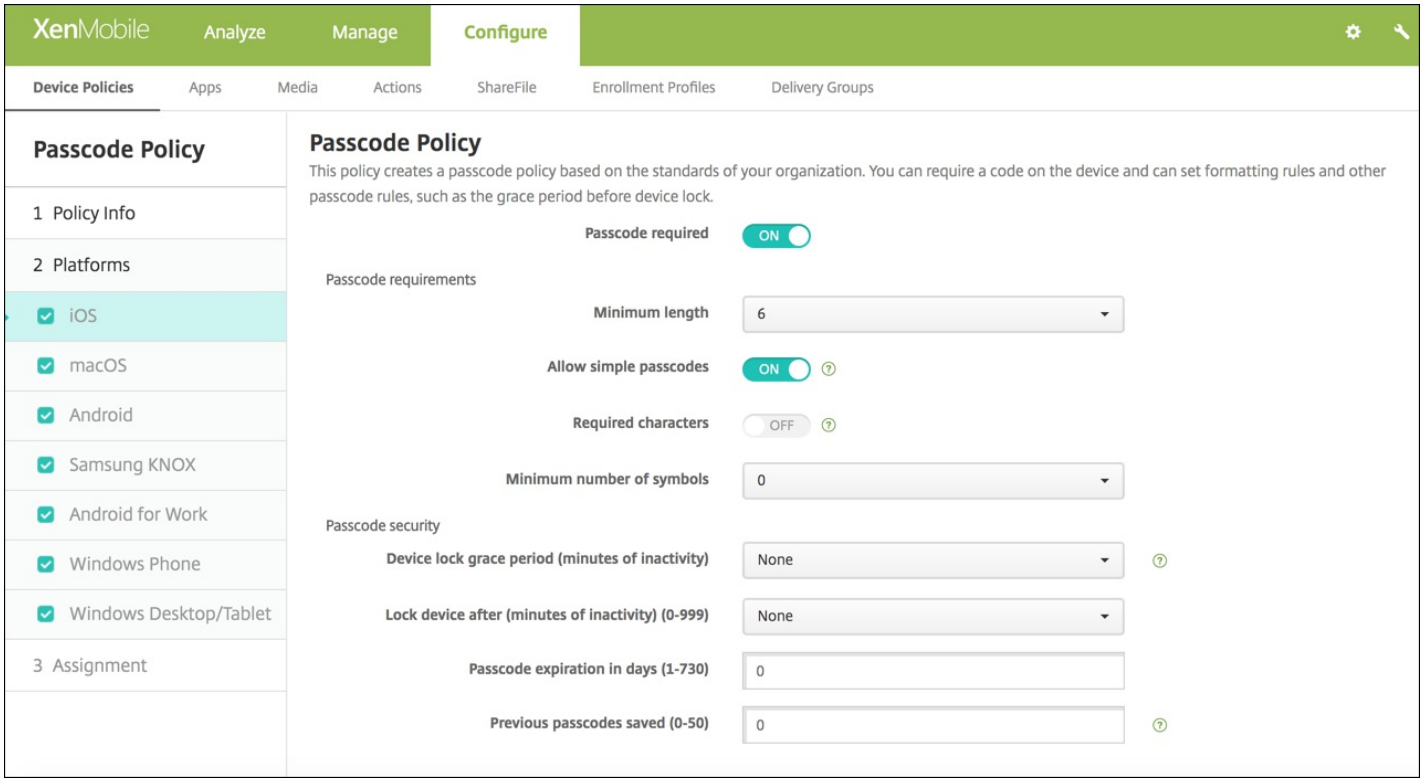
5. Clique em **Avançar**. A página **Plataformas** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

Definir as configurações do iOS

© 1999-2017 Citrix Systems, Inc. All rights reserved.



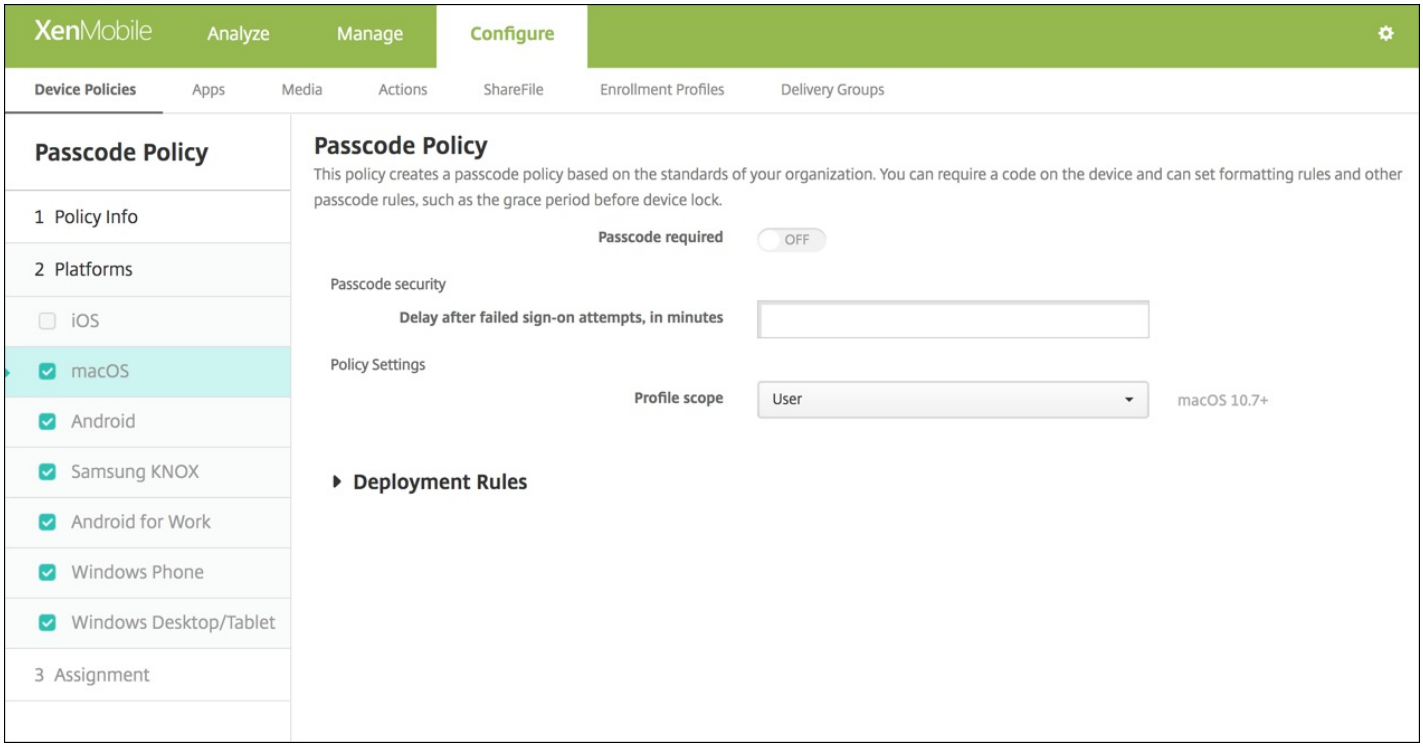
Faça as seguintes configurações:

- **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 **I**.
  - **Caracteres obrigatórios**: selecione se será obrigatório que os códigos secretos tenham pelo menos uma letra. O padrão é **O**.
  - **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 o código secreto 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**, 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 foi totalmente apagado com êxito. O padrão é **Não definido**.
- **Configurações de política**
  - Ao lado de **Remover política**, clique em **Selecionar data** ou em **Duração até remoção (em horas)**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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 de perfil**, digite a senha necessária.

Defina as configurações do macOS



Defina estas configurações:

- **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 a opção **Código secreto obrigatório**, 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 os respectivos códigos secretos.
- Se você ativar a opção **Código secreto obrigatório**, 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 **I**.
  - **Caracteres obrigatórios**: selecione se será obrigatório que os códigos secretos tenham pelo menos uma letra. O padrão é **O**.
  - **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

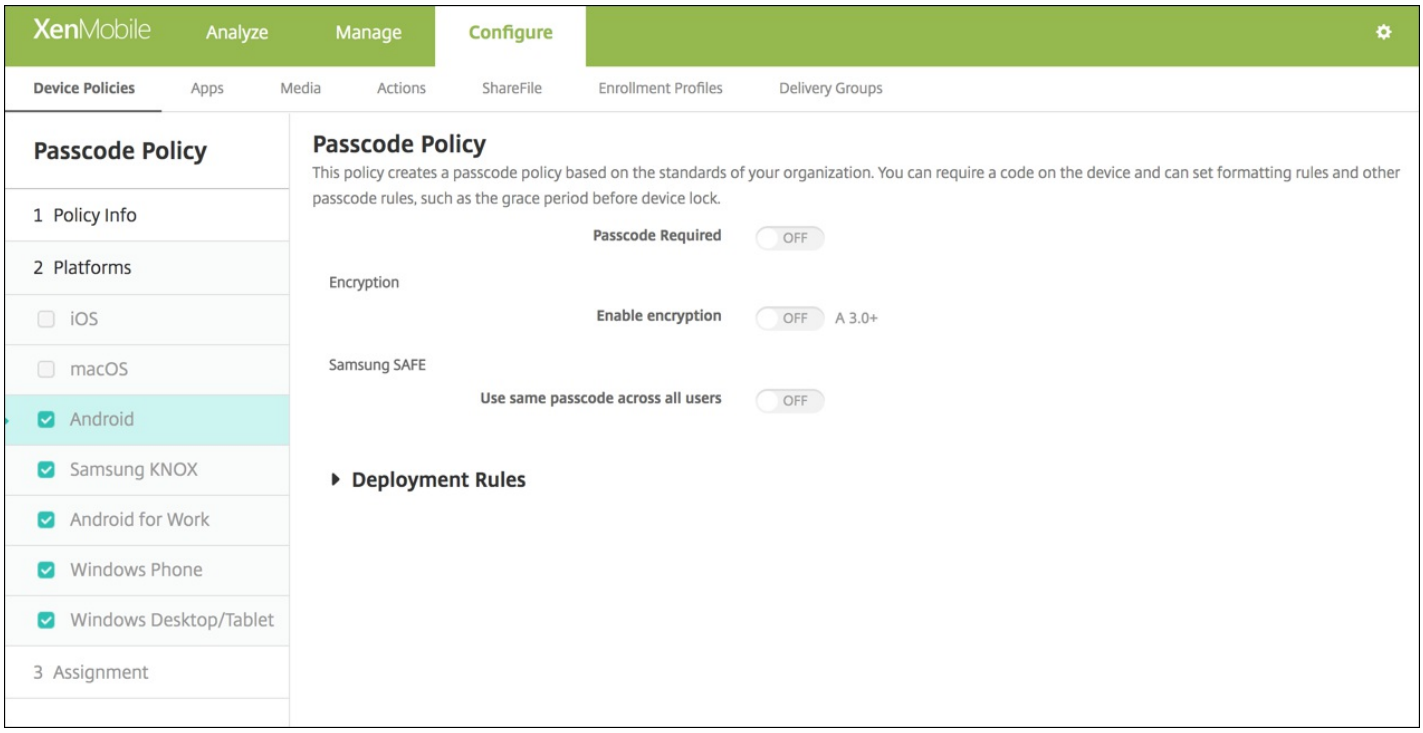
© 1999-2017 Citrix Systems, Inc. All rights reserved.

valores válidos são de 1 a 730. O padrão é **0**, o que significa que o código secreto 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**, 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.

- **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 de perfil**, digite a senha necessária.
  - Ao lado de **Escopo do perfil**, clique em **Usuário** ou **Sistema**. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

Definir as configurações do Android



Defina estas configurações:

Nota: a configuração padrão para o Android é **O**.

- **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 ativar essa opção, o campo Caracteres obrigatórios estará oculto. O padrão é **O**.
  - **Caracteres obrigatórios**: na lista, clique em Sem restrição, Letras e números, Apenas números ou Apenas letras para

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 **O**.
- Quando você ativar a opção **Regras avançadas** de cada uma das seguintes listas, clique no número mínimo de cada tipo de caractere que um código secreto 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 o código secreto 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**, 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 **Código secreto obrigatório**.

    Nota: para criptografar os dispositivos deles, 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**
  - **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 **O**. Essa configuração se aplica somente aos dispositivos Samsung SAFE e está disponível independentemente da configuração **Código secreto obrigatório**.
  - 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 opção **Código secreto obrigatório**, defina as seguintes configurações do Samsung SAFE:
    - **Caracteres alterados**: digite o número de caracteres que os usuários devem alterar do código secreto anterior deles. 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

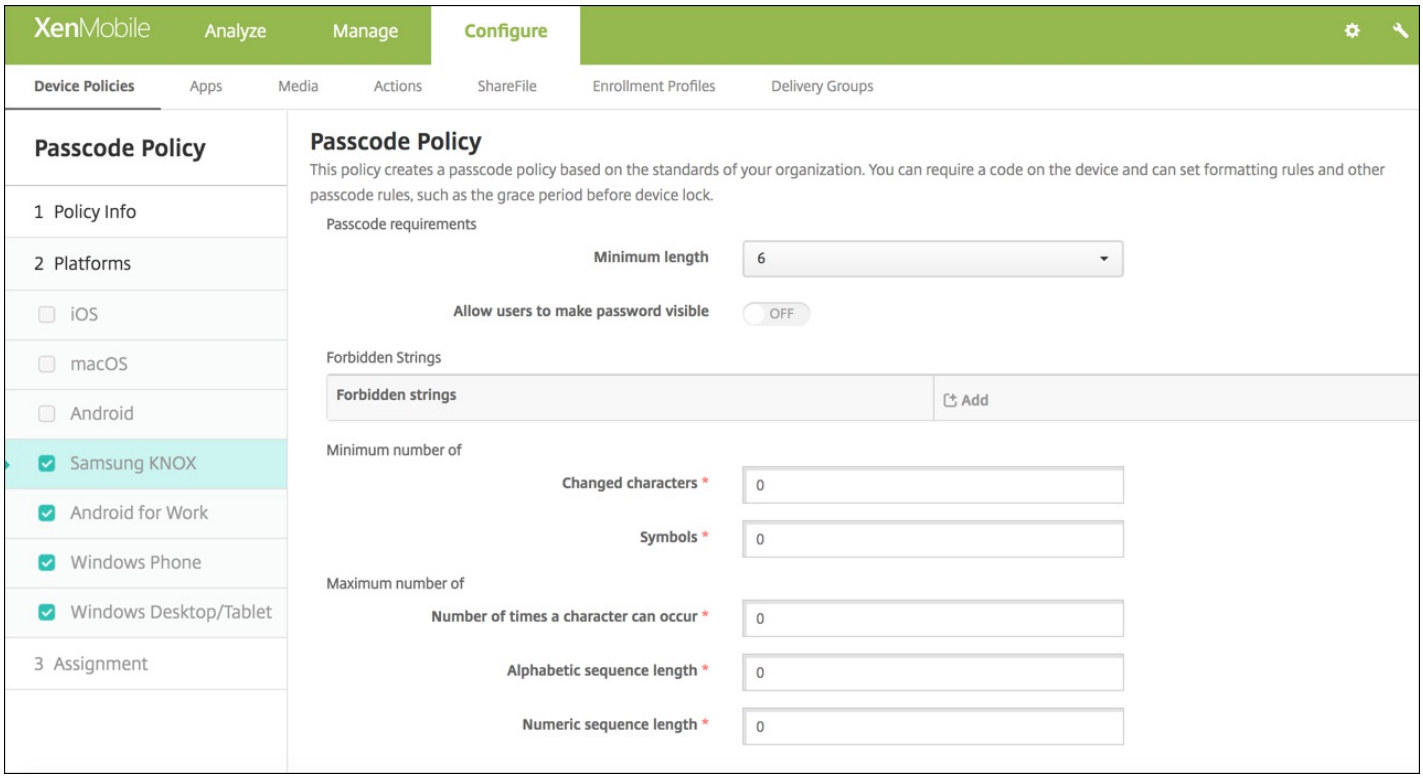
secretos deles. O padrão é **I**.

- **Configure a autenticação biométrica**. Selecione a autenticação biométrica deve ser ativada. O padrão é **O**. Se você configurá-la como **Ativada**, você pode definir essas opções:
  - **Permitir impressão digital**. Selecione para permitir que os usuários se autentiquem usando a impressão digital.
  - **Permitir íris**. Selecione para permitir que os usuários se autentiquem 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.

    Nota: para excluir uma cadeia de caracteres 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 uma cadeia de caracteres existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

Definir as configurações do Samsung KNOX



Defina estas configurações:

- **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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

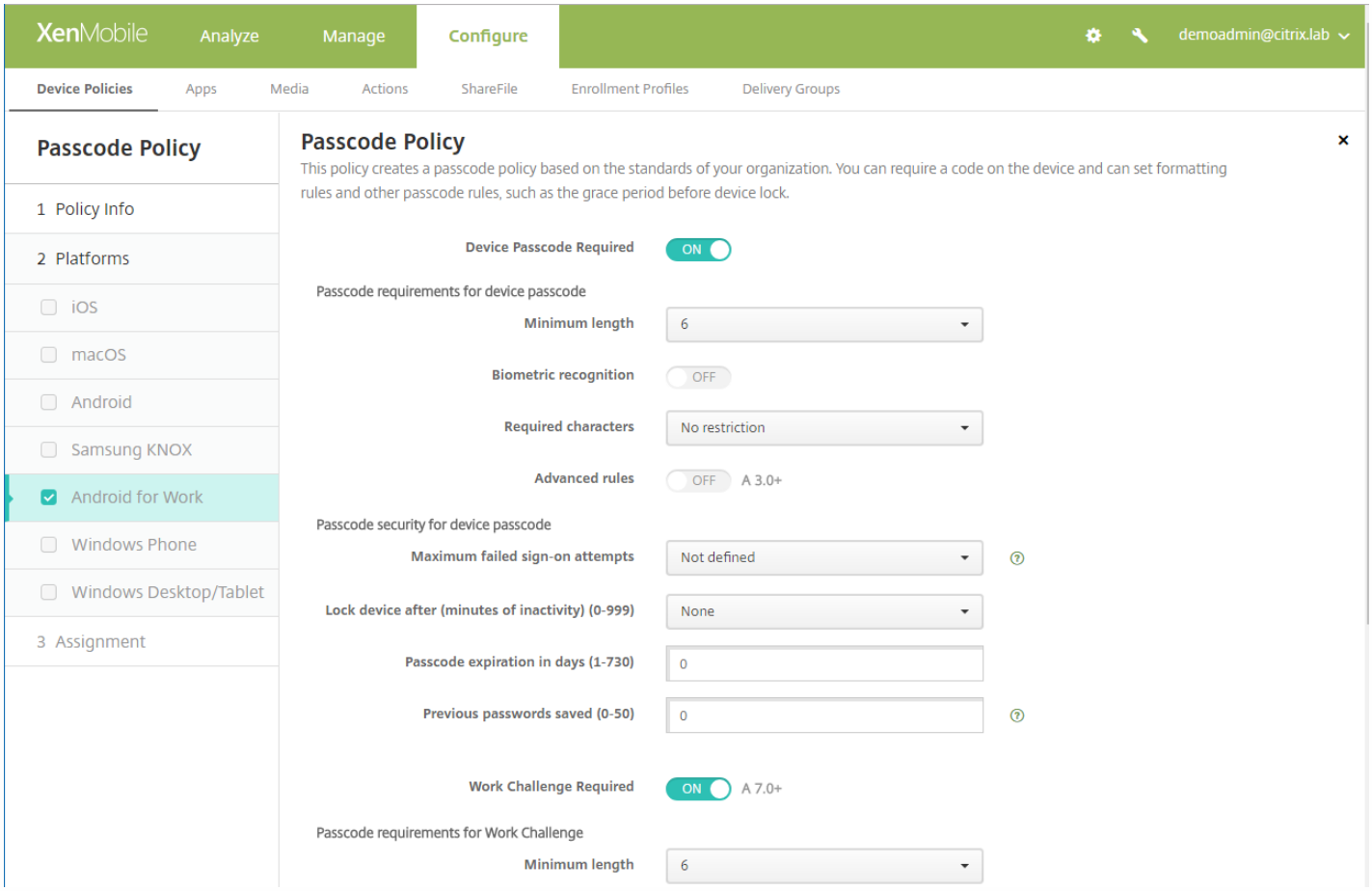
Nota: para excluir uma cadeia de caracteres existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de lixeira à direita. Uma caixa de diálogo de confirmação é exibida. Clique em **Excluir** para excluir a listagem ou em **Cancelar** para mantê-la.

Para editar uma cadeia de caracteres existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

- **Número mínimo de**
  - **Caracteres alterados**: digite o número de caracteres que os usuários devem alterar do código secreto anterior deles. 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 o código secreto 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**, que significa que os usuários podem reutilizar senhas.
  - **Se o número de tentativas de logon 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 logon 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 precisarão reinicializar o contêiner do KNOX após a limpeza. O padrão é **Não definido**.

Definir as configurações do Android for Work

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Defina estas configurações para Código secreto do dispositivo e Desafio de trabalho:

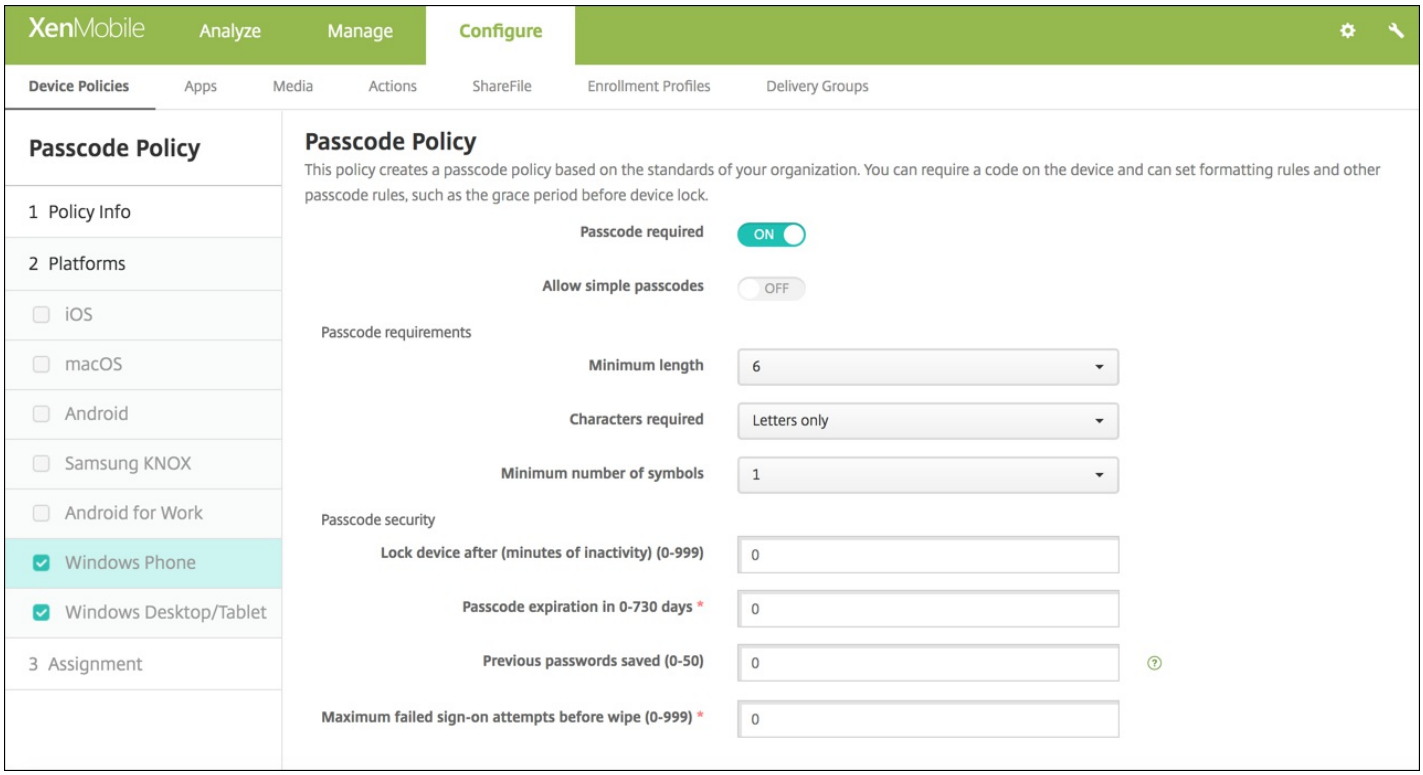
- **Código secreto obrigatório:** habilite esta configuração para exigir um código secreto e para exibir as opções de configuração de uma política de dispositivo de Código secreto do Android for Work. A página se expande para permitir que você defina as configurações dos requisitos de código secreto e segurança do código secreto. O padrão é **Off**.
- **Desafio de trabalho obrigatório:** habilite esta configuração para exigir que os usuários concluam um desafio de segurança para acessar aplicativos em execução em um perfil de trabalho do Android for Work. A página se expande para permitir que você defina as configurações dos requisitos de código secreto e segurança do código secreto. Essa opção não está disponível para dispositivos Android anteriores ao Android 7.0. O padrão é **Off**.
- **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 ativar essa opção, o campo **Caracteres obrigatórios** estará oculto. O padrão é **Off**. Observe que esse recurso não é compatível no momento.
  - **Caracteres obrigatórios**: na lista, clique em **Sem restrição**, **Letras e números**, **Apenas números** ou **Apenas letras** para configurar como os códigos secretos são compostos.
    - Para o código secreto do dispositivo: o padrão é **Sem restrição**.
    - Para o desafio de trabalho: use **Sem restrições** somente para dispositivos que executam o Android 7.0. A configuração **Sem restrições** não é respeitada pelo Android 7.1 e versões posteriores. O padrão é **Letras e números**.
  - **Regras avançadas**: selecione se regras avançadas de código secreto devem ser aplicadas. Essa opção não está disponível para dispositivos Android anteriores ao Android 5.0. O padrão é **O**.
  - Quando você ativar a opção **Regras avançadas** de cada uma das seguintes listas, clique no número mínimo de cada tipo de caractere que um código secreto deve conter:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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 número de minutos 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 o código secreto 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**, 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, após as quais o contêiner do KNOX (juntamente com os dados do KNOX) é apagado do dispositivo. Os usuários precisarão reinicializar o contêiner do KNOX após a limpeza. O padrão é **Não definido**.

Definir as configurações do Windows Phone



Defina estas configurações:

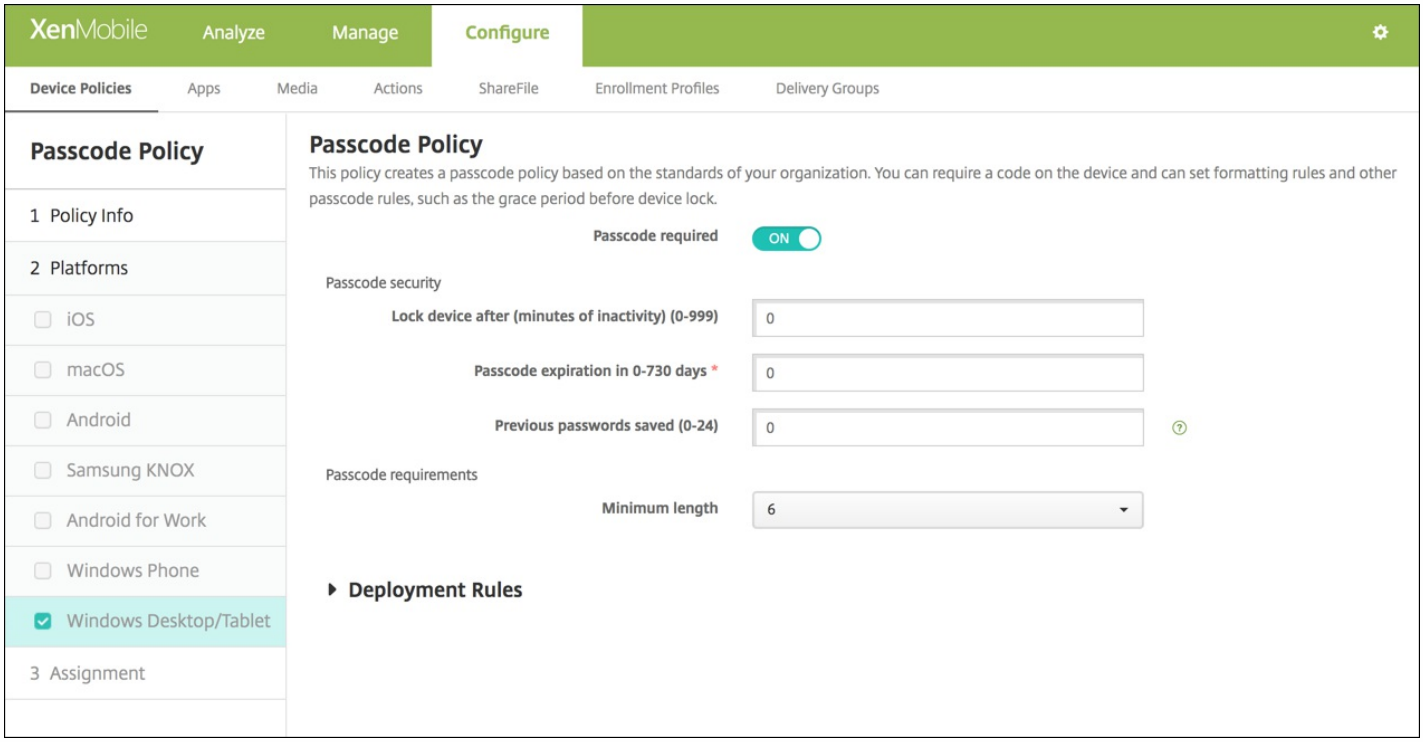
- **Código secreto obrigatório**: selecione essa opção para não exigir um código secreto para dispositivos Windows Phone. A configuração padrão é **I**, o que exige um código secreto. A página é recolhida e as opções a seguir desaparecem quando você desativa essa configuração.
- **Permitir código secreto 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**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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)**: digite o 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 o código secreto 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**, que significa que os usuários podem reutilizar senhas.
  - **Máximo de falhas em tentativas de logon antes de apagamento (0-999)**: digite o número de vezes que um usuário pode não conseguir fazer logon depois que os dados corporativos são apagados do dispositivo. O padrão é **0**.

Definir as configurações do Windows Desktop/Tablet



Defina estas configurações:

- **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 **O**.
- **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 o código secreto 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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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**.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo do ponto de acesso pessoal

Feb 21, 2018

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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. A página **Adicionar uma nova política** é exibida.

3. Expanda **Mais** e, em **Acesso à rede**, clique em **Ponto de acesso pessoal** A página de informações **Política de ponto de acesso pessoal** é exibida.

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 de informações **Plataforma iOS** é exibida.

6. Configure esta definição:

- **Desativar ponto de acesso pessoal**: selecione se pretende desativar a funcionalidade de ponto de acesso pessoal em dispositivos de usuários. O padrão é **O**, que desliga o ponto de acesso pessoal em dispositivos de usuários. Essa 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.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de remoção de perfil

Feb 21, 2018

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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página Políticas de dispositivo é exibida.

2. Clique em **Adicionar**. A caixa de diálogo **Adicionar uma nova política** é exibida.

3. Expanda **Mais** e, em **Segurança**, clique em **Remoção de perfil**. A página de informações **Política de remoção de perfil** é exibida.

4. No painel **Informações sobre a política**, digite as seguintes informações:

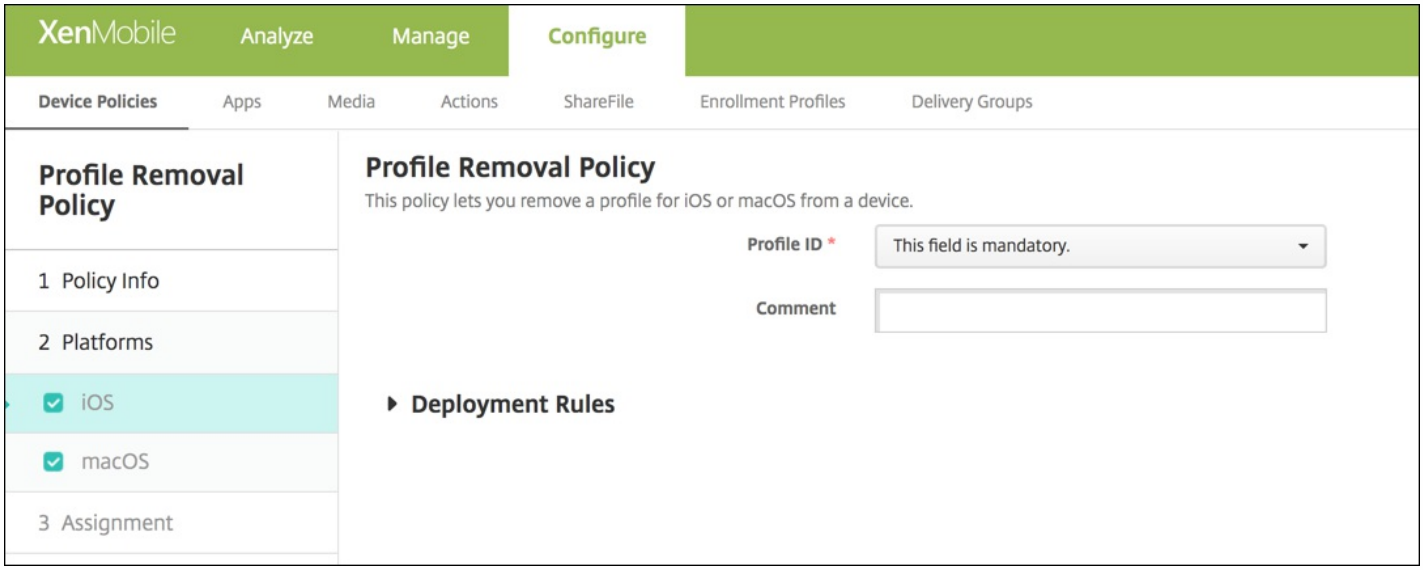
- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataformas** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

Definir as configurações do iOS

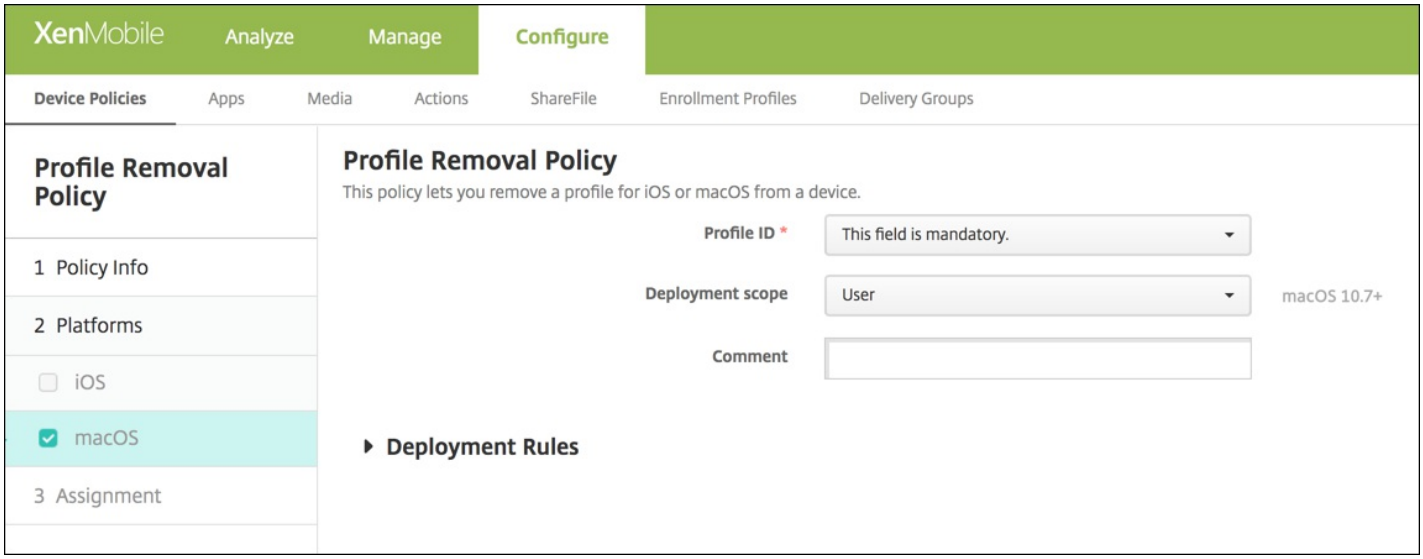


Defina estas configurações:

- **ID do perfil**: na lista, clique no ID do perfil do aplicativo. Este campo é obrigatório.
- **Comentário**: digite um comentário opcional.

Defina as configurações do macOS

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Defina estas configurações:

- **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.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo do perfil de provisionamento

Feb 21, 2018

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 Criando perfis de provisionamento no site Apple Developer.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

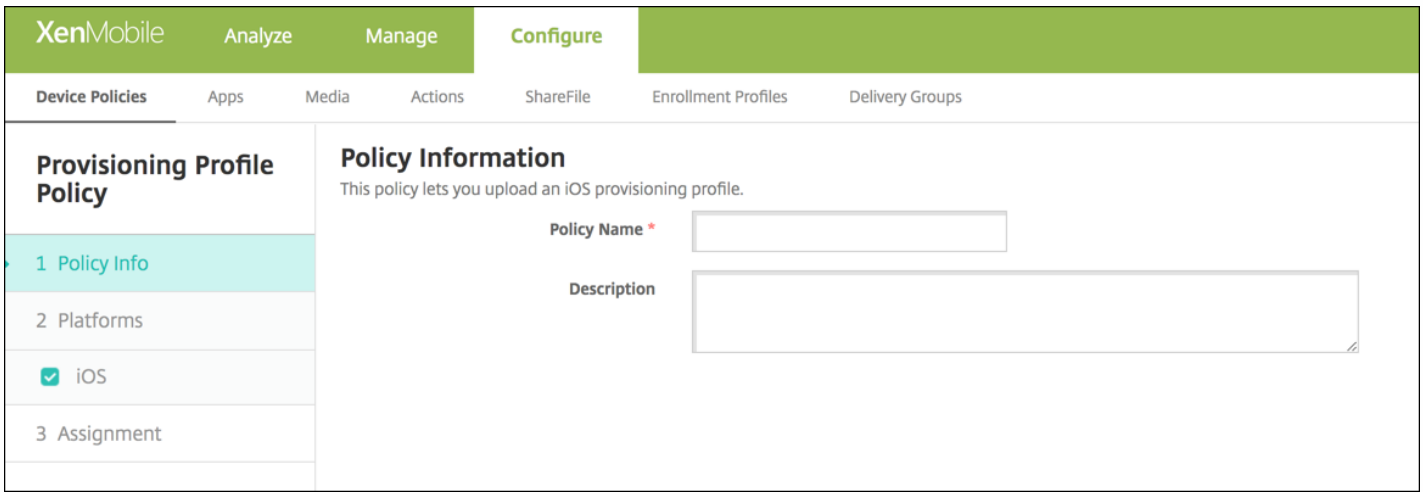
2. Clique em **Adicionar**. A página **Adicionar uma nova política** é exibida.

3. Expanda **Mais** e, em **Aplicativos**, clique em **Perfil de provisionamento**. A página de informações **Política de perfil de provisionamento** é exibida.

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 de informações **Plataforma iOS** é exibida.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

6. Defina esta configuração:

- **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.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo da remoção de perfil de provisionamento

Feb 21, 2018

Você pode remover os perfis de provisionamento do iOS com as políticas de dispositivo. Para obter mais informações sobre perfis de provisionamento, consulte Adição de um perfil de provisionamento.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. A página **Adicionar uma nova política** é exibida.

3. Expanda **Mais** e, em **Remoção**, clique em **Remoção de perfil de provisionamento**. A página de informações **Política de remoção de perfil de provisionamento** é exibida.

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 **Plataforma iOS** é exibida.

6. Defina estas configurações:

- **Perfil de provisionamento do iOS**: na lista, clique no perfil de provisionamento que deseja remover.
- **Comentário**: opcionalmente, adicione um comentário.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de proxy

Feb 21, 2018

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.

Nota: 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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Clique em **Mais** e, em **Acesso à rede**, clique em **Proxy**. A página **Política de proxy** é exibida.

4. No painel **Informações sobre a política**, insira as seguintes informações:

- **Nome da política**: insira um nome descritivo para a política.
- **Descrição**: opcionalmente, insira uma descrição para a política.

5. Clique em **Avançar**. A página **Plataforma de política** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

Definir as configurações do iOS

Defina estas configurações:

- **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 do usuário opcional para autenticação no servidor proxy.
    - **Senha**: digite uma senha opcional para autenticação no servidor proxy.
  - Se você clicar em **Automática**, defina estas configurações:
    - **URL PAC do Proxy**: digite o 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 **I**. 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 **O**.
- **Configurações de política**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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 de perfil**, digite a senha necessária.

Definir as configurações do Windows Mobile/CE

Defina estas configurações:

- **Rede**: na lista, clique no tipo de rede a ser usado. 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 o nome de domínio.
- **Ativar**: selecione se o proxy deve ser ativado. O padrão é **I**.

7. Configure as regras de implantação

8. Clique em **Avançar**. A página de atribuição **Política de proxy** é exibida.

9. Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega ou selecione na lista um grupo ou os grupos aos quais você deseja atribuir a política. Os grupos que você selecionar aparecerão na lista **Grupos de entrega que receberão a atribuição de aplicativos** à direita.

10. 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 **O**, nenhuma outra opção precisará ser configurada.
- Ao lado de **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 se aplicará 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

aplicam a todas as plataformas, exceto **Implantar para conexões permanentes**, que não se aplica ao iOS.

11. Clique em **Salvar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo do Registro

Feb 21, 2018

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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Expanda **Mais** e, em **Personalizado**, clique em **Registro**. A página de informações **Política de registro** é exibida.

4. No painel **Informações sobre a política**, digite as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma Windows Mobile/CE** é exibida.

6. Defina estas configurações:

- 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 até a chave do Windows da 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 da 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 ProgramFilesDir, digite *C:\Arquivos de programas*.
- Clique em **Salvar** para salvar as informações de chave do registro ou em **Cancelar** para não salvá-las.

  Nota: para excluir uma chave do registro, 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 uma chave do registro existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Suporte remoto à política de dispositivo

Feb 21, 2018

> ## 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 está disponível para os clientes do XenMobile Service e não é suportado para implantações em cluster do XenMobile Server 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 que você exiba informações de diagnóstico sobre o dispositivo, como as informações do sistema, os processos em execução, o gerenciador de tarefas (uso de memória e da CPU), o conteúdo da pasta do software instalado etc.
- **Premium**, que permite controlar remotamente a tela do dispositivo, incluindo o controle de cores (na janela principal ou em uma janela separada e flutuante), a capacidade de estabelecer uma sessão de Voice-over-IP (VoIP) entre o suporte técnico e o usuário, de definir configurações e de estabelecer uma sessão de chat entre o suporte técnico e o usuário.

Observação: 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 Políticas 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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

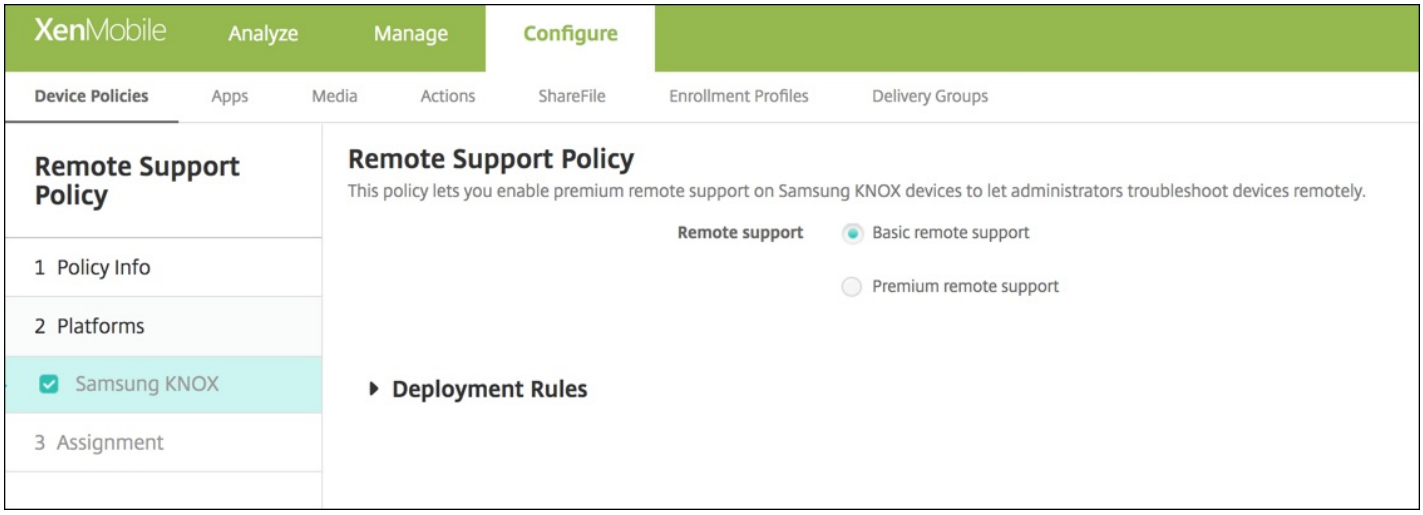
3. Comece a digitar **Suporte remoto** e, em seguida, clique em **Suporte remoto**. A página **Política de suporte remoto** é exibida.

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 de informações da plataforma **Samsung KNOX** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. Configure esta definição:

- **Suporte remoto**: selecione **Suporte remoto básico** ou **Suporte remoto premium**. O padrão é **Suporte remoto básico**.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de restrições

Feb 21, 2018

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.

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 estiver definido como **I**, o usuário poderá usar a câmera no seu dispositivo. Se estiver definido como **O**, o usuário não poderá usar a câmera no seu dispositivo.
- **Capturas de tela**. Se estiver definido como **I** o usuário poderá fazer capturas de tela no seu dispositivo. Se estiver definido como **O**, o usuário não poderá fazer capturas de tela no seu dispositivo.

> ## 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.

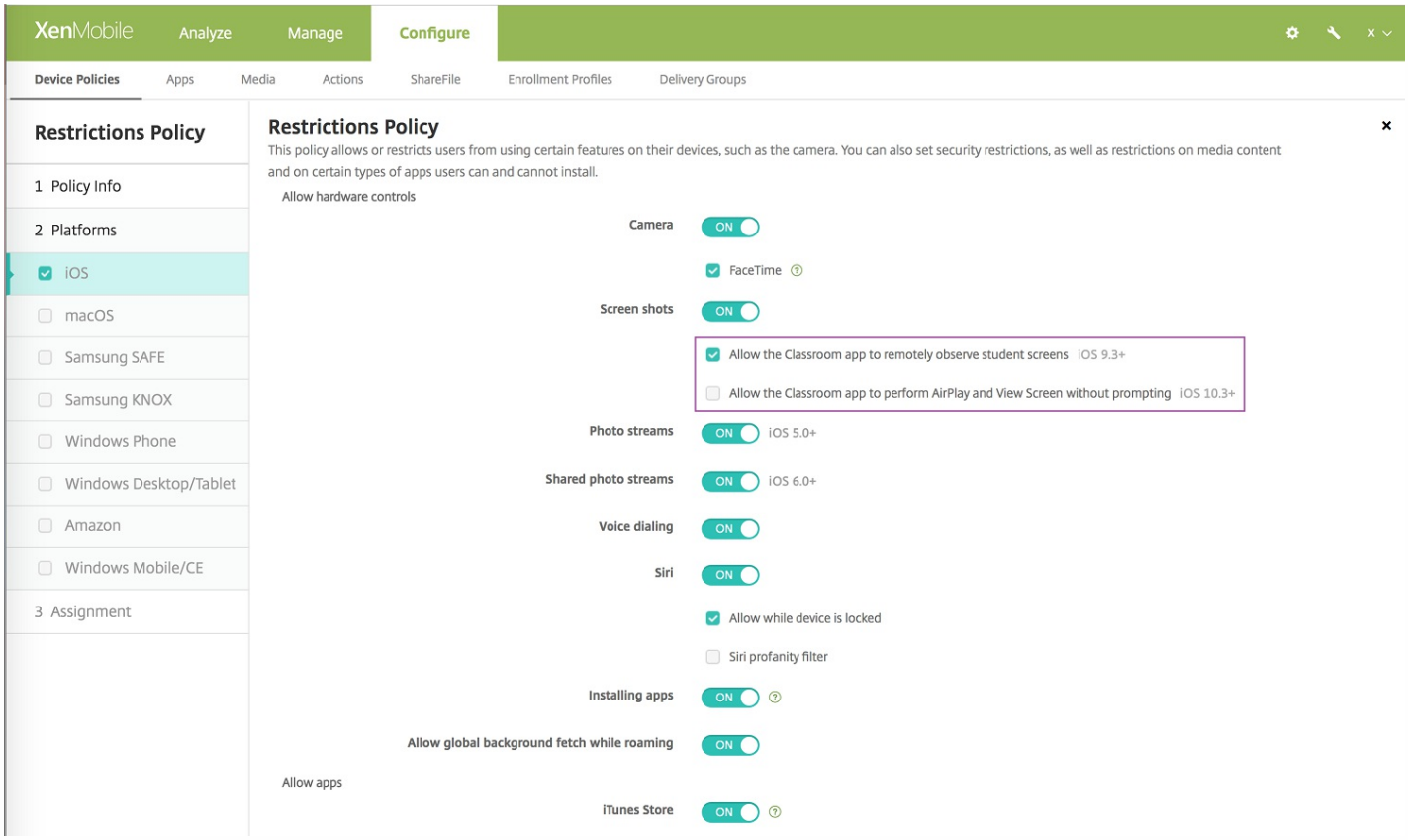
Para adicionar ou configurar a política, acesse **Configurar > Políticas de dispositivo**.

2. Clique em **Adicionar**. A página **Adicionar uma nova política** é exibida.

3. Clique em **Restrições**. A página de restrições **Informações sobre a política** é exibida.

iOS

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Configurações de iOS

Nota: Algumas das opções de restrições do iOS se aplicam somente a versões específicas do iOS (e, onde aplicável, essas versões estão descritas na página do console XenMobile). Por exemplo, a capacidade de permitir ou bloquear o AirDrop é compatível somente em dispositivos que executam o iOS 7 e versões posteriores. A capacidade de permitir ou bloquear fluxos de fotos do Photo Stream é compatível somente em dispositivos que executam o iOS 5 e versões posteriores. Além disso, algumas opções se aplicarão somente se o dispositivo for colocado no modo supervisionado. 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.

- **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. Essa restrição é desaconselhada em dispositivos iOS 10 não 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 supervisionados executando o iOS 9.3 (versão mínima).
    - **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 supervisionados executando o iOS 10.3 (versão mínima).
  - **Fluxos de foto**: permitir que os usuários usem o MyPhotoStream para compartilhar fotos usando o iCloud com todos os dispositivos iOS deles (disponível no iOS 5.0 e versões posteriores).
  - **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 (disponível no iOS 6.0 e versões posteriores).
  - **Discagem por voz**: ativa a discagem por voz nos dispositivos do usuário.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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. Essa restrição é desaconselhada em dispositivos iOS 10 não 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. Essa restrição é desaconselhada em dispositivos iOS 10 não 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 (iOS 5.0 e versões posteriores).
  - **Safari**: permitir que os usuários acessem o Safari. Essa restrição é desaconselhada em dispositivos iOS 10 não 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 (iOS 5.0 e versões posteriores). Essa restrição é desaconselhada em dispositivos iOS 10 não supervisionados.
  - **Backup do iCloud**: permitir que os usuários façam backup dos dispositivos deles no iCloud (iOS 5.0 e versões posteriores).
  - **Chaves do iCloud**: permitir que os usuários armazenem senhas, informações da rede WiFi e informações de cartão de crédito, entre outras, em Chaves do iCloud (iOS 7.0 e versões posteriores).
  - **Biblioteca de fotos na nuvem**: permitir que os usuários acessem a respectiva biblioteca de fotos do iCloud (iOS 9.0 e versões posteriores).
- **Segurança - Força**
  O padrão é restringir os recursos a seguir, o que significa que nenhum dos recursos de segurança é ativado.

  - **Backups criptografados**: Força a criptografia dos backups no iCloud.
  - **Rastreamento de anúncios limitado**: bloquear o acompanhamento de anúncios direcionados (iOS 7.0 e versões posteriores).
  - **Código secreto no primeiro emparelhamento do AirPlay**: exigir que os dispositivos ativados para AirPlay sejam verificados com um código de uso único na tela antes que eles possam usar o AirPlay (disponível no iOS 7.0 e versões posteriores).
  - **Apple Watch emparelhado para usar detecção de pulso**: exigir um Apple Watch emparelhado para usar a **detecção de pulso** (iOS 8.2 e versões posteriores).
  - **Compartilhamento de documentos gerenciados com o AirDrop:** o acesso ao AirDrop é uma opção supervisionada. Definir essa opção como **I** permite que os dispositivos supervisionados usem o AirDrop para compartilhar dados e mídia com dispositivos iOS próximos (iOS 9.0 e versões posteriores).
- **Segurança - Permitir**
  - **Aceitar certificados SSL não confiáveis**: permitir que os usuários aceitem certificados SSL não confiáveis de sites (iOS 5.0 e

© 1999-2017 Citrix Systems, Inc. All rights reserved.

versões posteriores).

- **Atualização automática de definições de segurança do certificado**: permitir que certificados confiáveis sejam atualizados automaticamente (iOS 7.0 e versões posteriores).
- **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 (iOS 7.0 e versões posteriores).
- **Notificações do Passbook quando o dispositivo está bloqueado**: permitir que notificações do Passbook apareçam na tela de bloqueio (iOS 6.0 e versões posteriores).
- **Handoff**: permitir que os usuários transfiram as atividades de um dispositivo iOS para outro dispositivo iOS próximo (iOS 8.0 e versões posteriores).
- **Sincronização do iCloud para aplicativos gerenciados**: permitir que os usuários sincronizem aplicativos gerenciados com o iCloud (iOS 8.0 e versões posteriores).
- **Backup para livros da empresa**: permitir o backup de livros da empresa para o iCloud (iOS 8.0 e versões posteriores).
- **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 (iOS 8.0 e versões posteriores).
- **Confiança de aplicativo empresarial**: permitir que aplicativos empresariais sejam confiáveis (iOS 9.0 e versões posteriores).
- **Resultados de Internet no Spotlight**: permitir que o Spotlight mostre os resultados da pesquisa da Internet, bem como do dispositivo (iOS 8.0 e versões posteriores).

- **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 (iOS 8.0 e versões posteriores).
  - **Configuração de restrições**: permitir que os usuários configurem os controles dos pais nos dispositivos deles (iOS 8.0 e versões posteriores).
  - **Podcasts**: permitir que os usuários baixem e sincronizem podcasts (iOS 8.0 e versões posteriores).
  - **Instalação de perfis de configuração**: permitir que os usuários instalem um perfil de configuração diferente daquele implantado por você (iOS 6.0 e versões posteriores).
  - **Modificação de impressão digital**: permitir que os usuários alterem ou apaguem a impressão digital Touch ID deles (iOS 8.3 e versões posteriores).
  - **Instalação de aplicativos do dispositivo:** (iOS 9.0 e versões posteriores).
  - **Atalhos de teclado**: permitir que os usuários criem atalhos de teclado personalizados para palavras ou frases que usam com frequência (iOS 9.0 e versões posteriores).
  - **Relógio emparelhado**: permitir que os usuários emparelhem um Apple Watch com um dispositivo supervisionado (iOS 9.0 e versões posteriores).
  - **Modificação de código secreto**: permitir que os usuários alterem a senha em um dispositivo supervisionado (iOS 9.0 e versões posteriores).
  - **Modificação do nome do dispositivo**: permitir que os usuários alterem o nome do seu dispositivo.
  - **Modificação do papel de parede**: permitir que o usuário altere o papel de parede nos dispositivos deles (iOS 9.0 e versões posteriores).
  - **Download automático de aplicativos** (iOS 9.0 e versões posteriores).
  - **AirDrop**: permitir que os usuários compartilhem fotos, vídeos, sites, locais, entre outros, com dispositivos iOS próximos (iOS 7.0 e versões posteriores).
  - **iMessage**: permitir que os usuários enviem mensagens de texto sobre WiFi usando o iMessage (iOS 6.0 e versões posteriores).
  - **Conteúdo gerado pelo usuário de Siri**: Permitir que a Siri consulte conteúdo gerado pelo usuário na Web. Os

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 (iOS 7.0 e versões posteriores).

- **iBooks**: permitir que os usuários usem o aplicativo iBooks (iOS 6.0 e versões posteriores).
- **Remoção de aplicativos**: permitir que usuários removam aplicativos dos dispositivos deles (iOS 7.0 e versões posteriores).
- **Game Center**: permitir que os usuários joguem jogos online usando o Game Center nos dispositivos deles (iOS 6.0 e versões posteriores).
  - **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 (iOS 7.0 e versões posteriores).
- **Modificando configurações de dados celulares do aplicativo**: permitir que os usuários modifiquem a forma como os aplicativos usam dados celulares (iOS 7.0 e versões posteriores).
- **Modificando configurações de Encontrar meus amigos**: permitir que os usuários alterem as respectivas configurações de Encontrar meus amigos (iOS 7.0 e versões posteriores).
- **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 (iOS 7.0 e versões posteriores).
- **Teclados intuitivos**: permitir que os dispositivos dos usuários usem teclados intuitivos para sugerir palavras conforme eles digitam (iOS 8.1.3 e versões posteriores). 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 (iOS 8.1.3 e versões posteriores). 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 (iOS 8.1.3 e versões posteriores). 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 (iOS 8.1.3 e versões posteriores). 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**: Crie 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 ou mais aplicativos, clique em **Adicionar** e faça o seguinte:

  a. **Nome do aplicativo**: insira um nome de aplicativo.
  b. Clique em **Salvar** ou em **Cancelar**.
  c. Repita as etapas a e b para cada aplicativo que você desejar adicionar.

  Dica: para excluir um aplicativo existente, passe o mouse sobre a linha que contém o nome do aplicativo e, em seguida, 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 aplicativo existente, passe o mouse sobre a linha que contém a o nome do aplicativo e clique no ícone de caneta à direita.

- **News**: permitir que os usuários usem o aplicativo News (iOS 9.0 e versões posteriores).
- **Serviço Apple Music**: permitir que os usuários usem o serviço Apple Music (iOS 9.3 e versões posteriores). Se você não permitir o serviço Apple Music, o aplicativo Música será executado no modo clássica.
- **iTunes Radio**: permite que os usuários usem o iTunes Radio (iOS 9.3 e versões posteriores).
- **Modificação de notificações** permitir que os usuários modifiquem configurações de notificação (iOS 9.3 e versões posteriores).
- **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 (iOS 9.3 e versões posteriores). Aplica-se somente a dispositivos supervisionados.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 Apple DEP para fazer login em suas contas Apple no Assistente de Instalação. Caso contrário, os usuários podem ter que desativar a autenticação de duas 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 Diagnóstico e uso em Configurações (iOS 9.3.2 e versões posteriores).
- **Modificação de Bluetooth**: permitir que os usuários modifiquem configurações de Bluetooth (iOS 10.0 e versões posteriores).
- **Permitir ditado**: supervisionado somente. Se essa restrição é definida como **Desativado**, a entrada de ditado não é permitida. A configuração padrão é **Ativado**. Para iOS 10.3 e posterior.
- **Entrar somente em redes WiFi instaladas por uma política de WiFi**: opcional Apenas supervisionado. Se esta restrição estiver definida como **Ativar**, 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**. Para iOS 10.3 e posterior.

- **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 supervisionados executando o iOS 10.3 (versão mínima).
- **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

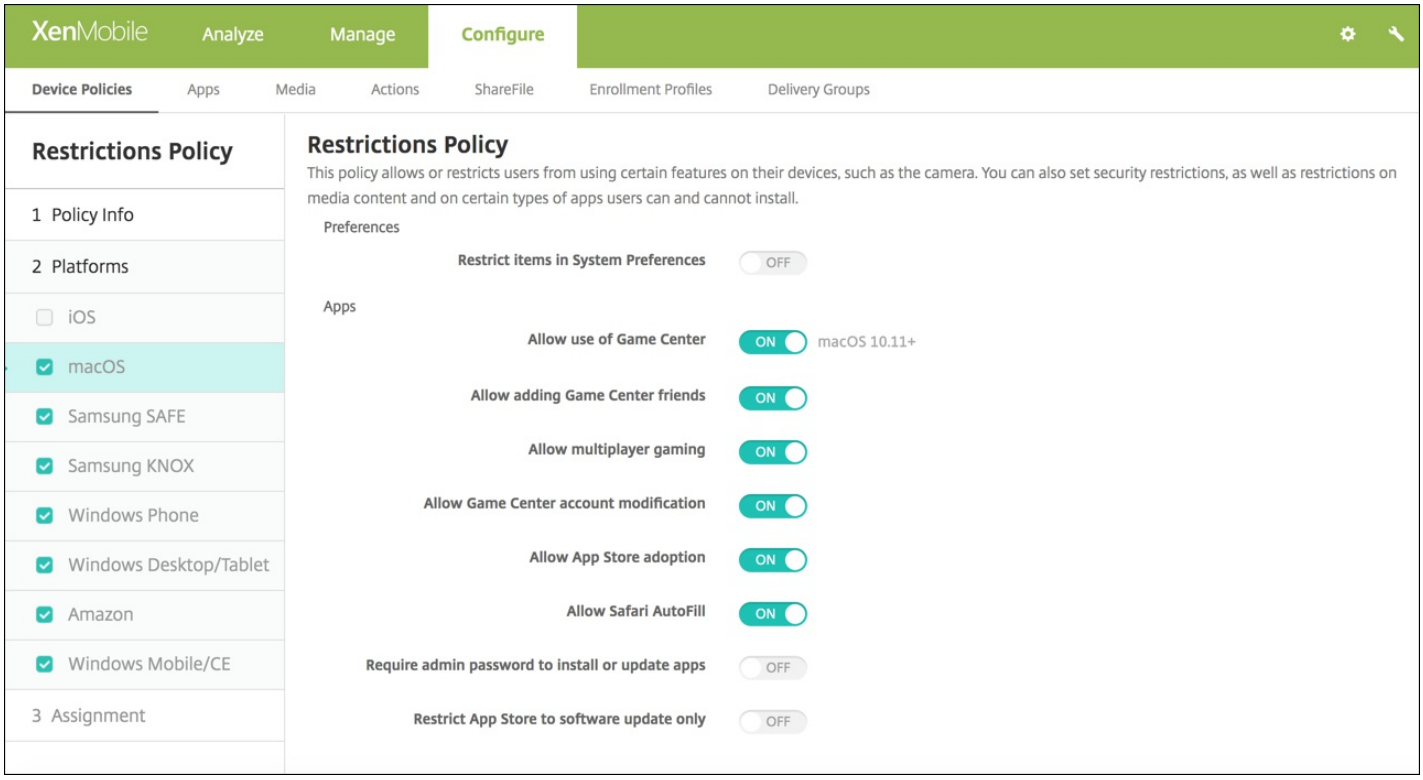
© 1999-2017 Citrix Systems, Inc. All rights reserved.

configurar novos dispositivos próximos. A configuração padrão é Ativado. Para dispositivos supervisionados executando o iOS 11 (versão mínima).

- **Segurança - Mostrar na tela de bloqueio**
  - **Centro de controle**: permitir acesso ao Centro de controle na tela de bloqueio, o que permite que os usuários modifiquem facilmente as configurações de Modo avião, WiFi, Bluetooth, Modo não perturbe e Bloquear rotação (iOS 7.0 e versões posteriores).
  - **Notificação**: permitir notificações na tela de bloqueio (iOS 7.0 e versões posteriores).
  - **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 (iOS 6.0 e versões posteriores).
  - **Região de classificações**: Defina 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**: Defina 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**: Defina 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**: Defina 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**
  - 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 de perfil**, digite a senha necessária.

macOS

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Configurações do macOS

- **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**: selecione 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

    - Notificações
    - Controles dos Pais
    - Impressoras e Scanners
    - Perfis
    - Segurança e Privacidade
    - Compartilhamento
    - Som
    - Dicção 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 **Ativado**.
    - **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 **Ativado**.
    - **Permitir jogos multiplayer**: permitir que os usuários iniciem jogos multiplayer. O padrão é **Ativado**.
    - **Permitir modificação de conta do Game Center**: permitir que os usuários modifiquem as próprias configurações de conta do Game Center. O padrão é **Ativado**.
    - **Permitir adoção da App Store**: permitir ou restringir a adoção de aplicativos que existiam previamente no OS X pela App Store. 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 **Ativado**.
    - **Exigir uma senha para instalar ou atualizar aplicativos**: exigir uma senha de administrador para instalar ou atualizar aplicativos. O padrão é **O**, 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 **O**, 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, /Applications/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 **O**, 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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 **O**, 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 **O**, 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 **O**, o que impede que os usuários utilizem as Sugestões do Spotlight. Para obter mais informações sobre as Sugestões do Spotlight, consulte a página Sugestões do Spotlight da Apple.
  - **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 O, 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 opção significa que o usuário usará somente um ID e uma senha para *todas* as telas de login nos respectivos Macs. O padrão é **I**, 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 **O**, o que impede que os usuários usem documentos e dados do iCloud nos Macs deles. Para obter mais informações, consulte a página Documentos e dados do iCloud da Apple.
    - **Permitir área de trabalho e documentos iCloud**: (macOS 10.12.4 e posterior) Selecionada por padrão.
  - **Permitir sincronização de chaves do iCloud**: permitir a sincronização de chaves do iCloud (macOS 10.12 e versões posteriores). O padrão é **Ativado**.
  - **Permitir Mail do iCloud**: permitir que os usuários usem o iCloud Mail (macOS 10.12 e versões posteriores). O padrão é **Ativado**.
  - **Permitir Contatos do iCloud**: permitir que os usuários usem os Contatos do iCloud (macOS 10.12 e versões posteriores). O padrão é **Ativado**.
  - **Permitir Calendários do iCloud**: permitir que os usuários usem os Calendários do iCloud (macOS 10.12 e versões posteriores). O padrão é **Ativado**.
  - **Permitir Lembretes do iCloud**: permitir que os usuários usem os Lembretes do iCloud (macOS 10.12 e versões posteriores). O padrão é **Ativado**.
  - **Permitir Favoritos do iCloud**: permitir que os usuários sincronizem com os Favoritos do iCloud (macOS 10.12 e versões posteriores). O padrão é **Ativado**.
  - **Permitir Notas do iCloud**: permitir que os usuários usem as Notas do iCloud (macOS 10.12 e versões posteriores). O padrão é **Ativado**.
  - **Permitir fotos do iCloud**: se você alterar essa configuração para **O**, 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 **Ativado**.
  - **Permitir desbloqueio automático**: para obter informações sobre essa opção e o Apple Watch, consulte http://www.imore.com/auto-unlock (macOS 10.12 e posterior). O padrão é **Ativado**.
  - **Permitir Touch ID para desbloquear Mac**: (macOS 10.12.4 e posterior). O padrão é **Ativado**.
- **Configuração 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 de perfil**, digite a senha necessária.

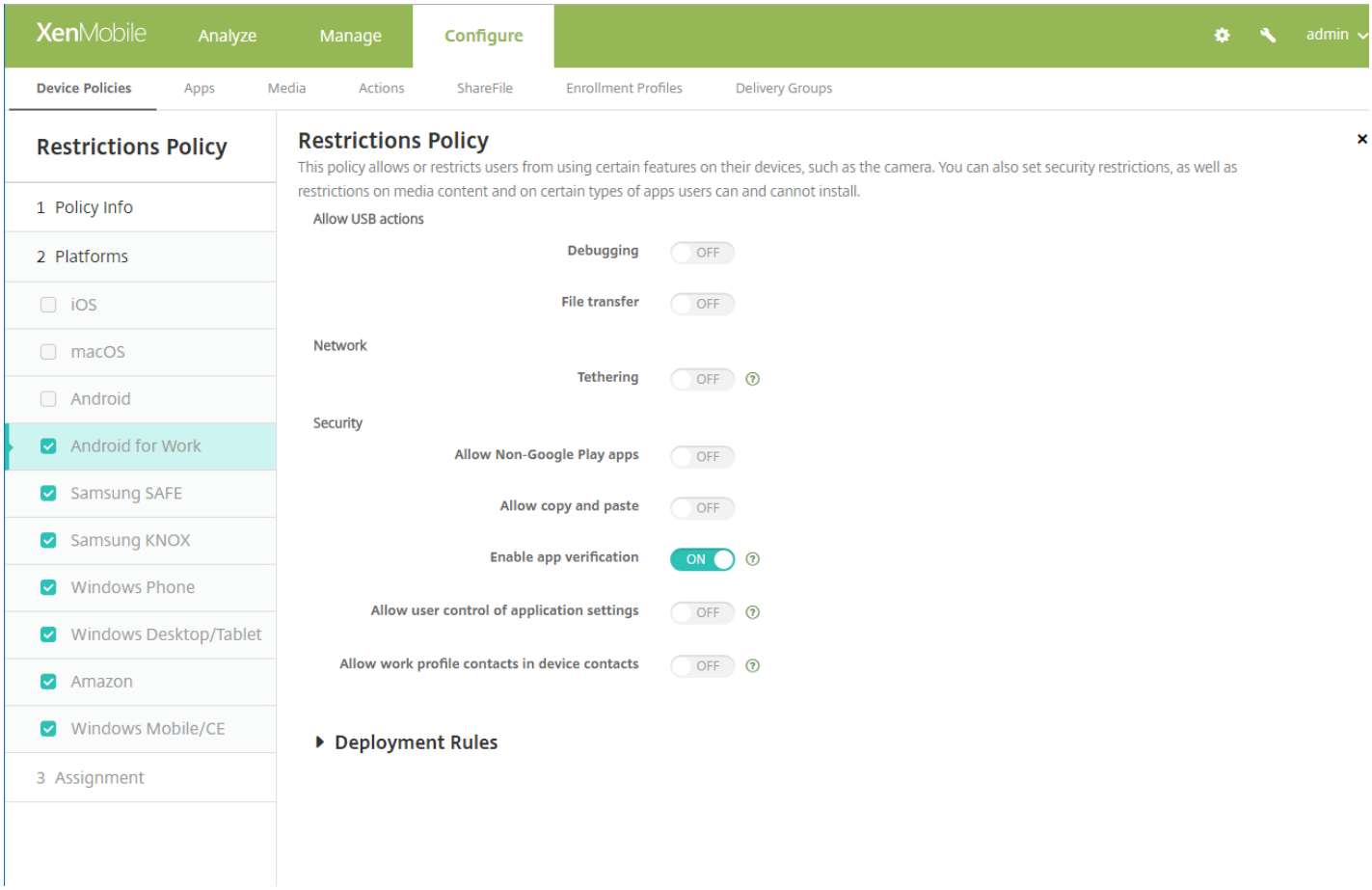
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Na lista **Escopo do perfil**, clique em **Usuário** ou **Sistema** (macOS 10.7 e versões posteriores).

Android

- **Câmera:** Permitir que os usuários usem a câmera nos dispositivos deles. Se o valor for **o**, a câmera está desabilitada. O padrão é **I**.

Android for Work



Por padrão, as configurações de Depuração de USB e Fontes desconhecidas são desativadas em um dispositivo quando ele é registrado no Android for Work no modo de perfil de trabalho.

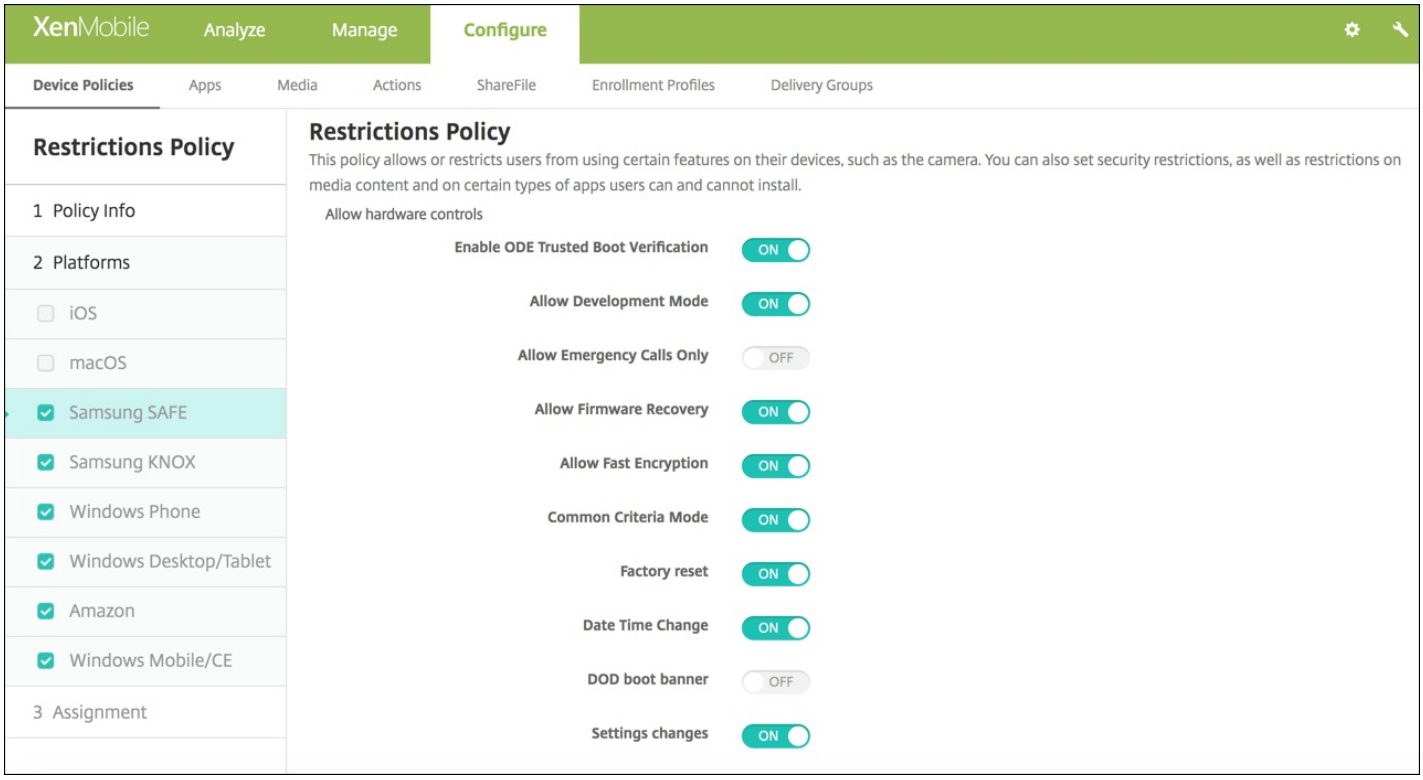
- **Depuração**: permite a depuração por USB (Android 5.0 e versões posteriores). O valor padrão é **Desativado**.
- **Transferência de arquivos**: permite a transferência de arquivos por USB (Android 5.0 e versões posteriores). O valor padrão é **Desativado**.
- **Tethering**: permite que os usuários configurem hotspots portáteis e vinculem dados (Android 5.0 e versões posteriores). O valor padrão é **Desativado.**
- **Permitir aplicativos não Google Play**: permite a instalação de aplicativos de lojas diferentes da Google Play (Android 5.0 e posterior). O valor padrão é **Desativado**.
- **Permitir copiar e colar**: permite ou impede o uso da área de transferência para copiar e colar entre aplicativos no perfil do Android for Work e aplicativos na área pessoal (Android 5.0 e posterior). O valor padrão é **Desativado**.
- **Ativar verificação de aplicativo**: permite que o sistema operacional verifique os aplicativos para detectar comportamentos mal-intencionados (Android 5.0 e posterior). O padrão é **Ativado**.
- **Permitir o controle do usuário das configurações do aplicativo**: permite que os usuários desinstalem aplicativos,

© 1999-2017 Citrix Systems, Inc. All rights reserved.

desativem aplicativos, limpem o cache e os dados, forcem a interrupção de qualquer aplicativo e cancelem os padrões (Android 5.0 e posterior). O valor padrão é **Desativado**.

- **Permitir contatos do perfil de trabalho nos contatos do dispositivo**: mostra contatos do perfil gerenciado do Android for Work no perfil pai, para chamadas recebidas (Android 7.0 e posterior). O valor padrão é **Desativado**.

Samsung SAFE



Configurações do Samsung SAFE

Nota: algumas opções estão disponíveis somente em APIs específicas de gerenciamento de dispositivo móvel da Samsung; elas estão marcadas com as informações de versão relevantes.

- **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 de critérios comuns**: colocar o dispositivo no modo de Critérios comuns. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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).
- **Captura 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 **O**.

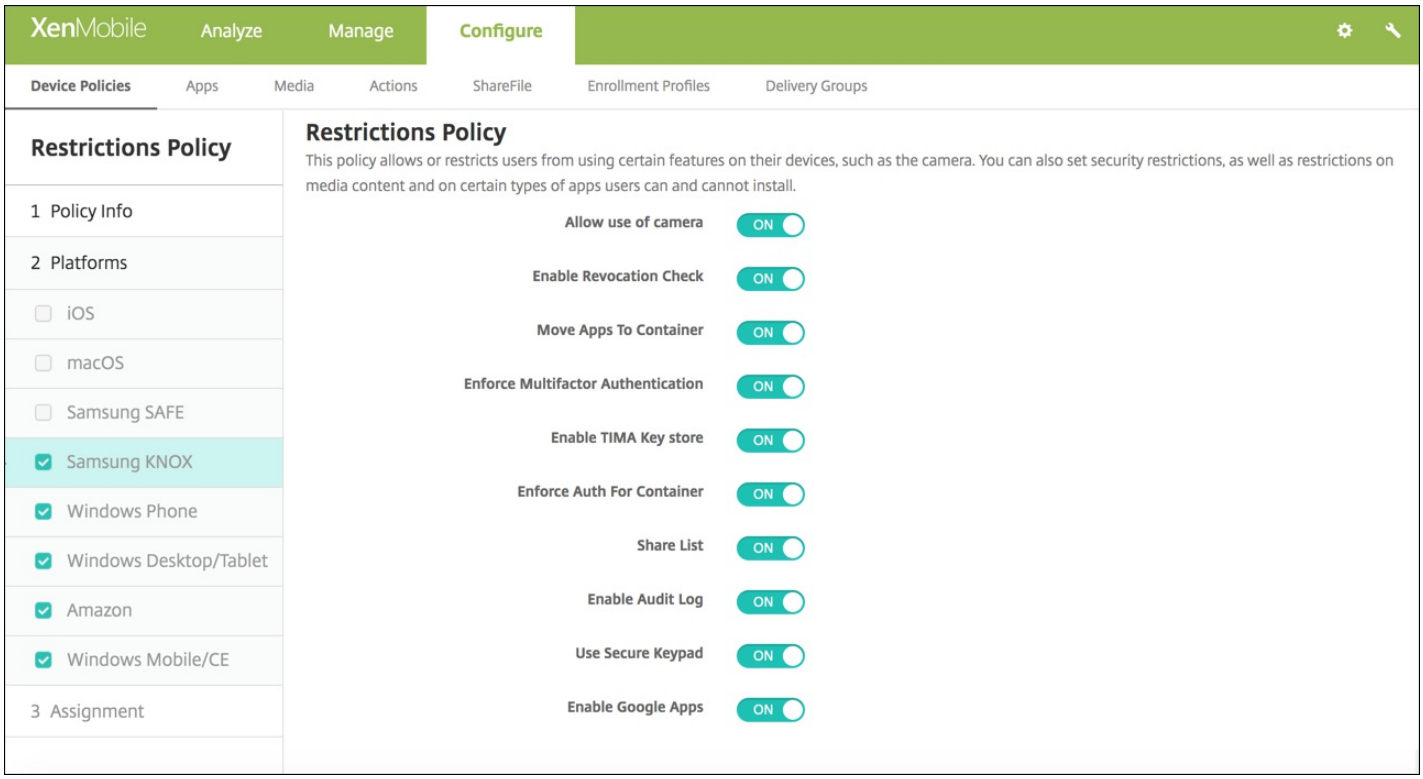
- **Permitir aplicativos**
  - **Navegador**: permitir que os usuários usem o navegador da Web.
  - **Youtube**: permitir que os usuários acessem o YouTube.
  - **Google Play/Marketplace**: permitir que os usuários acessem o Google Play e o Google Apps Marketplace.
  - **Permitir aplicativos não Google 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.
  - **WiFi**: permitir que usuários se conectem a redes WiFi.
    - **Tethering**: permitir que os usuários compartilhem uma conexão de dados móvel com outro dispositivo usando a conexão WiFi.
    - **Direto**: permitir que os usuários se conectem diretamente a outro dispositivo usando uma conexão WiFi (MDM 4.0 e versões posteriores).
    - **Alteração de estado**: permitir que os aplicativos alterem o estado da conectividade WiFi.
    - **Alterações de política de usuário**: permitir que os usuários alterem as políticas de WiFi. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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.

Samsung KNOX



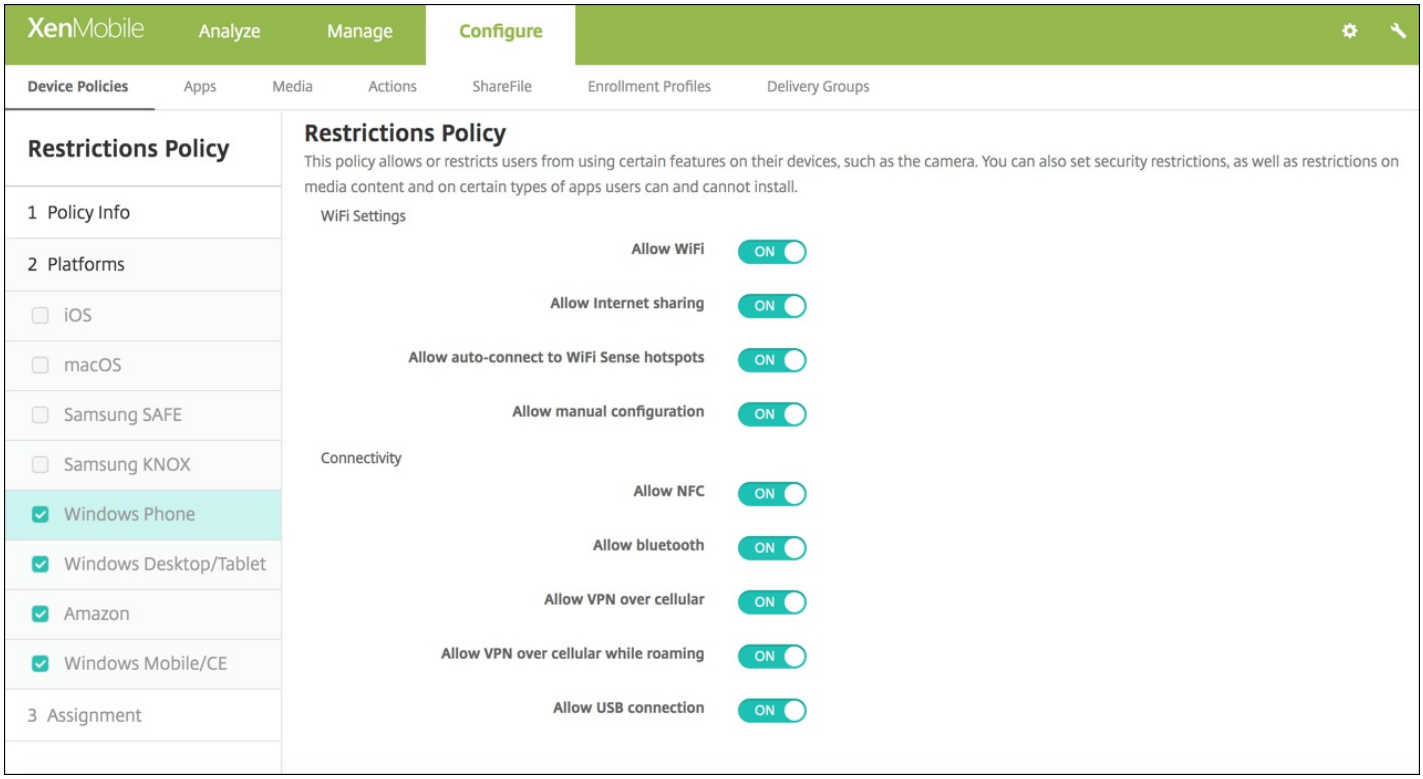
Configurações do Samsung KNOX

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nota: 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 usarem 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.

Windows Phone e Windows Desktop/Tablet



Configurações do Windows Phone e do Windows Desktop/Tablet

- **Configurações de WiFi**
  - **Permitir WiFi**: permitir que um dispositivo se conecte a uma rede WiFi. 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 hotspot WiFi.
  - **Permitir a conexão automática com pontos de acesso WiFi Sense**: permitir que um dispositivo se conecte

© 1999-2017 Citrix Systems, Inc. All rights reserved.

automaticamente a hotspots 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 WiFi. 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 **Destivado**, 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.
- **Sistema**
    - **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 **O**.
    - **Permitir copiar e colar**: permitir que os usuários copiem e colem 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

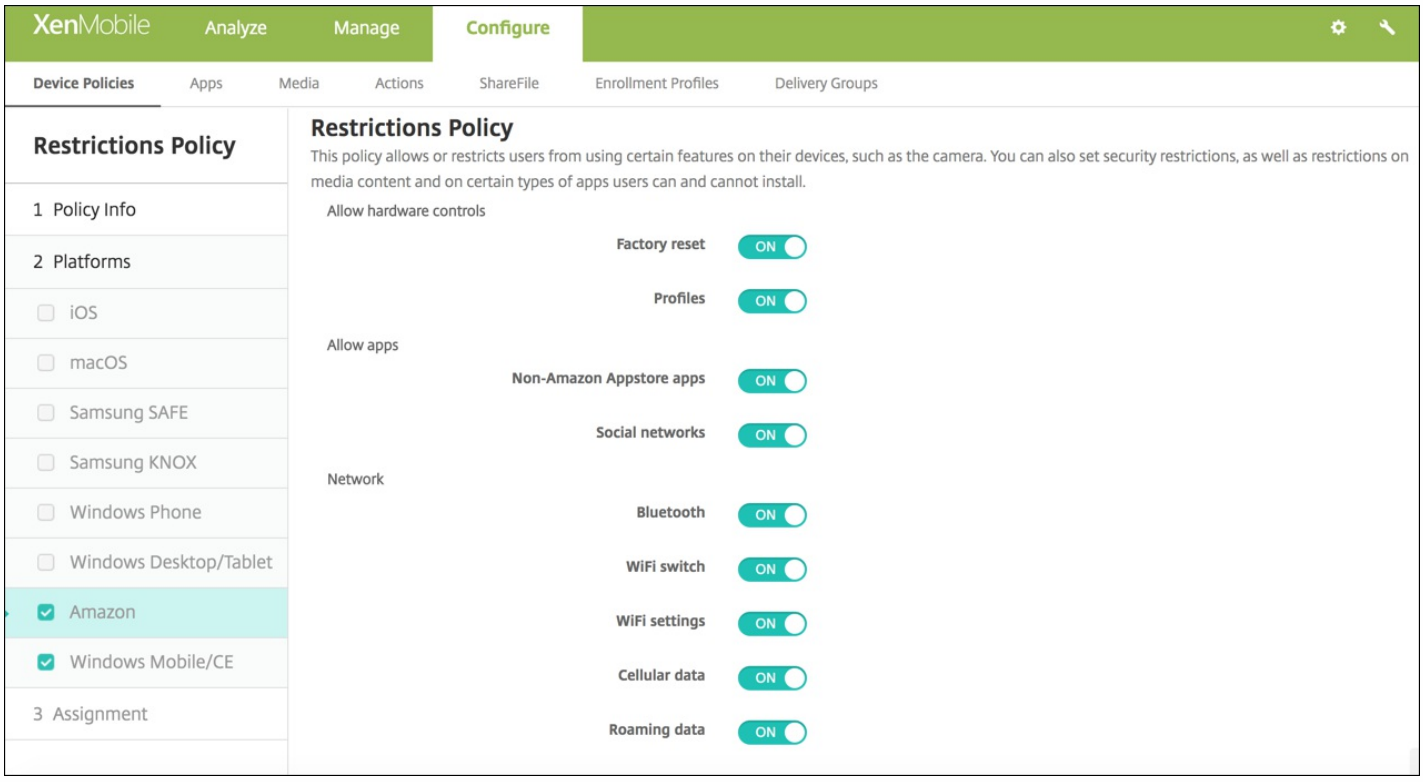
© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 entrada:** 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.

Amazon

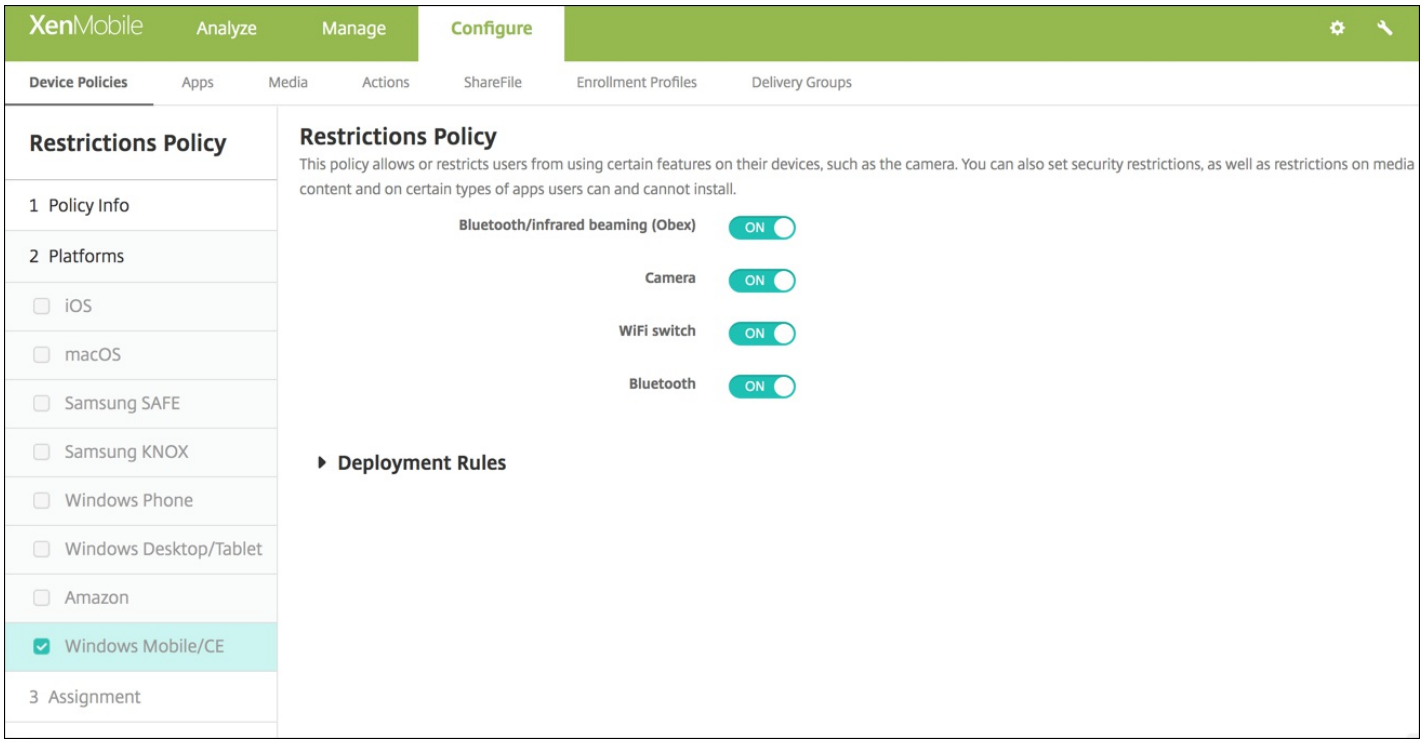


© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurações do Amazon

- **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 WiFi.
  - **Configurações de WiFi**: permitir que os usuários alterem as configurações de WiFi.
  - **Dados celulares**: permitir que os usuários usem a conexão celular deles para dados.
  - **Dados de roaming**: permitir que os usuários usem dados celulares 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.

Windows Mobile/CE



Configurações do Windows Mobile/CE

- **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 WiFi.
- **Bluetooth**: ativar Bluetooth nos dispositivos dos usuários.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo em roaming

Feb 21, 2018

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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Clique em **Mais** e, em **Acesso à rede**, clique em **Roaming**. A página de informações **Política de roaming** é exibida.

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 as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

Definir as configurações do iOS

Defina estas configurações:

- **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.

Definir as configurações do Windows Mobile/CE

Defina estas configurações:

- **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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

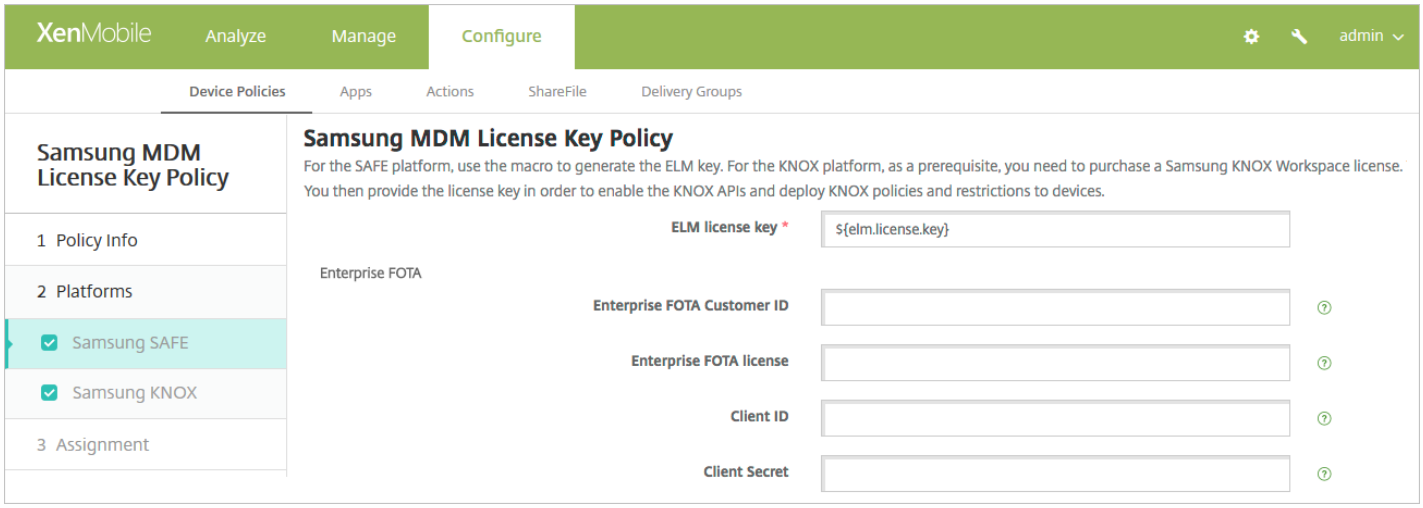
7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de chave de licença MDM Samsung

Feb 21, 2018

Configurações do Samsung SAFE



- **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

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.

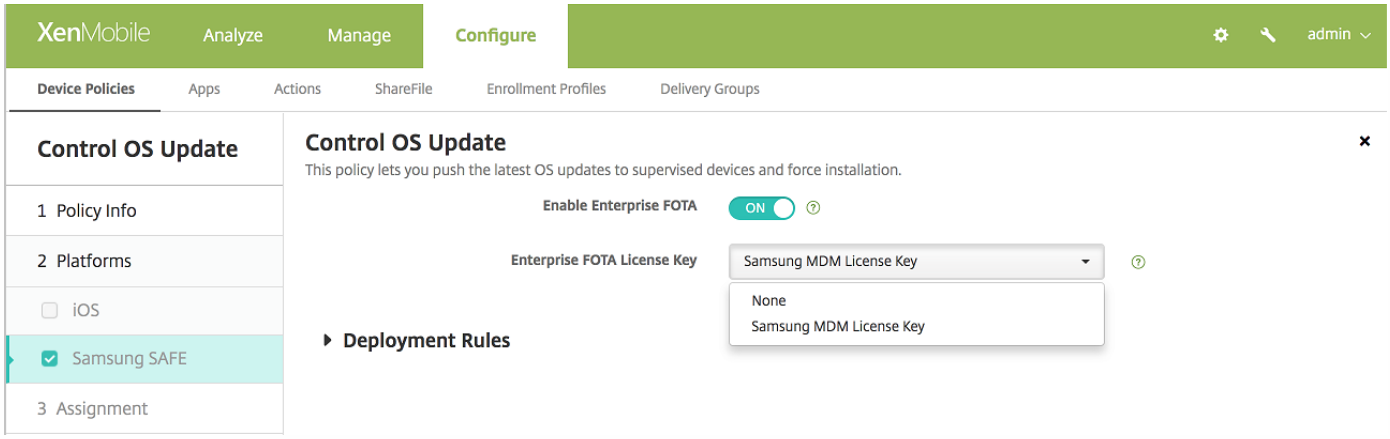
   Digite a **chave de licença ELM**: o XenMobile preenche previamente esse campo com a macro que gera a chave de licença ELM. Se o campo estiver em branco, digite esta macro ${elm.license.key}

   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. Crie uma política de dispositivo de controle de atualização do sistema operacional.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

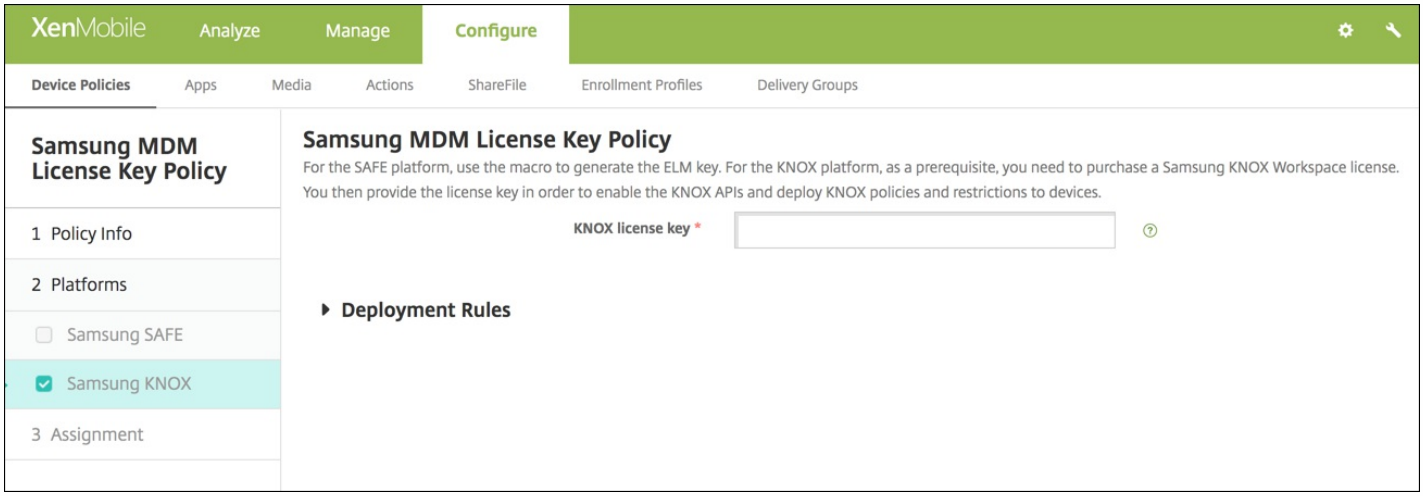


Defina estas configurações:

- **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 Samsung KNOX



Configure esta definição:

- **Chave de licença KNOX**: Digite a chave de licença KNOX que você obteve da Samsung.

> ## Nota
>
> Nota
>
> Para obter informações gerais sobre como configurar políticas, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de firewall do Samsung SAFE

Feb 21, 2018

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 desejar permitir ou bloquear. Você também pode definir o proxy e as configurações de redirecionamento do proxy.

Para adicionar essa política, acesse **Configurar > Políticas de dispositivo**.

Após adicionar um novo item à tabela: para editar um item existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Para excluir um item existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de lixeira à direita.

Configurações do Samsung SAFE

- **Permitir/Negar Hosts**
  Para cada host ao qual você desejar 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 desejar 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.
- **Configuração de redirecionamento**
  Para cada proxy que você desejar 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.

> ### Nota
>
> Para obter informações gerais sobre como configurar políticas, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo do SCEP

Feb 21, 2018

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 desejar 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.

Configurações do iOS

Configurações do macOS

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. A caixa de diálogo **Adicionar uma nova política** é exibida.

3. Expanda **Mais** e, em **Segurança**, clique em **SCEP**. A página de informações **Política de SCEP** é exibida.

4. No painel **Informações sobre a política**, digite as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

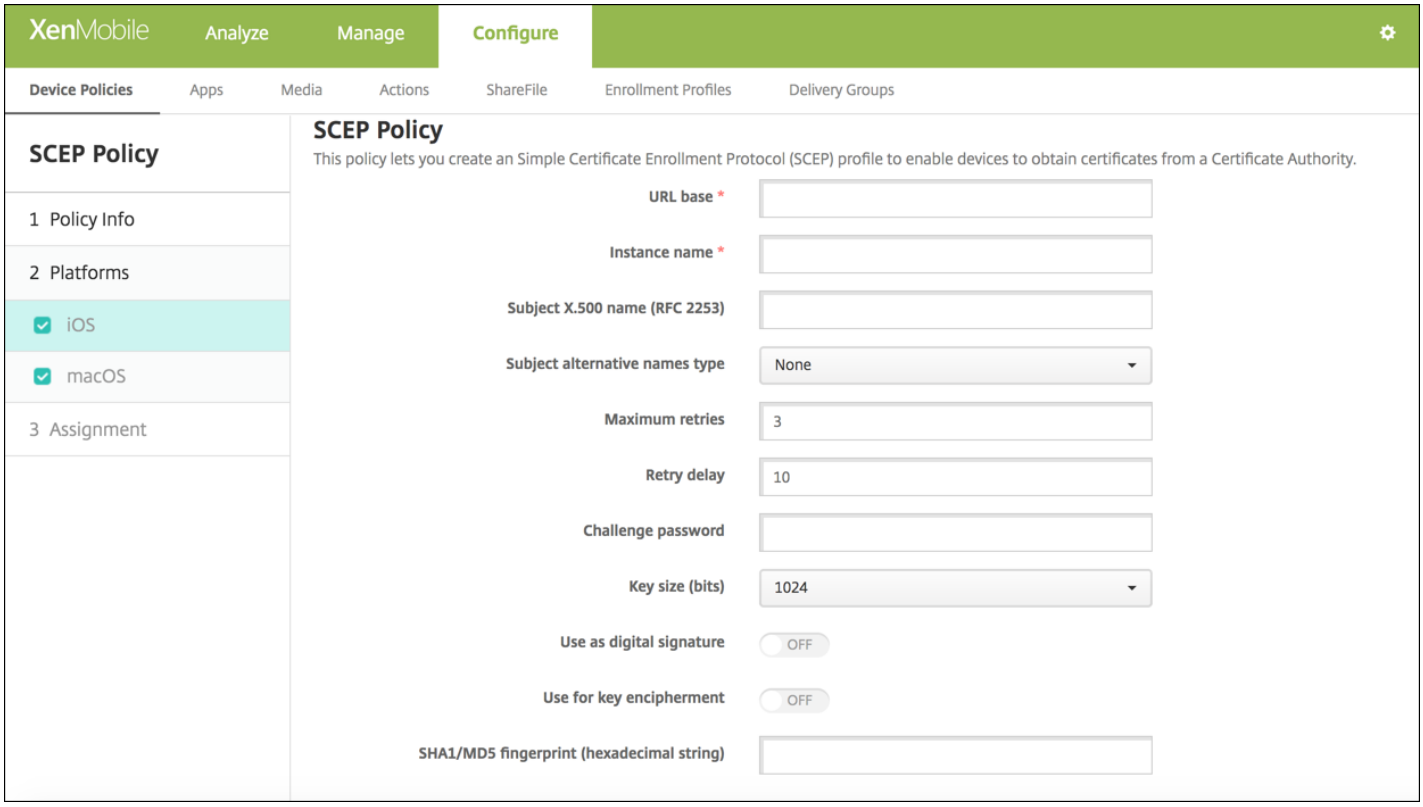
5. Clique em **Avançar**. A página **Plataformas** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

Definir as configurações do iOS

© 1999-2017 Citrix Systems, Inc. All rights reserved.



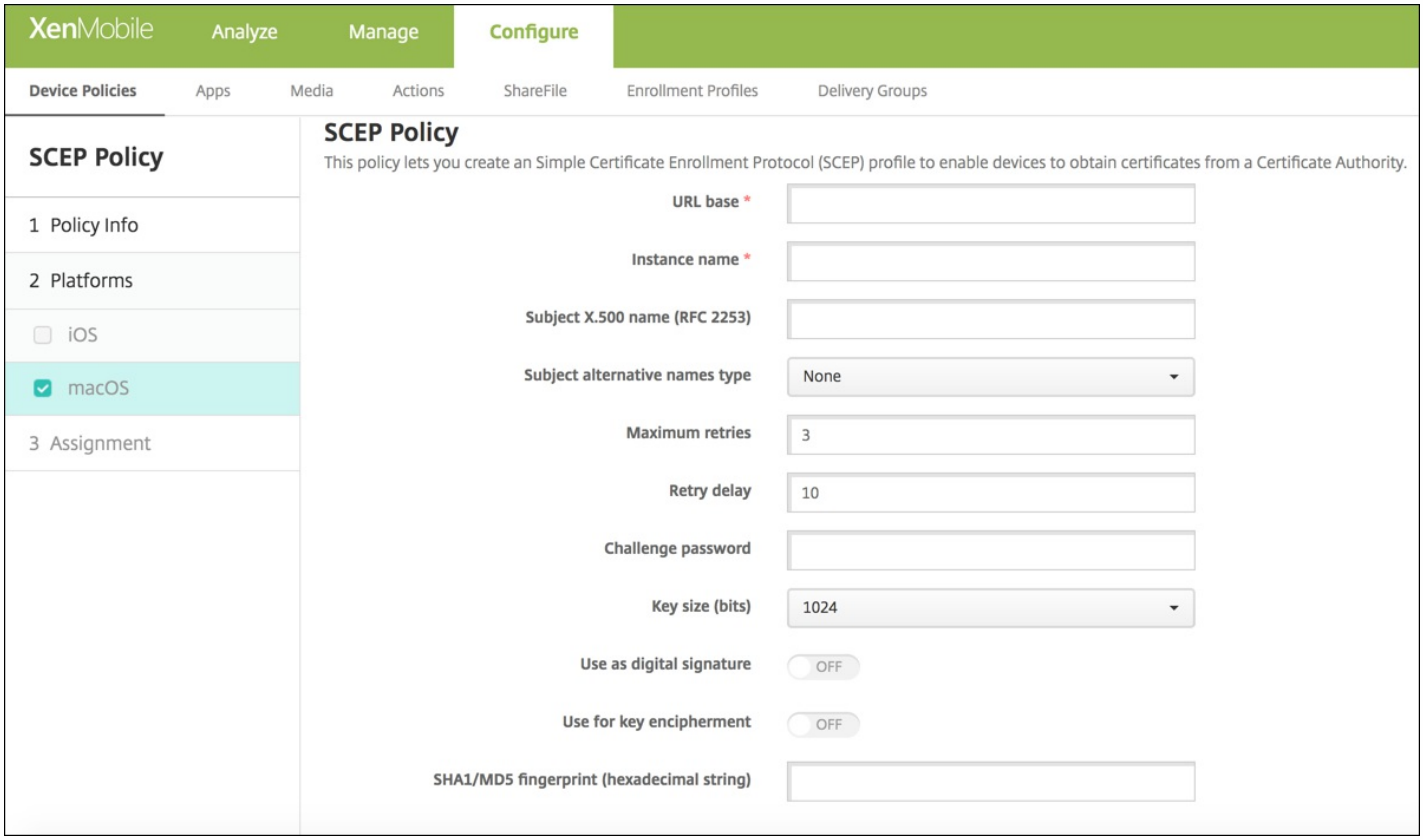
Defina estas configurações:

- **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)**: na lista, clique no tamanho da chave em bits, **1024** ou **2048**. O padrão é **1024**.
- **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 descriptografar o hash.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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**
  - 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 de perfil**, digite a senha necessária.

Defina as configurações do macOS



Defina estas configurações:

- **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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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**.
- **Verificar senha**: insira um segredo pré-compartilhado.
- **Tamanho da chave (bits)**: na lista, clique no tamanho da chave em bits, **1024** ou **2048**. O padrão é **1024**.
- **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 descriptografar 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**
  - 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 de perfil**, digite a senha necessária.
  - Ao lado de **Escopo do perfil**, clique em **Usuário** ou **Sistema**. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

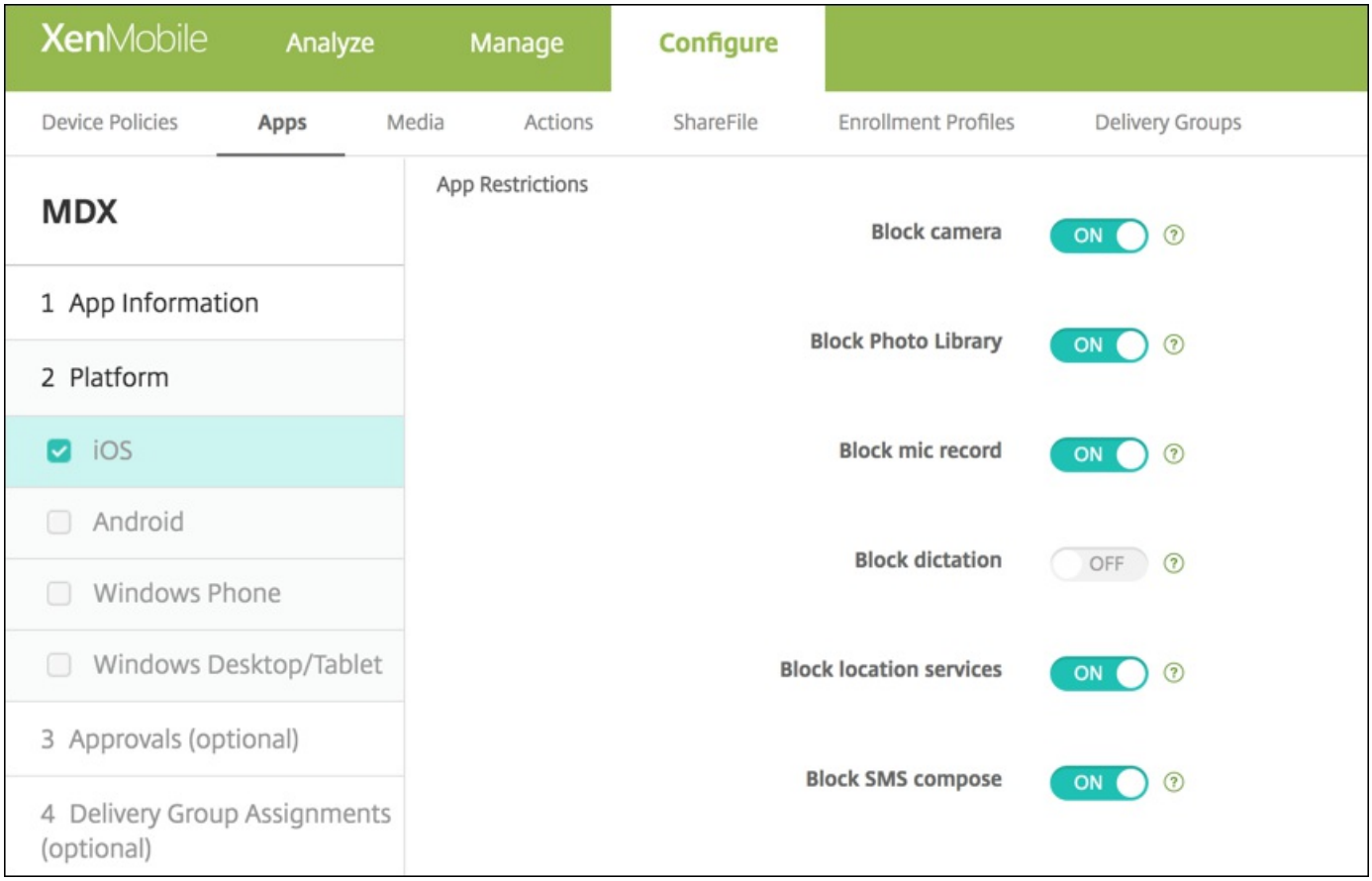
Siri e políticas de ditado

Feb 21, 2018

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.

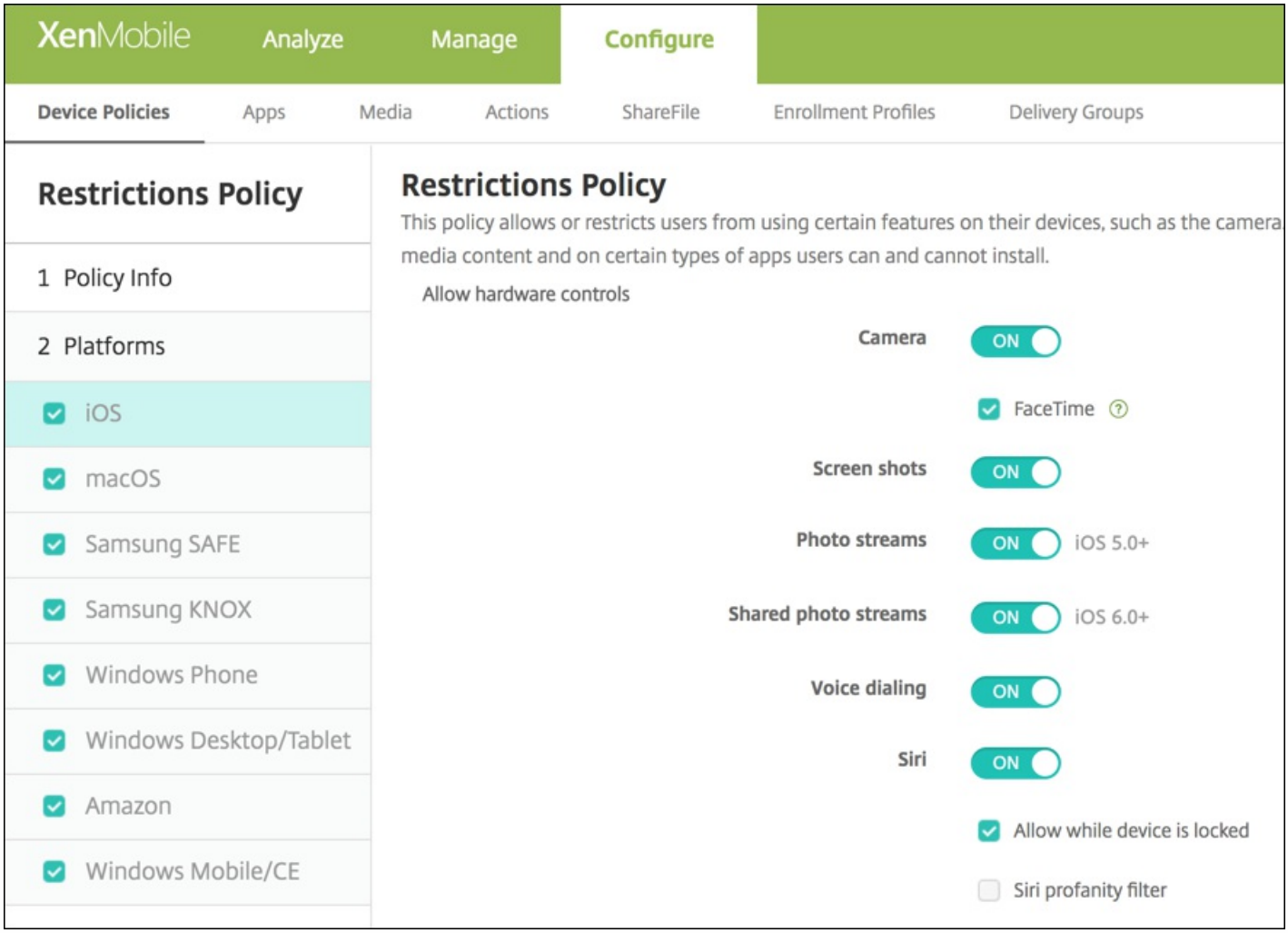
O XenMobile permite que você bloqueie a Siri e os serviços de ditado de acordo com o que determinam suas necessidades de segurança.

Em implantações MAM, a política **Bloquear ditado** para cada aplicativo é **I** por padrão, o que desativa o microfone do dispositivo. Configure como **O** 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**.



Em implantações MDM, você também pode desabilitar a Siri com a política da Siri em **Configurar Siri > Políticas de dispositivo > Política de restrições > iOS**. O uso do Siri é permitido por padrão.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 Apple reveals how long Siri keeps your data.
- Você pode revisar a política de privacidade da Apple acessando **Ajustes > Geral > Teclados** em qualquer dispositivo iOS e tocando no link em **Ativar ditado**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

404

© 1999- Citrix Systems, Inc. All rights reserved. | Terms of Use | Cookie Preferences

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de criptografia de armazenamento

Feb 21, 2018

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, Windows Phone e Android Sony. Cada plataforma exige um conjunto diferente de valores, que são descritos em detalhes neste artigo.

Configurações do Samsung SAFE

Configurações do Windows Phone

Configurações do Android Sony

Nota: para dispositivos Samsung SAFE, antes de configurar essa política, verifique se os seguintes requisitos foram atendidos:

- Você deve definir a opção de Bloqueio de Tela nos dispositivos dos usuários.
- Os dispositivos dos usuários devem estar conectados e 80% carregados.
- O dispositivo deve exigir uma senha que contenha números e letras ou símbolos.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Clique em **Mais** e, em **Segurança**, clique em **Criptografia de armazenamento**. A página de informações **Política de criptografia de armazenamento** é exibida.

4. No painel **Informações sobre a política**, digite as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma de política** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

Definir as configurações do Samsung SAFE

Defina estas configurações:

- **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 **I**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Criptografar armazenamento externo**: selecione se o armazenamento externo deve ser criptografado nos dispositivos dos usuários. O padrão é **I**.

Definir as configurações do Windows Phone

Defina estas configurações:

- **Exigir criptografia do dispositivo**: selecione se os dispositivos dos usuários devem ser criptografados. O padrão é **O**.
- **Desativar cartão de armazenamento**: selecione se os usuários devem ser impedidos de usar um cartão de memória nos respectivos dispositivos. O padrão é **O**.

Definir as configurações do Android Sony

Configure esta definição:

- **Criptografar armazenamento externo**: selecione se o armazenamento externo deve ser criptografado nos dispositivos dos usuários. O dispositivo deve exigir uma senha que contenha números e letras ou símbolos. O padrão é **I**.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de loja

Feb 21, 2018

Você pode criar uma política no XenMobile para especificar se os dispositivos iOS, Android ou Tablet Windows exibem um clipe Web da XenMobile Store na tela inicial dos dispositivos.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Expanda **Mais** e, em **Aplicativos**, clique em **Loja**. A página **Política da loja** é exibida.

4. No painel **Informações sobre a política**, insira as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: se desejar, digite uma descrição para a política.

5. Clique em **Avançar**. A página **Plataformas** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

7. Para cada plataforma que você configurar, selecione se o clipe Web da XenMobile Store aparece nos dispositivos dos usuários. O padrão é **I**.

Depois que você configurar cada plataforma, consulte a Etapa 8 para saber como definir as regras de implantação da plataforma.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de Calendários inscritos

Feb 21, 2018

Você pode adicionar uma política de dispositivo ao XenMobile para adicionar um calendário inscrito à lista de calendários nos dispositivos iOS de usuários. A lista de calendários públicos nos quais você pode se inscrever está disponível em www.apple.com/downloads/macosx/calendars.

Nota: você deve estar inscrito em um calendário antes de poder adicioná-lo à lista de calendários inscritos nos dispositivos dos usuários.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Clique em **Mais** e, em **Usuário final**, clique em **Calendários inscritos**. A página **Política de calendários inscritos** é exibida.

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 **Informações da plataforma iOS** é exibida.

6. Defina estas configurações:

- **Descrição**: insira uma descrição do calendário. Este campo é obrigatório.
- **URL**: insira o URL do calendário. Você pode inserir um URL webcal:// ou um link http:// em um arquivo do iCalendar (.ics). Este campo é obrigatório.
- **Nome de usuário**: insira o nome de login do usuário. 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 O.
- **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 de perfil**, digite a senha necessária.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo dos termos e condições

Feb 21, 2018

Crie as políticas de dispositivo dos termos e condições no XenMobile quando desejar que os usuários aceitam 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.

Configurações do iOS e do Android

Configurações do Windows Phone e do Tablet Windows

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Clique em **Termos e condições**. A página **Política de termos e condições** é exibida.

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 de informações **Plataformas de termos e condições** é exibida.

Configurações do iOS e do Android

Defina estas configurações:

- **Arquivo a ser importado**: selecione o arquivo de termos e condições a ser importado clicando em **Procurar** e navegando para 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 **O**.

Configurações do Windows Phone e do Tablet Windows

Defina estas configurações:

- **Arquivo a ser importado**: selecione o arquivo de termos e condições a ser importado clicando em **Procurar** e navegando para a localização do arquivo.
- **Imagem**: selecione o arquivo de imagem a ser importado clicando em **Procurar** e navegue para 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 **O**.

6. Clique em **Avançar**. A página de atribuição **Política de termos e condições** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

7. Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega ou selecione na lista um grupo ou os grupos aos quais você deseja atribuir a política. Os grupos que você selecionar aparecerão na lista **Grupos de entrega que receberão a atribuição de aplicativos** à direita.

8. Clique em **Salvar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo do VPN

Feb 21, 2018

Você pode adicionar uma política de dispositivo no XenMobile para definir as configurações de rede virtual privada (VPN) que permitem que os dispositivos dos usuários se conectem com segurança a recursos corporativos. Você pode configurar a política de VPN para as seguintes plataformas. Cada plataforma exige um conjunto diferente de valores, que são descritos em detalhes neste artigo.

Configurações do iOS

Configurações do macOS

Configurações do Android

Configurações do Samsung SAFE

Configurações do Samsung KNOX

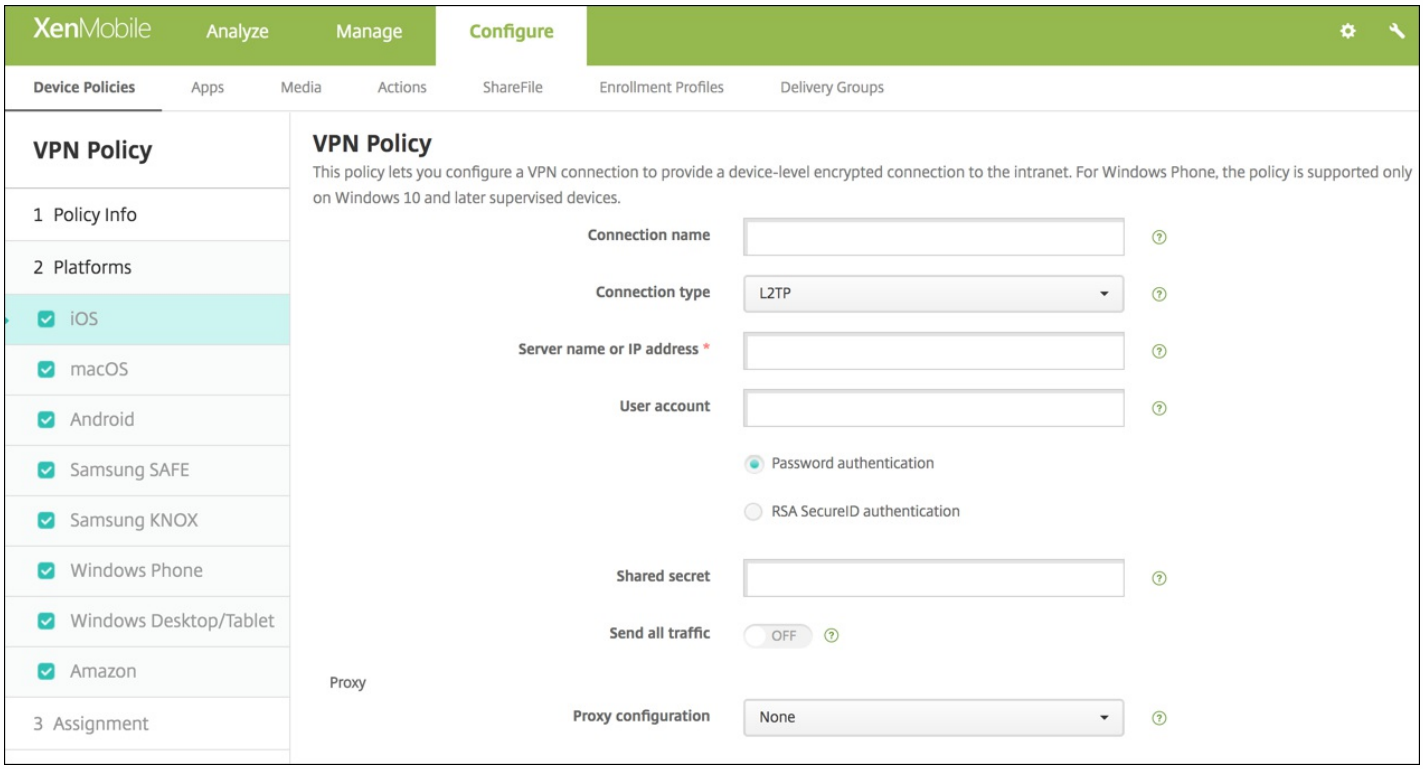
Configurações do Windows Phone

Configurações do Tablet Windows

Configurações do Amazon

Para adicionar ou configurar essa política, acesse **Configurar > Políticas de dispositivo**.

Definir as configurações do iOS



Defina estas configurações:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Nome da conexão**: digite um nome para a conexão.
- **Tipo de conexão**: na lista, clique no 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 do XenMobile em 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**: cliente VPN Juniper Networks SSL.
  - **F5**: cliente VPN SSL F5 Networks.
  - **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.
  - **Citrix VPN**: cliente Citrix VPN para iOS.
  - **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**.

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Configurar o protocolo L2TP

- **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 de senha** ou **Autenticação RSA SecureID**.
- **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 **O**.

Configurar o protocolo PPTP

- **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 de senha** ou **Autenticação RSA SecureID**.
- **Nível de criptografia**: na lista, clique em 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)**: sempre use criptografia de 128 bits.
- **Enviar todo o tráfego**: selecione se todo o tráfego deve ser enviado sobre a VPN. O padrão é **O**.

Configurar o protocolo IPSec

- **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, clique em **Segredo compartilhado** ou **Certificado** para o tipo de autenticação

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 **O**.
  - **Solicitar senha**: selecione se as senhas dos usuários devem ser solicitadas quando eles se conectarem à rede. O padrão é **O**.
- Se você ativar a opção **Certificado**, defina as seguintes configurações:
  - **Credencial de identidade**: na lista, clique na 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 **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 Configurar as opções de Ativar VPN sob demanda.
- **Ativar VPN por aplicativo**: selecione se a VPN por aplicativo deve ser ativada. O padrão é **O**. Disponível apenas no iOS 9.0 e versões posteriores.
- **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 **O**.
- **Domínios Safari**: clique em **Adicionar** para adicionar um nome de domínio do Safari.

Configurar o protocolo Cisco Legacy AnyConnect

Para fazer a transição do cliente Cisco Legacy AnyConnect 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, clique em **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**, defina as seguintes configurações:
    - **Credencial de identidade**: na lista, clique na 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 Configurar as opções de Ativar VPN sob demanda.
- **VPN por aplicativo**: selecione se a VPN por aplicativo deve ser ativada. O padrão é **O**. Disponível somente no iOS 7.0 e versões posteriores. 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 **O**.
  - **Domínios do Safari**: para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você desejar 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.

      Nota: para excluir um domínio 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

mantê-la.

Para editar um domínio existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

Configurar o protocolo Juniper SSL

- **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, clique em **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**, defina as seguintes configurações:
    - **Credencial de identidade**: na lista, clique na 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 **O**. Disponível somente no iOS 7.0 e versões posteriores. 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 **O**.
  - **Domínios do Safari**: para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você desejar 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.

      Nota: para excluir um domínio 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 domínio existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

Configurar o protocolo F5 SSL

- **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, clique em **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**, defina as seguintes configurações:
    - **Credencial de identidade**: na lista, clique na 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 **O**. Disponível somente no iOS 7.0 e versões posteriores. 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 desejar 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.

      Nota: para excluir um domínio 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 domínio existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

Configurar o protocolo SonicWALL

- **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, clique em **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**, defina as seguintes configurações:
    - **Credencial de identidade**: na lista, clique na 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 **O**. Disponível somente no iOS 7.0 e versões posteriores. 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.
  - **Domínios do Safari**: para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você desejar 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.

      Nota: para excluir um domínio 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 domínio existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configurar o protocolo Ariba VIA

- **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, clique em **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**, defina as seguintes configurações:
    - **Credencial de identidade**: na lista, clique na 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 **O**. Disponível somente no iOS 7.0 e versões posteriores. 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 desejar 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.

      Nota: para excluir um domínio 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 domínio existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

Configurar protocolos IKEv2

Essa seção inclui as configurações usadas para os protocolos IKEv2, AlwaysOn IKEv2 e AlwaysOn IKEv2 Dual Configuration.

- **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 **O**.
- **Nome do 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 de máquina**: escolha **Segredo compartilhado** ou **Certificado** 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.**
- **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**. (iOS 8.0 e versões posteriores)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Intervalo de DPD**: escolha quantas vezes um dispositivo par é contactado, para garantir que ele permaneça acessível. O padrão é **Nenhum**. As opções são: (iOS 8.0 e versões posteriores)
  - **Nenhum**: desative a detecção de par inativo.
  - **Baixo**: entre em contato com o par a cada 30 minutos.
  - **Médio**: entre em contato com o par a cada 10 minutos.
  - **Alto**: entre em contato com o par a cada minuto.
- **Desativar mobilidade e multihoming**: escolha se deseja desativar esse recurso. (iOS 9.0+)
- **Usar atributos de sub-rede interna IPv4/IPv6** : escolha se deseja ativar esse recurso. (iOS 9.0+)
- **Desativar redirecionamentos**: escolha se deseja desativar redirecionamentos. (iOS 9.0+)
- **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 WiFi e 110 segundos via rede celular. Você pode alterar o intervalo usando o parâmetro de intervalo de NAT keepalive. (iOS 9.0+)
- **Intervalo de keepalive NAT (segundos)**: O padrão é 20 segundos. (iOS 9.0+)
- **Ativar PFS (Perfect Forward Secrecy)**: escolha se deseja ativar esse recurso. (iOS 9.0+)
- **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. (iOS 10.0+)
- **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 os domínios na lista de domínios correspondentes complementares devem ser acrescentados à lista de domínios de pesquisa do resolvedor. **0** significa acrescentar; **1** significa não acrescentar. O padrão é **0**.
- **Domínios correspondentes suplementares**: opcional. Uma lista de cadeias de domínios usada para determinar as consultas DNS que devem usar as configurações de resolvedor 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 resolvedor DNS do túnel. Os hosts que não estejam em um dos domínios nessa são resolvidos por meio do resolvedor padrão do sistema.

Se esse parâmetro contiver uma cadeia vazia, esta será usada como o domínio padrão. É assim que uma configuração de túnel dividido pode direcionar todas as consultas DNS primeiramente para os servidores DNS da VPN antes dos servidores DNS primários. Se o túnel VPN se tornar a rota padrão da rede, os servidores DNS listados se tornarão o resolvedor 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, clique no algoritmo de criptografia IKE a ser usado. O padrão é **3DES**.
  - **Algoritmo de integridade**: na lista, clique no algoritmo de integridade a ser usado. O padrão é **SHA1-96**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Grupo Diffie Hellman**: na lista, clique no número do grupo Diffie Hellman. O padrão é **2**.
- **Tempo de vida em minutos**: digite um inteiro entre 10 e 1.440 que representa o tempo de vida SA (intervalo de rechaveamento). 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, clique em como lidar com a exceção de correio de voz. O padrão é **Permitir tráfego através do túnel**.
  - **AirPrint**: na lista, clique em 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 os usuários devem ter permissão para se conectar a hotspots públicos fora do túnel VPN. O padrão é **O**.
  - **Permitir o tráfego de todos os aplicativos de rede cativos fora do túnel VPN:** selecione se todos os aplicativos de rede hotspot devem ter permissão fora do túnel VPN. O padrão é **O**.
  - **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.

    Nota: para excluir um identificador de pacote de aplicativos existente, passe o mouse sobre a linha que contém a listagem e depois 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 identificador de pacote de aplicativos existente, passe o mouse sobre a linha que contém a listagem e depois clique no ícone de caneta à direita. Atualize a listagem e clique em **Salvar** para salvar a alteração ou em **Cancelar** para deixar a listagem inalterada.

- **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 **O**. Disponível apenas no iOS 9.0 e versões posteriores.
  - **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 **O**.
  - **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 VPN

O cliente Citrix VPN está disponível na Apple Store 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, clique em **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**, defina as seguintes configurações:
    - **Credencial de identidade**: na lista, clique na 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 **O**. Disponível somente no iOS 7.0 e versões posteriores. 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.
  - **Domínios do Safari**: para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você desejar 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.

      Nota: para excluir um domínio 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 domínio existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

- **XML personalizado**: para cada parâmetro XML personalizado que você desejar 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 NetScaler que são direcionadas a clientes de plug-in VPN. O **Valor** para essa chave é automaticamente acrescentado ao plug-in de VPN para as solicitações iniciadas pelo plug-in.

    Nota: para excluir um parâmetro 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 parâmetro existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

Configurar o protocolo SSL personalizado

Para fazer a transição do cliente Cisco Legacy AnyConnect para o cliente Cisco AnyConnect:

1. Configure a política de dispositivo VPN com o protocolo SSL personalizado. Implemente a política em dispositivos iOS.
2. Carregue o cliente Cisco AnyConnect para https://itunes.apple.com/us/app/cisco-anyconnect/id1135064690?mt=8, adicione o aplicativo ao XenMobile Server e implemente o aplicativo em dispositivos iOS.
3. Remova a política de dispositivo VPN antiga de dispositivos iOS.

- **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, clique em **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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Se você ativar a opção **Certificado**, defina as seguintes configurações:
  - **Credencial de identidade**: na lista, clique na 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 **O**. Disponível somente no iOS 7.0 e versões posteriores. 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 desejar 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.

      Nota: para excluir um domínio 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 domínio existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.
- **XML personalizado**: para cada parâmetro XML personalizado que você desejar 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 em **Cancelar** para não salvar.

    Nota: para excluir um parâmetro 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 parâmetro existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

Configurar as opções de Ativar VPN sob demanda

- **Proxy**
  - **Configuração de proxy**: na lista, clique em como a conexão VPN é direcionada por meio de um servidor proxy. O padrão é **Nenhum**.
    - Se você ativar **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 do servidor proxy.
      - **Senha**: digite uma senha opcional do servidor proxy.
    - Se você configurar a opção **Automática**, defina estas configurações:
      - **URL do servidor proxy**: digite o URL do servidor proxy. Este campo é obrigatório.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

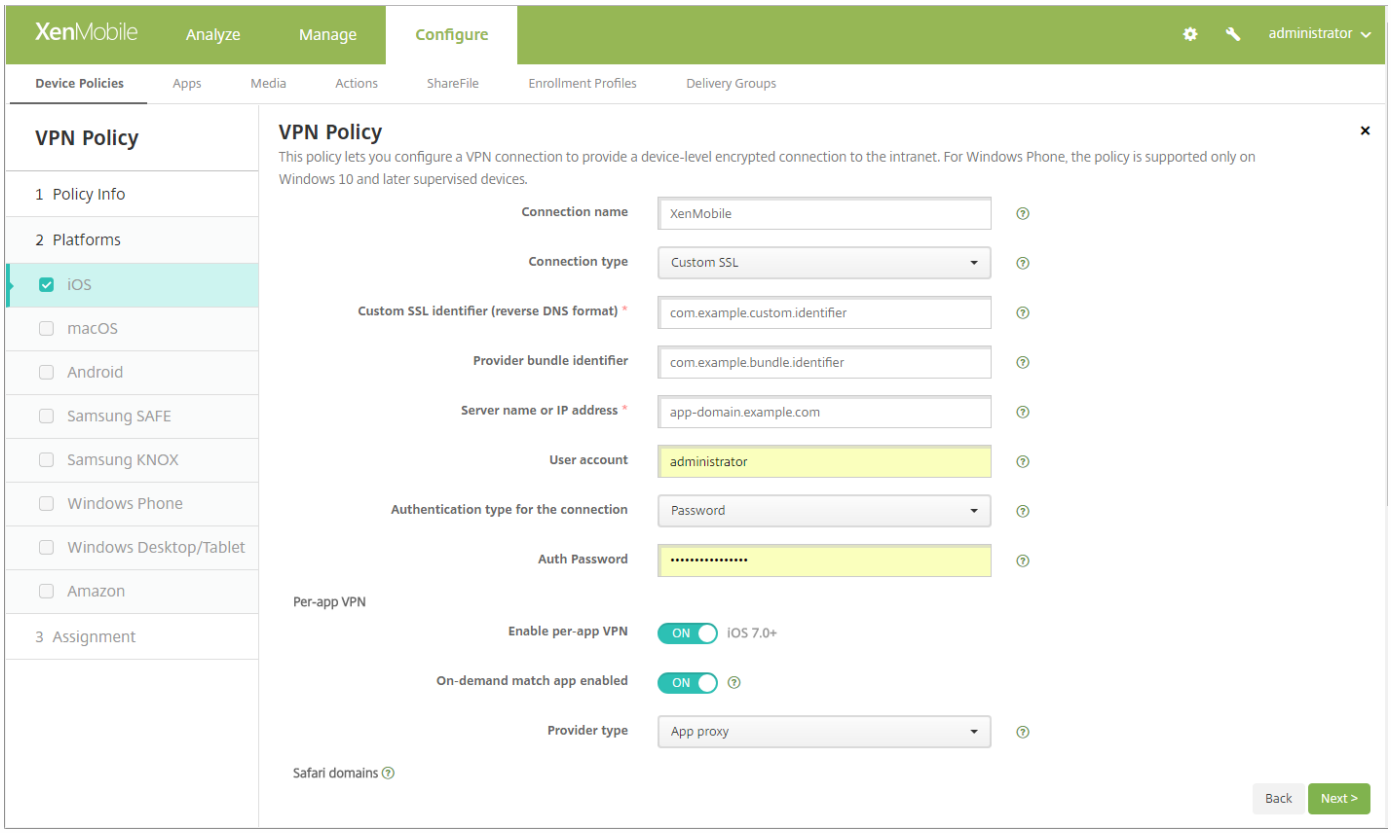
- **Configurações de política**
  - Em **Configurações de política**, ao lado de **Remover política**, clique em **Selecionar data** ou em **Duração até remoção (em horas)**.
  - Se você clicar em **Selecionar data**, clique no calendário para selecionar a data específica para remoção.
  - Na lista **Permitir 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 de perfil**, digite a senha necessária.

Configurar uma VPN por aplicativo

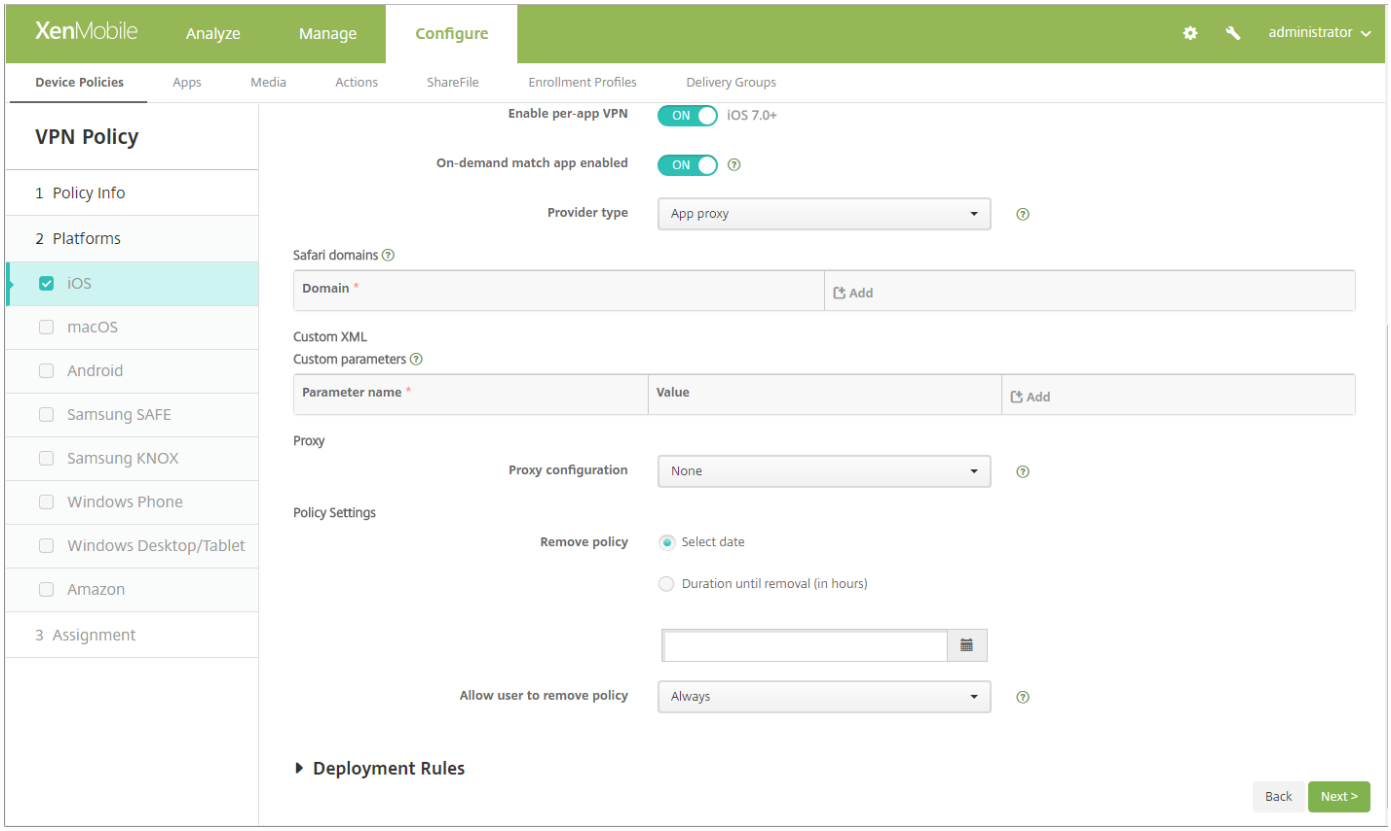
Opções de VPN por aplicativo para o iOS estão disponíveis para estes tipos de conexão: Cisco AnyConnect, Juniper SSL, F5 SSL, SonicWALL Mobile Connect, Ariba VIA, Citrix VPN e SSL personalizado.

Para configurar uma VPN por aplicativo:

1. Em **Configurar > Políticas de dispositivo**, crie uma política de VPN. Por exemplo:



© 1999-2017 Citrix Systems, Inc. All rights reserved.

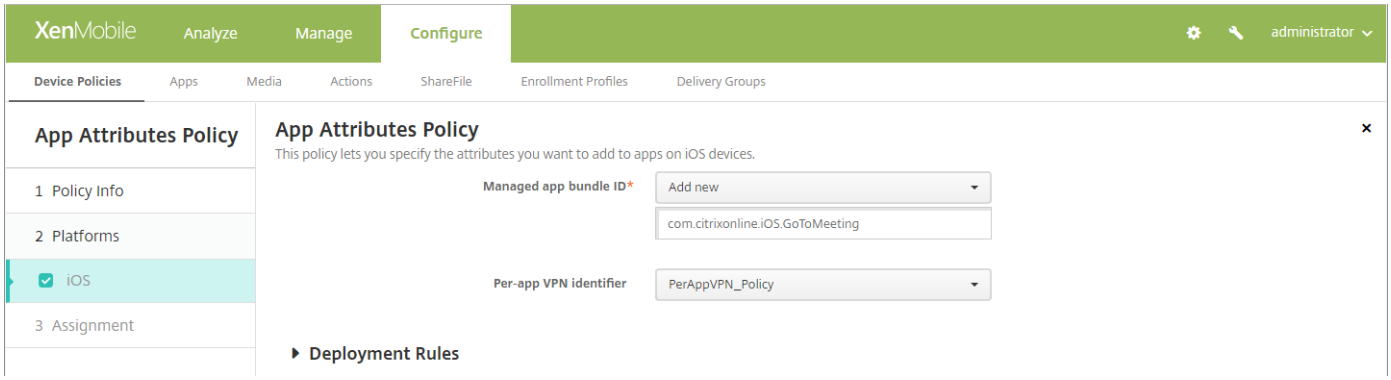


Uma política de VPN por aplicativo para o Secure Hub tem os seguintes requisitos de configuração:

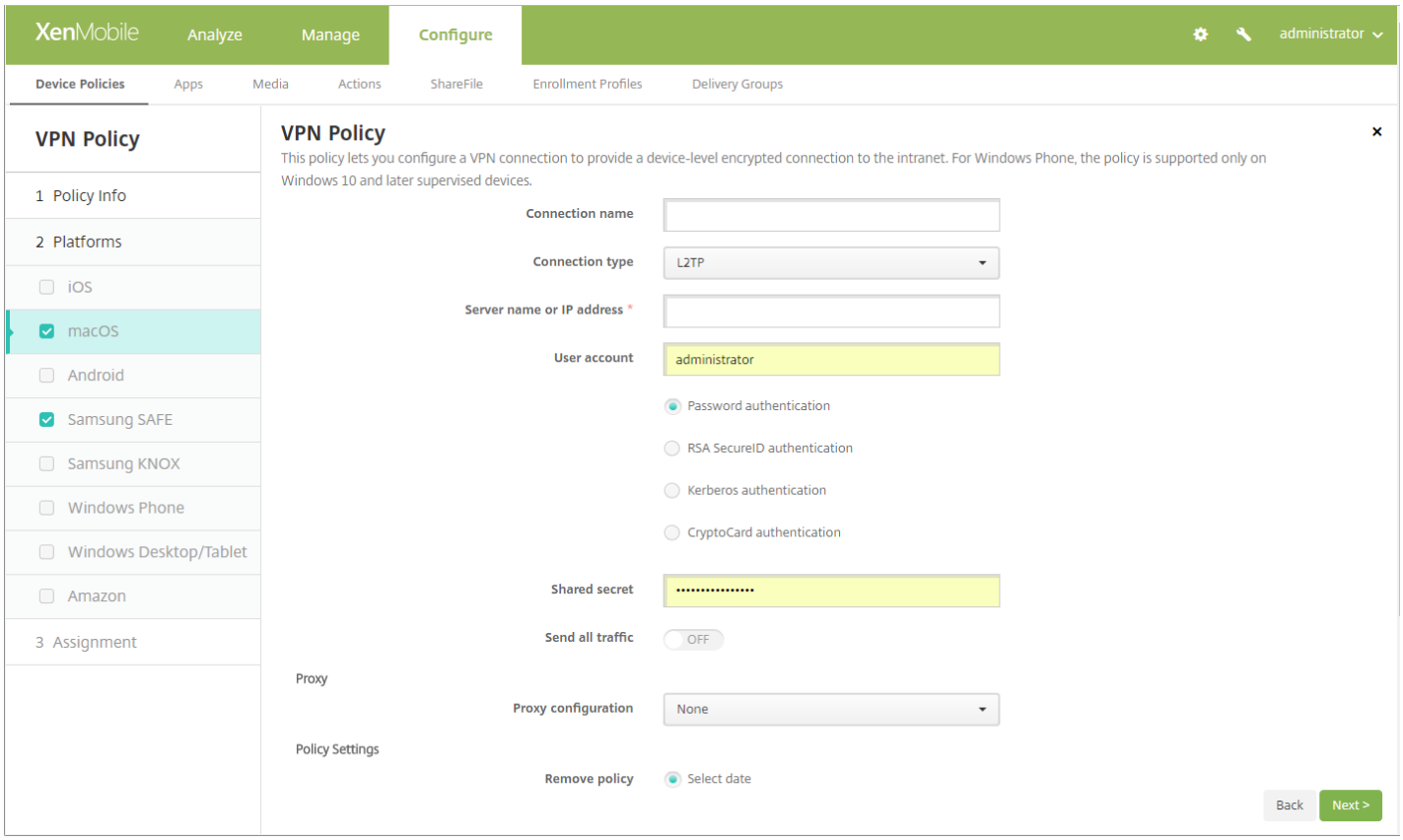
- **Nome da conexão**: defina como **XenMobile**. O XenMobile usa o Nome da conexão como a descrição localizada do provedor de VPN. O Secure Hub usa a descrição localizada da VPN para diferenciar o provedor no âmbito do dispositivo do provedor por aplicativo.
- **Tipo de conexão**: defina como **SSL personalizado**.
- **Identificador SSL personalizado**: defina o identificador de pacote do Secure Hub.
- **Identificador de pacote de provedor**: defina como o identificador de pacote da extensão de rede do Secure Hub. Esse identificador de pacote é o identificador de pacote do Secure Hub, especificado em **Identificador de SSL personalizado**, com **.NE** acrescentado.
- **Tipo de provedor**: defina como **Túnel de pacote**.

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).

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Defina as configurações do macOS



Defina estas configurações:

- **Nome da conexão**: digite um nome para a conexão.
- **Tipo de conexão**: na lista, clique no 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**: cliente VPN Juniper Networks SSL.
  - **F5**: cliente VPN SSL F5 Networks.
  - **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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Configurar o protocolo L2TP

- **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 uma das opções **Autenticação de senha**, **Autenticação RSA SecureID**, **Autenticação Kerberos**, **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 **O**.

Configurar o protocolo PPTP

- **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 uma das opções **Autenticação de senha**, **Autenticação RSA SecureID**, **Autenticação Kerberos**, **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): sempre use criptografia de 128 bits.
- **Enviar todo o tráfego**: selecione se todo o tráfego deve ser enviado sobre a VPN. O padrão é **O**.

Configurar o protocolo IPSec

- **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, clique em **Segredo compartilhado** ou **Certificado** para o tipo de autenticação dessa conexão. O padrão é **Segredo compartilhado**.
  - Se você ativar a autenticação de **Segredo compartilhado**, defina estas 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 **O**.
    - **Solicitar senha**: selecione se as senhas dos usuários devem ser solicitadas quando eles se conectarem à rede. O padrão é **O**.
  - Se você ativar a autenticação de **Certificado**, defina estas configurações:
    - **Credencial de identidade**: na lista, clique na 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 **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 Configurar as opções de Ativar VPN sob demanda.

Configurar o protocolo 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.

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Grupo**: digite um nome de grupo opcional.
- **Tipo de autenticação da conexão**: na lista, clique em **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**, defina as seguintes configurações:
    - **Credencial de identidade**: na lista, clique na 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 Configurar as opções de Ativar VPN sob demanda.
  - **VPN por aplicativo**: selecione se a VPN por aplicativo deve ser ativada. O padrão é **O**. 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 **O**.
    - **Domínios do Safari**: para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você desejar 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.

        Nota: para excluir um domínio 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 domínio existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

Configurar o protocolo Juniper SSL

- **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, clique em **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**, defina as seguintes configurações:
    - **Credencial de identidade**: na lista, clique na 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 **O**. 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 **O**.
  - **Domínios do Safari**: para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você desejar incluir,

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Nota: para excluir um domínio 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 domínio existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

Configurar o protocolo F5 SSL

- **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, clique em **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**, defina as seguintes configurações:
    - **Credencial de identidade**: na lista, clique na 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 **O**. 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 **O**.
  - **Domínios do Safari**: para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você desejar 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.

Nota: para excluir um domínio 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 domínio existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

Configurar o protocolo SonicWALL

- **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, clique em **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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Se você ativar a opção **Certificado**, defina as seguintes configurações:
  - **Credencial de identidade**: na lista, clique na 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 **O**. 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 **O**.
  - **Domínios do Safari**: para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você desejar 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.

      Nota: para excluir um domínio 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 domínio existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

Configurar o protocolo Ariba VIA

- **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, clique em **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**, defina as seguintes configurações:
    - **Credencial de identidade**: na lista, clique na 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 **O**. 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 **O**.
  - **Domínios do Safari**: para cada domínio do Safari que pode acionar uma conexão VPN por aplicativo que você desejar 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.

      Nota: para excluir um domínio 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para editar um domínio existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

Configurar o protocolo Citrix VPN

O cliente Citrix VPN está disponível na Apple Store 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, clique em **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**, defina as seguintes configurações:
    - **Credencial de identidade**: na lista, clique na 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 **O**. Disponível somente no iOS 7.0 e versões posteriores. 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 desejar 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.

      Nota: para excluir um domínio 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 domínio existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

- **XML personalizado**: para cada parâmetro XML personalizado que você desejar 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 NetScaler que são direcionadas a clientes de plug-in VPN. O **Valor** para essa chave é automaticamente acrescentado ao plug-in de VPN para as solicitações iniciadas pelo plug-in.

    Nota: para excluir um parâmetro 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 parâmetro existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

Configurar o protocolo SSL personalizado

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Identificador SSL personalizado (formato DNS inverso)**: digite o identificador SSL no formato 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, clique em **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**, defina as seguintes configurações:
    - **Credencial de identidade**: na lista, clique na 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 **O**. 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 desejar 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.

        Nota: para excluir um domínio 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 domínio existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

- **XML personalizado**: para cada parâmetro XML personalizado que você desejar 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.

    Nota: para excluir um parâmetro 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 parâmetro existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

Configurar as opções de Ativar VPN sob demanda

- **Domínio sob demanda**: para cada domínio e ação associada a ser tomada quando os usuários se conectarem a eles que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
  - **Domínio**: digite o domínio a ser adicionado.
  - **Ação**: na lista, clique em uma das ações possíveis:
    - **Sempre estabelecer**: o domínio sempre aciona uma conexão VPN.
    - **Nunca estabelecer**: o domínio nunca aciona uma conexão VPN.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Estabelecer, se necessário**: o domínio acionará uma tentativa de conexão VPN se a resolução de nome de domínio falhar, por exemplo, quando o servidor DNS não consegue resolver o domínio, redireciona para um servidor diferente ou atinge o tempo de espera.
- Clique em **Salvar** para salvar o domínio ou clique em **Cancelar** para não salvar.

- **Regras on demand**
  - **Ação**: na lista, clique na ação a ser tomada. O padrão é **EvaluateConnection.** As ações possíveis são:
    - **Permitir**: permitir que a VPN sob demanda se conecte quando acionada.
    - **Conectar**: inicie incondicionalmente uma conexão VPN.
    - **Desconectar**: remover a conexão VPN e não se reconectar sob demanda, desde que a regra seja correspondida.
    - **EvaluateConnection**: avalie 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 desejar 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 desejar 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 de 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 a qualquer interface de rede de hardware. Esse é o padrão.
    - **Ethernet**: corresponde somente a hardware de interface de rede Ethernet.
    - **WiFi**: corresponde somente a hardware de interface de rede WiFi.
    - **Celular**: corresponde somente a hardware de interface de rede Celular.
  - **SSIDMatch**: para cada SSID a ser correspondido em relação à rede atual que você desejar adicionar, clique em **Adicionar** e faça o seguinte.
    - **SSID**: digite o SSID a ser adicionado. Se a rede não for uma rede WiFi 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 um URL a ser obtido. Se essa URL for obtida com êxito sem redirecionamento, essa regra será correspondida.
  - **ActionParameters : Domains**: para cada domínio que EvaluateConnection verifica que você desejar 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, clique no comportamento da VPN dos domínios **ActionParameters : Domains** especificados. O padrão é **ConnectIfNeeded**. As ações possíveis são:
    - **ConnectIfNeeded**: o domínio acionará uma tentativa de conexão VPN se a resolução de nome de domínio falhar, por exemplo, quando o servidor DNS não consegue resolver o domínio, redireciona para um servidor diferente ou atinge o tempo de espera.
    - **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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

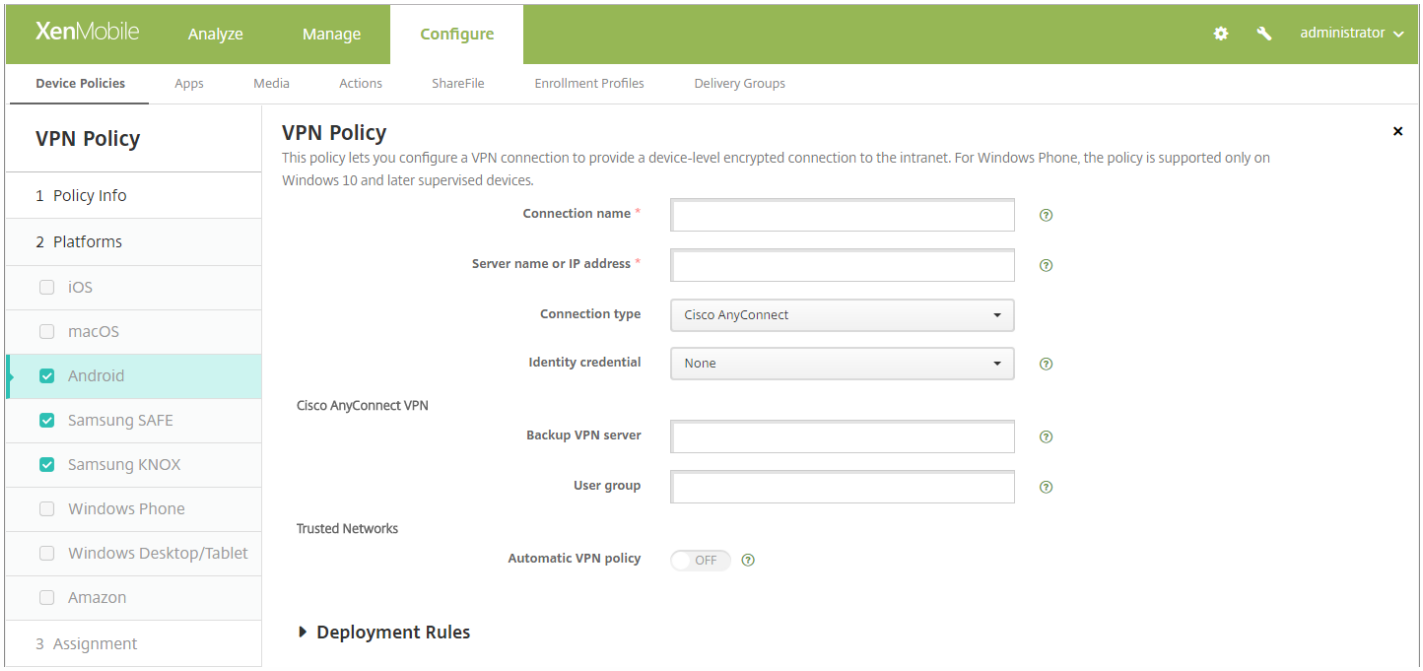
- Clique em **Salvar** para salvar o servidor DNS ou clique em **Cancelar** para não salvar.
- **ActionParameters : RequiredURLStringProbe**: opcionalmente, digite um URL HTTP ou HTTPS (preferencial) a ser investigada usando uma solicitação GET. Se não for possível resolver o nome de host da URL, se o servidor estiver inacessível ou se o servidor não tiver respondido com um código de status 200 HTTP, uma conexão VPN será estabelecida na resposta. Válido somente quando **ActionParameters** : **DomainAction** = **ConnectIfNeeded**.
- **OnDemandRules : XML content**: digite ou copie e cole as regras sob demanda da configuração XML.
  - Clique em **Verificar dicionário** para validar o código XML. Você verá XML Válido em texto verde abaixo da caixa de texto do conteúdo XML se o XML for válido; caso contrário, você verá uma mensagem de erro em texto laranja descrevendo o erro.

Proxy

- **Configuração de proxy**: na lista, clique em como a conexão VPN é direcionada por meio de um servidor proxy. O padrão é **Nenhum**.
  - Se você ativar **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 do servidor proxy.
    - **Senha**: digite uma senha opcional do servidor proxy.
  - Se você configurar a opção **Automática**, defina estas configurações:
    - **URL do servidor proxy**: digite o URL do servidor proxy. Este campo é obrigatório.
- **Configurações de política**
  - 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 de perfil**, digite a senha necessária.
  - Ao lado de **Escopo do perfil**, clique em **Usuário** ou **Sistema**. O padrão é **Usuário**. Essa opção está disponível somente no macOS 10.7 e versões posteriores.

Definir as configurações do Android

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Defina essas configurações para **Citrix VPN**:

- **Nome da conexão**: digite um nome para a conexão de VPN. Este campo é obrigatório.
- **Nome ou endereço IP do servidor**: digite o FQDN endereço IP do NetScaler 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**.
- **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 **O**.
  - **Lista branca** ou **Lista negra**: escolha uma configuração. Se for **Lista branca**, todos os aplicativos na lista branca passarão pelo túnel através dessa VPN. Se for **Lista negra**, todos os aplicativos, exceto os que estão na lista negra, passarão pelo túnel através dessa VPN.
  - **Lista de aplicativos:** especifique os aplicativos em lista branca ou lista negra. 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:
  - **disableL3Mode**: 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 nova conexão. Essa restrição é 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Defina essas configurações como **Cisco AnyConnect VPN**:

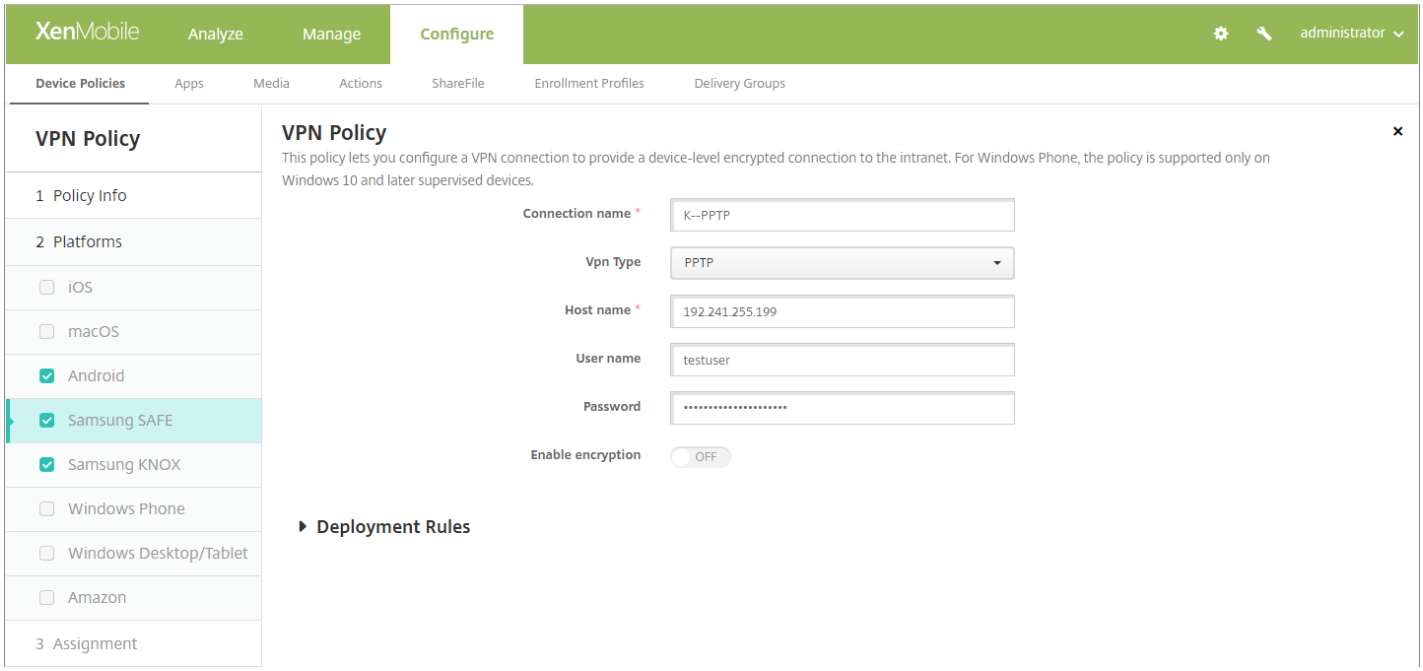
- **Nome da conexão**: digite um nome para a conexão VPN do Cisco AnyConnect. Este campo é obrigatório.
- **Nome ou endereço IP do servidor**: digite o nome ou endereço IP do servidor VPN. Este campo é obrigatório.
- **Servidor VPN de backup**: digite as informações do servidor VPN de backup.
- **Grupo de usuários**: digite as informações do grupo de usuários.
- **Credencial de identidade**: na lista, selecione uma credencial de identidade.
- **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, clique na política desejada. O padrão é **Desconectar**. As opções possíveis são:
      - **Desconectar**: o cliente encerra a conexão VPN na rede confiável. Esse é o padrão.
      - **Conectar**: o cliente inicia uma conexão VPN na rede confiável.
      - **Não fazer nada**: o cliente não toma nenhuma ação.
      - **Pausar**: suspende a sessão de VPN (em vez de desconectá-la) quando um usuário insere uma rede configurada como confiável após o estabelecimento de uma sessão VPN fora da rede confiável. Quando o usuário deixa a rede confiável novamente, a sessão é retomada. Isso elimina a necessidade de estabelecer uma nova sessão VPN após a saída de uma rede confiável.
    - **Política de rede não confiável**: na lista, clique na 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 pode ter 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 pode ter 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.

      Nota: para excluir um servidor 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 servidor existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

Definir as configurações do Samsung SAFE

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Defina estas configurações:

- **Nome da conexão**: digite um nome para a conexão.
- **Tipo de VPN**: na lista, clique no protocolo a ser usado para essa 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 é a configuração padrão.
  - **L2TP com certificado**: protocolo de encapsulamento de camada 2 com certificado.
  - **PPTP**: encapsulamento ponto a ponto.
  - **Empresarial**: 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.

As seções a seguir listam as opções de configuração de cada um dos tipos de VPN anteriores.

Configurar o protocolo L2TP com chave pré-compartilhada

- **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 protocolo de certificado

- **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, clique na credencial de identidade a ser usada. O padrão é **Nenhum**.

Configurar o protocolo PPTP

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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 da Empresa

- **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, em **Servidor VPN de backup**, digite o FQDN ou o endereço IP do servidor VPN de backup.
- **Ativar a autenticação de usuário**: selecione se a autenticação do usuário é exigida. 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, clique no método de autenticação que deve ser usado. As opções possíveis são:
  - **Certificado**: use a autenticação de certificado. Esse é o padrão. Se essa opção estiver selecionada, na lista Credencial de identidade, clique na credencial a ser usada. O padrão é **Nenhum**.
  - **Chave pré-compartilhada**: use uma chave pré-compartilhada. Se essa opção estiver selecionada, 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 AC**: na lista, clique no 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 **O**.
- **Ativar a autenticação de cartão inteligente**: selecione se os usuários têm permissão para autenticar usando cartões inteligentes. O padrão é **O**.
- **Ativar opção móvel**: selecione se a opção móvel deve ser ativada. O padrão é **O**.
- **Valor do grupo Diffie-Hellman (força da chave)**: na lista, clique na força da chave a ser usada. O padrão é 0.
- **Tipo de túnel dividido**: na lista, clique no 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, clique no 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.
  - **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

- **Nome do host**: digite o nome do host VPN. Essa opção é necessária.
- **Ativar a autenticação de usuário**: selecione se a autenticação do usuário é exigida. Se ativada, em **Senha**, digite a senha de usuário.
- **Nome de usuário**: digite um nome de usuário.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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, clique em **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 tipo de conexão IPSEC

- **Identidade**: digite um identificador opcional para essa configuração.
- **Tipo de ID de grupo IPsec**: na lista, clique no 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, clique na versão do Internet Key Exchange a ser usada. O padrão é **IKEv1**.
- **Método de autenticação**: na lista, clique no método de autenticação que deve ser usado. O padrão é **Certificado**. As opções possíveis são:
  - **Certificado**: use a autenticação de certificado. Se essa opção estiver selecionada, na lista **Credencial de identidade**, clique na credencial a ser usada. O padrão é **Nenhum**.
  - **Chave pré-compartilhada**: use uma chave pré-compartilhada. Se essa opção estiver selecionada, 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 Common Access Card (CAC) para autenticação.
- **Credencial de identidade**: na lista, clique na credencial de identidade a ser usada. O padrão é **Nenhum**.
- **Certificado AC**: na lista, clique no 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 **O**.
- **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).
- **Valor do grupo Diffie-Hellman (força da chave)**: na lista, clique na 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, clique no 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:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Rota de encaminhamento**: digite o endereço IP da rota de encaminhamento.
- Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.

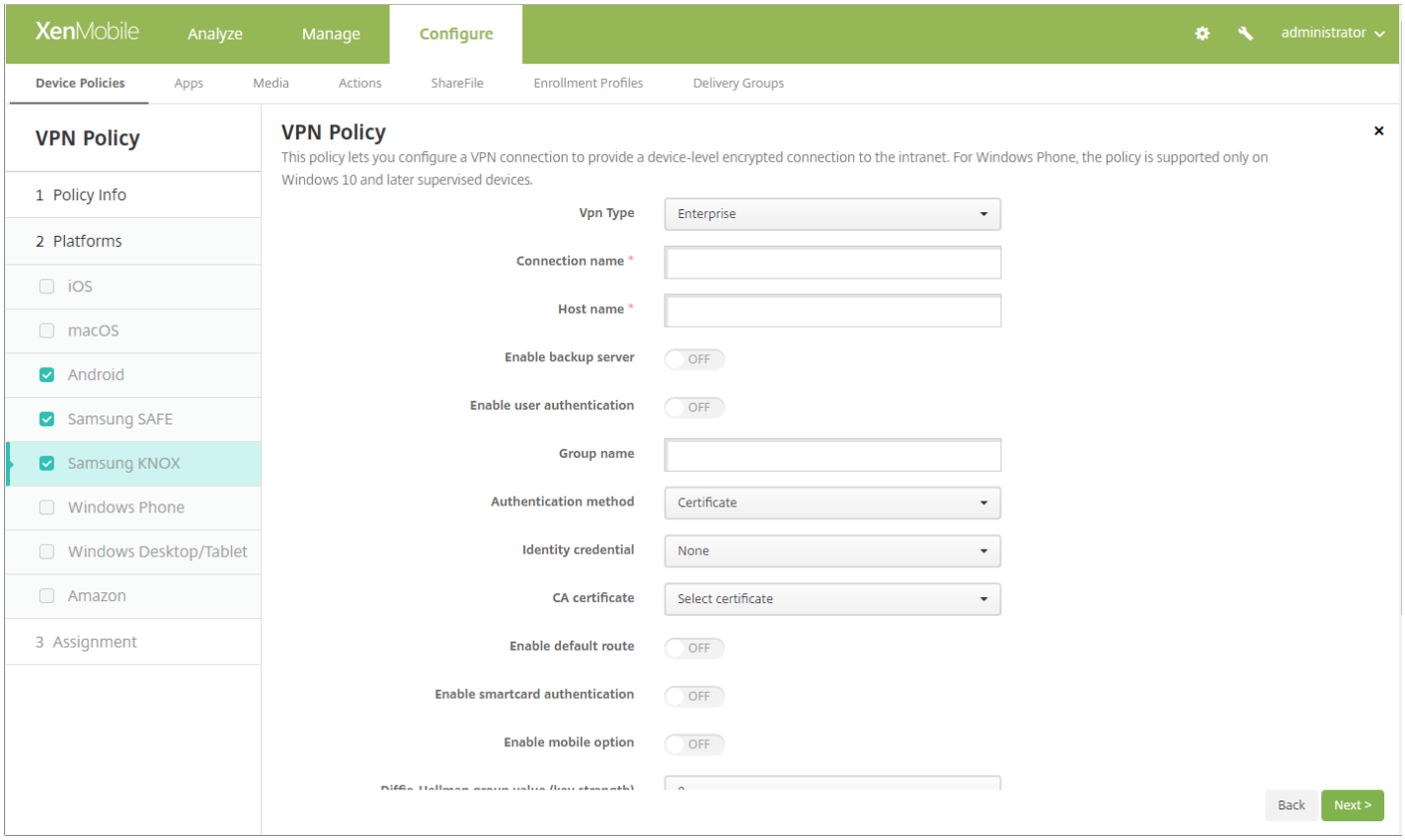
- **VPN por aplicativo**: para cada VPN por aplicativo que você desejar adicionar, clique em **Adicionar** e faça o seguinte:
  - **VPN por Aplicativo**: a configuração VPN que o aplicativo usa para se comunicar.
  - Clique em **Salvar** para salvar a VPN por aplicativo ou clique em **Cancelar** para não salvar.

Definir as configurações de tipo de conexão SSL

- **Método de autenticação**: na lista, clique no 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 essa opção estiver selecionada, na lista **Credencial de identidade**, clique na credencial a ser usada. O padrão é **Nenhum**.
  - **Autenticação baseada em CAC**: use um Common Access Card (CAC) para autenticação.
- **Certificado AC**: na lista, clique no 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, clique no 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.

Definir as configurações do Samsung KNOX

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Nota: quando você configura qualquer política para o Samsung KNOX, ela se aplica somente no contêiner do Samsung KNOX.

Defina estas configurações:

- **Tipo de VPN**: na lista, clique em **Empresarial** (aplicável a versões do KNOX anteriores à 2.0) ou em **Genérico** (aplicável à versão 2.0 do KNOX ou superior). O padrão é **Empresarial**.

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Configurar o protocolo da Empresa

- **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, em **Servidor VPN de backup**, digite o FQDN ou o endereço IP do servidor VPN de backup.
- **Ativar a autenticação de usuário**: selecione se a autenticação do usuário é exigida. 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, clique no método de autenticação que deve ser usado. As opções possíveis são:
  - **Certificado**: use a autenticação de certificado. Esse é o padrão. Se essa opção estiver selecionada, na lista Credencial de identidade, clique na credencial a ser usada. O padrão é Nenhum.
  - **Chave pré-compartilhada**: use uma chave pré-compartilhada. Se essa opção estiver selecionada, 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **EAP MSCHAPv2**: use a autenticação de handshake de desafio da Microsoft para autenticação mútua.
- **Certificado AC**: na lista, clique no 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 **O**.
- **Ativar opção móvel**: selecione se a opção móvel deve ser ativada.
- **Valor do grupo Diffie-Hellman (força da chave)**: na lista, clique na força da chave a ser usada. O padrão é **0**.
- **Tipo de túnel dividido**: na lista, clique no 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, clique no nível de criptografia NSA Suite B a ser usado. As opções possíveis são:
  - **GCM-128**: use a criptografia AES-GCM de 128 bits, que é 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

- **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 a autenticação de usuário**: selecione se a autenticação do usuário é exigida. 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, clique em **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**
  - **Identidade**: digite um identificador opcional para essa configuração.
  - **Tipo de ID de grupo IPsec**: na lista, clique no 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, clique na versão do Internet Key Exchange a ser usada. O padrão é **IKEv1**.
  - **Método de autenticação**: na lista, clique no método de autenticação que deve ser usado. O padrão é **Certificado**. As opções possíveis são:
    - **Certificado**: use a autenticação de certificado. Se essa opção estiver selecionada, na lista **Credencial de identidade**, clique na credencial a ser usada. O padrão é **Nenhum**.
    - **Chave pré-compartilhada**: use uma chave pré-compartilhada. Se essa opção estiver selecionada, no campo **Chave pré-compartilhada**, digite a chave secreta compartilhada.
    - **RSA híbrido**: use a autenticação híbrida usando certificados RSA.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

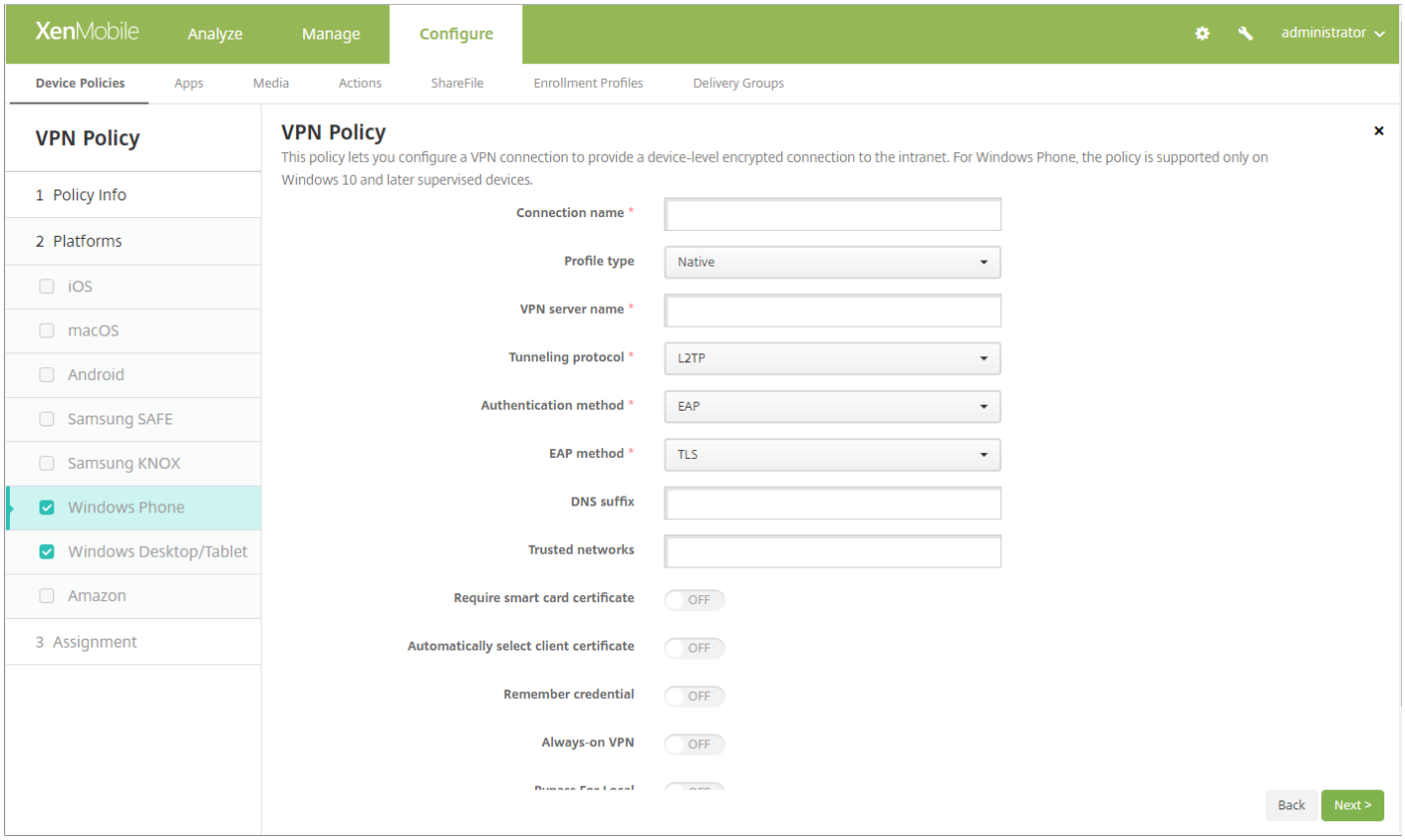
    - **EAP MD5**: autentique o par EAP no servidor EAP, mas não realize a autenticação mútua.
    - **EAP MSCHAPv2**: use a autenticação de handshake de desafio da Microsoft para autenticação mútua.
    - **Autenticação baseada em CAC**: use um Common Access Card (CAC) para autenticação.
  - **Certificado AC**: na lista, clique no 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 **O**.
  - **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, clique na 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, clique no 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, clique no 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 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 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. Esse é o padrão.
    - **Certificado**: use a autenticação de certificado. Esse é o padrão. Se essa opção estiver selecionada, na lista Credencial de identidade, clique na credencial a ser usada. O padrão é Nenhum.
    - **Autenticação baseada em CAC**: use um Common Access Card (CAC) para autenticação.
  - **Certificado AC**: na lista, clique no 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Tipo de túnel dividido**: na lista, clique no 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.
- **SuiteB Type:** na lista, clique no 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 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 as configurações do Windows Phone



Nota: essas configurações são compatíveis somente em telefones supervisionados com Windows 10 e versões posteriores.

Defina estas configurações:

- **Nome da conexão**: Insira um nome para a conexão. Este campo é obrigatório.

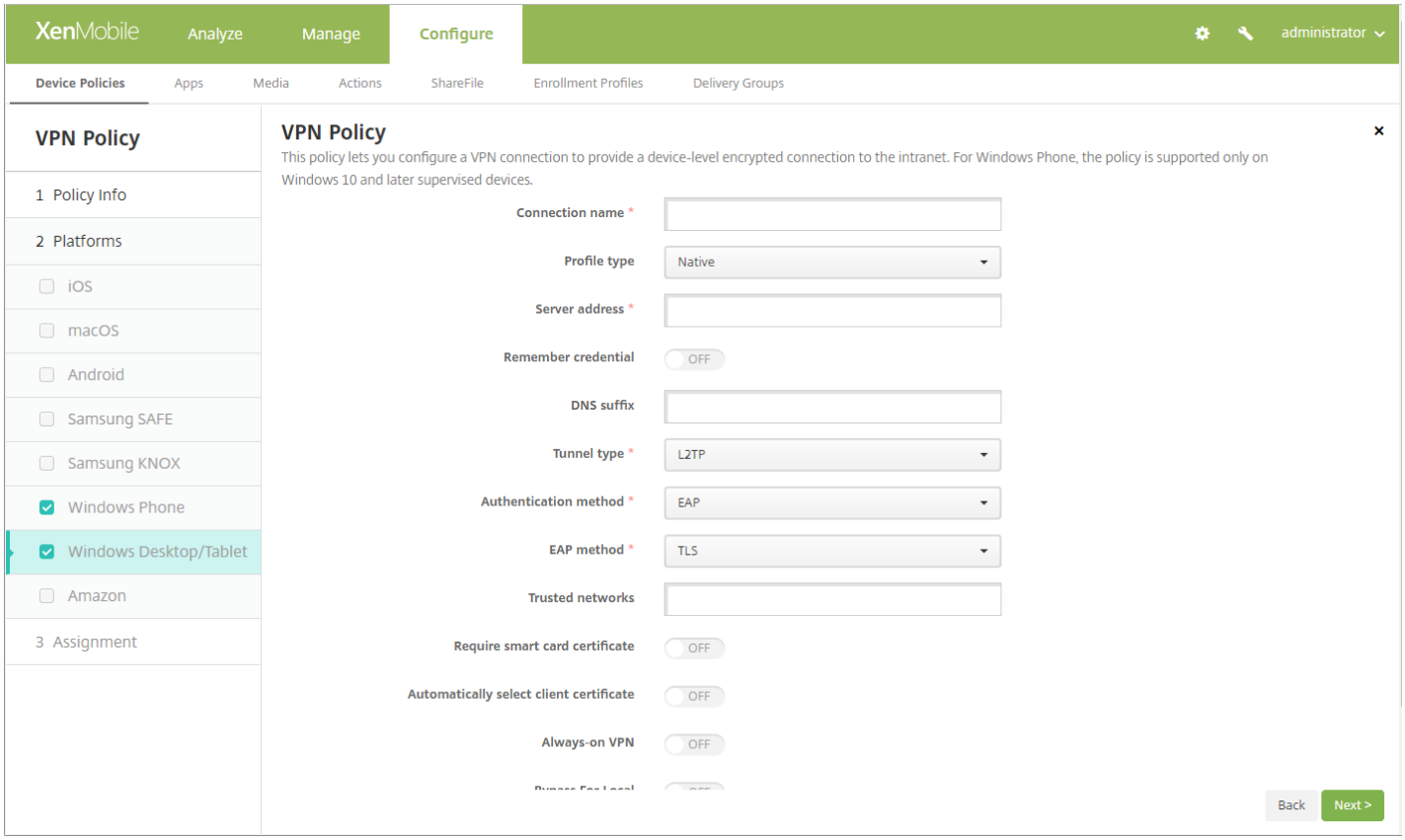
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Tipo de perfil**: na lista, clique em **Nativo** ou **Plug-in**. O padrão é **Nativo**. As seções a seguir descrevem as configurações de cada uma dessas opções.
- **Configurar 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 endereço IP do servidor VPN. Este campo é obrigatório.
  - **Protocolo de túnel**: na lista, clique no 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, clique no método de autenticação que deve 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. Essa opção não está disponível quando você seleciona IKEv2 como o tipo de túnel. Quando você seleciona MSChapV2, uma opção **Usar credenciais do Windows automaticamente** aparece; o padrão é **O**.
  - **Método EAP**: Na lista, clique no método EAP a ser usado. O padrão é **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 de plug-in -** Essas configurações se aplicam a plug-ins de VPN obtidos da Windows Store e instalados nos dispositivos dos usuários.
  - **Endereço de servidor**: digite o 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 a 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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.

Definir as configurações do Windows Desktop/Tablet



Defina estas configurações:

Definir as configurações do Windows 10

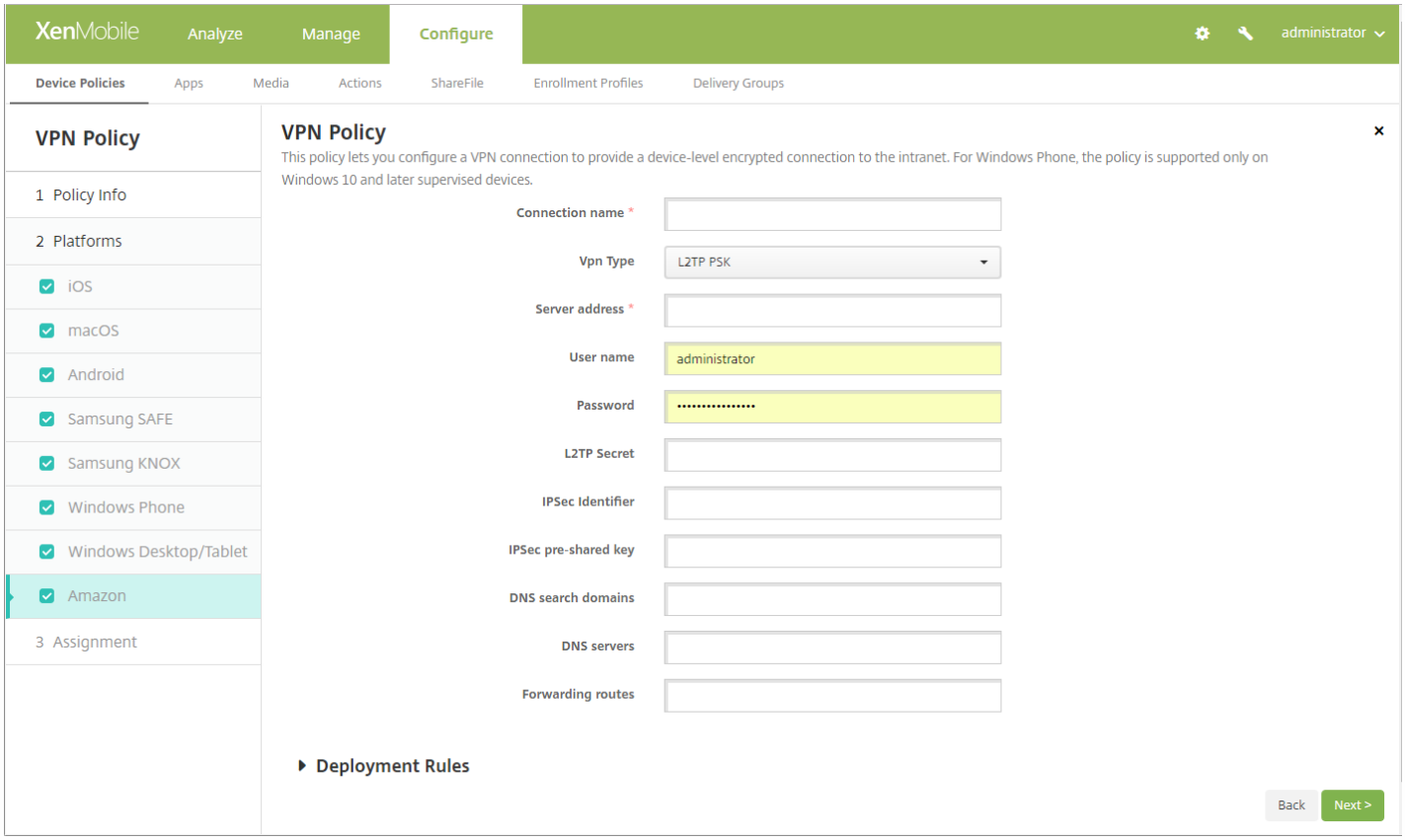
- **Nome da conexão**: Insira um nome para a conexão. Este campo é obrigatório.
- **Tipo de perfil**: Na lista, clique em **Nativo** ou **Plug-in**. O padrão é **Nativo**.
- **Configurar tipo de perfil nativo -** Essas configurações se aplicam à VPN interna nos telefones com Windows dos usuários.
  - **Endereço de servidor**: Digite o FQDN ou endereço IP do servidor de VPN. Este campo é obrigatório.
  - **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.
  - **Sufixo DNS**: Digite o sufixo DNS.
  - **Tipo de túnel**: Na lista, clique no 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, clique no método de autenticação que deve 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. Essa opção não está disponível quando você seleciona **IKEv2** como o tipo de túnel.
  - **Método EAP**: Na lista, clique no método EAP a ser usado. O padrão é **TLS.** Esse campo não está disponível quando a

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 **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 você ativa **Exigir um certificado de cartão inteligente**.
  - **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.
- **Configure tipo de perfil de plug-in -** 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 endereço IP do servidor de VPN. Este campo é obrigatório.
  - **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.
  - **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 **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.

Definir as configurações do Amazon

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Defina estas configurações:

- **Nome da conexão**: Insira um nome para a conexão.
- **Tipo de VPN**: clique no tipo de conexão. As opções possíveis são:
  - **L2TP PSK**: protocolo de encapsulamento de camada 2 com autenticação de chave pré-compartilhada. Esse é o 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

- **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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.

Definir as configurações do L2TP RSA

- **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, clique no certificado a ser usado.
- **Certificado AC**: na lista, clique no certificado AC a ser usado.
- **Credencial de identidade**: na lista, clique na 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 do IPSEC XAUTH PSK

- **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 do IPSEC AUTH RSA

- **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, clique no certificado a ser usado.
- **Certificado AC**: na lista, clique no certificado AC a ser usado.
- **Credencial de identidade**: na lista, clique na 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Clique em **Salvar** para salvar a rota ou em **Cancelar** para não salvar.

Definir as configurações do IPSEC HYBRID RSA

- **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, clique no certificado a ser usado.
- **Certificado AC**: na lista, clique no certificado 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 do PPTP

- **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 **O**.
- **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.

Nota

Para obter informações gerais sobre como configurar políticas, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de papel de parede

Feb 21, 2018

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 versões posteriores. 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.

Dispositivo		**Dimensões da imagem em pixels**
iPhone	**iPad**	
4, 4s		640 x 960
5, 5c, 5s		640 x 1136
6, 6s		750 x 1334
6 Plus		1080 x 1920
	Air, 2	1536 x 2048
	4, 3	1536 x 2048
	Mini 2, 3	1536 x 2048
	Mini	768 x 1024

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Expanda **Mais** e, em **Usuário final**, clique em **Papel de parede**. A página **Política de papel de parede** é exibida.

4. No painel **Informações sobre a política**, insira as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma de política** é exibida.

Defina estas configurações:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de filtro de conteúdo Web

Mar 09, 2018

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 brancas e listas negras. Essa política está disponível somente nos dispositivos iOS 7.0 e versões posteriores no modo Supervisionado. Para obter mais informações sobre como colocar um dispositivo iOS no modo Supervisionado, consulte Para colocar um dispositivo iOS no modo Supervisionado usando o Apple Configurator.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. A caixa de diálogo **Adicionar uma nova política** é exibida.

3. Clique em **Mais** e, em **Segurança**, clique em **Filtro de conteúdo Web**. A página **Política de filtro de conteúdo Web** é exibida.

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 de informações **Plataforma iOS** é exibida.

6. Defina estas configurações:

- **Tipo de filtro**: na lista, clique em **Integrado** ou **Plug-in**, e siga os procedimentos referentes à opção que você escolher. O padrão é **Integrado**.

Configurações de 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 **O**.
  - **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 desejar adicionar à lista branca, 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 branca ou clique em **Cancelar** para não salvar.
  - **URLs na lista negra**: os itens nessa lista são sempre bloqueados. Para cada URL que você desejar adicionar à lista negra, 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 negra ou clique em **Cancelar** para não salvar.
- **Lista branca de indicadores**
  - **Lista branca de indicadores**: especifica os sites que os usuários possam 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Título**: digite um título descritivo para o site. Por exemplo, digite “Google” para a URL http://google.com.
- Clique em **Salvar** para salvar o site na lista negra ou clique em **Cancelar** para não salvar.

> **Nota**: para excluir um site 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 site existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

Configurações de 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 desejar 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 salvar.

> **Nota:** para excluir uma chave 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 uma chave existente, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta à direita. Altere a listagem e clique em **Salvar** para salvar a listagem alterada ou em **Cancelar** para deixá-la inalterada.

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 de perfil**, digite a senha necessária.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de clipe Web

Feb 21, 2018

Você pode colocar atalhos, ou clipes Web, para sites que são exibidos ao lado dos aplicativos nos dispositivos dos usuários. Você pode especificar seus próprios ícones para representar os clipes Web para dispositivos iOS, macOS e Android; o Tablet Windows requer somente um rótulo e um URL.

Configurações do iOS

Configurações do macOS

Configurações do Android

Configurações do Windows Desktop/Tablet

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Expanda **Mais** e, em **Aplicativos**, clique em **Clipe Web** A página **Política de clipe Web** é exibida.

4. No painel **Informações sobre a política**, insira as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma de política** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

Definir as configurações do iOS

Defina estas configurações:

- **Rótulo**: digite o rótulo que deve ser exibido com o clipe Web.
- **URL**: digite o URL associado ao clipe Web. A URL deve começar com um protocolo, por exemplo, http://server.
- **Removível**: selecione se os usuários podem remover o clipe Web. O padrão é **O**.
- **Ícone a ser atualizado**: selecione o ícone a ser usado para o clipe 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 **O**.
- **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 de perfil**, digite a senha necessária.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Defina as configurações do macOS

Defina estas configurações:

- **Rótulo**: digite o rótulo que deve ser exibido com o clipe Web.
- **URL**: digite o URL associado ao clipe Web. A URL deve começar com um protocolo, por exemplo, http://server.
- **Ícone a ser atualizado**: selecione o ícone a ser usado para o clipe Web clicando em Procurar e navegando até a localização do arquivo.
- **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 de perfil**, digite a senha necessária.
  - Na lista **Escopo do perfil**, clique em **Usuário** ou **Sistema**. Essa opção está disponível no macOS 10.7 e versões posteriores.

Definir as configurações do Android

Defina estas configurações:

- **Regra**: selecione se essa política adiciona ou remove um clipe Web. O padrão é **Adicionar**.
- **Rótulo**: digite o rótulo que deve ser exibido com o clipe Web.
- **URL**: digite o URL associado ao clipe Web.
- **Definir um ícone**: selecione se um arquivo de ícone deve ser usado. O padrão é **O**.
- **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.

Definir as configurações do Windows Desktop/Tablet

Defina estas configurações:

- **Nome**: digite o rótulo que deve ser exibido com o clipe Web.
- **URL**: digite o URL associado ao clipe Web.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

8. Clique em **Avançar**. A página de atribuição **Política de clipe** Web é exibida.

9. Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega ou selecione na lista um grupo ou os grupos aos quais você deseja atribuir a política. Os grupos que você selecionar aparecerão na lista **Grupos de entrega que receberão a atribuição de aplicativos**.

10. 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 **O**, nenhuma outra opção precisará ser configurada.
- Ao lado de **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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Ao lado de **Implantar para conexões permanentes**, clique em **I** ou **O**. A opção padrão é **O**.

Nota:

- Essa opção se aplicará 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.

11. Clique em **Salvar** para salvar a política.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de WiFi

Feb 21, 2018

Crie políticas de dispositivo de WiFi novas ou existentes no XenMobile usando a página **Configurar > Políticas de dispositivo**. Políticas de WiFi permitem gerenciar como os usuários conectam seus dispositivos a redes WiFi, definindo os itens a seguir:

- Nomes e tipos de redes
- Políticas de autenticação e segurança
- Uso de servidores proxy
- Outros detalhes relacionados a WiFi

Você pode definir configurações de WiFi para os usuários nas seguintes plataformas. Cada plataforma exige um conjunto diferente de valores, que são descritos em detalhes neste artigo.

Configurações do iOS

Configurações do macOS

Configurações do Android (inclui dispositivos ativados para o Android for Work)

Configurações do Windows Phone

Configurações do Windows Desktop/Tablet

> ## Important
>
> 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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Clique em **WiFi**. A página **Política de WiFi** é exibida.

4. No painel **Informações sobre a política**, digite as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: opcionalmente, digite uma descrição para a política.

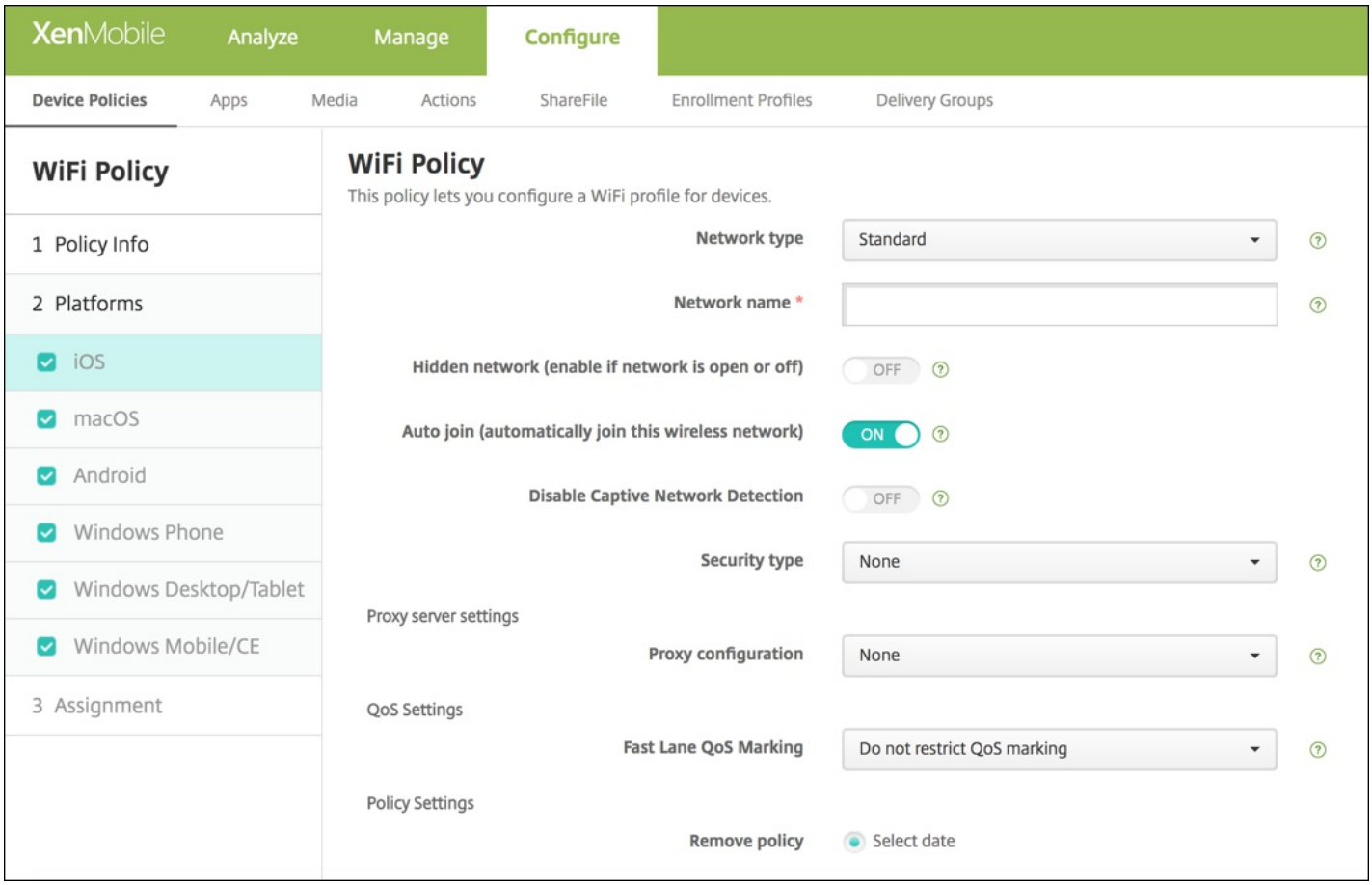
© 1999-2017 Citrix Systems, Inc. All rights reserved.

5. Clique em **Avançar**. A página **Plataformas** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para definir regras de implantação dessa plataforma.

Definir as configurações do iOS



Defina estas configurações:

- **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 a **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. O padrão é **I**.
- **Tipo de segurança**: na lista, clique no tipo de segurança que você planeja usar. Não se aplica a **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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

configure o SCEP. Em seguida, o XenMobile pode enviar o certificado a dispositivos para autenticação no servidor WiFi. 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.

WPA, WPA Pessoal, Qualquer (Pessoal)

Senha: digite uma senha opcional. Se você deixar esse campo em branco, os usuários poderão ser solicitados a inserir as senhas quando fizerem login.

WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Qualquer (Enterprise)

Nota: 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 **O** 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**: *obrigatória 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**.

      Para excluir um item, passe o mouse sobre a linha que contém a listagem e clique no ícone de lixeira no lado direito. Uma caixa de diálogo de confirmação é exibida. Clique em **Excluir** para excluir a listagem ou em **Cancelar** para mantê-la.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Para editar um item, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta no lado direito. Atualize a listagem e clique em **Salvar**.

- **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 **I**.

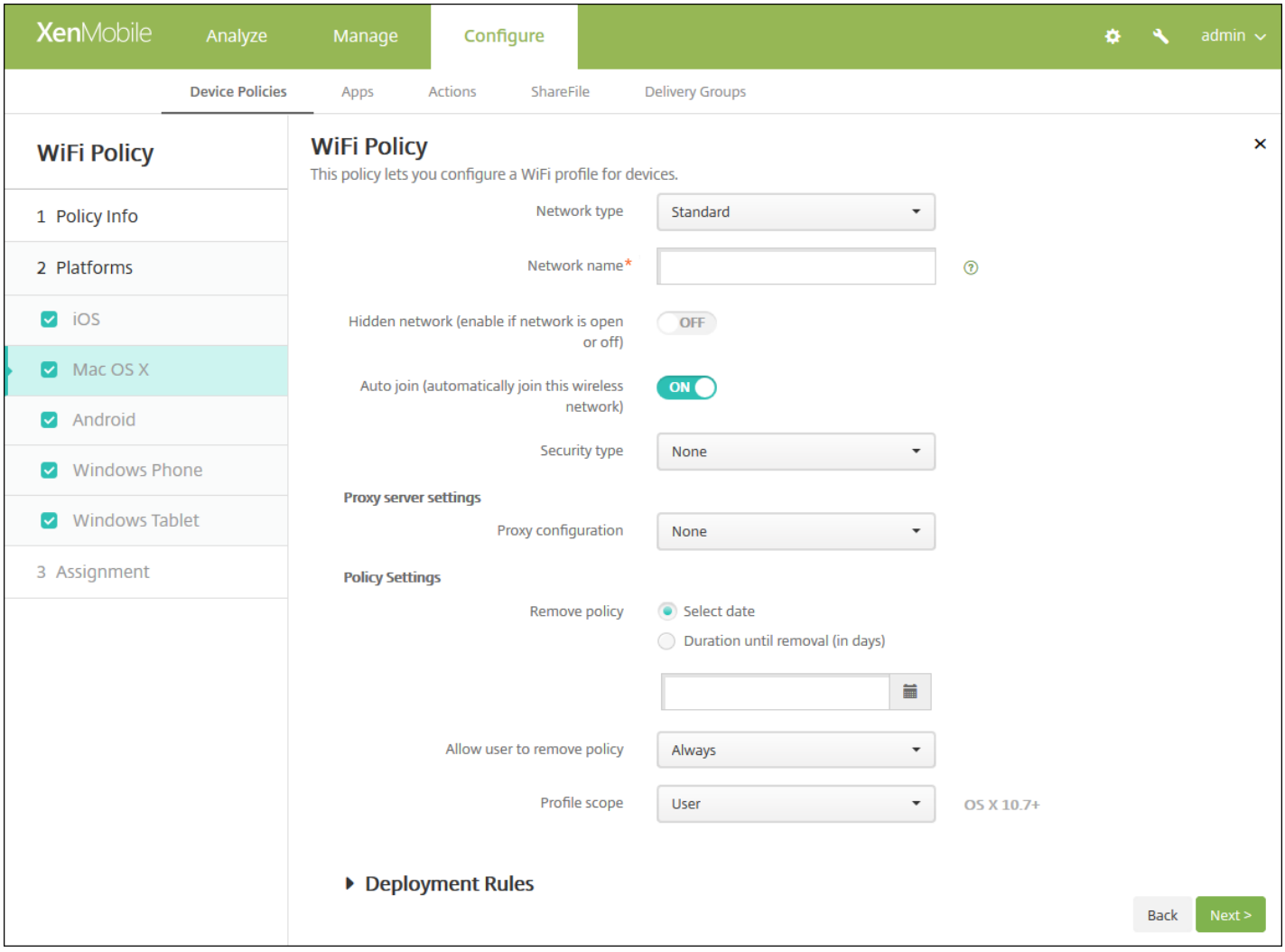
Configurações do servidor proxy

- **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 do 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 **I**. Essa opção está disponível somente no iOS 7.0 e versões posteriores.

- **Configurações de política**
  - Ao lado de **Remover política**, escolha **Selecionar data** ou **Duração até remoção (em horas)**.
  - Se você escolher **Selecionar data**, clique no calendário para escolher a data específica para remoção.
  - Na lista **Permitir que o usuário remova a política**, escolha **Sempre**, **Senha obrigatória** ou **Nunca**.
  - Se você escolher **Senha obrigatória**, ao lado de **Senha de remoção de perfil**, digite a senha necessária.

Defina as configurações macOS

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Defina estas configurações:

- **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 a **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. O padrão é **I**.
- **Tipo de segurança**: na lista, clique no tipo de segurança que você planeja usar. Não se aplica a **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.

WPA, WPA Pessoal, WPA 2 Pessoal, Qualquer (Pessoal)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Senha**: digite uma senha opcional. Se você deixar esse campo em branco, os usuários poderão ser solicitados a inserir as senhas quando fizerem login.

WEP Enterprise, WPA Enterprise, WPA2 Enterprise, Qualquer (Enterprise)

Nota: 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 **O** 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**: *obrigatória 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**.

      Para excluir um item, passe o mouse sobre a linha que contém a listagem e clique no ícone de lixeira no lado direito. Uma caixa de diálogo de confirmação é exibida. Clique em **Excluir** para excluir a listagem ou em **Cancelar** para mantê-la.

      Para editar um item, passe o mouse sobre a linha que contém a listagem e clique no ícone de caneta no lado direito. Atualize a listagem e clique em **Salvar**.
- **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 **I**.

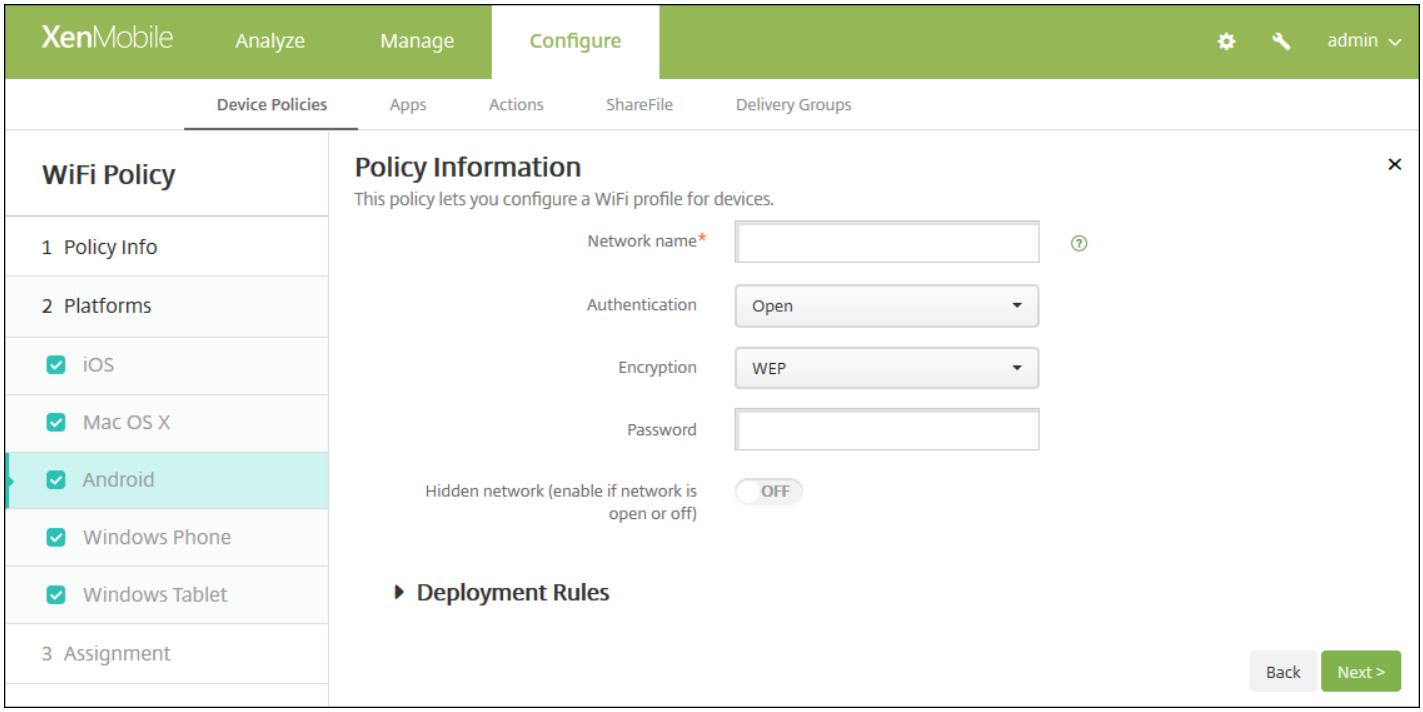
Usar como configuração de janela de login: escolha se deseja usar as mesmas credenciais que inseriu na janela de login para autenticar o usuário.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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 **I**. Essa opção está disponível somente no iOS 7.0 e versões posteriores.

- **Configurações de política**
  - Ao lado de **Remover política**, escolha **Selecionar data** ou **Duração até remoção (em horas)**.
  - Se você escolher **Selecionar data**, clique no calendário para escolher a data específica para remoção.
  - Na lista **Permitir que o usuário remova a política**, escolha **Sempre**, **Senha obrigatória** ou **Nunca**.
  - Se você escolher **Senha obrigatória**, ao lado de **Senha de remoção de perfil**, digite a senha necessária.
  - Ao lado de **Escopo do perfil**, clique em **Usuário** ou **Sistema**. O padrão é **Usuário**. Essa opção está disponível somente para macOS X 10.7 e versões posteriores.

Definir as configurações do Android



Defina estas configurações:

- **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 de WiFi.
  - Aberto

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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.

Aberto, Compartilhado

- **Criptografia**: na lista, escolha **Desativado** ou **WEP**. O padrão é **WEP**.
- **Senha**: digite uma senha opcional.

WPA, WPA-PSK, WPA2, WPA2-PSK

- **Criptografia**: na lista, escolha **TKIP** ou **AES**. O padrão é **TKIP**.
- **Senha**: digite uma senha opcional.

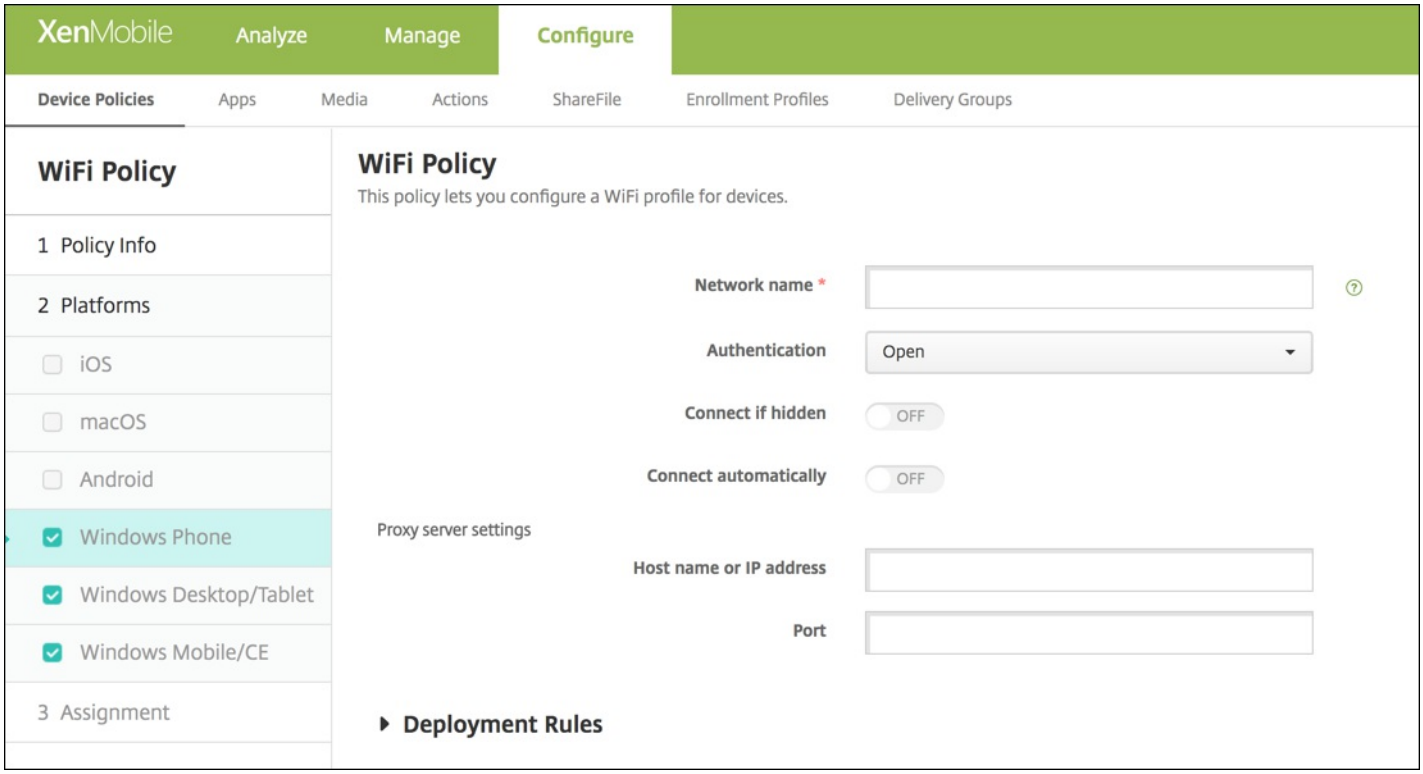
802.1x

- **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 AC**: 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.

Definir as configurações do Windows Phone

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Defina estas configurações:

- **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 de WiFi.
  - 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 WiFi. 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.

Aberto

- **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.

WPA Pessoal, WPA-2 Pessoal

- **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.

WPA-2 Enterprise

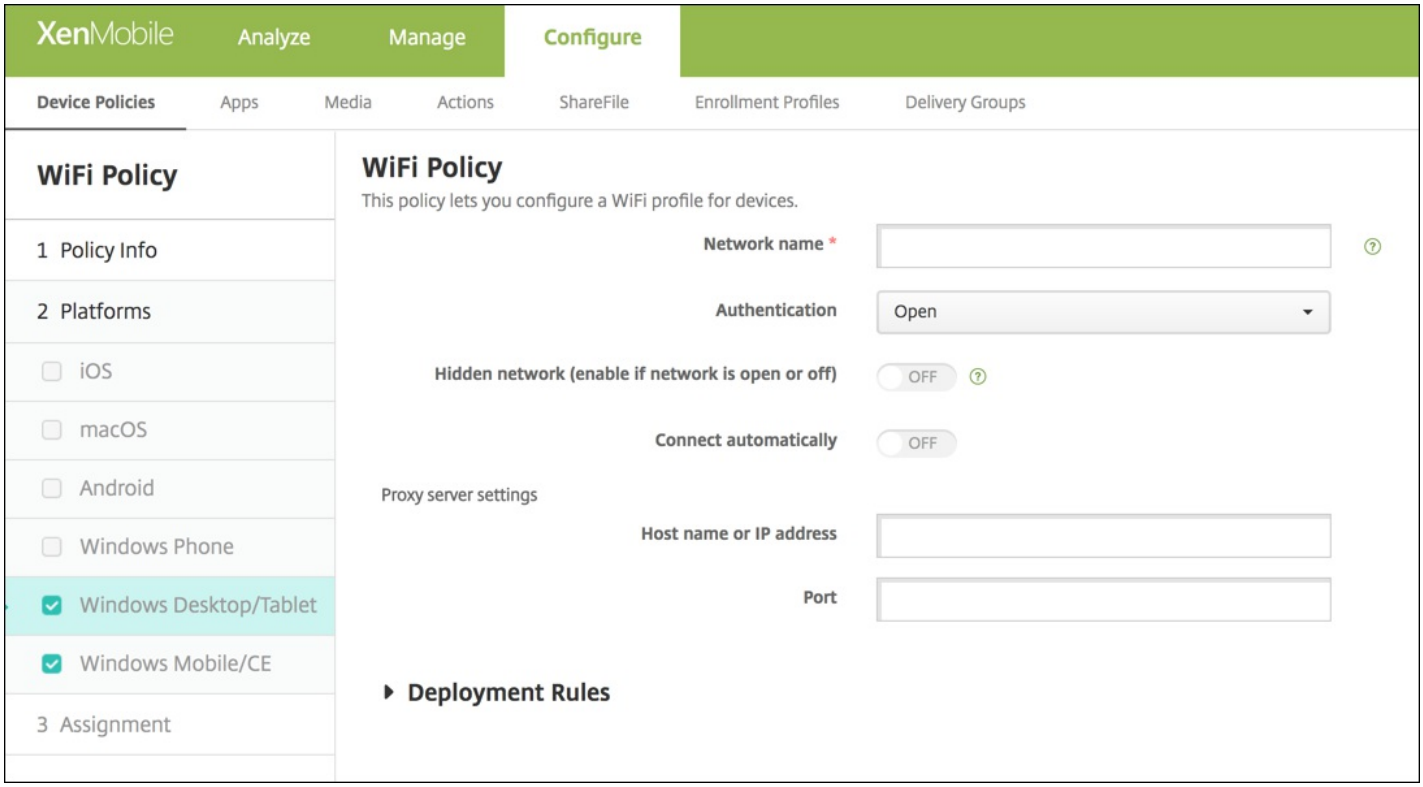
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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.

Definir as configurações do Windows Desktop/Tablet



Faça as seguintes configurações:

Configurações do Windows 10

- **Autenticação**: Na lista, clique no tipo de segurança para usar com a conexão de WiFi.
  - 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 WiFi. Para configurar o SCEP, vá para a página **Distribuição** de **Configurações > Provedores de credenciais**. Para obter mais informações, consulte Provedores de credenciais.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

As seções a seguir listam as opções de configuração de cada um dos tipos de conexão anteriores.

Aberto

- **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.

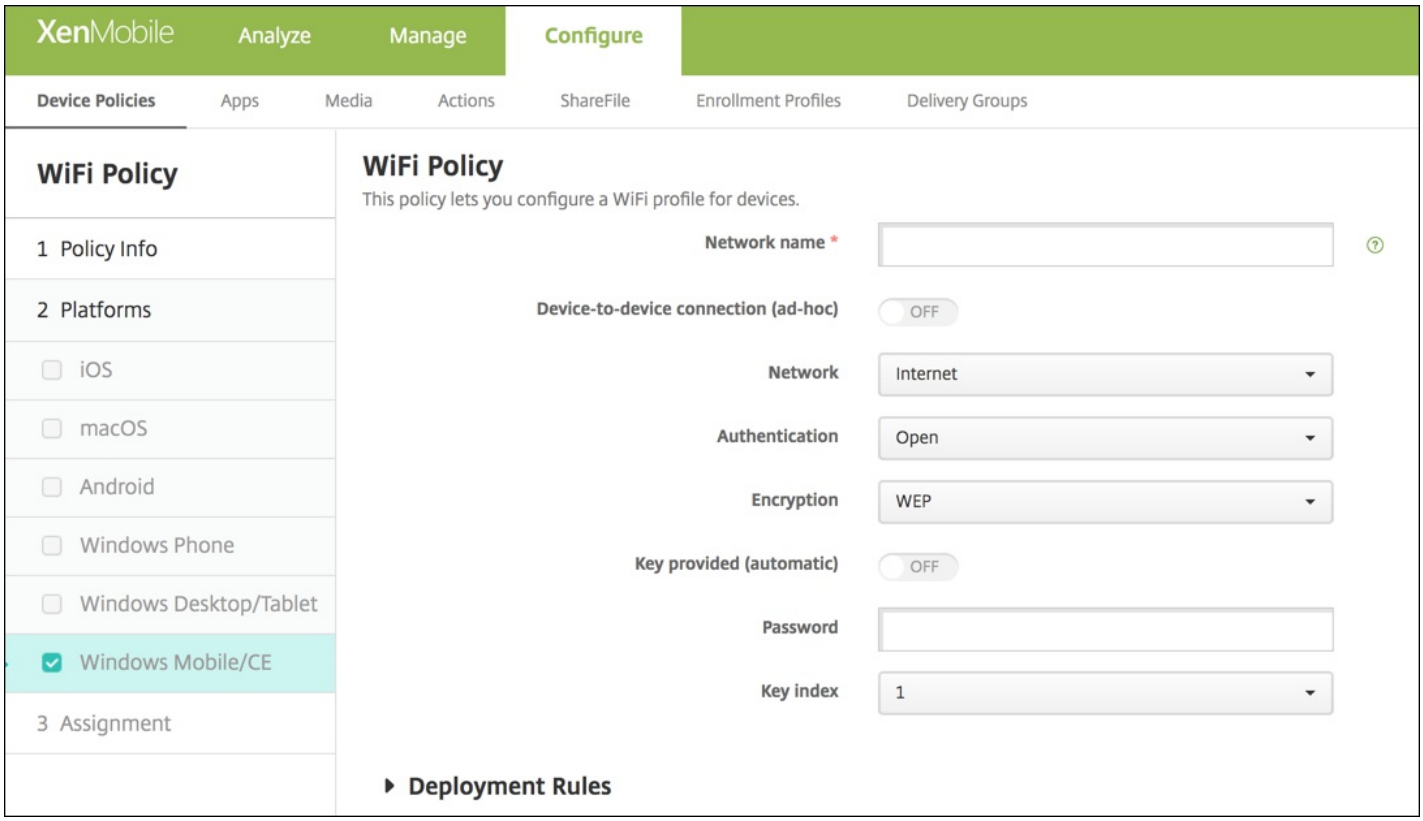
WPA Pessoal, WPA-2 Pessoal

- **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.

WPA-2 Enterprise

- **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**.

Configurar o Windows Mobile/CE



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Defina estas configurações:

- **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 valor 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 de WiFi.
  - 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.

Aberto

- **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.

WPA Pessoal, WPA-2 Pessoal

- **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.

WPA-2 Enterprise

- **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**.

Chave fornecida (automática): escolha se a chave fornecida é automaticamente ou não. O valor 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**.

7. Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo do certificado do Windows CE

Feb 21, 2018

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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. A caixa de diálogo **Adicionar uma nova política** é exibida.

3. Expanda **Mais** e, em **Segurança**, clique em **Certificado Windows CE**. A página de informações **Política de certificado Windows CE** é exibida.

4. No painel **Informações sobre a política**, digite as seguintes informações:

- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página de informações **Plataforma da política de certificado Windows CE** é exibida.

6. Defina estas configurações:

- **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.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

8. Clique em **Avançar**. A página de atribuição **Política de certificado Windows CE** é exibida.

9. Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega ou selecione na lista um grupo ou os grupos aos quais você deseja atribuir a política. Os grupos que você selecionar aparecerão na lista **Grupos de entrega que receberão a atribuição de aplicativos**.

10. 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 **O**, nenhuma outra opção precisará ser configurada.
- Ao lado de **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**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 se aplicará 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.

11. Clique em **Salvar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Windows Information Protection device policy

Feb 21, 2018

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 corporativos usando a WIP (Proteção de Informações do Windows) no Microsoft TechNet.

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.

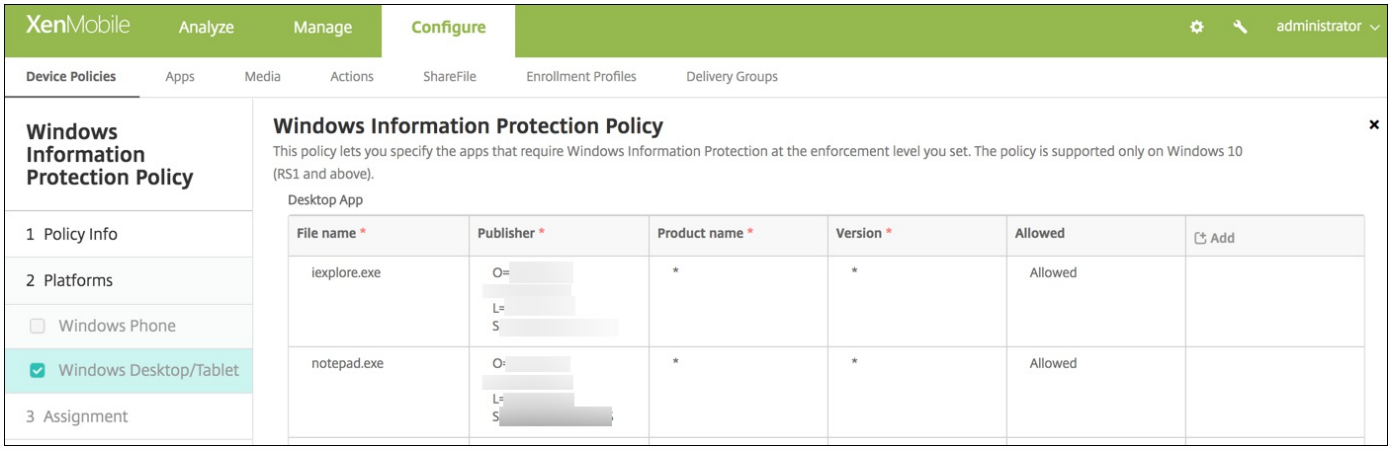
O XenMobile inclui alguns aplicativos comuns, e você pode adicionar outros. Especifique para a política um nível de execução que afete a experiência do usuário. Por exemplo, você pode:

- 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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.
2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.
3. Comece a digitar **Proteção de informações do Windows** e, em seguida, clique nesse nome nos resultados da pesquisa. A página **Informações da política de proteção de informações do Windows** é exibida.
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**. O painel **Plataforma de política** é exibido.
6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Defina essas configurações para cada plataforma escolhida:

- **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 **O**.
  - **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 CPS de relatório.
  - **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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 **I**. O padrão é **O**.

- **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 **Servidores proxy** que sejam usados para o tráfego 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 pelo WIP. Para cada recurso de nuvem, você também pode especificar um servidor proxy na lista **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 **I**, 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 **I**, a configuração **Exigir proteção durante bloqueio** será exibida. O valor 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 **I**.

- **Revogar o certificado WIP ou 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 **O**, as chaves não serão revogadas, e o usuário continuará a ter acesso a arquivos protegidos após o cancelamento do registro. O padrão é **I**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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 **O**.

> **Nota**
>
> Para obter informações gerais sobre como configurar políticas, consulte Adicionar uma política de dispositivo.

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 XenMobile Server, 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:

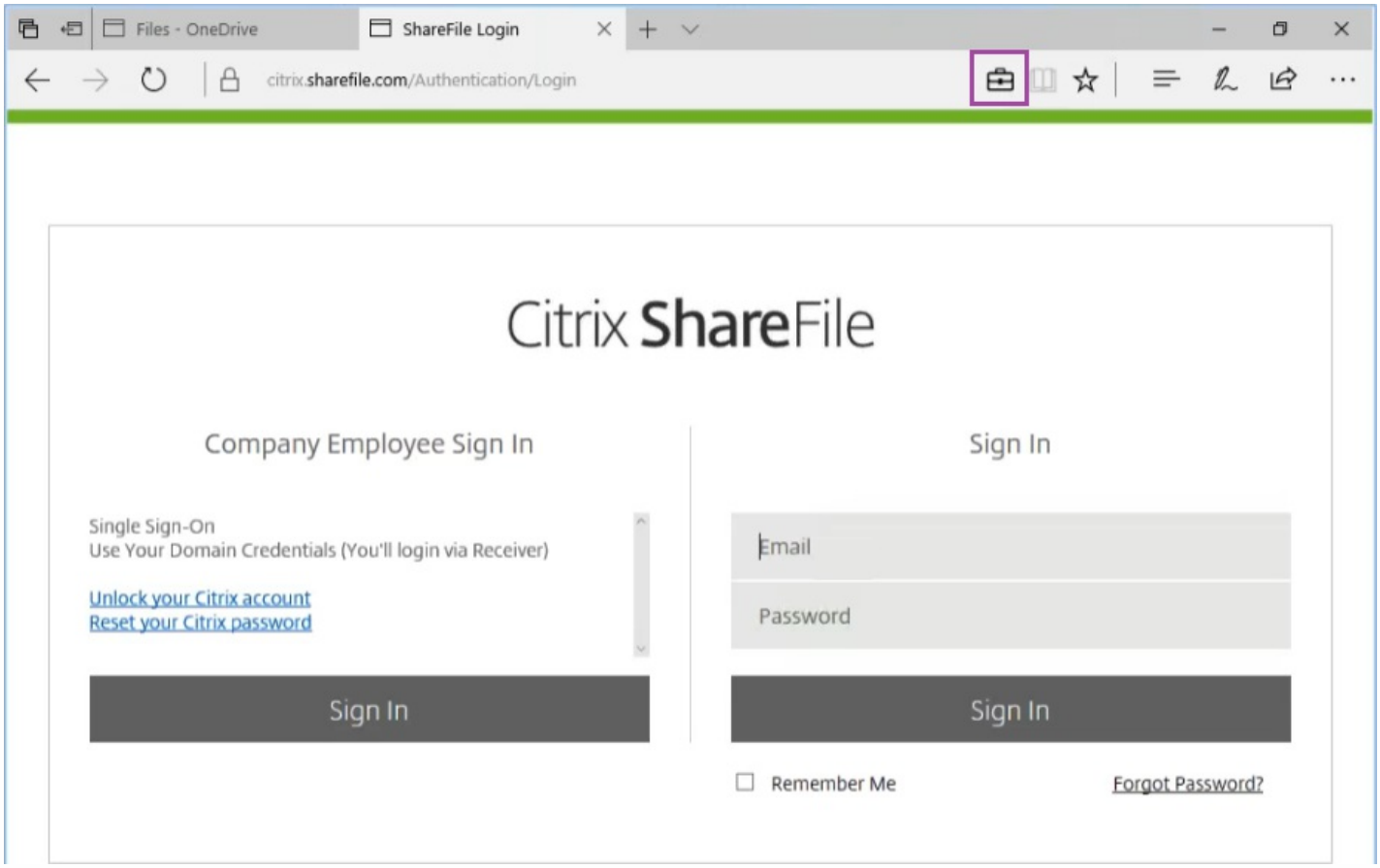
   cipher /r:ESFDRA
3. Quando solicitado, insira uma senha para proteger o arquivo de chave privada.

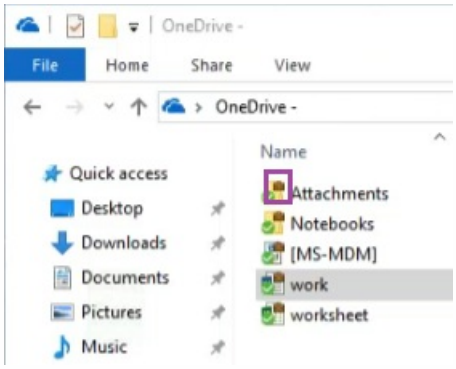
   O comando cipher cria um arquivo .cer e .pfx.
4. No console XenMobile, vá para **Configurações > Certificados** e importe o arquivo .cer, que se aplica a tablets e telefones Windows 10.

Experiência do usuário

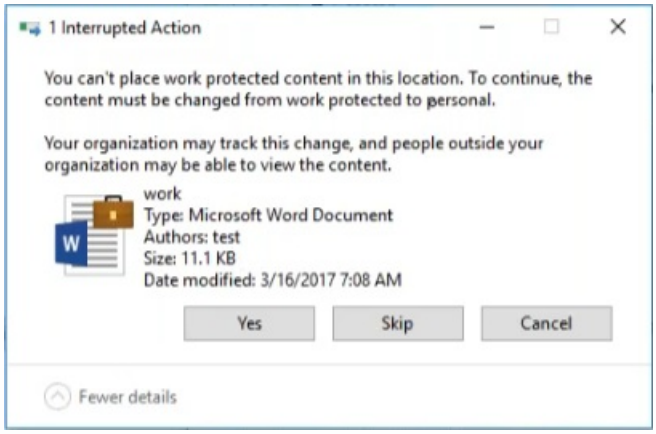
Quando a Proteção de informações do Windows está em vigor, aplicativos e arquivos incluem um ícone:

© 1999-2017 Citrix Systems, Inc. All rights reserved.





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.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Políticas de dispositivo das opções de XenMobile

Feb 21, 2018

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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Expanda **Mais** e, em **Agente XenMobile**, clique em **Opções do XenMobile**. A página **Política de opções do XenMobile** é exibida.

4. No painel **Informações sobre a política**, insira as seguintes informações:

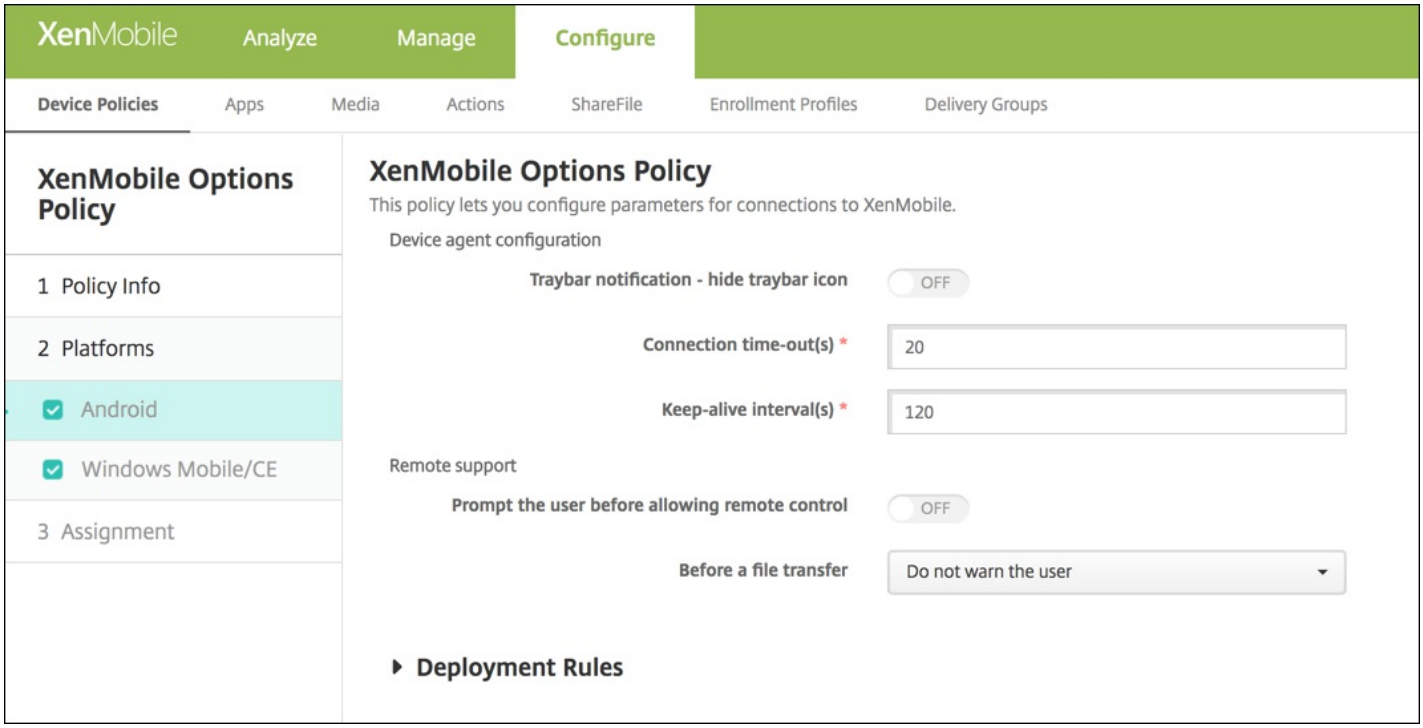
- **Nome da política**: digite um nome descritivo para a política.
- **Descrição**: digite uma descrição opcional para a política.

5. Clique em **Avançar**. A página **Plataforma de política** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

Definir as configurações do Android



Defina estas configurações:

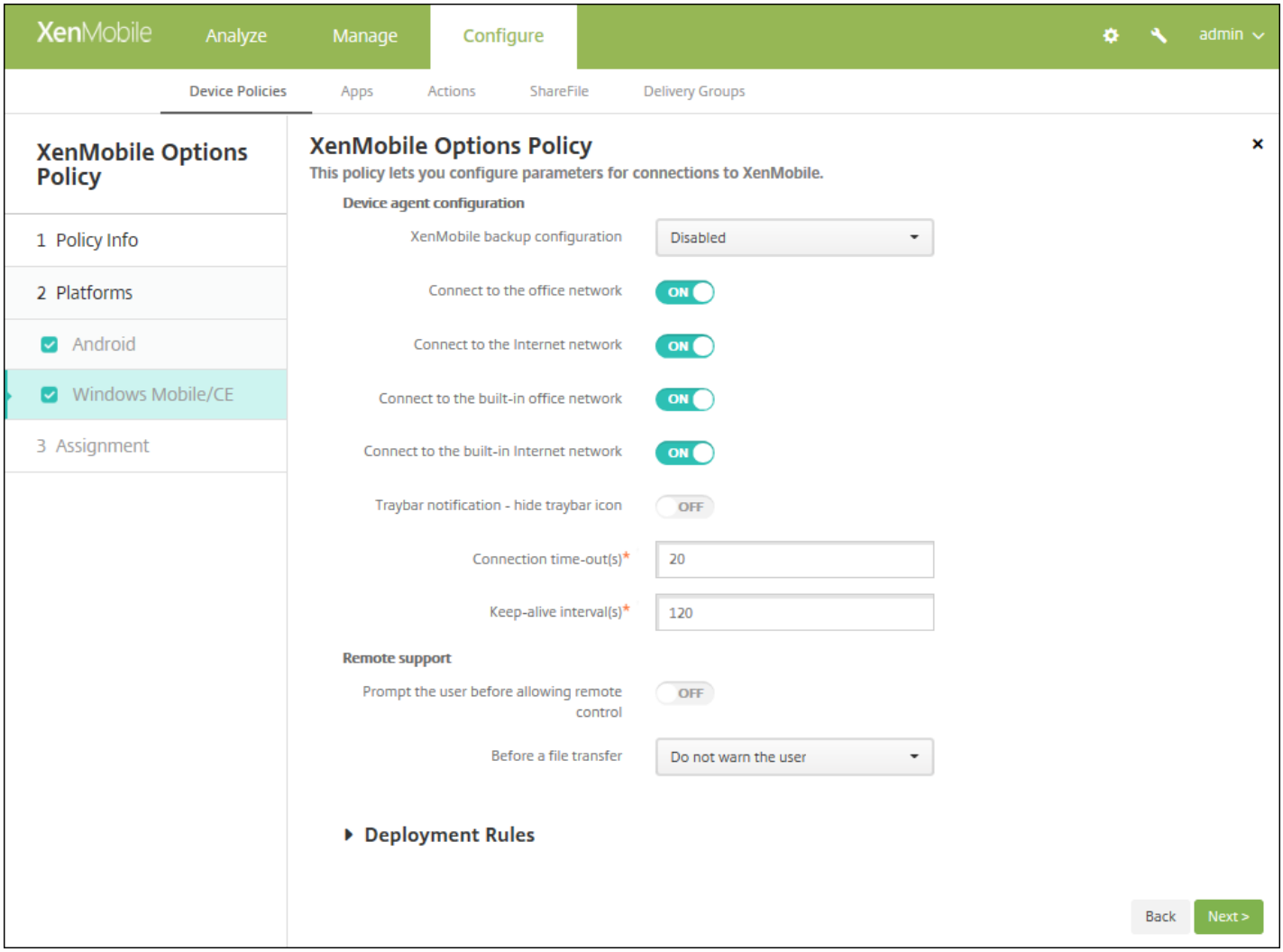
- **Notificação da barra da bandeja - ocultar ícone da barra da bandeja**: selecione se o ícone da bandeja do sistema

© 1999-2017 Citrix Systems, Inc. All rights reserved.

está visível ou oculto. O padrão é **Desativado**.

- **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 **Desativado**.
- **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**.

Definir as configurações do Windows Mobile/CE



Defina estas configurações:

- **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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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 **Desativado**.
- **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 **Desativado**.
  - **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**.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Política de dispositivo de desinstalação do XenMobile

Feb 21, 2018

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.

1. No console XenMobile, clique em **Configurar > Políticas de dispositivo**. A página **Políticas de dispositivo** é exibida.

2. Clique em **Adicionar**. É exibida a caixa de diálogo **Adicionar uma nova política**.

3. Expanda **Mais** e, em **Agente XenMobile**, clique em **Desinstalação do XenMobile**. A página **Política de Desinstalação do XenMobile** é exibida.

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 de informações **Plataforma de política** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando você terminar de definir as configurações de uma plataforma, consulte a Etapa 7 para saber como definir as regras de implantação dessa plataforma.

Definir as configurações do Android e do Windows Mobile/CE

Defina esta configuração para cada plataforma selecionada:

- **Desinstalar XenMobile dos dispositivos**: selecione se o XenMobile deve ser desinstalado de cada dispositivo no qual você implantar essa política. O padrão é **Desativado**.

7.Configure regras de implantação e escolha grupos de entrega. Para obter mais informações, consulte Adicionar uma política de dispositivo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Adicionar aplicativos

Mar 16, 2018

> ## Important
>
> O MDX 10.7.5 é a versão final compatível com a preparação de XenMobile Apps. Você não pode usar o MDX Toolkit ou o MDX Service 10.7.10 e versões posteriores para remover versões 10.7.5 ou versões posteriores do XenMobile Apps. Você deve acessar o XenMobile Apps nas lojas de aplicativos públicos.

Você adiciona aplicativos ao XenMobile para gerenciamento. Você pode adicionar os aplicativos ao console XenMobile, onde pode organizar os aplicativos em categorias e implantar os aplicativos para usuários.

Você pode adicionar os seguintes tipos de aplicativos ao XenMobile:

- **MDX** . Esses aplicativos são preparados com o MDX Toolkit. Implante os aplicativos MDX que você obtém de lojas internas e públicas.
- **Loja de aplicativos pública**. Estes aplicativos incluem os aplicativos gratuitos ou pagos em uma loja de aplicativos pública, como o iTunes ou o Google Play. Por exemplo, o GoToMeeting.
- **Web e SaaS**. Esses aplicativos incluem os aplicativos acessados em uma rede interna (aplicativos Web) ou em uma rede pública (SaaS). Você pode criar seus próprios aplicativos ou escolher de um conjunto de conectores de aplicativo para autenticação de logon único em aplicativos Web existentes. Por exemplo, GoogleApps_SAML.
- **Empresarial**. Estes aplicativos são aplicativos nativos não preparados com o MDX Toolkit e que não contêm as políticas associadas a aplicativos MDX.
- **Link da Web**. Esses aplicativos são endereços Web (URLs) para sites públicos ou privados ou para aplicativos Web que não exigem logon único.

> ## Nota
>
> A Citrix oferece suporte à instalação silenciosa de aplicativos iOS e Android da Samsung. A instalação silenciosa significa que os usuários não são solicitados a instalar aplicativos que você implanta no dispositivo. Os aplicativos são instalados silenciosamente em segundo plano.
>
> Pré-requisitos para implementar a instalação silenciosa:
>
> - Para aplicativos 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 aplicativos Android, ative políticas para Samsung for Enterprise (SAFE) ou 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.

Como funcionam os aplicativos móveis e MDX

> ## Important

© 1999-2017 Citrix Systems, Inc. All rights reserved.

> O MDX 10.7.5 é a versão final compatível com a preparação de XenMobile Apps. Você não pode usar o MDX Toolkit ou o MDX Service 10.7.10 e versões posteriores para remover versões 10.7.5 ou versões posteriores do XenMobile Apps. Você deve acessar o XenMobile Apps nas lojas de aplicativos públicas.

O XenMobile dá suporte aos aplicativos para iOS e Android, incluindo XenMobile Apps, como Secure Hub, Secure Mail e Secure Web, e ao uso de políticas do MDX. Usando o console XenMobile, você pode carregar aplicativos e fornecer os aplicativos para dispositivos de usuário. Além dos XenMobile Apps, você pode adicionar os seguintes tipos de aplicativos:

- Os aplicativos que você desenvolve para seus usuários.
- Os aplicativos em que você deseja permitir ou restringir os recursos de dispositivo usando as políticas do MDX.

Para distribuir XenMobile Apps, siga estas etapas gerais:

1. Baixe os arquivos public-store MDX em https://www.citrix.com/downloads/xenmobile/product-software/xenmobile-enterprise-edition-worx-apps-and-mdx-toolkit.html.

2. Carregue esses arquivos no console XenMobile (**Configurar > Aplicativos**), atualizando as políticas MDX conforme necessário.

3. Carregue os arquivos MDX nas lojas de aplicativos públicas. Para obter mais informações, consulte Adicionar um aplicativo MDX neste artigo.

O MDX Toolkit prepara aplicativos para dispositivos com iOS e Android com a lógica e as políticas da Citrix. A ferramenta pode preparar de forma segura um aplicativo que foi criado dentro da sua organização ou um aplicativo criado fora da empresa.

Sobre aplicativos obrigatórios e opcionais

Quando você adiciona aplicativos a um grupo de entrega, escolha se eles são opcionais ou necessários. 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.

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)
- MDX Toolkit 10.6 (versão mínima)
- Propriedade personalizada de servidor, force.server.push.required.apps

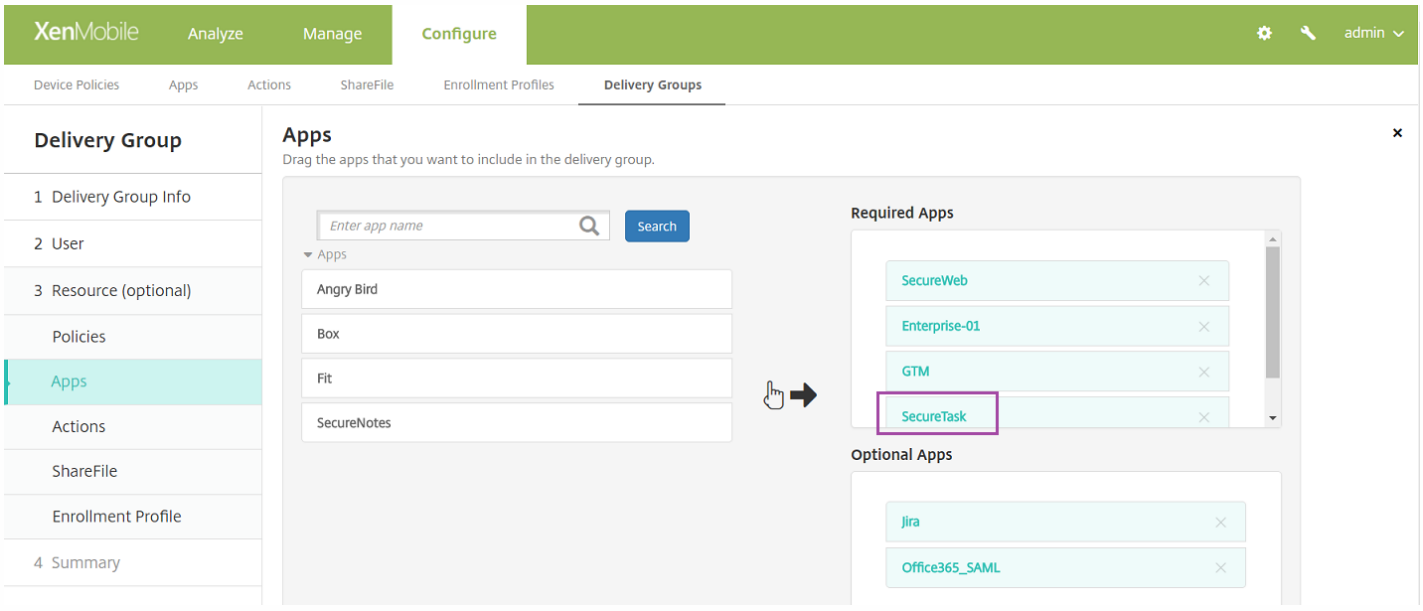
  A implantação forçada dos aplicativos necessários está desativada por padrão. Para ativar o recurso, crie uma propriedade personalizada de servidor principal. Definir a **Chave** e o **Nome de exibição** para **force.server.push.required.apps** e defina o **Valor** como **verdadeiro**.

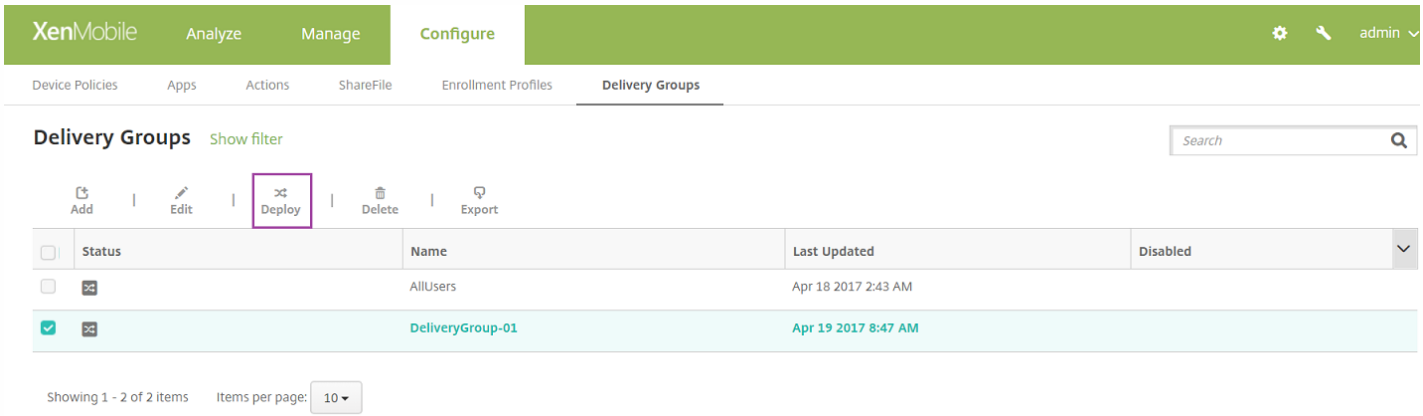
- Após a atualização do XenMobile Server e do Secure Hub: os usuários com dispositivos registrados devem fazer logoff e, em seguida, fazer logon no Secure Hub, uma vez, para obter as atualizações necessárias de implantação de aplicativos.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Exemplos

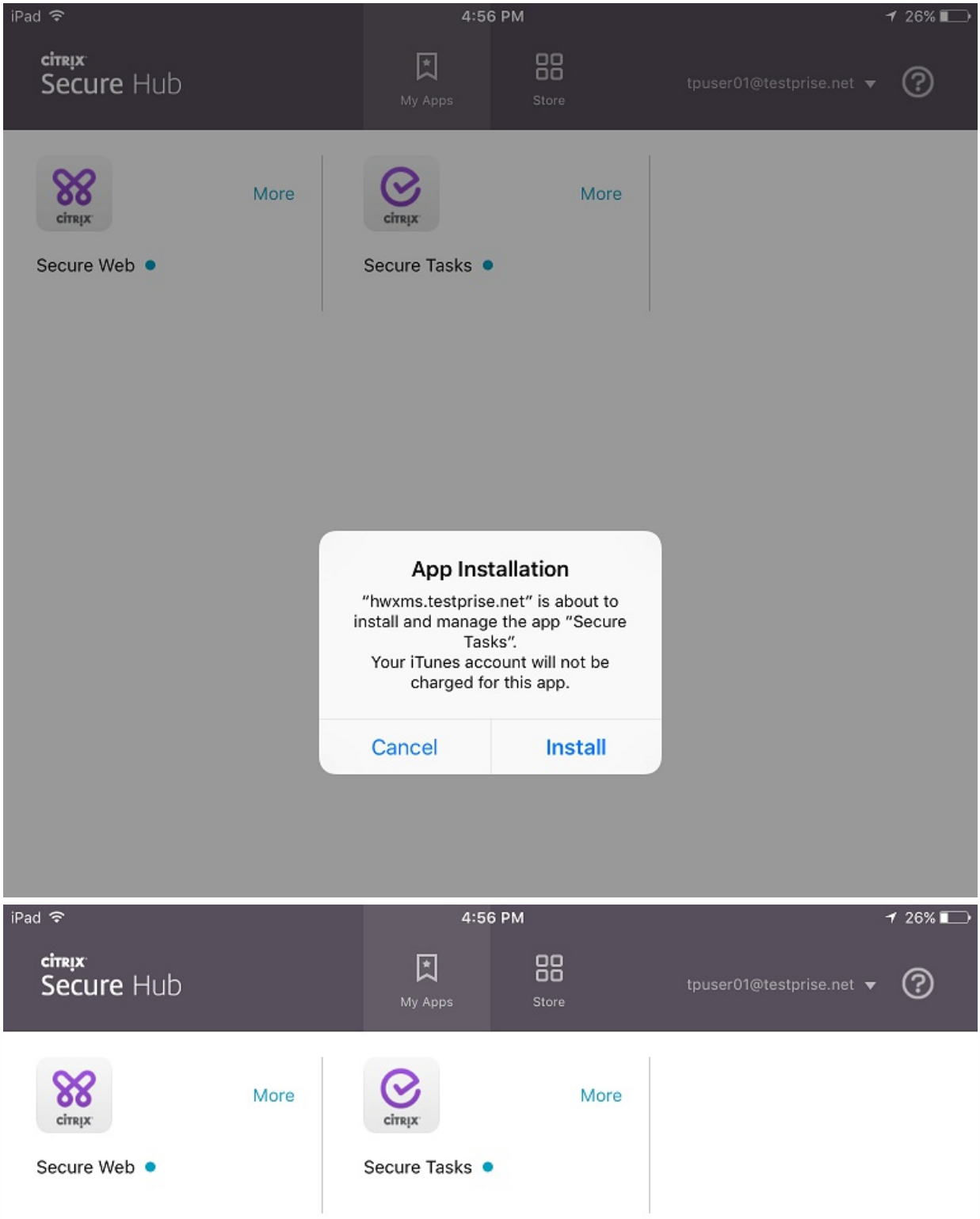
Os exemplos a seguir mostram a sequência de adicionar o aplicativo Secure Tasks a um grupo de entrega e, em seguida, implantar o grupo de entrega.





Depois que o aplicativo de exemplo, o Secure Tasks, implanta o dispositivo do usuário, o Secure Hub avisa ao usuário para instalar o aplicativo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Important

Os aplicativos necessários habilitados para MDX, incluindo aplicativos empresariais e aplicativos da loja de aplicativos pública, são atualizados imediatamente mesmo que você configure uma política MDX para um período de carência de atualização de aplicativo e o usuário opte por atualizar o aplicativo posteriormente.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.)

Como funcionam os aplicativos SaaS e da Web

O XenMobile vem com um conjunto de conectores de aplicativos, que são modelos que você pode configurar para logon único em aplicativos Web e SaaS. Às vezes, você pode configurar os modelos para gerenciamento e criação de contas de usuário. O XenMobile inclui os conectores Security Assertion Markup Language (SAML). Os conectores SAML são usados para aplicativos Web que dão suporte ao protocolo SAML para gerenciamento de conta de usuário e de SSO. O XenMobile dá suporte a SAML 1.1 e a SAML 2.0.

Você também pode criar seus próprios conectores SAML.

Para obter mais informações, consulte Adicionar um aplicativo Web ou SaaS neste artigo.

Como funcionam os aplicativos empresariais

Os aplicativos geralmente residem na sua rede interna. Os usuários podem se conectar aos aplicativos usando o Secure Hub. Quando você adiciona um aplicativo empresarial, o XenMobile cria o conector de aplicativo para ele. Para obter mais informações, consulte Adicionar um aplicativo empresarial neste artigo.

Como funciona a loja de aplicativos pública

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Você pode definir as configurações para obter nomes de aplicativo e descrições da Apple App Store e do Google Play. Quando você obtém as informações de aplicativo da loja, o XenMobile substitui o nome existente e a descrição. Para obter mais informações, consulte Adicionar um aplicativo de loja de aplicativos pública neste artigo.

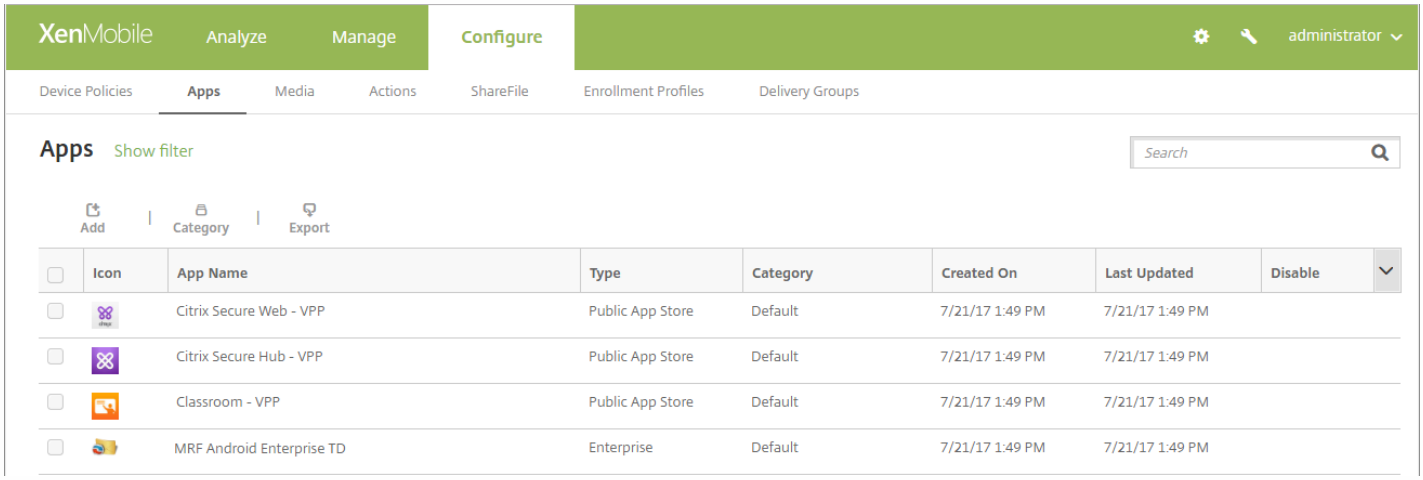
Como funcionam os links da Web

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. Quando você termina de configurar um link da Web, o link é exibido como um ícone na XenMobile Store. Quando os usuários fazem login no Secure Hub, o link é exibido com a lista de aplicativos e áreas de trabalho disponíveis. Para obter mais informações, consulte Adicionar um aplicativo de Link da Web neste artigo.

Acrescentar um aplicativo MDX

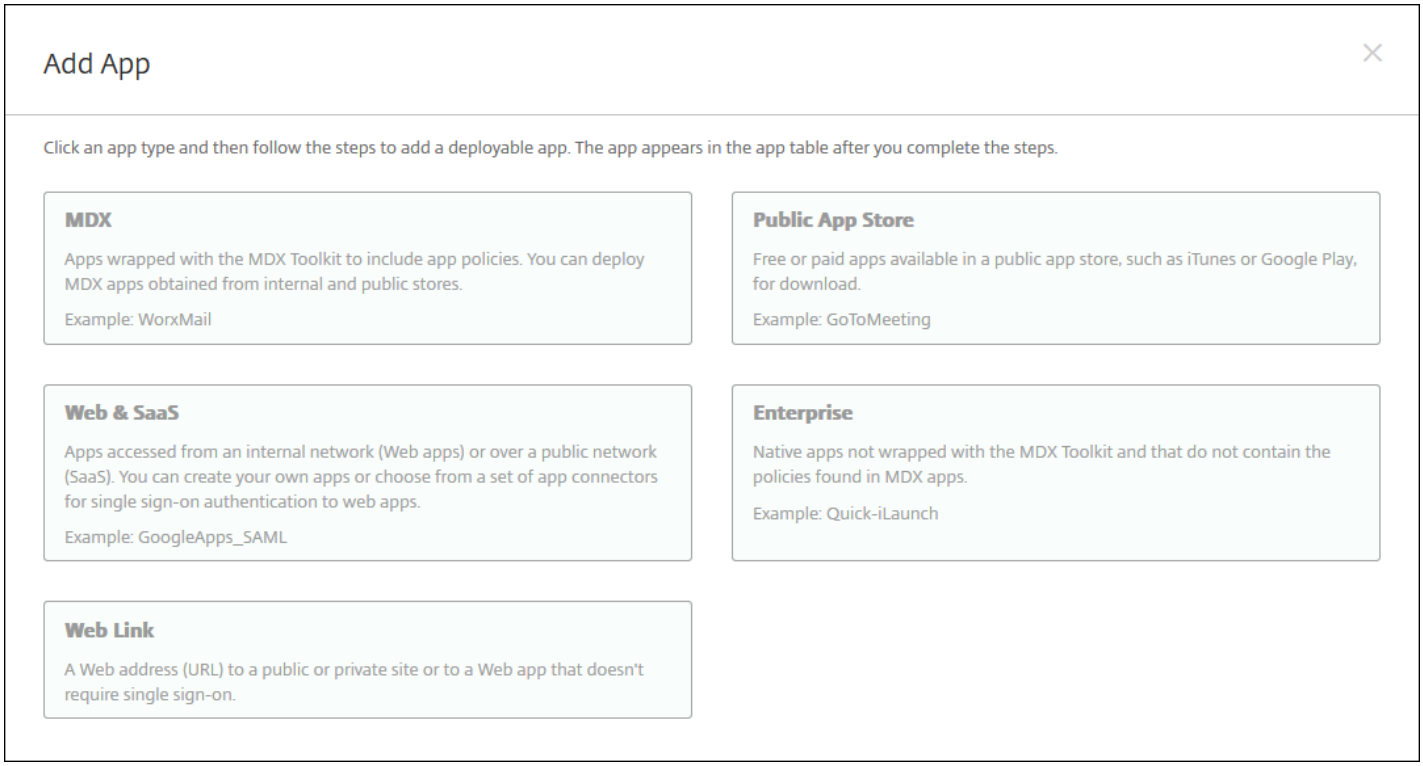
Quando você recebe um aplicativo móvel do MDX preparado para um dispositivo iOS ou Android, você pode carregar o aplicativo para o XenMobile. Depois de carregar o aplicativo, você pode configurar os detalhes do aplicativo e as configurações de política. Para obter mais informações sobre as políticas de aplicativo que estão disponíveis para cada tipo de plataforma de dispositivo, consulte Resumo das políticas do MDX. Aquela seção também contém descrições detalhadas da política.

1. No console XenMobile, clique em **Configurar** > **Aplicativos**. A página **Aplicativos** é exibida.



2. Clique em **Adicionar**. A caixa de diálogo **Adicionar aplicativo** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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. 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 Criar categorias de aplicativo.

5. Clique em **Avançar**. A página **Plataformas de aplicativo** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando terminar de definir as configurações de uma plataforma, consulte a Etapa 11 para saber como definir as regras de implantação dessa plataforma.

7. Selecione o arquivo MDX a ser carregado clicando em **Carregar** e navegando até a localização do arquivo.

- Se estiver adicionando um aplicativo iOS VPP B2B, clique em **Seu aplicativo é um aplicativo de VPP B2B?**. Em seguida, na lista, clique na conta de VPP B2B a ser usada.

8. Clique em **Avançar**. A página Detalhes do Aplicativo é exibida.

9. 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.
- **Versão do SO mínima**: opcionalmente, digite a versão mais antiga do sistema operacional que o dispositivo pode executar para usar o aplicativo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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 **I**.
- **Evitar o backup de dados do aplicativo**: selecione se deseja impedir que usuários façam backup de dados do aplicativo. O padrão é **I**.
- **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 **I**. Disponível no iOS 9.0 e versões posteriores.
- **Aplicativos implantados por meio de VPP**: selecione se você deseja implantar o aplicativo usando o VPP. Se estiver **ON** e você implantar uma versão do MDX do aplicativo e usar VPP para implantar o aplicativo, o Secure Hub mostra somente a instância VPP. O valor padrão é **Desativado**.

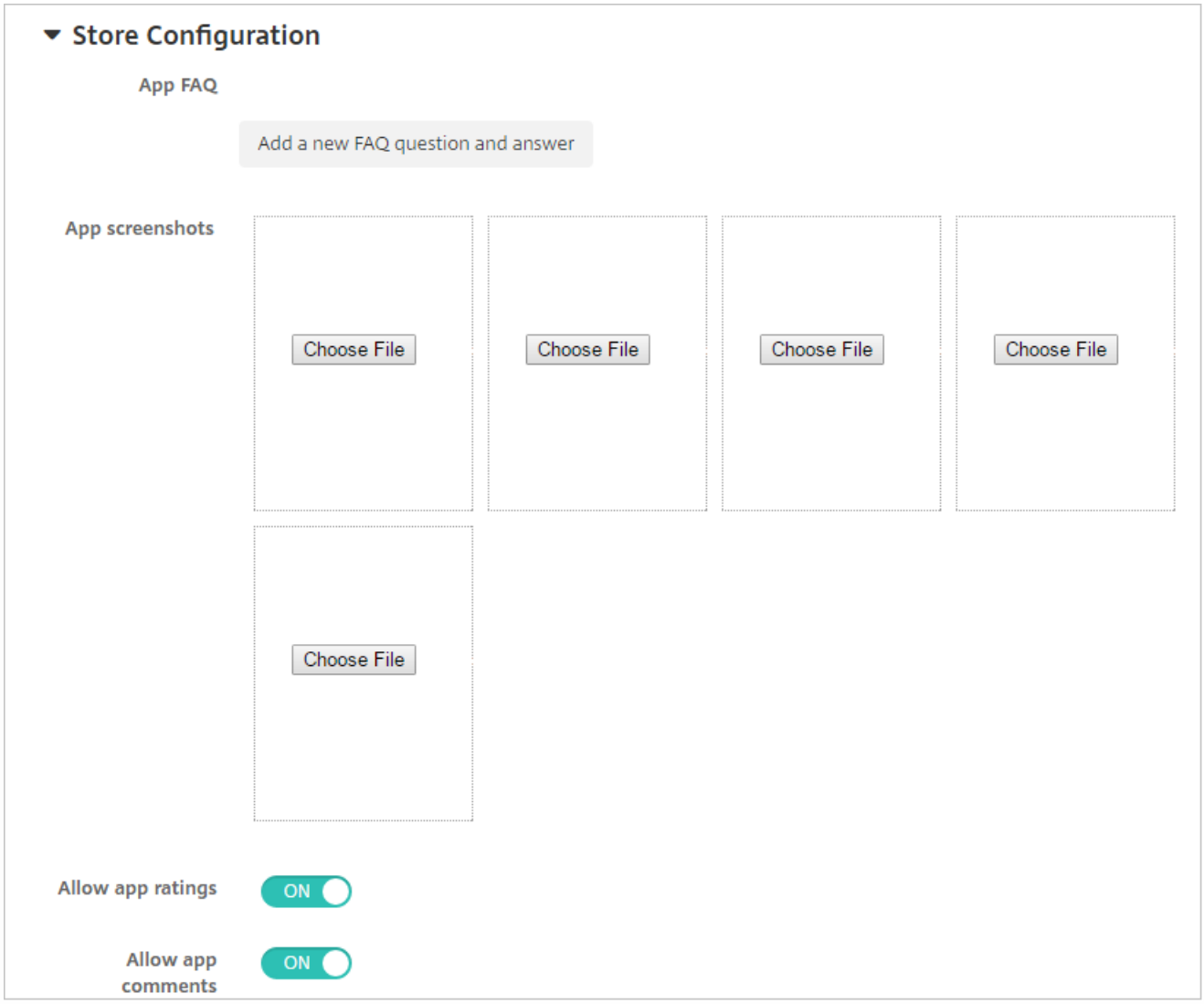
10. Configure as **Políticas de MDX**. As políticas de MDX variam por plataforma e incluem opções para áreas de política, como Autenticação, Segurança do dispositivo, Criptografia, Interação de aplicativo e Restrições de aplicativo. No console, cada uma das políticas tem uma dica de ferramenta que descreve a política.

Para obter mais informações sobre políticas de aplicativos para aplicativos MDX, consulte Visão geral de políticas MDX. Esse artigo inclui uma tabela que mostra quais políticas se aplicam a cada plataforma.

11. Configure as regras de implantação. Para obter informações, consulte Implantar recursos.

12. Expanda **Configuração da XenMobile Store**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

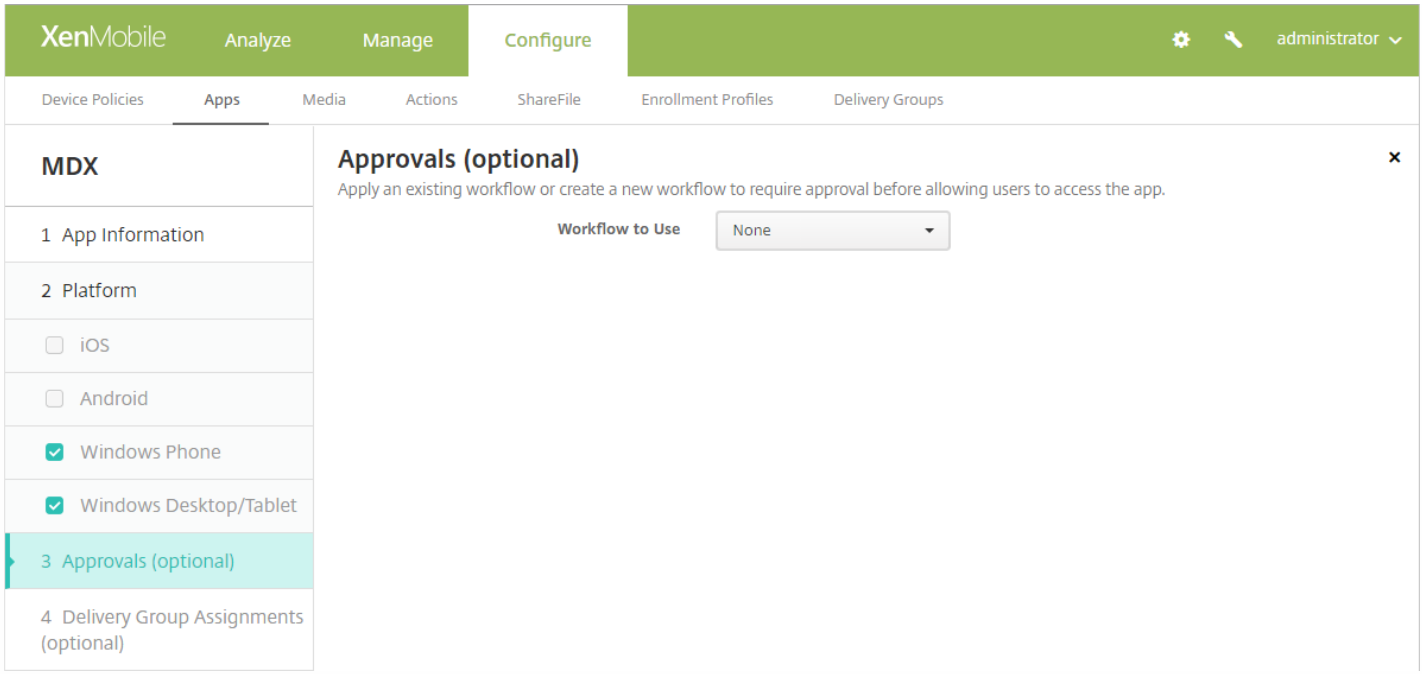


Opcionalmente, você pode adicionar ao aplicativo perguntas frequentes ou capturas de tela que são exibidas no XenMobile Store. Você também pode definir se os usuários podem classificar ou comentar no aplicativo.

- 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 XenMobile Store. 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**.

13. Clique em **Avançar**. A página **Aprovações** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Use fluxos de trabalho quando precisar de aprovação ao criar contas de usuário. Se você não precisar configurar fluxos de trabalho de aprovação, pule para a Etapa 15.

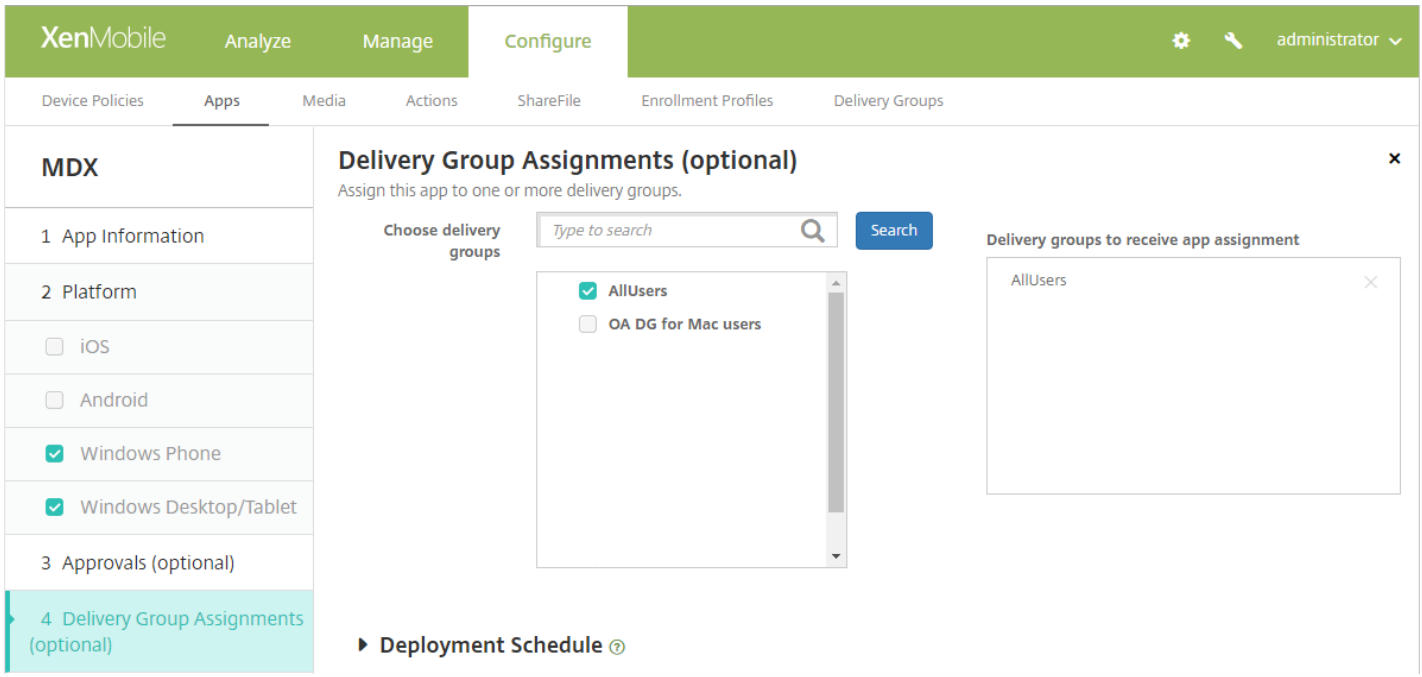
Configure esta definição se você precisar atribuir ou criar um fluxo de trabalho:

- **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 a opção **Criar um novo fluxo de trabalho**, defina estas configurações. Para obter mais informações, consulte Criar e gerenciar 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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 desejar remover.

14. Clique em **Avançar**. A página **Atribuição do grupo de entrega** é exibida.



15. Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega ou selecione um ou mais 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**.
- Ao lado de 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 se aplicará 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 **Salvar**.

Criar 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

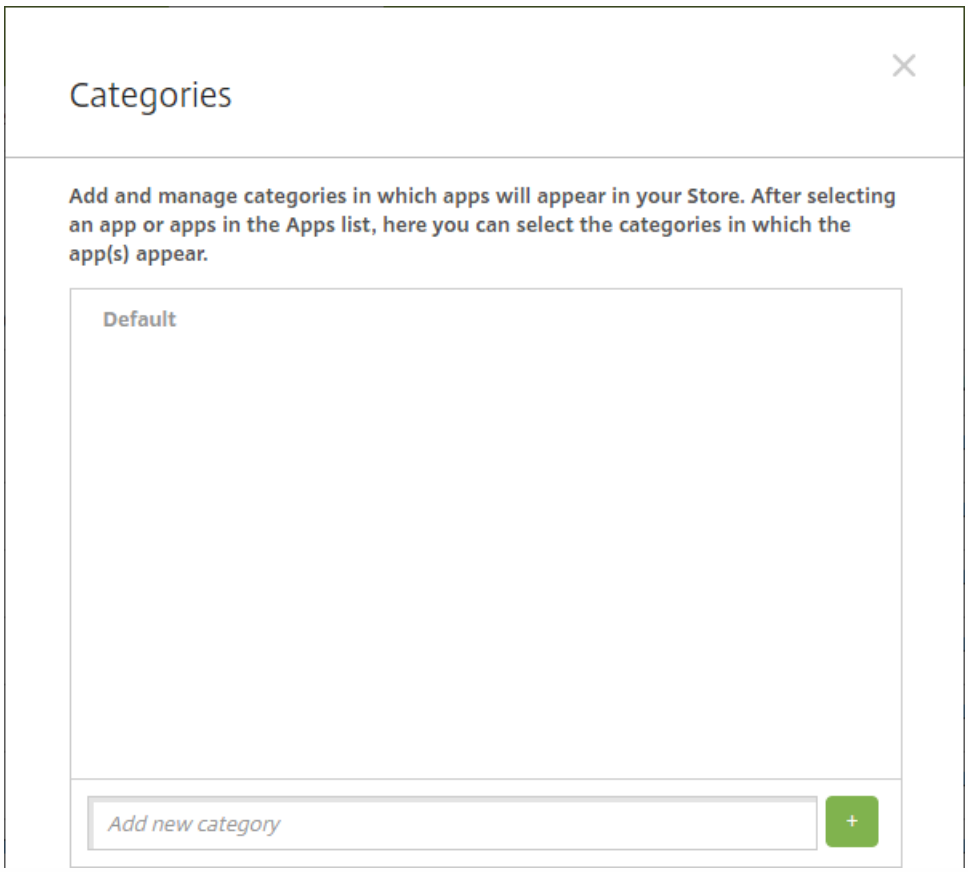
© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Configure as categorias na página **Aplicativos** do console XenMobile. Em seguida, 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**. A página **Aplicativos** é exibida.

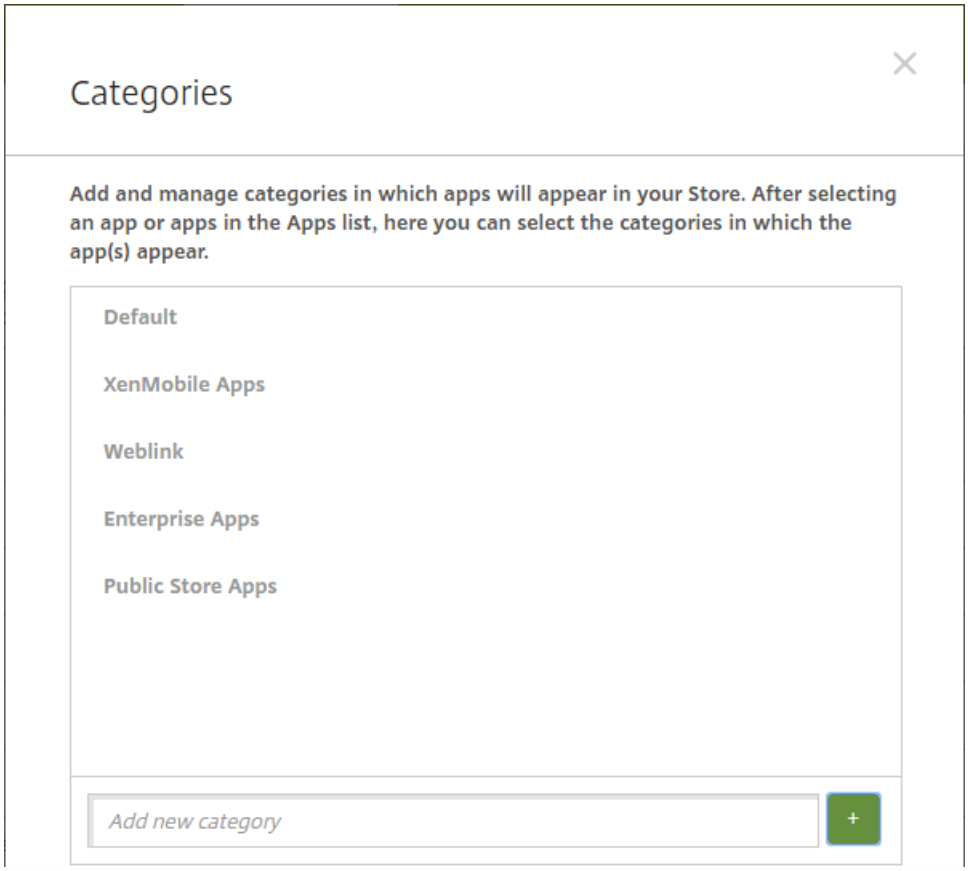
2. Clique em **Categoria**. A caixa de diálogo **Categorias** é exibida.



3. Para cada categoria que você desejar adicionar, faça o seguinte:

- Digite o nome da categoria que você deseja adicionar no campo **Adicionar nova categoria** na parte inferior da caixa de diálogo. Por exemplo, você pode digitar Aplicativos corporativos para criar uma categoria de aplicativos corporativos.
- Clique no sinal de adição (+) para adicionar a categoria. A categoria recém-criada é adicionada e aparece na caixa de diálogo **Categorias**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. Quando terminar de adicionar categorias, feche a caixa de diálogo **Categorias**.

5. Na página **Aplicativos**, você pode colocar um aplicativo existente em uma nova categoria.

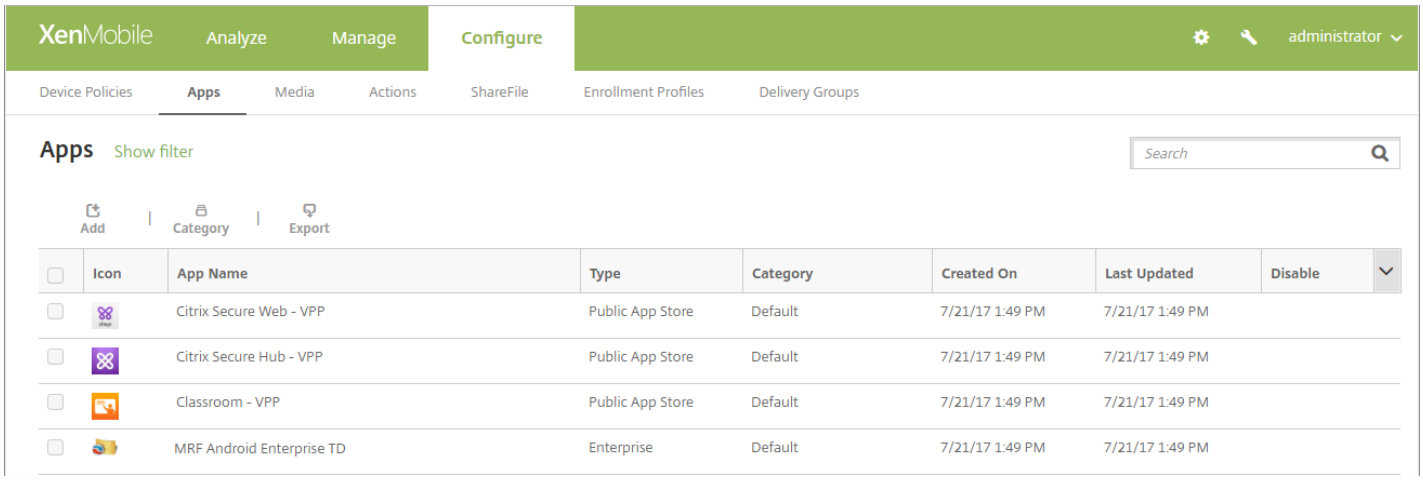
- Selecione o aplicativo que você deseja categorizar.
- Clique em **Editar**. A página **Informações do aplicativo** é exibida.
- Na lista **Categoria do aplicativo**, aplique a nova categoria marcando a caixa de seleção da categoria. Desmarque as caixas de seleção das categorias existentes que você 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 de loja de aplicativos pública

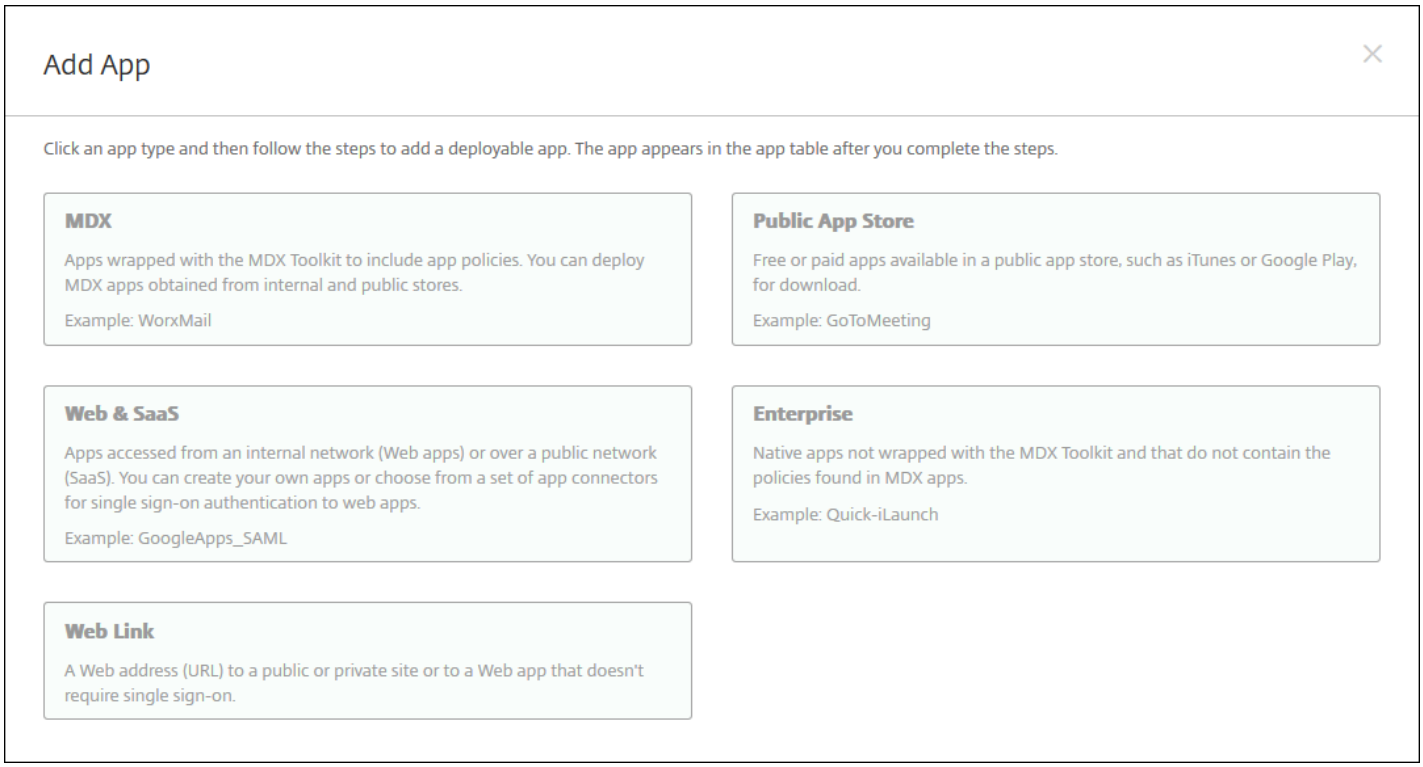
Você pode adicionar ao XenMobile aplicativos gratuitos ou pagos que estão disponíveis em uma loja de aplicativos pública, como o iTunes ou o Google Play. Por exemplo, o GoToMeeting. Além disso, quando você adiciona um aplicativo de loja de aplicativos pública pago para Android for Work, pode verificar 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 for Work simplifica o processo de localizar, comprar e distribuir aplicativos e outros dados em massa para uma organização.

1. No console XenMobile, clique em **Configurar** > **Aplicativos**. A página **Aplicativos** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Clique em **Adicionar**. A caixa de diálogo **Adicionar aplicativo** é exibida.



3. Clique em **Loja de aplicativos pública**. A página **Informações do aplicativo** é exibida.

4. 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 Criar categorias de aplicativo.

5. Clique em **Avançar**. A página **Plataformas de aplicativo** é exibida.

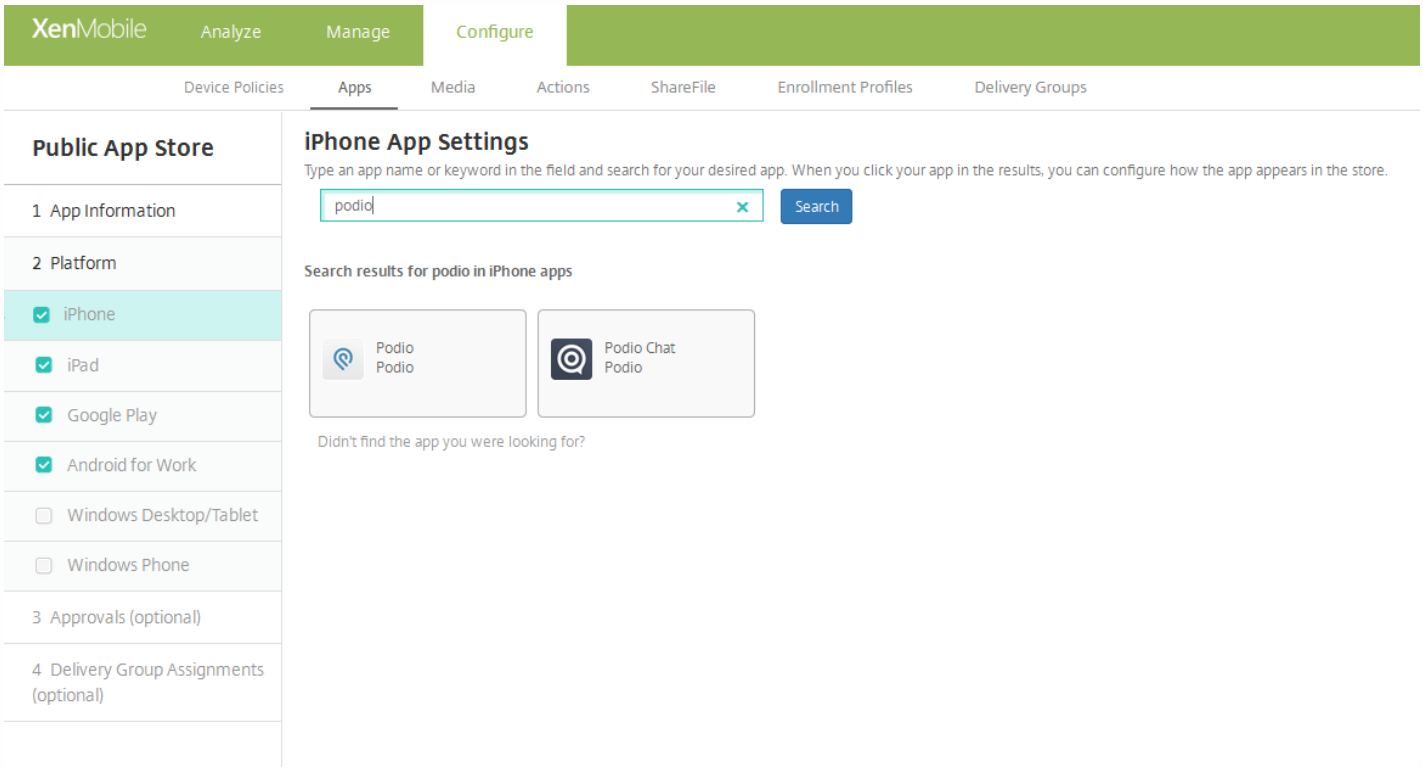
6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando terminar de definir as configurações de uma plataforma, consulte a Etapa 10 para saber como definir as regras de

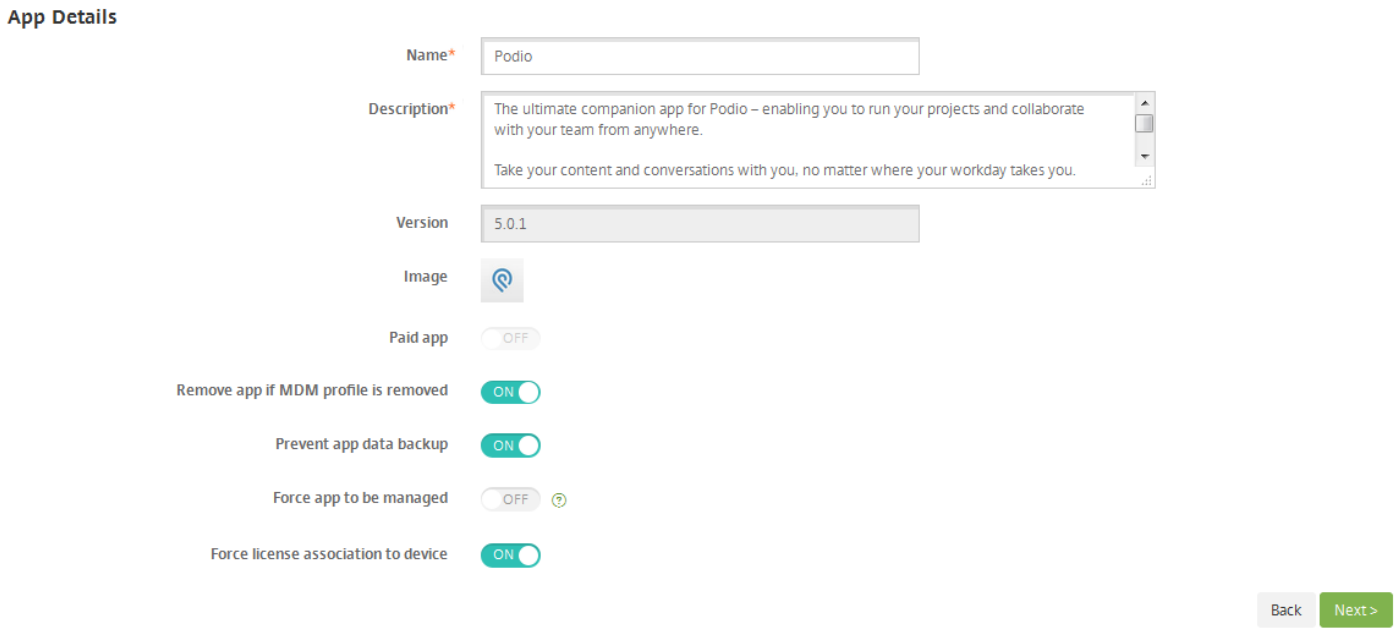
© 1999-2017 Citrix Systems, Inc. All rights reserved.

implantação dessa plataforma.

7. Selecione um aplicativo a ser adicionado digitando o respectivo nome na caixa Pesquisar e clicando em **Pesquisar**. Os aplicativos que correspondem aos critérios de pesquisa são exibidos. A figura a seguir mostra o resultado da pesquisa por **podio**.



8. Clique no aplicativo que você deseja adicionar. Os campos **Detalhes do aplicativo** são preenchidos previamente com informações relacionadas ao aplicativo escolhido (incluindo o nome, a descrição, o número de versão e a imagem associada).



9. Defina estas configurações:

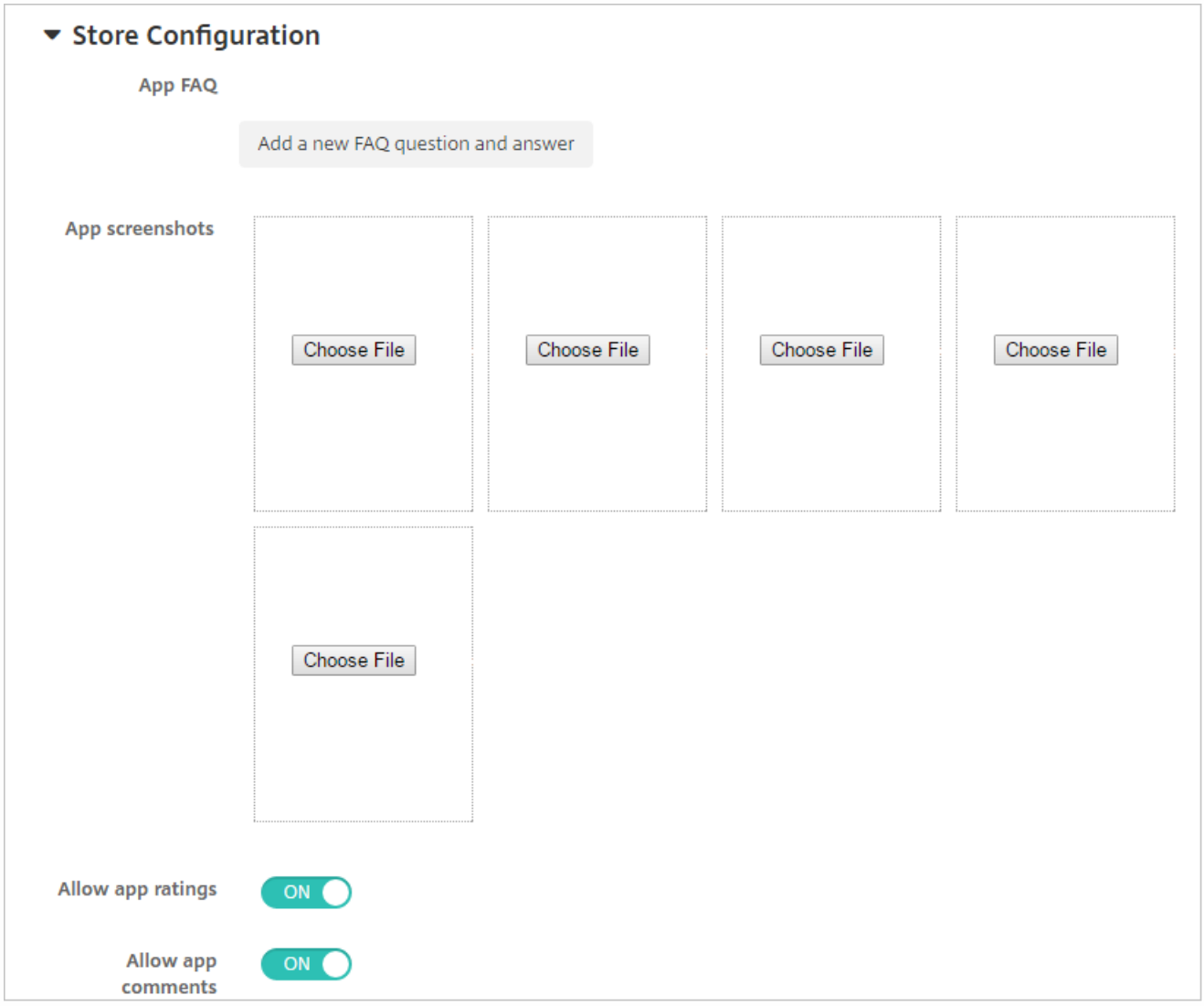
- Se necessário, altere o nome e a descrição do aplicativo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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**.
- **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.

10. Configure as regras de implantação. Para obter informações, consulte Implantar recursos.

11. Expanda **Configuração da XenMobile Store**.



Opcionalmente, você pode adicionar ao aplicativo perguntas frequentes ou capturas de tela que são exibidas no XenMobile Store. Você também pode definir se os usuários podem classificar ou comentar no aplicativo.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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 XenMobile Store. 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.

12. Expanda **Programa de Compra por Volume** ou, para o Android for Work, expanda **Compra em massa**.

Para o Volume Purchase Program, conclua as seguintes etapas.

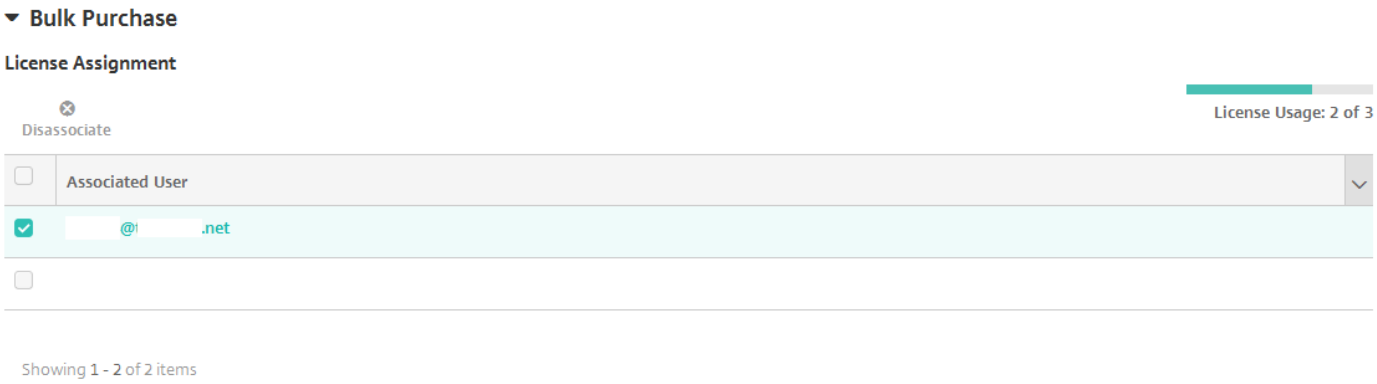
a. Na lista **Licença do VPP**, clique **Carregar um arquivo de licença do VPP** se você desejar ativar o XenMobile para aplicar uma licença de VPP ao aplicativo.

b. Na caixa de diálogo que é exibida, importe a licença.

Para Compra em massa do Android for Work, 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.

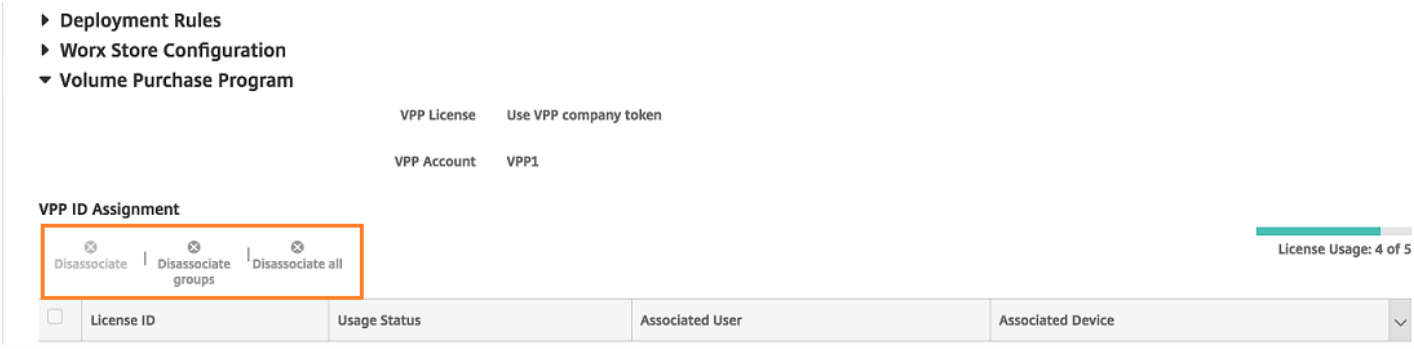
Para o Android for Work, você pode selecionar um usuário e clicar em **Desassociar** para encerrar a respectiva atribuição de licença e liberar uma licença para outro usuário. No entanto, você poderá desassociar a licença somente se o usuário não fizer parte de um grupo de entrega que contém o aplicativo específico.



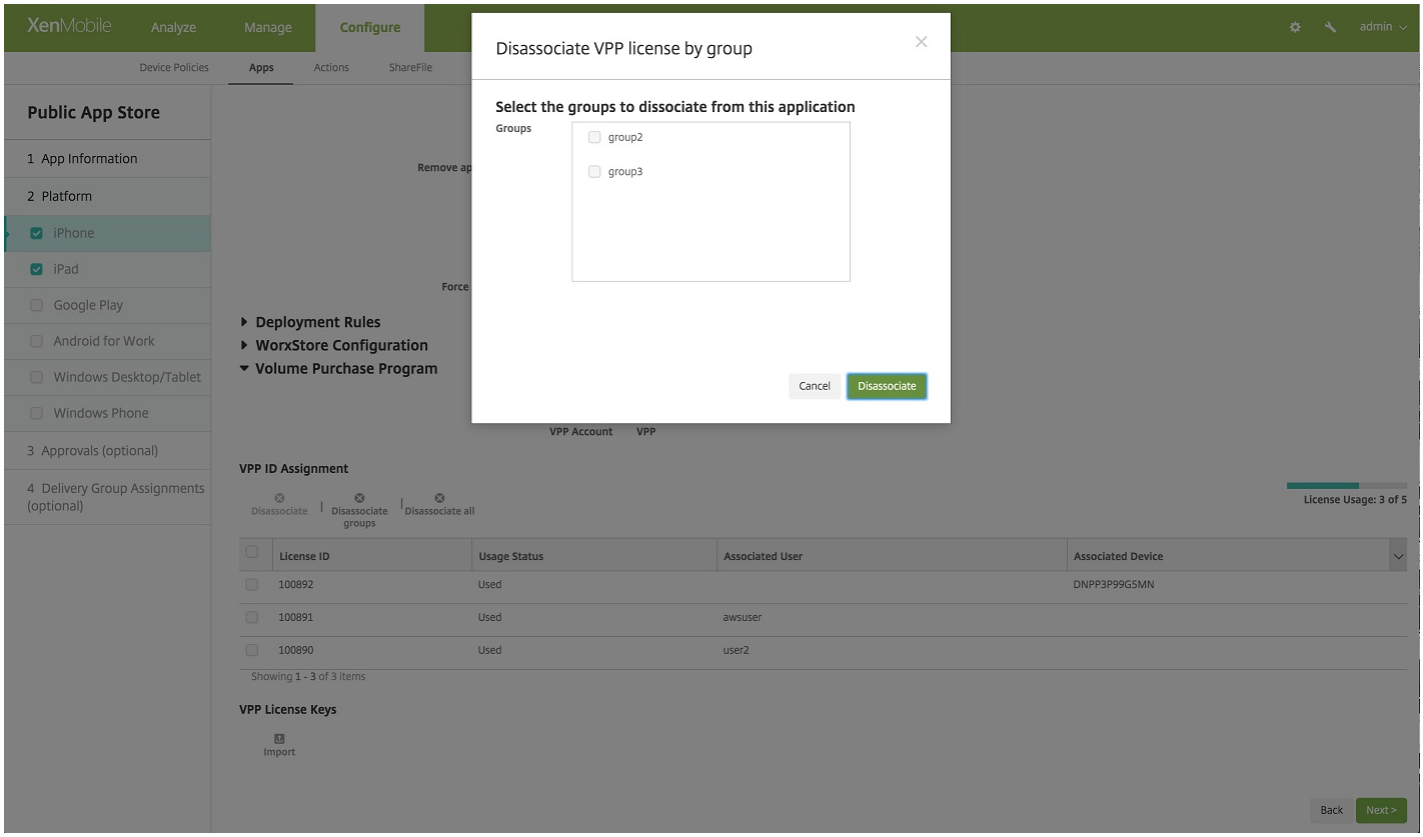
Para o Android for Work, você poderá desassociar uma licença somente se o usuário não fizer parte de um grupo de entrega que contém o aplicativo específico.

Para o iOS, você poderá desassociar licenças do Programa de Compra por Volume para usuários individuais, grupos de usuários ou todas as atribuições. Isso encerra as atribuições de licença e libera licenças.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Clicar em **Desassociar grupos** abre uma caixa de diálogo na qual você pode selecionar grupos.



13. Depois que você concluir o **Programa de Compra por Volume** ou as configurações de **Compra em massa**, clique em **Avançar**. A página **Aprovações** é exibida.

Use fluxos de trabalho quando precisar de aprovação ao criar contas de usuário. Se você não precisar configurar fluxos de trabalho de aprovação, poderá pular para a próxima etapa.

Configure estas definições se você precisar 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 a opção **Criar um novo fluxo de trabalho**, 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. 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 desejar remover.

14. Clique em **Avançar**. A página **Atribuição do grupo de entrega** é exibida.

15. Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega ou selecione um ou mais 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**.
- Ao lado de **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 se aplicará 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 **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

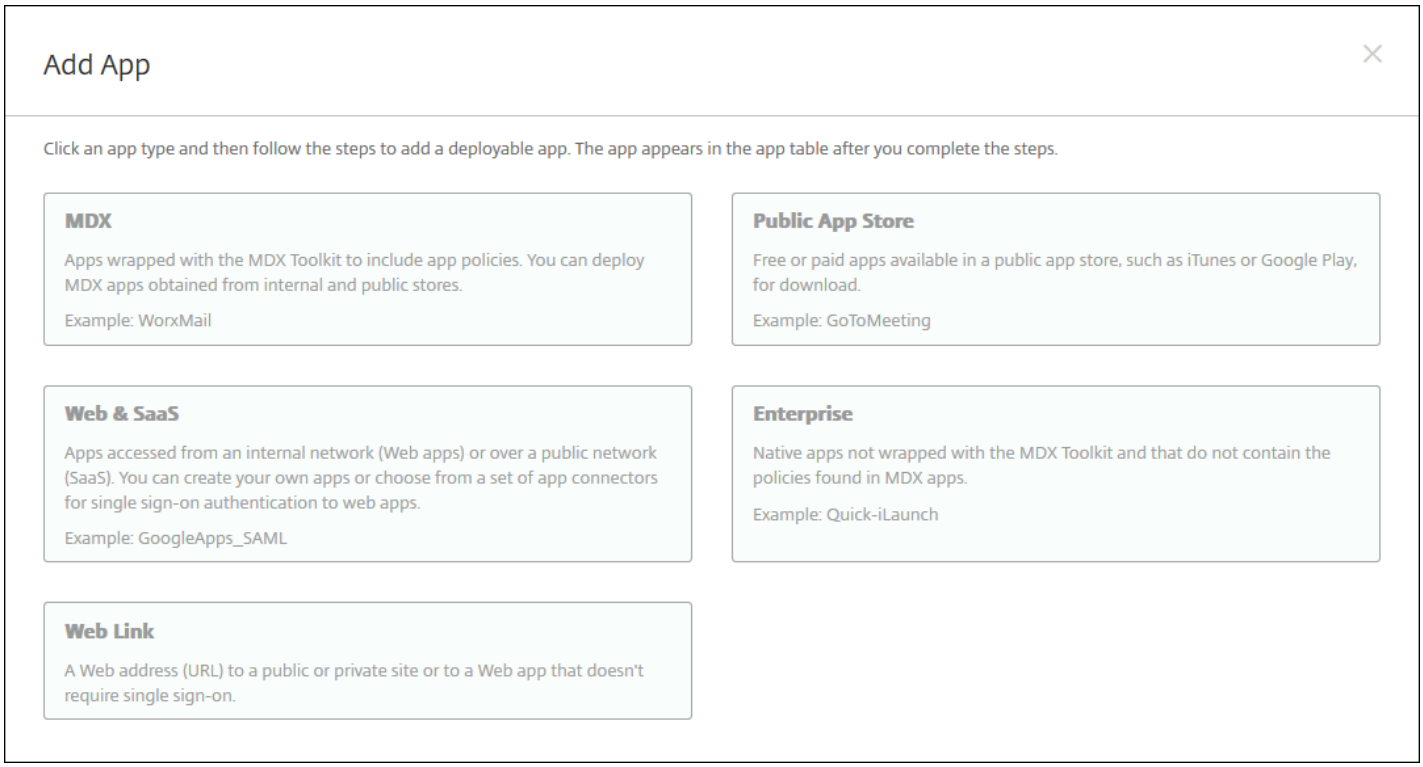
 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

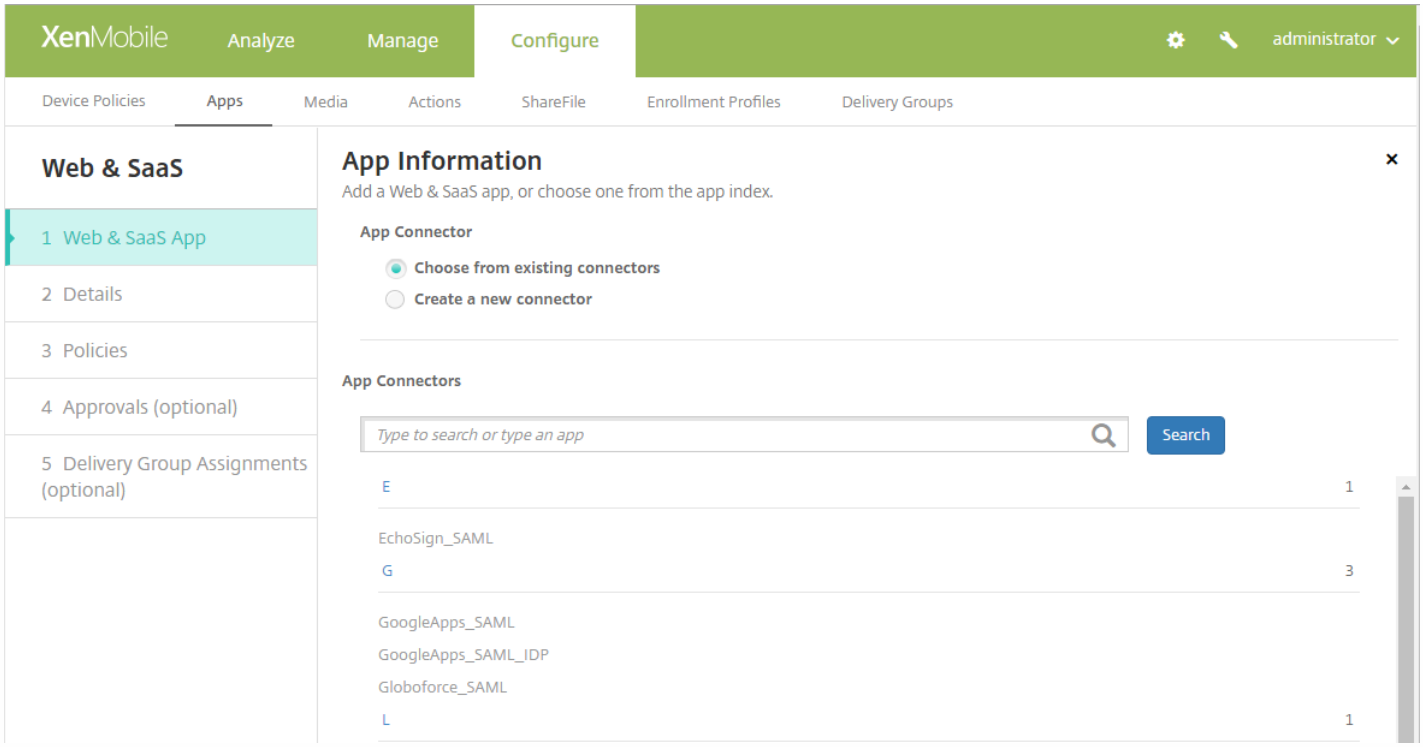
1. No console XenMobile, clique em **Configurar** > **Aplicativos**. A página **Aplicativos** é aberta.

2. Clique em **Adicionar**. A caixa de diálogo **Adicionar aplicativo** é exibida.



3. Clique em **Web e SaaS**. A página **Informações do aplicativo** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. Configure um aplicativo existente ou novo conector, da seguinte maneira.

Para configurar um conector de aplicativo existente

Na página **Informações do aplicativo**, **Escolha entre conectores existentes** já está selecionado, como mostrado acima. Clique no conector que você deseja usar na lista **Conectores de aplicativo**. As informações de conector de aplicativo são exibidas.

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 o URL preenchido 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 NetScaler Gateway. Definir essa opção como **I** adiciona a palavra-chave VPN ao aplicativo e permite que os usuários se conectem por meio do NetScaler 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 **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

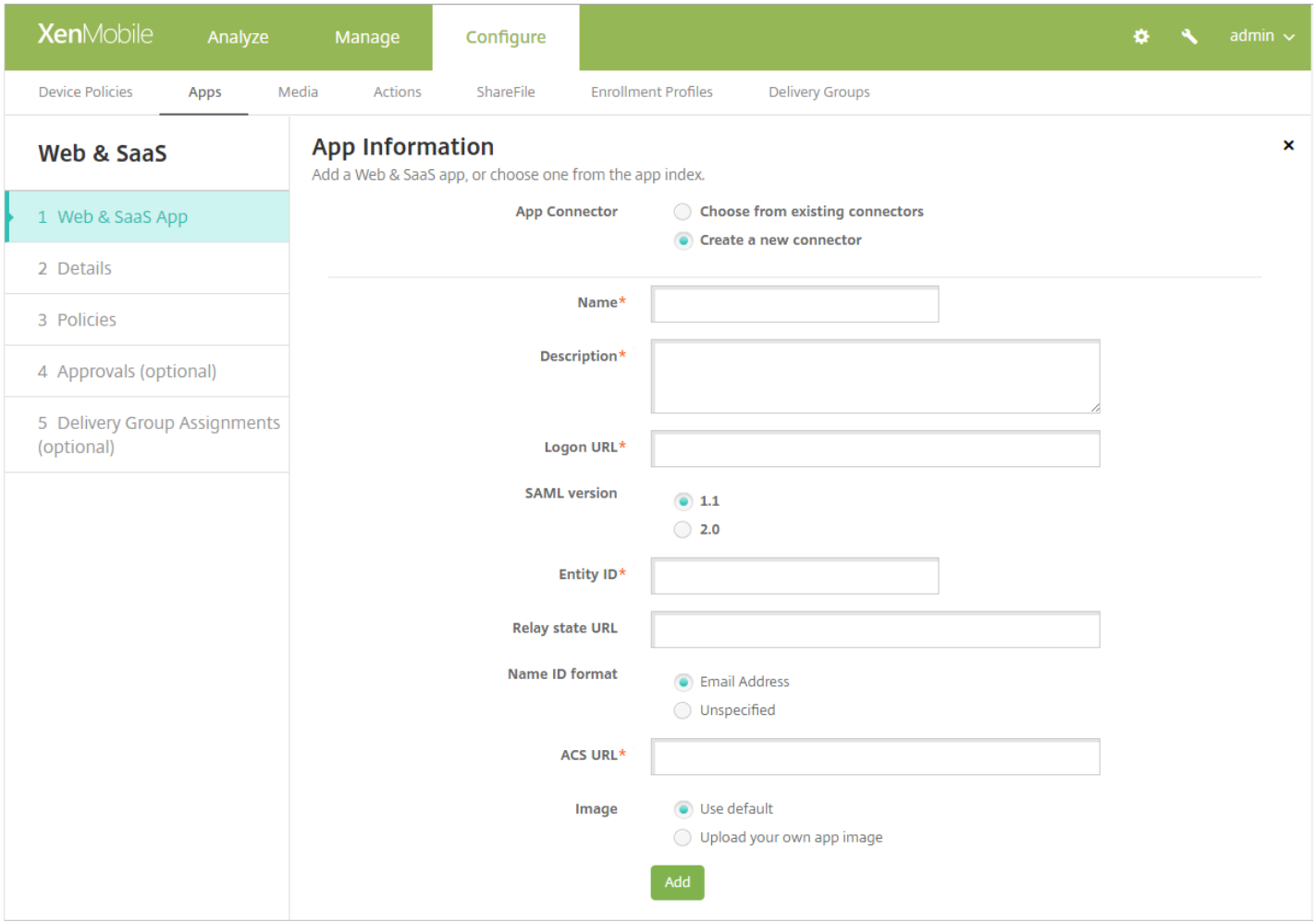
© 1999-2017 Citrix Systems, Inc. All rights reserved.

acesso ao aplicativo. O padrão é Desativar conta. As opções possíveis são:
    - Desativar a conta
    - Manter a conta
    - Remover a conta
- **Regra de Nome de Usuário**
    - Para cada regra de nome do usuário que você desejar 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 **Todos**.
        - **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 de **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

Na página **Informações do aplicativo**, selecione a opção **Criar um novo conector**. Os campos de conector de aplicativo são exibidos.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

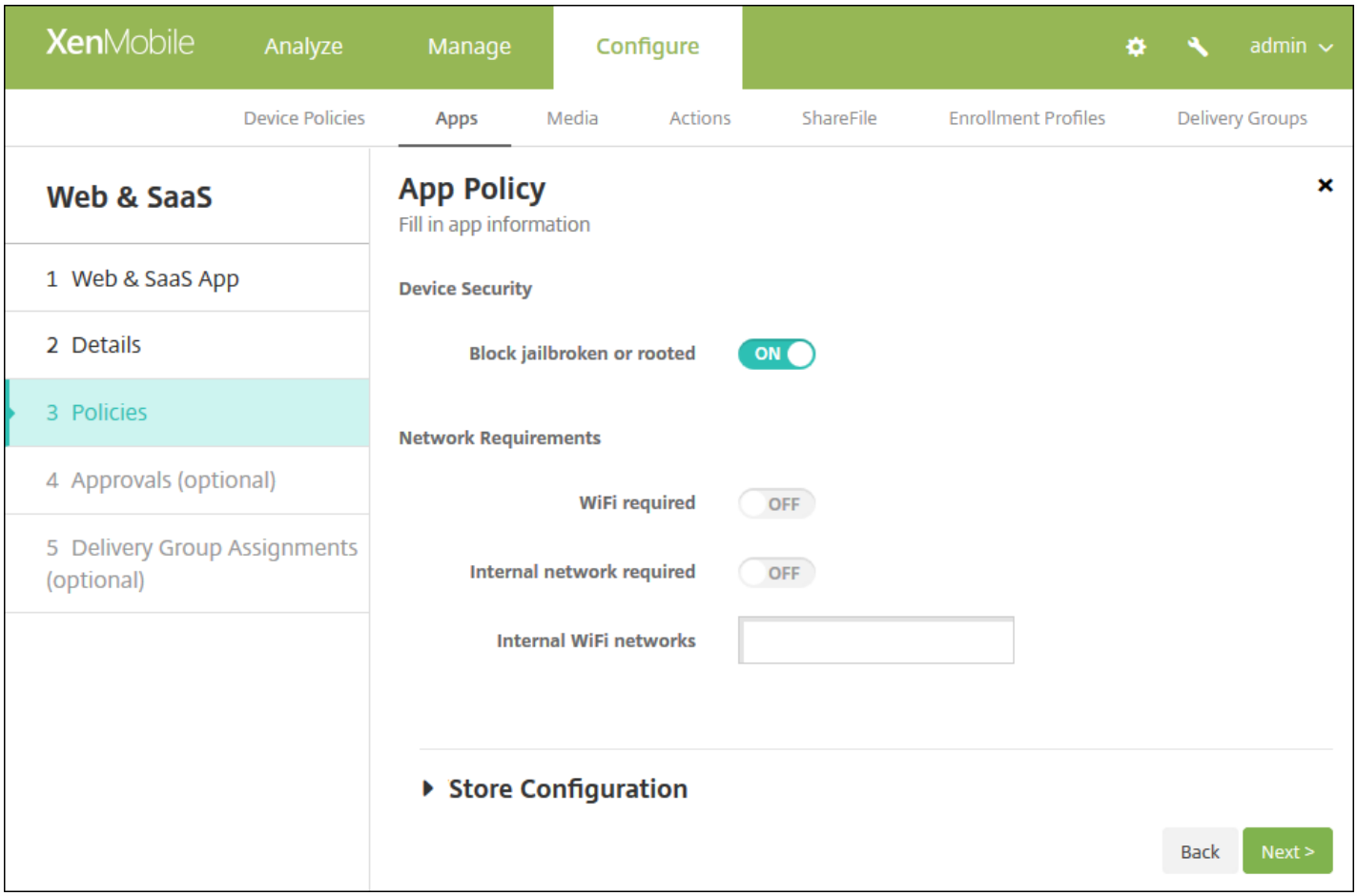


Defina estas configurações:

- **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 http://www.exemplo.com/login. 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 email**.
- **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 imagem do próprio aplicativo deve ser carregada. O padrão é Usar padrão.
  - Se quiser carregar sua própria imagem, selecione-a clicando em **Procurar** e navegando até a localização 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.
  - Quando terminar, clique em **Adicionar**. A página **Detalhes** é exibida.

5. Clique em **Avançar**. A página **Política de aplicativos** é exibida.

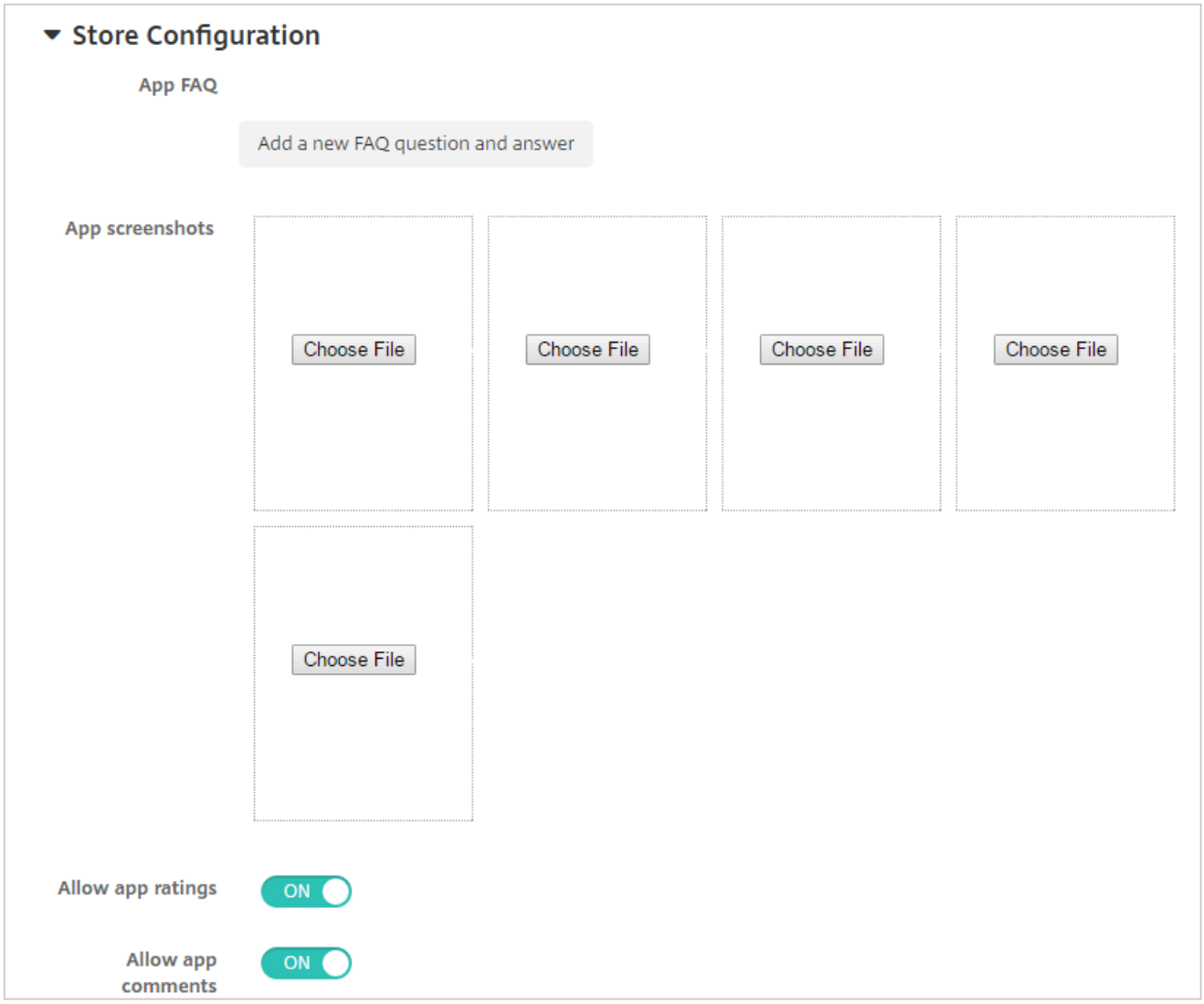
© 1999-2017 Citrix Systems, Inc. All rights reserved.



- 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 WiFi 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 WiFi internas**: se você tiver ativado a opção Requer WiFi, digite as redes WiFi internas a serem usadas.

6. Expanda **Configuração da XenMobile Store**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

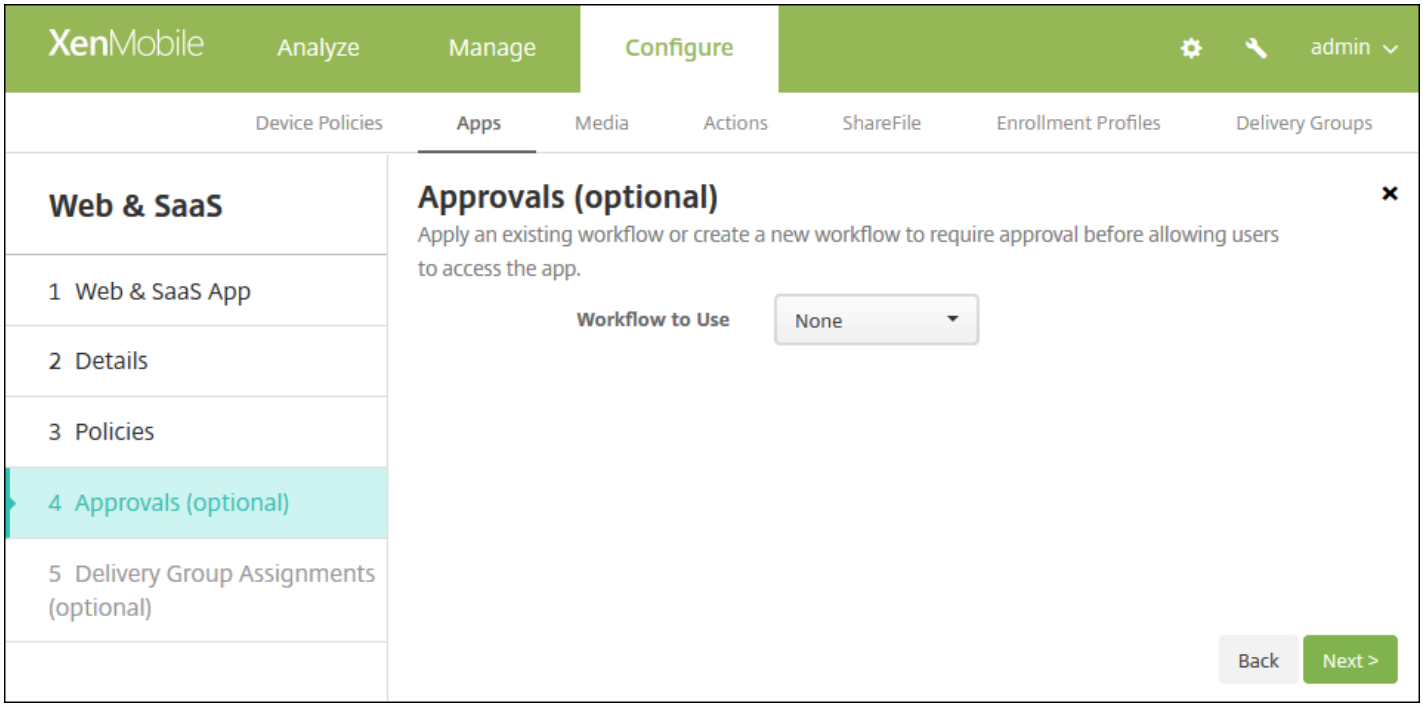


Opcionalmente, você pode adicionar ao aplicativo perguntas frequentes ou capturas de tela que são exibidas no XenMobile Store. Você também pode definir se os usuários podem classificar ou comentar no aplicativo.

- 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 XenMobile Store. 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**.

7. Clique em **Avançar**. A página **Aprovações** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Use fluxos de trabalho quando precisar de aprovação ao criar contas de usuário. Se você não precisar configurar fluxos de trabalho de aprovação, pule para a Etapa 8.

Configure estas definições se você precisar 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 a opção **Criar um novo fluxo de trabalho**, 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. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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 desejar remover.

8. Clique em **Avançar**. A página **Atribuição do grupo de entrega** é exibida.

9. 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**.

10. 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 de **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 se aplicará 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.

11. Clique em **Salvar**.

Acrescentar um aplicativo empresarial

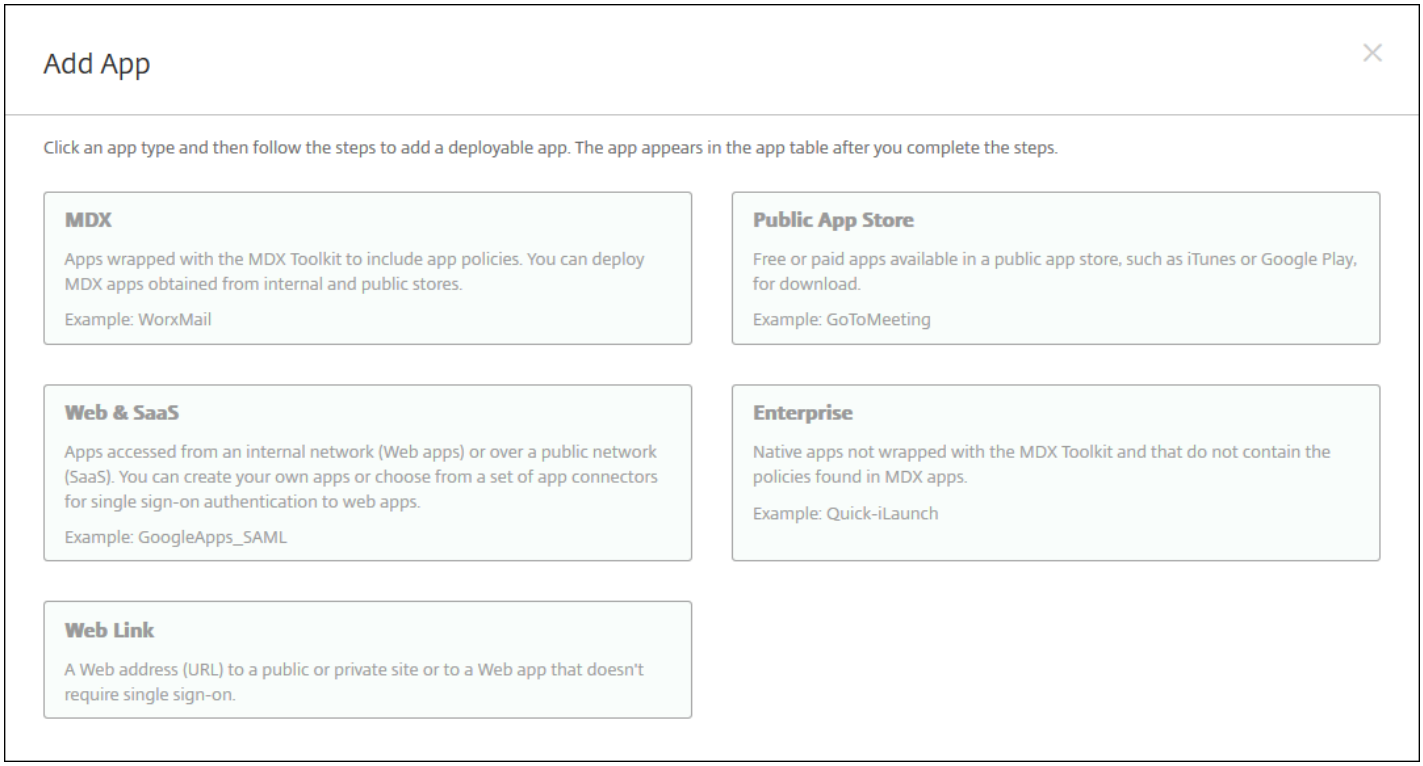
Os aplicativos empresariais no XenMobile representam aplicativos nativos que não são preparados com o MDX Toolkit e não contêm as políticas associadas a aplicativos do MDX. Você pode carregar um aplicativo empresarial na guia **Aplicativos** no console XenMobile. Os aplicativos empresariais são compatíveis com as seguintes plataformas (e tipos de arquivo correspondentes):

- iOS (arquivo .ipa)
- Android (arquivo .apk)
- Samsung KNOX (arquivo. apk)
- Android for Work (arquivo. apk)

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. Clique em **Empresarial**. A página **Informações do aplicativo** é exibida.

4. 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 Criar categorias de aplicativo.

5. Clique em **Avançar**. A página **Plataformas de aplicativo** é exibida.

6. Em **Plataformas**, selecione as plataformas que você desejar adicionar. Se você estiver configurando somente para uma única plataforma, desmarque as outras.

Quando terminar de definir as configurações de uma plataforma, consulte a Etapa 10 para saber como definir as regras de implantação dessa plataforma.

7. Para cada plataforma que você selecionou, selecione o arquivo a ser carregado clicando em **Procurar** e navegando até a localização do arquivo.

8. Clique em **Avançar**. A página de informações do aplicativo da plataforma é exibida.

9. 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

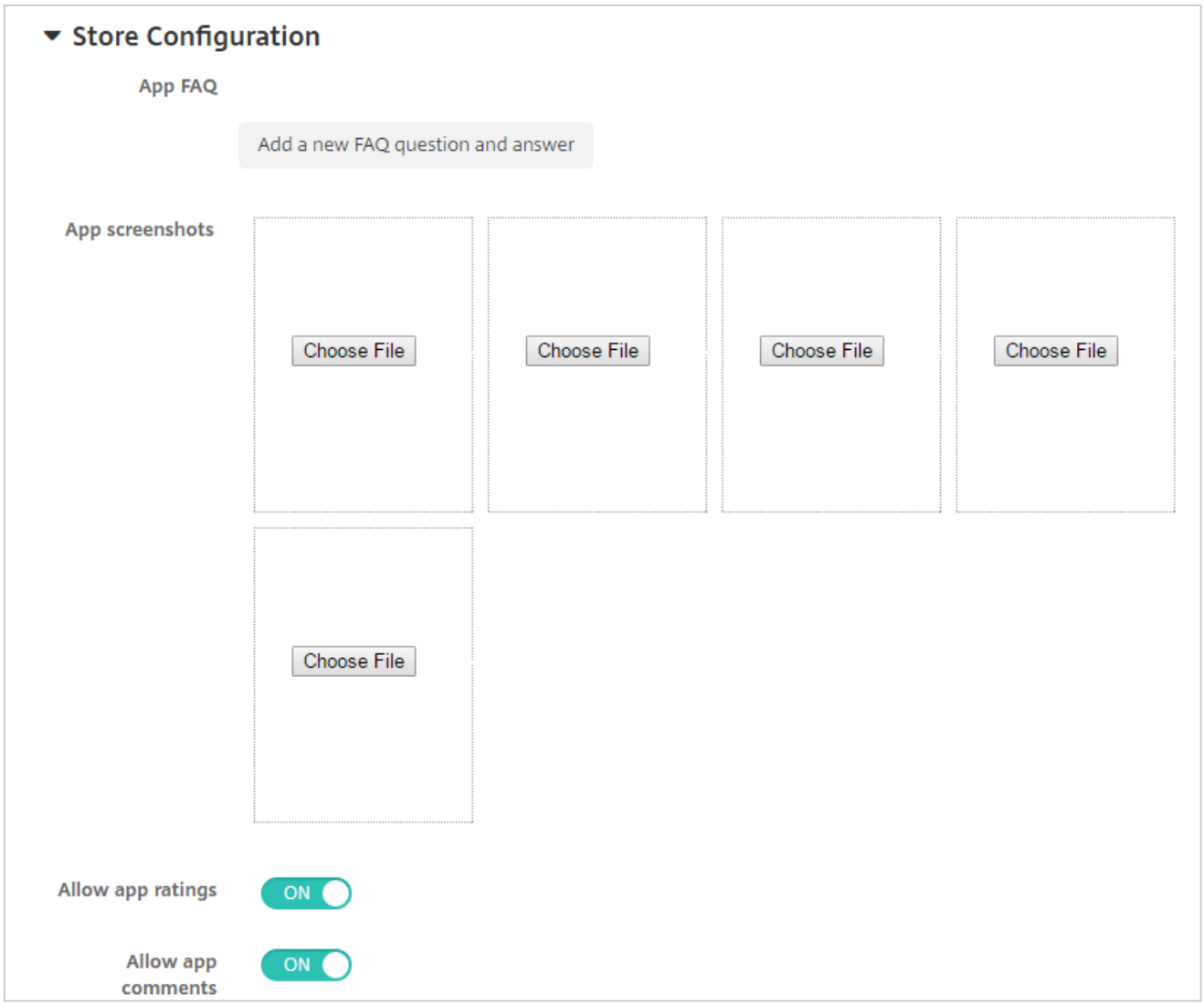
© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 **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**.
- **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. Essa configuração se aplica aos dispositivos iOS 9.x.

10. Configure as regras de implantação. Para obter informações, consulte Implantar recursos.

11. Expanda **Configuração da XenMobile Store**.



Opcionalmente, você pode adicionar ao aplicativo perguntas frequentes ou capturas de tela que são exibidas no XenMobile Store. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Instantâneos do aplicativo**: adicione capturas de tela para ajudar a classificar o aplicativo na XenMobile Store. 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**.

12. Clique em **Avançar**. A página **Aprovações** é exibida.

Use fluxos de trabalho quando precisar de aprovação ao criar contas de usuário. Se você não precisar configurar fluxos de trabalho de aprovação, pule para a Etapa 13.

Configure estas definições se você precisar 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 a opção **Criar um novo fluxo de trabalho**, 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. 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 desejar remover.

13. Clique em **Avançar**. A página **Atribuição do 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 na lista. 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:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Ao lado de **Implantar**, clique em **I** para agendar a implantação ou em **O** para impedi-la. A opção padrão é **I**.
- Ao lado de **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 se aplicará 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.

16. Clique em **Salvar**.

Adicionar um link da Web

No XenMobile, você pode estabelecer um endereço da Web (URL) para um site público ou privado ou para um aplicativo Web que não requer logon único (SSO).

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.

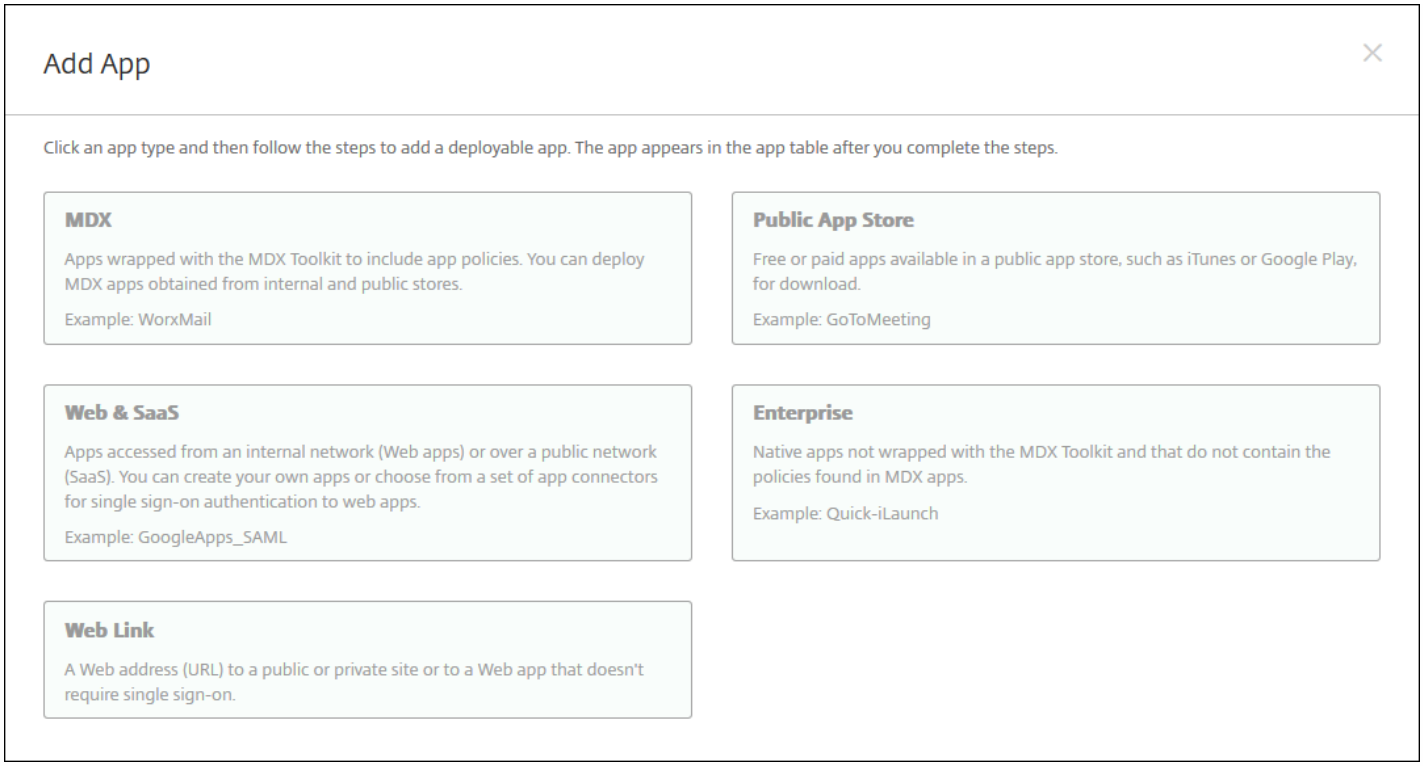
Para adicionar o link, forneça as seguintes informações:

- 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**. A página **Aplicativos** é exibida.

2. Clique em **Adicionar**. A caixa de diálogo **Adicionar aplicativo** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



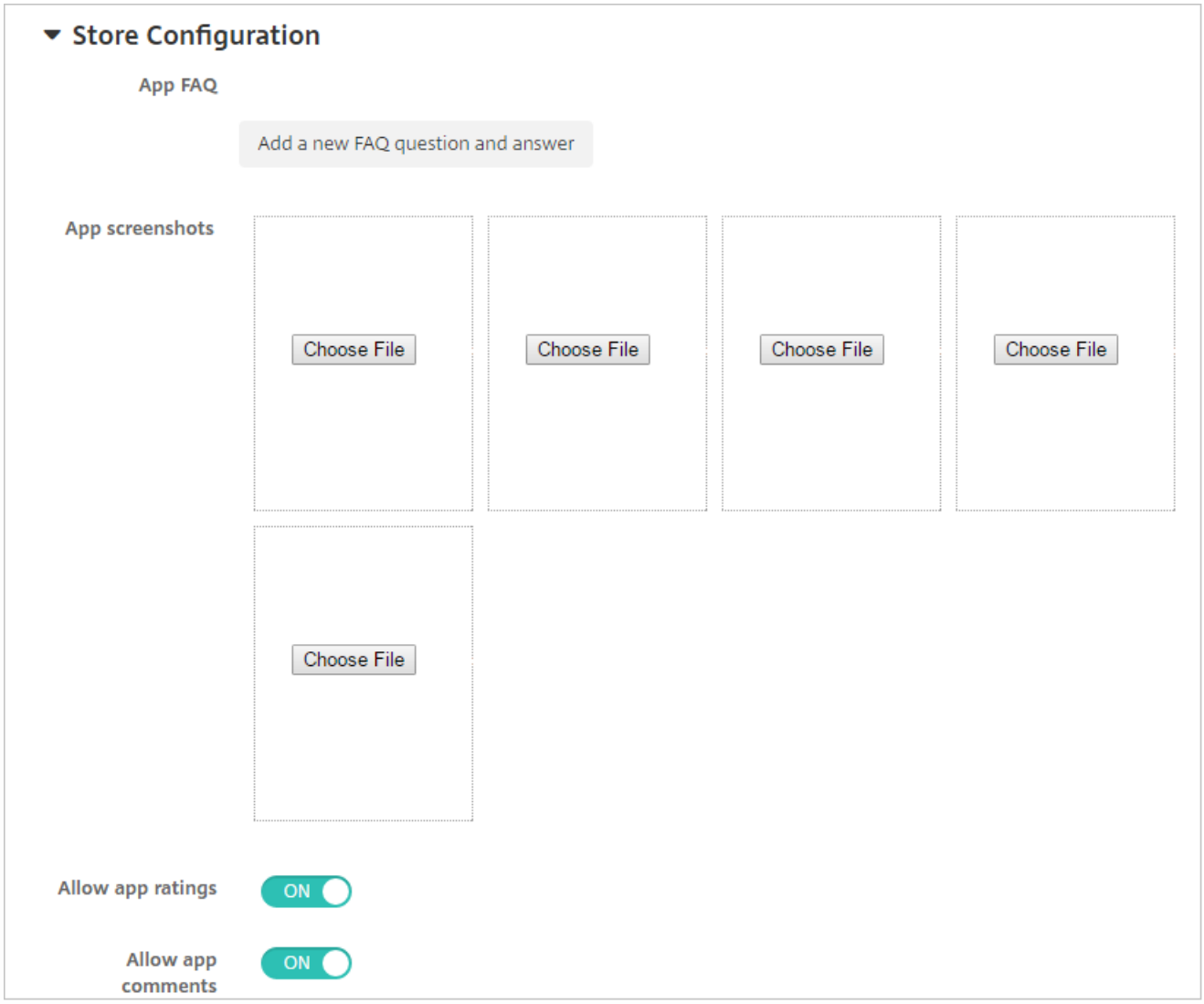
3. Clique em **Link da Web**. A página **Informações do aplicativo** é exibida.

4. 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 o URL preenchido 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 NetScaler Gateway. Definir essa opção como **I** adiciona a palavra-chave VPN ao aplicativo e permite que os usuários se conectem por meio do NetScaler 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 imagem do próprio aplicativo deve ser carregada. O padrão é Usar padrão.
  - Se quiser carregar sua própria imagem, selecione-a clicando em **Procurar** e navegando até a localização 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.

5. Expanda **Configuração da XenMobile Store**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Opcionalmente, você pode adicionar ao aplicativo perguntas frequentes ou capturas de tela que são exibidas no XenMobile Store. 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 XenMobile Store. 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**.

6. Clique em **Avançar**. A página **Atribuição do grupo de entrega** é exibida.

7. Ao lado de **Escolher grupos de entrega**, digite para localizar um grupo de entrega ou selecione um ou mais grupos na lista. Os grupos que você selecionar aparecerão na lista **Grupos de entrega que receberão a atribuição de aplicativos**.

8. 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 de **Cronograma de implantação**, clique em **Agora** ou em **Mais tarde**. A opção padrão é **Agora**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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 se aplicará 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.

9. 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 ShareFile transfiram documentos e dados para aplicativos do Microsoft Office 365. Para obter detalhes, consulte Ativar a interação segura com o Office 365.

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:

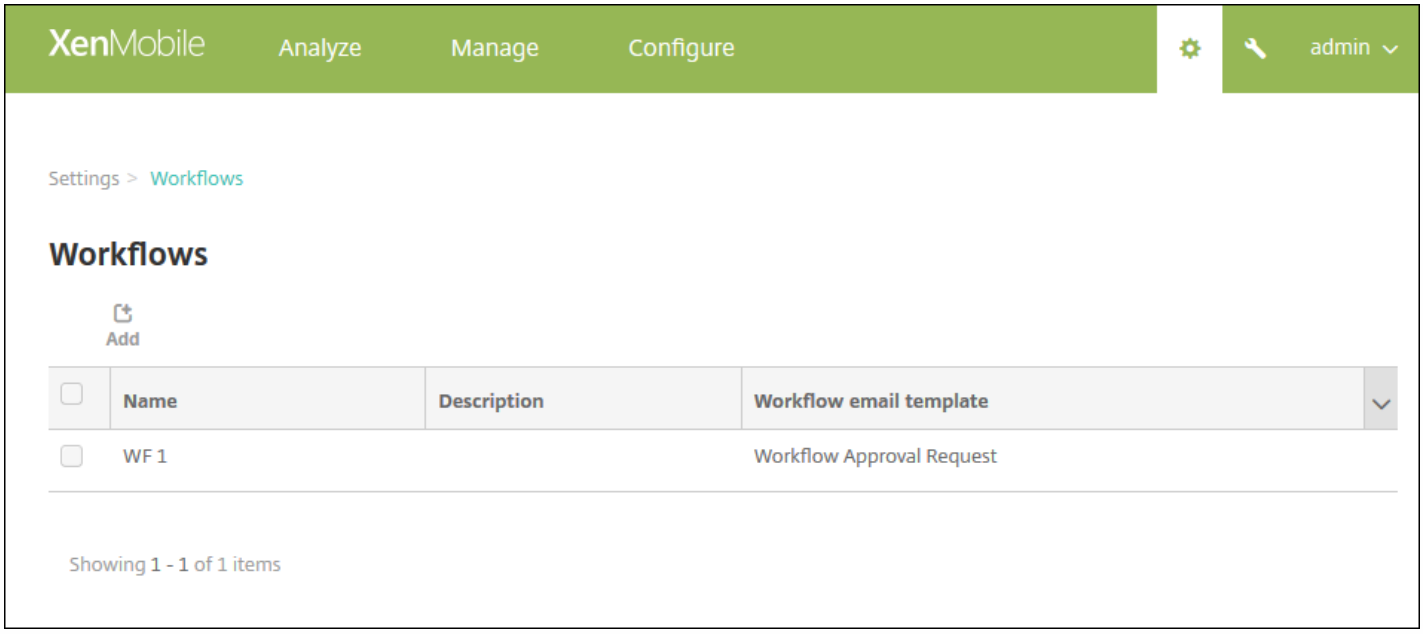
- Na página Fluxos de trabalho no console XenMobile. Na página Fluxos de trabalho, você pode configurar vários fluxos de trabalho para serem usados com as configurações do aplicativo. Ao configurar fluxos de trabalho na página Fluxos de trabalho, você pode selecionar o fluxo de trabalho durante a configuração 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.

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 pessoas por 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 **Configurações** é exibida.

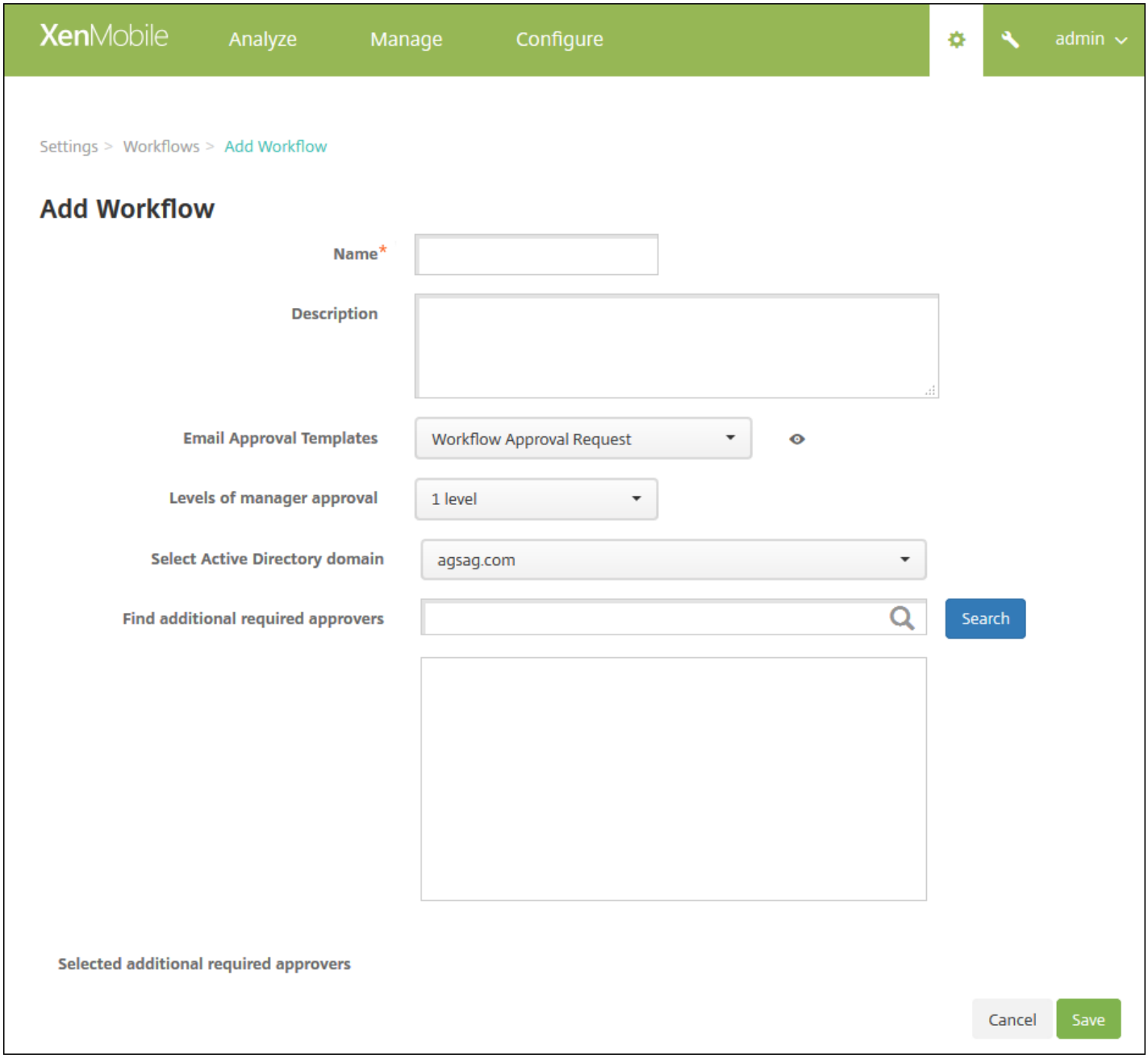
2. Clique em **Fluxos de trabalho**. A página **Fluxos de trabalho** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. Clique em **Adicionar**. A página **Adicionar fluxo de trabalho** é exibida.

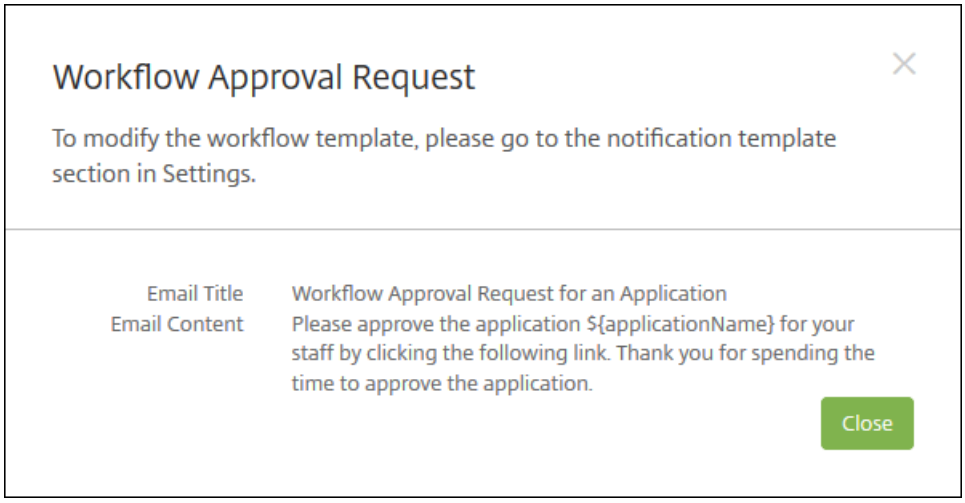
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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, a caixa de diálogo abaixo é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- **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 desejar 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, deverá criar outro fluxo de trabalho.

Para exibir os detalhes e excluir um fluxo de trabalho

1. Na página **Fluxos de trabalho**, selecione um fluxo de trabalho clicando na linha da tabela ou marcando 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Tipos de conector de aplicativo

Feb 21, 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		**Observação**: 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Atualizar aplicativos MDX ou empresariais

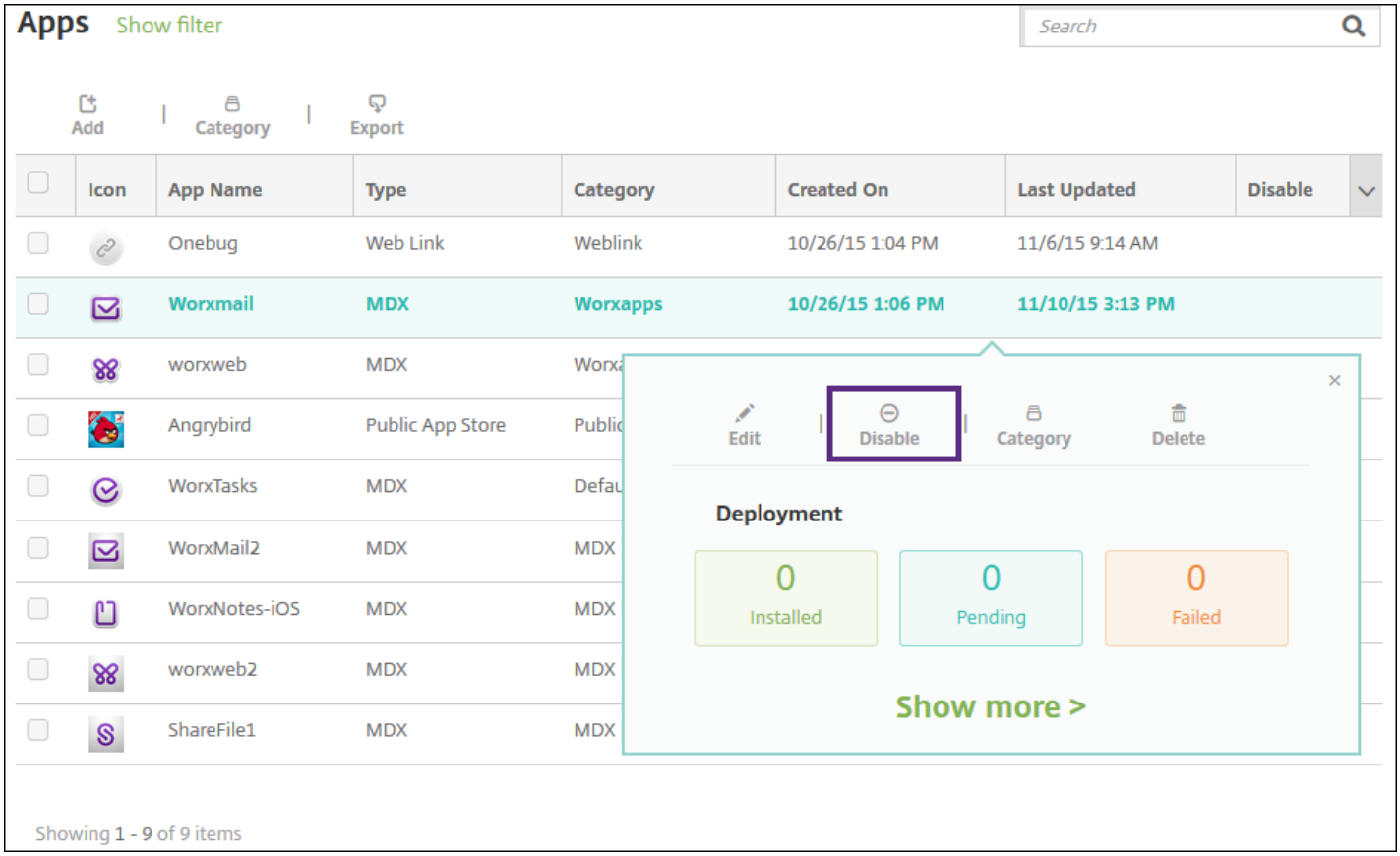
Feb 21, 2018

Para atualizar um aplicativo MDX ou Empresarial no XenMobile, desative o aplicativo no console do XenMobile e carregue a nova versão do aplicativo.

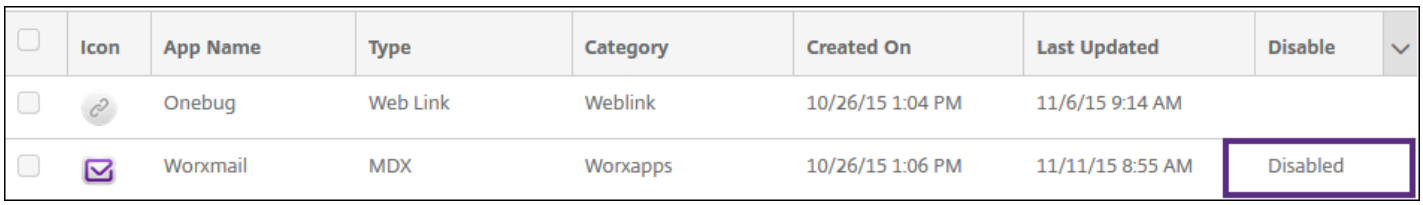
1. No console XenMobile, clique em **Configurar > Aplicativos**. A página **Aplicativos** é exibida.

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:

- Na tabela **Aplicativos**, marque a caixa de seleção ao lado do aplicativo ou clique na linha que contém o aplicativo que você deseja atualizar.
- Clique em **Desativar** no menu exibido.



- Clique em **Desativar** na caixa de diálogo de confirmação. *Desativado* é exibido na coluna **Desativar** do aplicativo.



Nota: desativar um aplicativo coloca o aplicativo no modo de manutenção. Enquanto o aplicativo está desativado, os usuários não podem se reconectar ao aplicativo depois que fazem logoff. Desativar um aplicativo é uma configuração

© 1999-2017 Citrix Systems, Inc. All rights reserved.

opcional, mas recomendamos desativar o aplicativo para evitar problemas com a funcionalidade dele. Os problemas podem resultar de atualizações da política, por exemplo, ou quando os usuários solicitam um download ao mesmo tempo que você está carregando o arquivo para o XenMobile.

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 originalmente escolheu 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:

- 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.
- Opcionalmente, altere os detalhes de aplicativo e as configurações de política para a plataforma.
- 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:

- Na tabela **Aplicativos**, clique para selecionar o aplicativo atualizado e, no menu exibido, clique em **Ativar**.
- 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Resumo das políticas de aplicativos MDX

Mar 16, 2018

Para obter uma tabela que lista as políticas de aplicativos MDX para iOS e Android com anotações sobre restrições e recomendações da Citrix, consulte Resumo das políticas de aplicativos MDX na documentação do MDX Toolkit.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Identidade visual do XenMobile Store e do Citrix Secure Hub

Feb 21, 2018

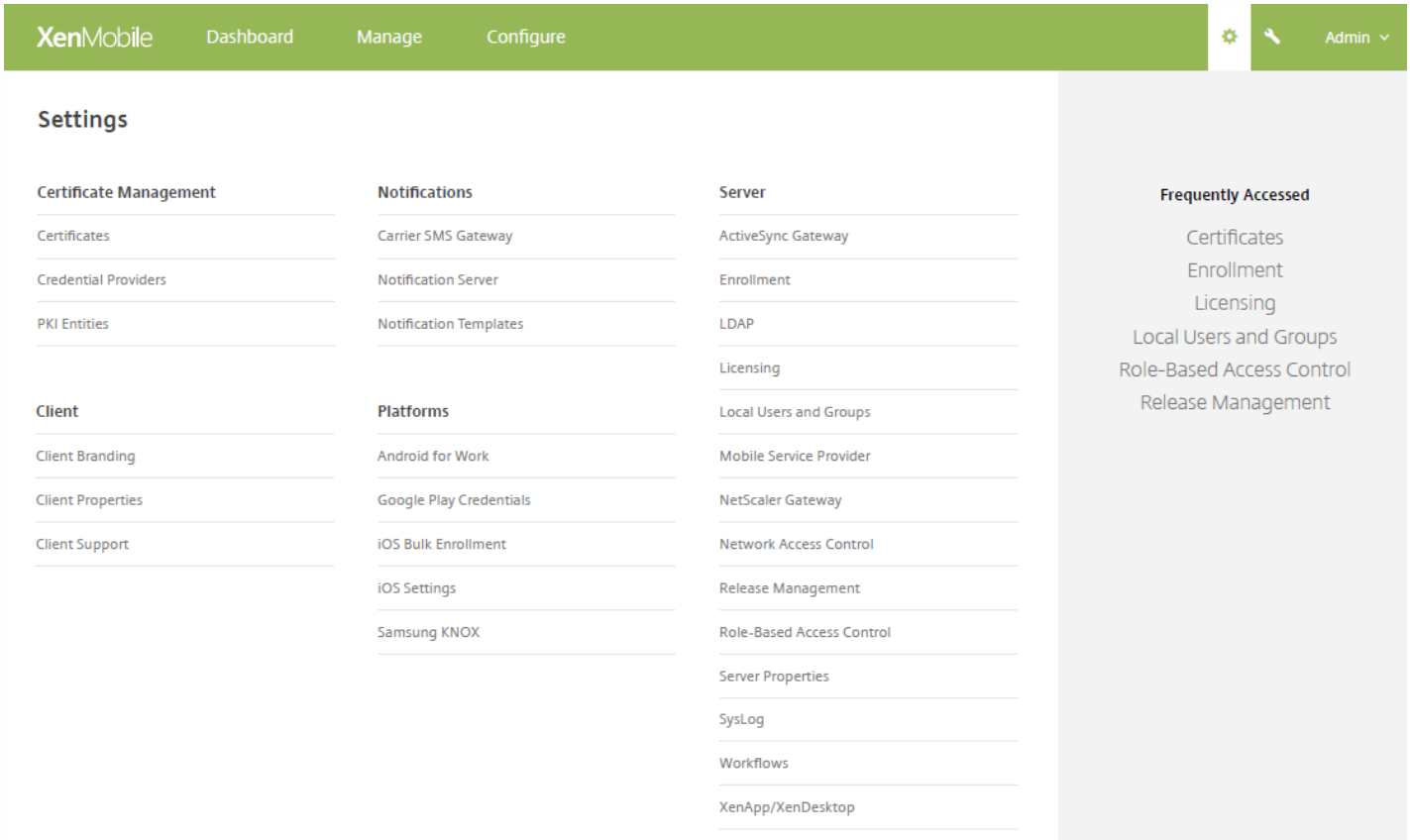
Você pode definir a forma como os aplicativos aparecem na loja e adicionar um logotipo para identificar o Secure Hub e a XenMobile Store. Esses recursos de identidade visual estão disponíveis para dispositivos iOS e Android.

Nota: antes de começar, verifique se a imagem personalizada está pronta e acessível.

A imagem personalizada deve atender a estes requisitos:

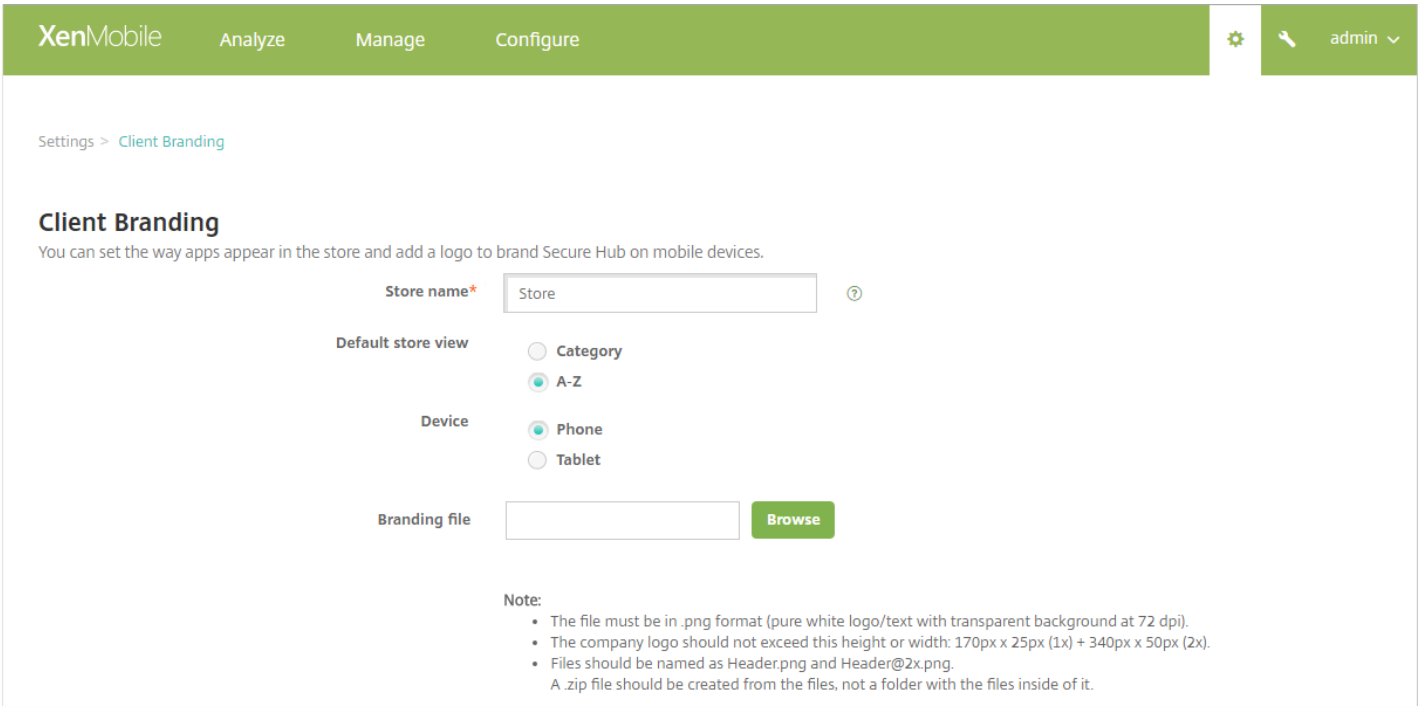
- O arquivo deve estar no formato .png
- Use um logotipo em branco puro ou texto com um fundo transparente em 72 ppp.
- O logotipo da empresa não deve exceder esta altura ou largura: 170 pixels x 25 pixels (1x) e 340 pixels x 50 pixels (2x).
- Dê os seguintes nomes aos arquivos: Header.png e Header@2x.png.
- Crie um arquivo .zip com os arquivos, não uma pasta que contenha os arquivos.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida.



2. Em **Cliente**, clique em **Identidade visual do cliente**. A página **Identidade visual do cliente** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Faça as seguintes configurações:

- **Nome do armazenamento**: o nome do armazenamento será exibido nas informações de conta do usuário. Alterar o nome também altera a URL usada para acessar os serviços de armazenamento. Geralmente, não é necessário alterar o nome padrão.
- **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**.

Para implantar este pacote nos dispositivos dos usuários, você precisa criar um pacote de implantação e implantar o pacote nos dispositivos dos usuários.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix Launcher

Feb 21, 2018

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. Você pode adicionar a **Política de configuração do Launcher** para controlar esses recursos do Citrix Launcher:

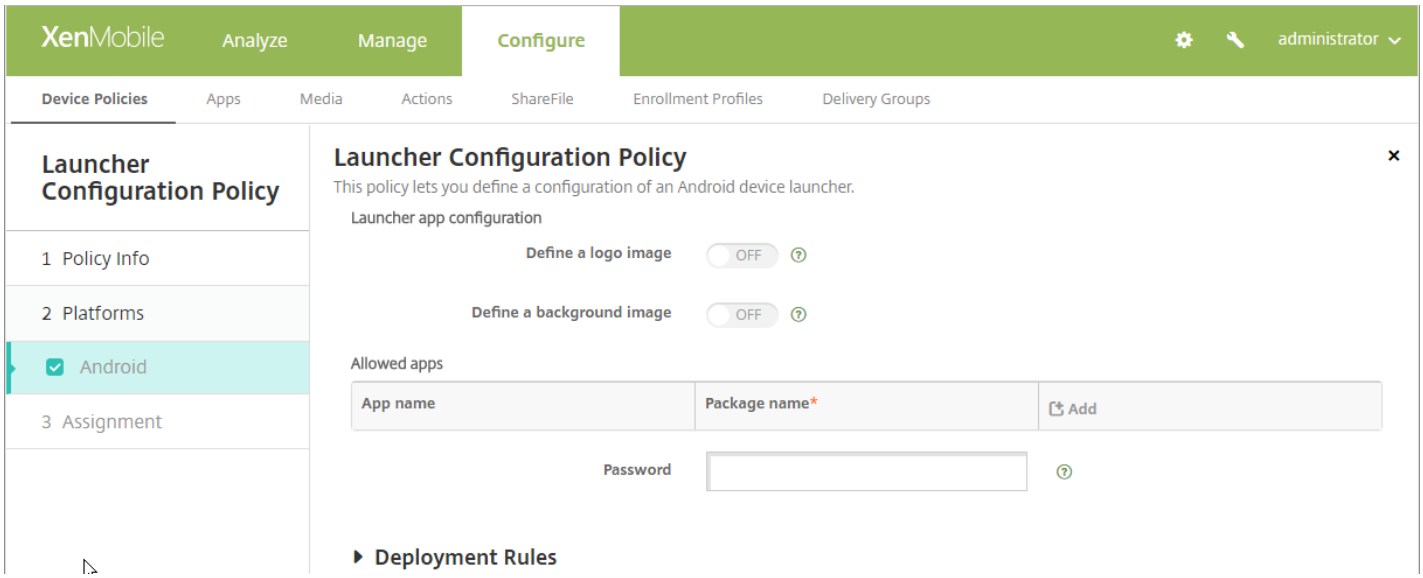
- Gerenciar dispositivos Android para que os usuários possam acessar somente os aplicativos que você especificar.
- Opcionalmente, especifique uma imagem de logotipo personalizado para o ícone do Citrix Launcher e uma imagem de plano de fundo personalizado para o Citrix Launcher.
- Especifique uma senha 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.

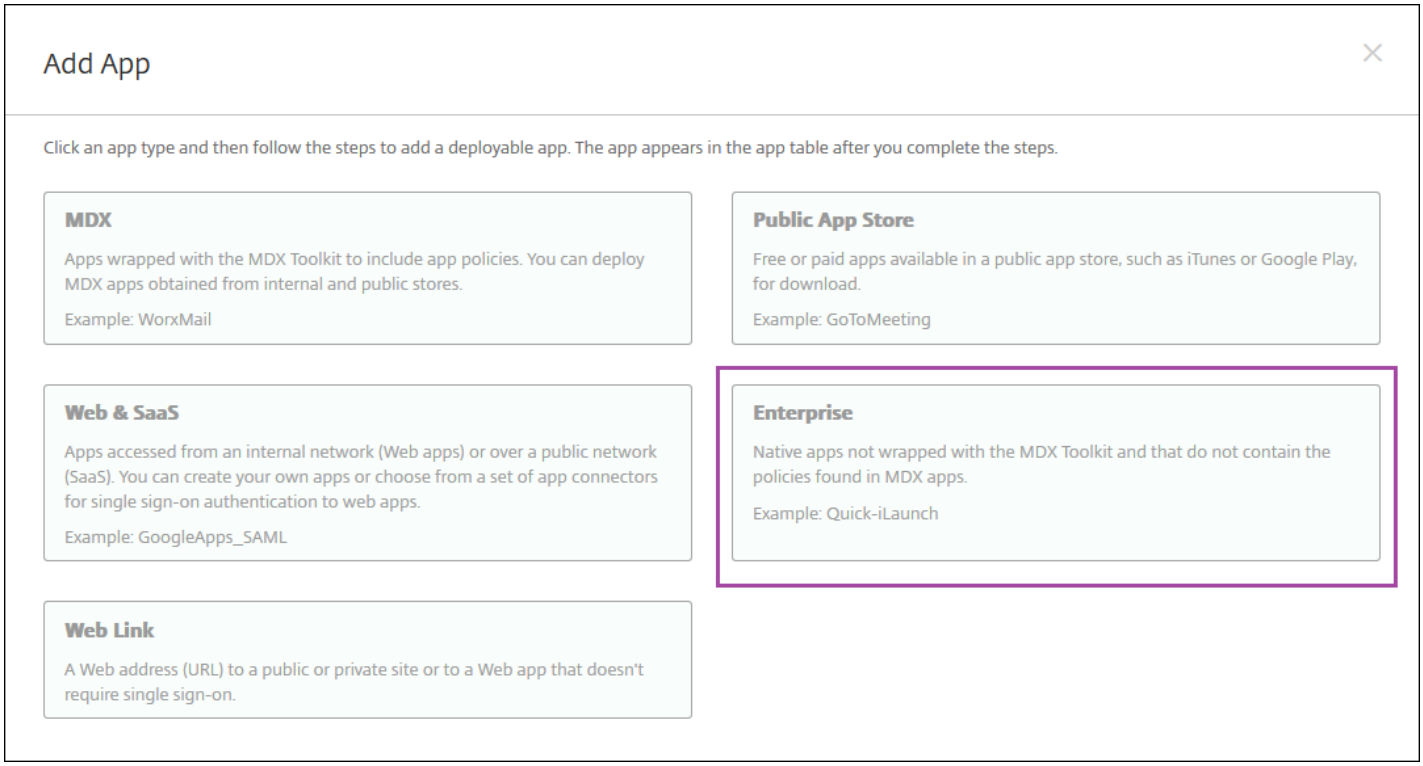
1. Baixe o aplicativo Citrix Launcher da página de downloads do XenMobile para obter sua edição do XenMobile. O nome do arquivo é CitrixLauncher.apk. O arquivo está pronto para carregar no XenMobile e não requer preparação.

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.



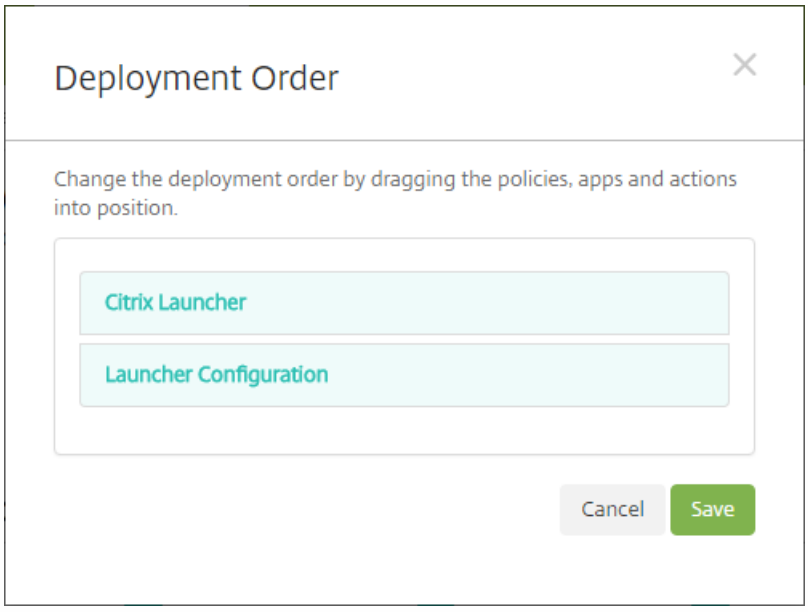
3. Adicione o aplicativo Citrix Launcher ao XenMobile como um aplicativo corporativo. Em **Configurar > Aplicativos**, clique em **Adicionar** e, em seguida, clique em **Empresarial**. Para obter mais informações, consulte Adicionar um aplicativo empresarial.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Volume Purchase Plan do iOS

Feb 21, 2018

Você pode gerenciar o licenciamento de aplicativos iOS usando o Apple iOS Volume Purchase Program (VPP). O VPP simplifica o processo para localizar, comprar e distribuir aplicativos e outros dados em massa para uma organização.

Com VPP, você pode usar o XenMobile para distribuir aplicativos de loja de aplicativos pública. Não há suporte para VPP para XenMobile Apps ou para aplicativos preparados por meio do MDX Toolkit. Embora você possa distribuir os aplicativos de loja pública do XenMobile com o VPP, a implantação não é otimizada. São necessários mais melhorias no XenMobile Server e no armazenamento do Secure Hub para resolver as limitações. Para obter uma lista de problemas conhecidos com a implantação do XenMobile aplicativos de loja pública por meio de VPP e possíveis soluções alternativas, consulte este artigo do knowledge center da Citrix.

Com VPP, 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 do VPP do iOS no XenMobile.

O XenMobile reimporta periodicamente as licenças do VPP da Apple para garantir que elas reflitam todas as alterações. Essas alterações incluem quando você exclui manualmente um aplicativo importado do VPP. Por padrão, o XenMobile atualiza a linha de base da licença do VPP no mínimo a cada 720 minutos. Você pode alterar o intervalo de linha de base por meio da propriedade de servidor, intervalo de linha de base do VPP (vpp.baseline). Para obter instruções, consulte Propriedades do servidor.

Este artigo aborda usando VPP com licenças gerenciadas, o que permite que você usar o XenMobile para distribuir aplicativos. Se você atualmente usa códigos de resgate e deseja mudar para distribuição gerenciada, consulte este documento do Suporte Apple: Migrar de códigos de resgate para distribuição gerenciada com o Programa de compras por volume.

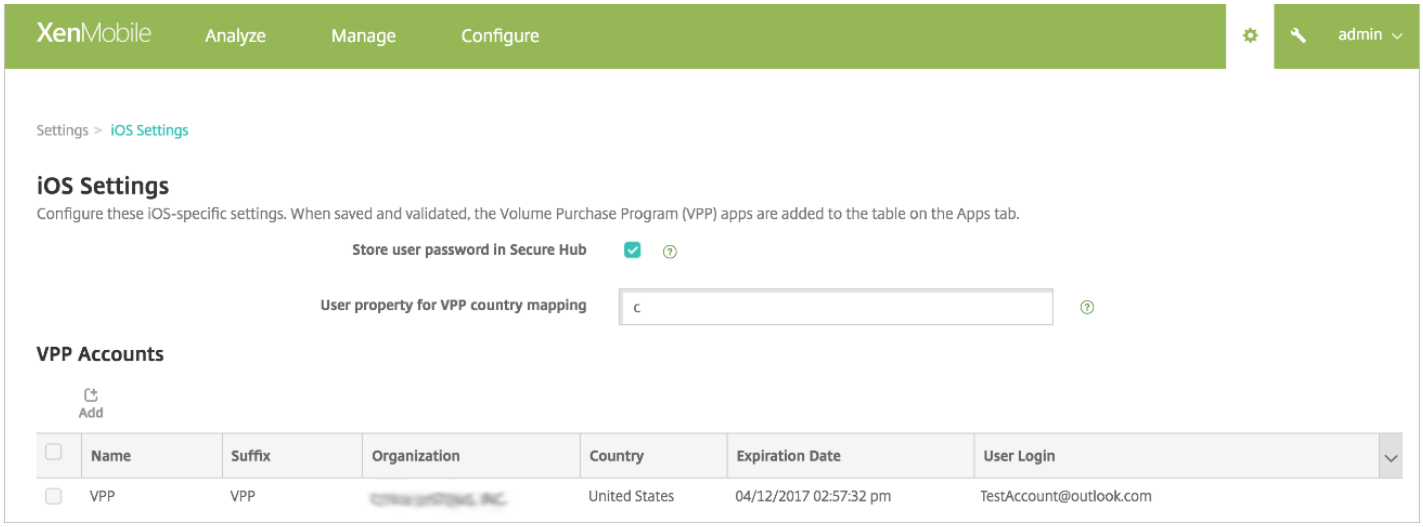
Para obter informações sobre o VPP do iOS, consulte http://www.apple.com/business/vpp/. Para se registrar no VPP, vá para https://deploy.apple.com/qforms/open/register/index/avs . Para acessar o armazenamento de VPP no iTunes, vá para https://vpp.itunes.apple.com/?l=en .

Depois que você salva as configurações de VPP 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 **Configurações** é exibida.

2. Em **Plataforma**, clique em **Configurações de iOS**. A página de configuração **Configurações de iOS** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



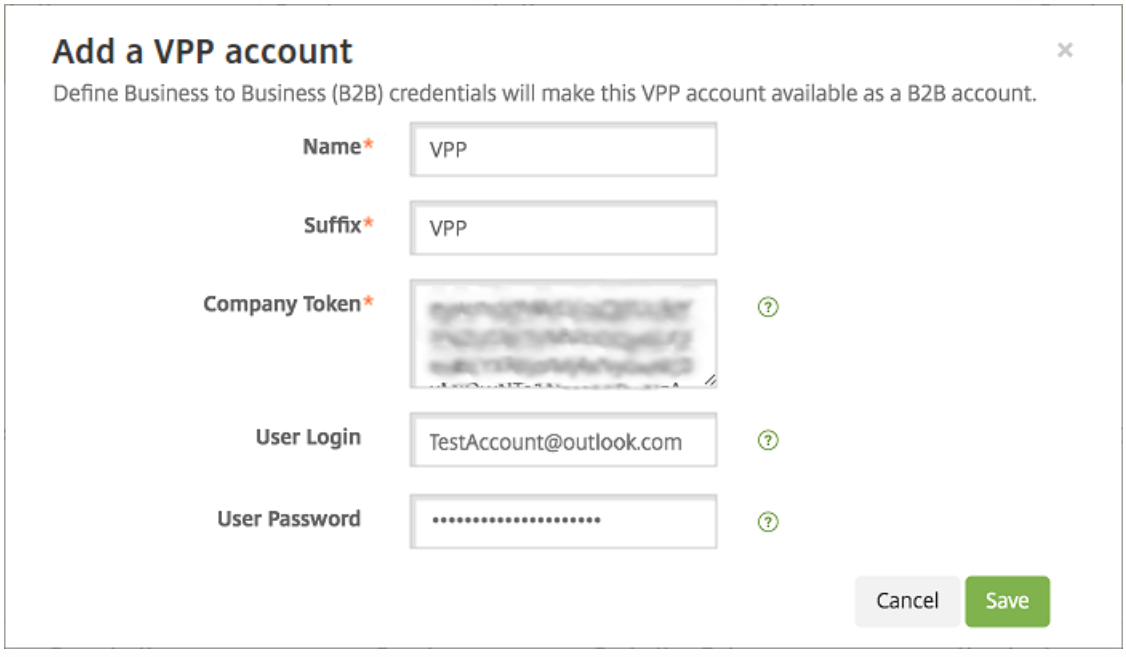
3. Defina estas configurações:

- **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 de usuário para mapeamento de país do VPP**: 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 do VPP. Por exemplo, se a propriedade do usuário for Estados Unidos, ele não poderá baixar aplicativos se o código VPP do aplicativo for para o Reino Unido. Contate o administrador do plano VPP para obter mais informações sobre o código de mapeamento do país.

Contas VPP

- Para cada conta VPP que você desejar adicionar, clique em **Adicionar**. A caixa de diálogo **Adicionar uma conta VPP** é exibida.



Defina estas configurações para cada conta que você adicionar:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nota: Se você estiver usando o Apple Configurator 1, carregue um arquivo de licença da seguinte maneira: vá até **Configurar > aplicativos**, vá para uma página da plataforma e expanda **Programa de Compra por Volume**.

- **Nome**: Digite o nome da conta VPP.
- **Sufixo**: Digite o sufixo a ser exibido com os nomes dos aplicativos obtidos usando a conta VPP. Por exemplo, se você inserir **VPP**, o aplicativo Secure Mail é exibido na lista de aplicativos, como **Secure Mail - VPP**.
- **Token da empresa**: Digite ou copie e cole o token de serviço de VPP obtido da Apple. Para obter o token: Na página **Resumo da conta** do portal do Apple VPP, clique no botão **Baixr** para gerar e baixar o arquivo de VPP. 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 VPP autorizada usado para importar aplicativos B2B personalizados.
- **Senha de usuário**: Digite a senha de administrador de conta de VPP.

5. Clique em **Salvar** para fechar a caixa de diálogo.

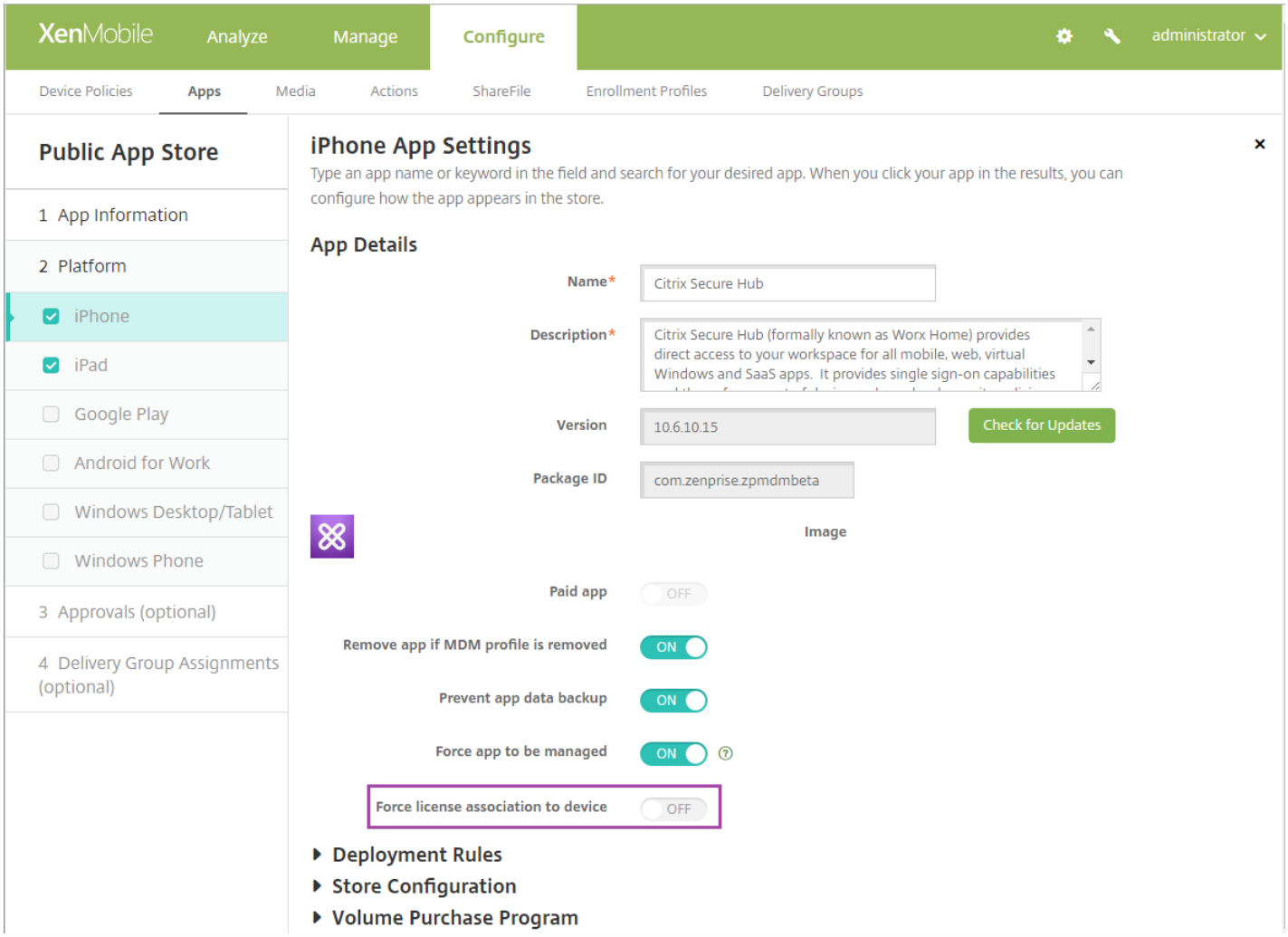
6. Clique em **Salvar** para salvar as configurações do iOS.

É exibida uma mensagem que informa que o XenMobile adiciona os aplicativos à página **Configurar > Aplicativos**. Naquela página, observe que os nomes dos aplicativos da sua conta do VPP contêm o sufixo que você forneceu na configuração acima.

Você pode agora definir as configurações de aplicativo VPP e, em seguida, ajustar as entrega grupo e o dispositivo as configurações de política para aplicativos VPP. Depois de concluir essas configurações, os usuários podem registrar seus dispositivos. A seguir indica fornecem considerações para esses processos.

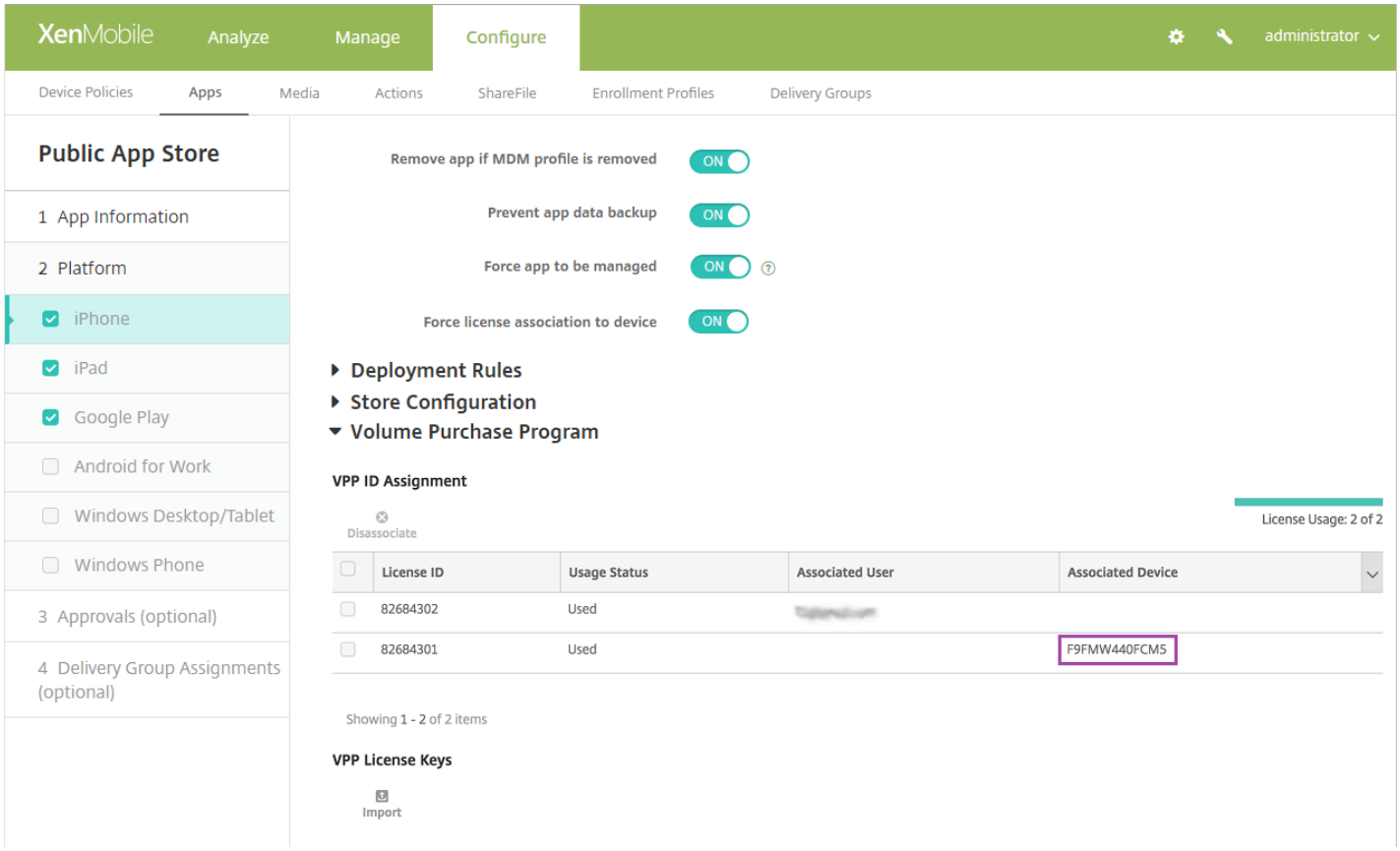
- Ao definir as configurações de aplicativo VPP (**Configurar > Aplicativos**), ativar **Forçar associação de licença ao dispositivo** . Uma vantagem de usar o Apple VPP e DEP com dispositivos supervisionados: a capacidade de usar o XenMobile para atribuir o aplicativo no nível de dispositivo (em vez de usuário). Desse modo, você não precisa usar um dispositivo com Apple ID. Além disso, os usuários não recebem um convite para participar do programa VPP. Os usuários também podem baixar aplicativos sem entrar na respectiva conta do iTunes.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



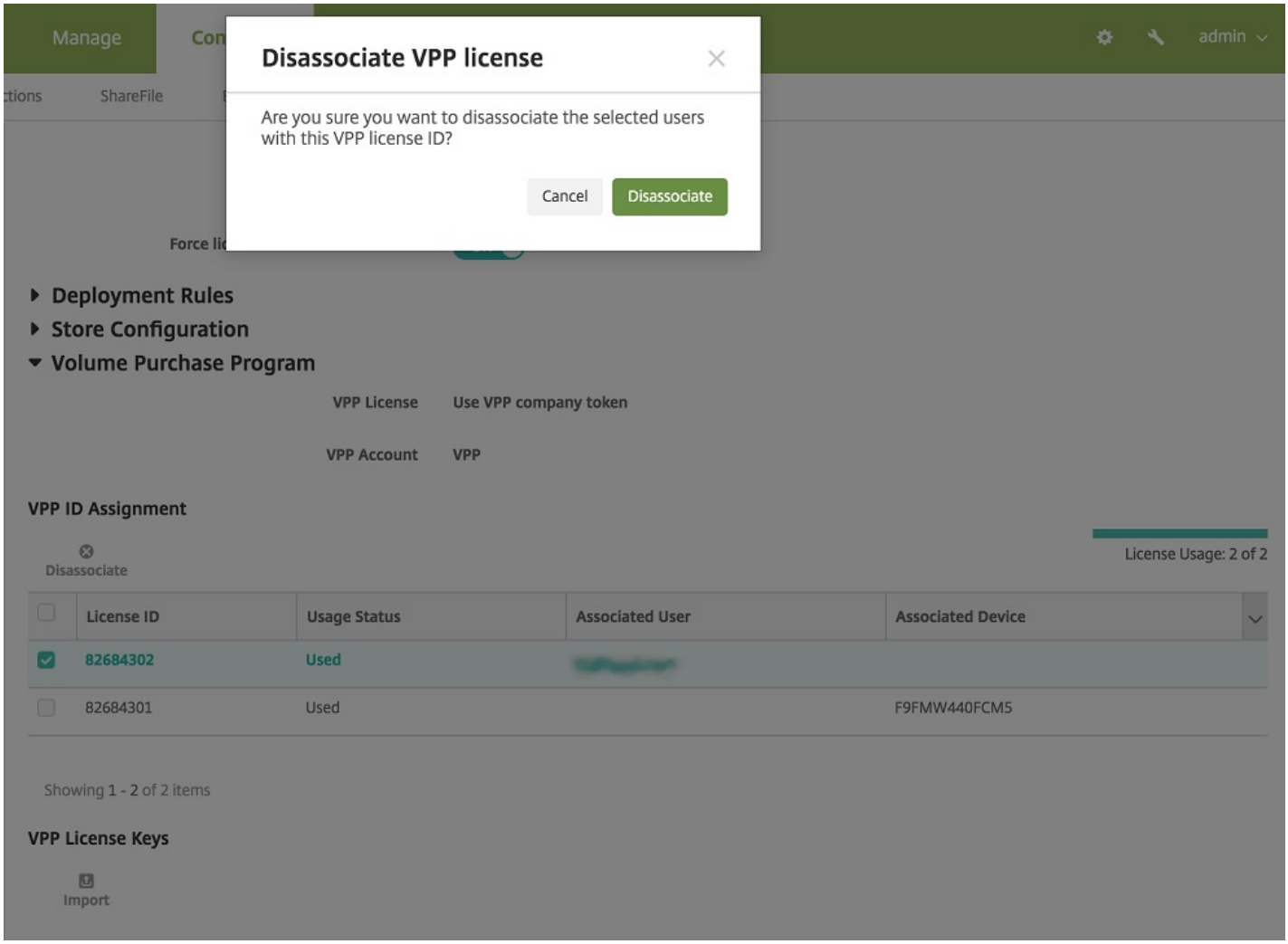
Para exibir as informações VPP para esse aplicativo, expanda **Programa de Compra por Volume**. Na tabela **Atribuição de ID de VPP**, note que a licença é associada a um dispositivo. O número de série do dispositivo é exibido na **Dispositivo associado** coluna. Se o usuário remove o token e, em seguida, importa-o novamente, a palavra **Oculto** é exibida em vez do número de série, devido a restrições de privacidade da Apple.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



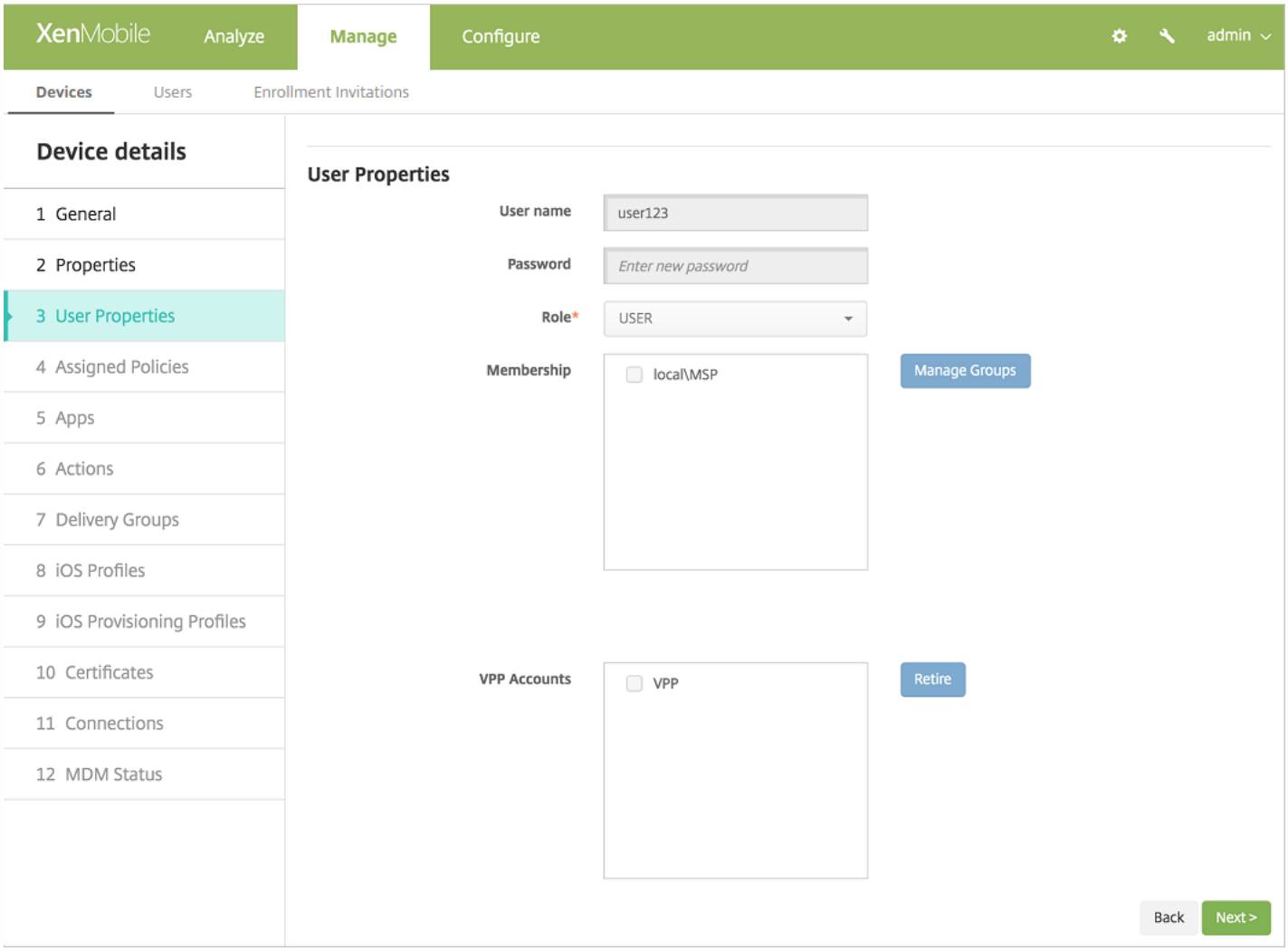
Para desassociar uma licença, clique na linha da licença e clique em **Desassociar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



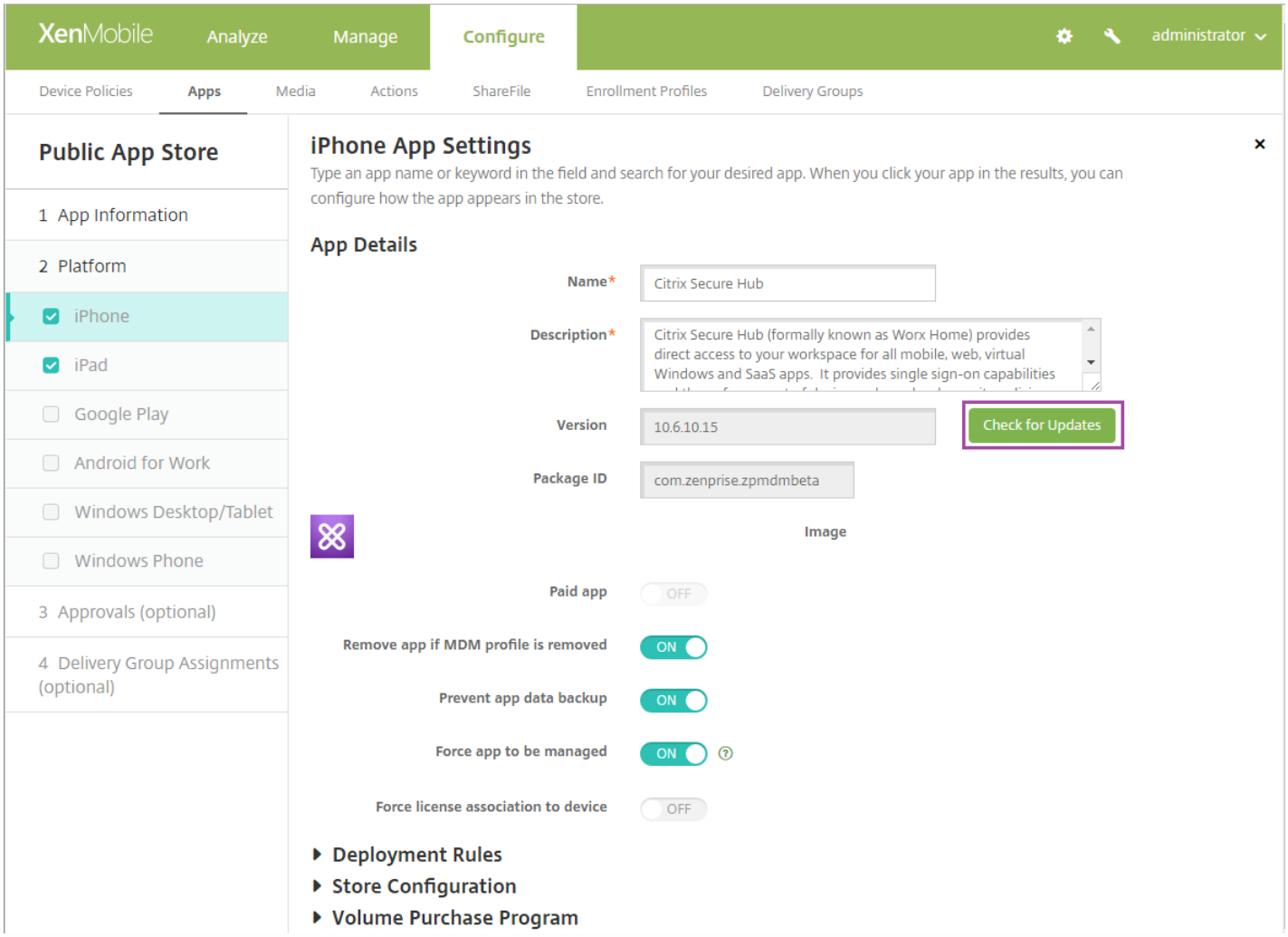
Se você associar licenças de VPP usuários, XenMobile integra os usuários em sua conta VPP e associa sua ID do iTunes com a conta VPP. A ID do iTunes dos usuários nunca é visível para a sua empresa para o XenMobile Server. Apple transparente cria a associação para manter a privacidade do usuário. Você pode desativar um usuário do programa VPP, para desassociar a todas as licenças da conta de usuário. Para desativar um usuário, vá para **Gerenciar > Dispositivos** .

© 1999-2017 Citrix Systems, Inc. All rights reserved.

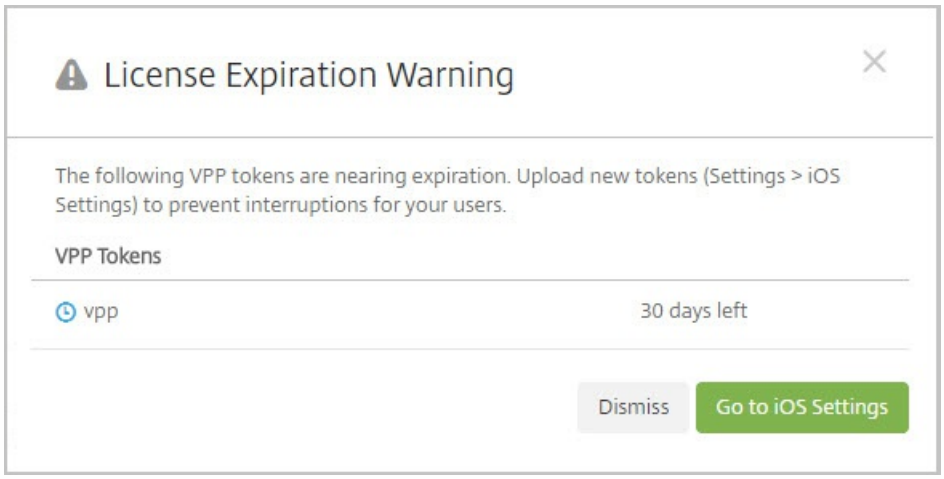


- Quando você atribuir um aplicativo a um grupo de entrega, como padrão, o XenMobile identifica o aplicativo como um aplicativo opcional. Para garantir que o XenMobile implante um aplicativo para dispositivos, vá até **Configurar > Grupos de entrega.** Na página **Aplicativos**, mova o aplicativo para a lista **Aplicativos obrigatórios**.
- Quando uma atualização de um aplicativo de loja de aplicativos pública está disponível: quando o VPP envia o aplicativo, o aplicativo não é atualizado automaticamente nos dispositivos até que você verifique se há atualizações e as aplique. Para enviar uma atualização para o Secure Hub quando atribuídas ao 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



O XenMobile exibe um Aviso de Expiração de Licença quando os tokens Apple VPP estão prestes a expirar ou expiraram.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenApp e XenDesktop através do Citrix Secure Hub

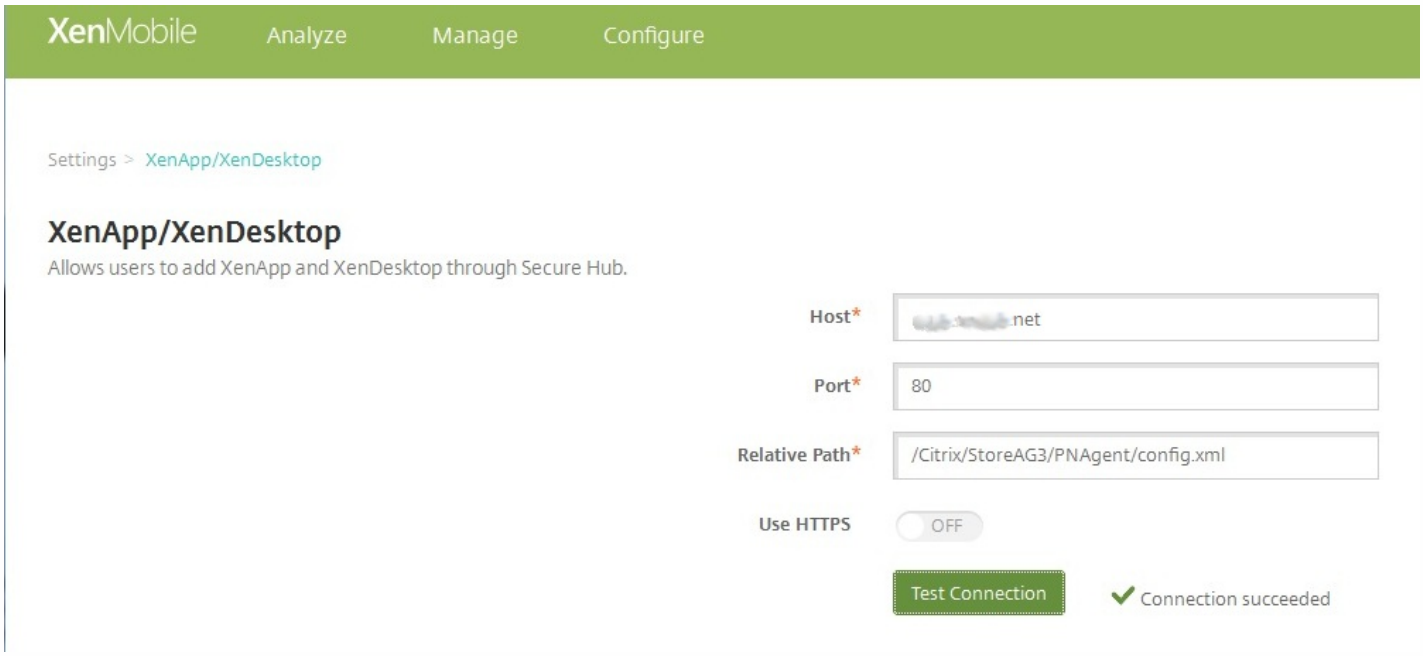
Feb 21, 2018

O XenMobile pode coletar aplicativos do XenApp e do XenDesktop 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 dos usuários 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 **Configurações** é exibida.

2. Clique em **XenApp/XenDesktop**. A página **XenApp/XenDesktop** é exibida.



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 XenApp e ao XenDesktop Server especificado.

5. Clique em **Salvar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Uso do ShareFile com o XenMobile

Mar 08, 2018

O XenMobile tem duas opções para integração com o ShareFile: ShareFile Enterprise e StorageZone Connectors. A integração com o ShareFile Enterprise ou com os StorageZone Connectors requer o XenMobile Enterprise Edition.

ShareFile Enterprise

Se você tem o XenMobile Enterprise Edition, pode configurar o XenMobile para fornecer acesso à sua conta do ShareFile Enterprise. Essa configuração:

- Permite que usuários móveis acessem o conjunto completo de recursos do ShareFile, como StorageZone Connectors, sincronização de arquivos e compartilhamento de arquivos.
- Pode fornecer ao ShareFile autenticação de logon único de usuários de XenMobile Apps, provisionamento de contas de usuário com base no AD e políticas abrangentes de controle de acesso.
- Fornece configuração, monitoramento de nível de serviço e monitoramento do uso de licenças do ShareFile por meio do console XenMobile.

Para obter mais informações sobre como configurar o XenMobile para o ShareFile Enterprise, consulte SAML para logon único com o ShareFile.

Conectores StorageZone

Você pode configurar o XenMobile para fornecer acesso somente a StorageZone Connectors que você cria por meio do console XenMobile. Essa configuração:

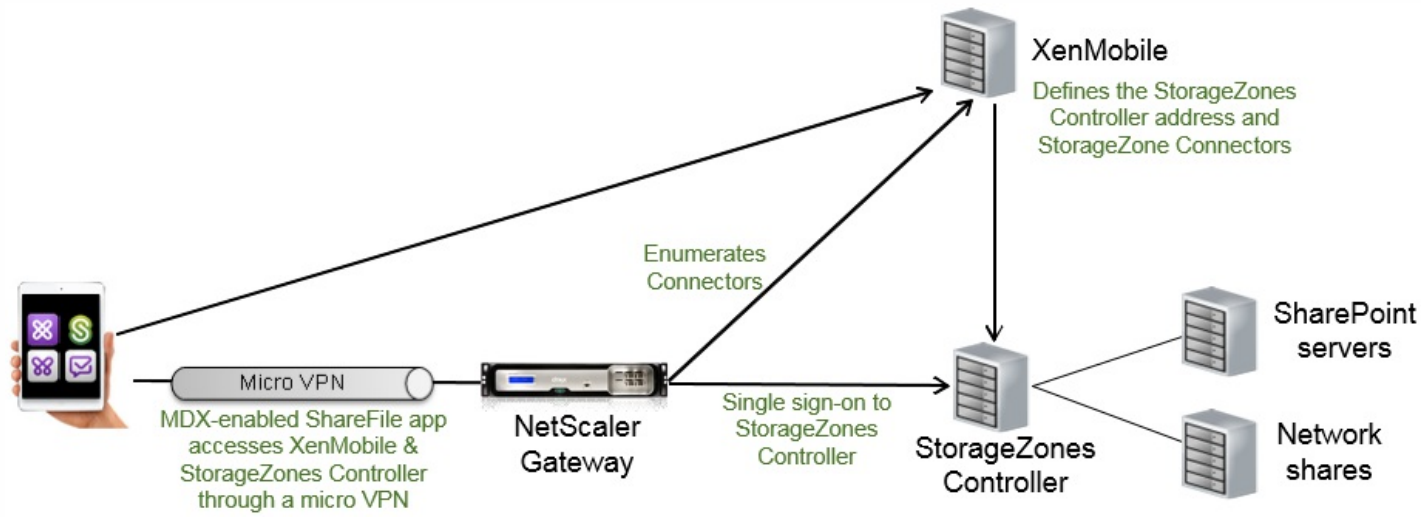
- Fornece aos usuários acesso móvel em repositórios de armazenamento no local existentes, como sites do SharePoint e compartilhamentos de arquivos de rede.
- Não requer que você configure um subdomínio do ShareFile, provisione usuários para o ShareFile ou hospede dados do ShareFile.
- Fornece aos usuários acesso móvel aos seus dados armazenados por meio dos XenMobile Apps do ShareFile 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 StorageZone Connectors por meio do console XenMobile. Se mais tarde você decidir usar a funcionalidade completa do ShareFile com o XenMobile, poderá alterar a configuração no console XenMobile.
- Requer o XenMobile Enterprise Edition.

Apenas para uma XenMobile integração com conectores StorageZone:

- O ShareFile usa sua configuração de logon único para o NetScaler Gateway para autenticar com o StorageZones Controller.
- O XenMobile não se autentica via SAML porque o plano de controle do ShareFile não é usado.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

O diagrama a seguir mostra a arquitetura de alto nível para o uso do XenMobile com StorageZone Connectors.



Requisitos

- Versões mínimas dos componentes:
  - XenMobile Server 10.5 (no local)
  - ShareFile para iOS (MDX) 5.3
  - ShareFile for Android (MDX) 5.3
  - ShareFile StorageZones Controller 5.0

    Este artigo contém instruções sobre como configurar o ShareFile StorageZones Controller 5.0
- Verifique se o servidor que deverá executar o StorageZones Controller atende aos requisitos de sistema. Para obter os requisitos, consulte as seções a seguir em "Requisitos do sistema" na documentação do ShareFile StorageZones Controller:
  - StorageZones Controller
  - StorageZone Connectors para SharePoint
  - StorageZone Conector para compartilhamentos de arquivos de rede

    Os requisitos de StorageZones para dados do ShareFile e StorageZones restritas não se aplicam a uma integração de XenMobile apenas com StorageZone Connector.

    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 seguintes, na ordem apresentada para instalar e configurar o StorageZones Controller. Estes passos são específicos para uma XenMobile integração com conectores StorageZone: Alguns desses artigos estão na documentação do StorageZones Controller.

1. Configurar o NetScaler para o StorageZones Controller

   Você pode usar o NetScaler como um proxy DMZ para StorageZones Controller.

2. Instalar um certificado SSL

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Um StorageZones Controller que hospeda zonas padrão requer um certificado SSL. Um StorageZones Controller que hospeda zonas restritas e usa um endereço interno não requer um certificado SSL.

3. Prepare o seu servidor

   É necessário instalar o IIS e ASP.NET para conectores de StorageZone.

4. Instalação do StorageZones Controller

5. Preparar o StorageZones Controller para uso com somente StorageZone Connectors

6. Especificar um servidor proxy para StorageZones

   O console do StorageZones Controller permite que você especifique um servidor proxy para StorageZones Controllers. Você também pode especificar um servidor proxy usando outros métodos.

7. Configure o controlador de domínio para confiar no StorageZones Controller para delegação

   Configure o controlador de domínio para oferecer suporte à autenticação NTLM ou Kerberos em compartilhamentos de rede ou sites do SharePoint.

8. Juntar um StorageZones Controller secundário a uma StorageZone

   Para configurar uma StorageZone para alta disponibilidade, conecte pelo menos dois StorageZones Controllers a ele.

Instalação do StorageZones Controller

1. Baixe e instale o software StorageZones Controller:

   a. Na página de download do ShareFile em http://www.citrix.com/downloads/sharefile.html faça login e baixe o instalador do StorageZones Controller mais recente.

   b. A instalação do StorageZones Controller altera o site padrão no servidor para o caminho de instalação do controlador. Ativar a **Autenticação anônima** no site da Web padrão.

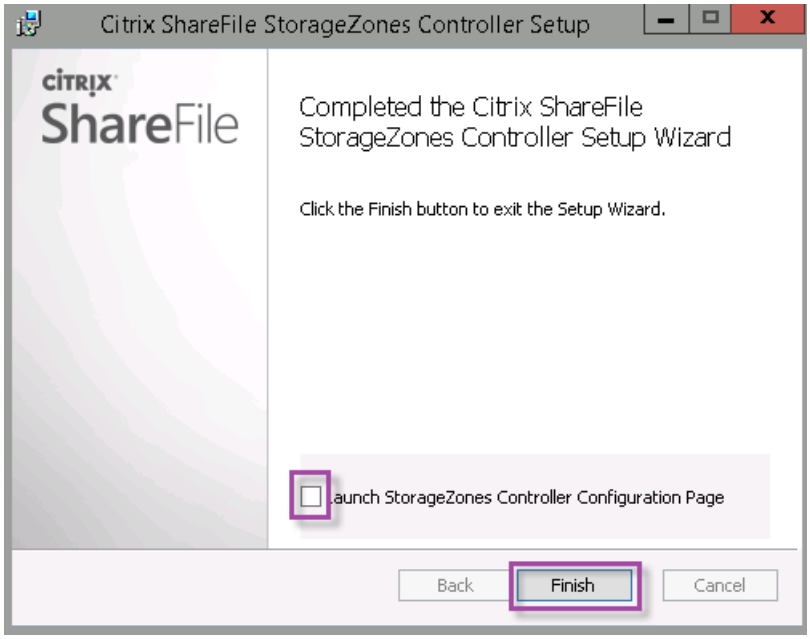
2. No servidor em que você deseja instalar o StorageZones Controller, execute StorageCenter.msi.

   Inicia o Assistente de instalação do ShareFile StorageZones Controller.

3. Responda às solicitações:

- Na página **Destination Folder** página, se os serviços de informações da Internet (IIS) estiver instalado 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 StorageZones Controller Configuration Page** e, em seguida, clique em **Finish**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. Quando solicitado, reinicie o StorageZones Controller.

5. Para testar se a instalação foi bem-sucedida, navegue até http://localhost/. Se a instalação for bem-sucedida, o logotipo do ShareFile é exibida.

Se o logotipo do ShareFile não for exibido, limpe o cache do navegador e tente novamente.

> ## Important
>
> Se você planeja clonar o StorageZones Controller, capture a imagem de disco antes de continuar configurando o StorageZones Controller.

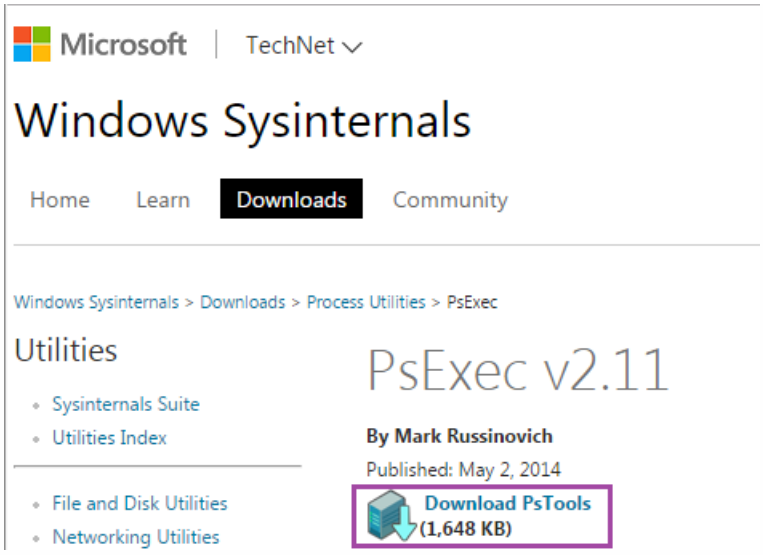
Preparar o StorageZones Controller para uso com somente StorageZone Connectors

Para uma integração somente com conectores StorageZone, você não usa o console administrativo StorageZones Controller. Aquela interface requer uma conta de administrador do ShareFile, o que não é necessário para esta solução. Como resultado, você pode executar um script do PowerShell para preparar o StorageZones Controller para uso sem plano de controle do ShareFile. O script faz o seguinte:

- Registra o StorageZones Controller atual como um StorageZones Controller primário. Mais tarde você pode juntar StorageZones Controllers secundários ao controlador primário.
- Cria uma zona e define a senha para ela.

1. No seu servidor de StorageZone Controller, 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.

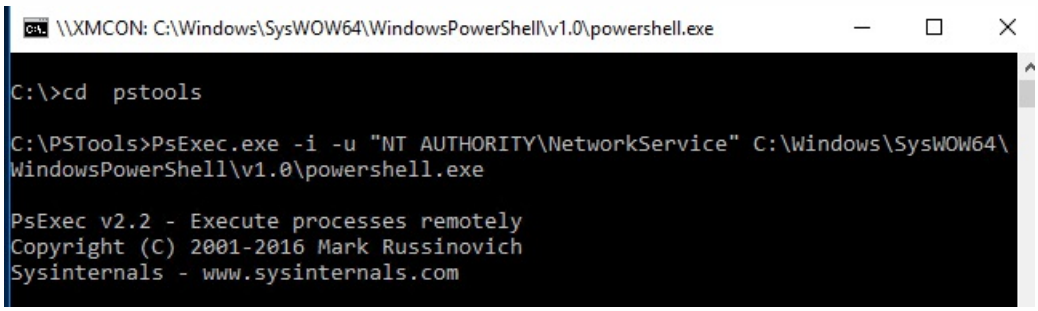
© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Execute a ferramenta PsExec: Abra o aviso de comando como o usuário de administrador e, em seguida, digite o seguinte:

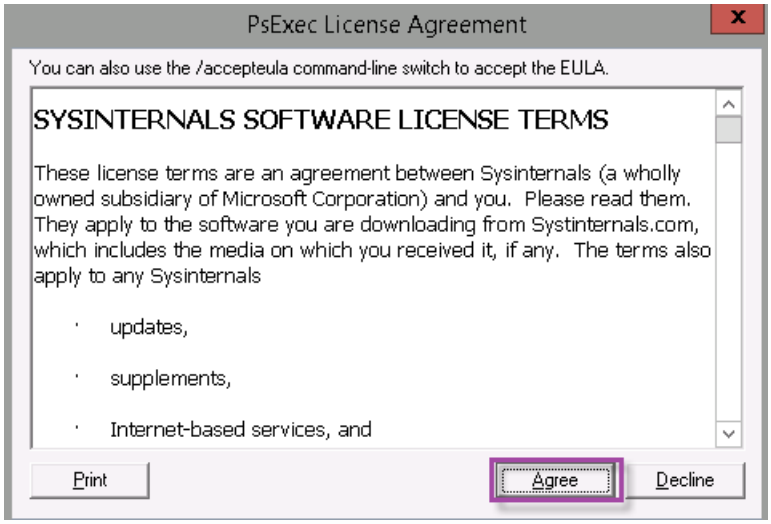
comando COPIAR

```
cd c:\pstools

PsExec.exe -i -u "NT AUTHORITY\NetworkService" C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
```



3. Quando solicitado, clique em **Concordar** para executar a ferramenta Sysinternals.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



É aberta uma janela do PowerShell.

4. Na janela do PowerShell, digite o seguinte:

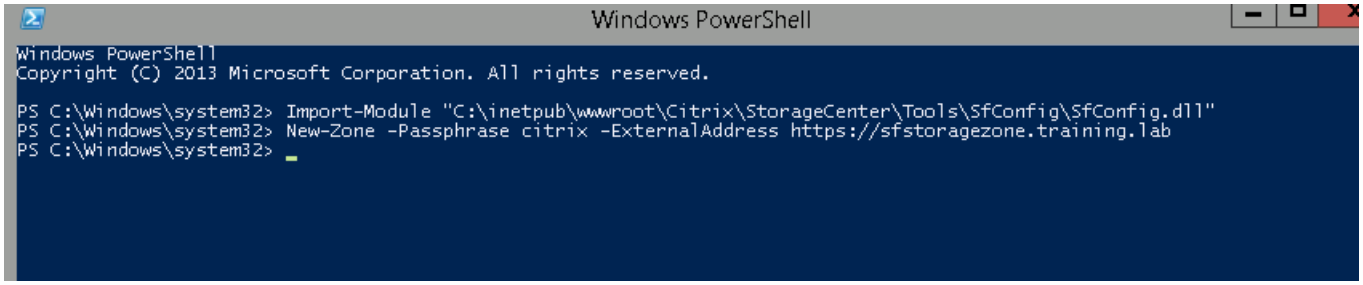
comando COPIAR

```
Import-Module "C:\inetpub\wwwroot\Citrix\StorageCenter\Tools\SfConfig\SfConfig.dll"

New-Zone  -Passphrase passphrase -ExternalAddress https://szcfqdn.com
```

Onde:

Passphrase: É a senha que você deseja atribuir o site. Anote-a. Não é possível recuperar a senha por meio do controlador. Se você perder a senha, não poderá reinstalar StorageZones, juntar mais StorageZones Controllers à StorageZone nem recuperar a StorageZone se o servidor falhar.

ExternalAddress: É o nome de domínio totalmente qualificado externo do servidor StorageZones Controller.



Seu StorageZones Controller primário agora está pronto.

Antes de fazer logon no XenMobile para criar StorageZone Connectors: conclua a configuração a seguir, se aplicável:

Especificar um servidor proxy para StorageZones

Configure o controlador de domínio para confiar no StorageZones Controller para delegação

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Juntar um StorageZones Controller secundário a uma StorageZone

Para criar StorageZone Connectors, veja Definir conexões do StorageZones Controller no XenMobile.

Juntar um StorageZones Controller secundário a uma StorageZone

Para configurar uma StorageZone para alta disponibilidade, conecte pelo menos dois StorageZones Controllers a ele. Para juntar um StorageZones Controller secundário a uma zona, instale o StorageZones Controller em um segundo servidor. Em seguida, junte esse controlador à zona do controlador principal.

1. Abra uma janela do PowerShell no servidor StorageZones Controller que você deseja juntar ao servidor primário.

2. Na janela do PowerShell, digite o seguinte:

Join-Zone -Passphrase -PrimaryController

Por exemplo:

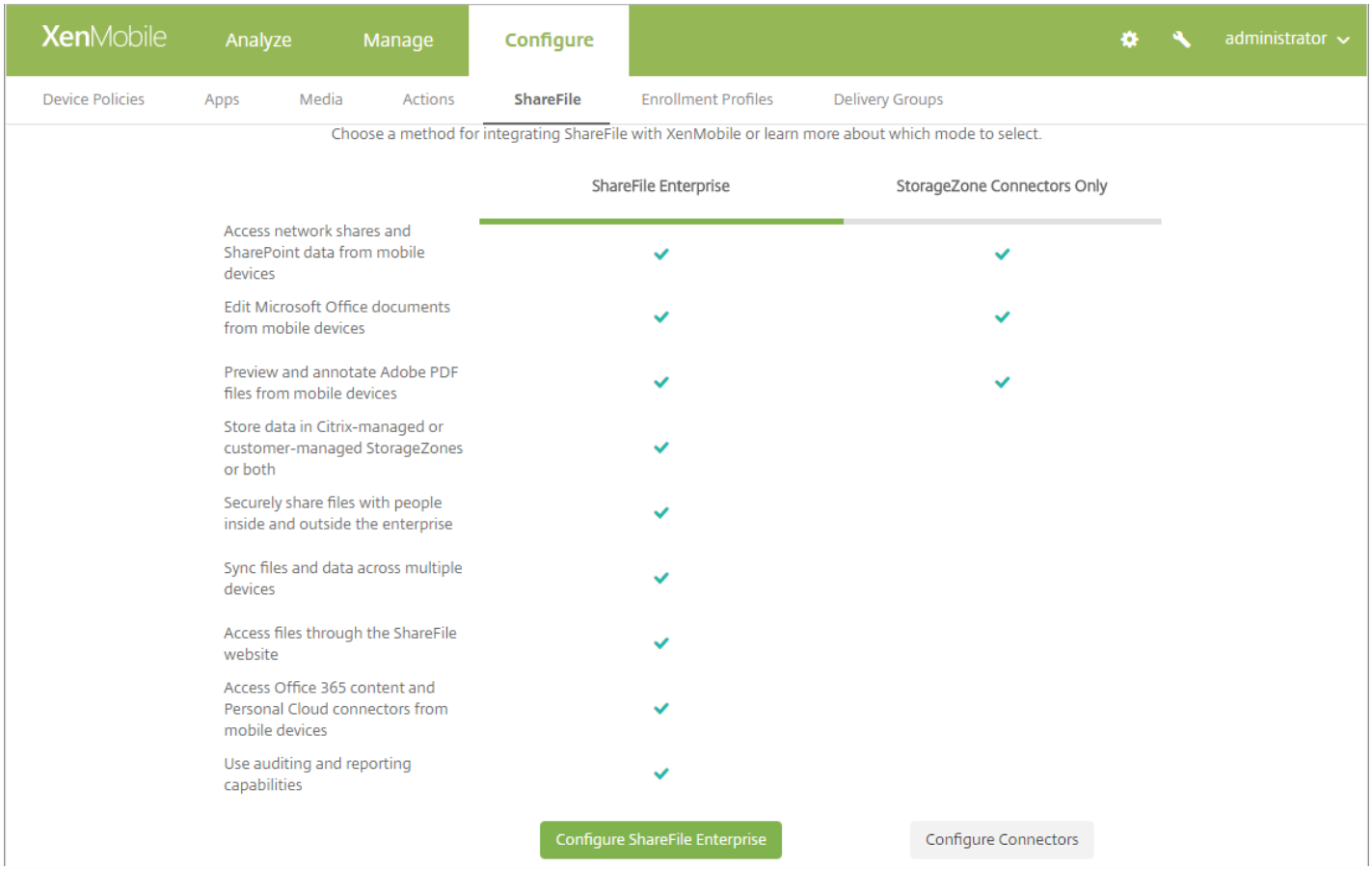
Join-Zone -Passphrase secret123 -PrimaryController 10.10.110.210

Definir conexões do StorageZones Controller no XenMobile

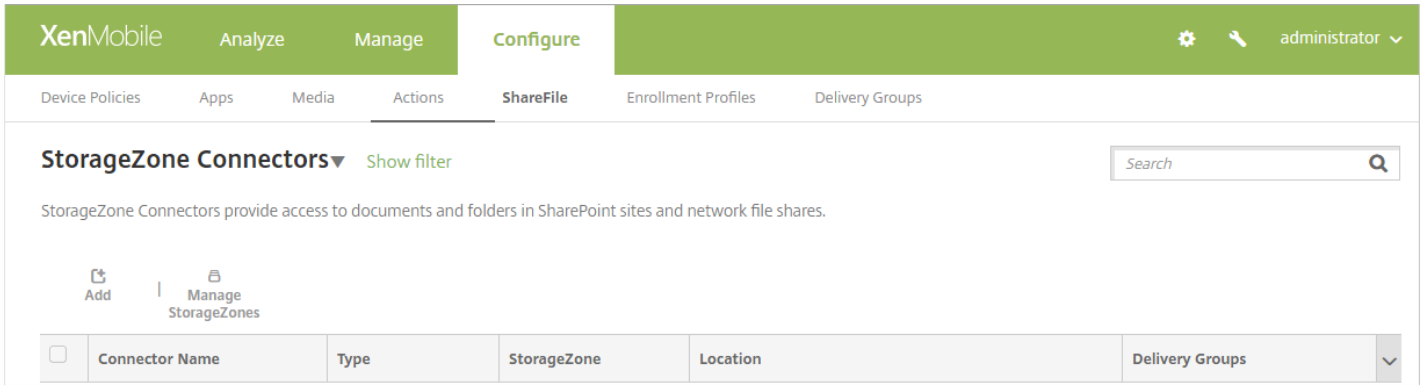
Antes de adicionar StorageZone Connectors, configure informações de conexão para cada StorageZones Controller ativado para StorageZone Connectors. Você pode definir StorageZones Controllers conforme descrito nesta seção ou ao adicionar um conector.

Na sua primeira visita à página **Configurar > ShareFile**, a página resume as diferenças entre o uso do XenMobile com o ShareFile Enterprise e StorageZone Connectors.

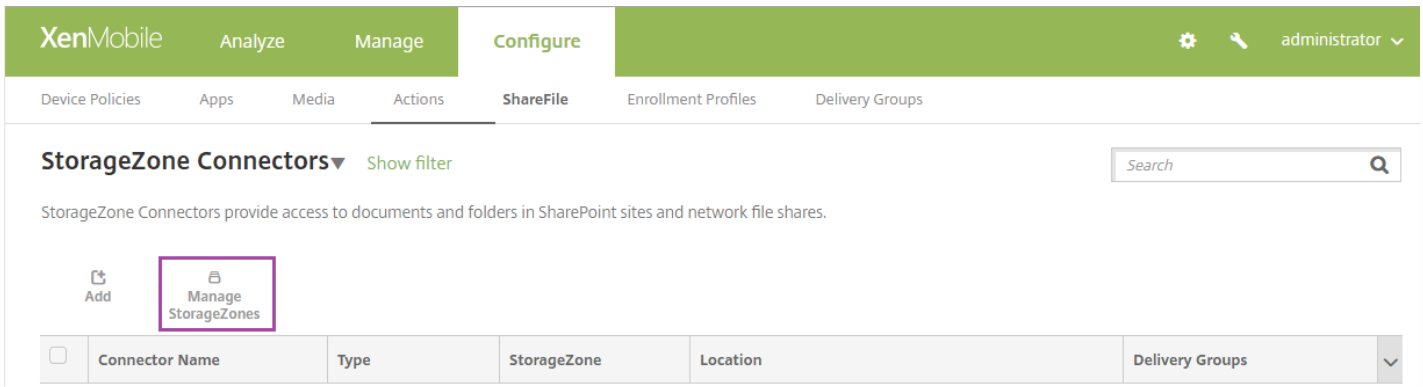
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Clique em **Configurar conectores** para continuar com as etapas de configuração neste artigo.

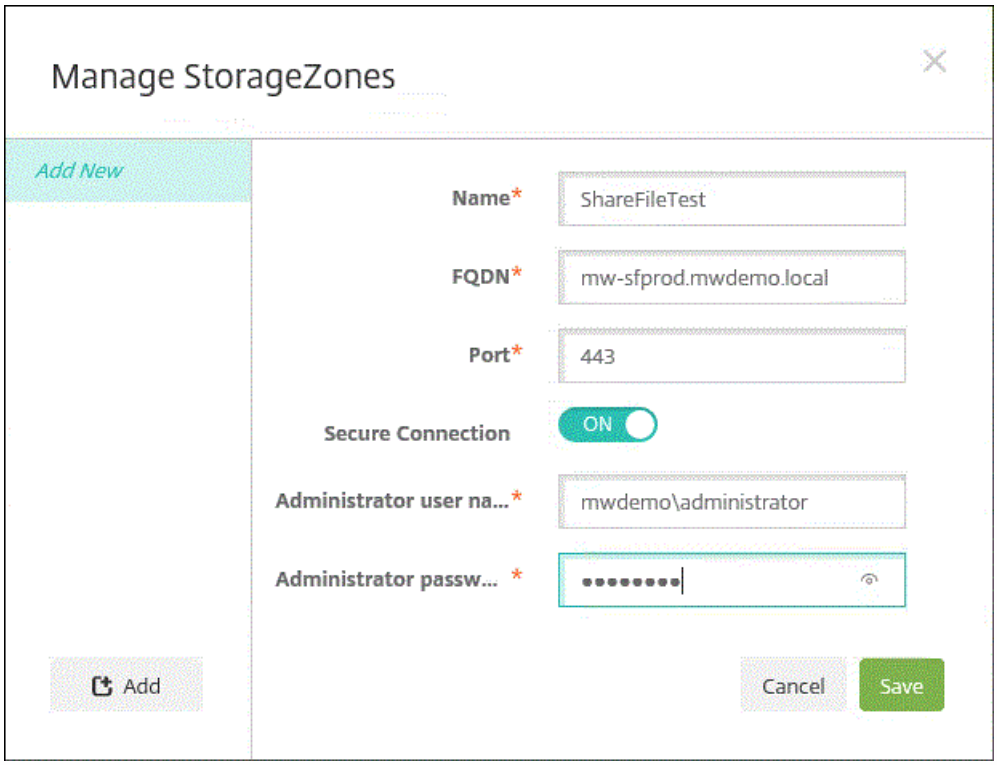


1. Em **Configurar > ShareFile**, clique em **Gerenciar StorageZones**.



2. Em **Gerenciar StorageZones**, adicione as informações de conexão.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



- **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 do StorageZones Controller que pode ser alcançada a partir do XenMobile Server.
- **Conexão segura**: se você usar SSL para conexões com o StorageZones Controller, 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 StorageZones Controllers.

3. Clique em **Salvar**.

4. Para testar a conexão, verifique se o XenMobile Server pode alcançar o nome de domínio totalmente qualificado do StorageZones Controller na porta 443.

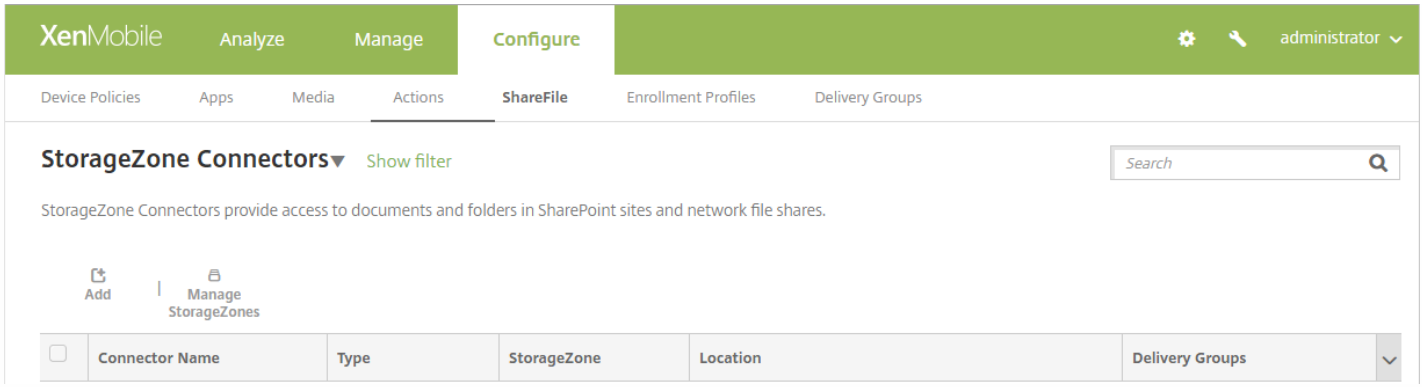
5. Para definir outra conexão com o StorageZones Controller, clique no botão **Adicionar** em **Gerenciar StorageZones**.

Para editar ou excluir as informações de uma conexão do StorageZones Controller, selecione o nome da conexão em **Gerenciar StorageZones**. Em seguida, clique em **Editar** ou **Excluir**.

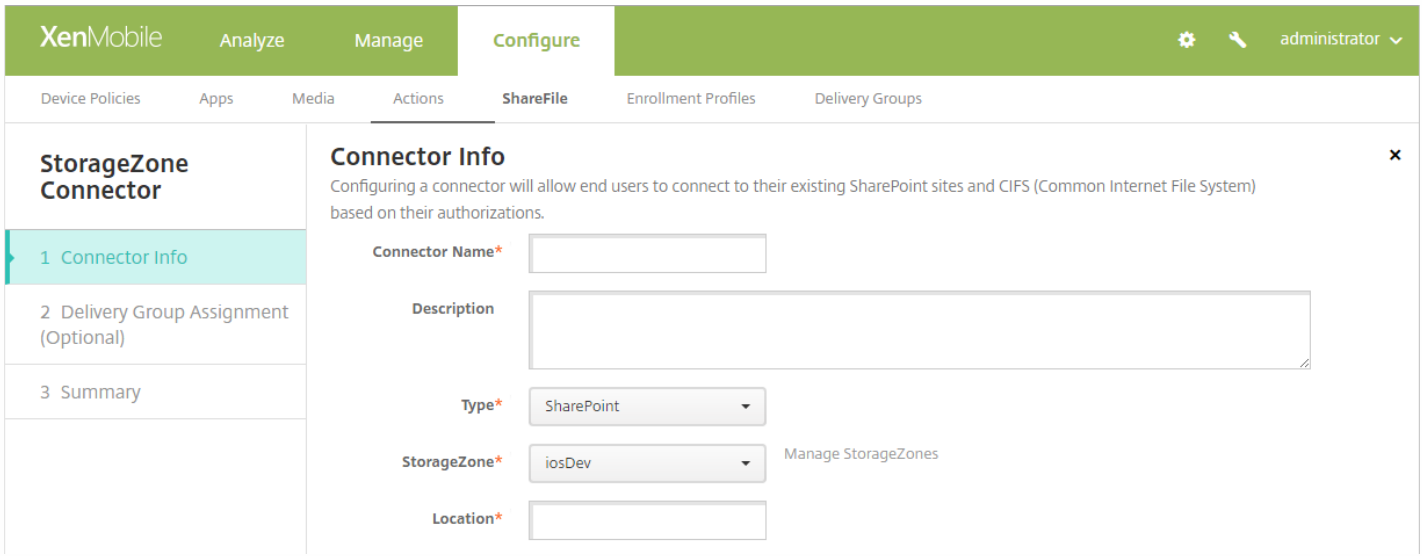
Adicionar um StorageZone Connector no XenMobile

1. Vá até **Configurar > ShareFile** e clique em **Adicionar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



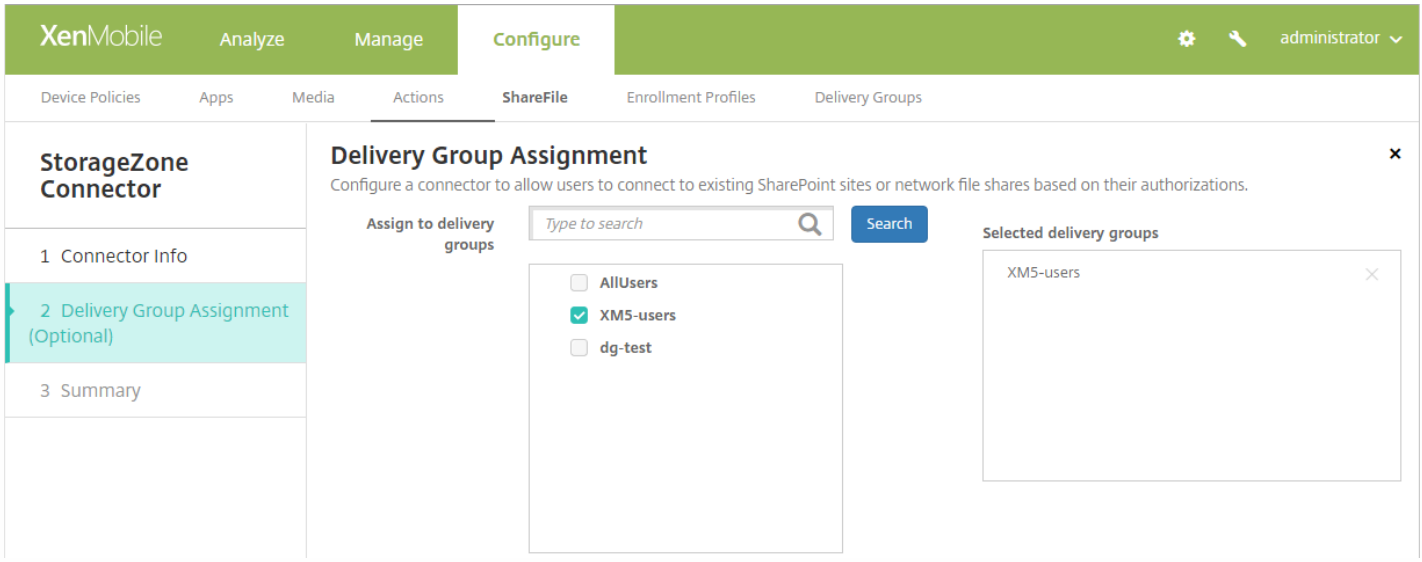
2. Na página **Informações do conector**, defina estas configurações:



- **Nome do conector**: um nome que identifica o StorageZone Connector no XenMobile.
- **Descrição**: observações opcionais sobre esse Conector.
- **Tipo**: escolha **SharePoint** ou **Rede**.
- **StorageZone**: escolha o StorageZone associado ao Conector. Se o StorageZone não estiver na lista, clique em **Gerenciar StorageZones** para definir o StorageZones Controller.
- **Localização**: para o SharePoint, especifique o URL do site de nível raiz, o conjunto de sites ou a biblioteca de documentos do SharePoint, no formato https://sharepoint.empresa.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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. Na página **Resumo**, você pode rever as opções configuradas. Para ajustar a configuração, clique em **Voltar**.

5. Clique em **Salvar** para salvar o Conector.

6. Teste o conector:

a. Ao preparar os clientes do ShareFile, 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 de ShareFile. O tráfego é redirecionado por meio do NetScaler Gateway por meio de uma aplicativo específico micro VPN.

- Definir a política de modo VPN preferida para **Secure browse**.

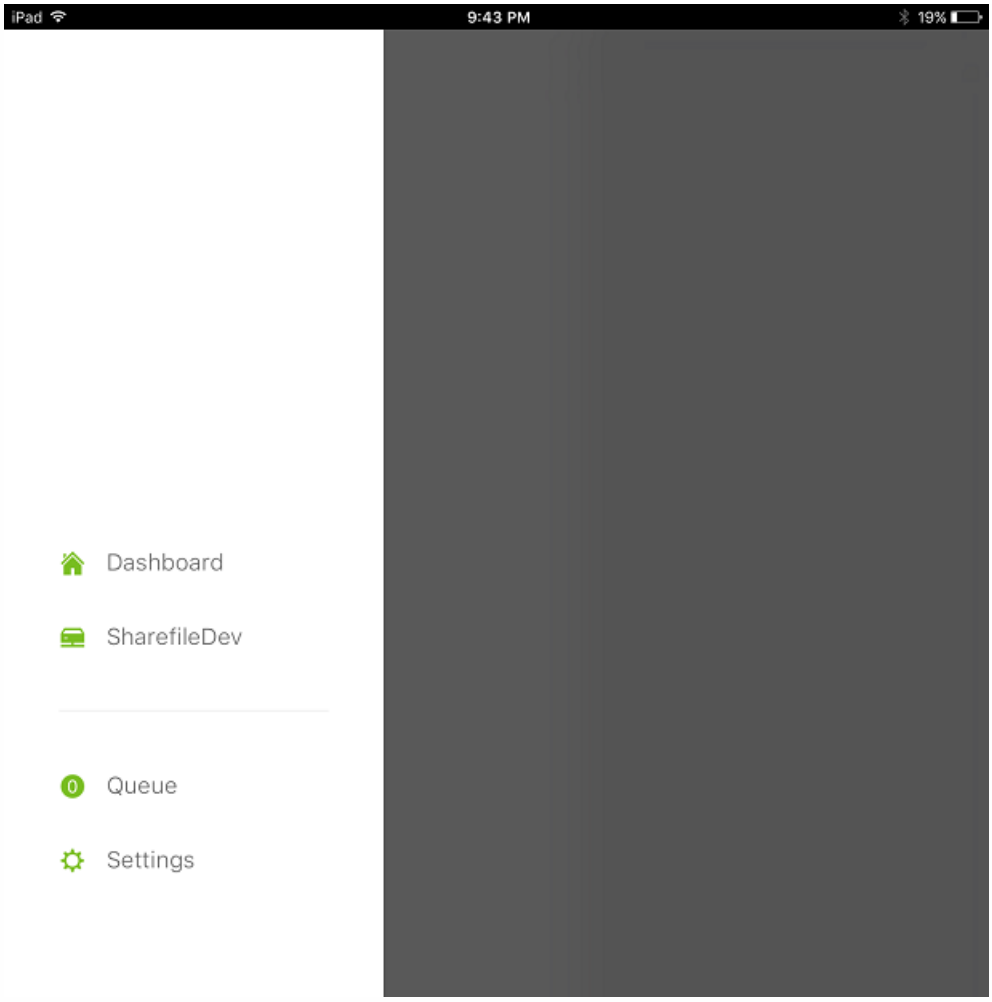
  Nesse modo de criação de túneis, o framework MDX termina o tráfego SSL/HTTP a partir de um aplicativo MDX. O MDX depois inicia novas conexões para conexões a conexões internas em nome do usuário. Essa configuração de política permite que o framework de MDX detecte e responda aos desafios de autenticação emitidos por servidores da web.

b. Para adicionar clientes ShareFile ao XenMobile. Para obter detalhes, consulte Para acrescentar os clientes do ShareFile ao XenMobile.

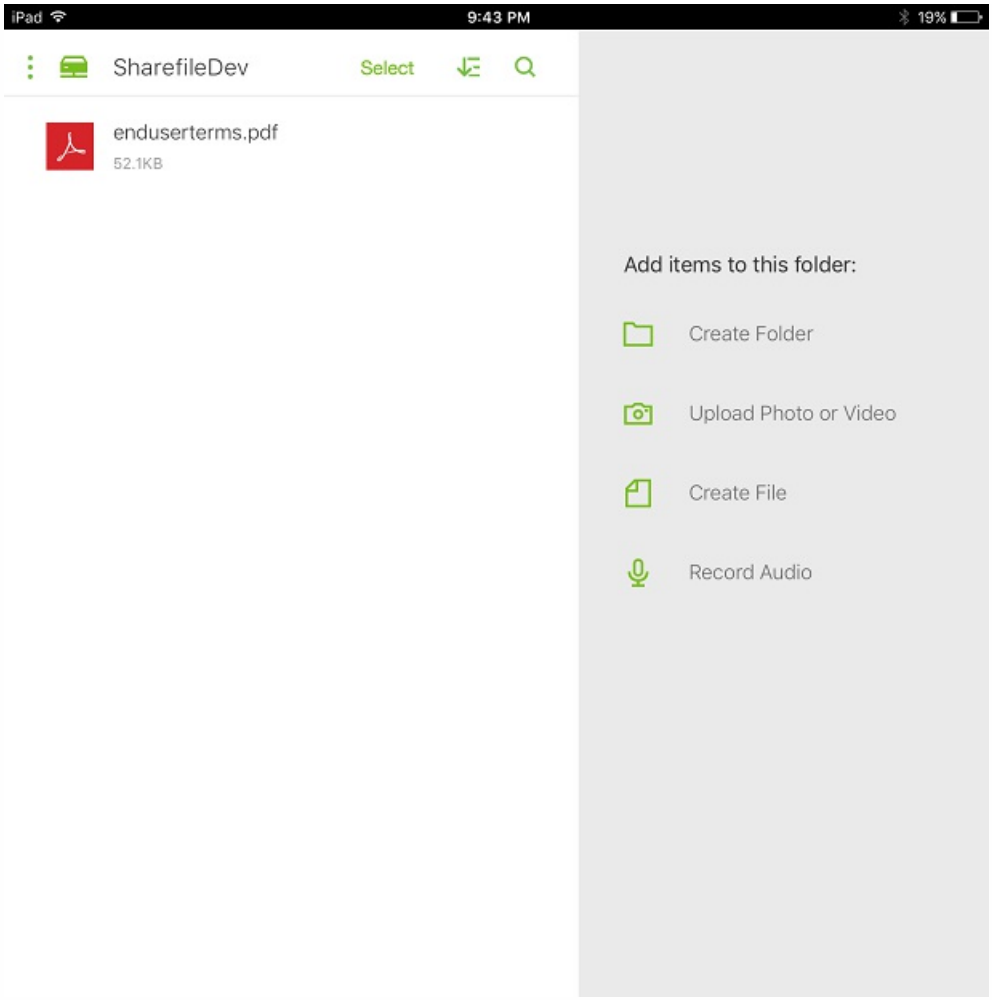
c. A partir de um dispositivo com suporte, verifique o logon único para o ShareFile e conectores.

Nos exemplos a seguir, SharefileDev é o nome de um conector.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



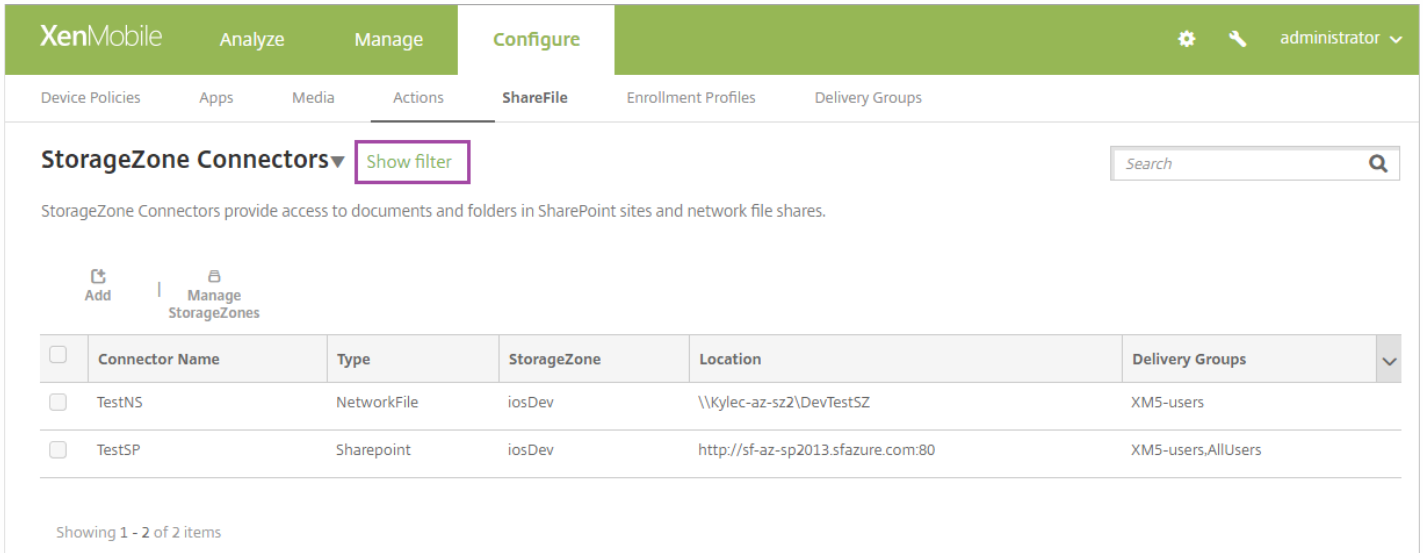
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Filtrar a lista de StorageZone Connectors

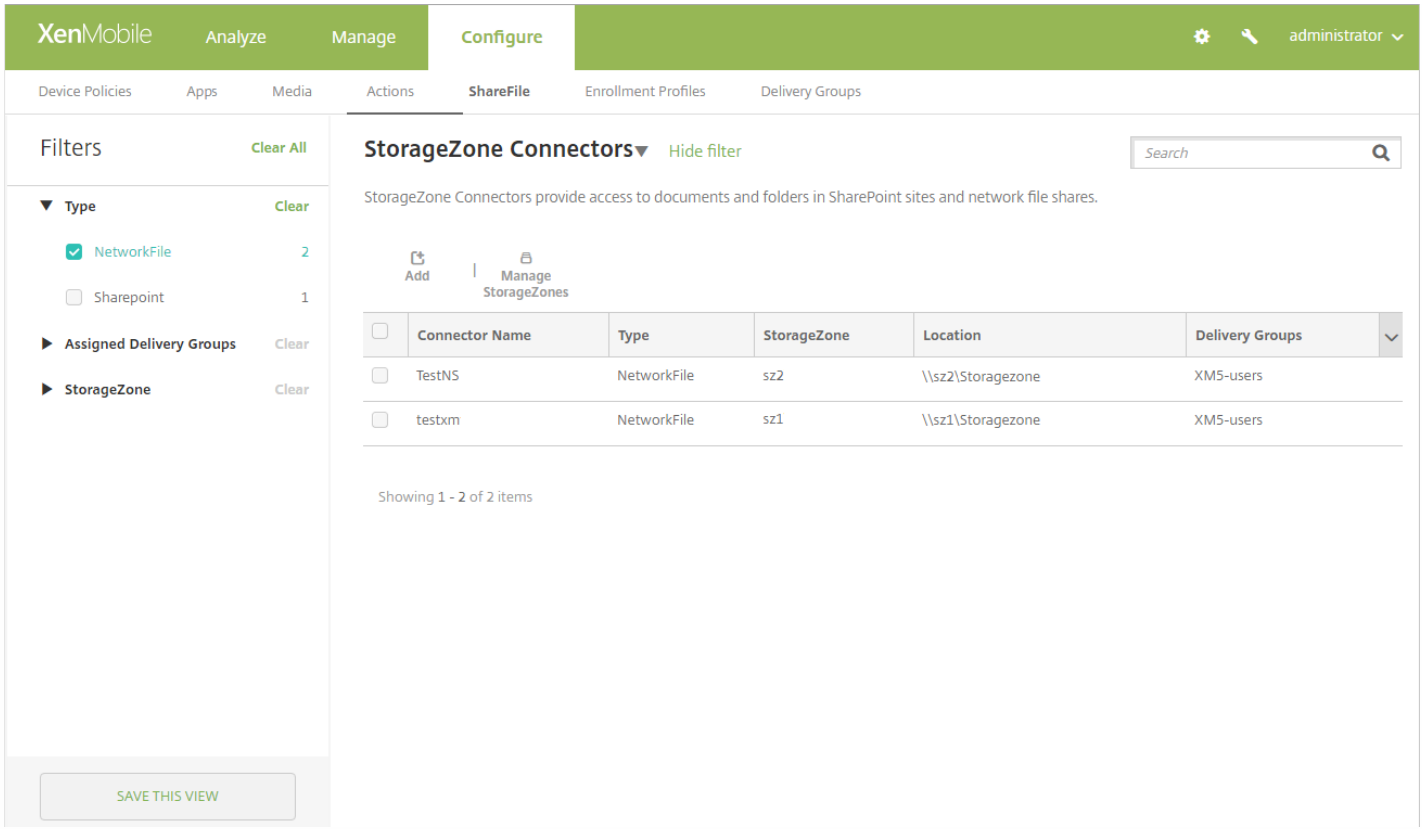
Você pode filtrar a lista de StorageZone Connectors por tipo de Conector, grupos de entrega atribuídos e StorageZone.

1. Vá até **Configurar > ShareFile** e clique em **Mostrar filtro**.



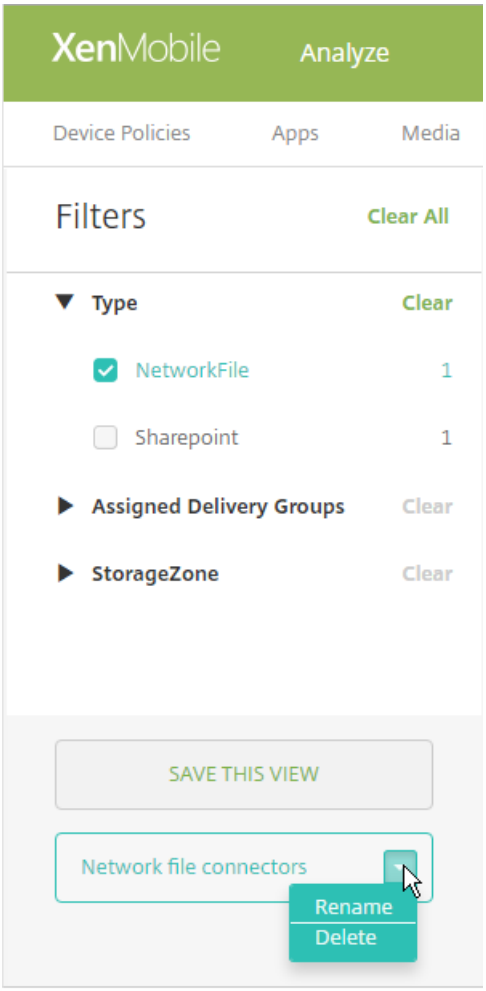
2. Expanda os títulos de filtro para fazer seleções. Para salvar um filtro, clique em **Salvar esta exibição**, digite o nome do filtro e clique em **Salvar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. Para renomear ou excluir um filtro, clique no ícone de seta ao lado do nome do filtro.

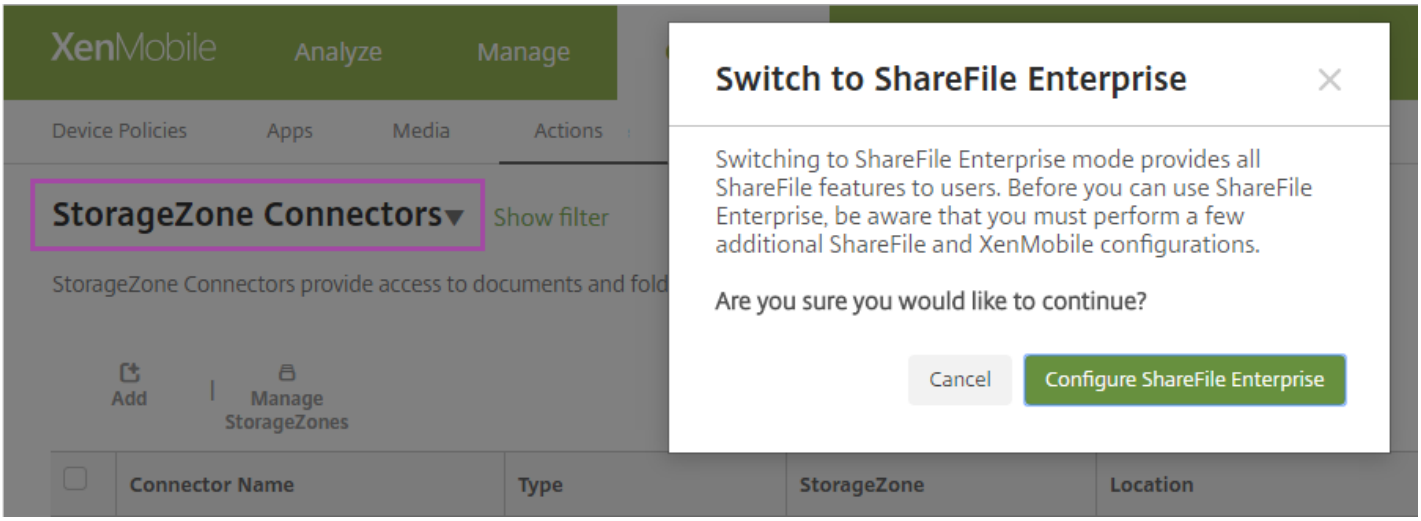
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Mudar para o ShareFile Enterprise

Depois de integrar os StorageZone Connectors ao XenMobile, você pode mudar posteriormente para o conjunto completo de recursos do ShareFile Enterprise. O uso do conjunto de recursos do ShareFile Enterprise requer o XenMobile Enterprise Edition. O XenMobile mantém as configurações de integração existentes do StorageZone Connector.

Vá até **Configurar > ShareFile**, clique no menu suspenso **StorageZone Connectors** e clique em **Configurar ShareFile Enterprise**.



Para obter informações sobre como configurar o ShareFile Enterprise, consulte SAML para logon único com o ShareFile.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

SmartAccess para aplicativos HDX

Feb 21, 2018

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 no XenApp e no XenDesktop 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:

- XenApp e XenDesktop 7.6
- StoreFront 3.7 ou 3.8
- O XenMobile Server configurado reúne os 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 do XenApp e do XenDesktop 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.

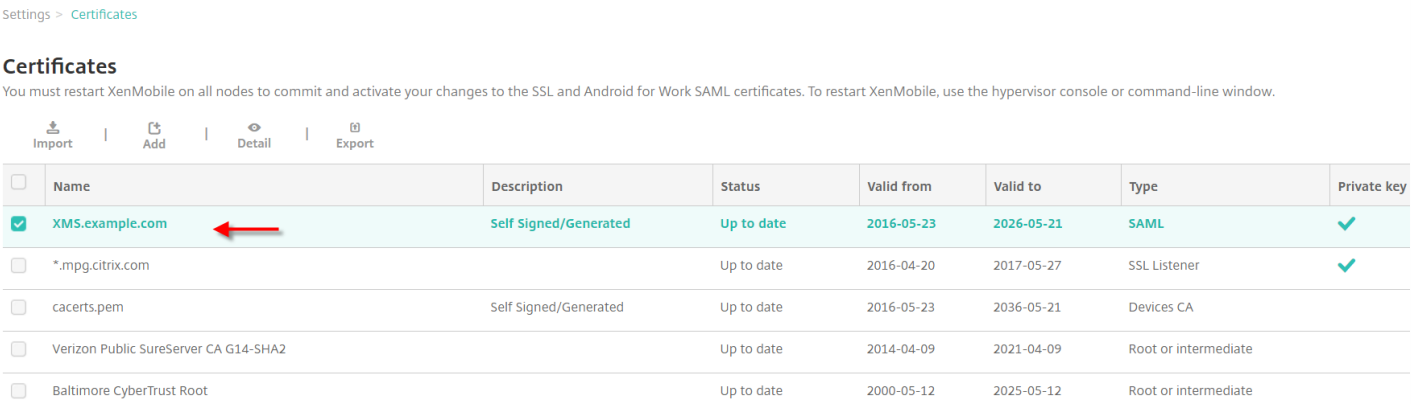
Para obter mais informações sobre como integrar o StoreFront e o XenMobile quando o XenMobile estiver ativado com autenticação baseada em domínio e em certificado, consulte o Support Knowledge Center.

Exportar o certificado SAML do XenMobile Server

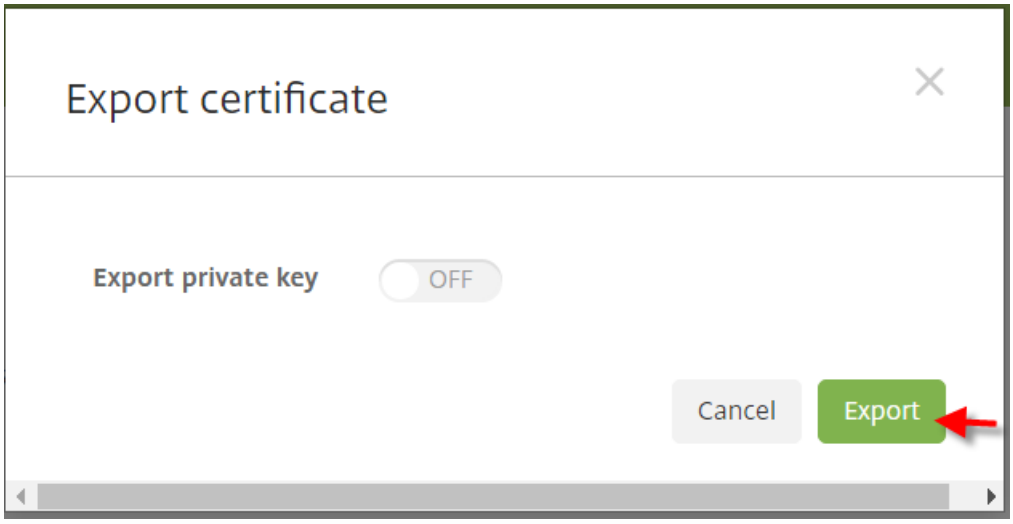
1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida. Clique em **Certificados**.

2. Localize o certificado SAML do XenMobile Server.

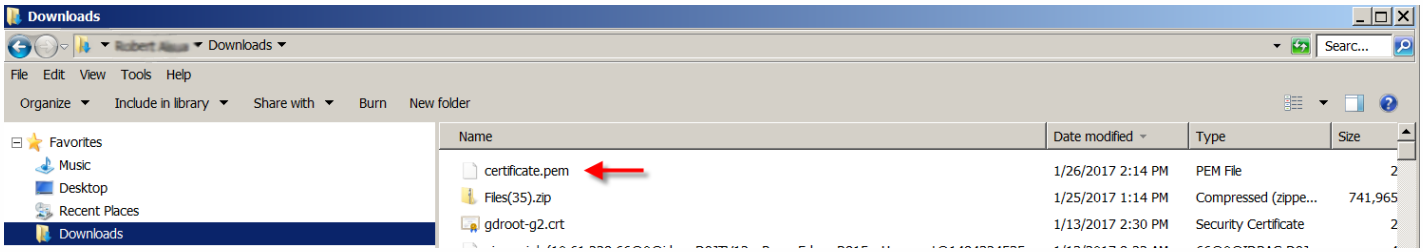
© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. Verifique se a opção **Exportar chave privada** está definida como **O**. Clique em **Exportar** para exportar o certificado para o diretório de download.



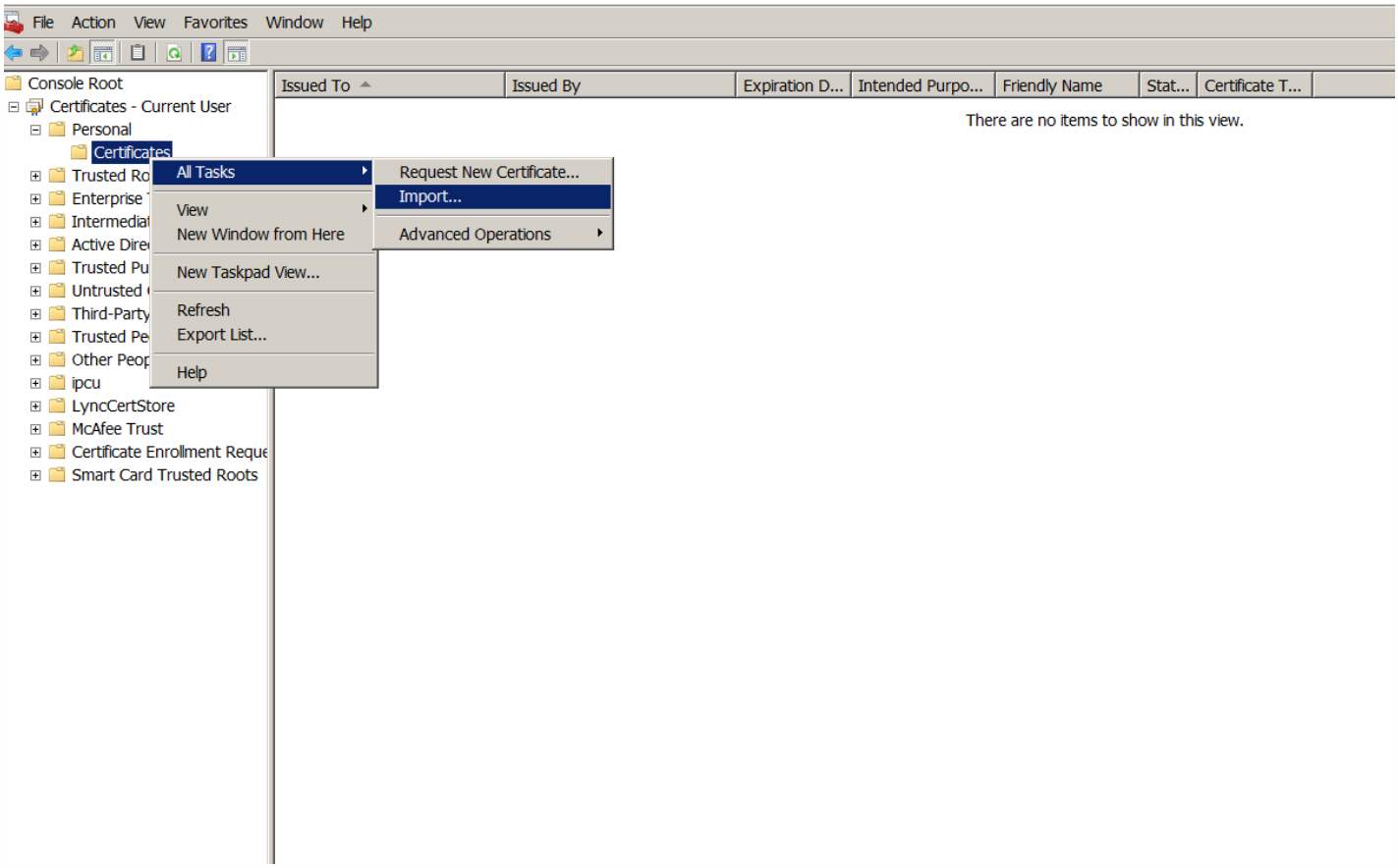
4. Localize o certificado no diretório de download. O certificado está no formato PEM.



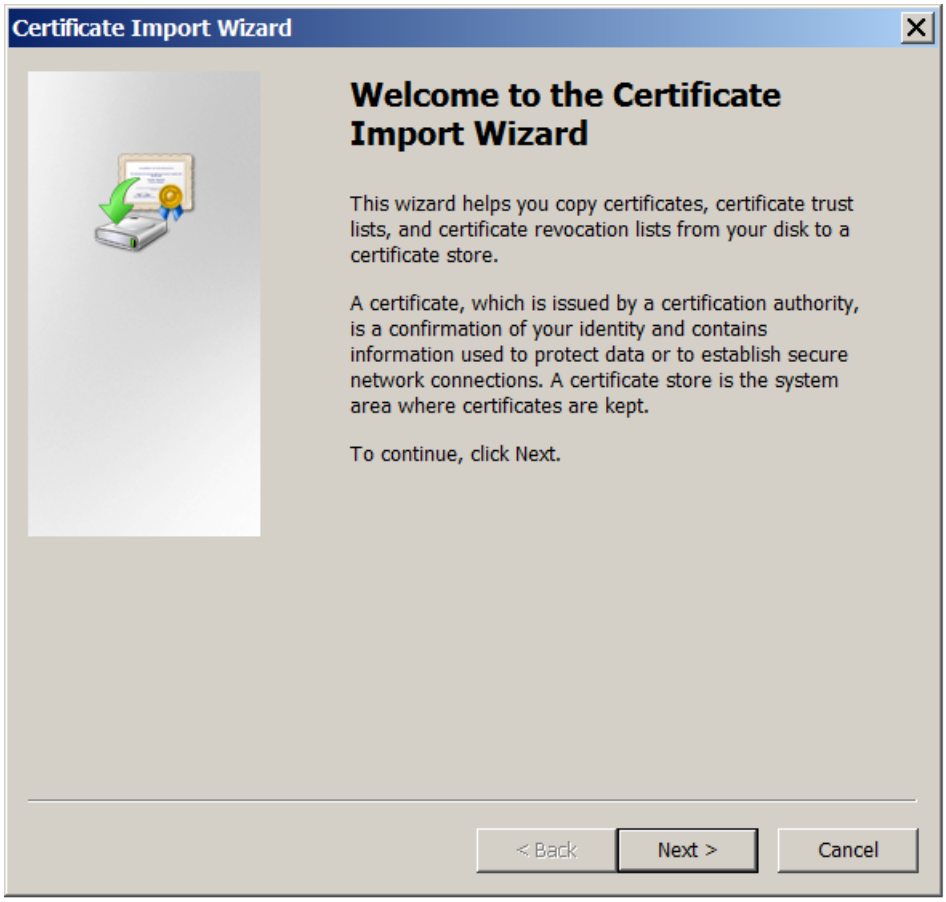
Converter o certificado de PEM para CER

1. Abra o Console de Gerenciamento Microsoft (MMC) e clique com o botão direito do mouse em **Certificados > Todas as tarefas > Importar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

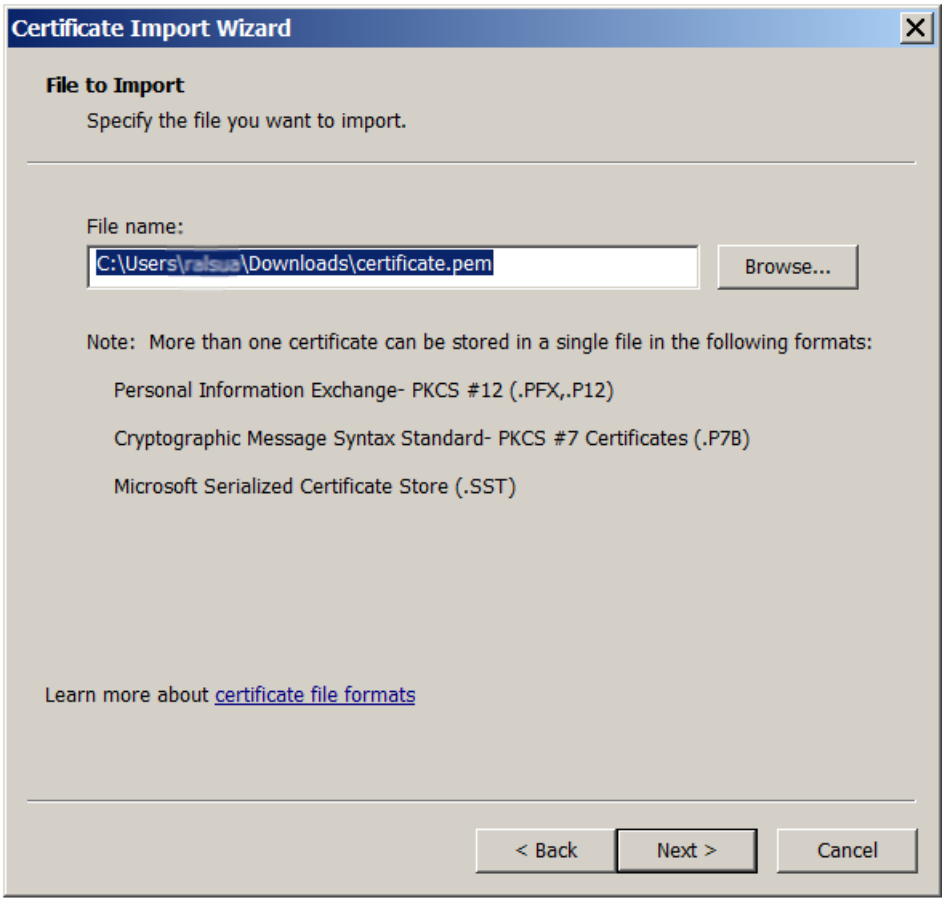


2. Quando o assistente de importação de certificado for exibido, clique em **Avançar**.



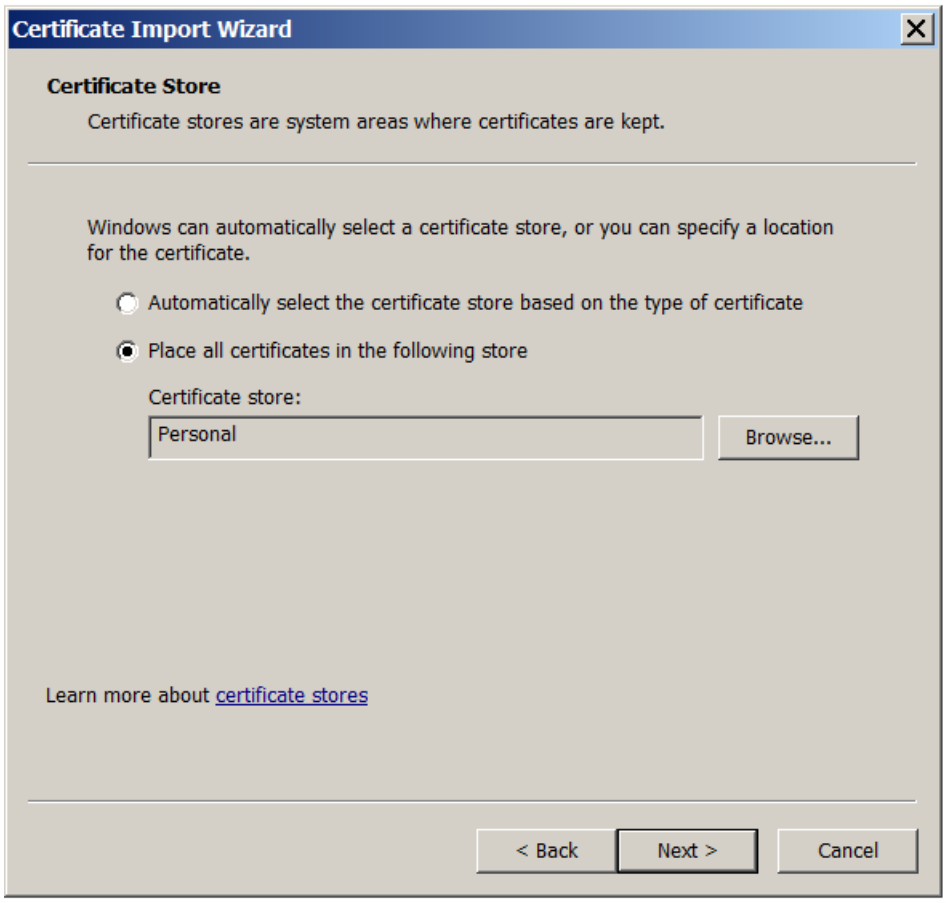
© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Navegue até o certificado no diretório de download.



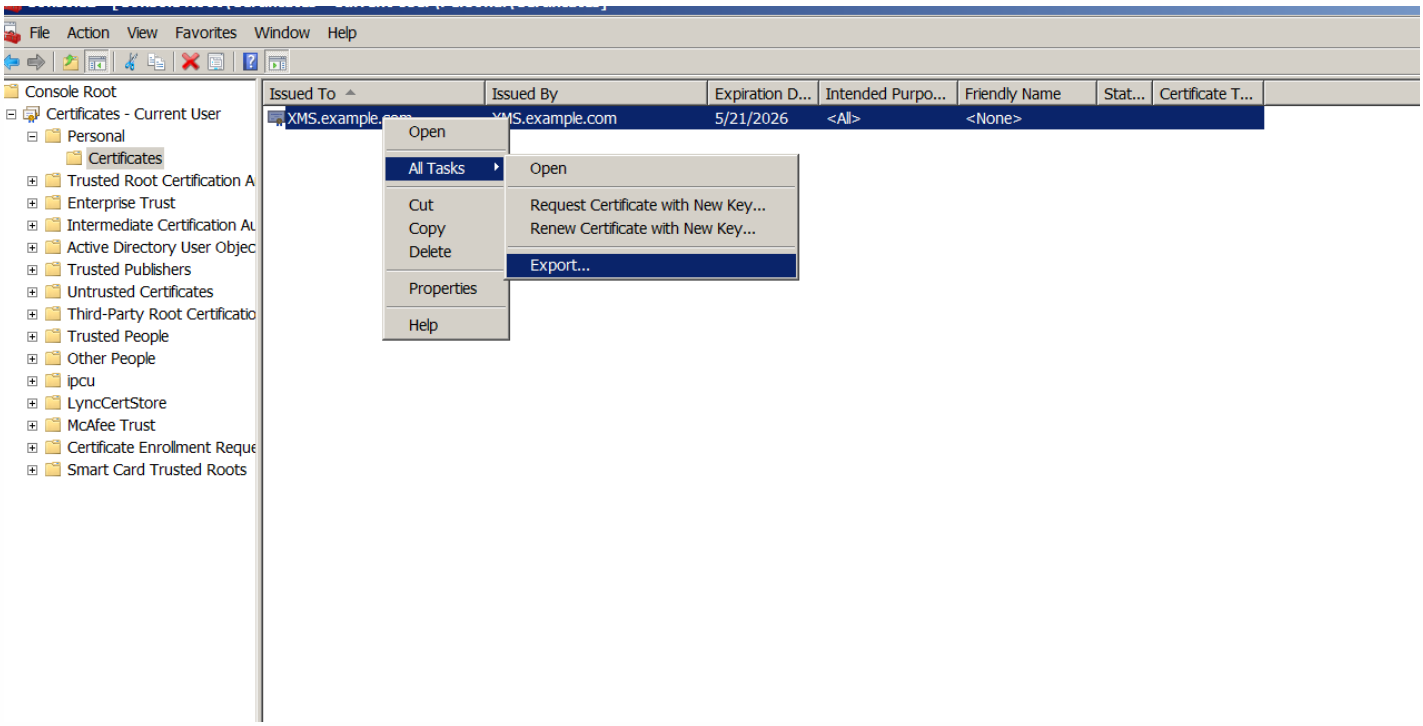
4. Selecione **Colocar todos os certificados no repositório a seguir** e selecione **Pessoal** como o repositório de certificados. Clique em **Avançar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. Revise suas seleções e clique em **Concluir**. Clique em **OK** para ignorar a janela de confirmação.

6. No MMC, clique com o botão direito do mouse no certificado e escolha **Todas as tarefas > Exportar**.

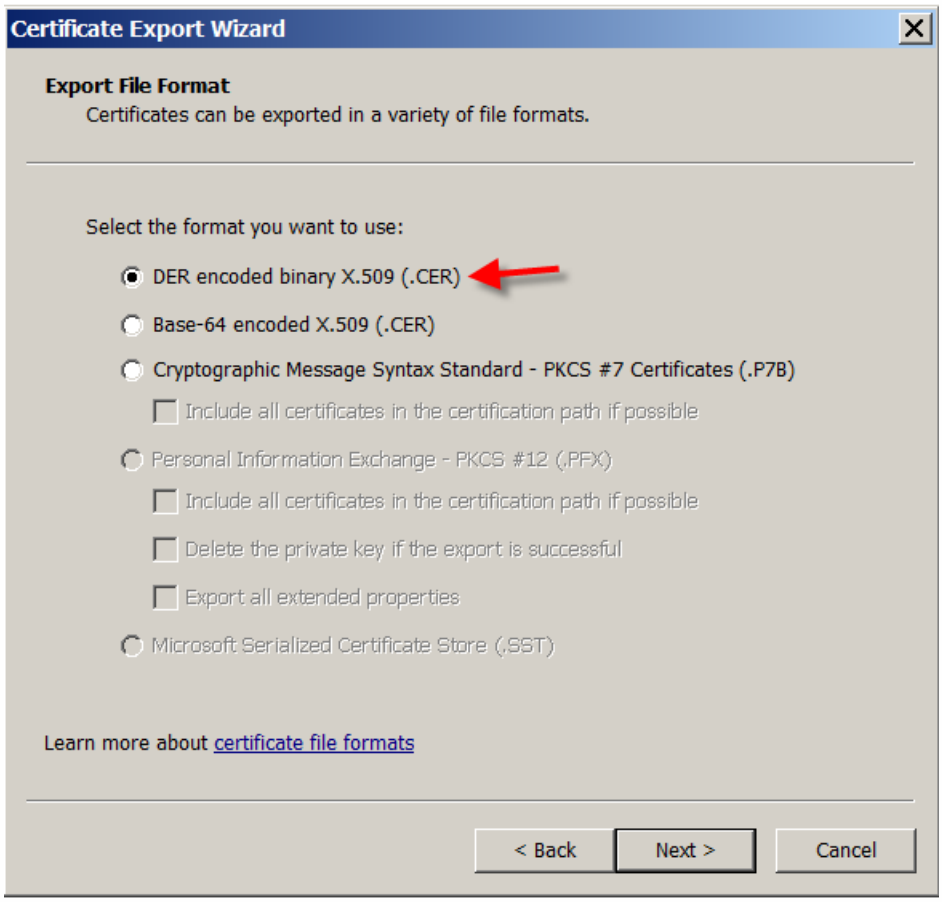


7. Quando o assistente de exportação de certificado for exibido, clique em **Avançar**.

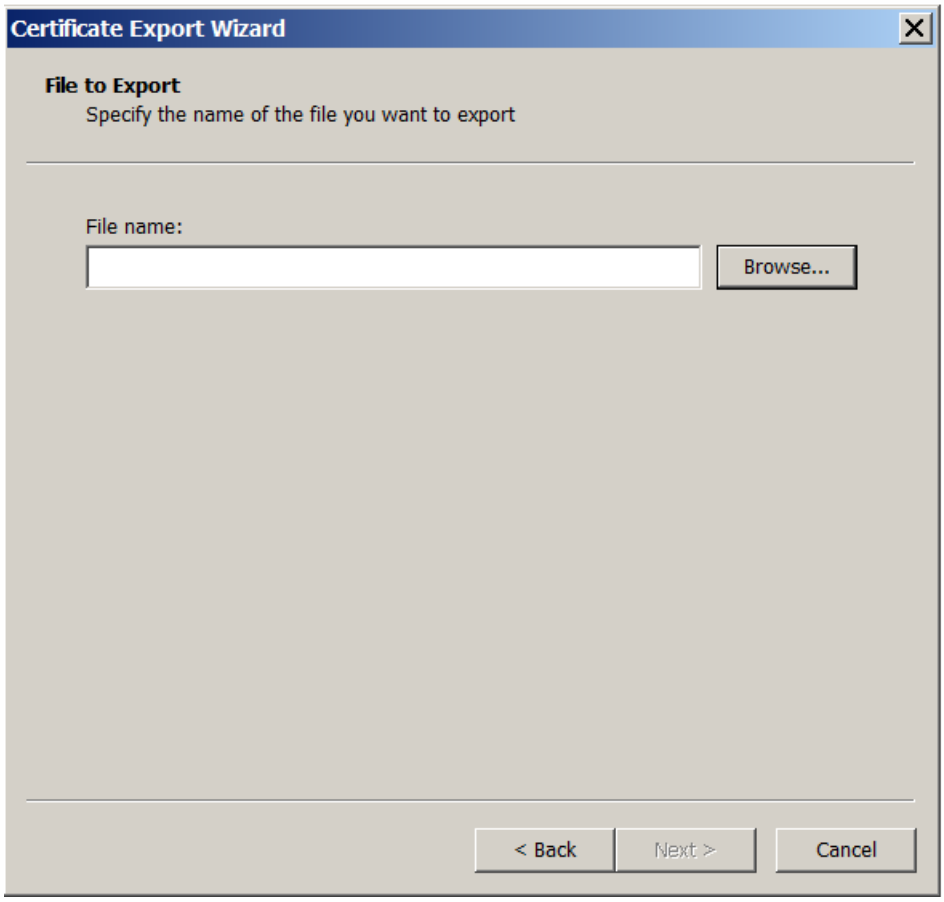
© 1999-2017 Citrix Systems, Inc. All rights reserved.

8. Escolha o formato **x.509 binário codificado por DER (.CER)**. Clique em **Avançar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

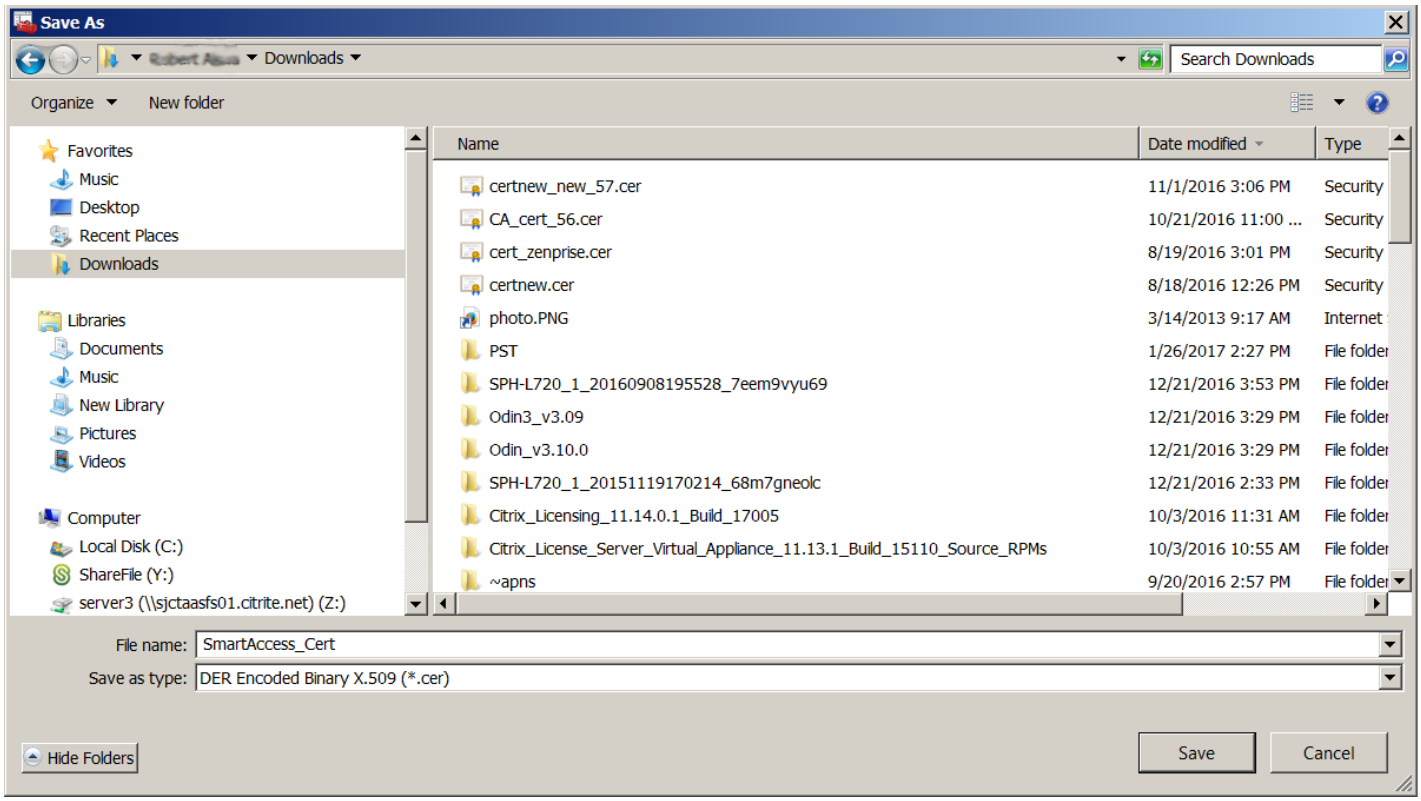


9. Procure o certificado. Digite um nome para o certificado e clique em **Avançar**.

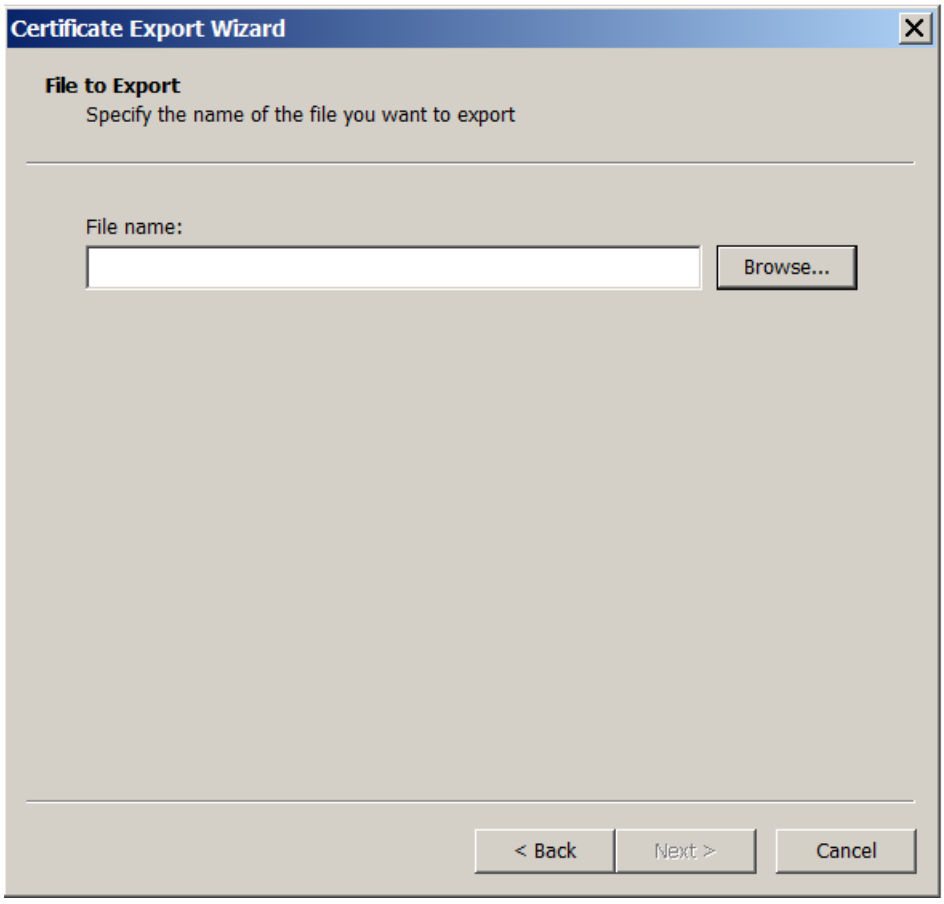


© 1999-2017 Citrix Systems, Inc. All rights reserved.

10. Salve o certificado.

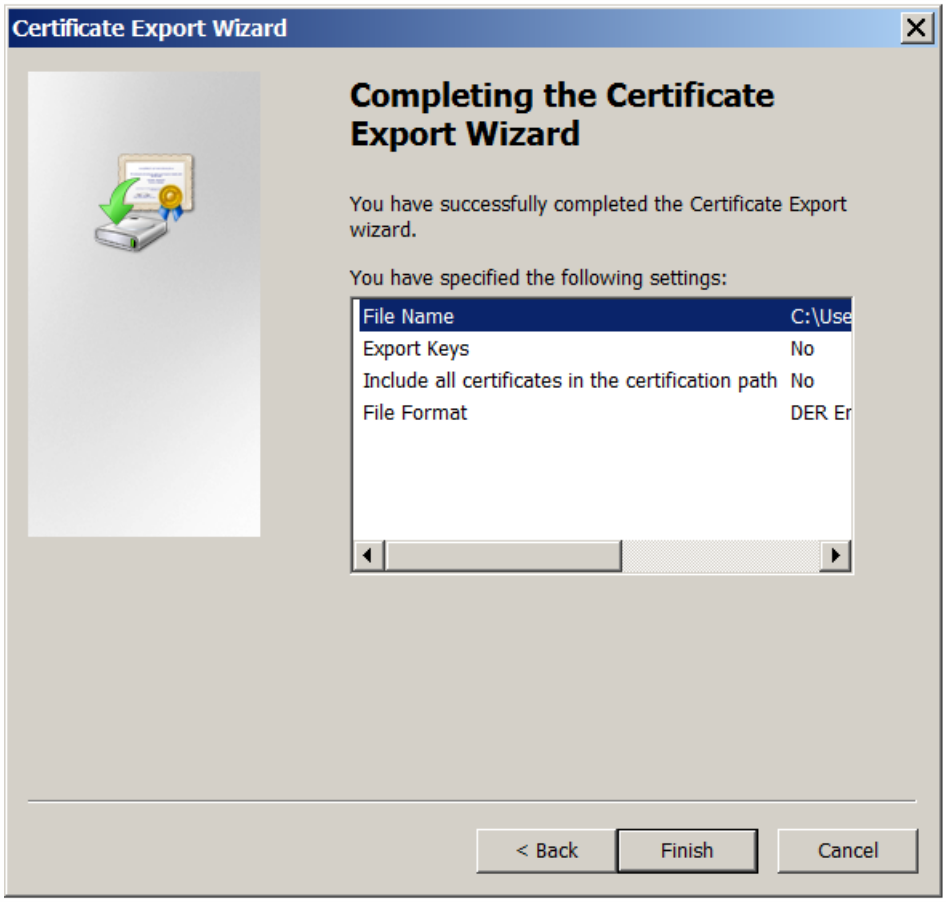


11. Procure o certificado e clique em **Avançar**.

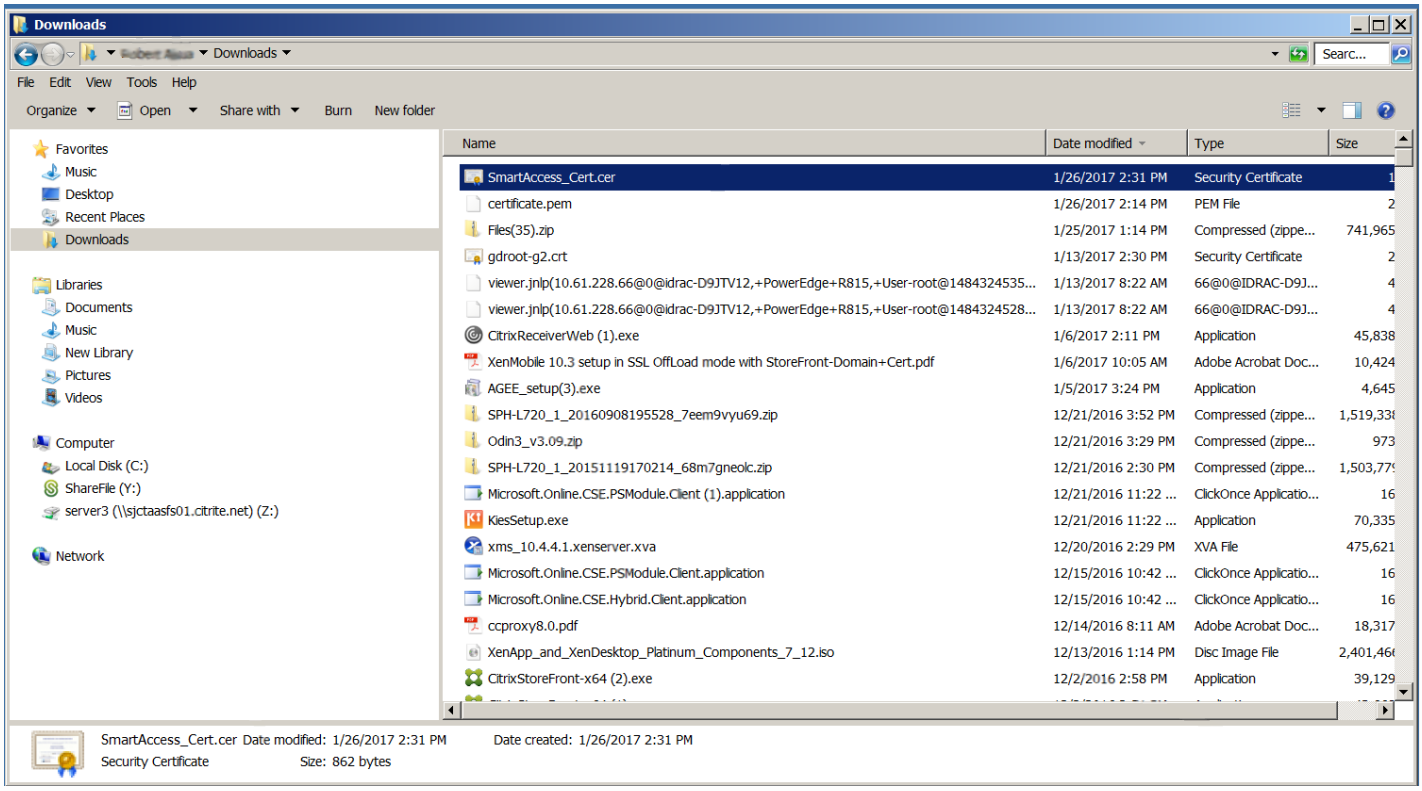


© 1999-2017 Citrix Systems, Inc. All rights reserved.

12. Revise suas seleções e clique em **Concluir**. Clique em **OK** para ignorar a janela de confirmação.



13. Localize o certificado no diretório de download. Observe que o certificado está no formato CER.

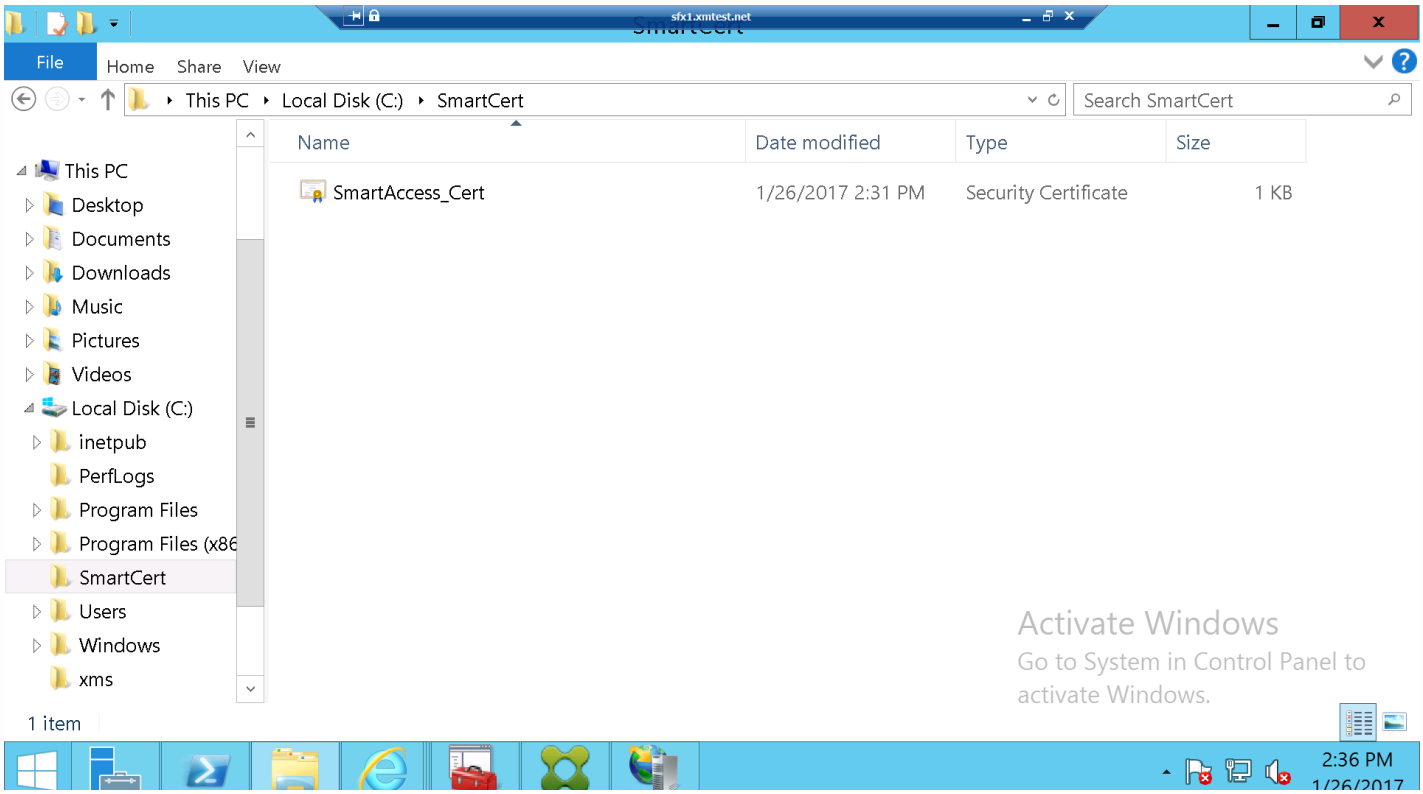


Copie o certificado para o Servidor StoreFront

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. No servidor StoreFront, crie uma pasta chamada **SmartCert**.

2. Copie o certificado para a pasta **SmartCert**.

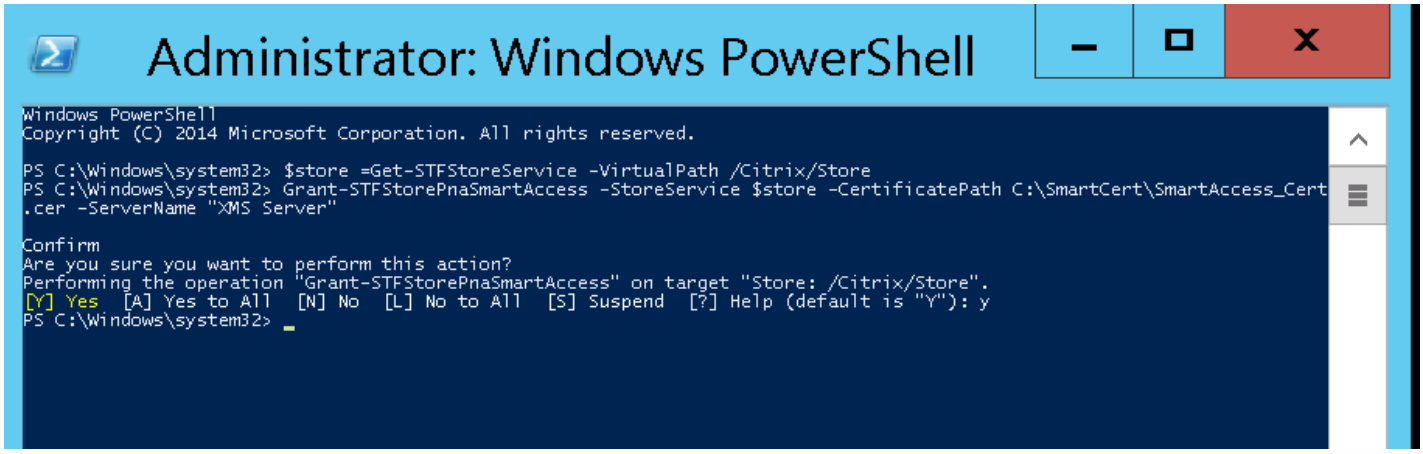


Configure o certificado no repositório do StoreFront

No servidor StoreFront, execute este comando do PowerShell para configurar o certificado do XenMobile Server convertido no repositório:

comando COPIAR

```
Grant-STFStorePnaSmartAccess –StoreService $store –CertificatePath “C:\xms\xms.cer” –ServerName “XMS server”
```



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Se não houver certificados existentes no repositório do StoreFront, execute este comando do PowerShell para revogá-los:

comando COPIAR

```
Revoke-STFStorePnaSmartAccess –StoreService $store –All
```

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:

comando COPIAR

```
$store = Get-STFStoreService –VirtualPath /Citrix/Store

Revoke-STFStorePnaSmartAccess –StoreService $store –ServerName “My XM Server”
```

- Revogar por impressão digital:

comando COPIAR

```
$store = Get-STFStoreService –VirtualPath /Citrix/Store

Revoke-STFStorePnaSmartAccess –StoreService $store –CertificateThumbprint “1094821dec7834d5d42 bb456329efe4fca86c60b”
```

- Revogar por objeto de servidor:

comando COPIAR

© 1999-2017 Citrix Systems, Inc. All rights reserved.

```
$store = Get-STFStoreService –VirtualPath /Citrix/Store

$access = Get-STFStorePnaSmartAccess –StoreService $store

Revoke-STFStorePnaSmartAccess –StoreService $store –SmartAccess $access.AccessConditionsTrusts[0]
```

Configure a política SmartAccess para o XenApp e o XenDesktop

Para adicionar a política SmartAccess necessária ao grupo de entrega que fornecer o aplicativo HDX:

1. No XenApp e no XenDesktop Server, abra o Citrix Studio.

2. Selecione **Grupos de entrega** no painel de navegação do Studio.

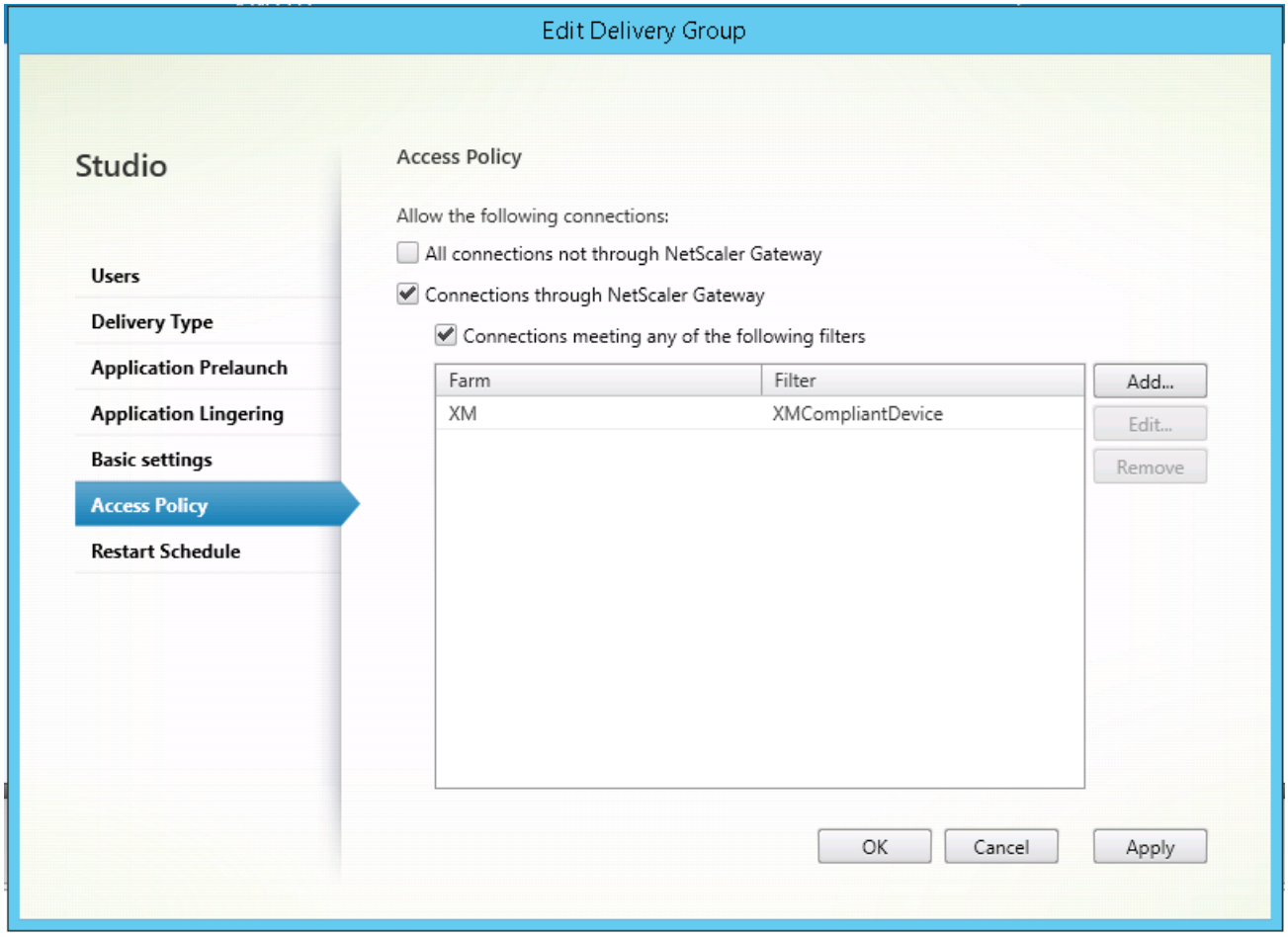
3. Selecione um grupo de entrega para o aplicativo ou os aplicativos aos quais você deseja controlar o acesso. Em seguida, selecione **Editar grupo de entrega** no painel **Ações**.

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**.

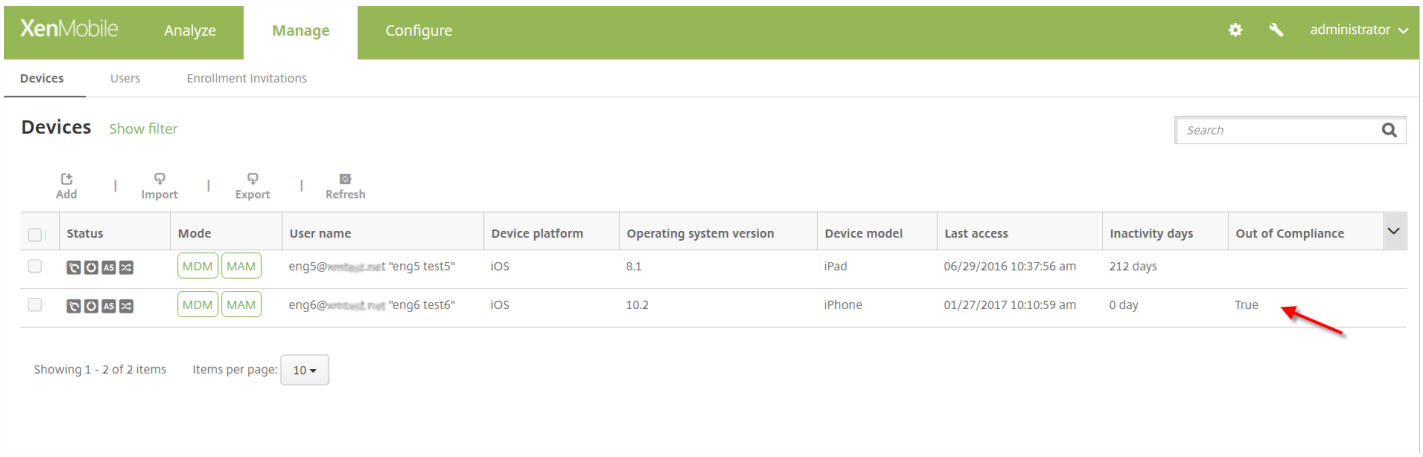
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.



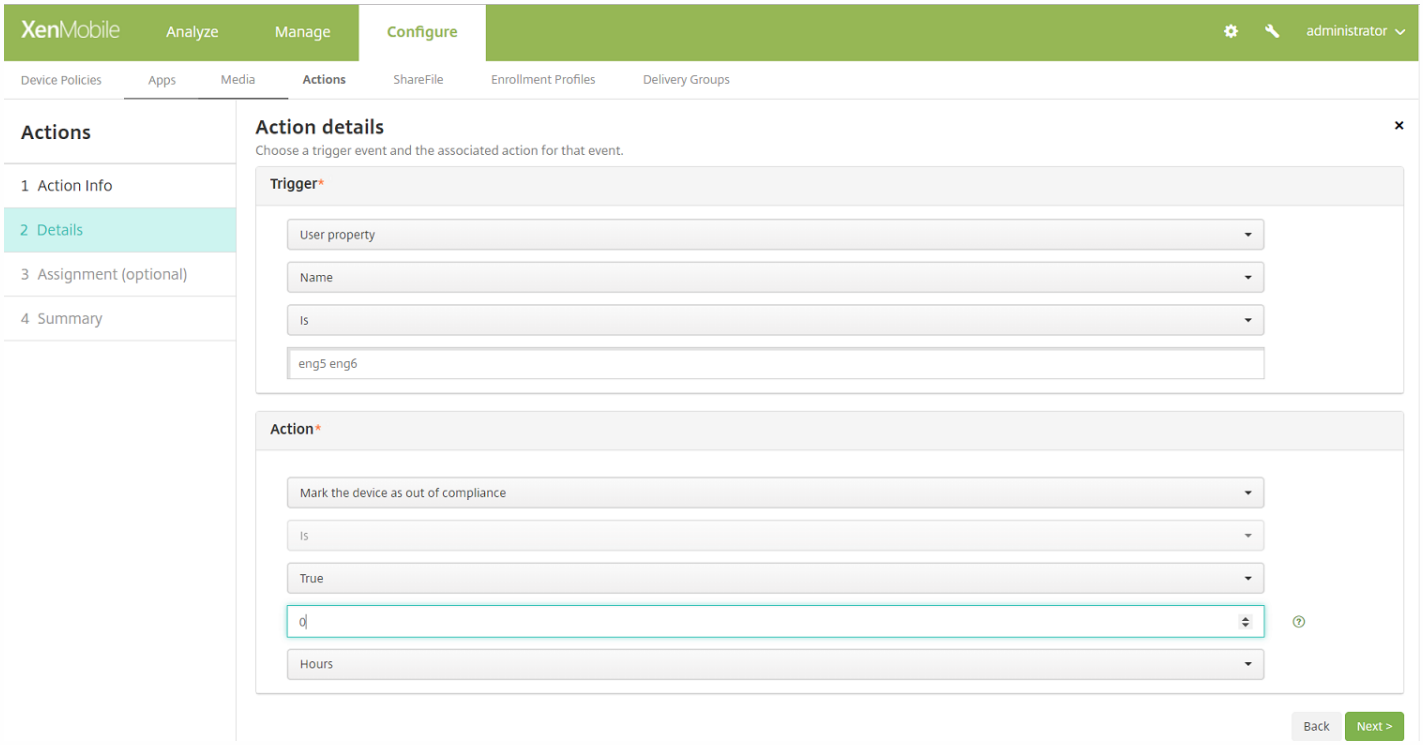
1. No console XenMobile, clique em **Configurar > Ações**. A página **Ações** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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**.



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 **É**.
- 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.

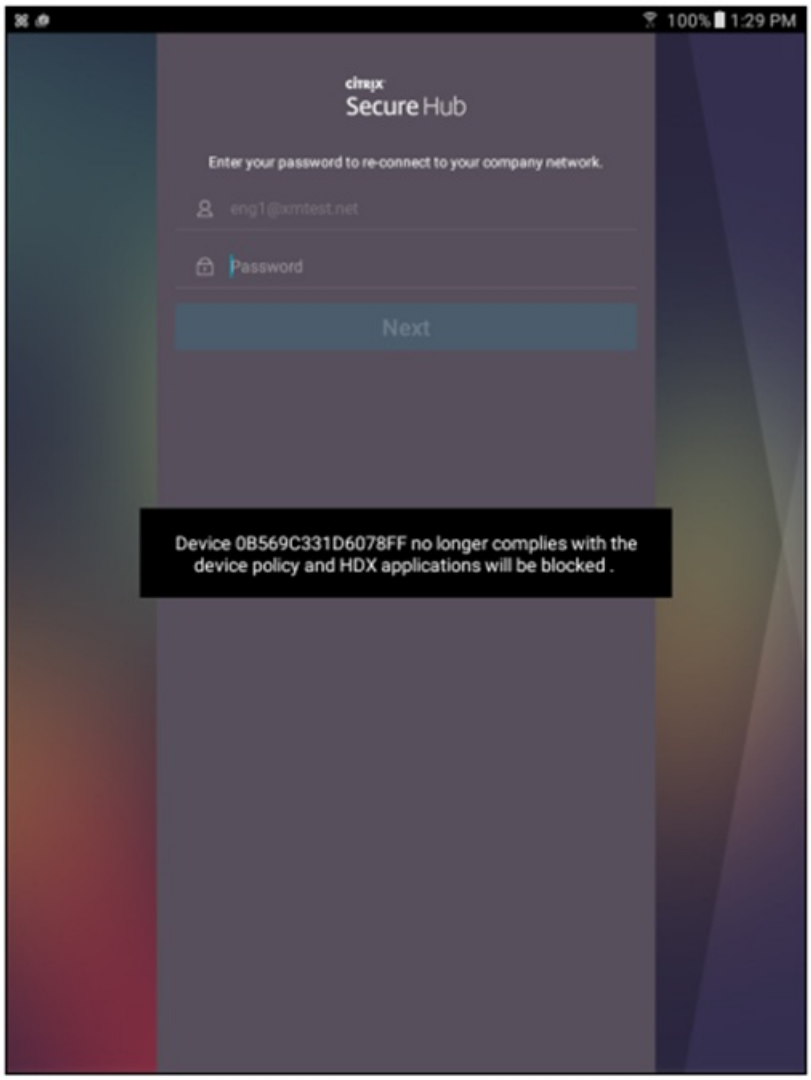
9. Clique em **Avançar** e em **Salvar**.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

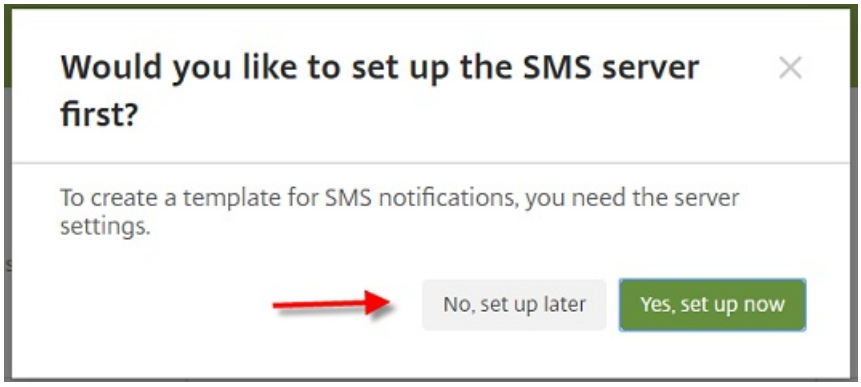
1. No console XenMobile, clique no ícone de engrenagem no canto superior direito do console. A página **Configurações** é exibida.

2. Clique em **Modelos de notificação**. A página **Modelos de notificação** é exibida.

3. Clique em **Adicionar** para acrescentar à página **Modelos de notificação**.

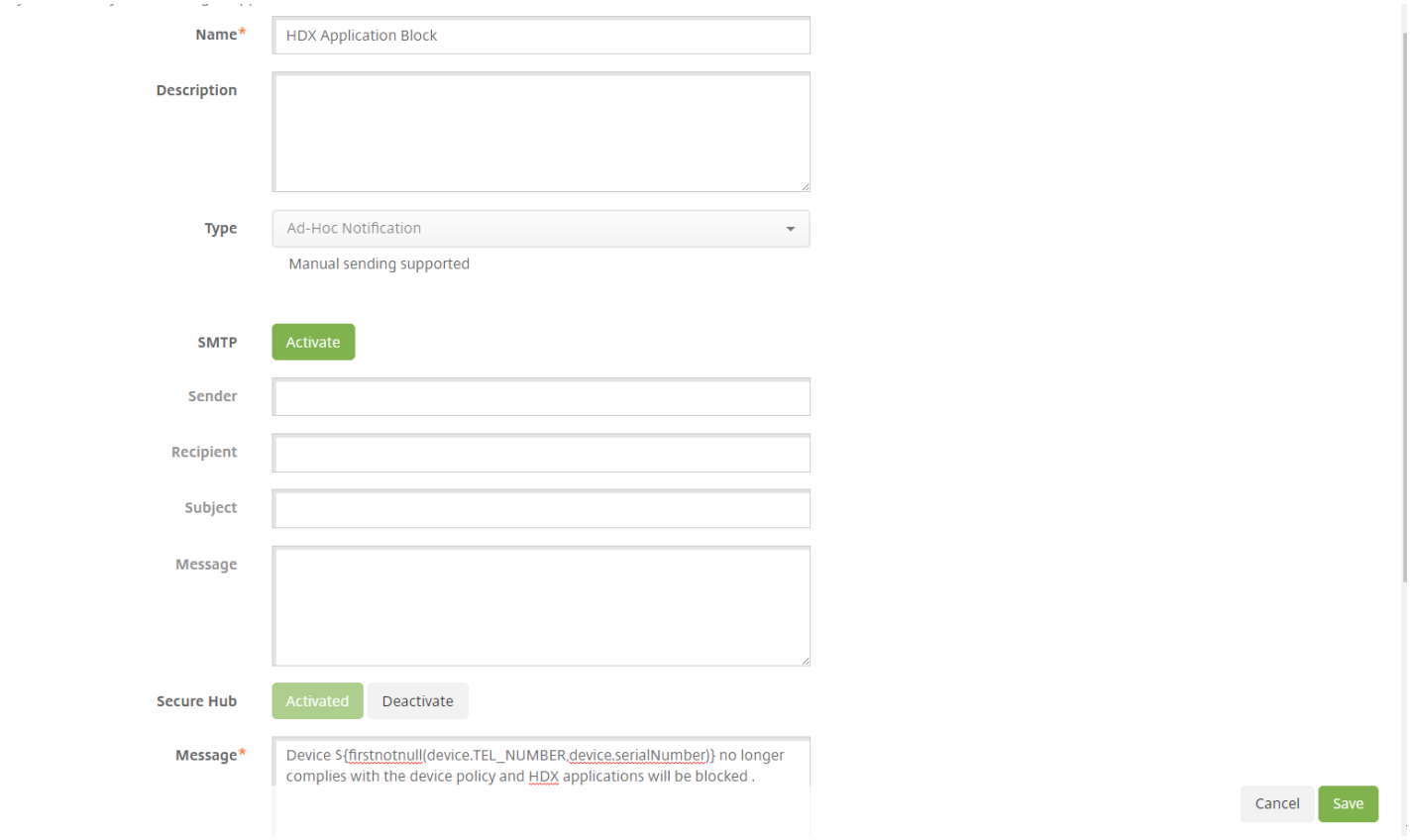
4. Quando solicitado a configurar primeiro o servidor SMS, clique em **Não, configurar mais tarde**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.



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:

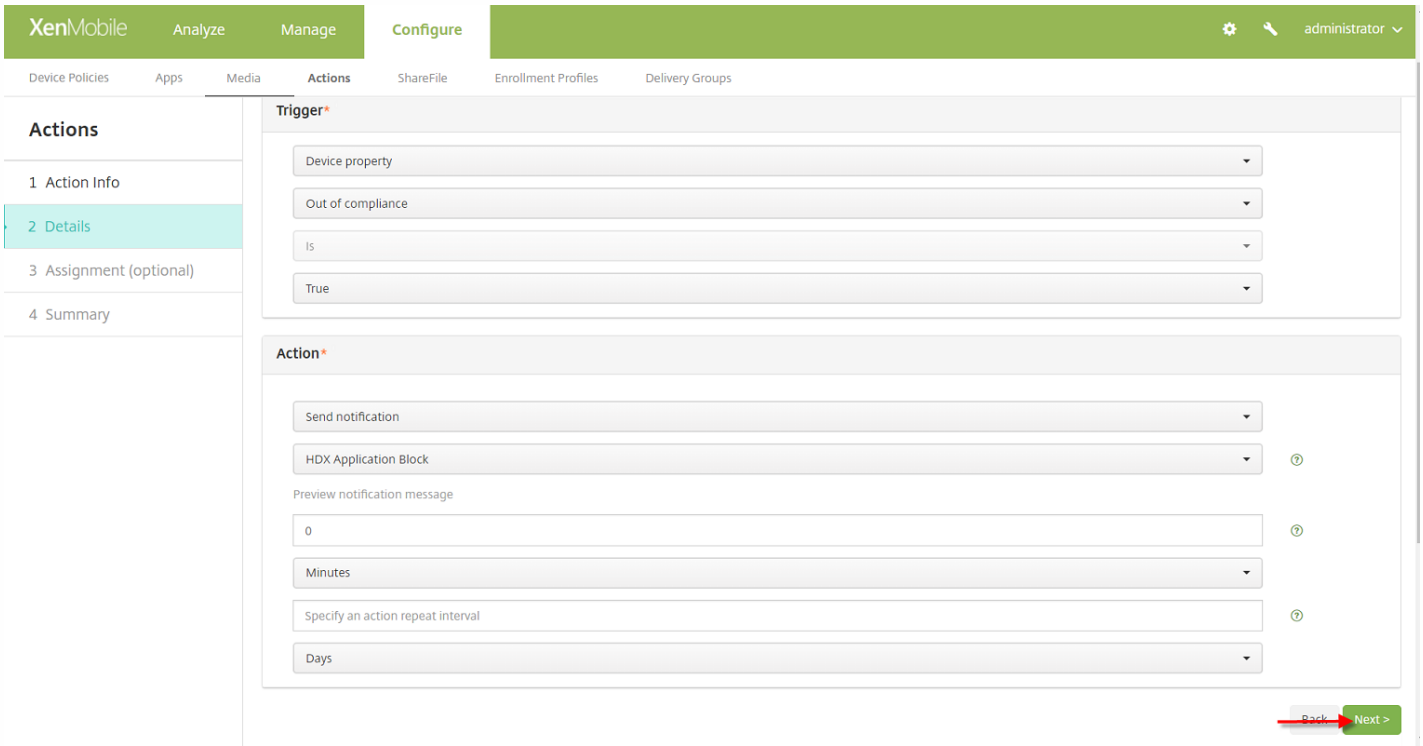
© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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 **É**.
- Escolha **True**.



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

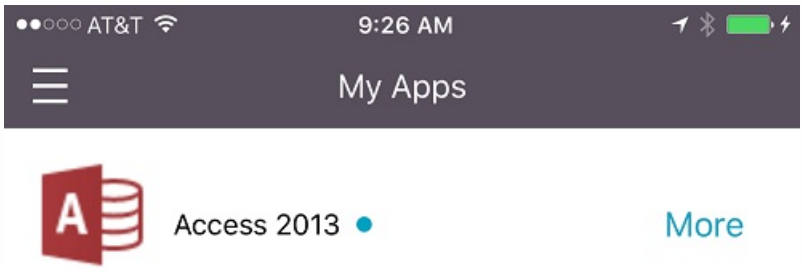
Os usuários podem acessar aplicativos HDX novamente depois que o dispositivo é recolocado em conformidade:

1. No dispositivo, vá até a loja do Secure Hub para atualizar os aplicativos na loja.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Adicionar mídia

Feb 21, 2018

Você adiciona mídia ao XenMobile para poder implantar a mídia em dispositivos de usuário. Você pode usar o XenMobile para implantar iBooks que obtém por meio do Programa Apple Volume Purchase (VPP).

Depois de configurar uma conta VPP no XenMobile, seus livros comprados e gratuitos aparecem em **Configurar > Mídia**. Nas páginas de **Mídia**, você configura iBooks para implantação em dispositivos iOS escolhendo grupos de entrega e especificando regras de implantação.

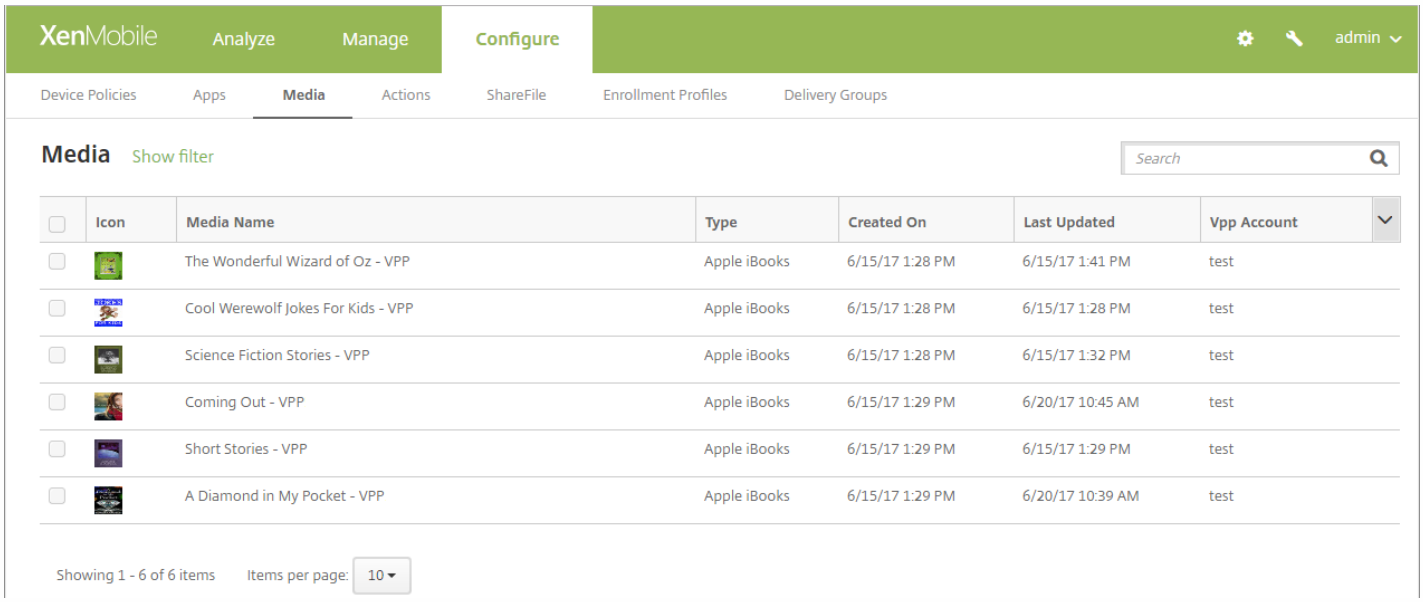
A primeira vez que um usuário recebe um iBook e aceita a licença VPP, os livros implantados são instalados no dispositivo. Os livros aparecem no aplicativo Apple iBook. Você não pode desassociar a licença do livro do usuário ou remover o livro do dispositivo. O XenMobile instala iBooks como mídia necessária. Se um usuário exclui um livro instalado do seu dispositivo, o livro permanece no aplicativo iBook, pronto para download.

Pré-requisitos

- Dispositivos iOS (versão mínima iOS 8)
- Configurar o VPP do iOS no XenMobile, conforme descrito em Volume Purchase Plan do iOS.

Configurar iBooks

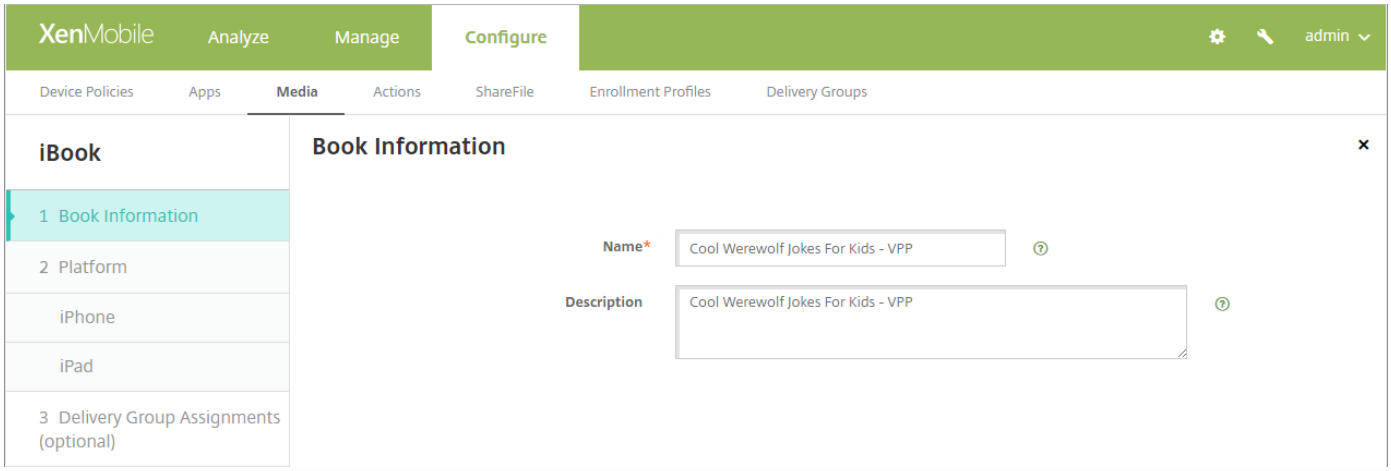
Os iBooks obtidos através do VPP aparecem na página **Configurar > Mídia**.



Para configurar um iBook para implantação:

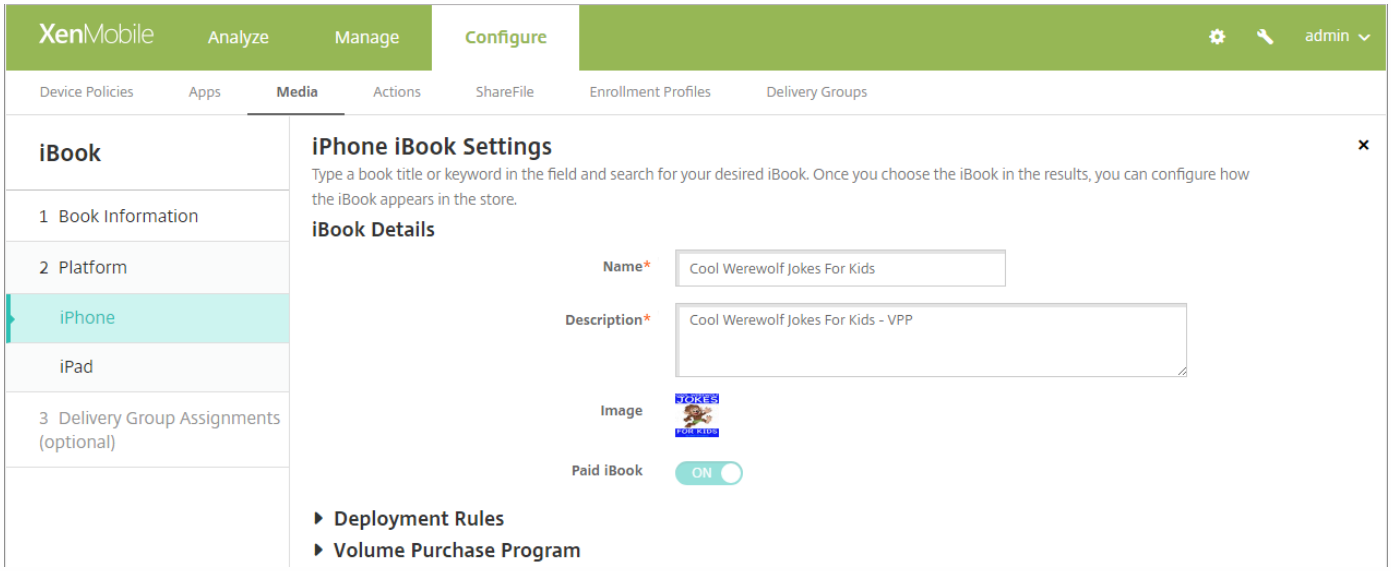
1. Em **Configurar > Mídia**, selecione um iBook e clique em **Editar**. A página **Informações do livro** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



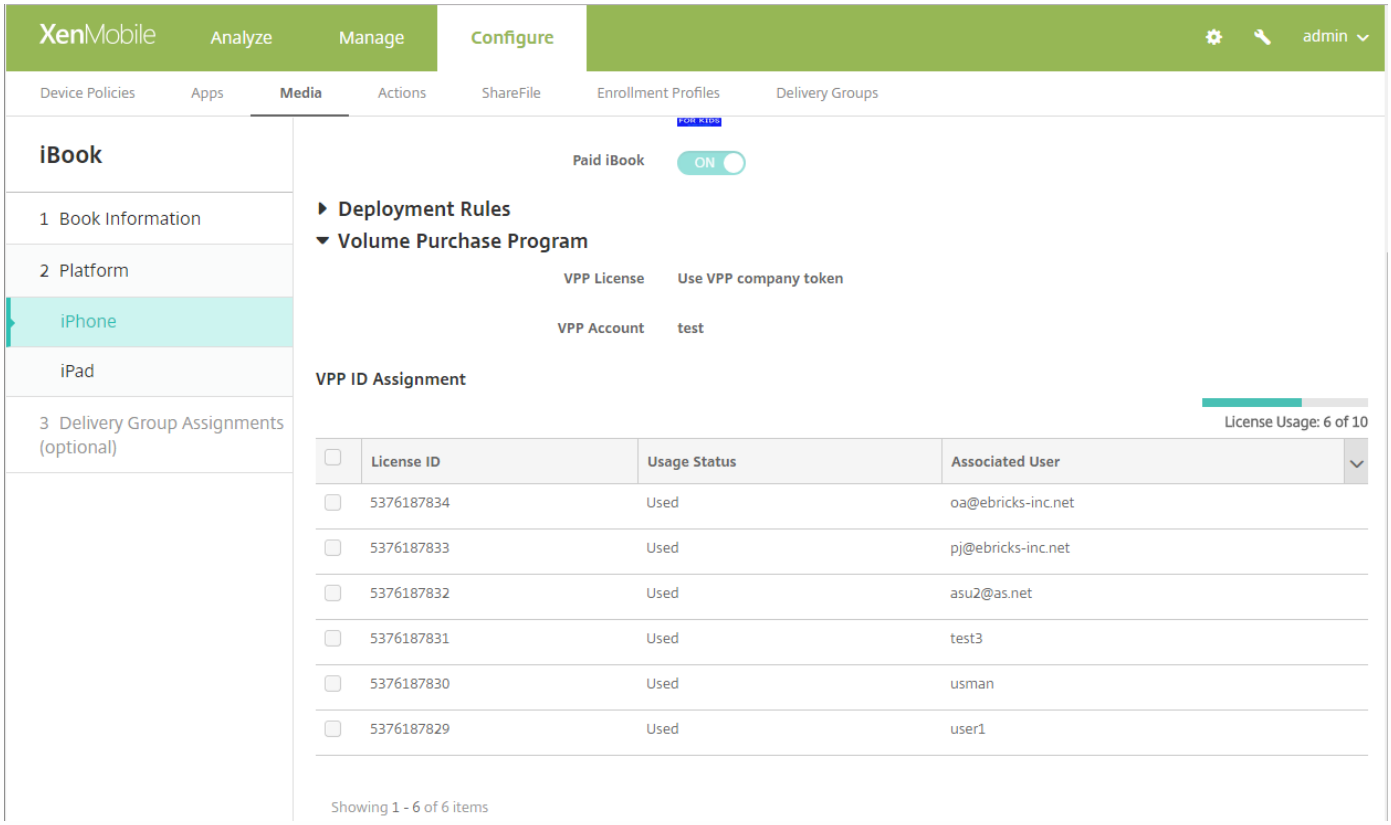
O **Nome** e **Descrição** são exibidos somente no console XenMobile e logs.

2. Nas páginas de **Configurações iPhone iBook** e **Configurações iPad iBook**: ainda que possa opcionalmente alterar o nome e a descrição do iBook, a Citrix recomenda que você não altere essas configurações. A imagem é para sua informação e não é editável. **iBook pago** indica que um iBook é adquirido através do VPP.

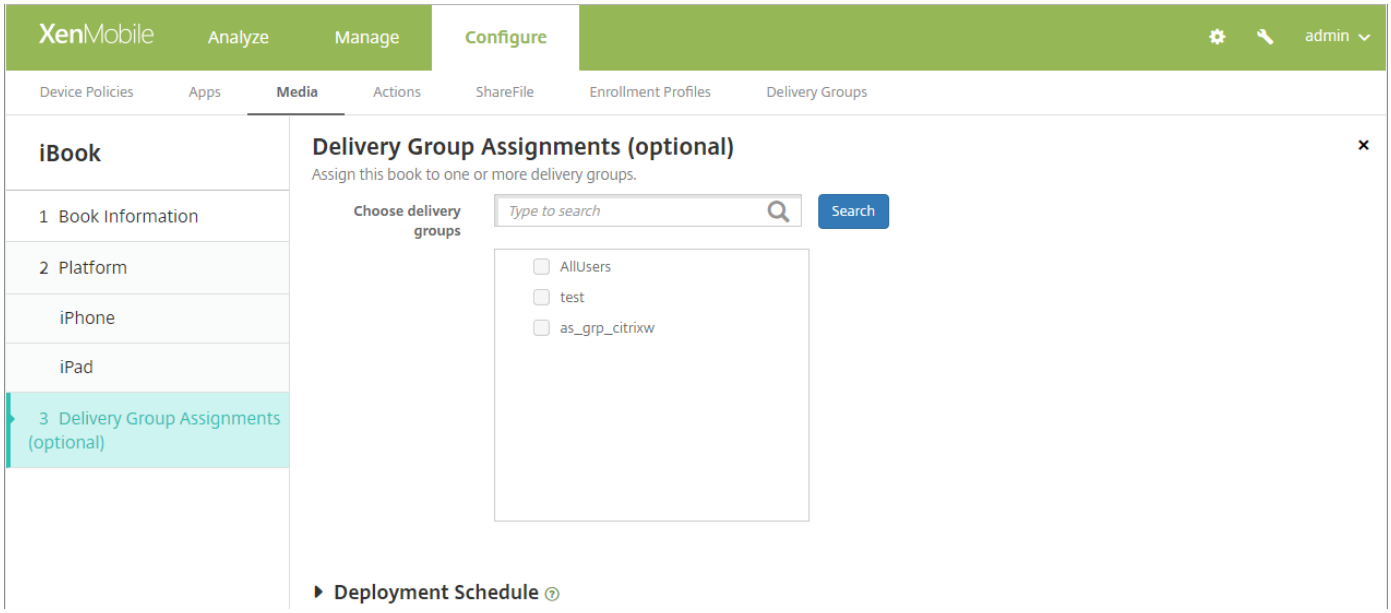


Você também pode especificar regras de implantação ou visualizar informações de VPP.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

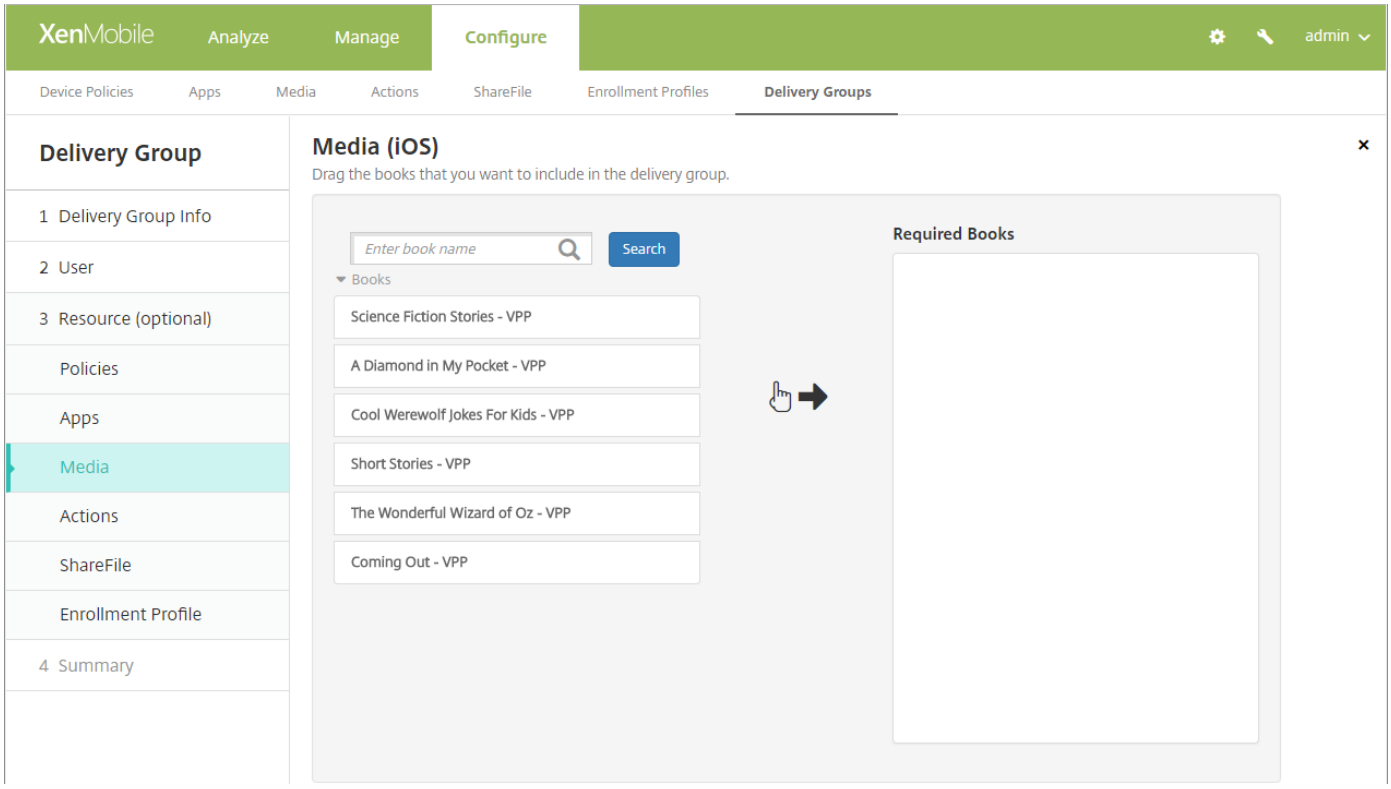


3. Opcionalmente, atribua o iBook aos grupos de entrega e defina um cronograma de implantação.

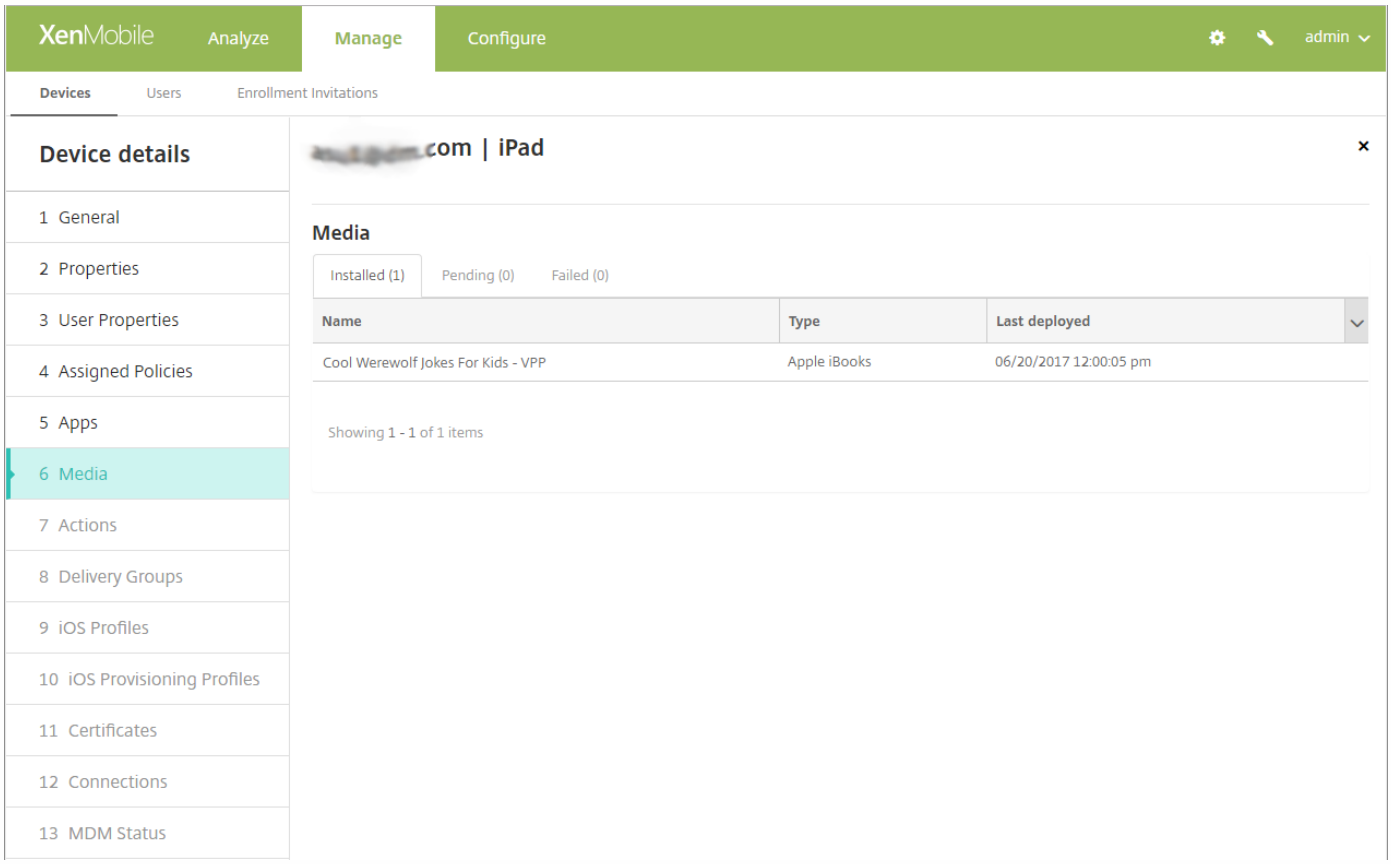


Você também pode atribuir iBooks a grupos de entrega na guia **Mídia** em **Configurar > Grupos de entrega**. Atualmente, o XenMobile suporta apenas a implantação de livro necessária.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



4. Use a guia **Mídia** em **Gerenciar > Dispositivos** para visualizar o status da implantação.



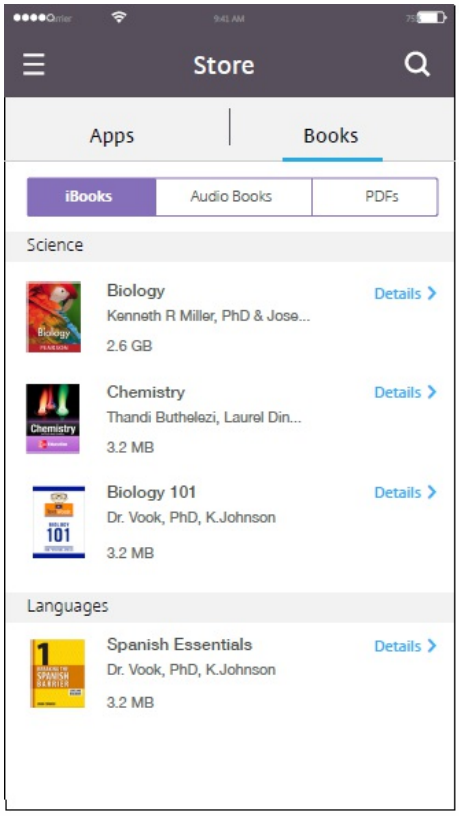
Nota

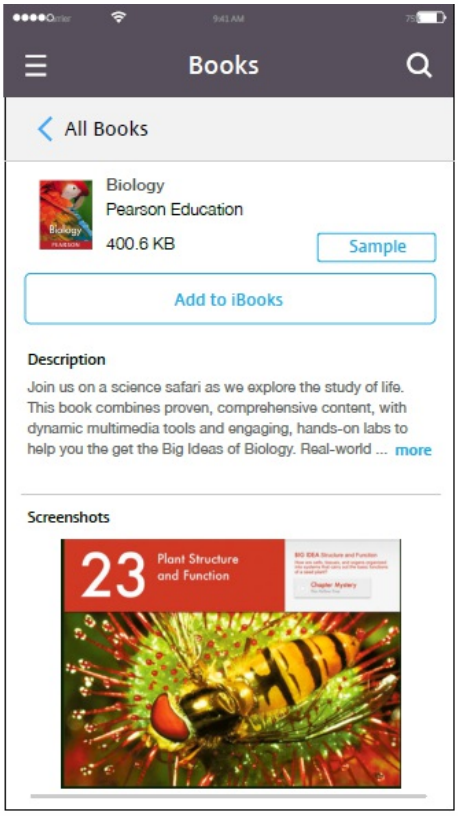
Na página **Configurar > Mídia**, se você selecionar um livro e clicar em **Excluir**, o XenMobile remove o livro da lista. No entanto,

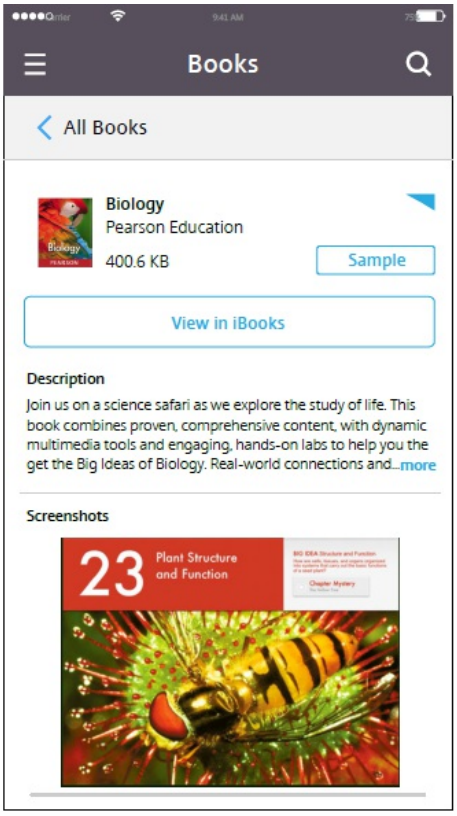
© 1999-2017 Citrix Systems, Inc. All rights reserved.

na próxima vez que o XenMobile se sincronizar com o VPP, o livro reaparecerá na lista, a menos que tenha sido removido do VPP. A exclusão de um livro da lista não remove o livro dos dispositivos.

Os iBooks são exibidos nos dispositivos dos usuários, como mostrado nestes exemplos.







© 1999-2017 Citrix Systems, Inc. All rights reserved.

Implantar recursos

Feb 21, 2018

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 conhecida como a *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. Dessa forma, você pode reavaliar os dispositivos e implantar políticas, aplicativos, mídias e ações. 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 é compatível somente com o modo 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, a políticas, aplicativos, mídias, 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 especificar 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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

um determinado valor.

- **Cronograma de implantação:** o XenMobile usa o cronograma de implantação que você especificar 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

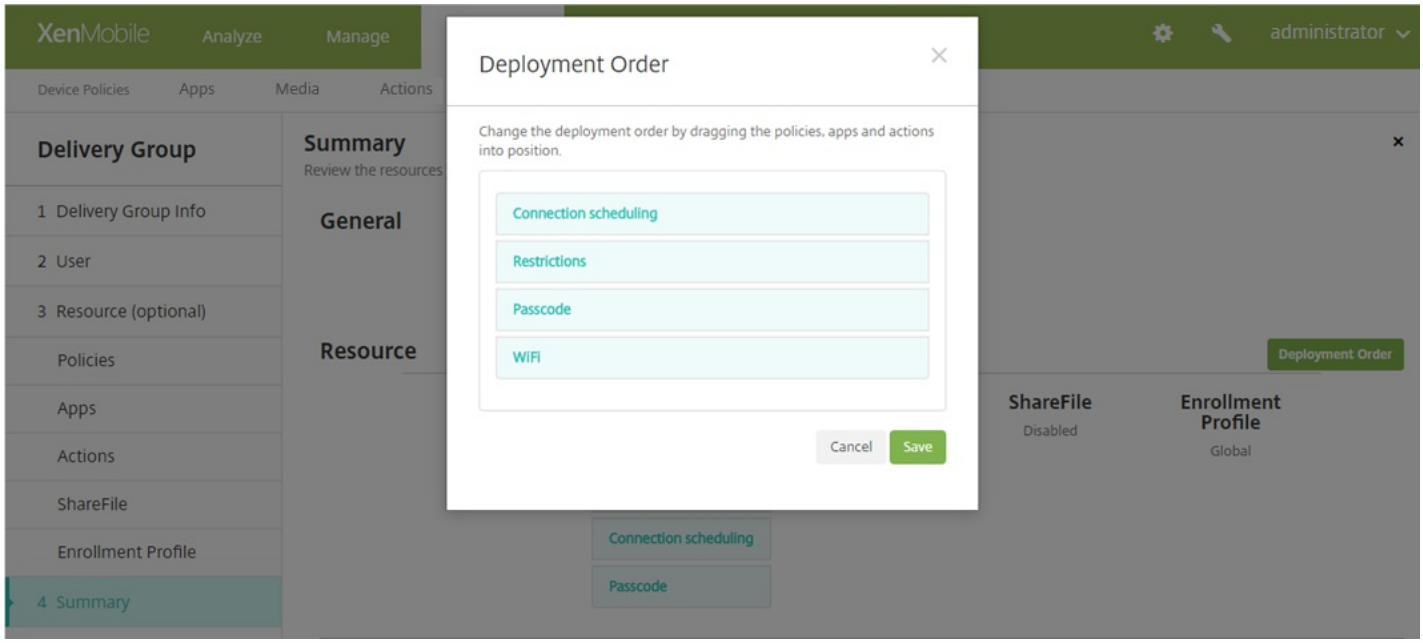
c. Durante a classificação, se uma ordem de implantação definida pelo usuário for especificada para os recursos de um grupo de entrega, mantenha essa ordem. Caso contrário, classifique os recursos no grupo de entrega por nome do recurso.

d. Se o mesmo recurso aparecer 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 ao 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**.



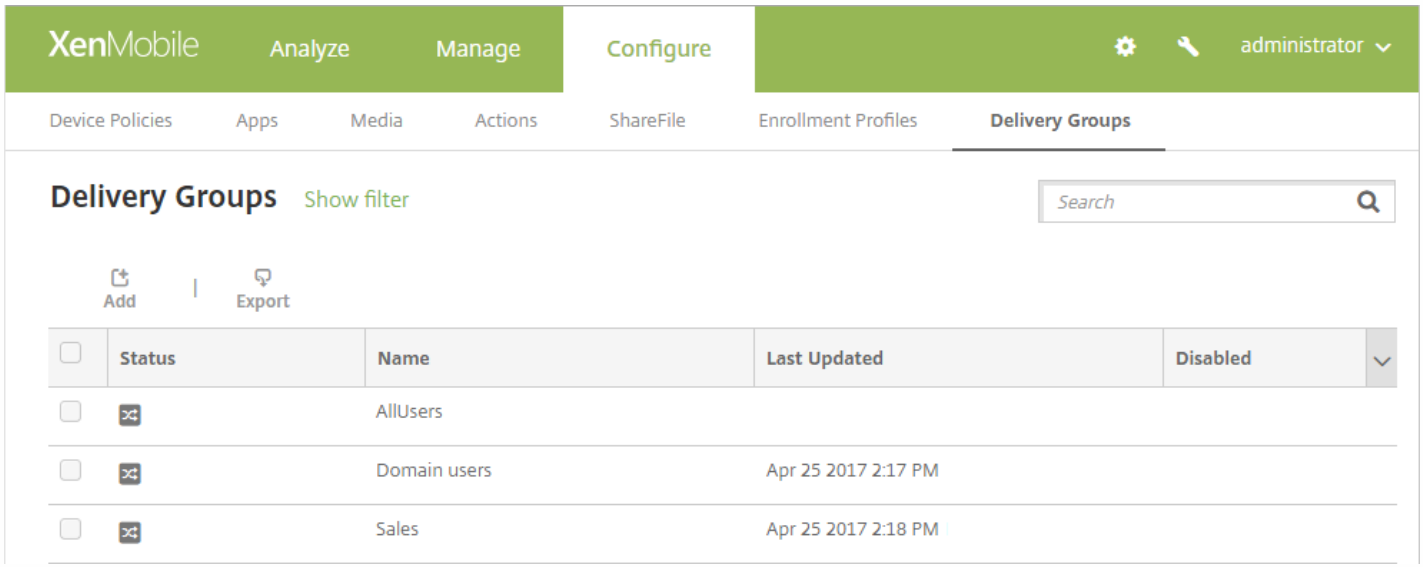
Se o algoritmo de cálculo tiver classificado grupos de implantação apenas por nome, o XenMobile realizará a implantação nessa ordem, começando com o grupo de entrega Gerentes de conta 1:**WiFi**, **Código secreto**, **Agendamento de conexão** e **Restrições**. O XenMobile ignoraria **Código secreto** 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 ignora as políticas de **WiFi** 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.

Para adicionar um grupo de entrega

© 1999-2017 Citrix Systems, Inc. All rights reserved.

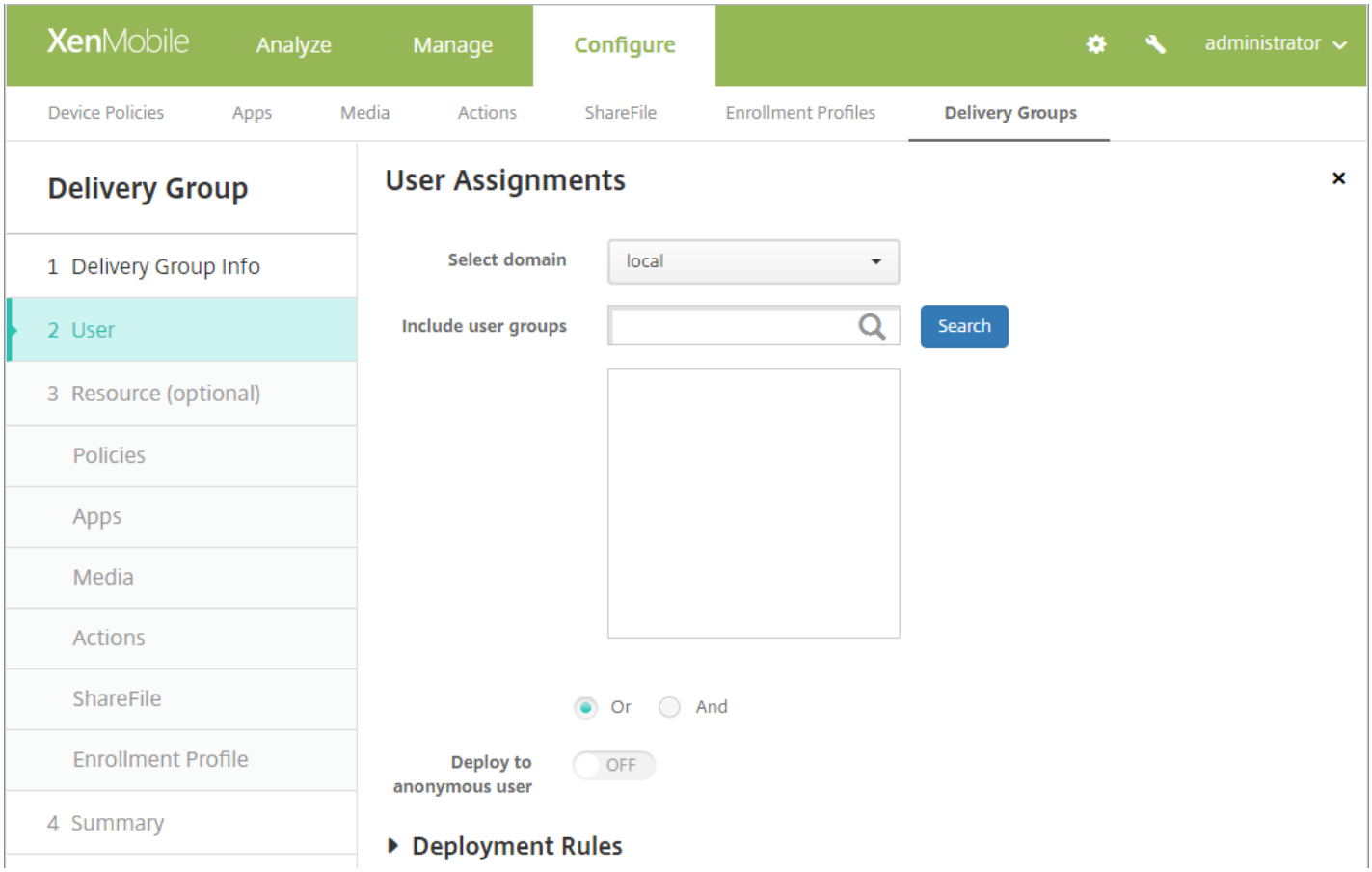
1. No console XenMobile, clique em **Configurar > Grupos de entrega**. A página **Grupos de entrega** é exibida.



2. Na página **Grupos de entrega**, clique em **Adicionar**. Quando a página **Informações de grupo de entrega** for exibida, insira as seguintes informações:

- **Nome**: digite um nome descritivo para o grupo de entrega.
- **Descrição**: digite uma descrição opcional para o grupo de entrega.

3. Clique em **Avançar**. A página **Atribuições do usuário** é exibida.



4. Defina estas configurações:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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.

  Nota: usuários não autenticados são usuários que você não tem permissão para autenticar, mas cujos dispositivos se conectam ao XenMobile de qualquer maneira.

5. Configure as regras de implantação

a. Expanda **Regras de implantação** e defina estas configurações: a guia **Base** é exibida por padrão.

- Nas listas, clique nas opções para especificar 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 quiser adicionar condições. Você pode adicionar quantas condições desejar.

b. Clique na guia **Avançado** para combinar as regras com opções boolianas. As condições que você escolheu na guia **Base** são exibidas.

c. Você pode usar a lógica booliana mais avançada para combinar, editar ou adicionar regras.

- Clique em **AND**, **OR** ou **NOT**.
- Para adicionar a condição à regra, nas listas, selecione as condições que você deseja adicionar à regra e, em seguida, clique no sinal de mais (+) no lado direito.

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** novamente se quiser adicionar condições.

d. Clique em **Avançar**. A página **Recursos do 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nota: para ignorar um recurso, em **Recursos (opcional)**, clique no recurso que você deseja adicionar e siga as etapas para esse recurso.

Para adicionar recursos opcionais aos grupos de entrega

Você pode adicionar recursos opcionais aos grupos de entrega para:

- Aplicar políticas específicas
- Fornecer aplicativos obrigatórios e opcionais
- Adicionar ações automáticas
- Habilitar o ShareFile para logon único para dados e conteúdo

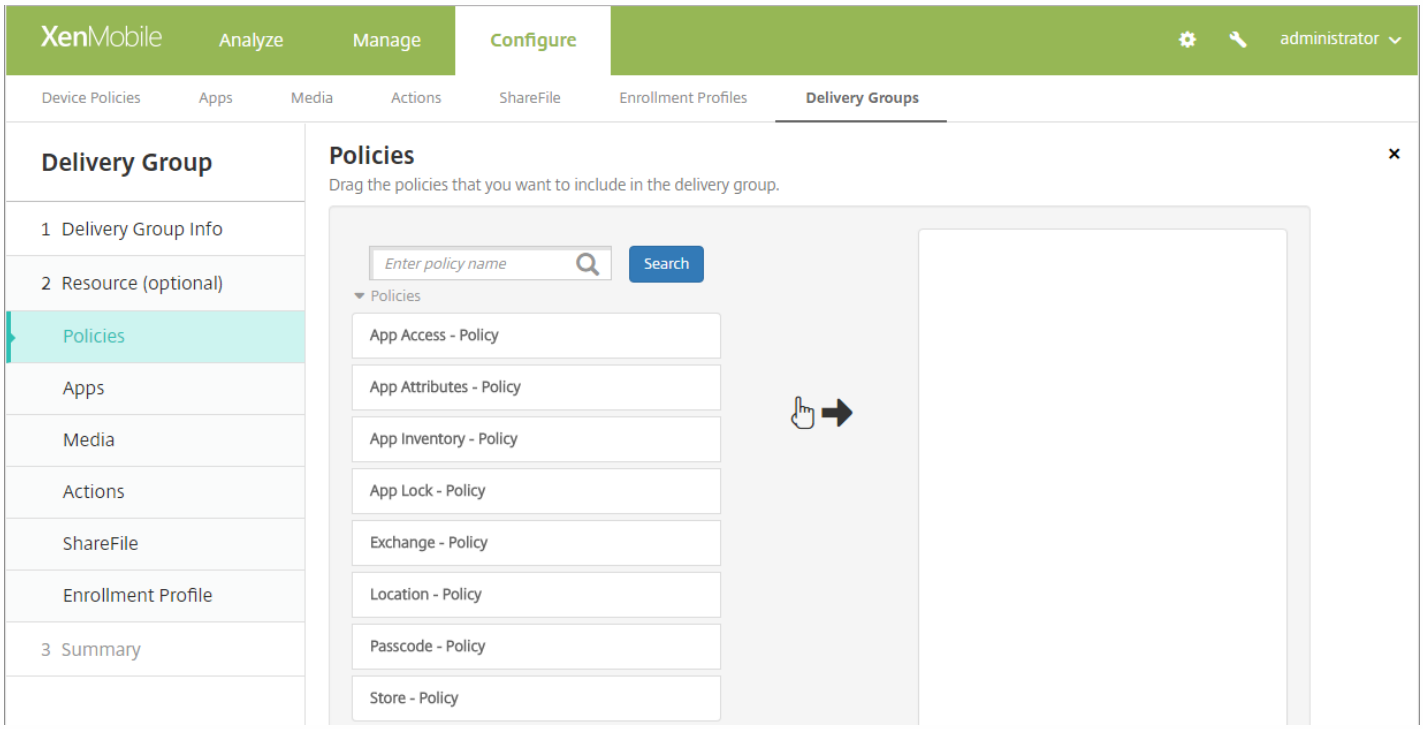
As seções a seguir descrevem como adicionar políticas, aplicativos e ações, além de como ativar o ShareFile. Você pode adicionar qualquer, todos ou nenhum desses recursos ao grupo de entrega. Para ignorar a adição de um recurso, clique em **Resumo** .

Adicionar políticas

1. Para cada política que você desejar 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 um nome completo ou parcial de aplicativo na caixa de pesquisa e, em seguida, clique em **Pesquisar**.
- Clique na política que deseja adicionar e arraste-a até a caixa à direita.

Nota: 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.

É muito provável que, em um ambiente típico, vários grupos de entrega sejam atribuído a um único usuário, com os seguintes

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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:

Adicionar aplicativos

1. Para cada aplicativo que você desejar adicionar, faça o seguinte:

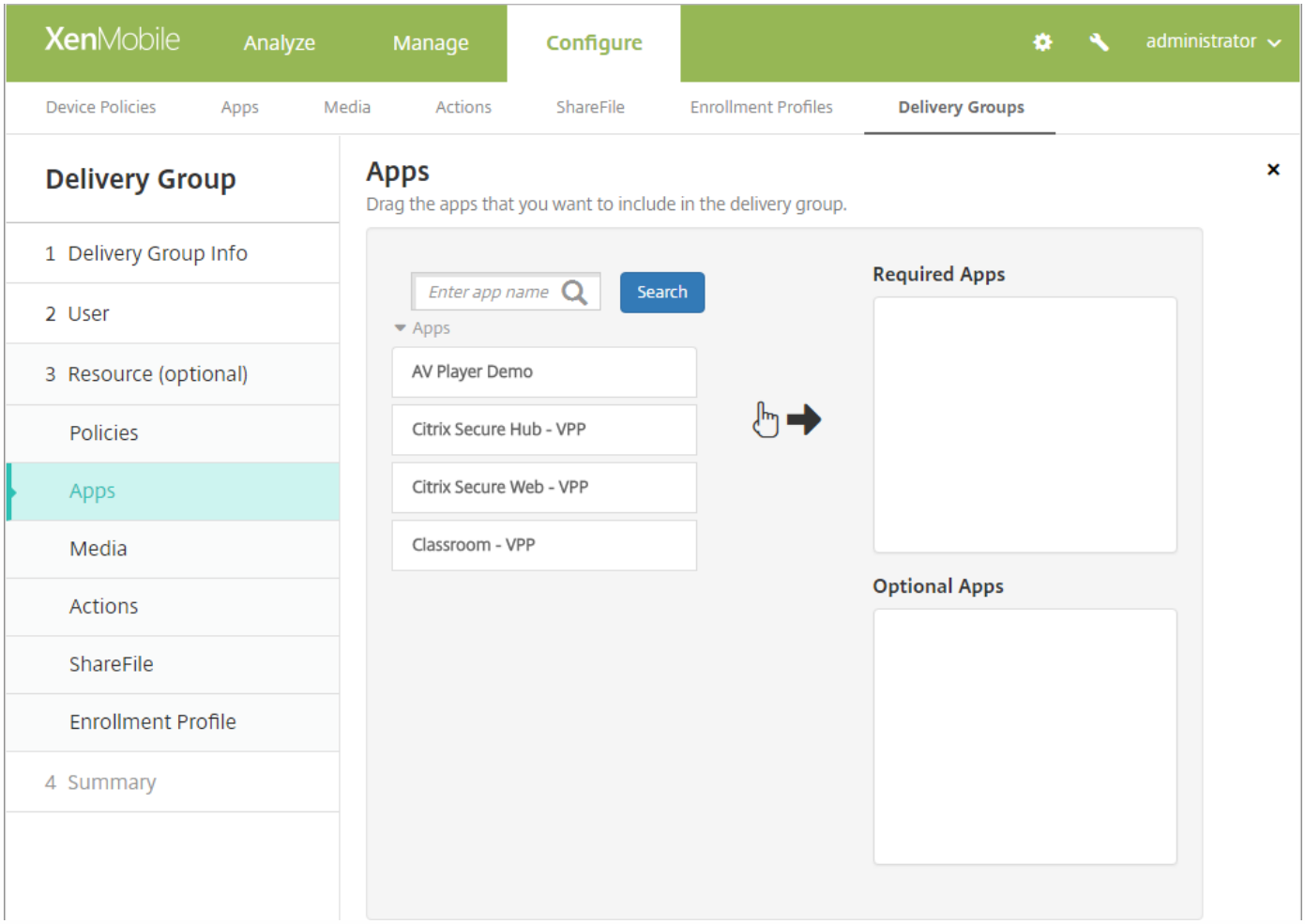
   - Role pela lista de aplicativos disponíveis para localizar o aplicativo que você deseja adicionar.
   - Ou, para limitar a lista de aplicativos, digite um nome completo ou parcial de aplicativo na caixa de pesquisa e, em seguida, clique em **Pesquisar**.
   - Clique no aplicativo que você deseja adicionar 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 necessários, incluindo como habilitar o recurso, consulte Sobre aplicativos necessários e opcionais.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Para remover um aplicativo, clique no **X** ao lado do nome do aplicativo na caixa à direita.

2. Clique em **Avançar**. A página **Mídias** é exibida.

Adicionar mídia

1. Para cada livro que você desejar 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 um nome completo ou parcial de livro na caixa de pesquisa e, em seguida, clique em **Pesquisar**.
   - Clique no livro que você desejar adicionar e arraste-o para a caixa de **Livros necessários**.

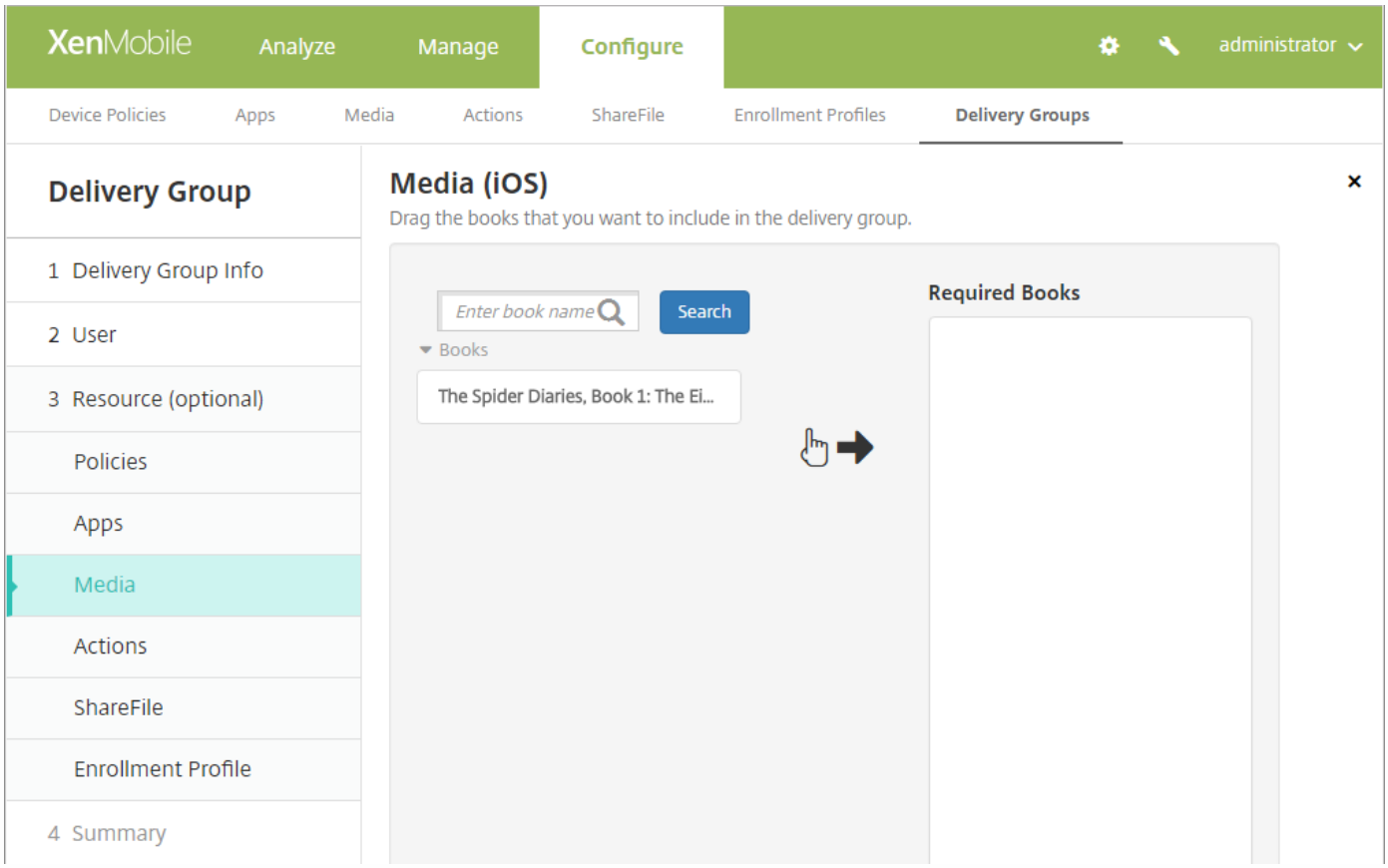
   É muito provável que, em um ambiente típico, vários grupos de entrega sejam atribuído a um único usuário, com os seguintes resultados possíveis:

   - 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Etapas de cálculo:



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:

Para livros marcados como necessários, 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.

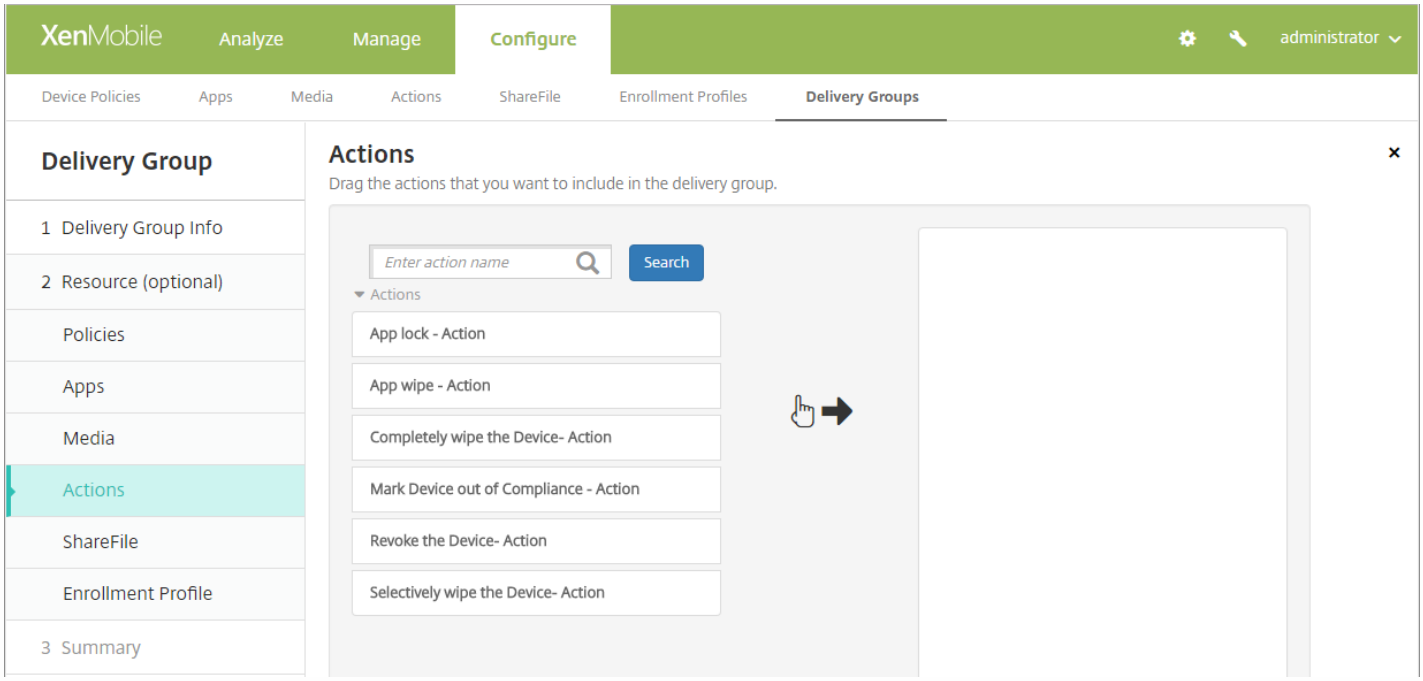
Adicionar ações

1. Para cada ação que você desejar adicionar, faça o seguinte:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Role pela lista de ações disponíveis para localizar o aplicativo que você deseja adicionar.
- Ou, para limitar a lista de ações, digite um nome completo ou parcial de aplicativo na caixa de pesquisa e, em seguida, clique em **Pesquisar**.
- Clique na ação que deseja adicionar e arraste-a até a caixa à direita.

Nota: para remover uma ação, clique no **X** ao lado do nome da ação na caixa à direita.



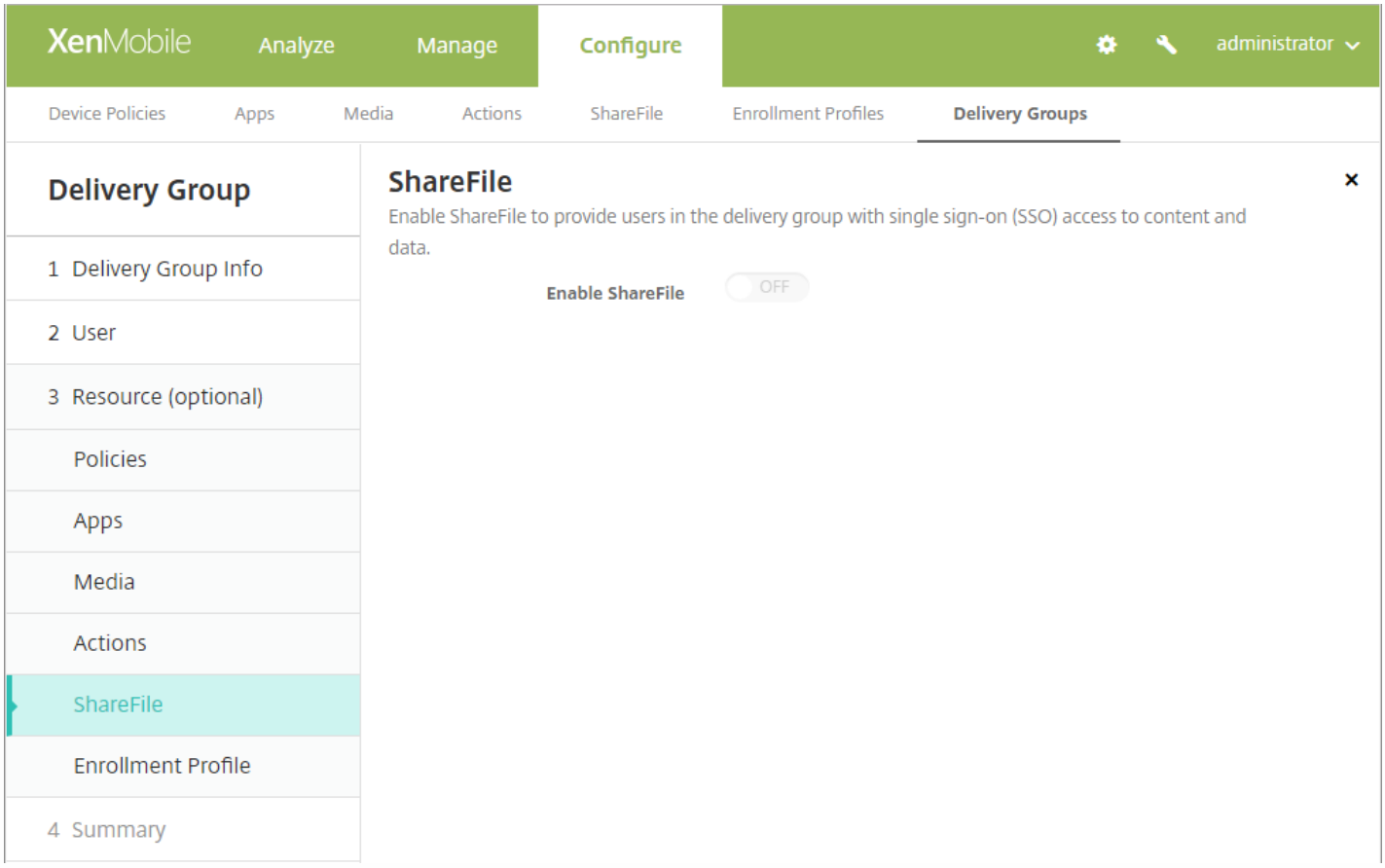
2. Clique em **Avançar**. A página **ShareFile** é exibida.

Aplicar a configuração ShareFile

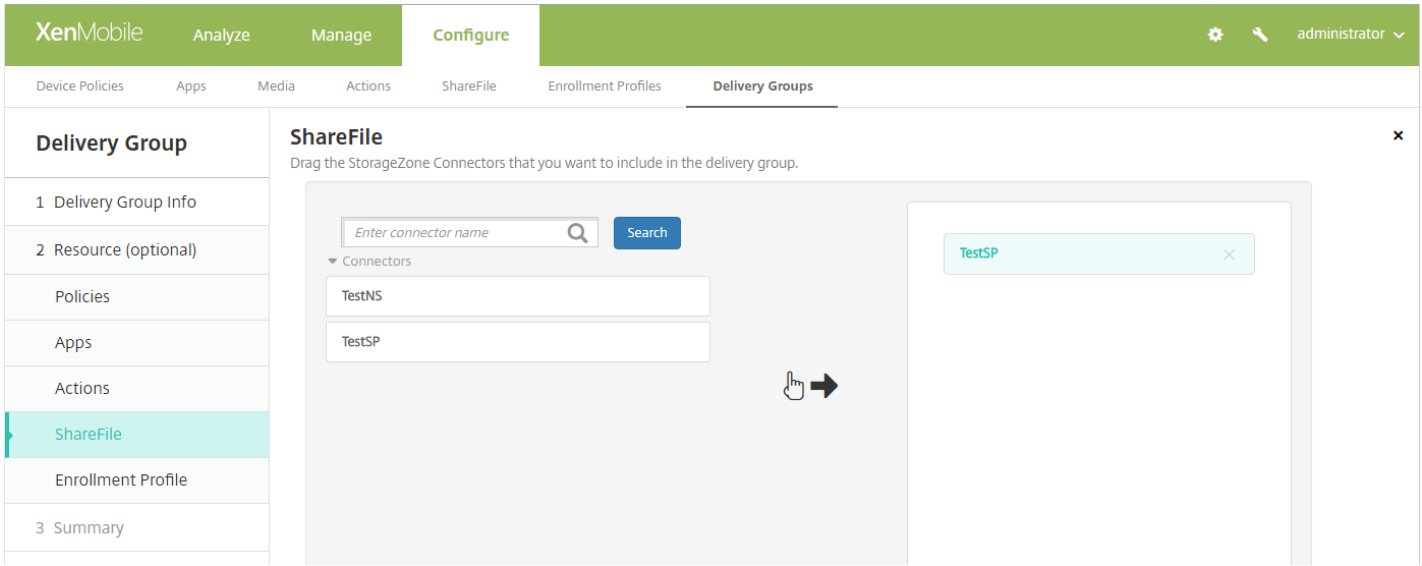
A página ShareFile difere dependendo de você ter configurado o XenMobile (**Configurar > ShareFile**) para o ShareFile Enterprise ou para os StorageZone Connectors.

Se tiver configurado o ShareFile Enterprise para uso com o XenMobile, defina **Ativar ShareFile** como **I** para fornecer de acesso logon único ao grupo de entrega para o conteúdo e os dados do ShareFile.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

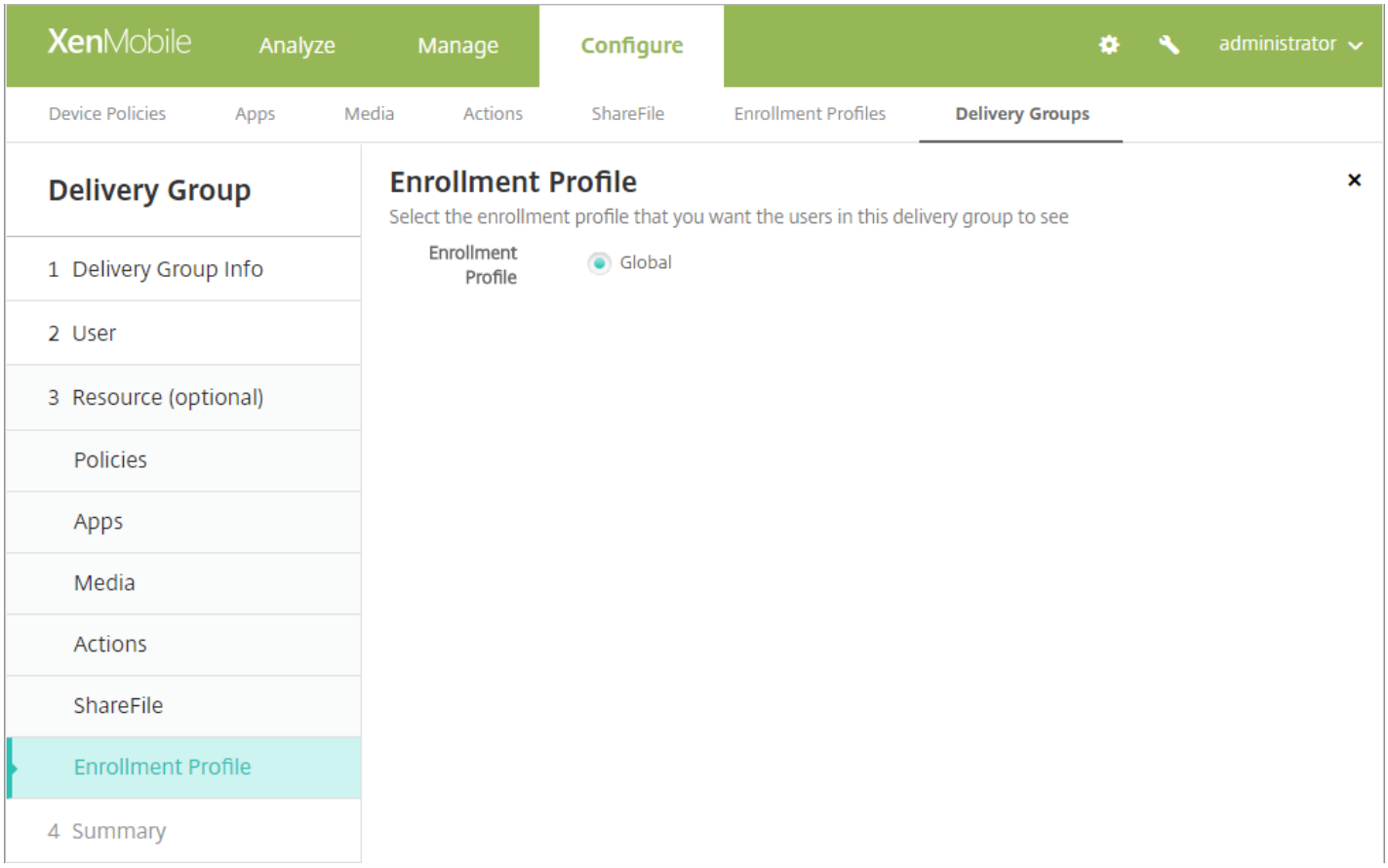


Se você tiver configurado os StorageZone Connectors para uso com o XenMobile, selecione os StorageZone Connectors que devem ser incluídos no grupo de entrega.



Perfil de registro

© 1999-2017 Citrix Systems, Inc. All rights reserved.



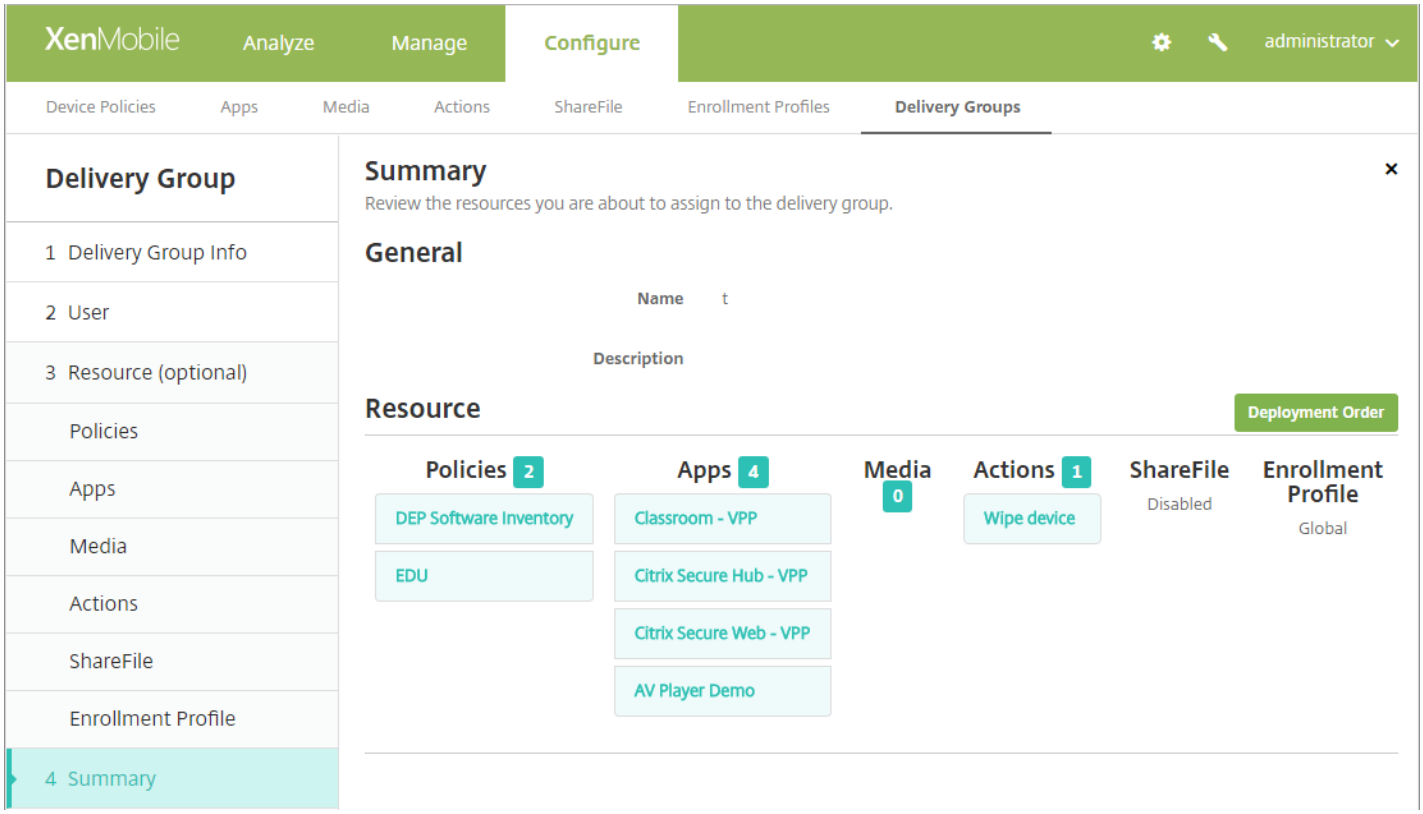
1. Configure esta definição:

- **Perfil de registro**: selecione um perfil de registro. Para criar um perfil de registro, consulte Limite de registro de dispositivos.

2. Clique em **Avançar**. A página **Resumo** é exibida.

Revisar as opções configuradas e alterar a ordem de implantação

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.

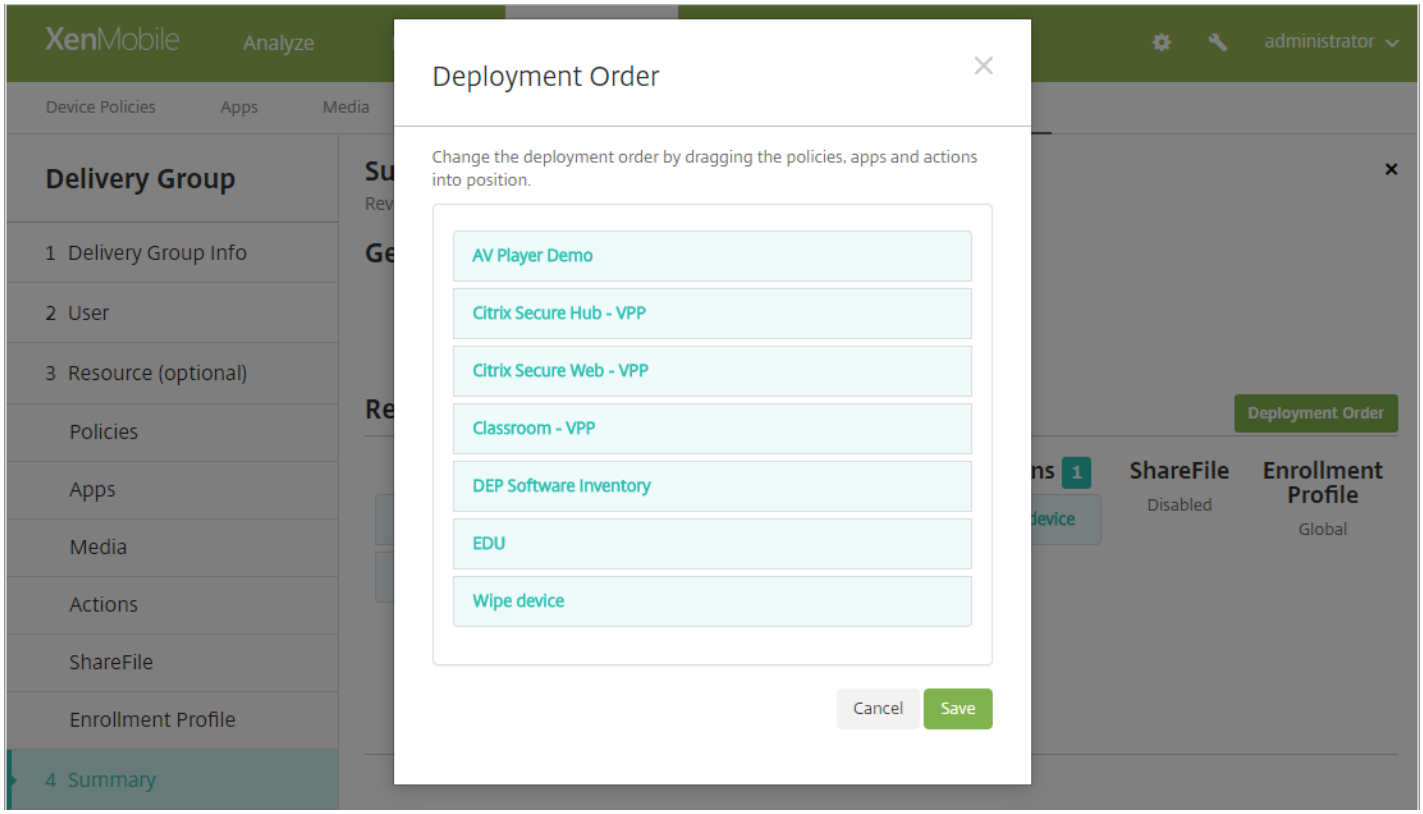
2. Clique em **Ordem de implantação** para exibir a ordem de implantação ou para reordenar a ordem de implantação.

3. Clique em **Salvar** para salvar o grupo de entrega.

Para alterar a ordem de implantação

1. Clique no botão **Ordem de implantação**. A caixa de diálogo **Ordem de implantação** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. 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.

3. Clique em **Salvar** para salvar a ordem de implantação.

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

> **Nota**
>
> AllUsers é o único grupo de entrega que você pode ativar ou desativar.

1. 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:

Nota: dependendo de como você selecionou AllUsers, o comando **Ativar** ou **Desativar** é exibido acima ou à direita do grupo de entrega AllUsers.

- 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 título **Desativado** na tabela do grupo de entrega.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

Nota: 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**.

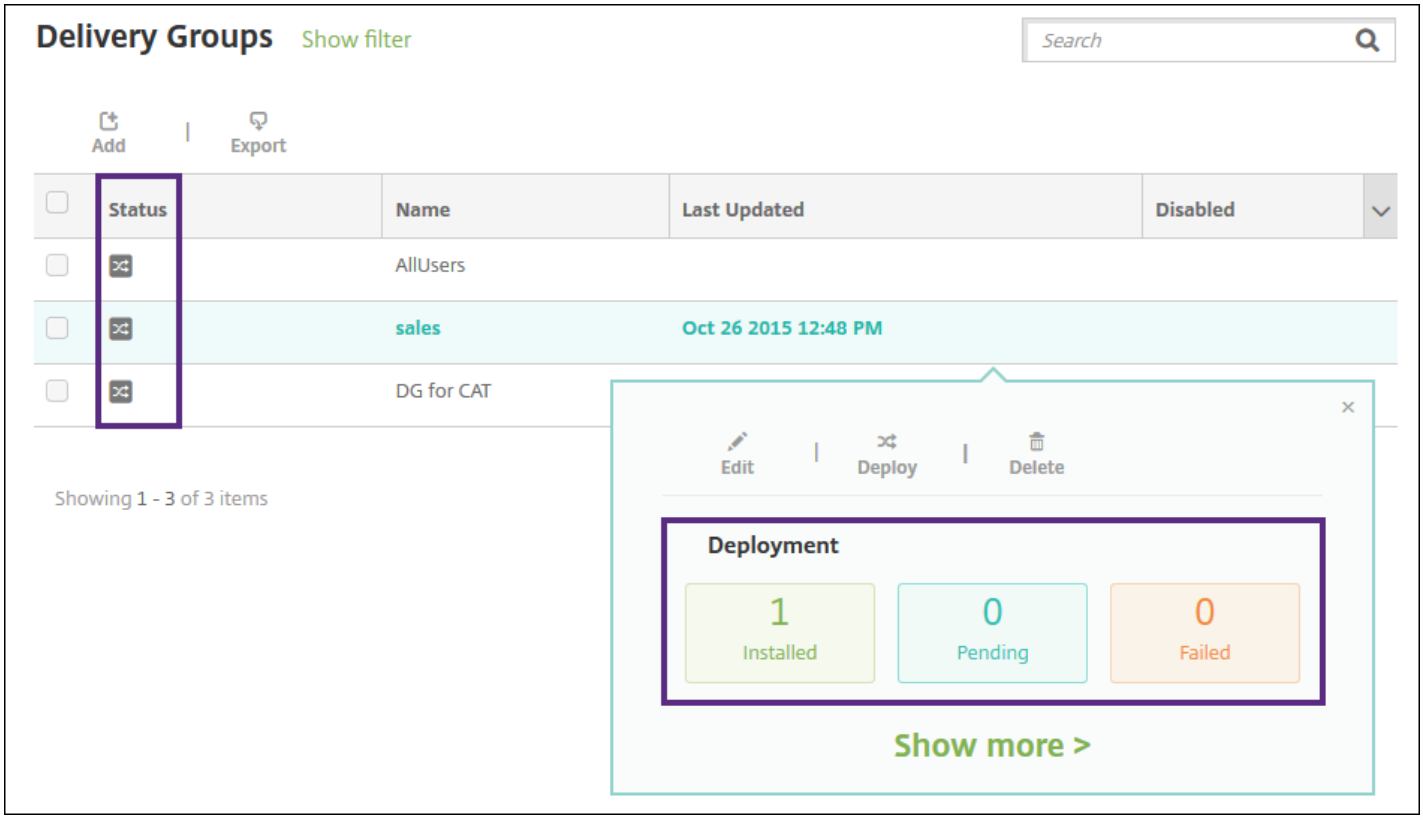
Nota: dependendo de como você selecionar um único grupo de entrega, o comando **Implantar** será exibido acima ou à direita do grupo de entrega.

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 título **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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Para excluir grupos de entrega

> ## Nota
>
> 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.

Nota: dependendo de como você selecionar um único grupo de entrega, o comando **Excluir** será exibido acima ou à direita do grupo de entrega.

3. Clique em **Excluir**.

> ## Important
>
> Não é possível desfazer essa ação.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Macros

Feb 21, 2018

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)]}

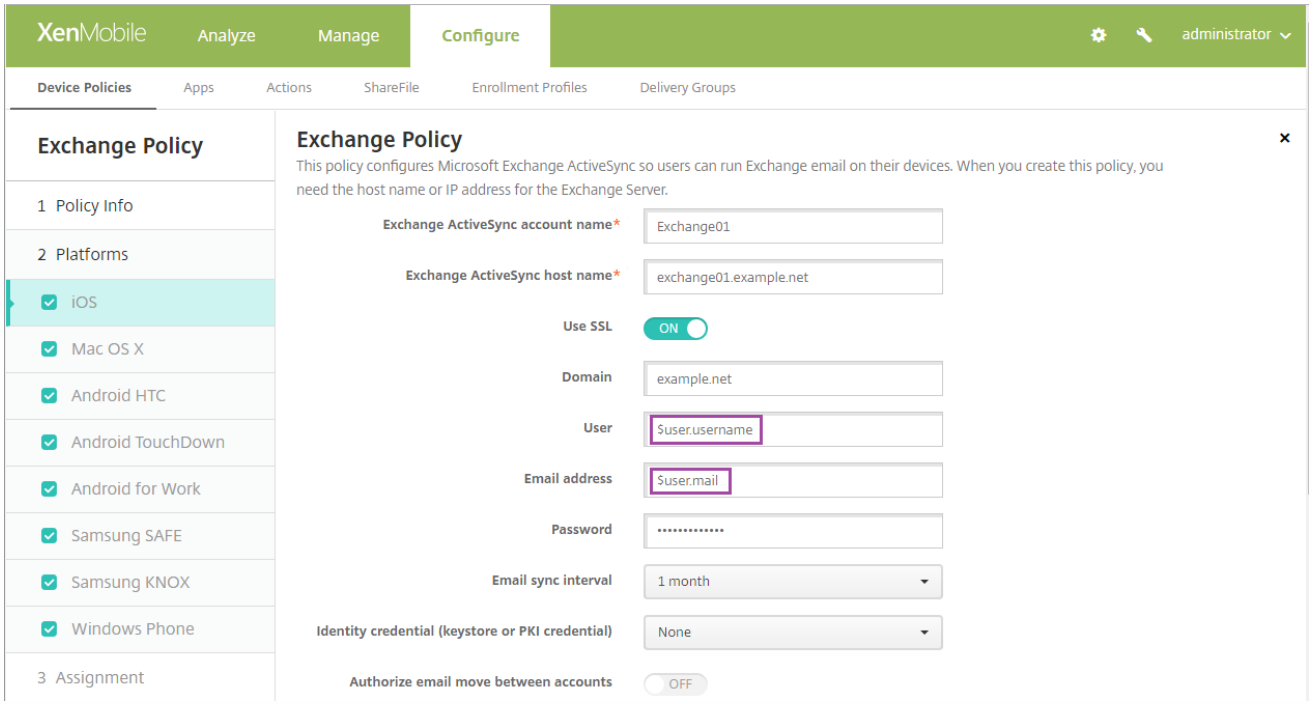
Coloque toda a sintaxe após o cifrão ($) entre chaves ({ }).

- 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 de um prefixo, seguido do nome real da propriedade.
- Propriedades de usuário assumem a forma ${user.[PROPERTYNAME] (prefix="user.")}.
- Propriedades de dispositivo assumem a forma ${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. Essa macro para uma mensagem de notificação inclui a função **firstnotnull**:

  O dispositivo ${firstnotnull(device.TEL_NUMBER,device.serialNumber)} foi bloqueado...

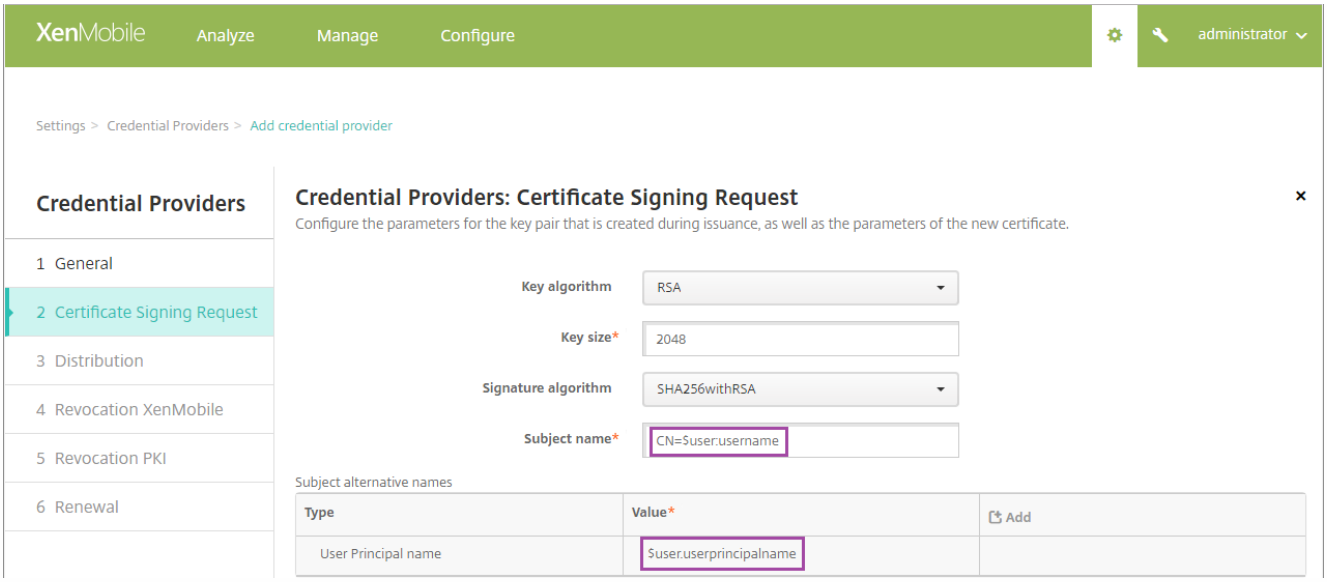
- Para macros personalizadas (propriedades que você define), o prefixo é ${custom}. Você pode omitir o prefixo.

Este é um exemplo de macro comum, ${user.username}, que preenche o valor de nome do usuário no campo de texto de uma política. Essa macro é útil para configurar perfis do Exchange ActiveSync e outros perfis usados por vários usuários. O exemplo a seguir mostra como usar macros em uma política do Exchange. A macro para **Usuário** é **${user.username}**. A macro para **Endereço de email** é **${user.mail}**.



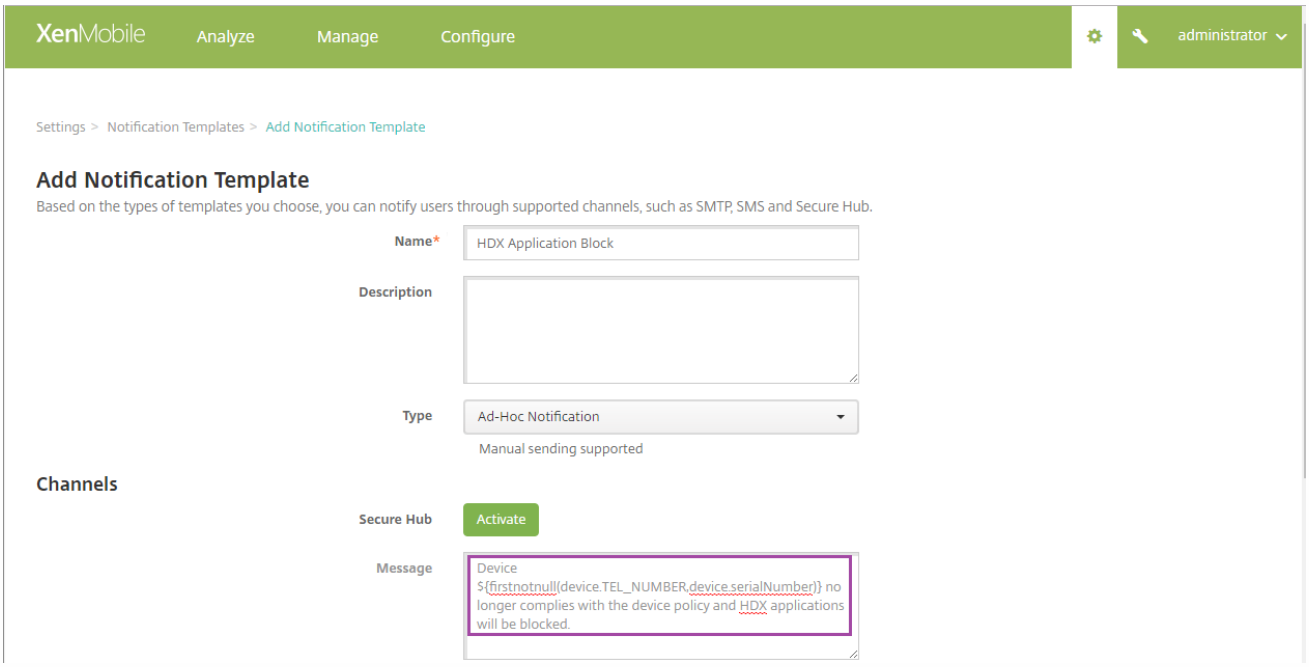
O exemplo a seguir mostra como usar macros para uma solicitação de assinatura de certificado. A macro para **Nome de entidade** é **CN=$user.username**. A macro para o **Valor** de um **Nome de entidade alternativo** é **$user.userprincipalname**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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:

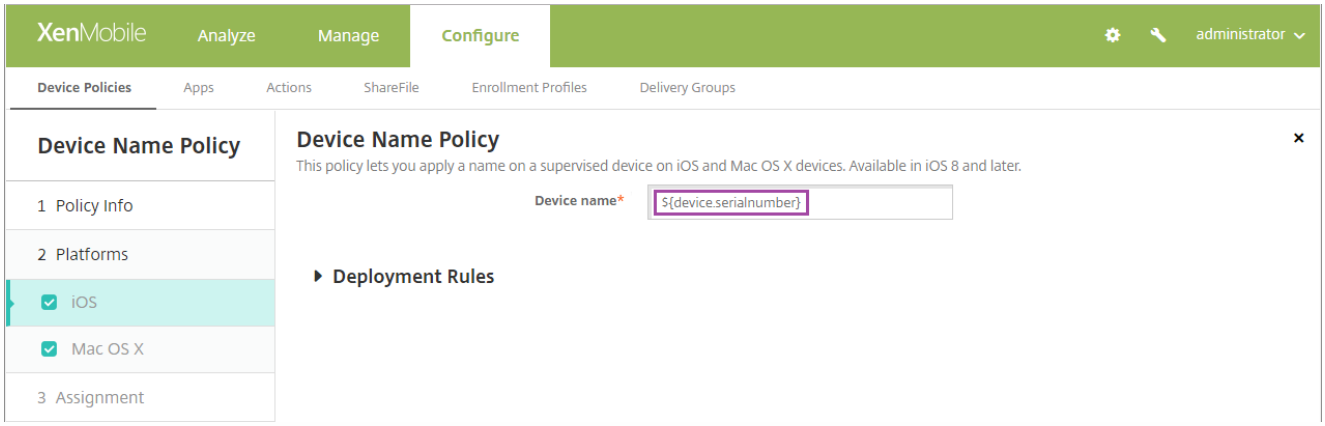
O dispositivo ${firstnotnull(device.TEL_NUMBER,device.serialNumber)} não está mais em conformidade com a política de dispositivo, e os aplicativos HDX serão bloqueados.



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 os nomes do dispositivo como o número de série de cada dispositivo. Use ${device.serialnumber} ${ user.username } para incluir o nome de usuário no nome do dispositivo. A política de dispositivo Nome do Dispositivo funciona em dispositivos supervisionados iOS e macOS.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Macros para modelos de notificação padrão

Você pode usar as seguintes macros nos modelos de notificação padrão:

- ${account.SUPPORT_EMAIL}
- ${applicationName}
- ${enrollment.andriod.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)}
- ${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 Webclip, 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	$device.id
IMEI do dispositivo	$device.imei
Família de SO	$device.OSFamily
Número de série	$device.serialNumber

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Macros para todas as propriedades de dispositivo

Nome de exibição	Elemento da Web	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_ACTIVESYNC_ID	${device.EXCHANGE_ACTIVESYNC_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 de dispositivo do Android for Work	GOOGLE_AW_DEVICE_ID	${device.GOOGLE_AW_DEVICE_ID}
Dispositivo Android for Work ativado?	GOOGLE_AW_ENABLED_DEVICE	${device.GOOGLE_AW_ENABLED_DEVICE}
Android para o tipo de instalação de trabalho	GOOGLE_AW_INSTALL_TYPE	${device.GOOGLE_AW_INSTALL_TYPE}
Status de assinatura de antispyware	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}

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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}
Baregia 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 de BES conhecido por MSP	BES_DEVICE_KNOWN_BY_ZMSP	${device.BES_DEVICE_KNOWN_BY_ZMSP}
PIN DO BES	BES_PIN	${device.BES_PIN}
ID do BES servidor agente	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 de Bit Locker	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 do celular	GPS_ALTITUDE_FROM_CELLULAR	${device.GPS_ALTITUDE_FROM_CELLULAR}
Curso do celular	GPS_COURSE_FROM_CELLULAR	${device.GPS_COURSE_FROM_CELLULAR}
Precisão horizontal do celular	GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR	${device.GPS_HORIZONTAL_ACCURACY_FROM_CELLULAR}
Latitude celular	GPS_LATITUDE_FROM_CELLULAR	${device.GPS_LATITUDE_FROM_CELLULAR}
Longitude da rede celular	GPS_LONGITUDE_FROM_CELLULAR	${device.GPS_LONGITUDE_FROM_CELLULAR}
Velocidade do celular	GPS_SPEED_FROM_CELLULAR	${device.GPS_SPEED_FROM_CELLULAR}
Tecnologia celular	CELLULAR_TECHNOLOGY	${device.CELLULAR_TECHNOLOGY}
Timestamp celular	GPS_TIMESTAMP_FROM_CELLULAR	${device.GPS_TIMESTAMP_FROM_CELLULAR}

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Precisão vertical do 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}
Registo de DEP por	DEVICE_ASSIGNED_BY	${device.DEVICE_ASSIGNED_BY}
Data de registro de DEP	DEVICE_ASSIGNED_DATE	${device.DEVICE_ASSIGNED_DATE}
Descrição	DESCRIÇÃO	${device.DESCRIPTION}
Modelo do dispositivo	SYSTEM_OEM	${device.SYSTEM_OEM}
Nome do dispositivo	NOME DO DISPOSITIVO	${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}

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 Directory	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}
Timestamp 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}

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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}
Versão de API HTC	HTC_MDM_VERSION	${device.HTC_MDM_VERSION}
API MDM de HTC disponível	HTC_MDM	${device.HTC_MDM}
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}

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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}
NitroDesk TouchDown instalado	TOUCHDOWN_FIND	${device.TOUCHDOWN_FIND}
NitroDesk TouchDown licenciados por meio do MDM	TOUCHDOWN_LICENSED_VIA_MDM	${device.TOUCHDOWN_LICENSED_VIA_MDM}
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}

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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	NOME_DA_DIRETIVA	${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}

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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	NÚM_SÉRIE	${device.SERIAL_NUMBER}
Com capacidade de SMS	IS_SMS_CAPABLE	${device.IS_SMS_CAPABLE}
API de Enterprise Sony disponível	SONY_MDM	${device.SONY_MDM}
Versão da API de Enterprise Sony	SONY_MDM_VERSION	${device.SONY_MDM_VERSION}
Supervisionado	SUPERVISED	${device.SUPERVISED}
Motivo da suspensão	GOOGLE_AW_DIRECTORY_SUSPENTION_REASON	${device.GOOGLE_AW_DIRECTORY_SUSPENTION_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}

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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)	${user.domainname}
loginname (nome de usuário mais nome de domínio)	${user.loginname}
username (nome de login menos o domínio, se houver)	${user.username}

Macros para todas as propriedades de usuário

Nome de exibição	**Elemento da Web**	**Macros**
Tentativas de login do Active Directory com falha	badpwdcount	${user.badpwdcount}
Email de usuário do ActiveSync	asuseremail	${user.asuseremail}
Origem de dados ASM	asmpersonsource	${user.asmpersonsource}
Nome de conta DEP ASM	asmdepaccount	${user.asmdepaccount}

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ID gerenciada da Apple ASM	asmpersonmanagedappleid	${user.asmpersonmanagedappleid}
Tipo de código de acesso ASM	asmpersonpasscodetype	${user.asmpersonpasscodetype}
ID pessoal ASM	asmpersonid	${user.asmpersonid}
Status pessoal ASM	asmpersonstatus	${user.asmpersonstatus}
Título pessoal ASM	asmpersontitle	${user.asmpersontitle}
ID exclusivo pessoal ASM	asmpersonuniqueid	${user.asmpersonuniqueid}
ID de sistema de origem ASM	asmpersonsourcesystemid	${user.asmpersonsourcesystemid}
Nível escolar de status ASM	asmpersongrade	${user.asmpersongrade}
Email de usuário de BES	besuseremail	${user.besuseremail}
Empresa	company	${user.company}
Nome da empresa	companyname	${user.companyname}
País	c	${user.c}
Departamento	department	${user.department}
Descrição	description	${user.description}
Usuário desativado	disableduser	${user.disableduser}
Nome de exibição	nome para exibição	${user.displayname}
Nome distinto	distinguishedname	${user.distinguishedname}
Nome de domínio	domainname	${user.domainname}
E-mail	mail	${user.mail}
Nome	givenname	${user.givenname}
Endereço (residencial)	homestreetaddress	${user.homestreetaddress}
Cidade (residencial)	homecity	${user.homecity}
País (residencial)	homecountry	${user.homecountry}
Fax (residencial)	homefax	${user.homefax}
Telefone (residencial)	homephone	${user.homephone}
Estado/região (residencial)	homestate	${user.homestate}
CEP (residencial)	homezip	${user.homezip}
Telefone IP	ipphone	${user.ipphone}
Inicial do meio	middleinitial	${user.middleinitial}
Segundo nome	middlename	${user.middlename}

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Celular	mobile	${user.mobile}
Nome	cn	${user.cn}
Endereço (comercial)	physicaldeliveryofficename	${user.physicaldeliveryofficename}
Cidade (comercial)	l	${user.l}
Número de fax (comercial)	facsimiletelephonenumber	${user.facsimiletelephonenumber}
Estado/província (comercial)	st	${user.st}
Endereço (comercial)	officestreetaddress	${user.officestreetaddress}
Número de telefone (comercial)	telephonenumber	${user.telephonenumber}
Código postal (comercial)	postalcode	${user.postalcode}
Caixa postal	postofficebox	${user.postofficebox}
Pager	pager	${user.pager}
ID de grupo primário	primarygroupid	${user.primarygroupid}
Conta SAM	samaccountname	${user.samaccountname}
Endereço	streetaddress	${user.streetaddress}
Sobrenome	sn	${user.sn}
Título	title	${user.title}
Nome de login do usuário	userprincipalname	${user.userprincipalname}

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Ações automatizadas

Feb 21, 2018

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. Ao criar uma ação automatizada, você estabelece o efeito sobre o dispositivo do usuário quando é conectado ao XenMobile com base nos gatilhos da ação. Quando um evento é disparado, você pode enviar uma notificação para o usuário corrigir um problema, antes que medidas mais sérias sejam necessárias.

Por exemplo, se você desejar detectar um aplicativo que tenha incluído anteriormente na lista negra (por exemplo, Words with Friends), poderá especificar um gatilho que defina o dispositivo do usuário como fora de conformidade quando Words with Friends for detectado no dispositivo. Em seguida, a ação os notifica que eles devem remover o aplicativo para que o dispositivo esteja novamente em conformidade. Você pode definir um tempo limite para o tempo de espera pela conformidade do usuário antes de tomar uma ação mais grave, como limpar seletivamente o dispositivo.

Em casos em que um dispositivo do usuário for colocado em um limite de estado de conformidade e, em seguida, o usuário corrige o dispositivo para que o dispositivo está em conformidade, você precisará configurar uma política para implantar um pacote que reinicia o dispositivo em um estado de conformidade.

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.

Este artigo explica como adicionar, editar e filtrar ações automatizadas no XenMobile, além de como configurar bloqueio de aplicativo e ações de apagamento de aplicativos para o modo somente MAM.

> ## Nota
>
> 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 no XenMobile. 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 Para criar ou atualizar modelos de notificação no XenMobile.

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 nova ação.
- Selecione uma ação existente para editar ou excluir. Clique na opção desejada.

Nota: quando você marca a caixa de seleção ao lado de uma ação, o menu de opções é exibido acima da lista de ações; quando você clica em qualquer outro lugar na lista, o menu de opções é exibido à direita da listagem.

3. A página **Informações sobre a ação** é exibida.

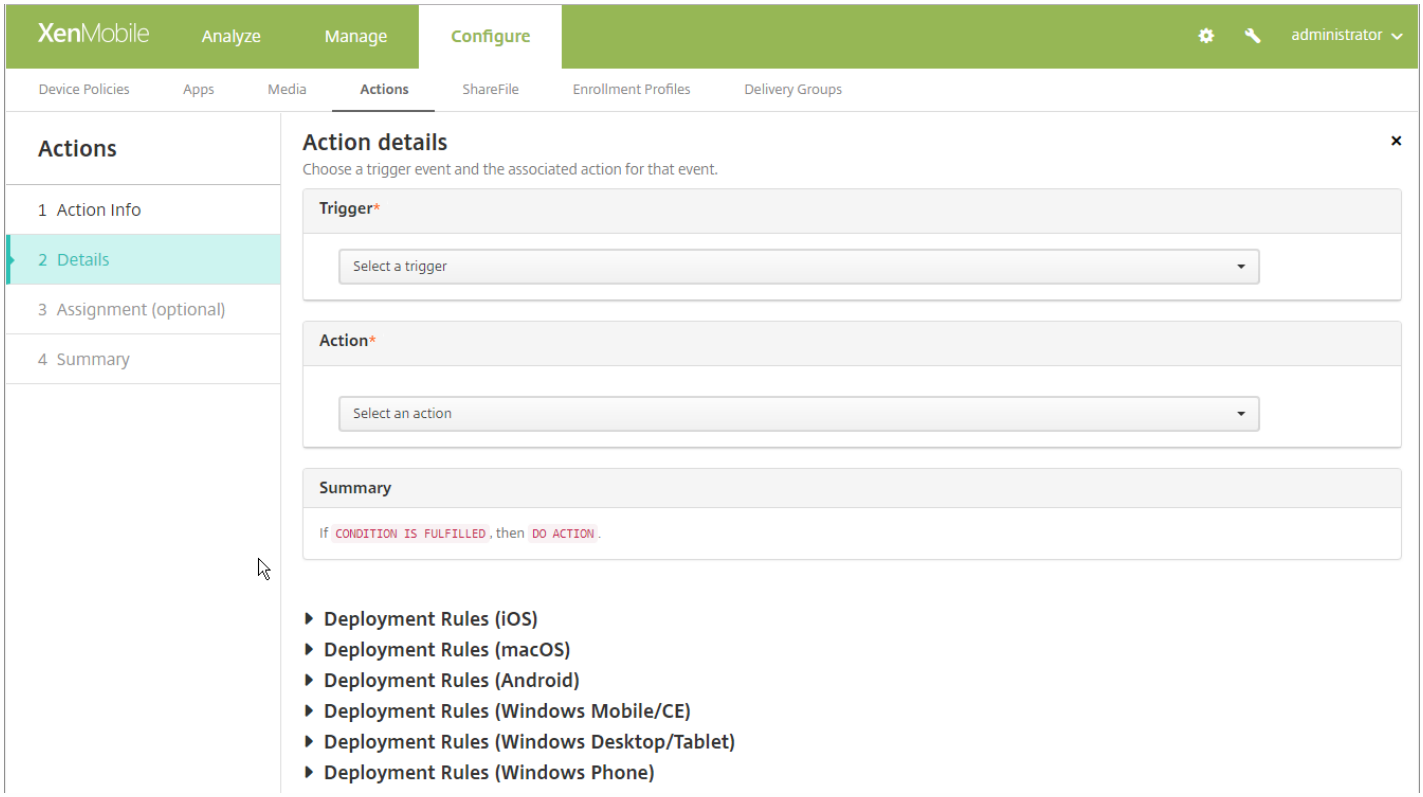
4. Na página **Informações sobre a ação**, insira ou modifique as seguintes informações:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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.

Observação: 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.



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 no dispositivo obtido no modo do MDM e reage a ele. Para obter mais informações, consulte Nomes e valores de propriedades do dispositivo.
  - **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 Para adicionar uma política de dispositivo de inventário de aplicativos.

7. Na próxima lista, clique na resposta para o gatilho.

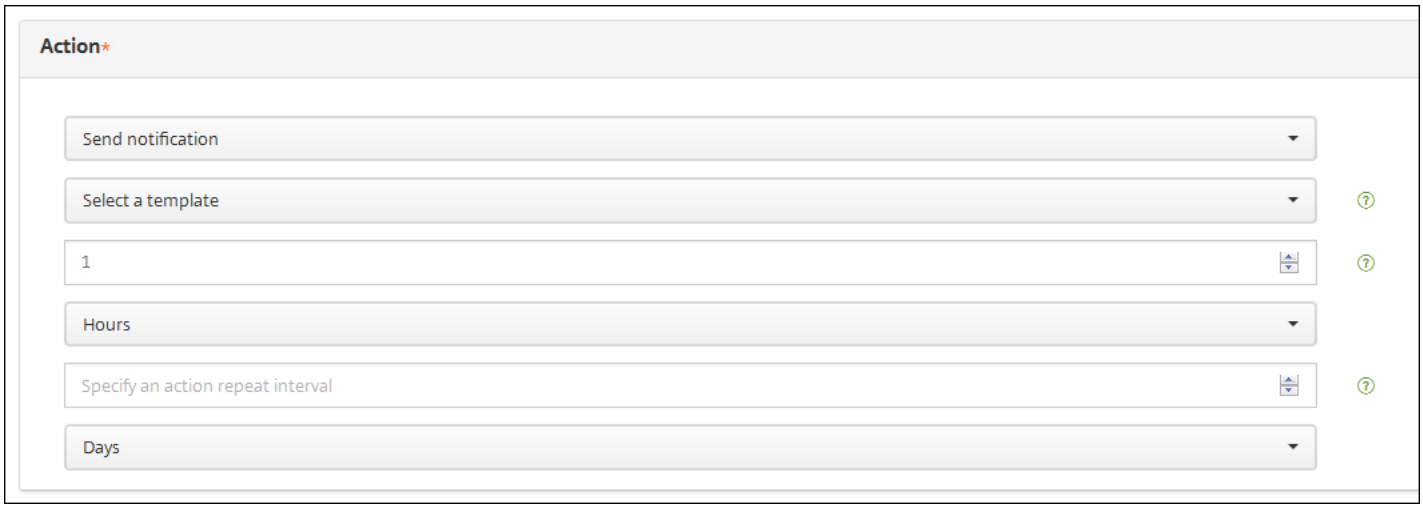
8. Na lista **Ação**, clique na ação a ser executada quando o critério de gatilho é cumprido. Com exceção da opção **Enviar notificação**, você escolhe um período de tempo durante o qual os usuários podem resolver o problema que causou o gatilho. Se o problema não for resolvido nesse período, a ação selecionada será tomada. Para obter uma definição das ações, consulte Ações de segurança.

Se você escolher **Enviar notificação**, o restante deste procedimento explicará como enviar uma ação de notificação.

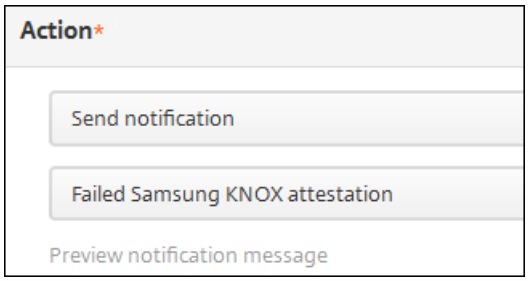
© 1999-2017 Citrix Systems, Inc. All rights reserved.

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**.

Observação: 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 no XenMobile. 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 Para criar ou atualizar modelos de notificação no XenMobile.



Observação: depois de selecionar o modelo, você poderá visualizar a notificação clicando em **Visualizar mensagem de notificação**.



10. Nos campos seguintes, defina o atraso em dias, horas ou minutos antes de tomar a ação e o intervalo no qual a ação se repete até o usuário resolver o problema do gatilho.

11. Em **Resumo**, verifique se você criou a ação automatizada como desejado.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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

- Expanda as Regras de implantação. A guia Base é exibida por padrão.
- Nas listas, clique em opções para determinar quando a ação deve ser implantada.
  1. Você pode optar por implantar a ação quando todas as condições forem atendidas ou quando qualquer condição for atendida. A opção padrão é **Tudo**.
  2. Clique em **Nova regra** para definir as condições.
  3. Nas listas, clique nas condições, como **Propriedade do dispositivo** e **BYOD**.
  4. Clique em **Nova regra** novamente se você desejar adicionar mais condições. Você pode adicionar quantas condições desejar.
- Clique na guia **Avançado** para combinar as regras com as opções boolianas.
- As condições que você escolheu na guia Base são exibidas.
- Você pode usar a lógica booliana mais avançada para combinar, editar ou adicionar regras.
  1. Clique em **AND**, **OR** ou **NOT**.
  2. Nas listas que aparecem, selecione as condições que você desejar adicionar à regra e, 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.
  3. Clique em **Nova regra** novamente se você desejar adicionar mais condições.
     Neste exemplo, a propriedade do dispositivo deve ser **BYOD**, a criptografia local de dispositivo deve ser **Verdadeiro**, o dispositivo deve ser compatível com o código secreto e o código de país do dispositivo móvel não pode ser apenas de Andorra.

14. Quando você terminar de definir as regras de implantação para a ação de plataforma, clique em **Avançar**. A página de **atribuição 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 na lista o grupo ou os grupos aos quais você deseja atribuir a política. Os grupos que você selecionar aparecerão na lista **Grupos de entrega que receberão a atribuição de aplicativos** à direita.

16. Expanda o 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 **O**, nenhuma outra opção precisará ser configurada.
- Ao lado de **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**.
  Observação: essa opção se aplicará quando você tiver configurado a chave de implantação em segundo plano do agendamento em **Configurações** > **Propriedades do servidor**. A opção sempre conectada não está disponível para

© 1999-2017 Citrix Systems, Inc. All rights reserved.

dispositivos iOS.

Observação: o cronograma de implantação configurado 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 de 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 **do Active Directory desativado usuário** a **apagamento de aplicativos** e **bloqueio de aplicativo** ações não serão exibidos.

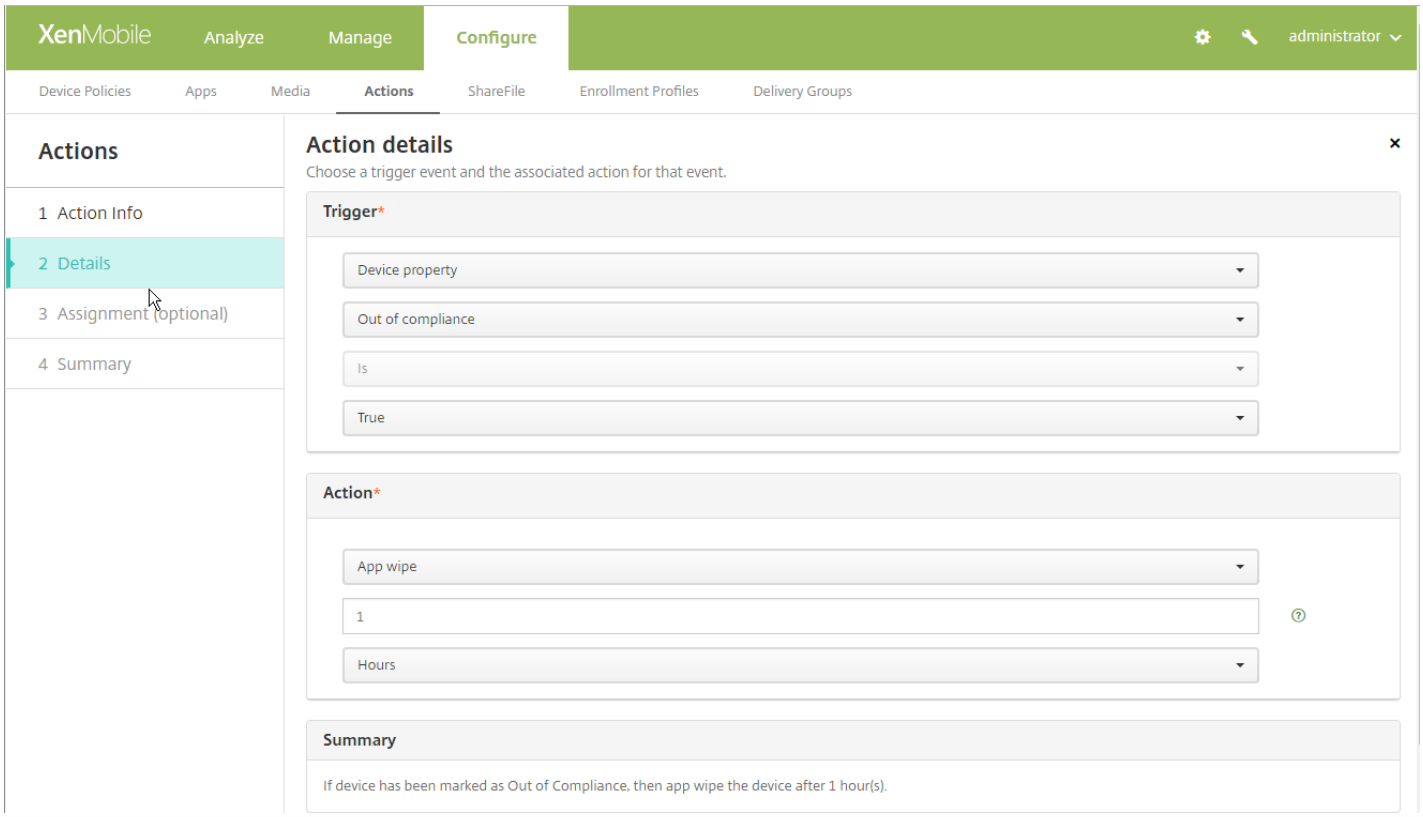
Quando o tipo de gatilho for **Propriedade do dispositivo** e o valor for **Modo MDM Perdido ativado**, não serão exibidas as seguintes ações:

- 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. O atraso oferece tempo aos usuários para corrigir um problema, se possível antes que a ação seja realizada. Você pode saber mais sobre o bloqueio de aplicativo do apagamento de aplicativos e ações no tópico em Configurar funções com RBAC.

> **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 adicional 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



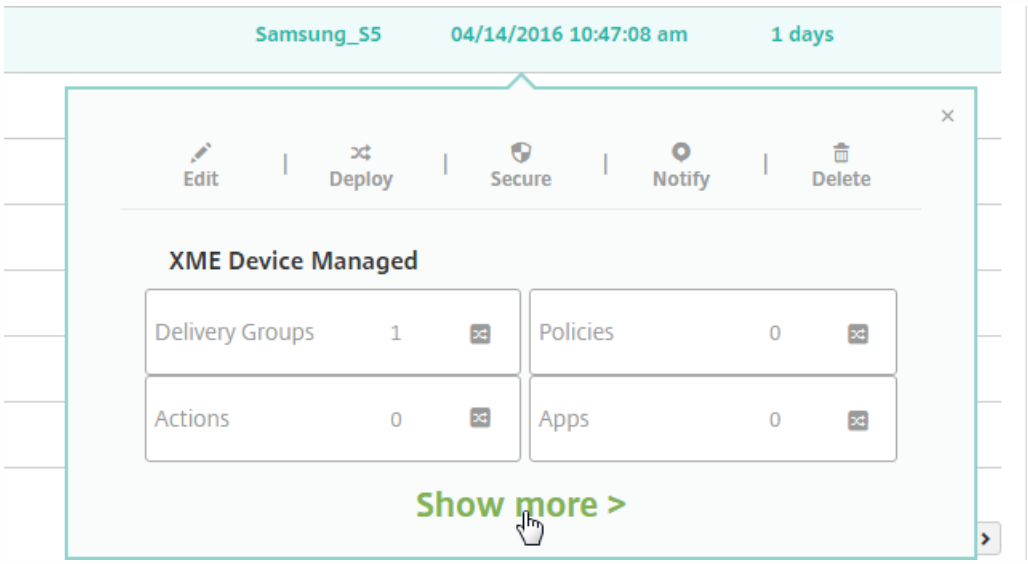
6. Configure as regras de implantação e clique em **Avançar**.

7. Configure as atribuições do grupo de entrega e um cronograma de implantação, e clique em **Avançar**.

8. Clique em **Salvar**.

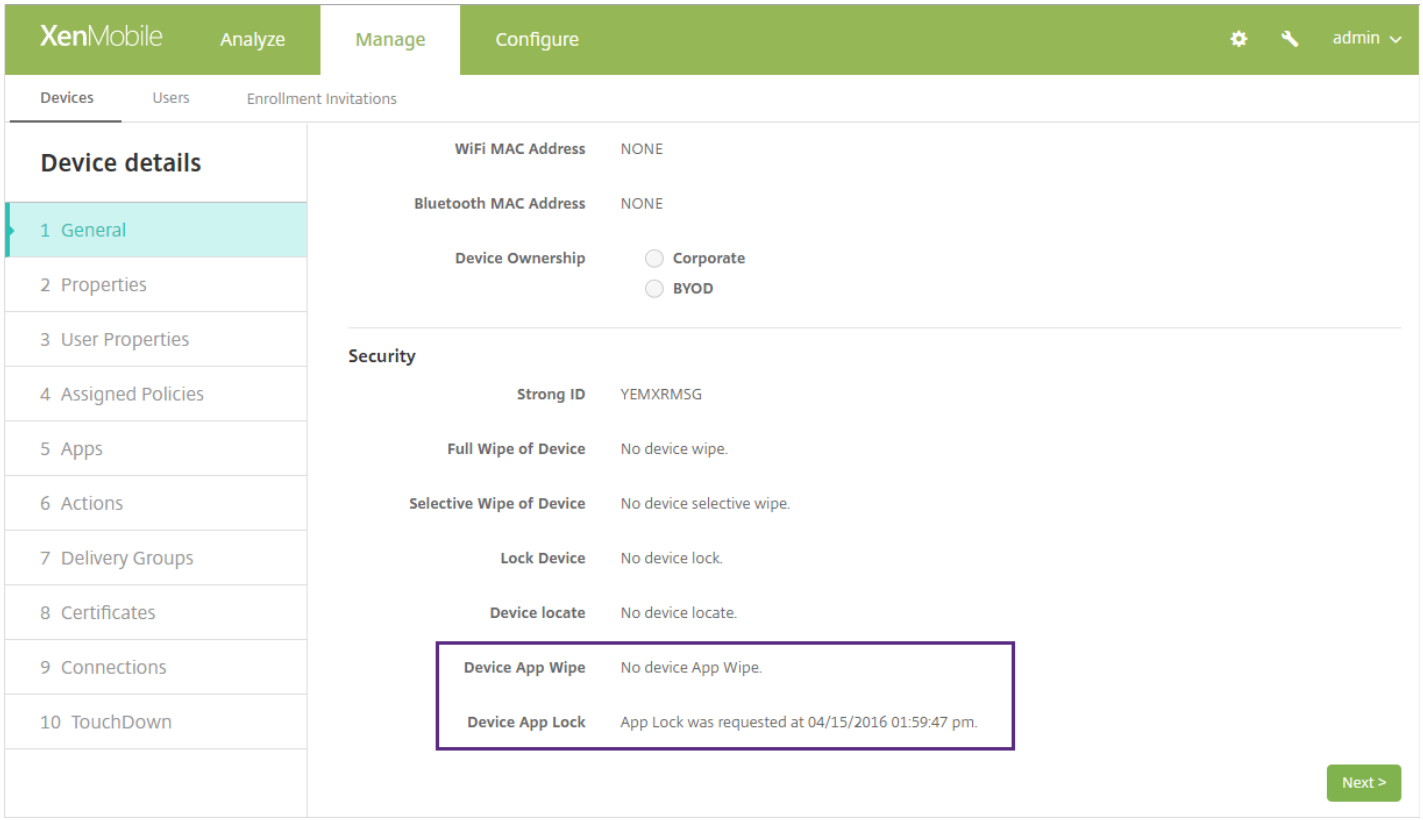
Para verificar o status do apagamento de aplicativos ou do bloqueio de aplicativo

1. Acesse **Gerenciar > Dispositivos**, clique em um dispositivo e clique em **Mostrar mais**.

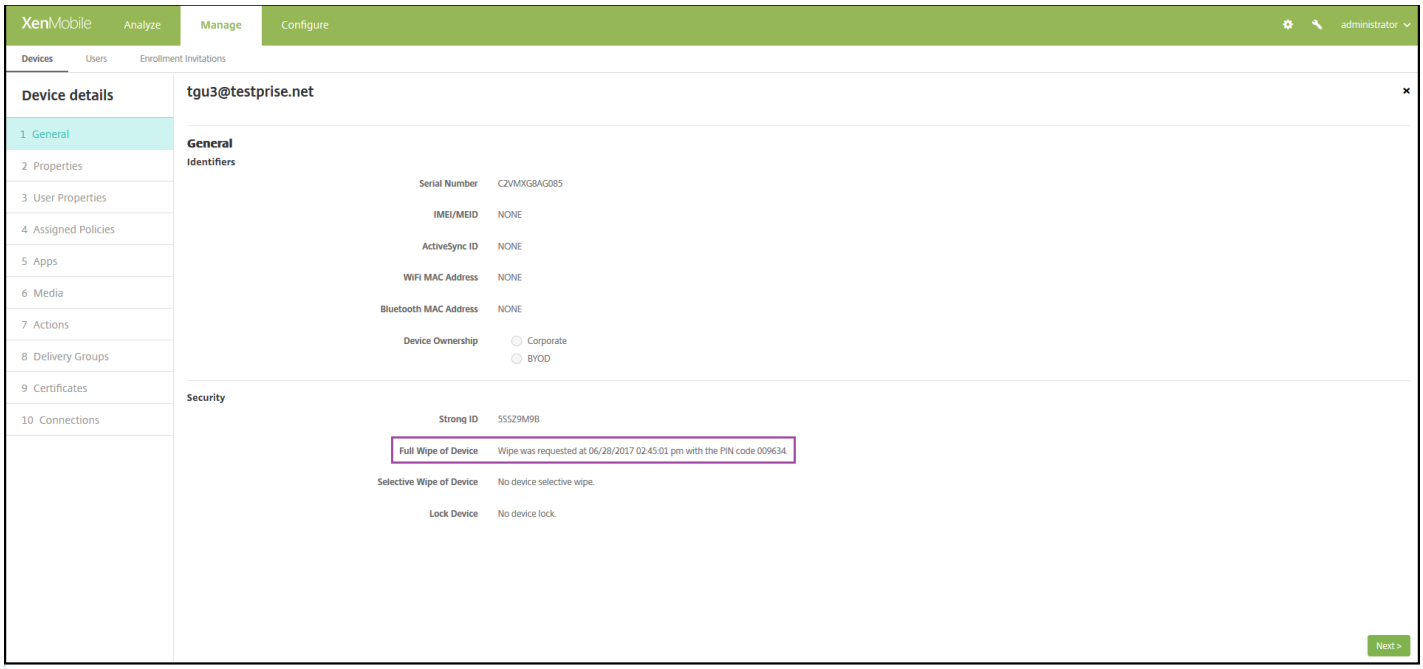


2. Role até **Apagamento de aplicativos do dispositivo** e **Bloqueio de aplicativo do dispositivo**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Monitoração e suporte

Feb 21, 2018

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.

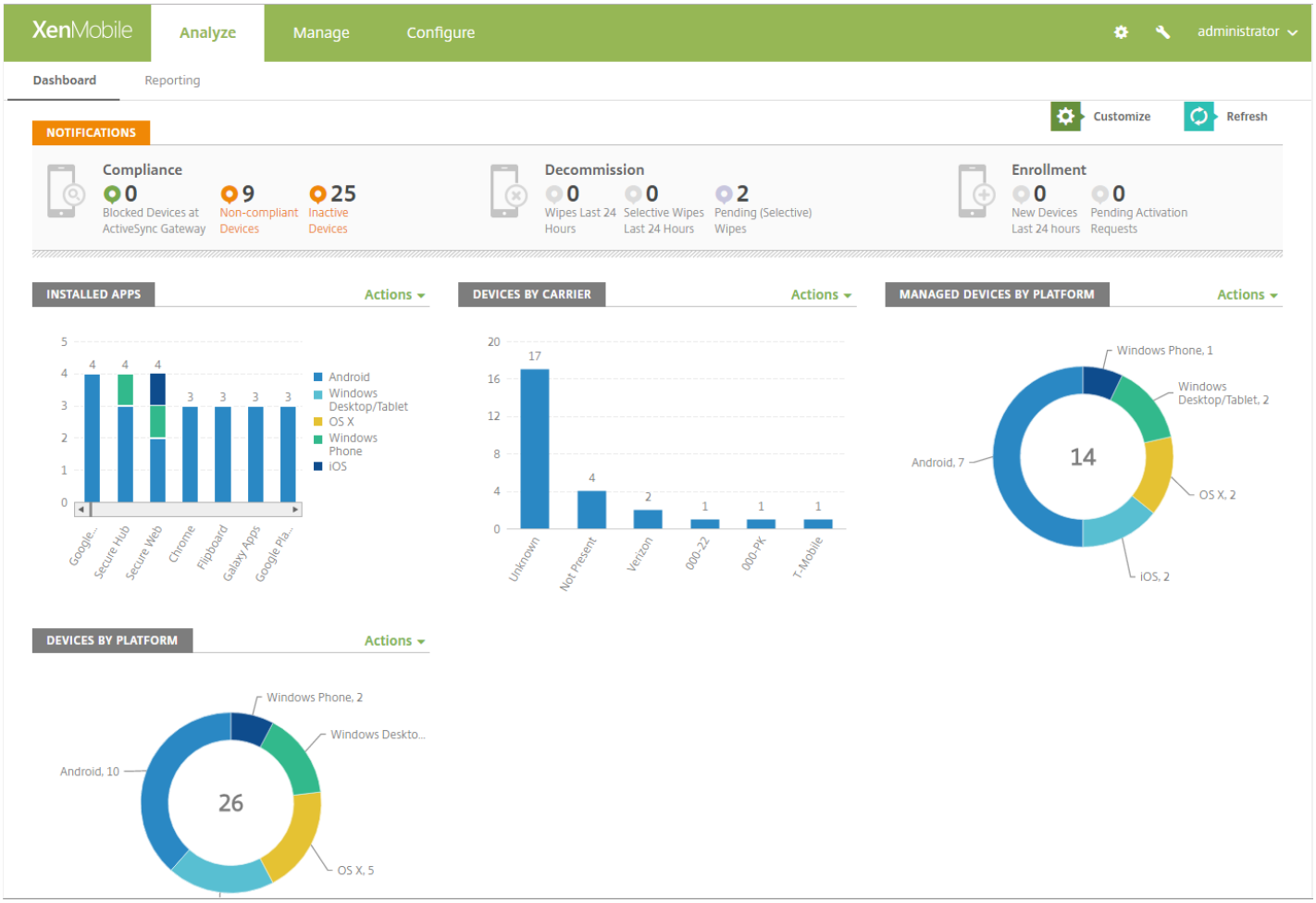
A página de solução de problemas e suporte é exibida.

Use a página **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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.

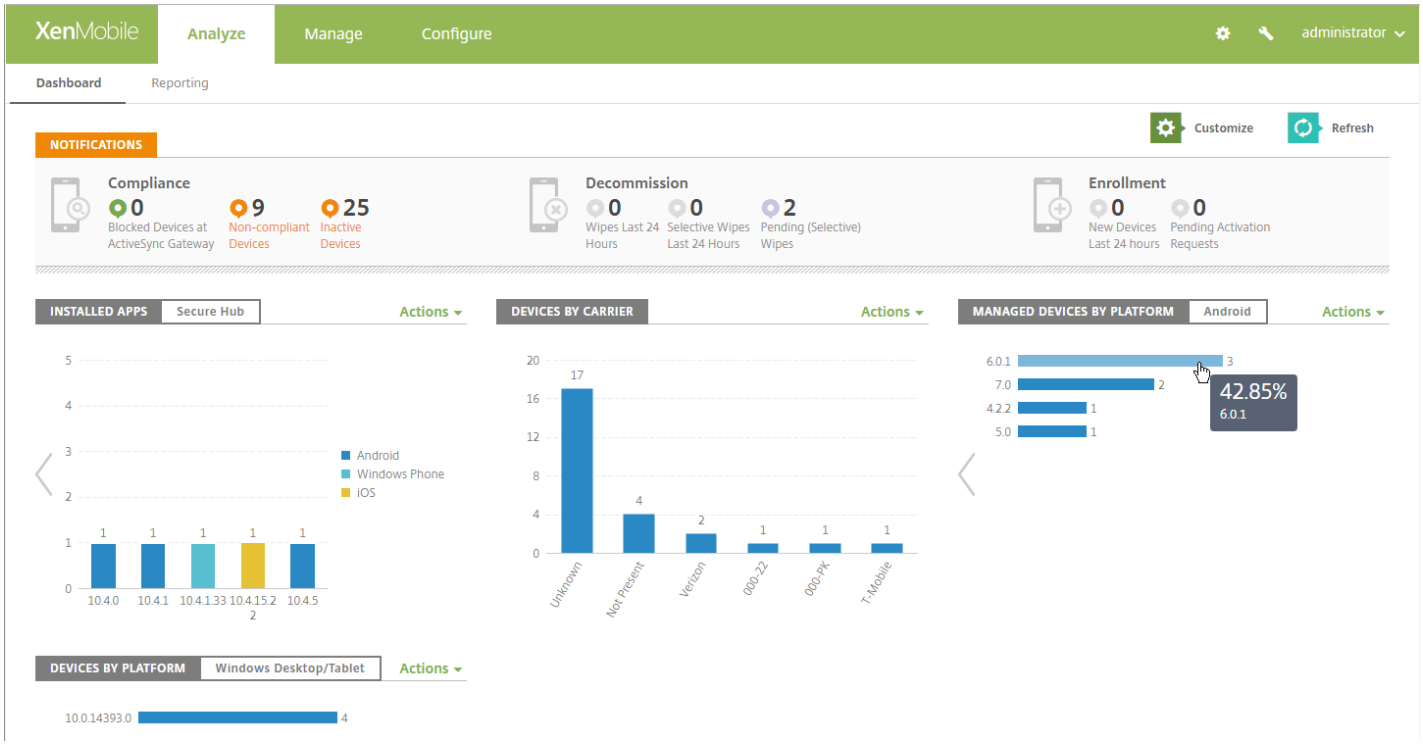
- **Meus painéis**: você pode salvar até quatro painéis. Você pode editar esses painéis separadamente e exibir cada um selecionando o painel salvo.
- **Estilo de layout**: nessa linha você pode selecionar quantos widgets são exibidos no painel e a sua disposição.
- **Seleção de widgets**: você pode escolher 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 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 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

de mostram o status de propriedade de propriedade da empresa, propriedade do funcionário ou desconhecido.

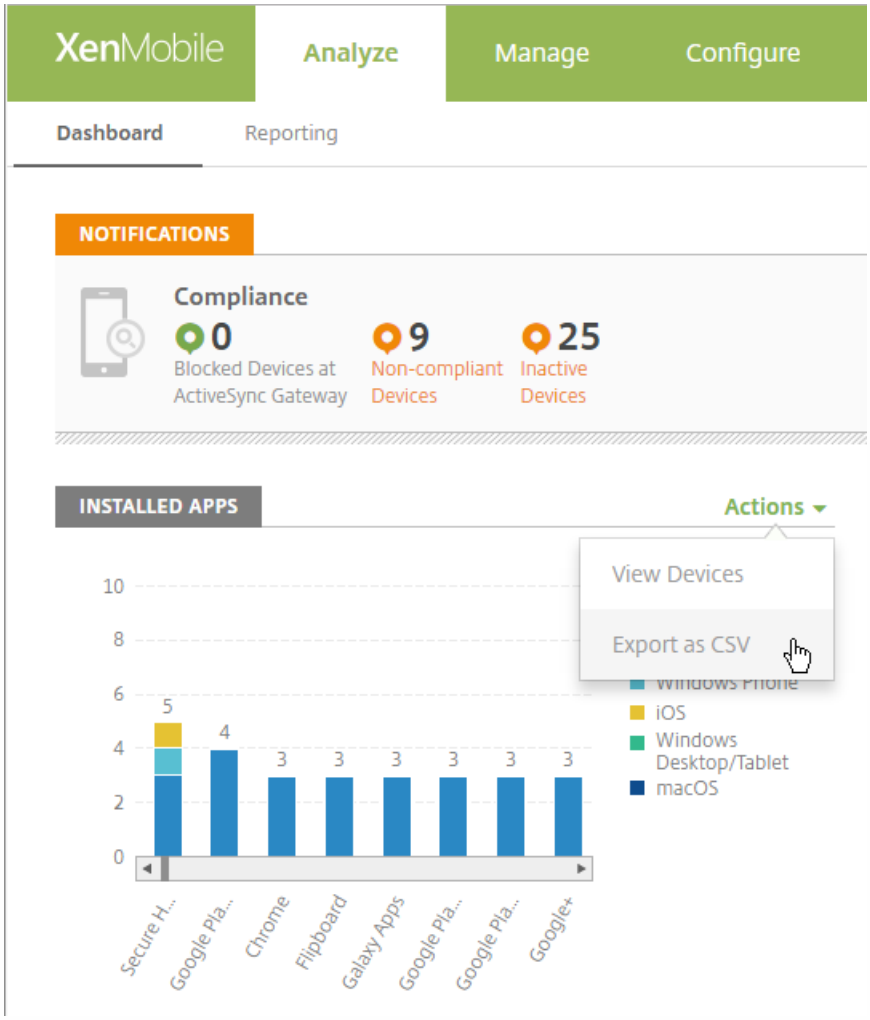
- **Status de licença do android TouchDown**: exibe o número de dispositivos que têm uma licença do TouchDown.
- **Implantações de grupo de entrega com falha**: exibe o número total de falhas de implantação por pacote. Apenas os pacotes que têm falhas de implementação.
- **Dispositivos por motivo de bloqueio**: exibe o número de dispositivos bloqueados pelo ActiveSync
- **Aplicativos instalados**: digite um nome de aplicativo para um gráfico de informações de aplicativos.
- **Uso de licenças de aplicativos de VPP**: exibe as estatísticas de uso de licença de aplicativos do Apple Volume Purchase Program.

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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

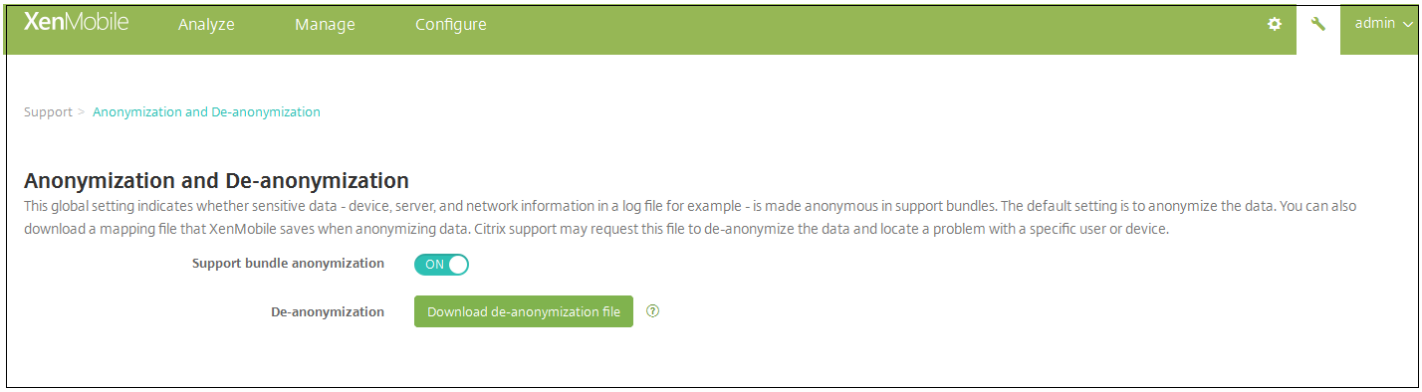
Anonimizar dados nos pacotes de suporte

Feb 21, 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 da Citrix quando eles precisarem de informações específicas do dispositivo ou do usuário para diagnosticar um problema.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Verificações de conectividade

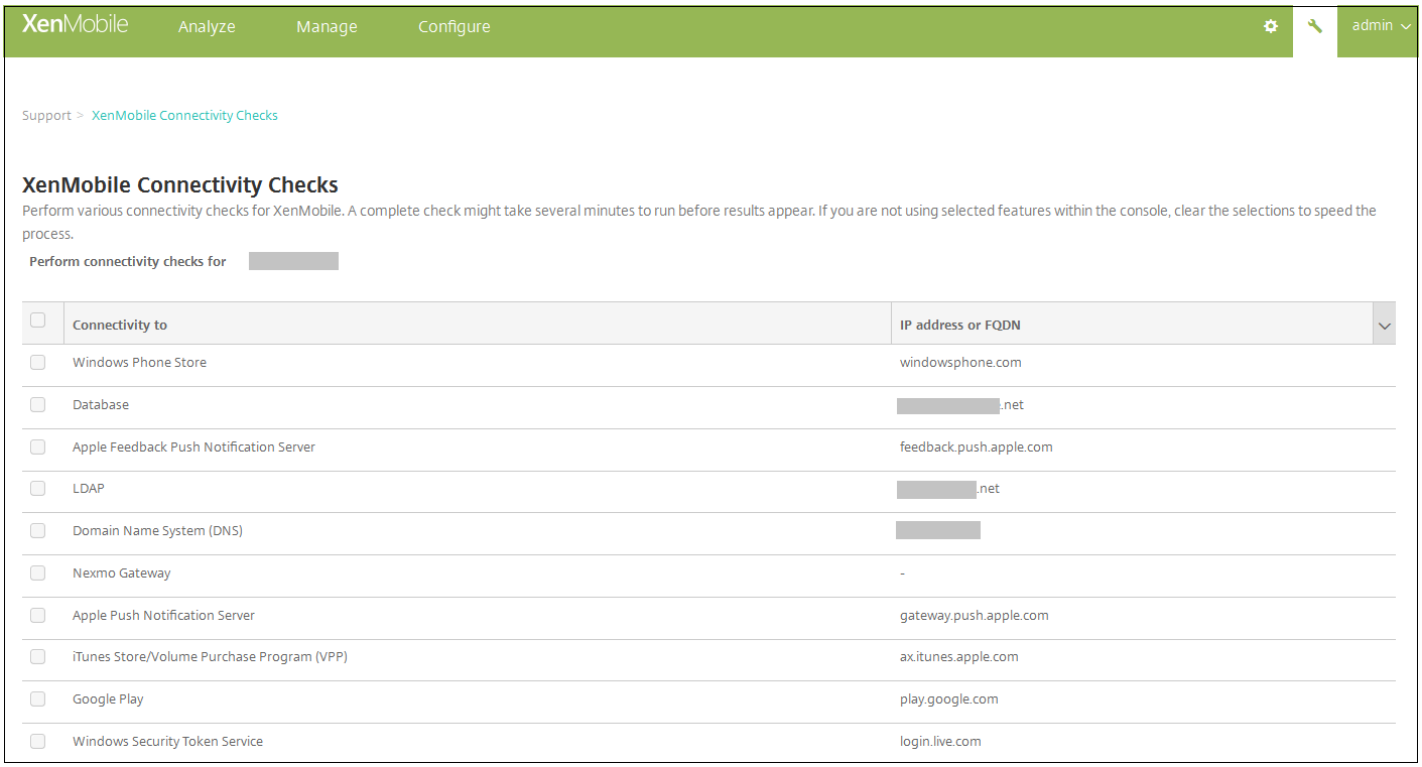
Feb 21, 2018

Na página **Suporte do XenMobile**, você pode verificar a conexão do XenMobile com o NetScaler Gateway e outros servidores e localizações.

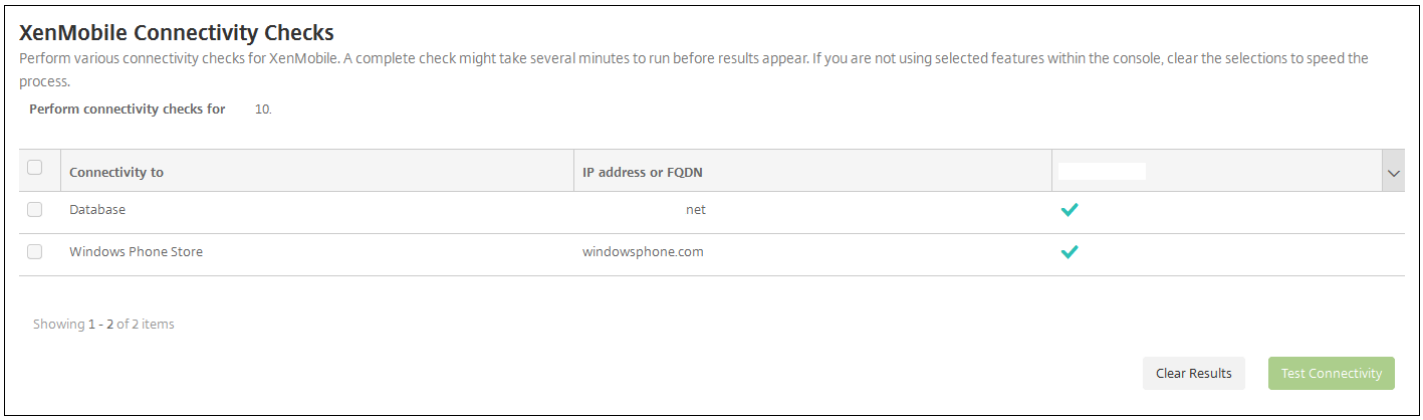
Conduzindo verificações de conectividade XenMobile

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.

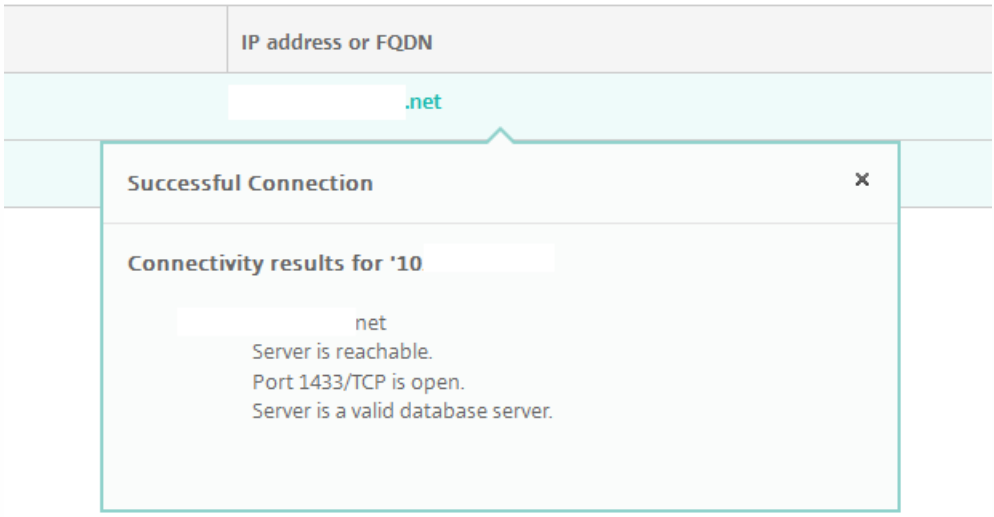


2. Selecione os servidores que você desejar incluir no teste de conectividade e clique em **Testar conectividade**. A página de resultados de teste é exibida.



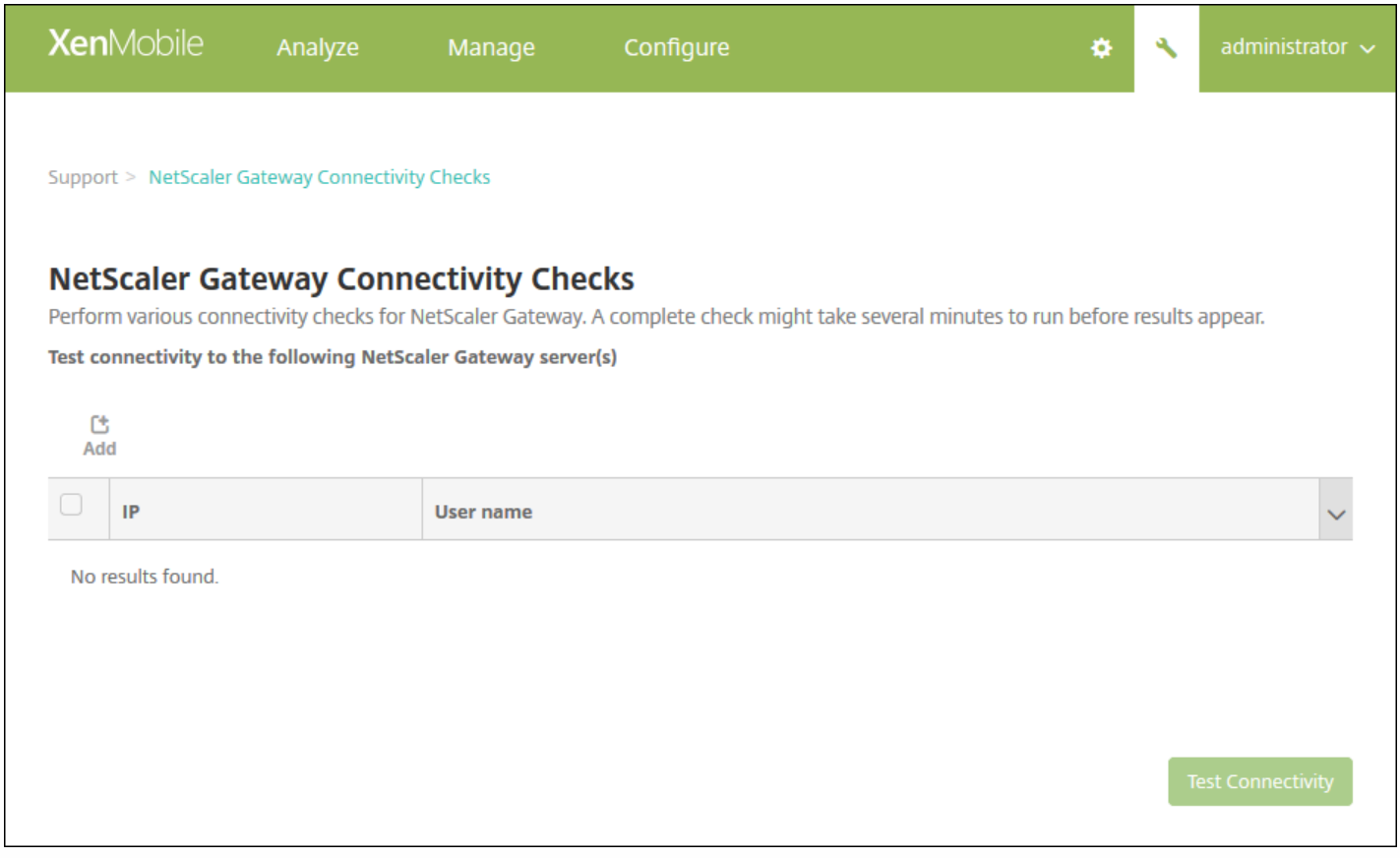
3. Selecione um servidor na tabela dos resultados do teste para ver os resultados detalhados desse servidor.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



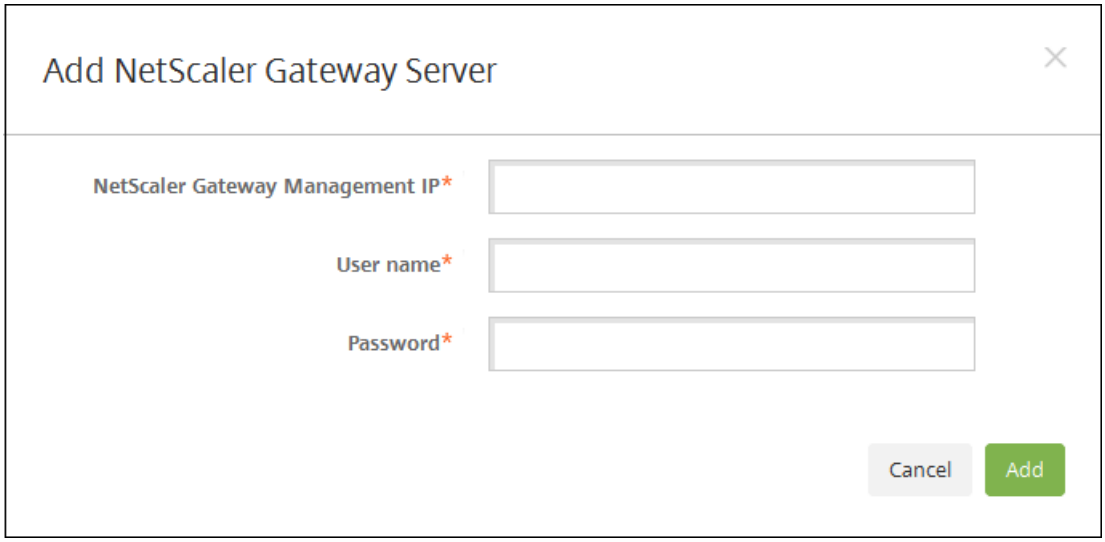
Conduzindo verificações de conectividade do NetScaler Gateway

1. Na página **Suporte**, em **Diagnósticos**, clique em **Verificações de conectividade do NetScaler Gateway**. A página **Verificações de conectividade do NetScaler Gateway** é exibida. A tabela estará vazia se você ainda não tiver adicionado nenhum servidor do NetScaler Gateway.



2. Clique em **Adicionar**. A caixa de diálogo **Adicionar servidor do NetScaler gateway** é exibida.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. Em **IP de gerenciamento do NetScaler Gateway**, digite o endereço IP do servidor que executa o NetScaler Gateway que você deseja testar.

Observação: se você estiver conduzindo uma verificação de conectividade para um servidor do NetScaler Gateway que já foi adicionado, o endereço IP será fornecido.

4. Digite as suas credenciais de administrador para esse NetScaler Gateway.

Observação: se você estiver conduzindo uma verificação de conectividade para um servidor do NetScaler Gateway que já foi adicionado, o nome do usuário será fornecido.

5. Clique em **Adicionar**. O NetScaler Gateway é adicionado à tabela na página **Verificações de conectividade do NetScaler Gateway**.

6. Selecione o servidor do NetScaler 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

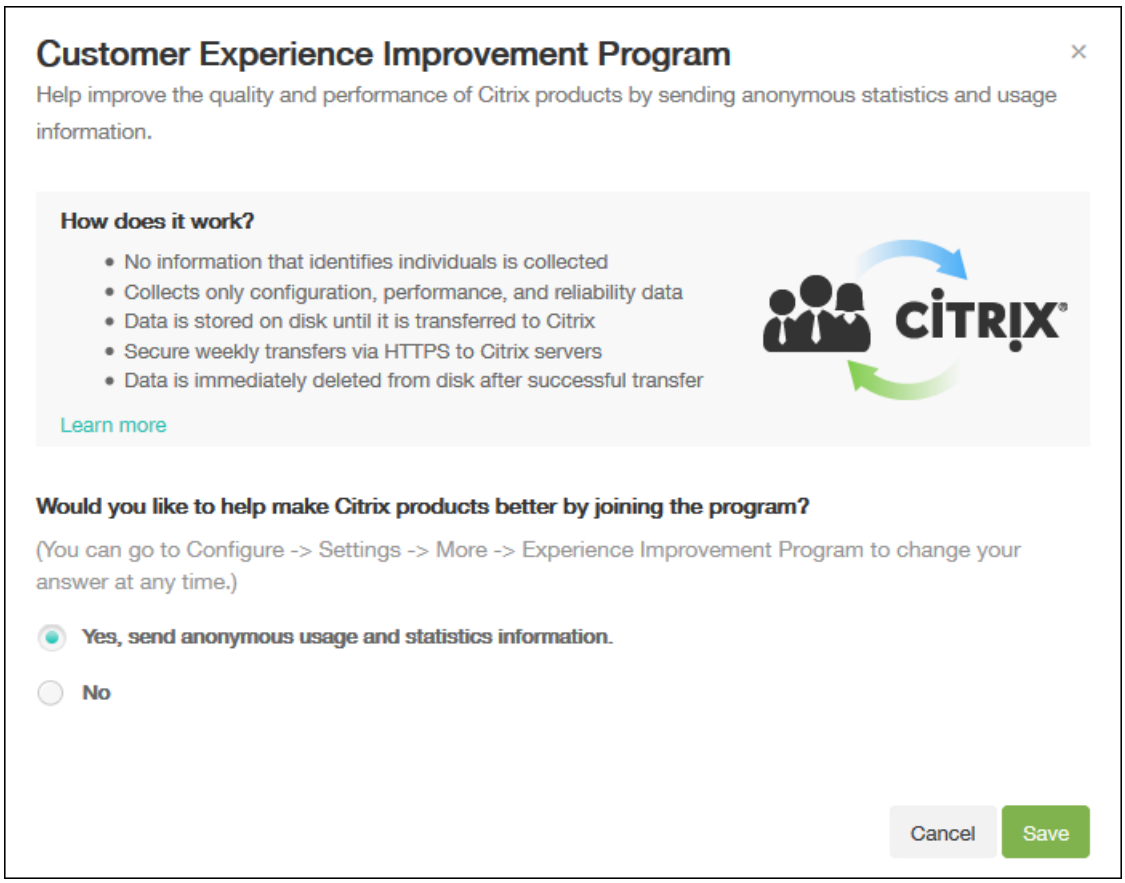
Programa de Melhoria de Experiência do Cliente

Feb 21, 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.

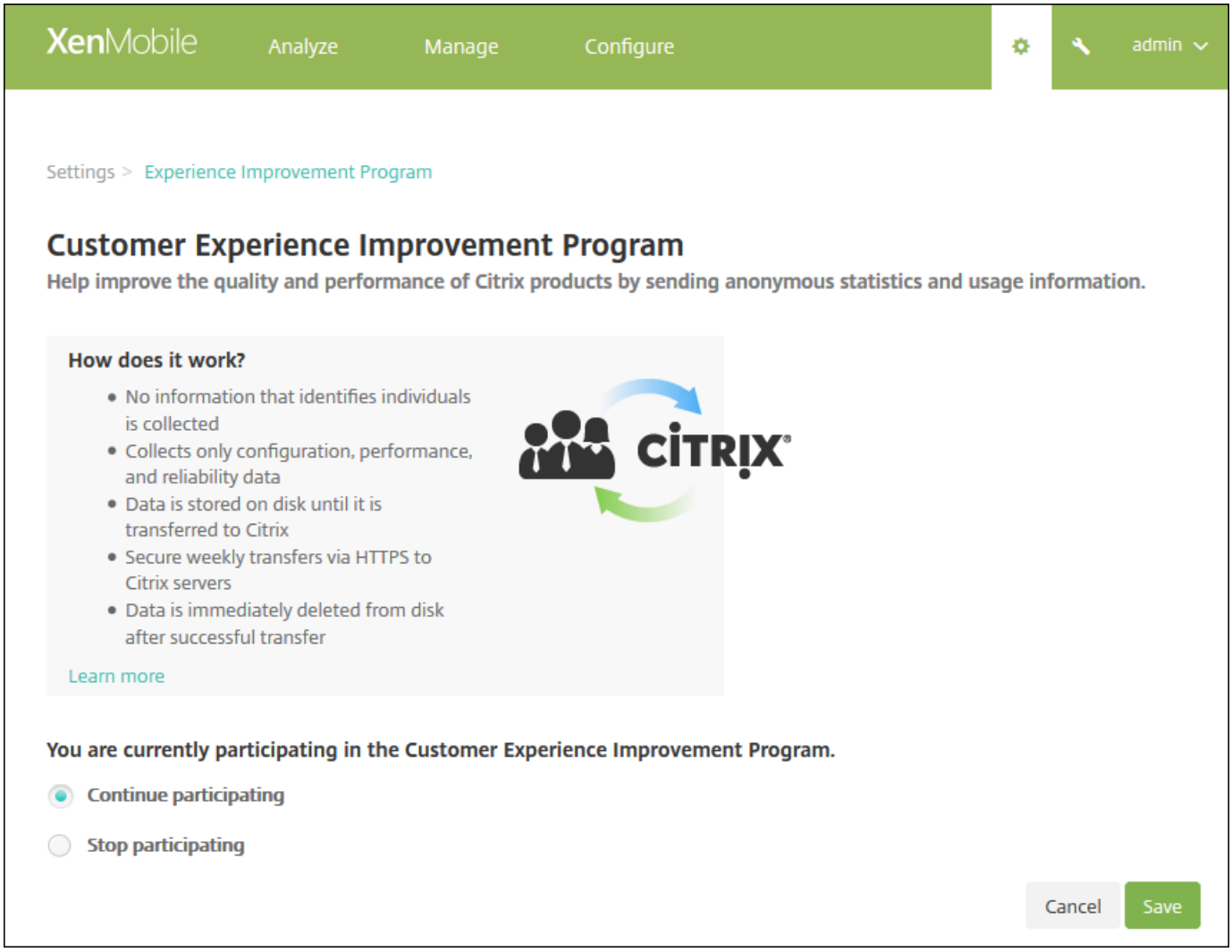


Alterar sua configuração de participação no CEIP

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

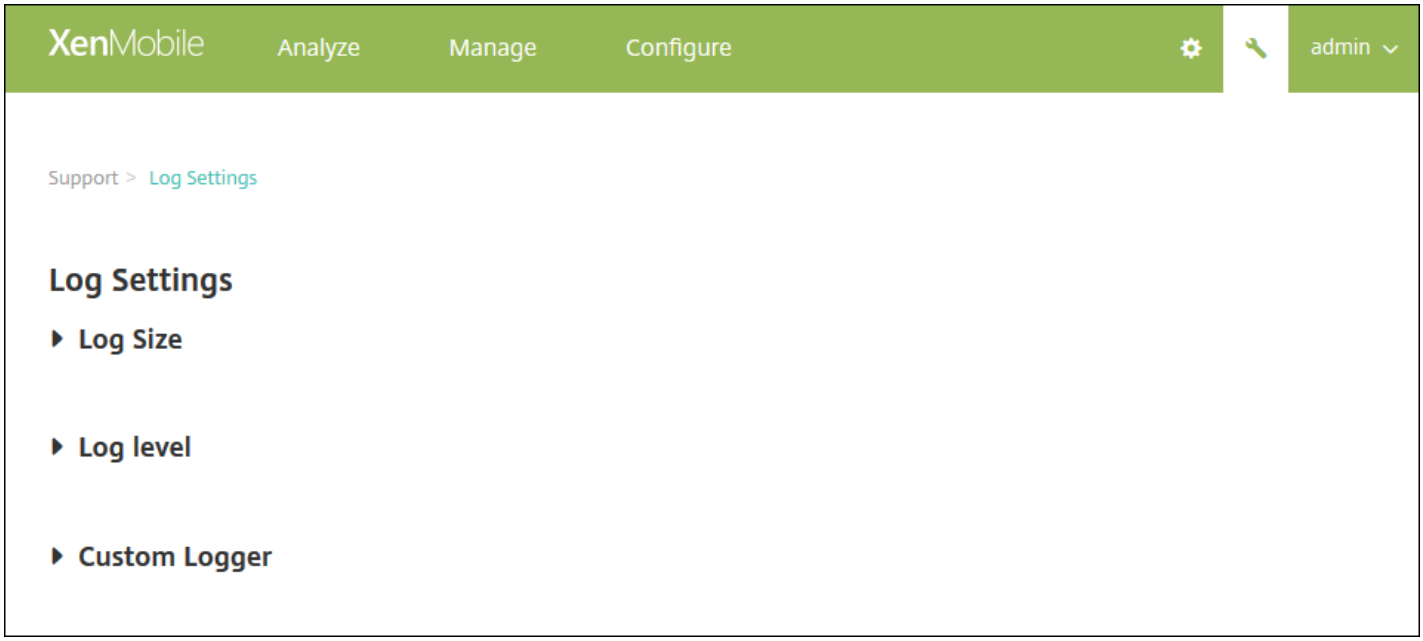
Logs

Feb 21, 2018

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.



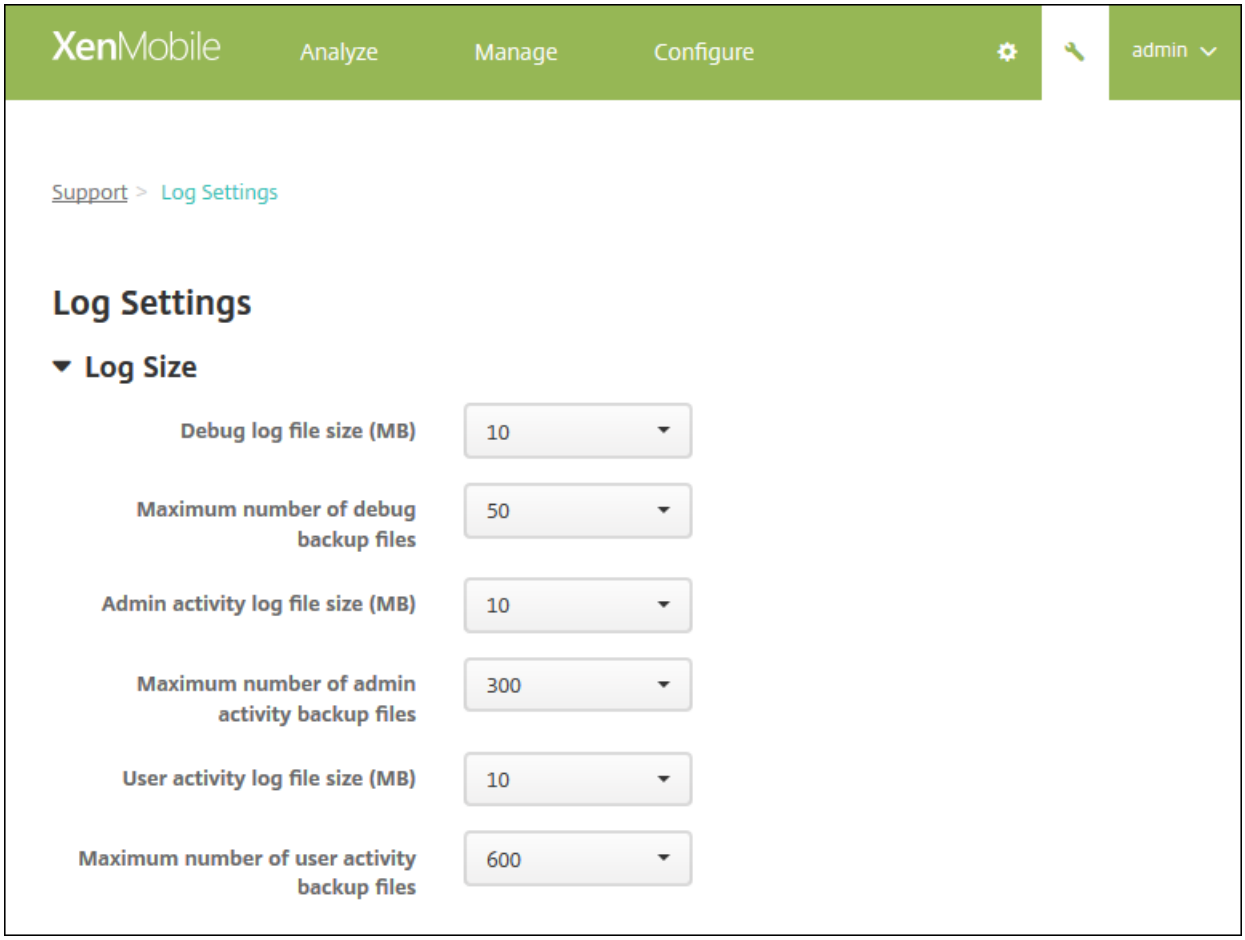
Na página **Configurações de log**, você pode acessar as seguintes opções:

- **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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Defina estas configurações:

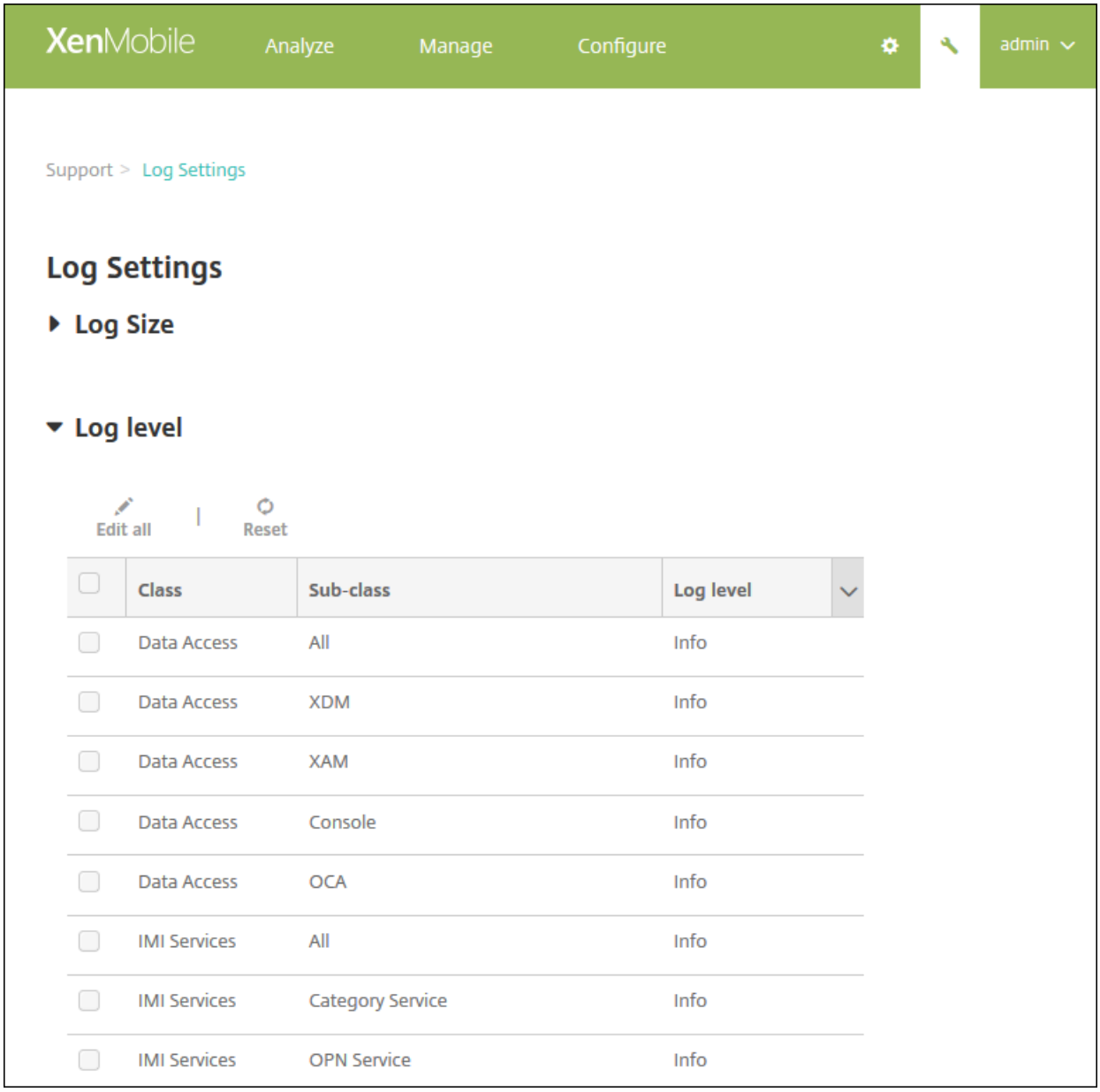
- **Tamanho de arquivo do log de depuração (MB)**: na lista, clique em um tamanho entre 5 MB e 20 MB para alterar o tamanho máximo do arquivo de depuração. O tamanho padrão do arquivo é **10 MB**.
- **Número máximo de arquivos de backup de depuração**: na lista, clique no número máximo de arquivos de 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 padrão do arquivo é **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 padrão do arquivo é **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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

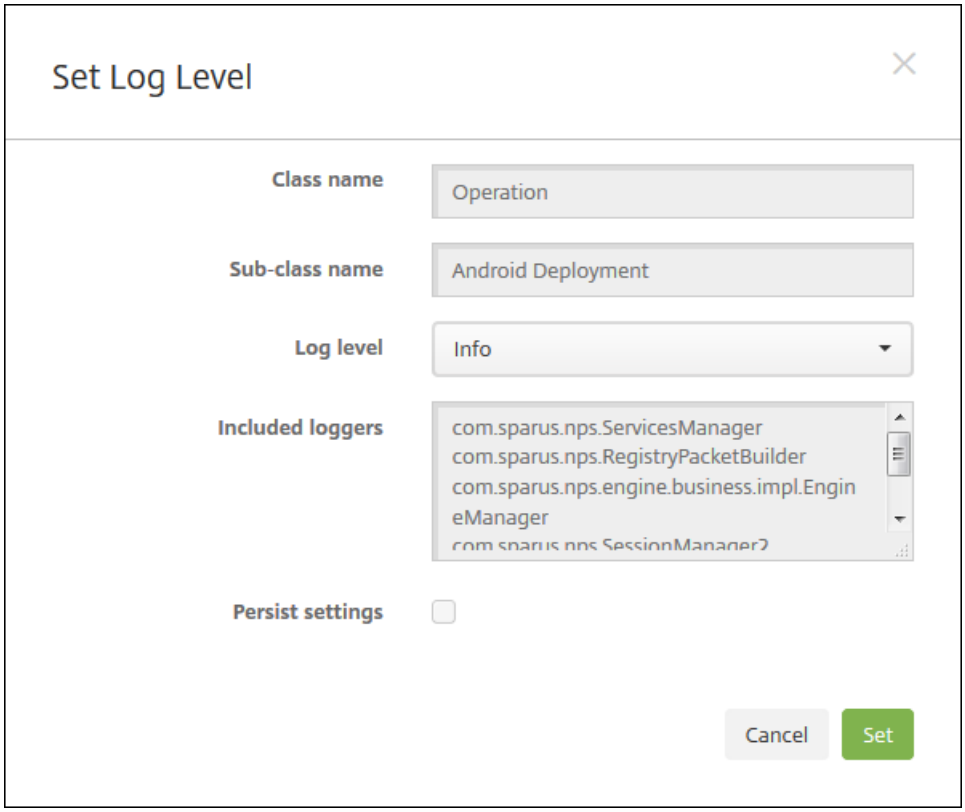


2. Você pode optar por um dos seguintes procedimentos:

- Clique na caixa de seleção ao lado de uma classe e, em seguida, clique em **Definir nível** para alterar o nível de log somente dessa classe.
- Clique em **Editar** tudo para aplicar a alteração de nível de log a todas as classes na tabela.

É exibida a caixa de diálogo **Definir nível de log**, na qual você pode definir o nível de log e selecionar se as configurações de nível de log deverão ser mantidas quando você reiniciar o XenMobile Server.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



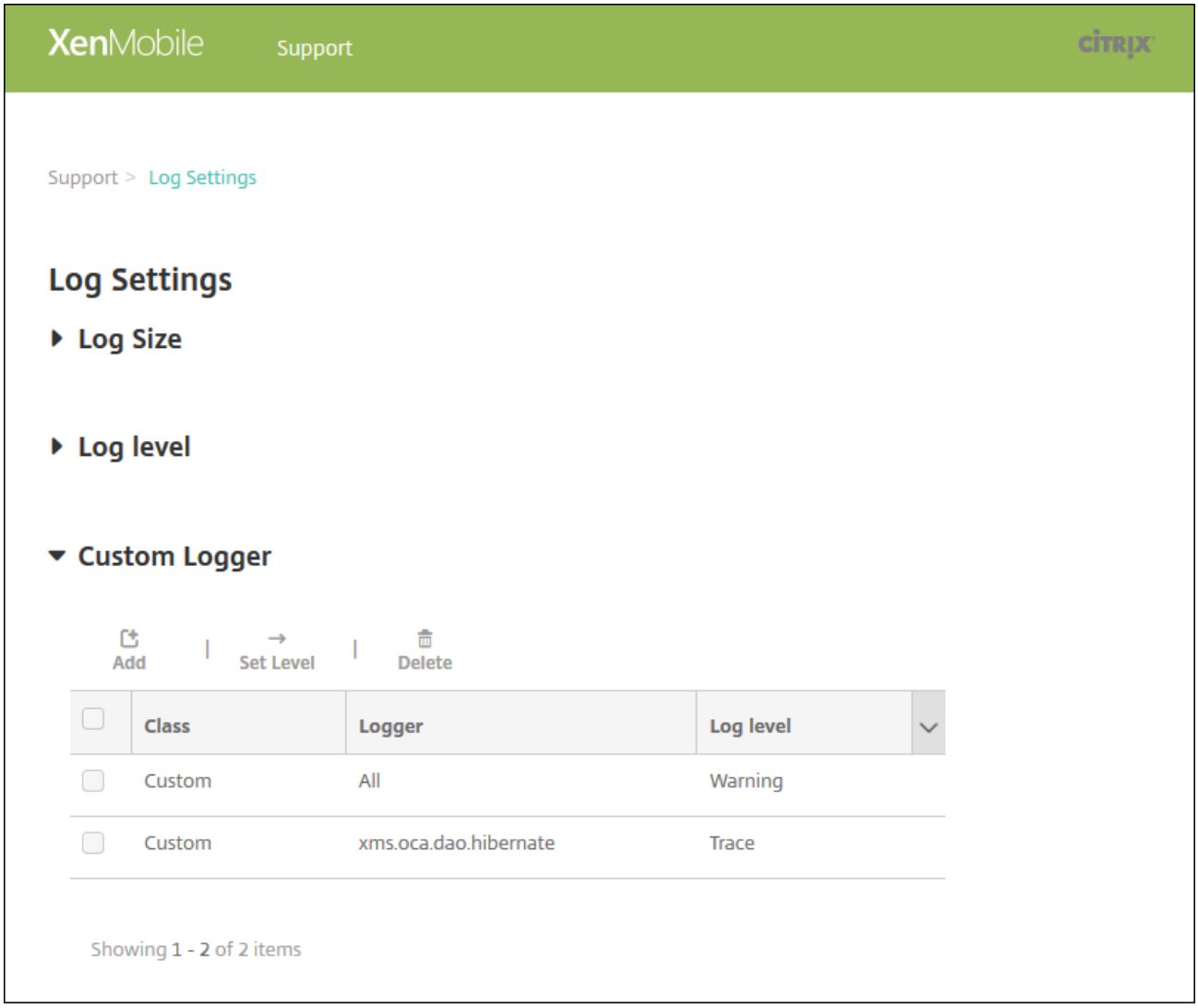
- **Nome da classe**: esse campo exibirá Todas quando você estiver alterando o nível de log de todas as classes ou exibe o nome da classe individual; ele não é editável.
- **Nome da subclasse**: esse campo exibirá Todas quando você estiver alterando o nível de log de todas as classes ou exibe o nome 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.

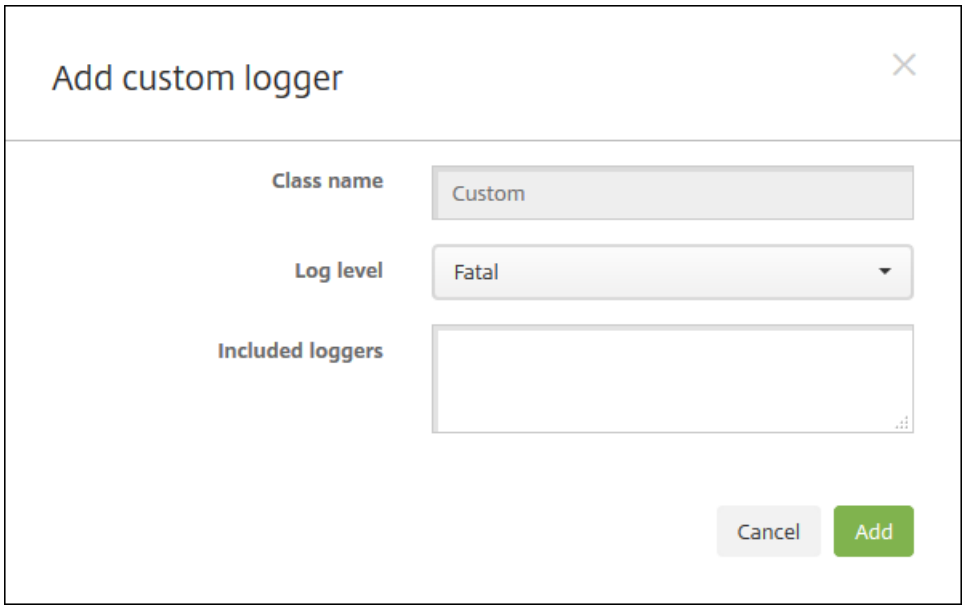
Para adicionar um Agente de Log Personalizado

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



2. Clique em Adicionar. A caixa de diálogo **Adicionar agente de log personalizado** é exibida.



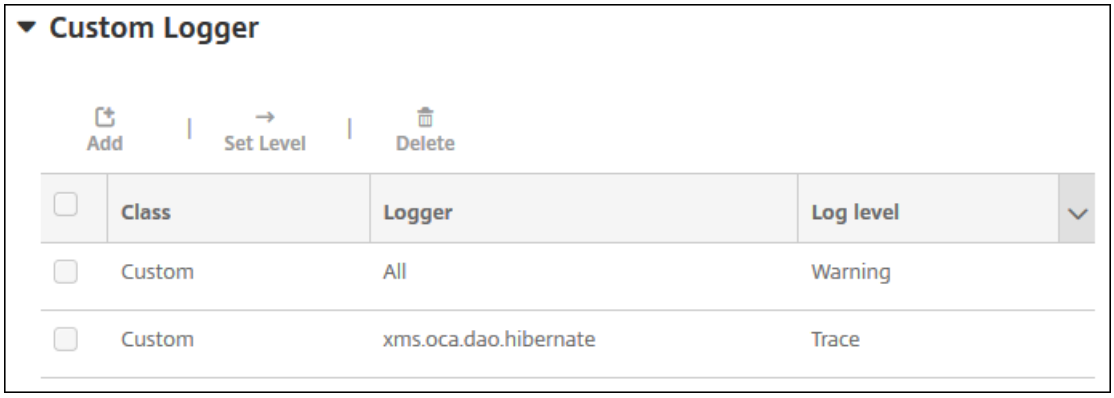
3. Defina estas configurações:

- **Nome da classe**: esse campo exibe **Personalizado**; ele não é editável.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **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 desejar 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**.



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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Provedor de serviços móveis

Feb 21, 2018

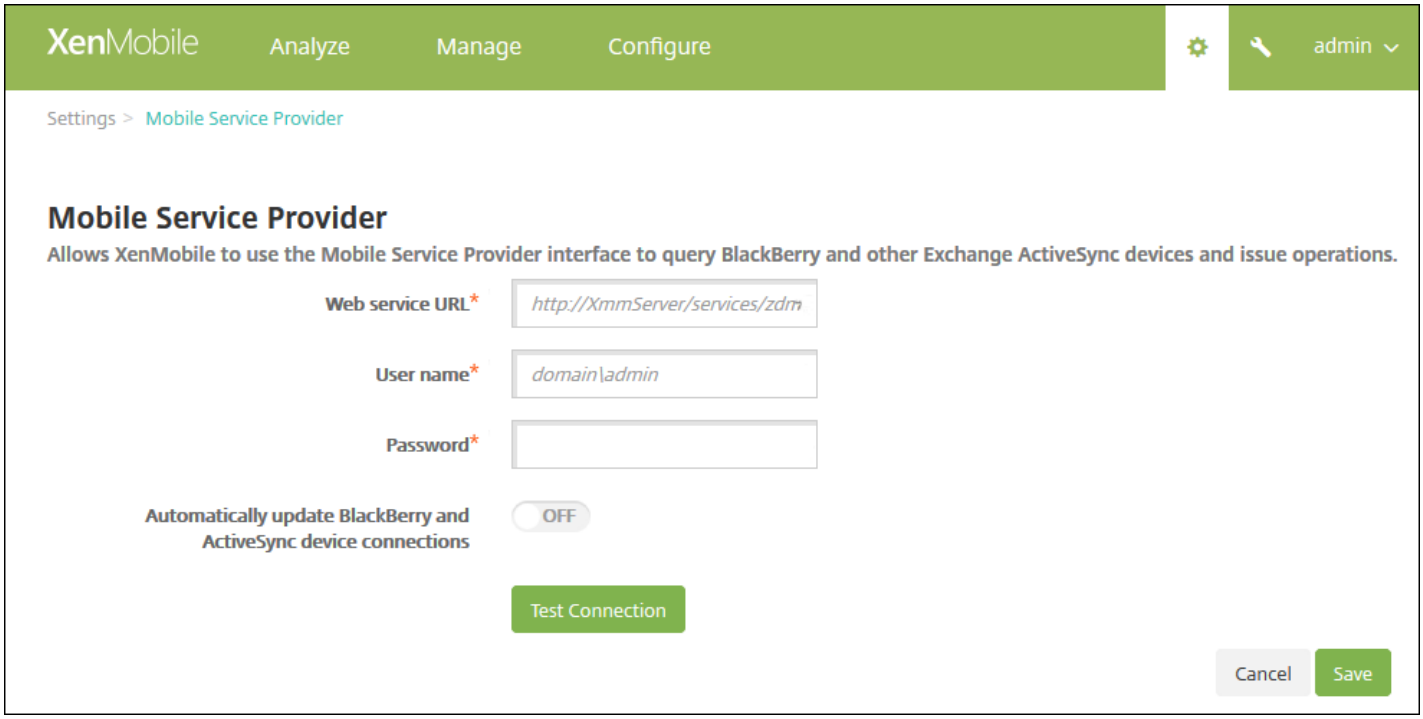
Você pode ativar o XenMobile para usar a interface do Provedor de Serviços Móveis para consultar o BlackBerry e dispositivos Exchange ActiveSync e emitir operações.

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 **Configurações** 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 o URL do serviço da Web; por exemplo, http://XmmServer/services/xdmservice
- **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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Relatórios

Feb 21, 2018

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.

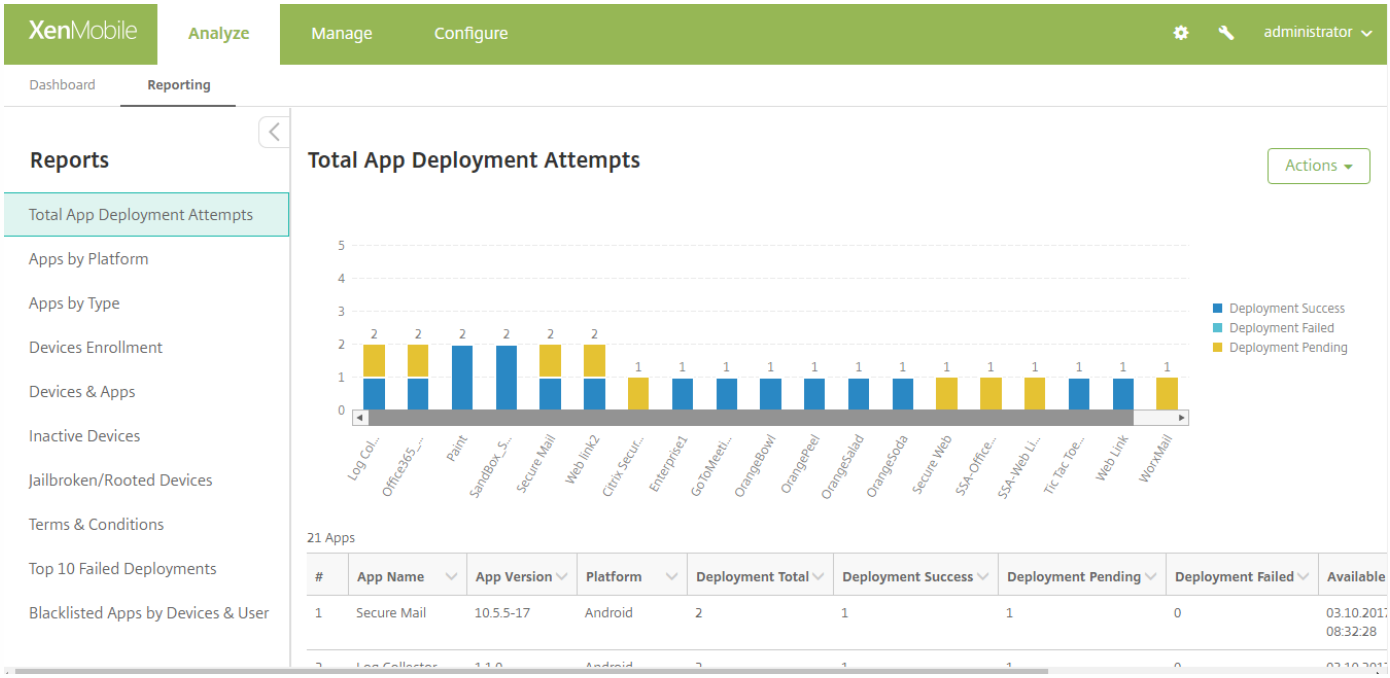
- **Total de tentativas de implantação de aplicativos**: lista aplicativos implantados que os usuários tentaram instalar em seus dispositivos.
- **Aplicativos por plataforma**: lista os aplicativos e as versões de aplicativo por plataforma e versão do dispositivo.
- **Aplicativos por tipo**: lista os 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 em lista negra que os usuários têm em seus dispositivos.

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:

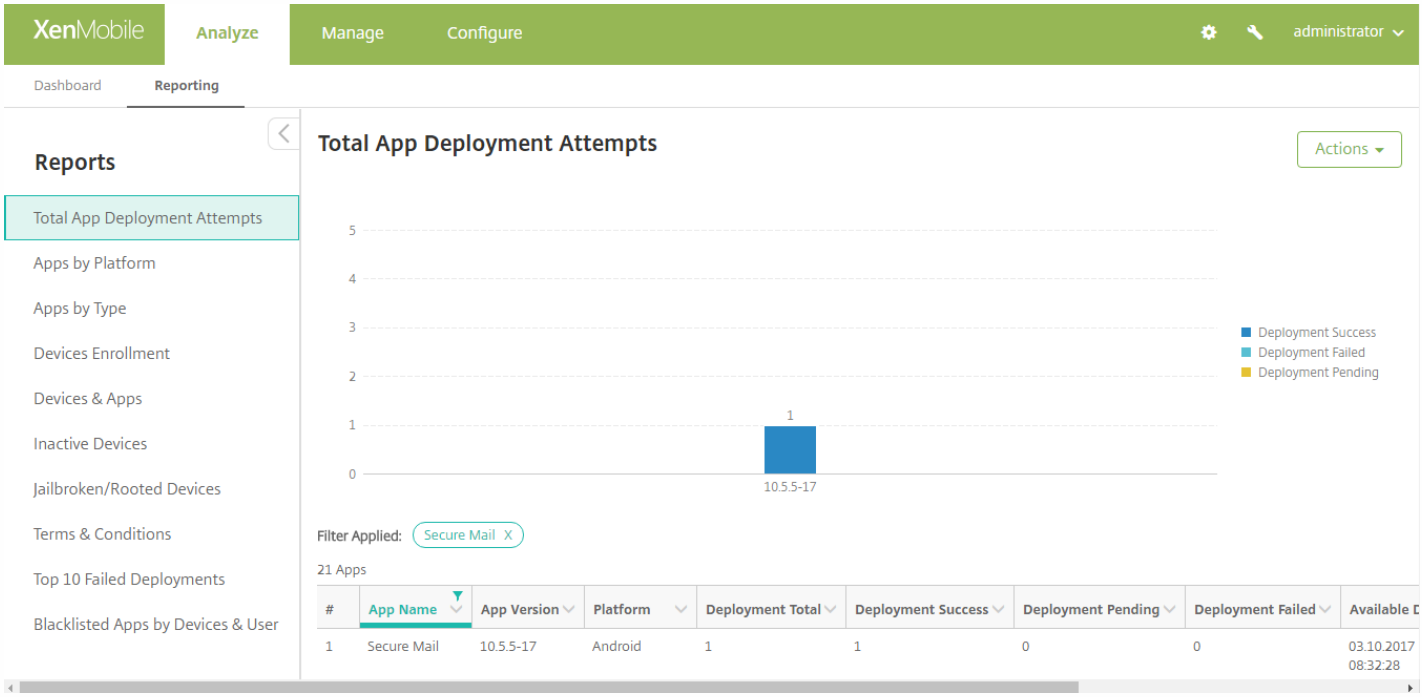
1. No console XenMobile, clique em **Analisar > Relatórios**. A página **Relatórios** é exibida.
2. Clique no relatório que você desejar gerar.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



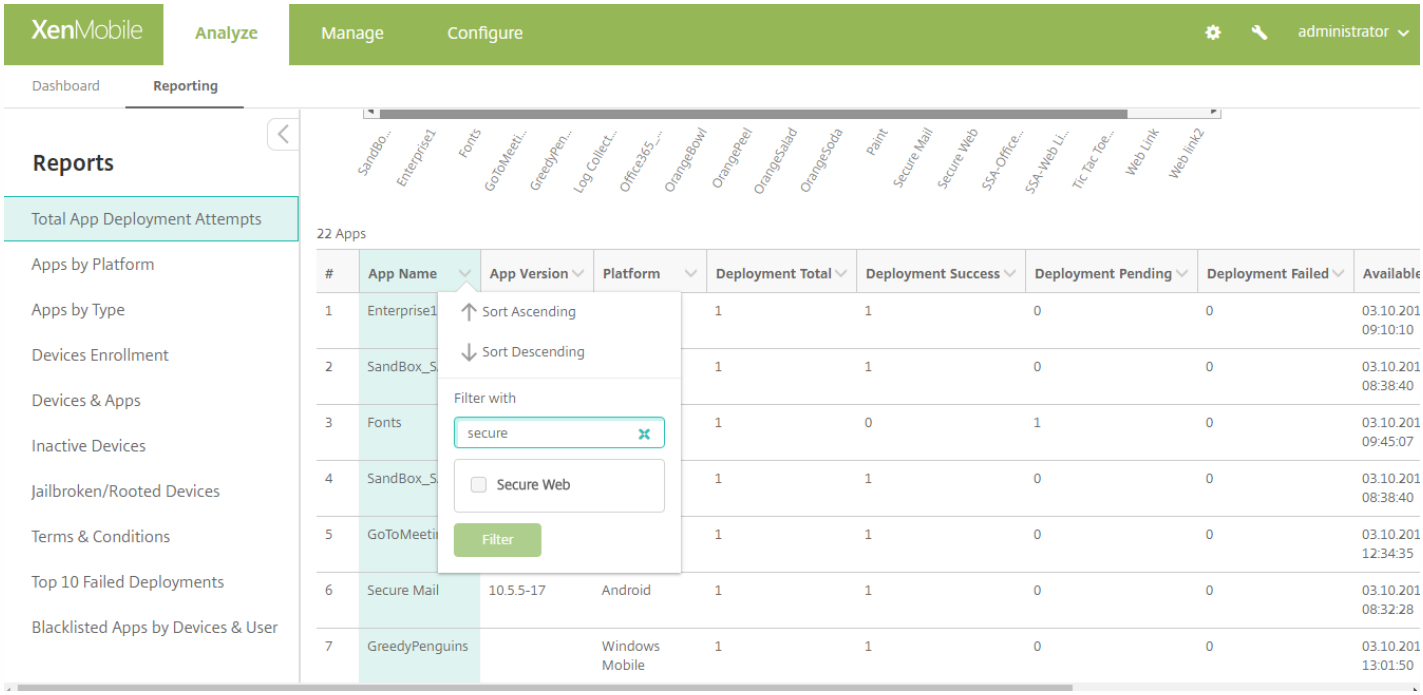
Para exibir mais detalhes de um relatório:

- Clique em áreas do gráfico para fazer uma busca detalhada e obter mais informações sobre detalhes.



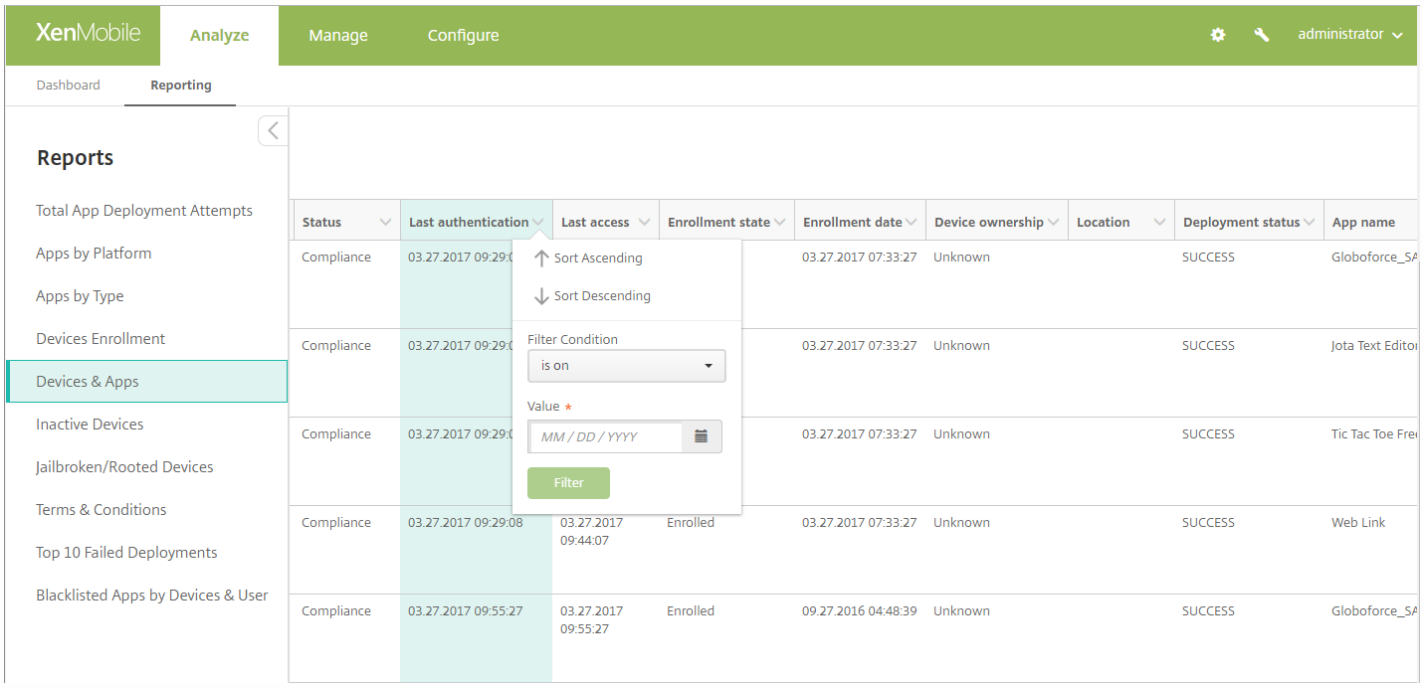
- Para classificar, filtrar ou pesquisar uma coluna da tabela, clique no cabeçalho da coluna.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



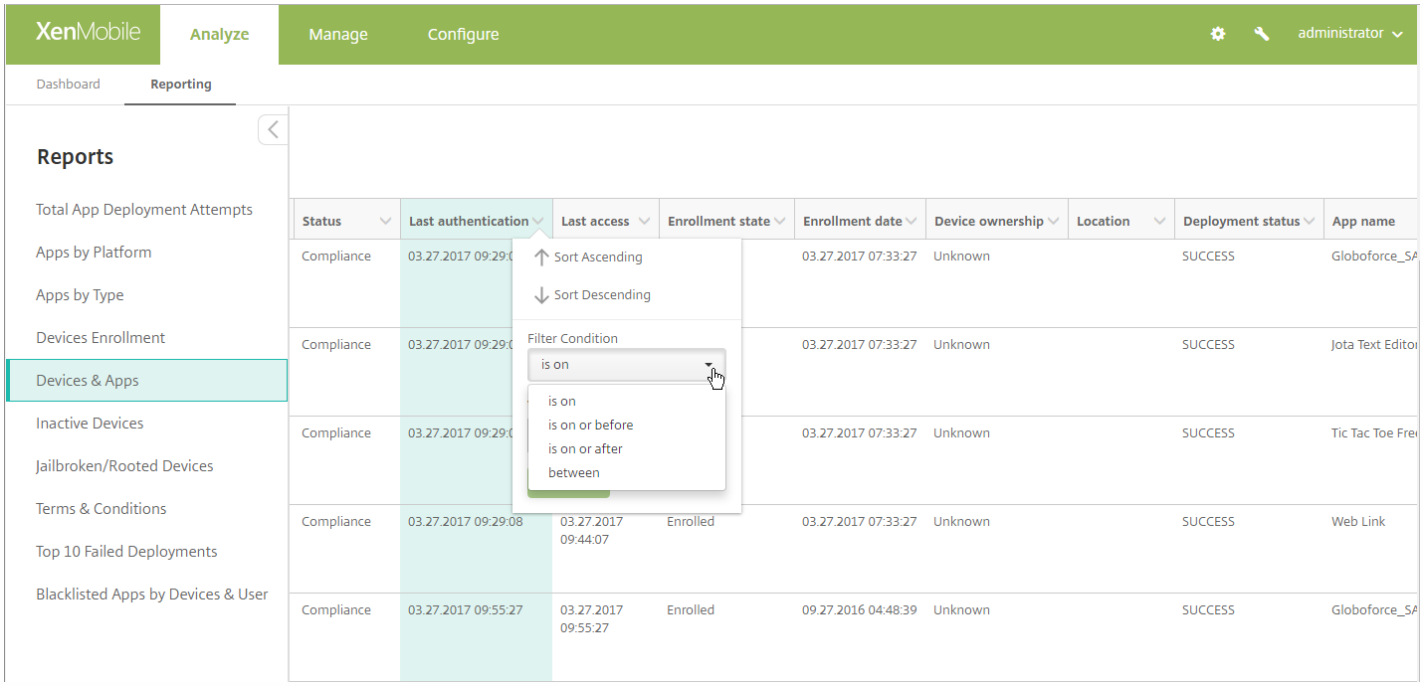
- Para filtrar o relatório por data:

  Clique em um cabeçalho de coluna para exibir as configurações de filtro.

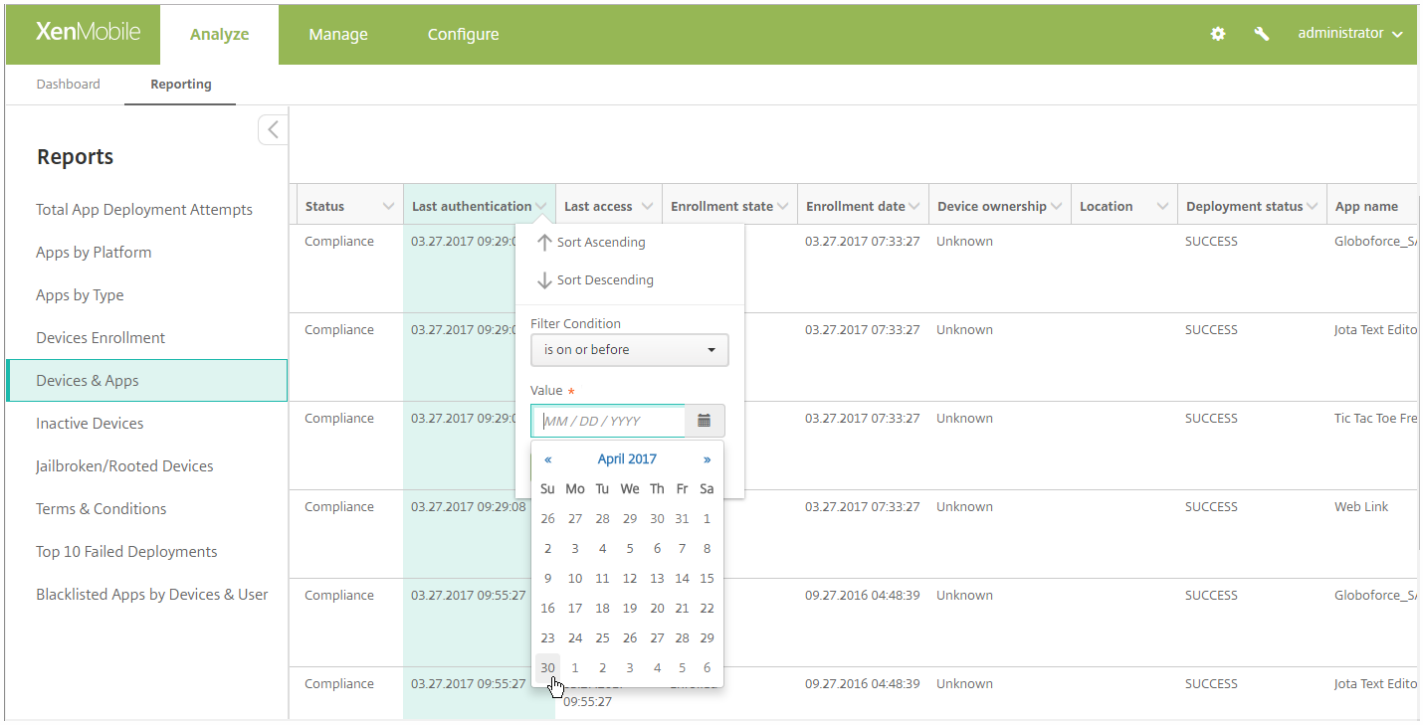


Em **Condição do filtro**, escolha como você deseja restringir as datas informadas.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

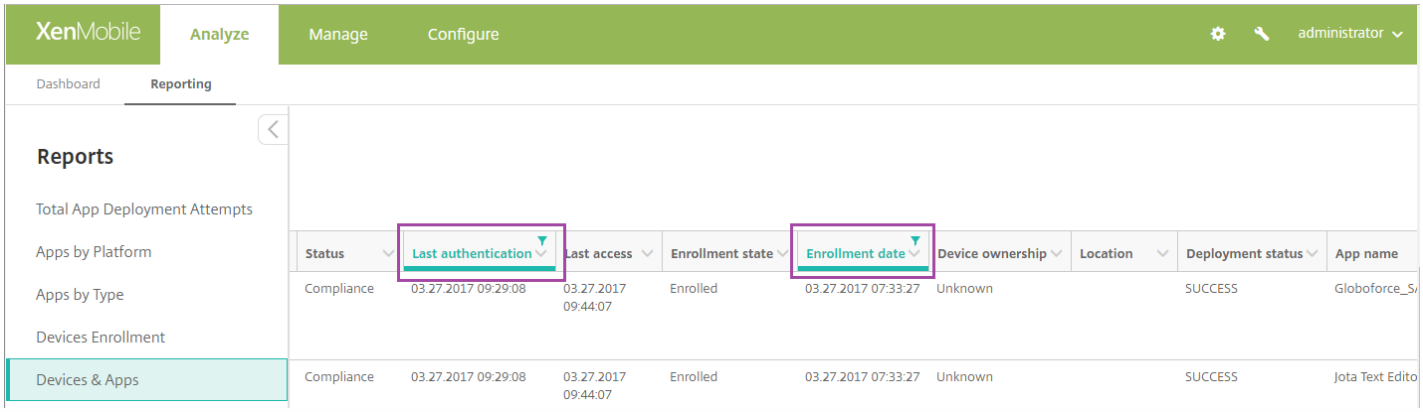


Use o seletor de data para especificar as datas.

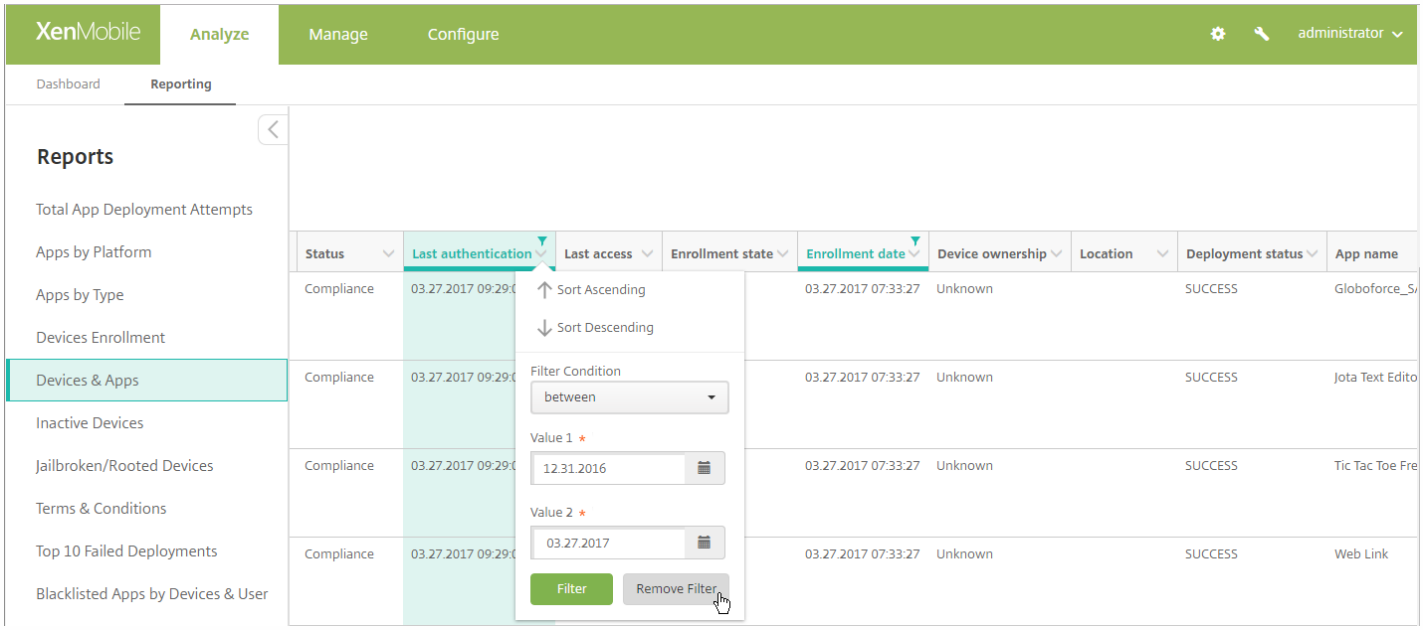


Uma coluna com um filtro de data é exibida conforme o exemplo a seguir.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

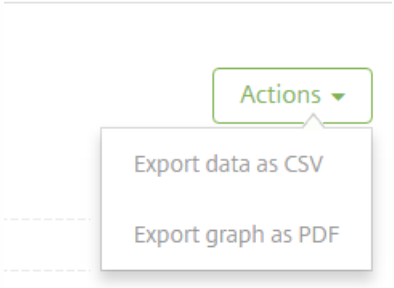


Para remover um filtro, clique no cabeçalho da coluna e depois em **Remover filtro**.



Para exportar um gráfico ou uma tabela:

- Para exportar o plano no formato PDF, clique em **Ação > Exportar gráfico como PDF**.
- Para exportar os dados da tabela no formato CSV, clique em **Ação > Exportar dados como CSV**.



Important

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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

com várias associações JOIN que leva algum tempo para executar prejudica o desempenho do XenMobile Server durante esse período.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

SNMP monitoring

Mar 19, 2018

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.

SNMP v3 Monitoring é compatível com o XenMobile Server 10.8 e versões posteriores.

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 no local.

As etapas gerais para configurar o SNMP são as seguintes.

1. **Acrescentar 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	Identificador de objeto (OID) de monitoramento	Descrição
Carga do processador	.1.3.6.1.2.1.25.3.3.1.2	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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

		interceptação SNMP.
Média de carga em um minuto	.1.3.6.1.4.1.2021.10.1.5.1	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.
Média de carga em cinco minutos	.1.3.6.1.4.1.2021.10.1.5.2	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.
Média de carga em 15 minutos	.1.3.6.1.4.1.2021.10.1.5.3	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.
Memória disponível total	.1.3.6.1.4.1.2021.4.11	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
Armazenamento total em disco usado	.1.3.6.1.4.1.2021.9.1.9.1	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.
Utilização da memória heap de Java	.1.3.6.1.4.1.3845.5.1.2.4.0	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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

		personalizado, o XenMobile gera a interceptação SNMP.
Uso de metaespaço de Java	.1.3.6.1.4.1.3845.5.1.2.5.0	Monitora o uso de metaspace Java do XenMobile para cada intervalo definido pelo usuário. Se o uso exceder o valor de limite, o XenMobile gera a interceptação SNMP.
Conectividade de LDAP	.1.3.6.1.4.1.3845.5.1.1.18.1.0	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.
Conectividade de DNS	.1.3.6.1.4.1.3845.5.1.1.18.2.0	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.
Conectividade do servidor do Google Store	.1.3.6.1.4.1.3845.5.1.1.18.3.0	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.
Conectividade do Windows Phone Store	.1.3.6.1.4.1.3845.5.1.1.18.4.0	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.
Conectividade do Windows Tab Store	.1.3.6.1.4.1.3845.5.1.1.18.5.0	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.
Conectividade do servidor do Windows Security Token	.1.3.6.1.4.1.3845.5.1.1.18.6.0	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.
Conectividade do servidor do Windows Notification	.1.3.6.1.4.1.3845.5.1.1.18.7.0	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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Conectividade do servidor do APNs (Apple Push Notification Service)	.1.3.6.1.4.1.3845.5.1.1.18.8.0	Monitora a conectividade entre o APNs e os nós XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.
Conectividade do servidor Apple Feedback	.1.3.6.1.4.1.3845.5.1.1.18.9.0	Monitora a conectividade entre o servidor do Apple Feedback e os nós XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.
Conectividade do servidor do Apple Store	.1.3.6.1.4.1.3845.5.1.1.18.10.0	Monitora a conectividade entre o servidor do Apple Store e os nós XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.
Conectividade com o banco de dados XenMobile	.1.3.6.1.4.1.3845.5.1.1.18.11.0	Monitora a conectividade entre o banco de dados XenMobile e os nós XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.
Conectividade do servidor do Google Cloud Messaging	.1.3.6.1.4.1.3845.5.1.1.18.12.0	Monitora a conectividade entre o servidor do Google Cloud Messaging e os nós XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.
Conectividade do servidor de licenças Citrix	.1.3.6.1.4.1.3845.5.1.1.18.13.0	Monitora a conectividade entre o servidor de licença Citrix e os nós XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.
Conectividade do NetScaler Gateway	.1.3.6.1.4.1.3845.5.1.1.18.15.0	Monitora a conectividade entre o NetScaler Gateway e os nós XenMobile para o intervalo definido pelo usuário. Se a conectividade falhar, o XenMobile gera a interceptação SNMP.
Conectividade entre nós do XenMobile	.1.3.6.1.4.1.3845.5.1.1.18.16.0	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.
Conectividade do serviço de nó do	.1.3.6.1.4.1.3845.5.1.1.18.17.0	Monitora a conectividade entre o serviço de nó do XenMobile Tomcat e os nós XenMobile para o

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile Tomcat		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:

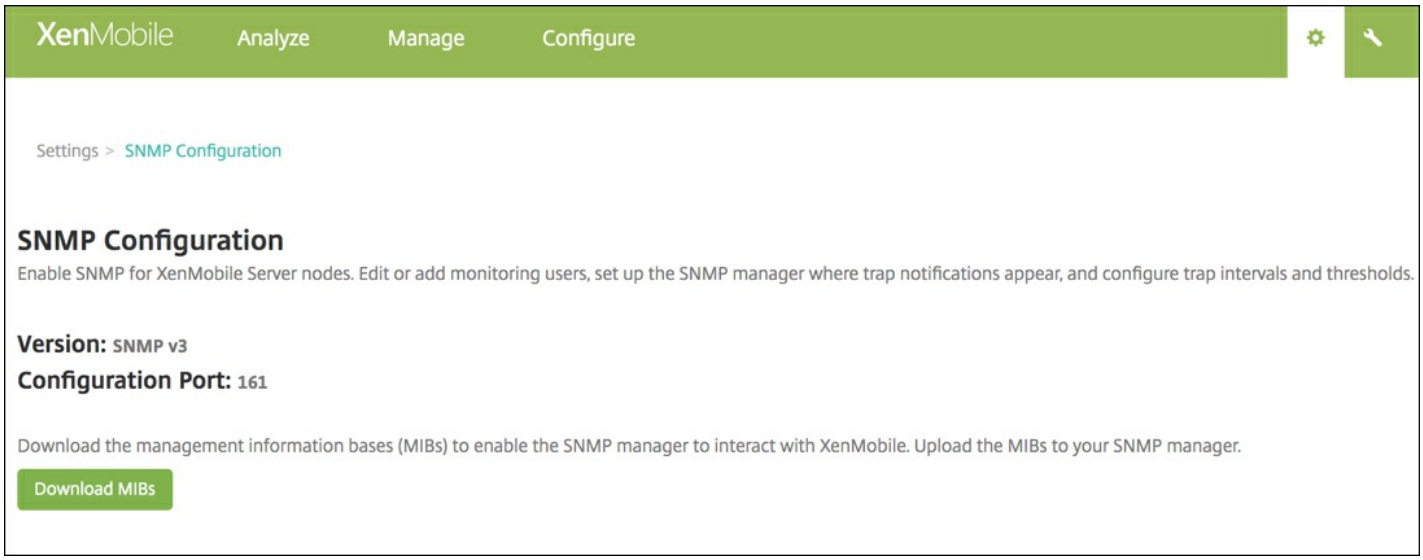
- Frequência de chamadas
- Dados de interceptação a serem coletados e as verificações de limite
- O mecanismo de comunicação entre nós
- Freqüência de verificações de conectividade
- Tempos limite de falhas durante as verificações

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 **Configurações** é exibida.

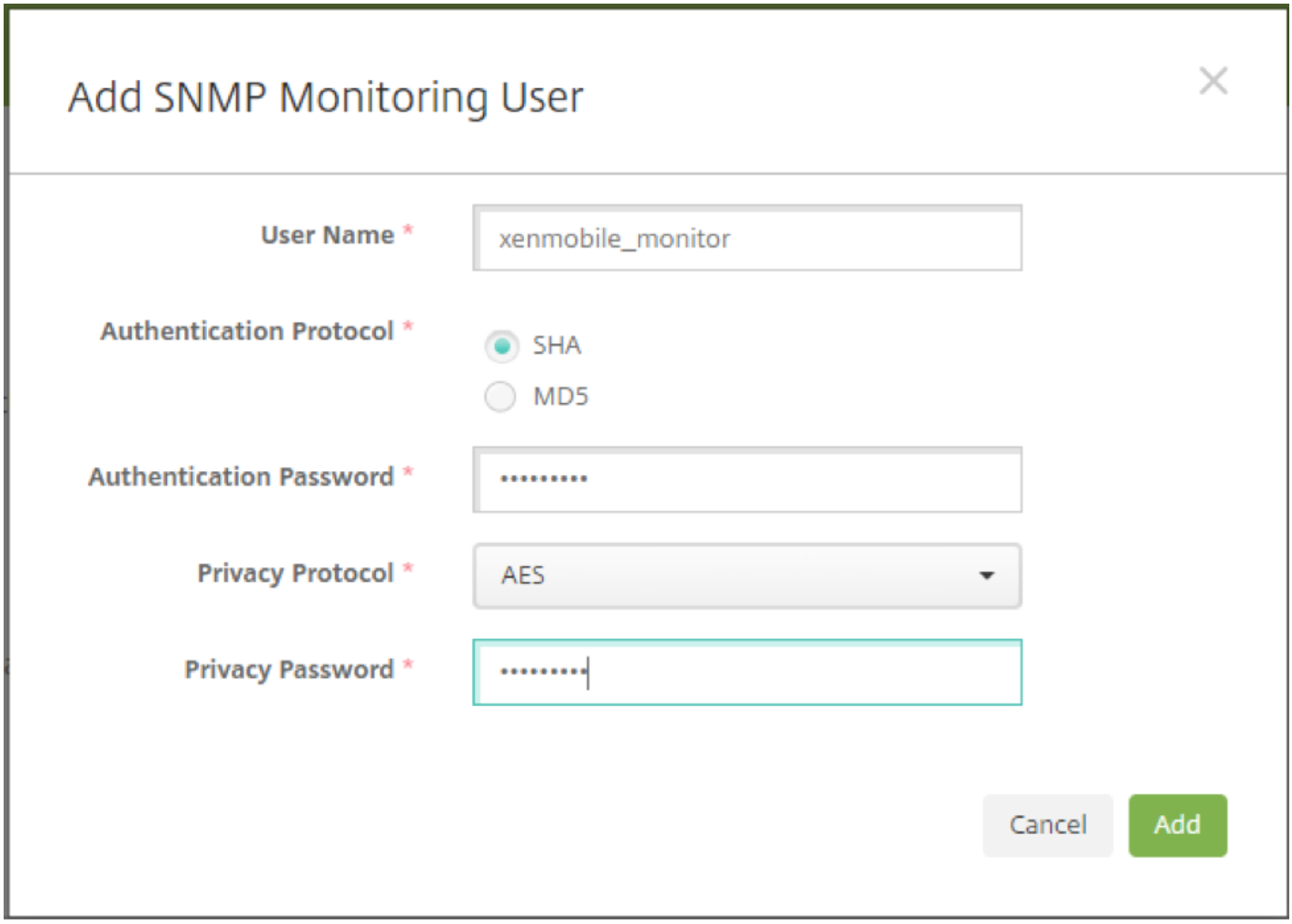
2. Em **Monitoramento**, clique em **Configuração SNMP**. A página **Configuração SNMP** é exibida.



3. Em **Usuários de SNMP Monitoring**, clique em **Adicionar**.

4. Na caixa de diálogo **Adicionar usuário de SNMP Monitoring**, defina as seguintes configurações:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Nome de usuário: o nome do usuário usado para efetuar logon 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)

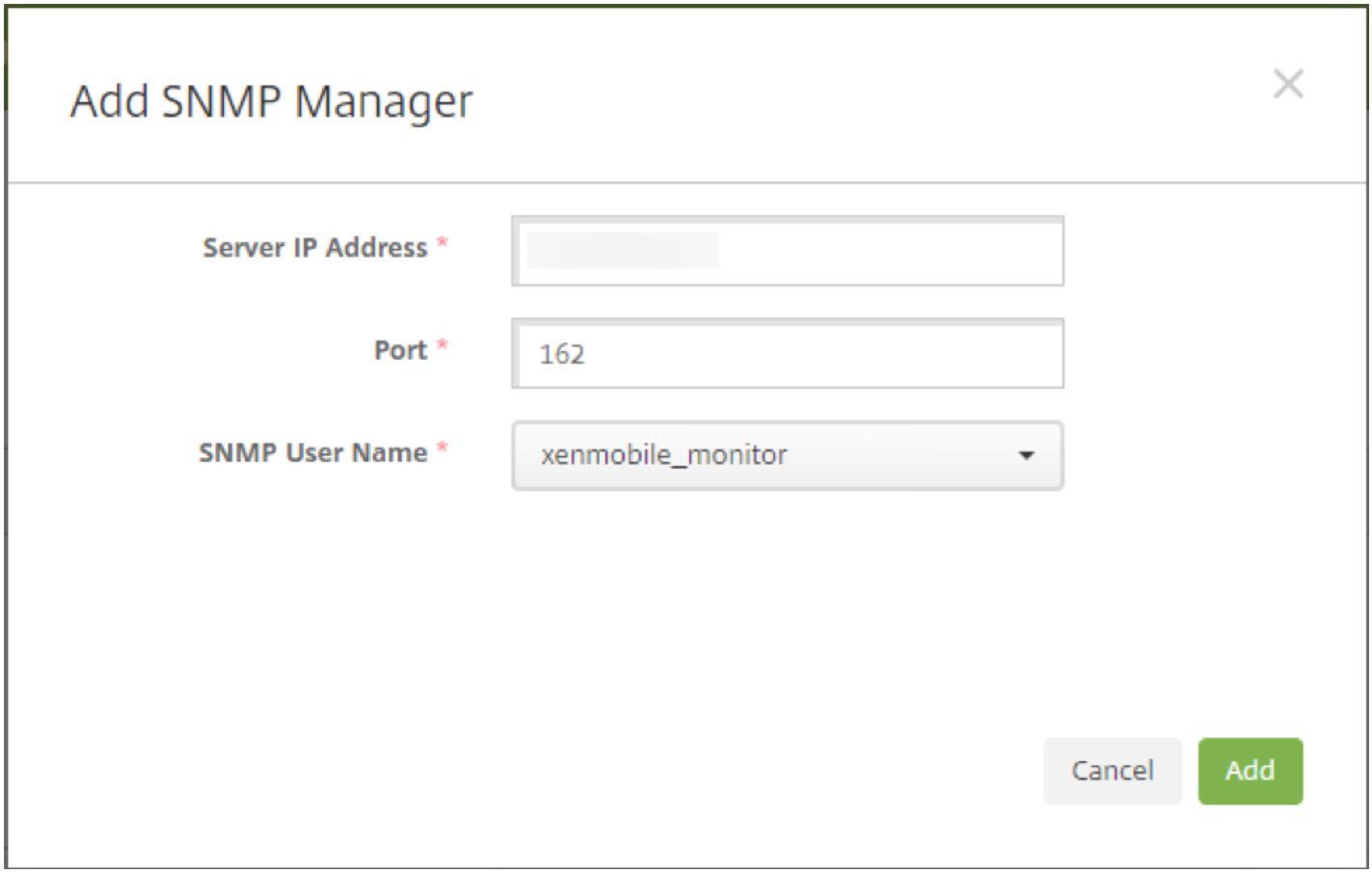
Senha de privacidade: digite uma senha de 8 a 18 caracteres. Você pode incluir caracteres alfanuméricos e especiais.

Para adicionar um SNMP Manager

1. Em **SNMP Managers**, clique em **Adicionar**.

2. Na caixa de diálogo **Adicionar SNMP Manager**, defina as seguintes configurações:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 gerenciador.

Para ativar e configurar interceptações SNMP

Para ajudar a determinar as configurações de interceptação 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 interceptação nos SNMP Managers configurados.

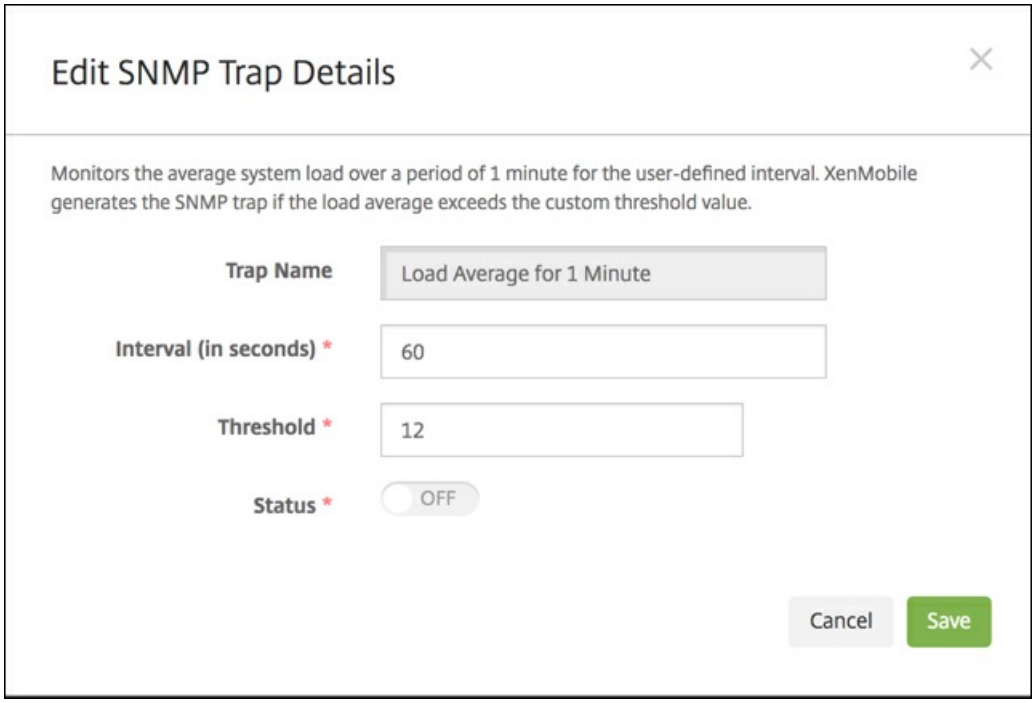
1. Para ativar interceptações individuais, siga um dos destes procedimentos:

- Marque a caixa de seleção ao lado do parâmetro e, em seguida, clique em **Ativar**.
- Para ativar todas as interceptações da lista, marque a caixa de seleção na parte superior e clique em **Ativar**.

2. Para editar uma interceptação, selecione o parâmetro e, em seguida, clique em **Editar**.

3. Na caixa de diálogo **Editar detalhes da interceptação SNMP**, você pode editar os valores de limite para interceptações individuais.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Nome da interceptação: o nome da interceptação. 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 interceptações:

- 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Pacotes de suporte

Feb 27, 2018

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.

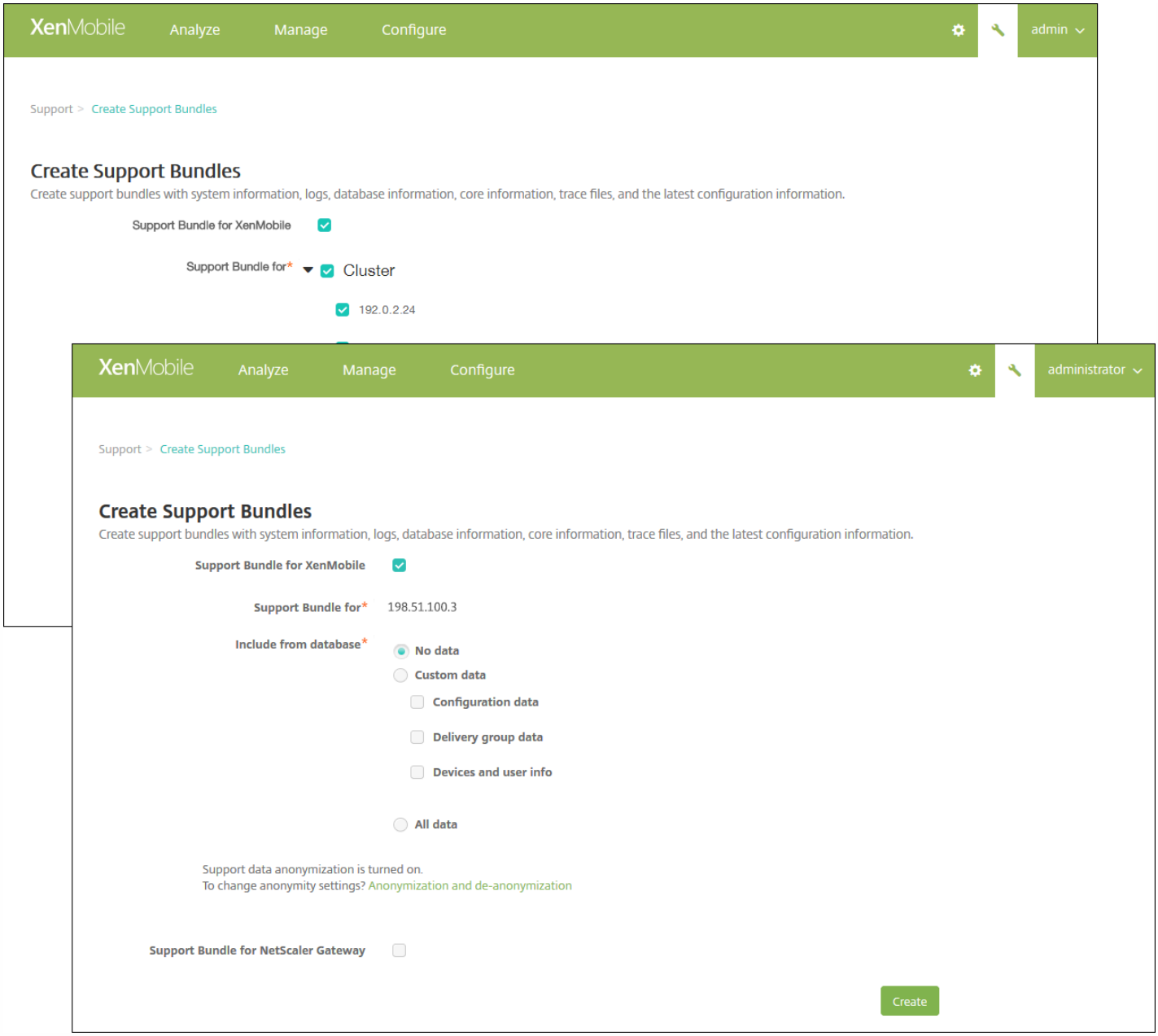
- DebugLogFile.log
- AdminAuditLogFile.log
- UserAuditLogFile.log
- HibernateStats.log

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



3. Verifique se a caixa de seleção **Pacote de suporte para XenMobile** está marcada.

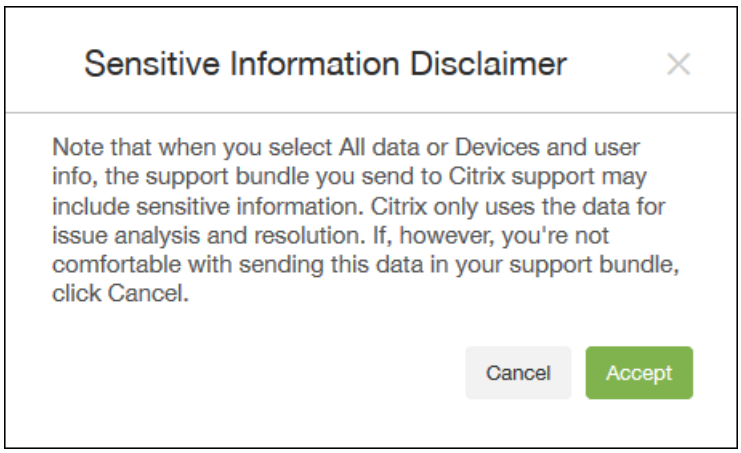
4. Se o seu ambiente do XenMobile contiver nós de cluster, em **Pacote de suporte para**, você poderá selecionar todos os nós ou qualquer combinação de nós dos quais extrair dados.
5. Em **Incluir do banco de dados**, você pode optar por um dos seguintes procedimentos:

- 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

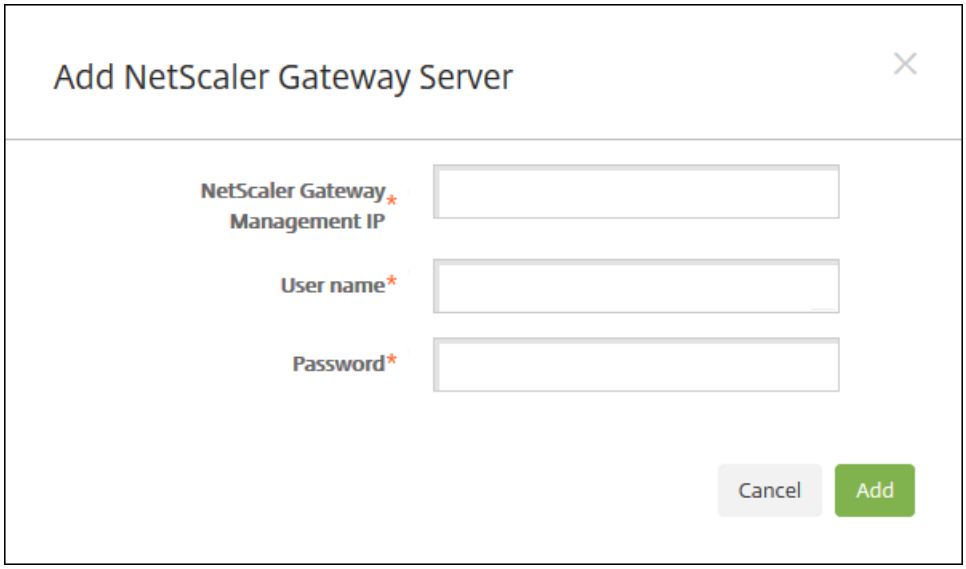


6. A opção **Anonimização de dados de suporte está ativada** indica que a configuração padrão é anonimizar os dados. A anonimização de dados significa que dados confidenciais do usuário, do servidor e da rede são feitos anônimos nos pacotes de suporte.

Para alterar essa configuração, clique em **Anonimização e desanonimização**. Para obter mais informações sobre a anonimização de dados, consulte Anonimização de dados nos pacotes de suporte.

7. Para incluir pacotes de suporte do NetScaler Gateway: marque a caixa de seleção **Pacote de suporte para o NetScaler Gateway** e faça o seguinte:

a. Clique em Adicionar. A caixa de diálogo **Adicionar servidor do NetScaler Gateway** é exibida.



b. Em **IP de gerenciamento do NetScaler Gateway**, digite o endereço IP de gerenciamento do NetScaler para o NetScaler Gateway do qual você deseja extrair os dados de pacote de suporte.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nota: se você estiver criando um pacote de um servidor NetScaler 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 NetScaler Gateway.

Nota: se você estiver criando um pacote de um servidor NetScaler Gateway que já foi adicionado, o nome do usuário será fornecido.

7. Clique em Adicionar. O novo pacote de suporte do NetScaler Gateway é adicionado à tabela.

8. Repita a Etapa 7 para adicionar mais pacotes de suporte do NetScaler Gateway.

9. Clique em **Criar**. O pacote de suporte é criado, e dois novos botões, **Carregar em CIS** e **Baixar para o cliente** são exibidos.

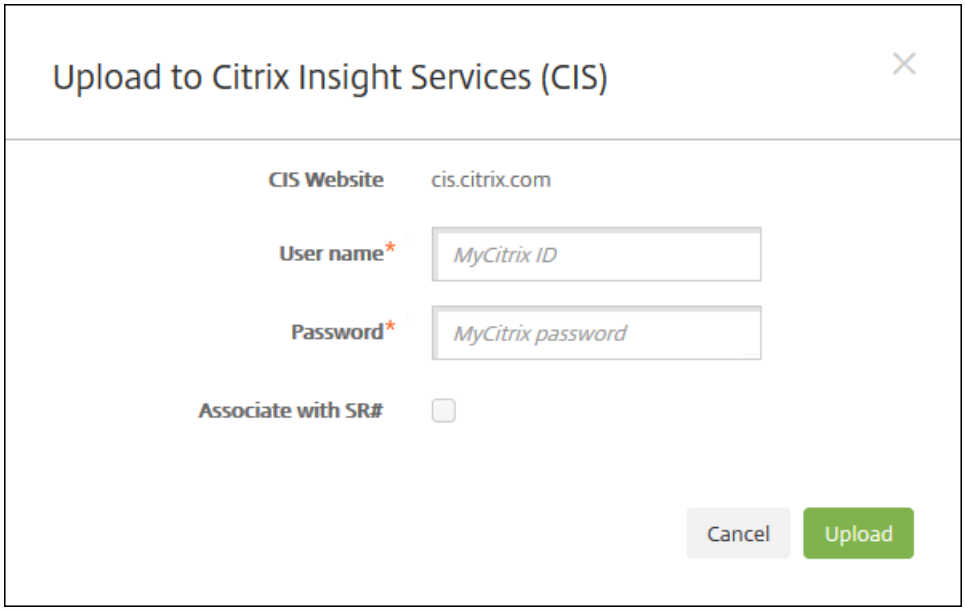
Carregando pacotes de suporte para o Citrix Insight Services

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**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

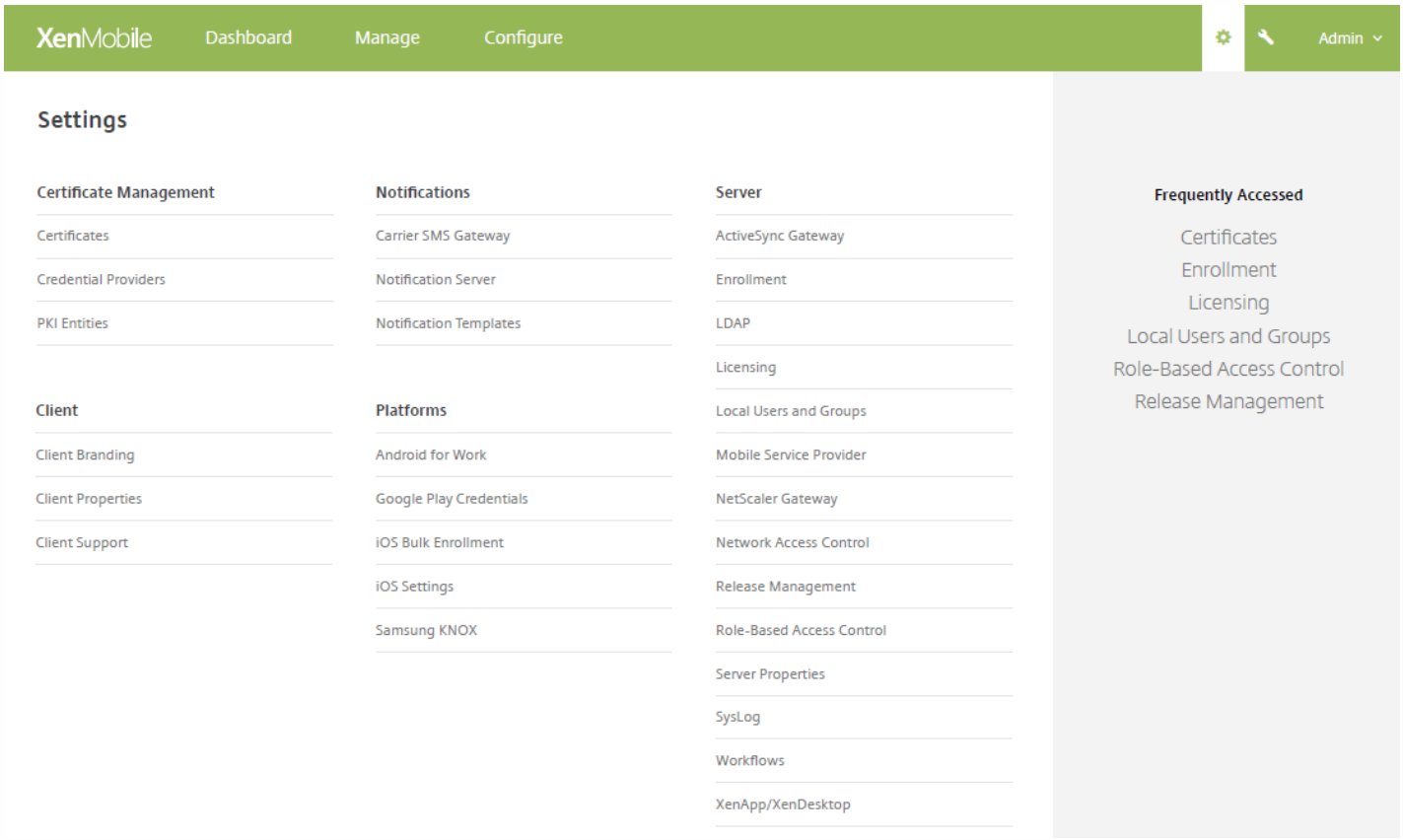
Opções de suporte e suporte remoto

Feb 21, 2018

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 **Configurações** 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 são exibidas. Se você ativar a opção Armazenar logs no ShareFile, os logs serão enviados diretamente ao ShareFile. Caso contrário, os logs serão enviados ao XenMobile e, em seguida, enviados por email para o suporte técnico. Além disso, é exibida a opção **Se o envio direto falhar, usar email**, que é ativada por padrão. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

4. Clique em **Salvar**.

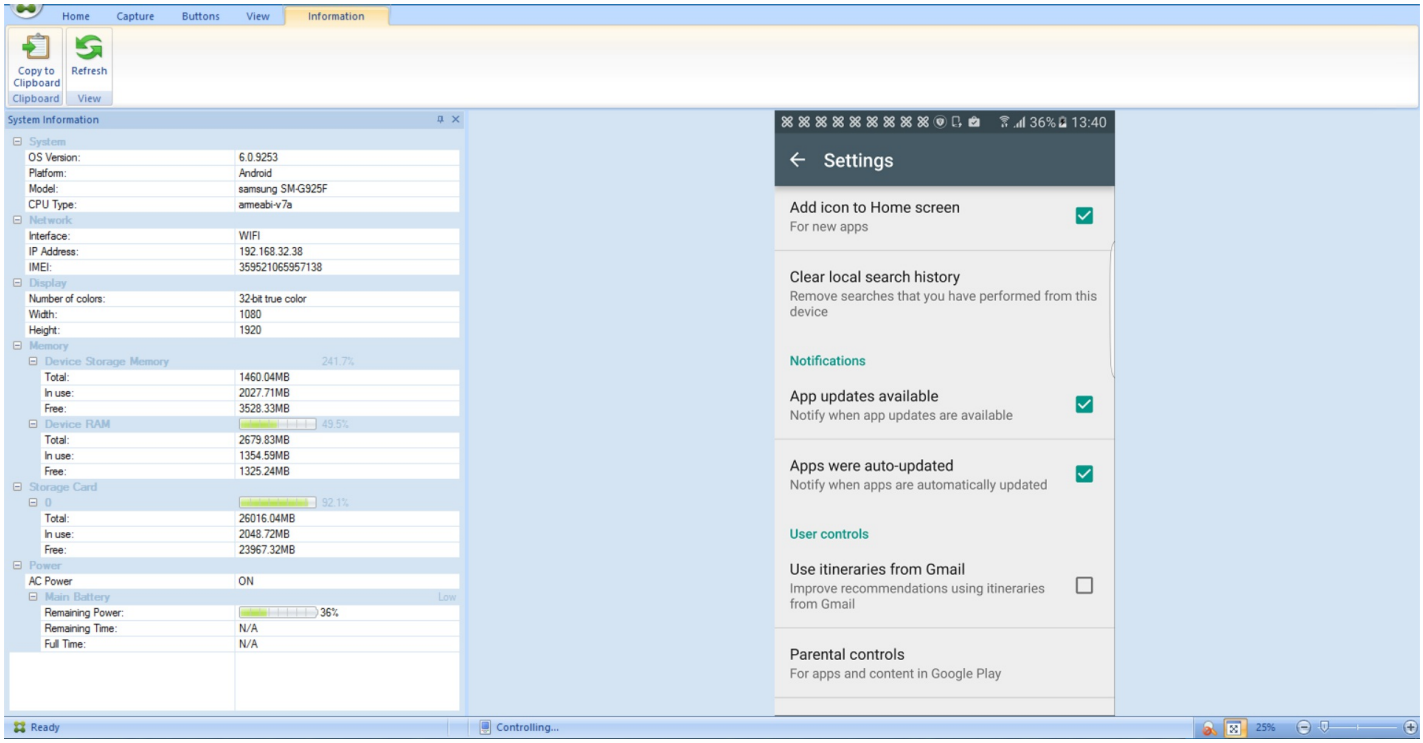
Suporte remoto

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 os clientes do XenMobile Service e não é suportado para implantações em cluster do XenMobile Server 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:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- 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 software de Suporte Remoto

1. Para baixar o instalador do Remote Support, vá para a página de download do XenMobile 10 e faça login na sua conta.
2. Expanda **Ferramentas** e baixe o XenMobile Remote Support v9.
   O nome de arquivo do Remote Support é XenMobileRemoteSupport-9.0.0.35265.exe.
3. Clique duas vezes no instalador de Suporte Remoto e siga as instruções do assistente de instalação.

Para instalar o Suporte a partir da linha de comando:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Digite o seguinte comando:

RemoteSupport.exe /S

RemoteSupport é o nome do programa de instalação. Por exemplo:

XenMobileRemoteSupport-9.0.0.35265.exe/S

Você pode usar as variáveis a seguir ao instalar o Remote Support software:

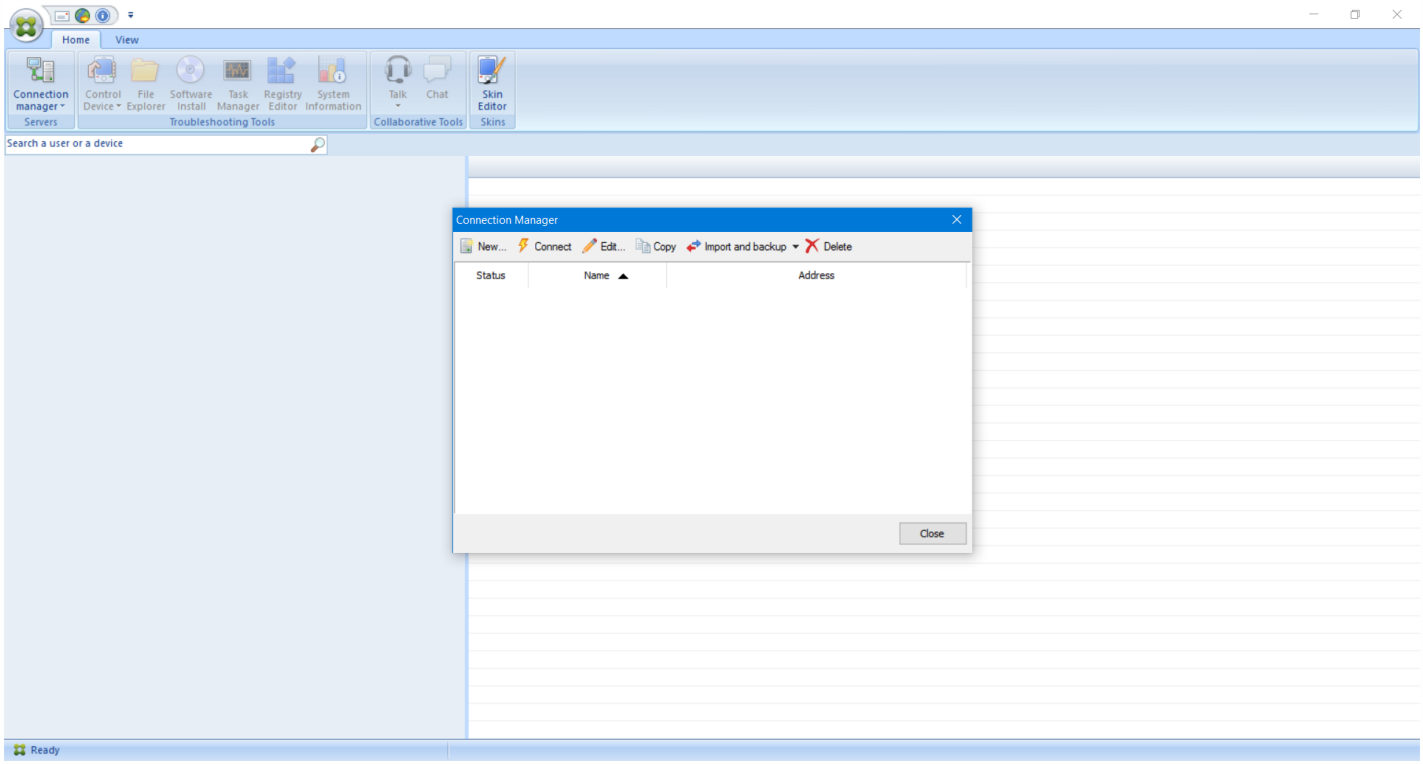
- /S: para instalar o software do Remote Support com os parâmetros padrão.
- /D=dir: para especificar um diretório de instalação personalizado.

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 Políticas 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

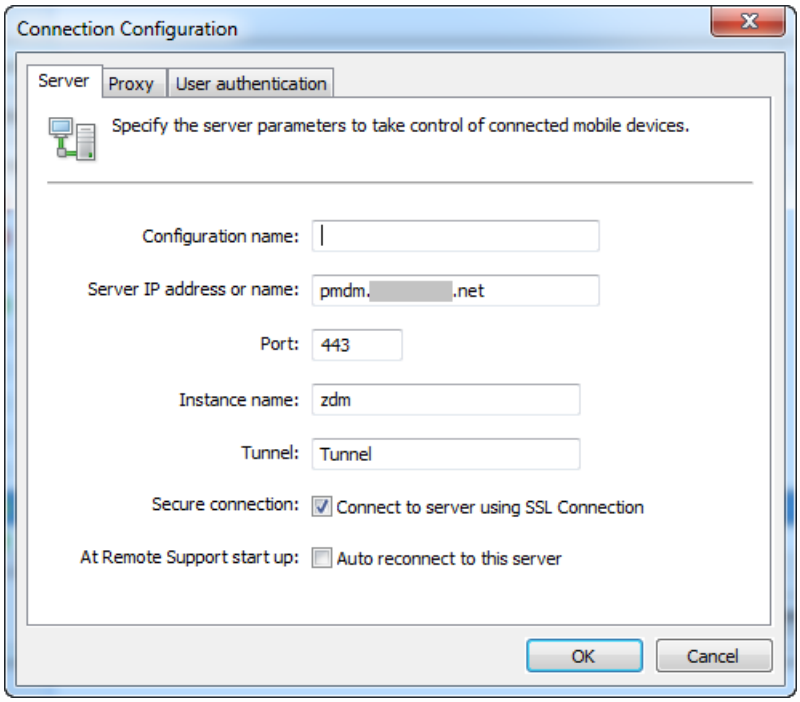
c. Em **Port:** digite um número de porta TCP, conforme definido na configuração de XenMobile Server.

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 for iniciado.



4. Na guia **Proxy**, selecione **Use a http proxy server** e, em seguida, insira as seguintes informações:

a. Em **Proxy IP Address**, digite o endereço IP do servidor proxy.

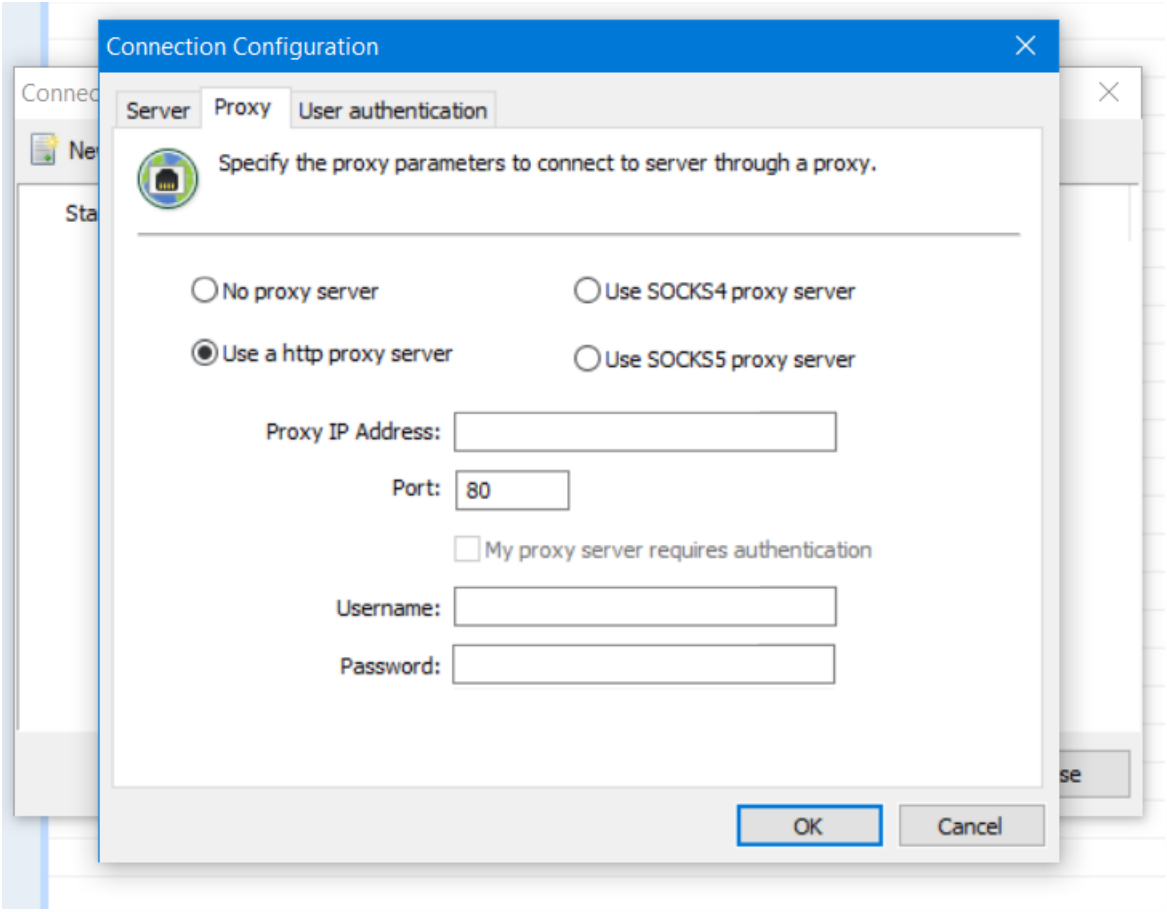
b. Em **Port**, digite um número de porta TCP usada pelo proxy.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 remotamente a tela de dispositivo de controle. 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 Políticas de dispositivo de chave de licença MDM Samsung.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 cadeia de caracteres **Anonymous** aparece na lista.) Você pode controlar esses dispositivos exatamente como o dispositivo de um usuário que fez logon.

Para controlar um dispositivo, selecione o dispositivo clicando na linha respectiva 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Syslog

Feb 21, 2018

Você pode configurar o XenMobile Server (somente no local) para enviar arquivos de log a 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

Você pode usar essas informações para analisar a origem do alerta e executar a ação corretiva, se necessário.

> ## Nota
>
> Nas implantações em nuvem do XenMobile Service, a Citrix não oferece suporte à integração de syslog com um servidor syslog no local. Em vez disso, você pode baixar os logs na página Suporte no console XenMobile. Quando fizer isso, você deverá clicar em **Baixar todos** para obter os logs do sistema. Para obter detalhes, consulte Exibindo e analisando arquivos de log no XenMobile.

1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** 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**.

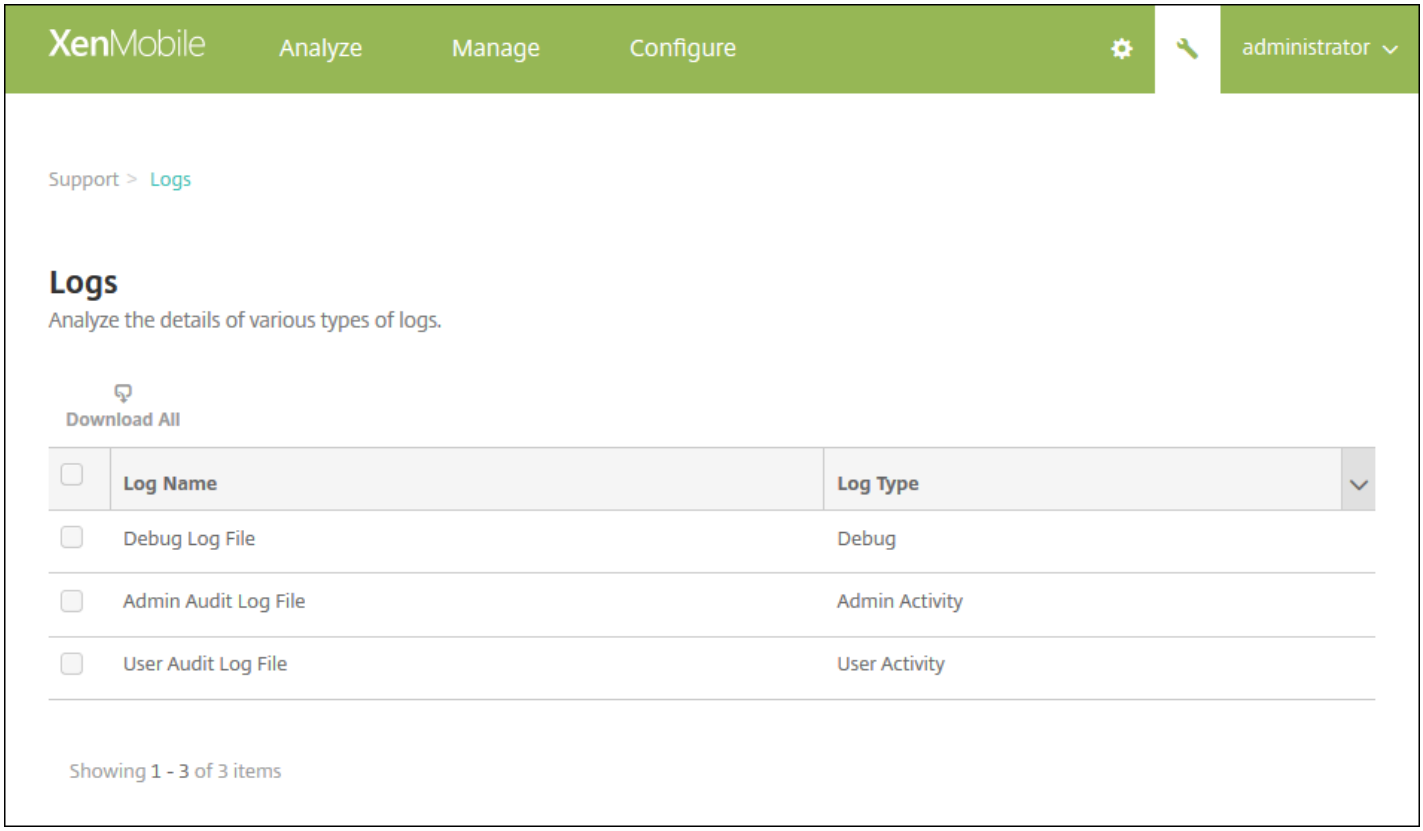
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Exibir e analisar arquivos de log no XenMobile

Feb 21, 2018

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.

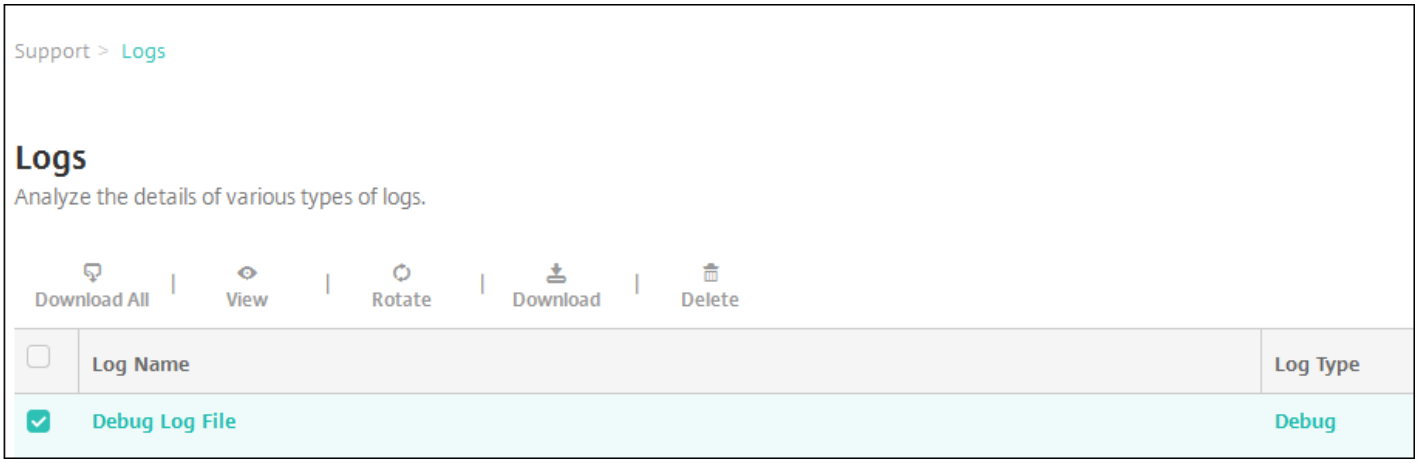


3. Selecione o log que você deseja exibir:

- 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

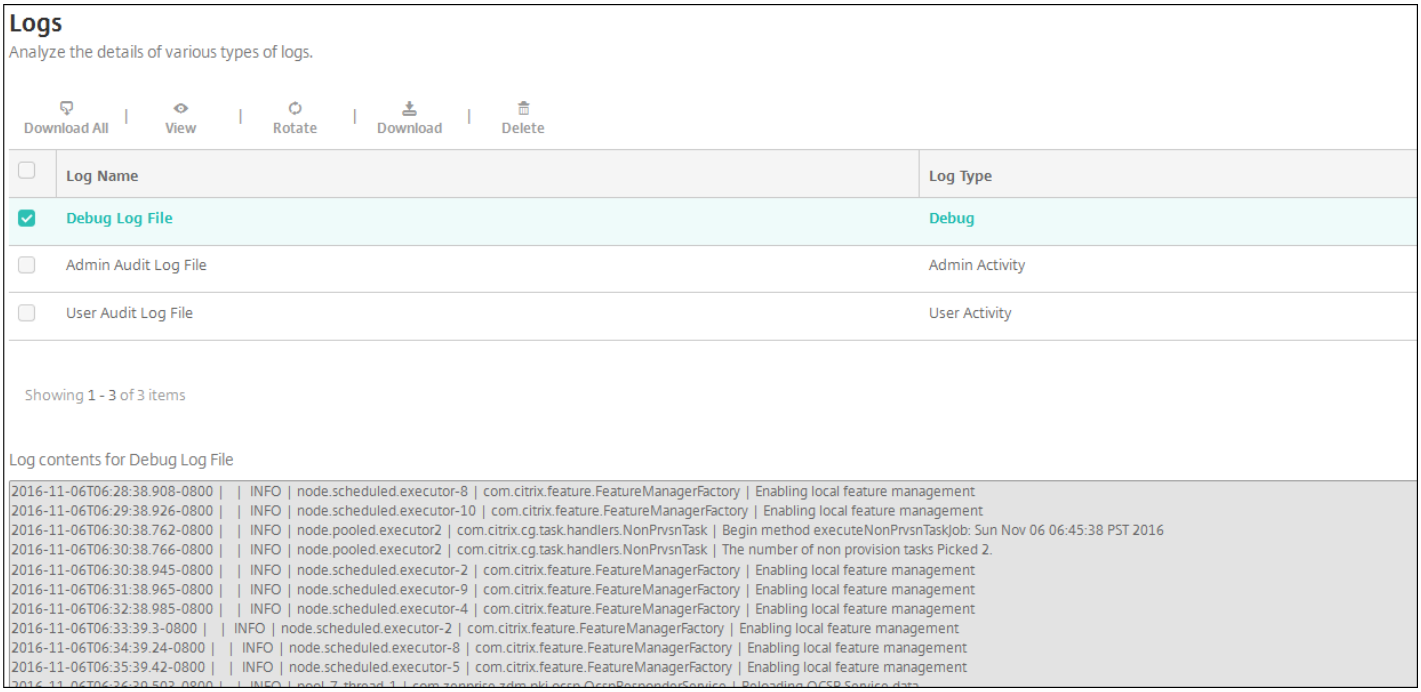


Nota:

- 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).
- **Visualizar**: 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.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Ferramenta XenMobile Analyzer

Feb 21, 2018

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.

Neste artigo:

- Acessar e iniciar o XenMobile Analyzer
- Execução de uma verificação de ambiente
- Executar uma verificação do NetScaler
- Adicionar um agendamento para verificações de ambiente
- Realizar outras verificações informativas
- Problemas conhecidos
- Problemas resolvidos

Principais recursos

- 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 NetScaler.
- 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 ShareFile**.**

Novidades

- O Relatório de configuração do NetScaler exibe uma notificação de selo indicando o número de recomendações. As recomendações baseiam-se nas verificações de Configuração essencial em um NetScaler 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: Lista de ambiente da nova interface do usuário

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nota: Esse vídeo não contém som de áudio. Ele é melhor visualizado no modo de tela inteira.

Acessar e iniciar o XenMobile Analyzer

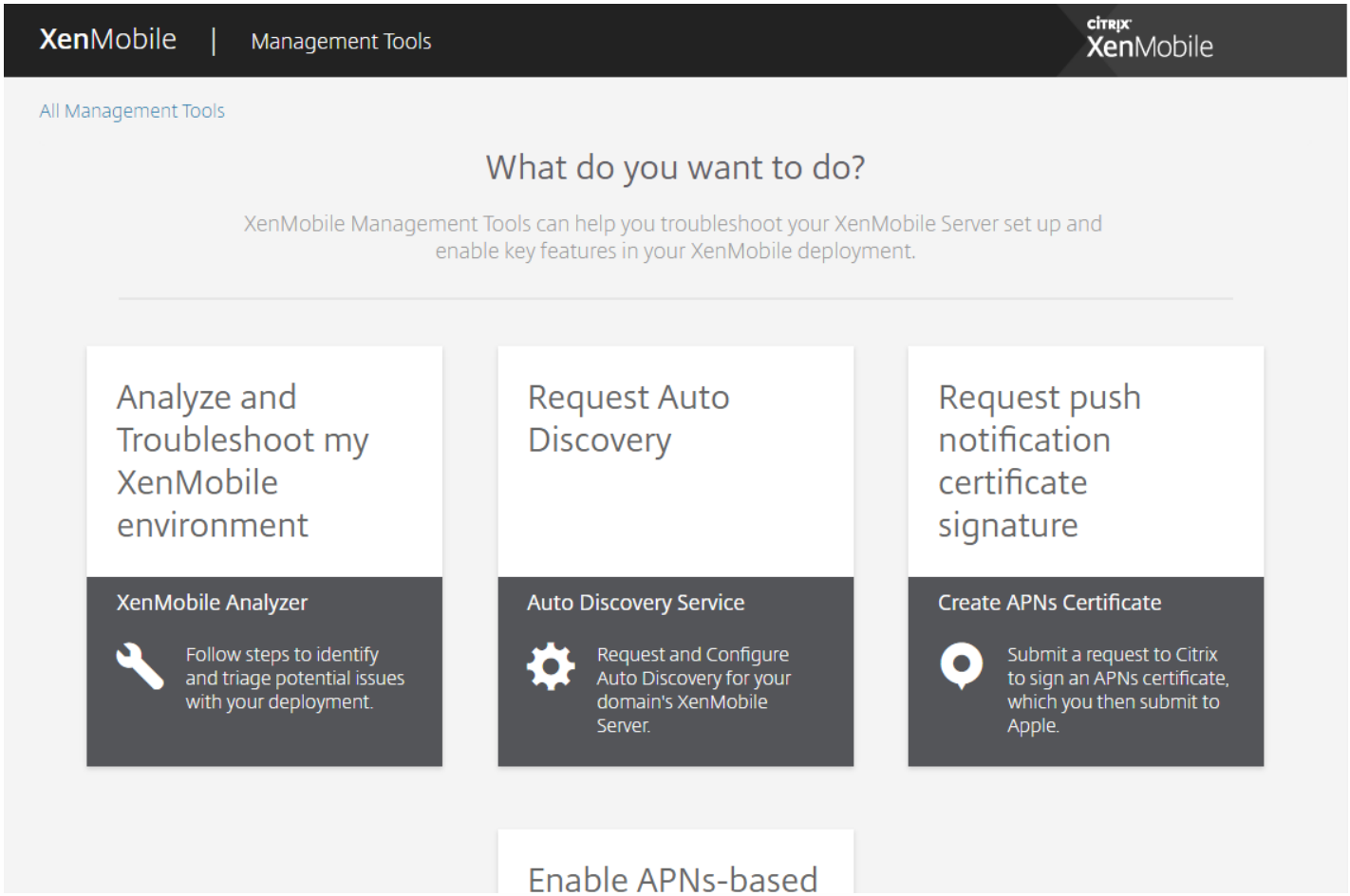
Pré-requisitos

Produto	Versão com suporte
XenMobile Server	10.3.0 e versões posteriores
NetScaler 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 do My Citrix para acessar a ferramenta em https://xenmobiletools.citrix.com. Na página XenMobile Management Tools exibida, para iniciar o XenMobile Analyzer, clique em **Analyze and Troubleshoot my XenMobile Environment**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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:

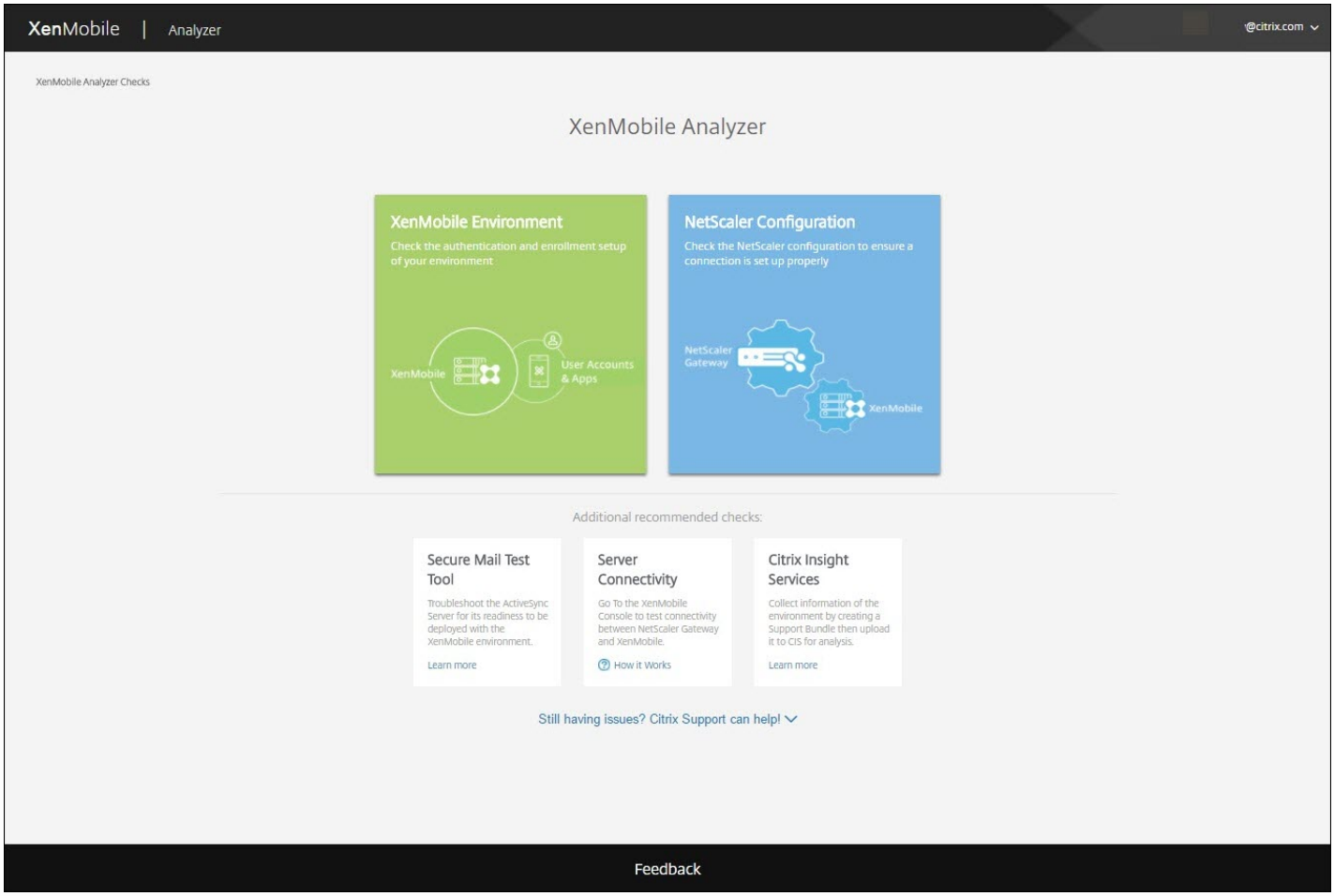
- **Environment Check** - Essa etapa o orienta na configuração de testes para verificar a configuração em caso de problemas. A etapa também fornece recomendações e soluções para problemas no dispositivo, registro de usuário e autenticação.
- **NetScaler Check** - Esta etapa o orienta na verificação das suas configurações do NetScaler para preparação de implantação do XenMobile.
- **Advanced Diagnostics** - Essa etapa fornece informações sobre como usar o Citrix Insight Services para encontrar mais problemas que a verificação de ambiente possa ter deixado de detectar.
- **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 para que a sua prontidão seja implantada com um ambiente XenMobile.
- **Server Connectivity Checks** - Essa etapa instrui você a testar a conectividade dos seus servidores.
- **Contact Citrix Support** - Essa 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

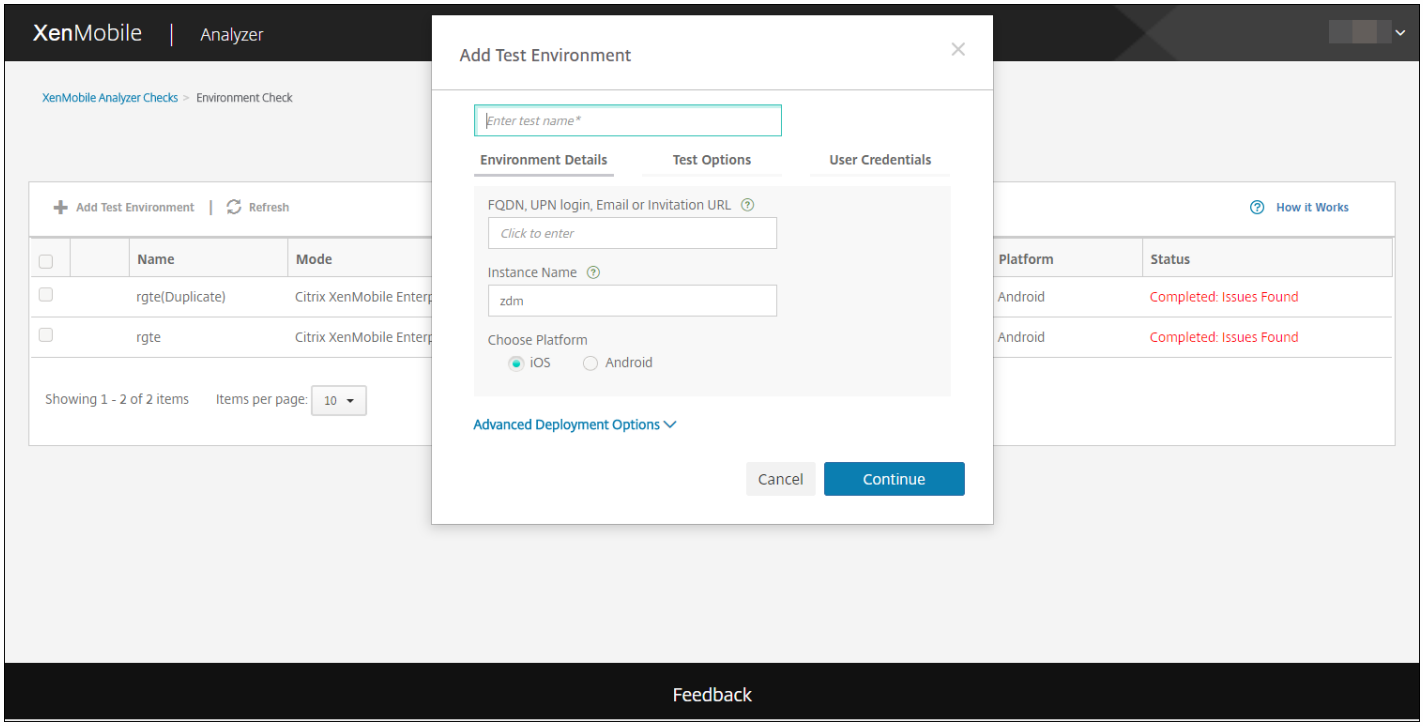
1. Faça login no XenMobile Analyzer e clique em **XenMobile Environment**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

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. As opções disponíveis são **Enterprise (MDM + MAM)**, **App Management (MAM)** ou **Device Management (MDM)**.

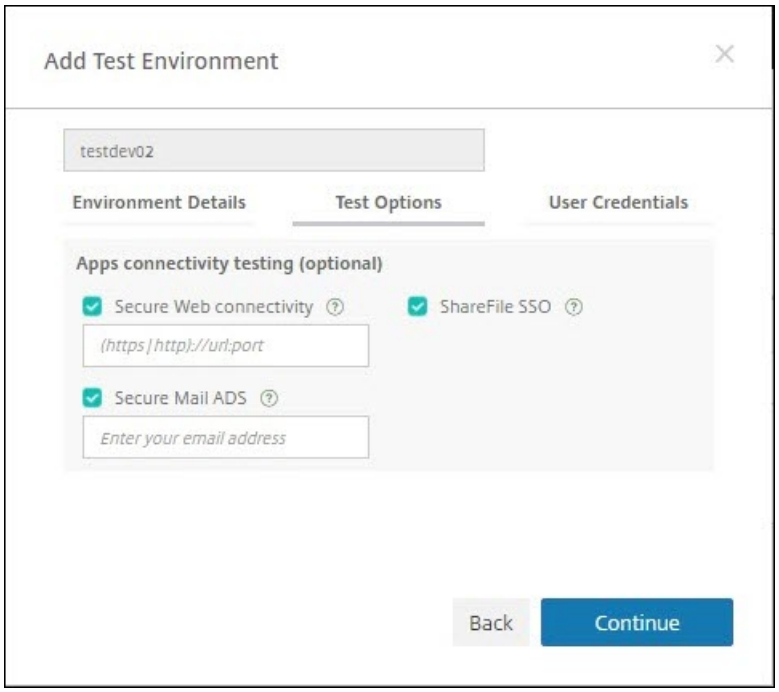
d. Clique em **Continue**.

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.

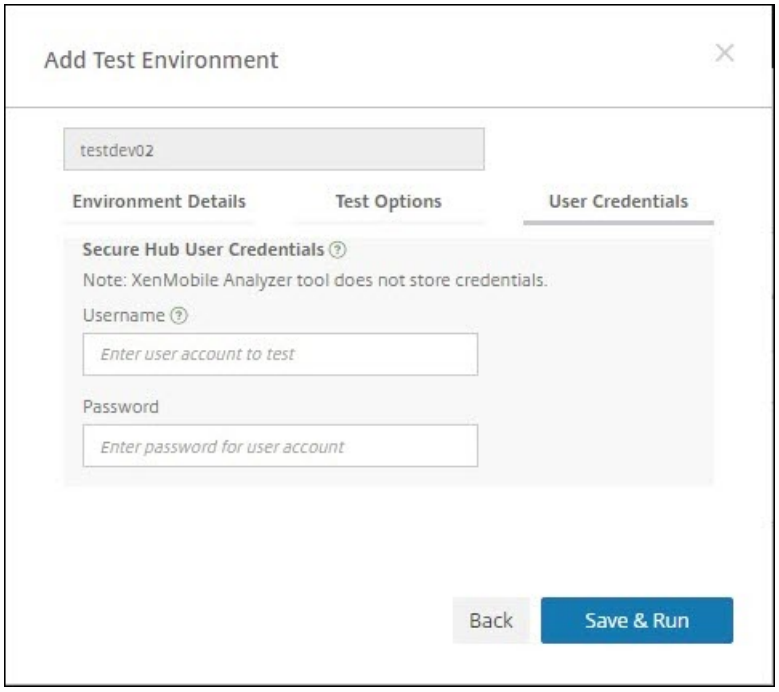
b. ADS do Secure Mail. Forneça um ID de email de usuário. Essa ID é usada para testar a detecção automática do Microsoft Exchange Server em seu ambiente XenMobile. Ele detecta se há problemas relacionados à detecção automática de Secure Mail.

c. ShareFile SSO. Se selecionado, o XenMobile Analyzer testará se a resolução DNS do ShareFile tem êxito. A ferramenta também verifica se o logon único (SSO) do ShareFile é compatível com as credenciais de usuário fornecidas.



5. Na guia **User Credentials**, dependendo da configuração do servidor, você verá campos diferentes. Os campos possíveis são **Username**, **Username and Password** ou **Username, Password** e **Enrollment PIN**.

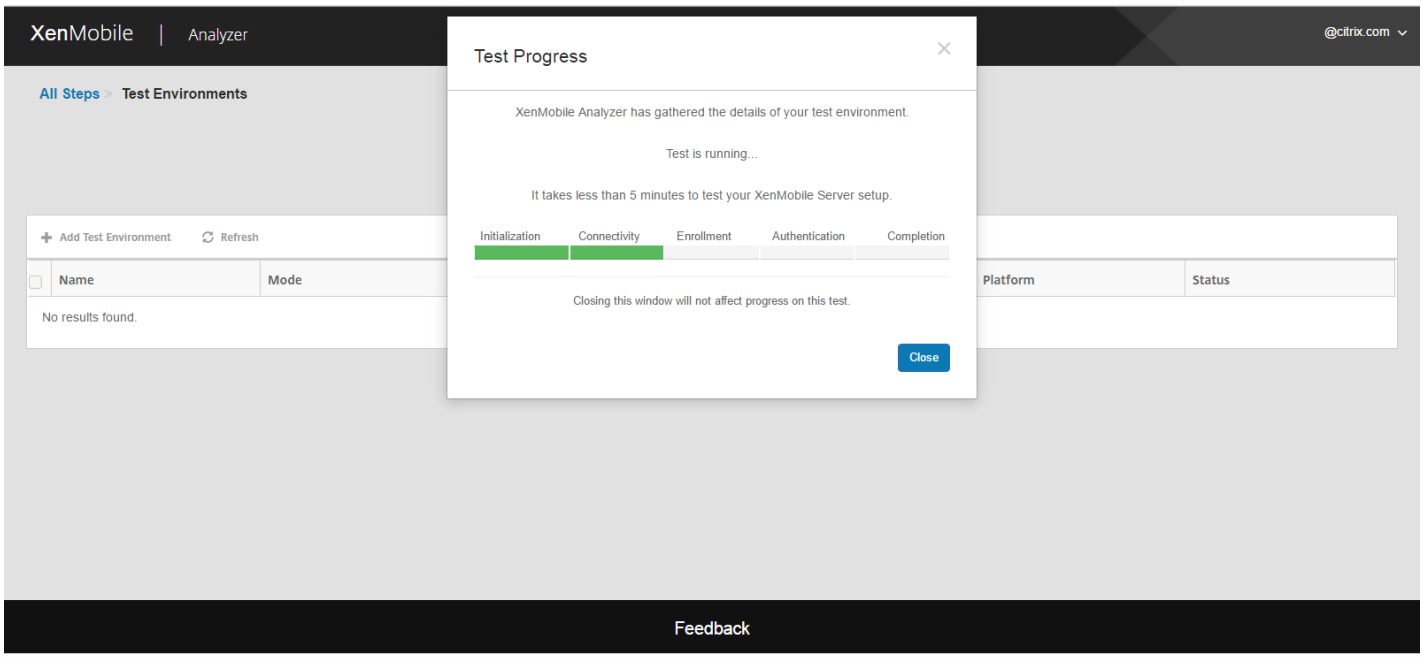
© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. Clique em **Save & Run** para iniciar os testes.

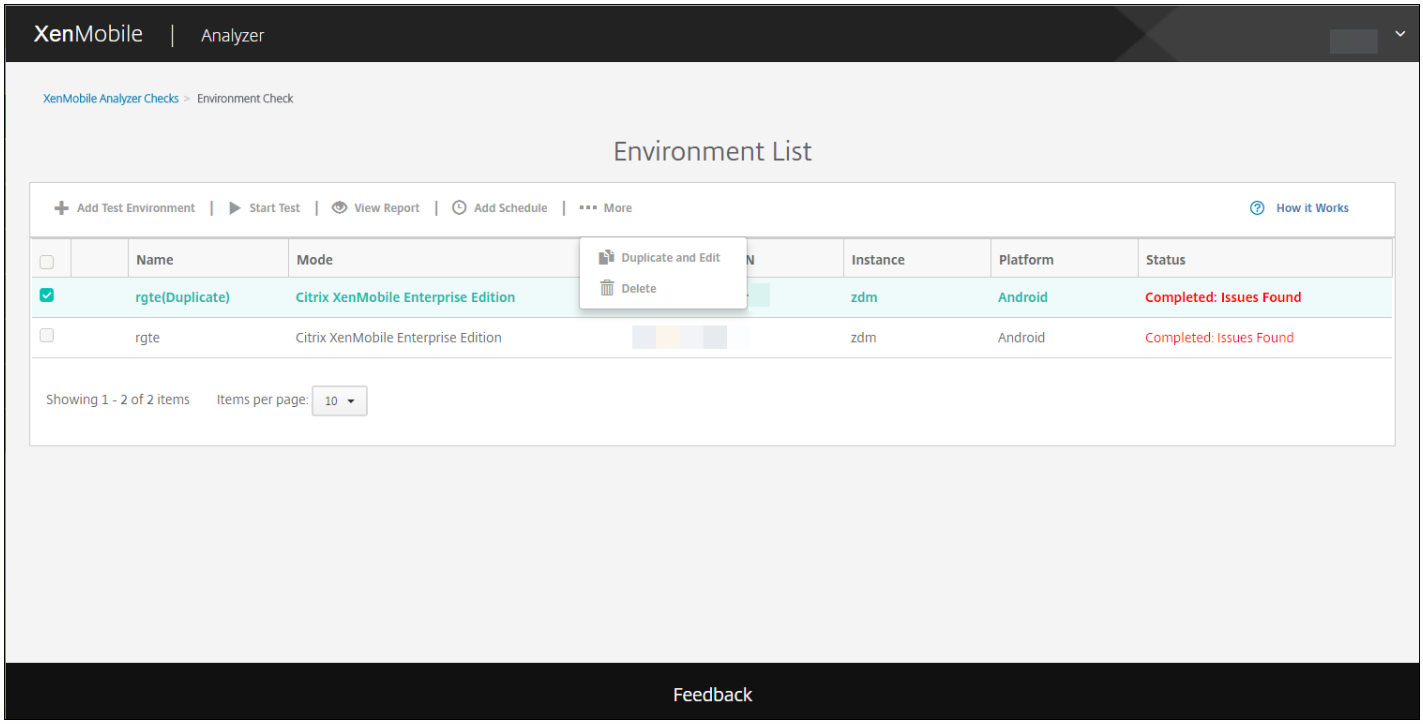
Uma notificação de progresso é exibida. Você pode deixar a caixa de diálogo de progresso aberta ou fechar a caixa de diálogo a execução dos testes continua.

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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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**.

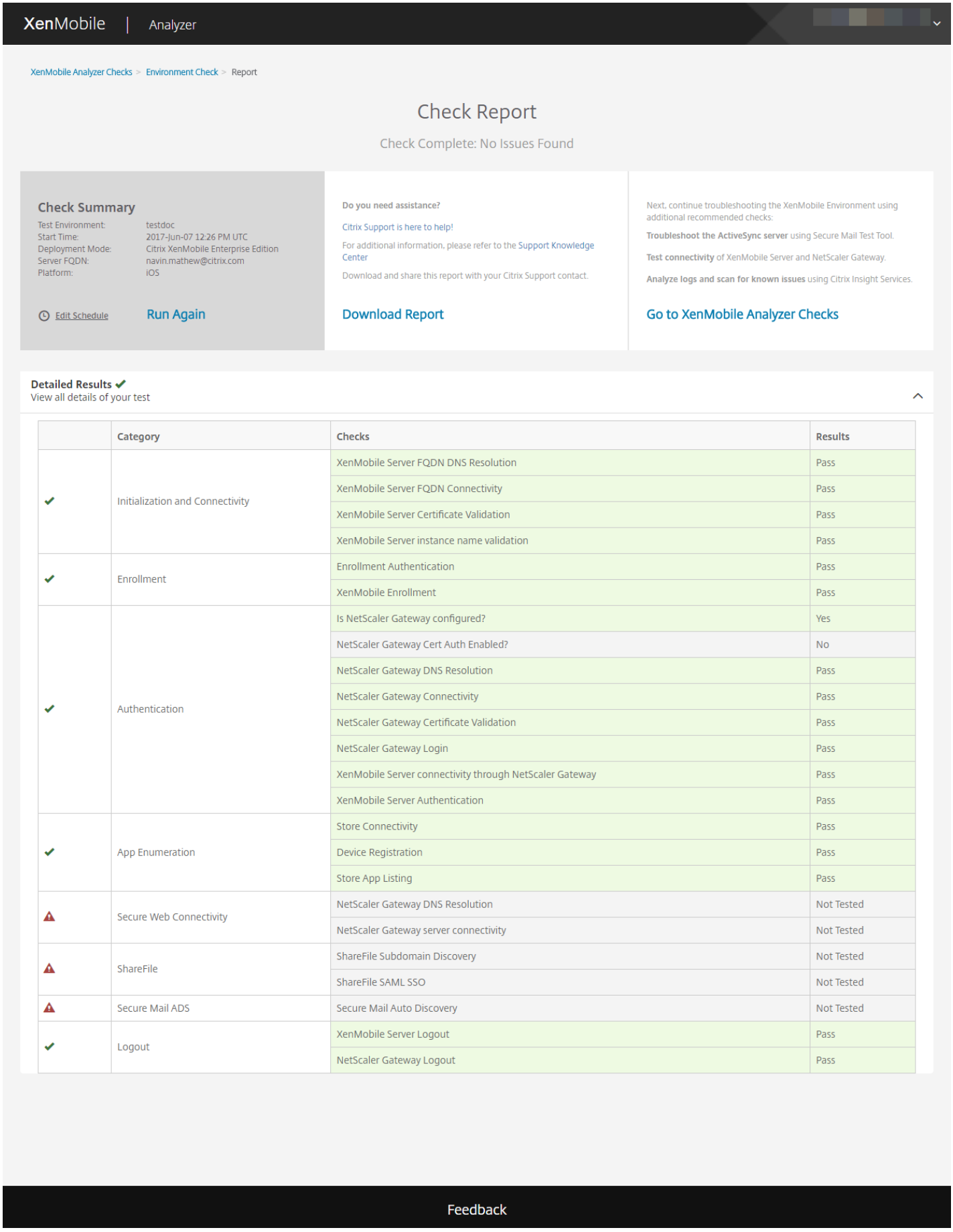
    b. Para retornar à lista de ambientes de teste, clique em **Environment Check**.

    c. Para executar novamente o mesmo teste, clique em **Run Again**.

    d. Se quiser 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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

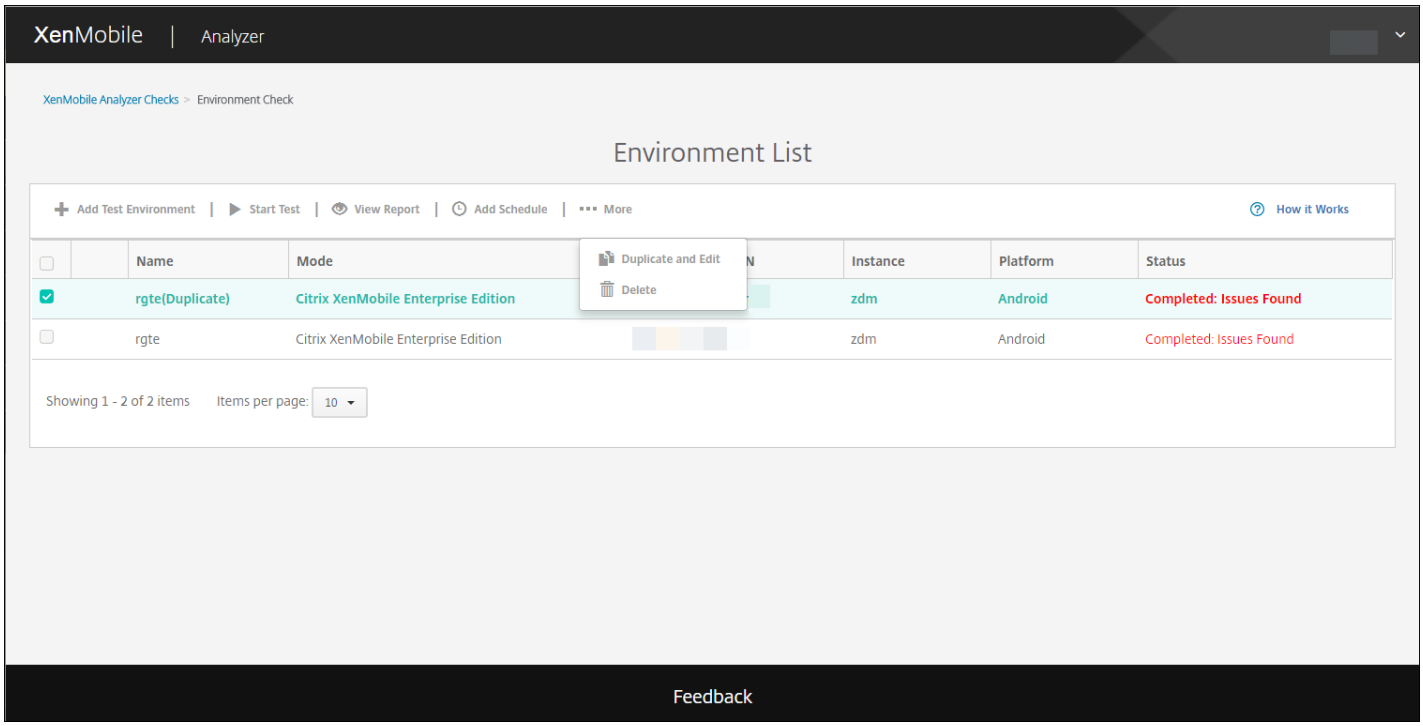


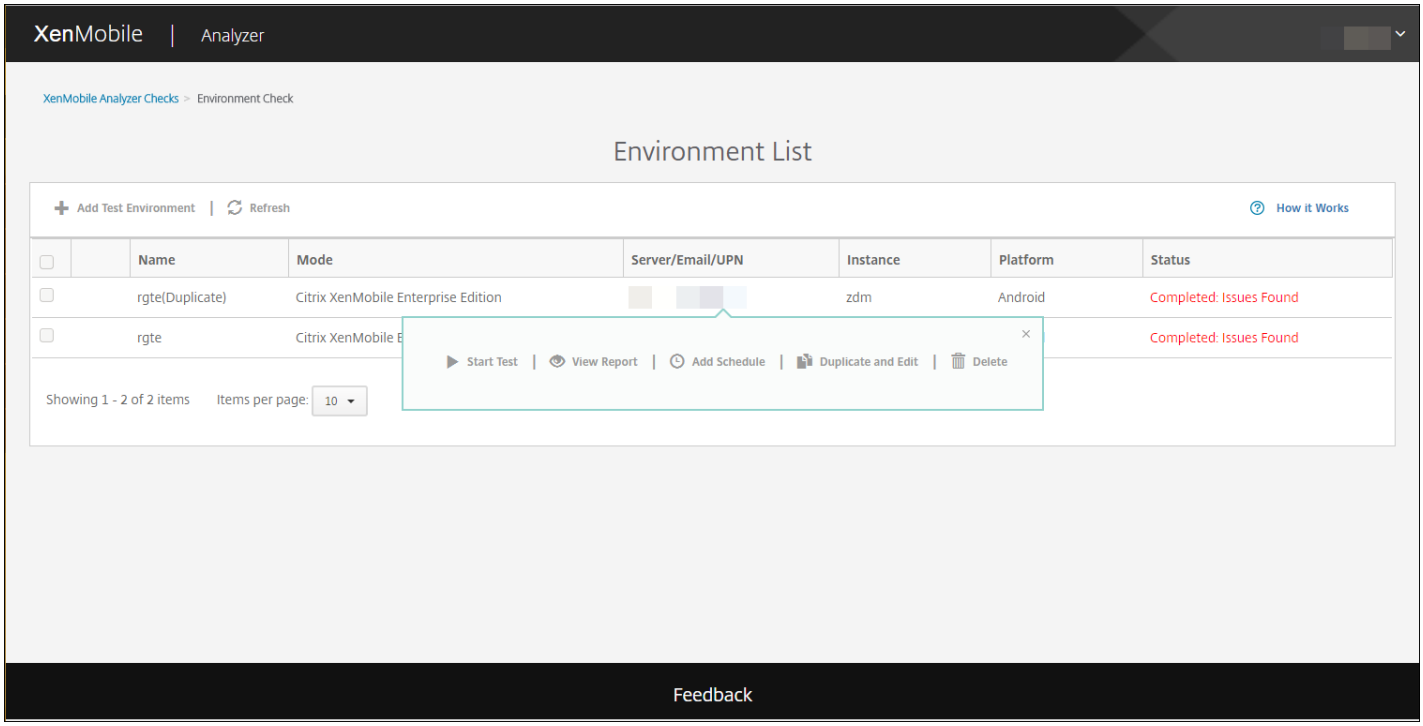
	Category	Checks	Results
✔	Initialization and Connectivity	XenMobile Server FQDN DNS Resolution	Pass
		XenMobile Server FQDN Connectivity	Pass
		XenMobile Server Certificate Validation	Pass
		XenMobile Server instance name validation	Pass
✔	Enrollment	Enrollment Authentication	Pass
		XenMobile Enrollment	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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

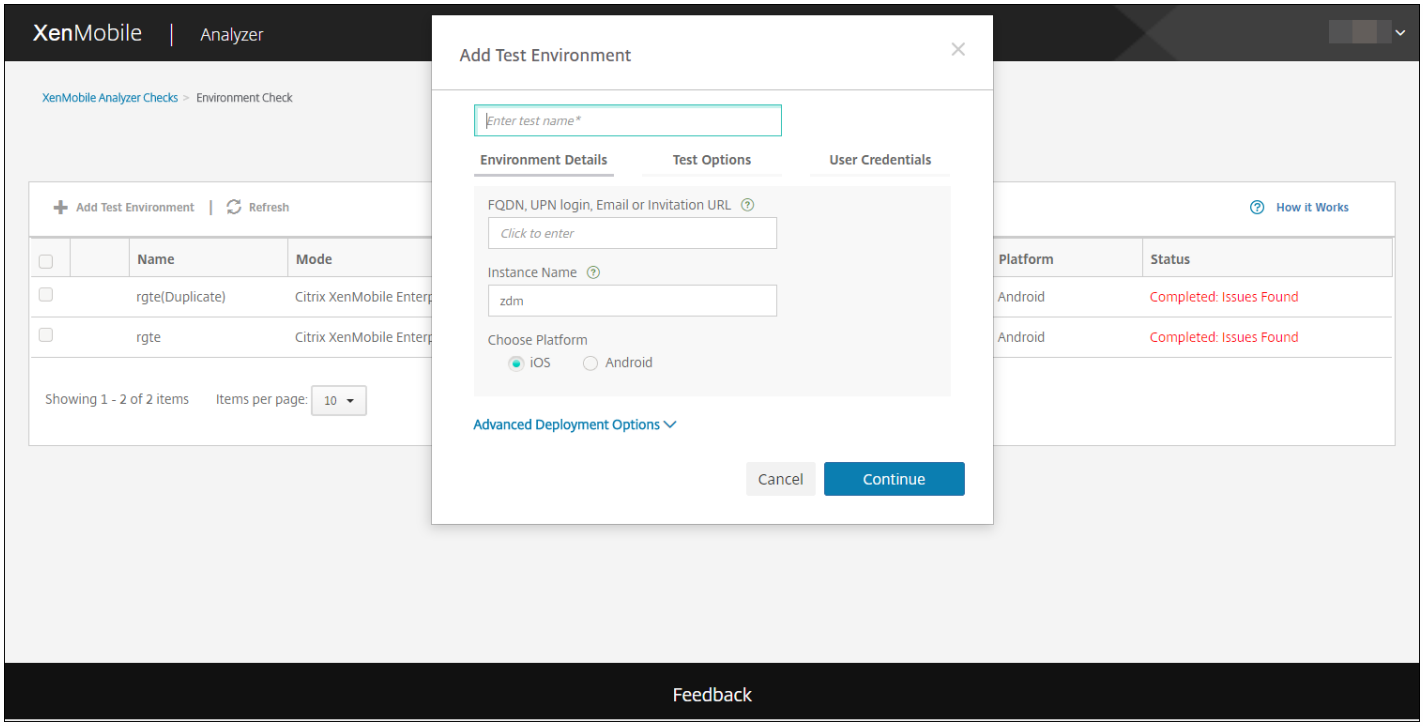
9. Na página ambientes de teste, você pode copiar e editar testes. Para fazer isso, selecione um teste e, em seguida, clique em **More** e selecione **Duplicate and Edit**.

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.





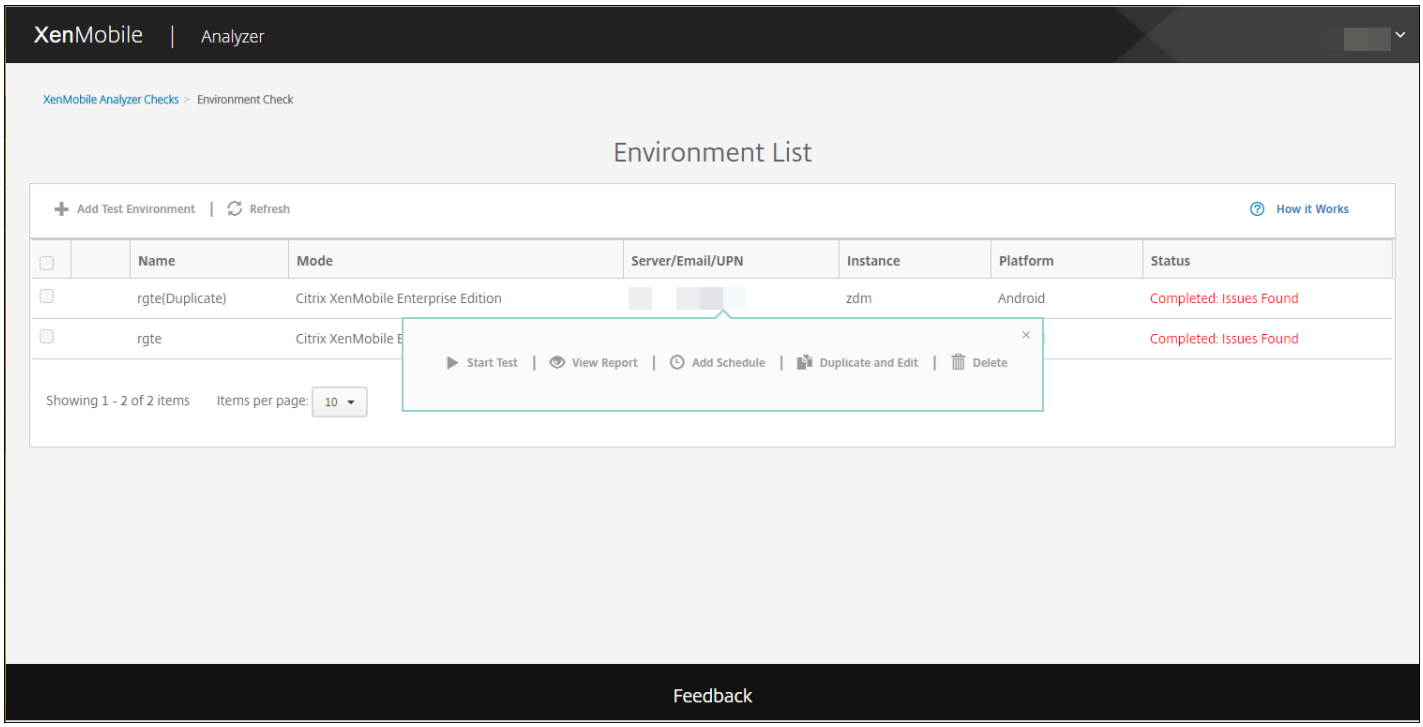
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Adicionar um agendamento para verificações de ambiente

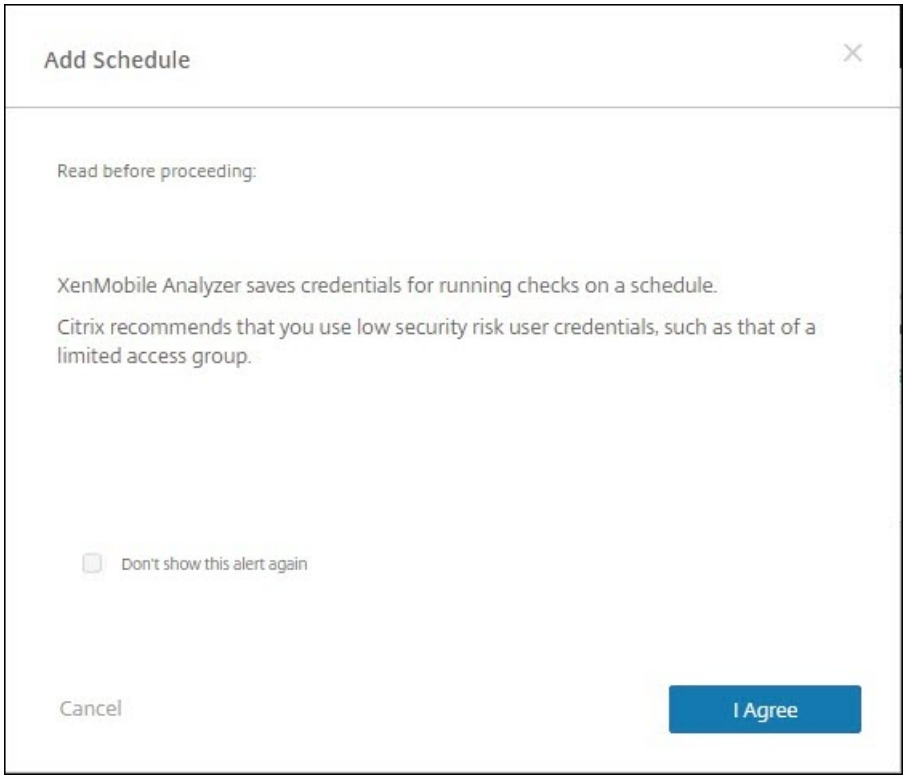
Você pode configurar testes para executar em um agendamento automático com resultados enviados para uma lista de usuários que você configura.

1. Na página **Environment List**, selecione o ambiente para a qual você deseja agendar e clique em **Add Schedule**.

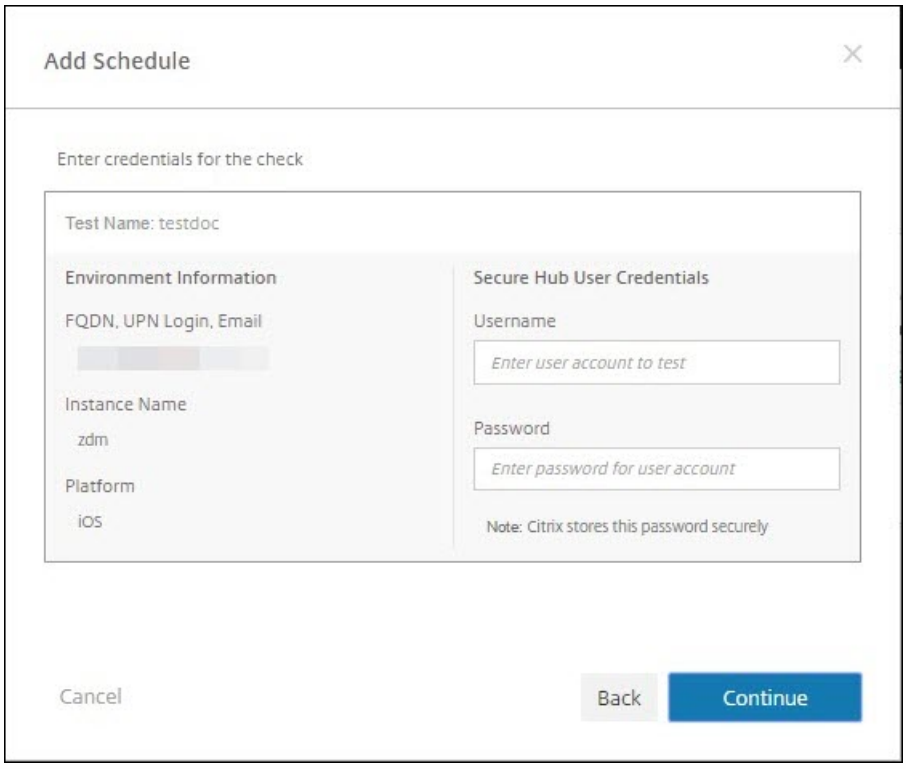


2. A janela **Add Schedule** exibe uma mensagem para avisar você que o XenMobile Analyzer salva as credenciais para executar testes em um agendamento. A Citrix recomenda que você use uma conta com acesso limitado para executar testes programados. Clique em **I Agree**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

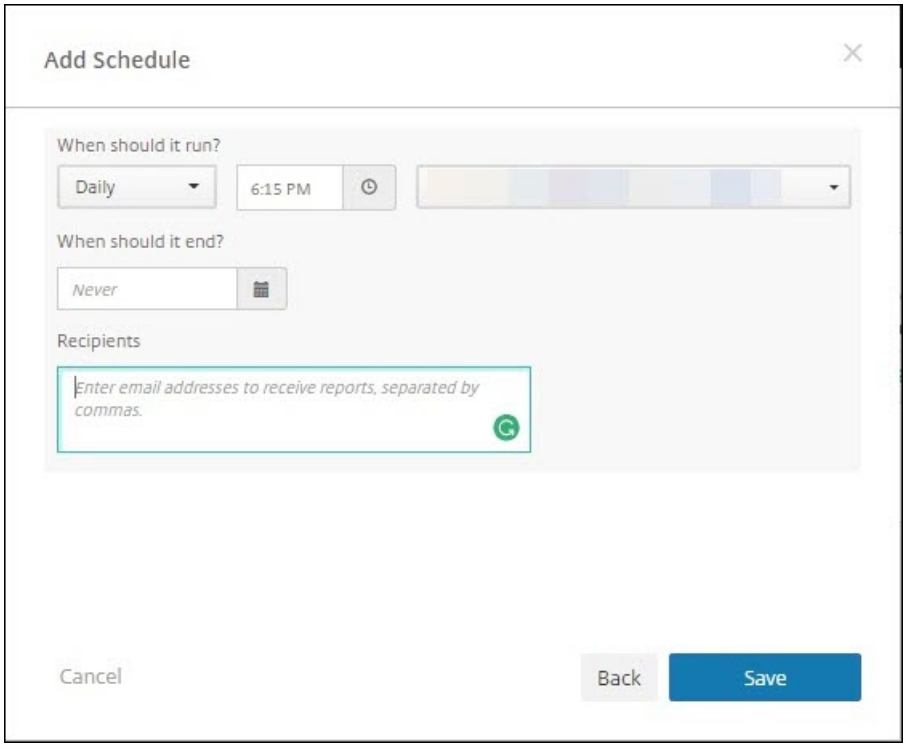


3. Digite um **Nome de usuário** e **Senha** para executar o teste.

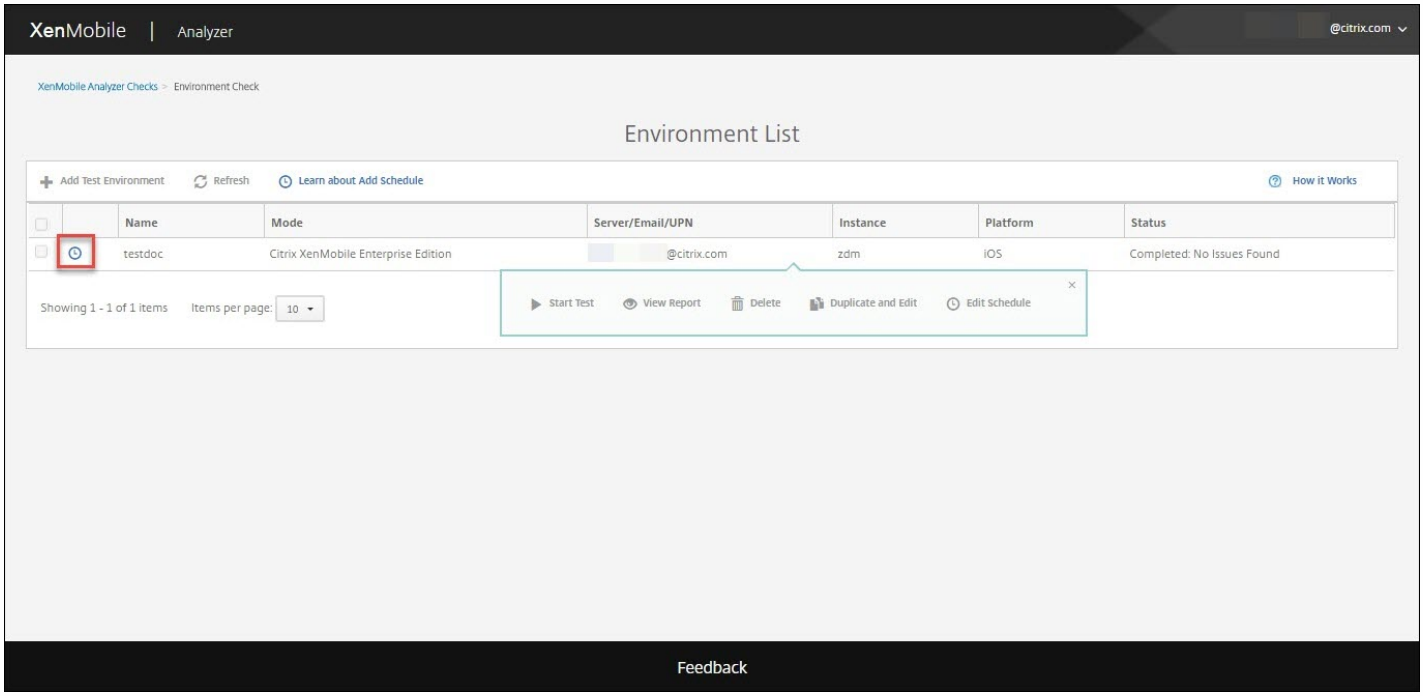


4. Configure um agendamento para execução do teste. Você pode selecionar **Daily** ou **Weekly** na lista suspensa. Selecione uma hora do dia para executar o teste e um fuso horário. Use o botão para selecionar uma data para que o teste agendado pare de ser executado ou deixe em branco para que o teste seja executado indefinidamente. Forneça uma lista de endereços de email para receber relatórios, separados por vírgulas. Clique em **Salvar**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

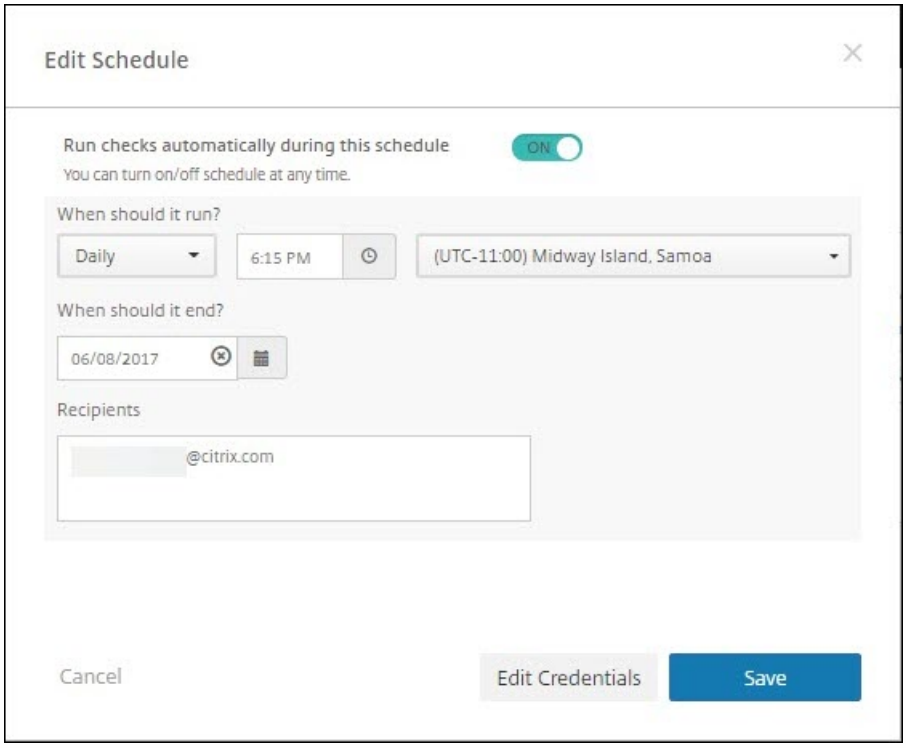


5. Um símbolo de relógio à esquerda do seu teste indica que está configurado um agendamento. Se você selecionar o seu teste, você pode clicar em **Edit Schedule** para alterar quando o teste for executado.



6. 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

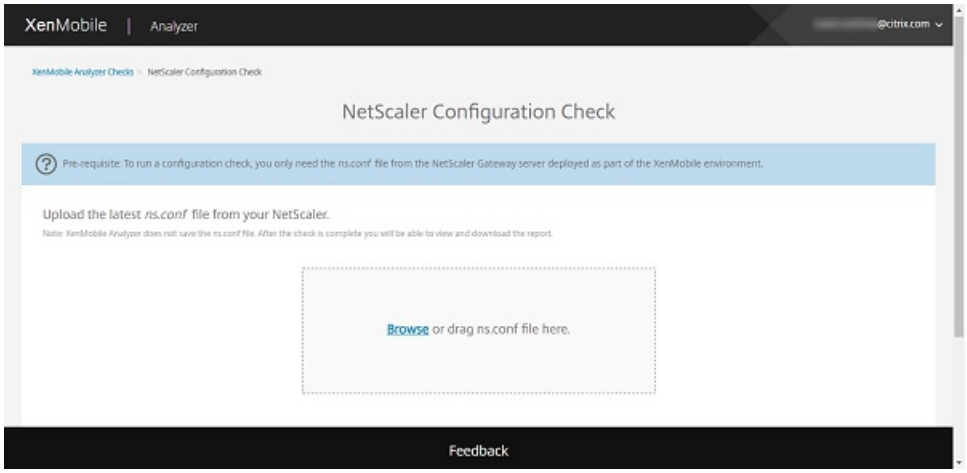


Executar uma verificação do NetScaler

1. Faça login no XenMobile Analyzer e, em seguida, clique em **Configuração do NetScaler**.

2. Carregue o arquivo ns.conf mais recente da sua instância do NetScaler. Você pode arrastar o arquivo para a caixa de upload ou clicar em **Procurar** para procurar e adicionar o arquivo ns.conf. Para obter mais informações sobre como você pode baixar o arquivo ns.conf mais recente, consulte o Support Knowledge Center.

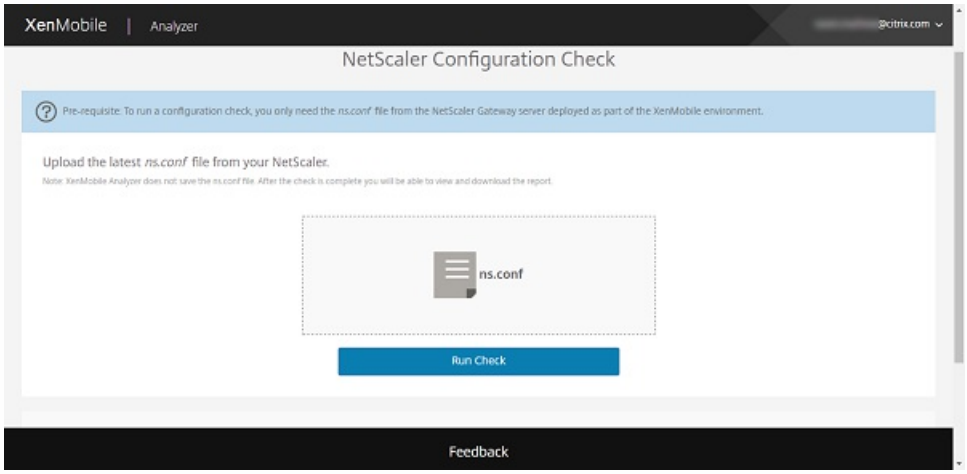
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Nota

O XenMobile Analyzer não salva o arquivo ns.conf. Depois que a verificação estiver concluída, você pode exibir e baixar o relatório.

3. Clique em **Run Check**.

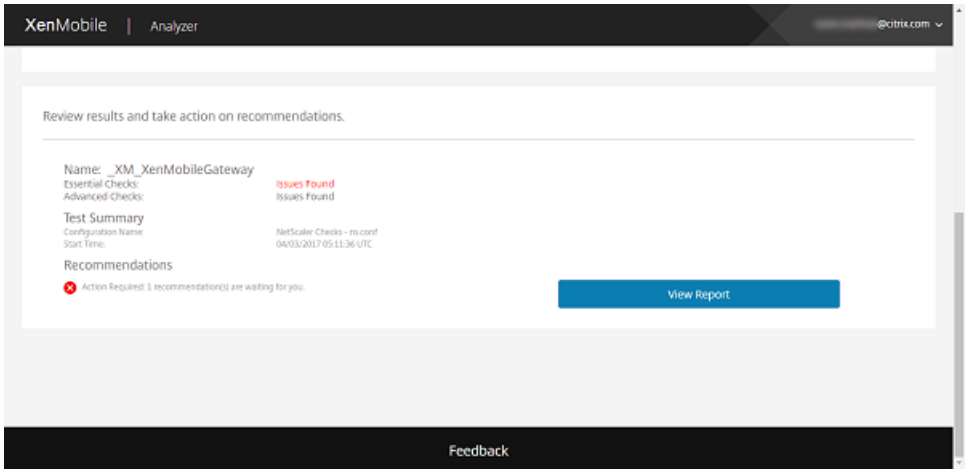


O XenMobile Analyzer executa dois tipos de verificação de configuração.

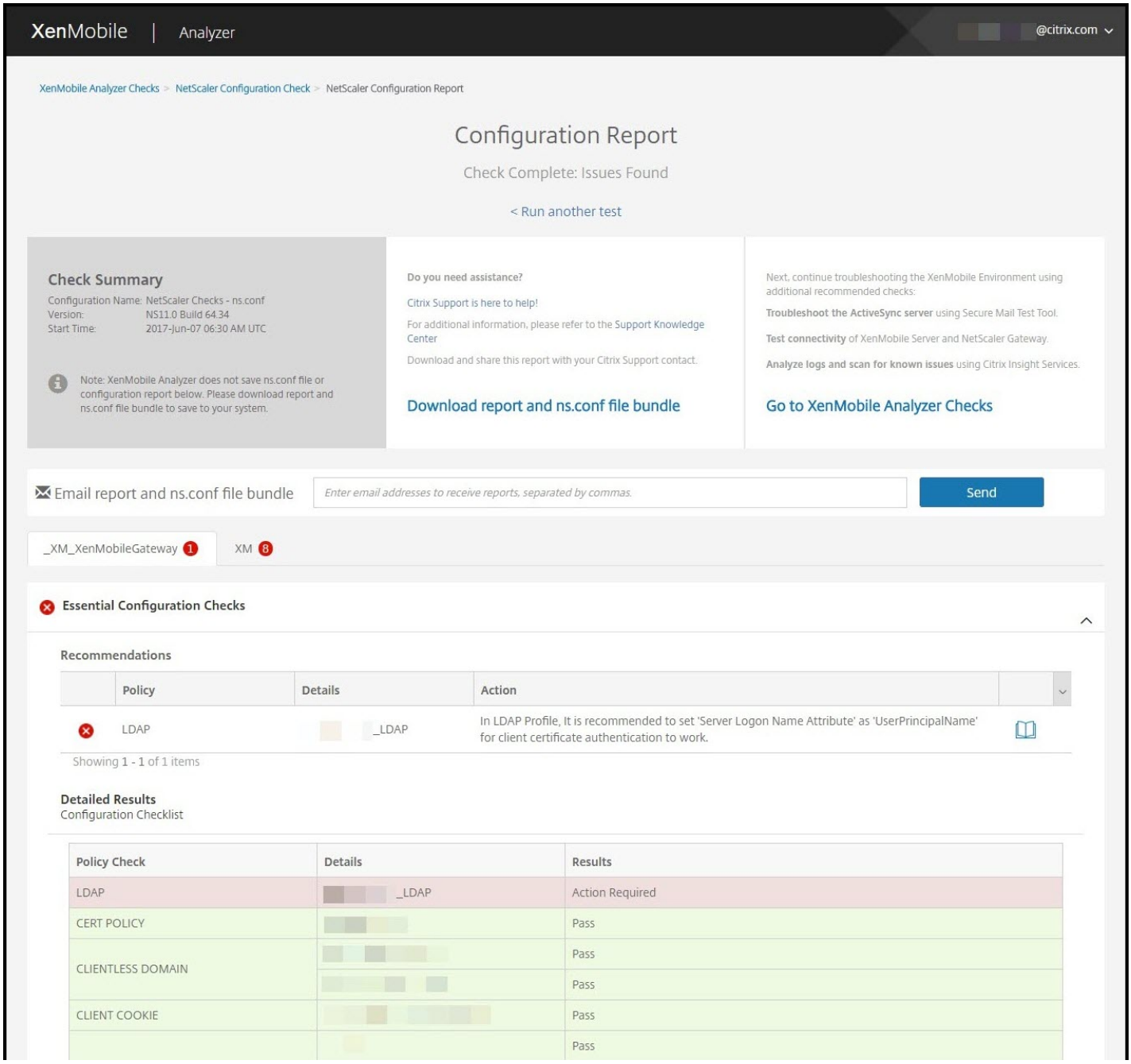
- A opção Essential Checks procura por componentes que são essenciais para uma implantação com êxito do XenMobile.
- A opção Advanced Checks procura por componentes que não são essenciais, mas complementares para implantações do XenMobile.

4. Para exibir as recomendações em Essential Checks e Advanced Checks para NetScaler, clique em **View Report**.

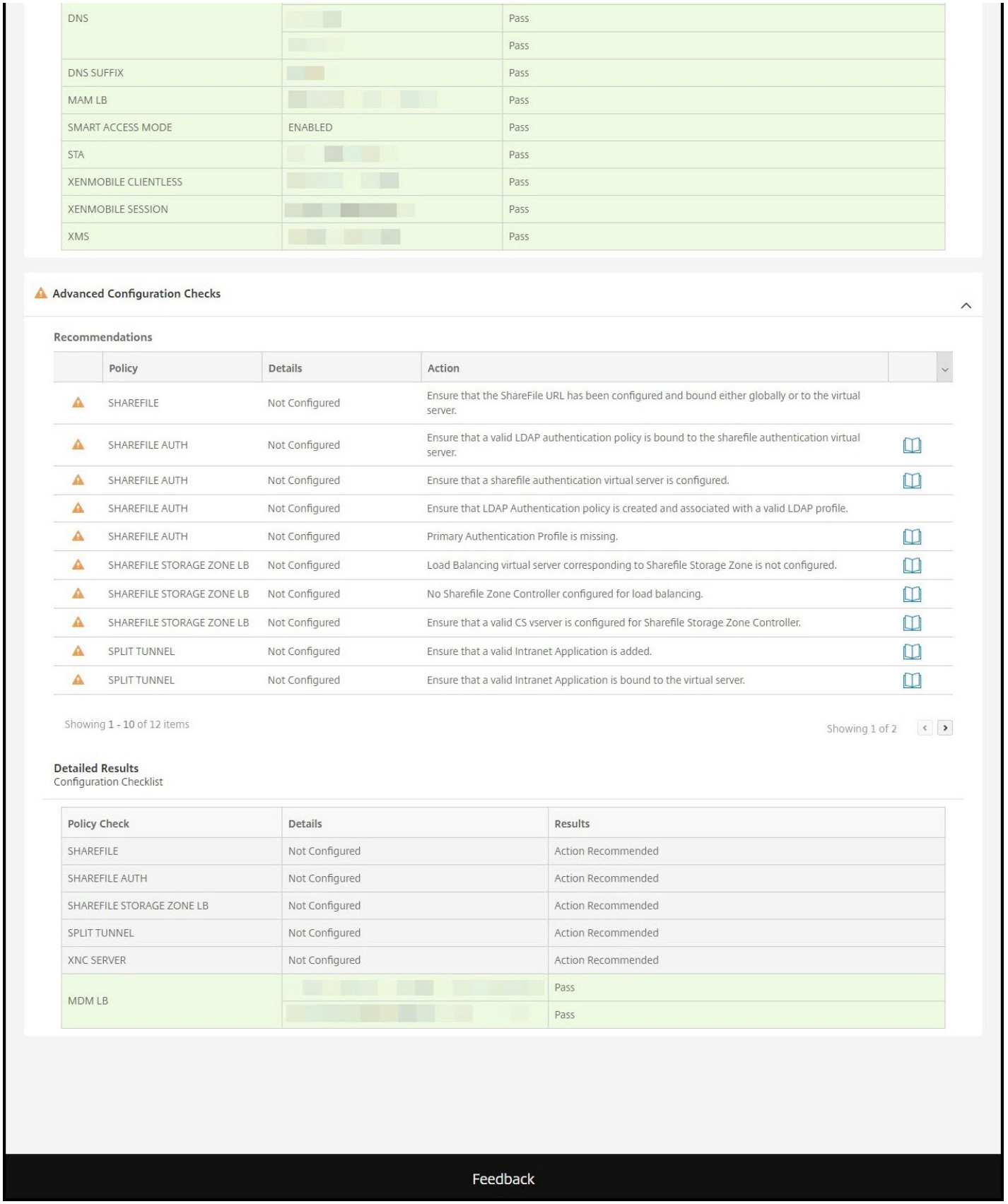
© 1999-2017 Citrix Systems, Inc. All rights reserved.



A página **Configuration Report** é exibida.



© 1999-2017 Citrix Systems, Inc. All rights reserved.



DNS		Pass
		Pass
DNS SUFFIX		Pass
MAM LB		Pass
SMART ACCESS MODE	ENABLED	Pass
STA		Pass
XENMOBILE CLIENTLESS		Pass
XENMOBILE SESSION		Pass
XMS		Pass

Advanced Configuration Checks

Recommendations

	Policy	Details	Action	
⚠	SHAREFILE	Not Configured	Ensure that the ShareFile URL has been configured and bound either globally or to the virtual server.	
⚠	SHAREFILE AUTH	Not Configured	Ensure that a valid LDAP authentication policy is bound to the sharefile authentication virtual server.	📖
⚠	SHAREFILE AUTH	Not Configured	Ensure that a sharefile authentication virtual server is configured.	📖
⚠	SHAREFILE AUTH	Not Configured	Ensure that LDAP Authentication policy is created and associated with a valid LDAP profile.	
⚠	SHAREFILE AUTH	Not Configured	Primary Authentication Profile is missing.	📖
⚠	SHAREFILE STORAGE ZONE LB	Not Configured	Load Balancing virtual server corresponding to Sharefile Storage Zone is not configured.	📖
⚠	SHAREFILE STORAGE ZONE LB	Not Configured	No Sharefile Zone Controller configured for load balancing.	📖
⚠	SHAREFILE STORAGE ZONE LB	Not Configured	Ensure that a valid CS vserver is configured for Sharefile Storage Zone Controller.	📖
⚠	SPLIT TUNNEL	Not Configured	Ensure that a valid Intranet Application is added.	📖
⚠	SPLIT TUNNEL	Not Configured	Ensure that a valid Intranet Application is bound to the virtual server.	📖

Showing 1 - 10 of 12 items

Showing 1 of 2 ‹ ›

Detailed Results
Configuration Checklist

Policy Check	Details	Results
SHAREFILE	Not Configured	Action Recommended
SHAREFILE AUTH	Not Configured	Action Recommended
SHAREFILE STORAGE ZONE LB	Not Configured	Action Recommended
SPLIT TUNNEL	Not Configured	Action Recommended
XNC SERVER	Not Configured	Action Recommended
MDM LB		Pass
		Pass

Feedback

Nota

O XenMobile Analyzer é compatível com servidores de gateway configurados por meio do Assistente do NetScaler. As instâncias do NetScaler Gateway sempre seguem a seguinte convenção de título: '_XM_*nome-usado-pelo-usuário-na-implementação'.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

O status geral é Success quando as verificações de configuração essenciais tiveram dado resultado positivo.

Quando uma verificação de configuração essenciais falha, as tabela de recomendações lista a **Política**, **Detalhes** e **Resultados (ação obrigatória)**.

Quando uma verificação de configuração avançada falha, as tabela de recomendações lista a **Política**, **Detalhes** e **Resultados (ação recomendada)**.

O selo de notificação no relatório de configuração indica o número de recomendações na verificação de Configuração essencial para servidores de gateway configurados por meio do assistente do NetScaler e de Gateways configurados pelo usuário.

Na página **Configuration Report**, estão disponíveis as opções a seguir.

a. Para exibir os detalhes, clique em **Essential Configuration Checks/Advanced Configuration Checks** (ou no ícone de expandir).

b. para executar outra verificação de configuração do NetScaler, clique em **Run another test**.

c. Para exibir outras solução de problemas e ferramentas de análise, clique em **Go to XenMobile Analyzer Checks**.

d. para baixar um relatório dos resultados, clique em **Download report and ns.conf file bundle** ou em **Email report and ns.conf bundle**, digite seu endereço de email. Em seguida, clique em **Send**.

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 nos 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 ShareFile.
- **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 do 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

APIs REST

Feb 21, 2018

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 XenMobile 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 sobre como definir o acesso com base em função, consulte Configurando funções com o 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

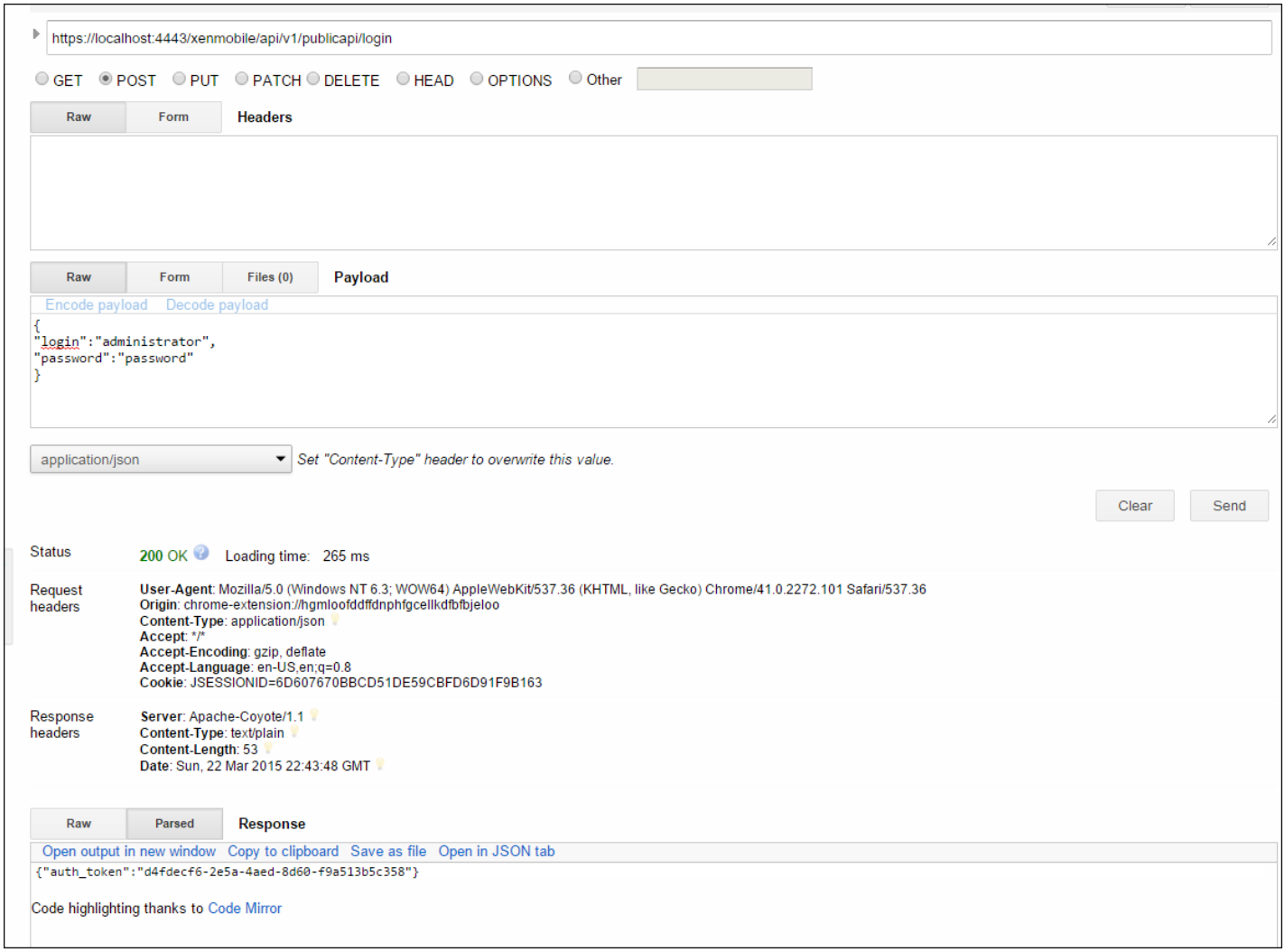
URL: https://:/xenmobile/api/v1/authentication/login

Solicitação: { "login":"administrator", "password":"password" }

Tipo de método: POST

Tipo de conteúdo: application/json

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Informações relacionadas

- XenMobile REST API

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile Mail Manager 10.x

Feb 23, 2018

O XenMobile Mail Manager oferece a funcionalidade que estende 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 realize um EAS Wipe em um dispositivo móvel.
- A capacidade para que o XenMobile acesse informações sobre dispositivos BlackBerry e execute operações de controle, como Wipe e ResetPassword.

Para baixar o XenMobile Mail Manager, acesse a seção Server Components em Servidor XenMobile 10 em Citrix.com.

Este artigo inclui as seções a seguir:

- O que há de novo na versão 10.1
- Problemas resolvidos
- Arquitetura
- Requisitos do sistema e pré-requisito
- Pré-requisitos do XenMobile Mail Manager
- Requisitos do Office 365 Exchange
- Instalar e configurar
- Impor políticas de email com IDs do ActiveSync
- Regras de controle de acesso
- Monitoramento de dispositivo
- Resolução de problemas e diagnósticos
- Ferramentas de solução de problemas

O que há de novo na versão 10.1

Regras de acesso

A janela Análise de regras tem uma caixa de seleção que, quando selecionada, exibe somente as regras que são conflitos, substituições, redundâncias ou suplementos.

Acesso padrão (Permitir, Bloquear ou Unchanged) e modos de comando ActiveSync (PowerShell ou Simulação) são definidos separadamente para cada ambiente do Microsoft Exchange configurado na sua implantação do XenMobile.

Instantâneos

Você pode configurar o número máximo de instantâneos mostrado no histórico de instantâneos.

Você pode configurar os erros para ignorar durante um instantâneo principal. Quando um instantâneo principal retorna os erros que não estão configurados como ignoráveis, os resultados dos instantâneos são descartados.

Para configurar os erros como ignoráveis, edite o arquivo config.xml usando um editor de XML:

- Se o Exchange Server for o Office 365, navegue para o nó /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeOnline']/IgnorableErrors e adicione o texto que deve corresponder como um elemento-filho no mesmo formato que o elemento-filho Error já existente. É possível usar expressões regulares.
- Se o Exchange Server for local, navegue para o nó /ConfigRoot/EnvironmentBridge/AccessLayer/SpecialistsDefaults/PowerShells/PowerShell[@id='ExchangeColocated']/IgnorableErrors e adicione o texto que deve corresponder como um elemento-filho no mesmo formato que o elemento-filho Error já existente. É

© 1999-2017 Citrix Systems, Inc. All rights reserved.

possível usar expressões regulares.

- Se houver mais de um ambiente do Exchange configurado, navegue até o nó /ConfigRoot/EnvironmentBridge/AccessLayer/Environments/Environment[@id='ID Corresponding to the desired Exchange environment']/ExchangeServer/Specialists/PowerShell. Adicione um nó filho IgnorableErrors para o nó do PowerShell para cada erro a ser ignorado. Adicione um nó filho Error ao nó IgnorableErrors com o texto correspondente contido em uma seção CDATA. É possível usar expressões regulares.

Salve o config.xml e reinicie o serviço do XenMobile Mail Manager.

PowerShell e Exchange

O XenMobile Mail Manager agora determina dinamicamente os cmdlets que devem ser usados com base na versão do Exchange ao qual está conectado. Por exemplo, para o Exchange 2010, ele usa Get-ActiveSyncDevice, mas para o Exchange 2013 e o Exchange 2016, ele usa Get-MobileDevice.

Configuração do Exchange

As configurações do Exchange Server podem ser editadas e atualizadas sem reiniciar o serviço do XenMobile Mail Manager.

Duas novas colunas adicionadas ao resumo do ambiente do Exchange exibem cada modo de comando (PowerShell ou Simulação) e o modo de acesso (Permitir, Bloquear ou Inalterado).

Resolução de problemas e diagnósticos

Um conjunto de utilitários do PowerShell para solução de problemas está disponível na pasta Support\PowerShell.

Testar a conectividade com o serviço do Exchange usando o botão de teste de conectividade na janela de configuração do console executa todos os cmdlet de somente leitura usados pelo serviço, executa os testes de permissões RBAC com relação ao Exchange Server para o usuário configurado, e exibe os erros ou avisos identificados por cores (azul-amarela para avisos, vermelho-laranja para erros).

Uma nova 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. Ela pode salvar saída bruta de todos os cdmlets em um arquivo de texto.

Em cenários de suporte, todas as propriedades para todas as caixas de correio em todos os dispositivos gerenciados pelo XenMobile Mail Manager podem ser salvas selecionando-se uma caixa de seleção de diagnóstico no console.

Em cenários de suporte, agora há suporte log de nível de rastreamento.

Autenticação

O XenMobile Mail Manager oferece suporte para a autenticação básica para implantações no local. Isso permite que o XenMobile Mail Manager seja usado quando o servidor XenMobile Mail Manager não é um membro do domínio no qual o Exchange Server está localizado.

Problemas resolvidos

Regras de acesso

O XenMobile Mail Manager aplica as regras de controle de acesso local a todos os grupos de usuários no AD (Active Directory), mesmo se um grupo do AD contiver mais de 1000 usuários. Anteriormente, o XenMobile Mail Manager aplicava as regras de controle de acesso ao local somente aos primeiros 1000 usuários de um grupo do AD. [#548705]

Às vezes, o console XenMobile Mail Manager não respondia ao consultar grupos do Active Directory que continham mais de 1.000 usuários. [CXM-11729]

A janela de configuração de LDAP janela não exibe mais um modo de autenticação incorreto. [CXM-5556]

Instantâneos

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Os nomes de usuários com apóstrofos não provocam mais falhas em instantâneos secundários. [#617549]

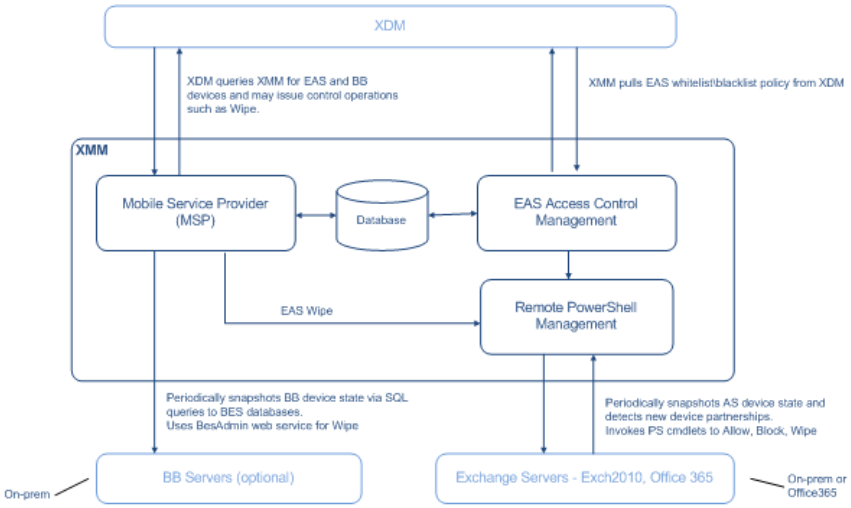
Em cenários de suporte em que o pipelining está desativado (a opção de desativar pipelining está selecionada na janela de configuração do console XenMobile Mail Manager), os principais instantâneos não apresentam mais falhas em ambientes do Exchange locais. [#586083]

Em cenários de suporte em que o pipelining está desabilitado (a opção de desativar pipelining foi selecionada na janela de configuração do console XenMobile Mail Manager), os dados para instantâneos profundos não são mais obtidos independentemente de o ambiente ter sido configurado para instantâneos profundos ou superficiais. Agora os dados para instantâneos profundos são coletados apenas quando o ambiente está configurado para instantâneos profundos. [#586092]

O primeiro instantâneo importante após a instalação inicial ocasionalmente encontrava um erro que impedia que o XenMobile Mail Manager executasse outro instantâneo principal até que o serviço XenMobile Mail Manager fosse reiniciado. Isso não ocorre mais. [CXM-5536]

Arquitetura

O seguinte diagrama mostra os principais componentes do XenMobile Mail Manager. Para obter um diagrama detalhado da arquitetura de referência, consulte o artigo do XenMobile Deployment Handbook Reference Architecture for On-Premises Deployments.



Os três componentes principais são:

- **Gerenciamento de controle de acesso do Exchange ActiveSync**. 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).
- **Gerenciamento do PowerShell remoto**. 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.
- **Provedor de serviços móveis**. Fornece uma interface de serviço da Web para que o XenMobile possa consultar dispositivos do Exchange ActiveSync e/ou BlackBerry, bem como emitir operações de controle, como Apagar, em relação a eles.

Requisitos do sistema e pré-requisito

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Os seguintes requisitos mínimos do sistema são necessários para usar o XenMobile Mail Manager:

- Windows Server 2012 R2, Windows Server 2008 R2 (deve ser um servidor baseado no idioma inglês)
- Microsoft SQL Server 2016, SQL Server 2014, SQL Server 2012, SQL Server 2012 Express LocalDB ou SQL Server Express 2008
- Microsoft .NET Framework 4.5
- 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 SP2

Os clientes de email do dispositivo

Nem todos os clientes de email sempre retornam a mesma ID do ActiveSync para um dispositivo. Como o XenMobile Mail Manager espera uma ID exclusiva do ActiveSync para cada dispositivo, somente os clientes de email que forma consistente geram o ID do ActiveSync mesmo e exclusivo para cada dispositivo são compatíveis. Esses clientes de email foram testados pela Citrix e executados sem erros:

- Cliente de email nativo HTC
- Cliente de email nativo Samsung
- Cliente de email nativo iOS
- Touchdown para Smartphones

Pré-requisitos do XenMobile Mail Manager

- O Windows Management Framework deve estar instalado.
  - PowerShell V5, V4 e V3
- A política de execução do PowerShell deve ser definida como RemoteSignedvia Set-ExecutionPolicy RemoteSigned.
- A porta TCP 80 deve estar aberta entre o computador que executa o XenMobile Mail Manager e o Exchange Server remoto.

Requisitos para o computador no local executando o Exchange

Permissões. 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Get-ManagementRole
- Get-ManagementRoleAssignment

- Se o XenMobile Mail Manager estiver configurado para exibir a floresta inteira, deve ter sido concedida permissão para executar: **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.
- De acordo com o artigo da Microsoft TechNet about_Remote_Requirements, para estabelecer uma conexão remota e executar comandos remotos, as credenciais devem corresponder a um usuário que seja um administrador no computador remoto. Segundo esta postagem do blog, You Don't Have to Be An Administrator to Run Remote PowerShell Commands, Set-PSSessionConfiguration pode ser usado para eliminar o requisito administrativo, mas o suporte e a discussão dos pormenores desse comando estão além do escopo deste documento.
- 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 XenMobile Mail Manager 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**. Com isso em mente, no mínimo, 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 Office 365 por meio do Shell remoto. Por padrão, o administrador online do Office 365 tem os privilégios necessários.
- **Políticas de limitação**. 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 três no Office 365. Quando o limite de conexão é atingido, o XenMobile Mail Manager 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 XenMobile Mail Manager.

2. Deixe a opção **Launch the Configure utility** selecionada na última tela do assistente de configuração. Ou, no menu **Iniciar**, abra o **XenMobile Mail Manager**.

3. Configure as seguintes propriedades de banco de dados:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

a. Selecione a guia **Configure** > **Database**.

b. Digite o nome do SQL Server (o padrão é localhost).

c. 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 do XenMobile Mail Manager deverão ser alteradas para uma conta do Windows que tenha permissões para acessar o SQL Server. Para fazer isso, abra **Painel de controle** > **Ferramentas administrativas** > **Serviços**, clique com o botão direito do mouse na entrada do Serviço do XenMobile Mail Manager e clique na guia **Login**.
  Nota: 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:

a. Se você estiver gerenciando um único ambiente do Exchange, precisará de um único servidor especificado. Se estiver gerenciando vários ambientes do Exchange, precisará de um único Exchange Server especificado para cada ambiente do Exchange.

b. Selecione a guia **Configure > Exchange**. c. Clique em **Add**.

d. Selecione o tipo de ambiente do Exchange Server: **On Premise** ou **Office 365**.

e. Se você selecionar **On Premise**, digite o nome do Exchange Server que será usado para os comandos do PowerShell Remoto.

f. Digite o nome do usuário de uma identidade do Windows que tenha os direitos adequados no Exchange Server, conforme especificado na seção **Requisitos**.

g. Digite a **senha** do usuário.

h. Selecione o cronograma da execução de instantâneos principais. Um instantâneo principal detecta cada parceria do Exchange ActiveSync.

i. Selecione o cronograma da execução de instantâneos secundários. Um instantâneo secundário detecta parcerias do Exchange ActiveSync recém-criadas.

j. Selecione o Snapshot Type: **Deep** ou **Shallow**. Os instantâneos superficiais são tipicamente muito mais rápidos e são suficientes para executar todas as funções de Controle de Acesso do Exchange ActiveSync do XenMobile Mail Manager. Os instantâneos profundos podem demorar significativamente mais tempo e serão necessários somente se o Provedor de Serviços Móveis estiver ativado para o ActiveSync; isso permite que o XenMobile consulte dispositivos não gerenciados.

k. Selecione o acesso padrão: **Allow**, **Block** ou **Unchanged**. Essa opção controla como todos os dispositivos diferentes dos identificados por regras explícitas do XenMobile ou Locais são tratados. Se você selecionar Allow, o acesso ao ActiveSync será permitido para todos os dispositivos; se selecionar Block, o acesso será negado; se selecionar Unchanged, nenhuma alteração será feita.

l. Selecione o modo de comando ActiveSync: **PowerShell** ou **Simulation**.

- No modo PowerShell, o XenMobile Mail Manager emitirá comandos do PowerShell para efetuar o controle de acesso desejado.
- No modo Simulation, o XenMobile Mail Manager não emitirá comandos do PowerShell, mas registrará 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.

m.Selecione **View Entire Forest** para configurar o XenMobile Mail Manager para exibir toda a floresta no Active Directory no ambiente

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

do Exchange.

n. Selecione o protocolo de autenticação: **Kerberos** ou **Basic**. O XenMobile Mail Manager oferece suporte para a autenticação básica para implantações no local. Isso permite que o XenMobile Mail Manager seja usado quando o servidor XenMobile Mail Manager não é um membro do domínio no qual o Exchange Server está localizado.

o. Clique em **Test Connectivity** para verificar se uma conexão com o Exchange Server pode ser realizada e clique em **Save**.

p. Uma mensagem solicita que você reinicie o serviço. Clique em **Yes**.

8. Configure as regras de acesso:

a. Selecione a guia **Configure** > **Access Rules**.

b. Clique na guia **XDM Rules**.

c. Clique em **Add**.

d. Digite um nome para as regras do XenMobile Server, como XdmHost.

e. Modifique a sequência de caracteres da URL para se referir ao servidor XenMobile; por exemplo, se o nome do servidor for XdmHost, e o nome da instância for zdm, insira http://XdmHostName/zdm/services/MagConfigService.

f. Insira um usuário autorizado no servidor.

g. Insira a senha de usuário.

h. Mantenha os valores padrão de Baseline Interval, Delta Interval e Timeout values.

i. Clique em **Test Connectivity** para verificar a conexão com o servidor e depois clique em **OK**.

Nota: se a caixa de seleção Disabled estiver marcada, o XenMobile Mail Manager não coletará a política do servidor XenMobile.

9. Clique na guia **Local Rules**.

a. Se você desejar criar regras locais que operam em Grupos do Active Directory, clique em **Configure LDAP** e, em seguida, configure as propriedades de conexão LDAP.

b. 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. Para obter detalhes, consulte Regras de controle de acesso do XenMobile Mail Manager.

c. Insira texto ou fragmentos de texto na caixa de texto. Opcionalmente, clique no botão de consulta para exibir as entidades que correspondem ao fragmento.

Nota: 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.

d. 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) fará 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".

e. 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 **Salve**.

10. Configure o Provedor de Serviços Móveis.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Nota: o Provedor de serviços móveis é opcional e será necessário somente se o XenMobile também estiver configurado para usar a interface do Provedor de serviços móveis para consultar dispositivos não gerenciados.

a. Selecione a guia **Configure** > **MSP**.

b. Defina o tipo de transporte de serviço, como HTTP ou HTTPS para o serviço do Provedor de serviços móveis.

c. Defina a Service Port (normalmente 80 ou 443) do serviço do Provedor de Serviços Móveis.

Nota: se você usar a porta 443, ela exigirá um certificado SSL associado a ela no IIS.

d. 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.

e. Defina se as consultas do ActiveSync estão ativadas ou não.

Nota: se as consultas do ActiveSync estiverem ativadas para o XenMobile Server, o tipo de Instantâneo de um ou mais Exchange Servers deverá ser definido como **Deep**; isso poderá afetar significativamente o desempenho da obtenção de instantâneos.

f. Por padrão, os dispositivos ActiveSync que correspondam à expressão regular Secure Mail.* não serão enviados para o XenMobile. Para alterar esse comportamento, altere o campo Filter ActiveSync conforme necessário.

Nota: em branco significa que todos os dispositivos serão encaminhados ao XenMobile.

g. Clique em **Salvar**.

11. Opcionalmente, configure um ou mais BlackBerry Enterprise Servers (BES):

a. Clique em Adicionar.

b. Insira o nome de servidor do SQL Server do BES.

c. Insira o nome do banco de dados de gerenciamento do BES.

d. Selecione o modo de Autenticação**.** Se você selecionar a autenticação Windows Integrated, a conta de usuário do serviço do XenMobile Mail Manager será a conta usada para conexão com o SQL Server do BES.

Nota: se você também escolher Windows Integrated para a conexão de banco de dados do XenMobile Mail Manager, a conta do Windows especificada aqui deverá também ter acesso ao banco de dados do XenMobile Mail Manager.

e. Se você selecionar SQL authentication, digite o nome do usuário e a senha.

f. Defina a opção Sync Schedule. Esse é o calendário usado para conexão com o SQL Server do BES e verifica se há alguma atualização de dispositivo.

g. Clique em **Test Connectivity** para verificar a conectividade com o SQL Server.

Nota: se você selecionar Windows Integrated, esse teste usará o usuário conectado no momento, e não o usuário do serviço do XenMobile Mail Manager e, portanto, não testará a autenticação do SQL corretamente.

h. Se desejar oferecer suporte ao Apagamento remoto e/ou à Redefinição de Senha de dispositivos BlackBerry do XenMobile, marque a caixa de seleção **Enabled**.

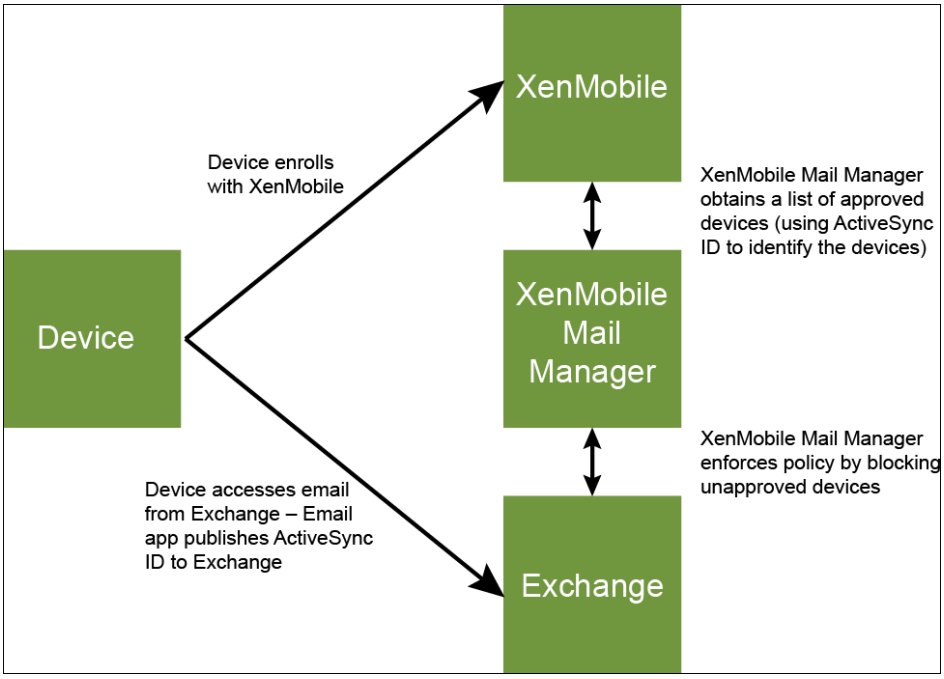
- Insira o nome de domínio totalmente qualificado (FQDN) do BES.
- Insira a porta do BES usada para o serviço da Web de administração.
- Insira o usuário totalmente qualificado e a senha exigidos pelo serviço do BES.
- Clique em **Test Connectivity** para testar a conexão com o BES.
- Clique em **Salve**.

Impor políticas de email com IDs do ActiveSync

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 XenMobile Mail Manager e o XenMobile trabalham juntos para impor essa política de email. O XenMobile define a política para acesso ao email corporativo e, quando um dispositivo não aprovado se registra no XenMobile, o XenMobile Mail Manager a impõe.

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 ID do ActiveSync, que é usado para identificar exclusivamente 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 XenMobile Mail Manager pode determinar se um dispositivo específico deve ter acesso ao email corporativo. A figura a seguir ilustra esse conceito:



Se o XenMobile enviar para o XenMobile Mail Manager um ID do ActiveSync diferente do ID que o dispositivo publica no Exchange, o XenMobile Mail Manager não conseguirá indicar para o Exchange o que fazer com o dispositivo.

A correspondência de IDs do ActiveSync funciona de maneira 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.
- Em todas as outras plataformas Android, envie por push o aplicativo Touchdown e a configuração do ActiveSync do Touchdown do XenMobile.

No entanto, isso não impede que um funcionário instale um cliente de email diferente do Touchdown em um dispositivo Android. 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 XenMobile Mail Manager para bloquear emails definindo a política estática como Deny by default. Isso significa que se um funcionário configurar um cliente de email diferente do Touchdown 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 XenMobile Mail Manager fornece uma abordagem baseada em regras para configurar dinamicamente o controle de acesso a dispositivos Exchange ActiveSync. Uma regra de controle de acesso do XenMobile Mail Manager 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 **Cancelar** 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 XenMobile Mail Manager tem três tipos de regras: regras locais, regras de servidor XenMobile (também conhecidas como regras do 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 nem a regra de acesso padrão serão consultadas. As regras locais são configuradas localmente no XenMobile Mail Manager 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 de servidor XenMobile. As regras do XenMobile são referências a um servidor XenMobile externo que fornece regras sobre dispositivos gerenciados. O servidor XenMobile 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 jailbreak ou se o dispositivo contém aplicativos proibidos. O XenMobile avalia as regras de alto nível e produz um conjunto de IDs de Dispositivo ActiveSync permitidos ou bloqueados, que são então entregues ao XenMobile Mail Manager em seguida.

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 servidor XenMobile, 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 XenMoble será permitido.
- **Acesso padrão – Bloquear**. Qualquer dispositivo que não for correspondido por uma regra local ou do XenMoble será bloqueado.
- **Default Access - Unchanged**. Qualquer dispositivo que não for correspondido por uma regra local ou do XenMoble não terá o respectivo estado de acesso modificado de forma nenhuma pelo XenMobile Mail Manager. 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 XenMobile Mail Manager, as regras são avaliadas em sequência, da prioridade mais alta para a mais baixa, desta forma:

- Regras locais
- Regras de servidor XenMobile
- 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 servidor XenMobile 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 for encontrada, a avaliação será interrompida.

O XenMobile Mail Manager reavalia o conjunto de regras definido no momento quando as propriedades de dispositivo são alteradas,

© 1999-2017 Citrix Systems, Inc. All rights reserved.

quando dispositivos são adicionados ou removidos, ou quando as regras em si 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 XenMobile Mail Manager. O Exchange pode ser configurado com três níveis de regras: isenções pessoais, regras de dispositivo e configurações de organização. O XenMobile Mail Manager 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 XenMobile Mail Manager efetivamente assume o gerenciamento do recurso de listas de isenção no Exchange. Para obter detalhes, consulte este artigo da Microsoft.

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:

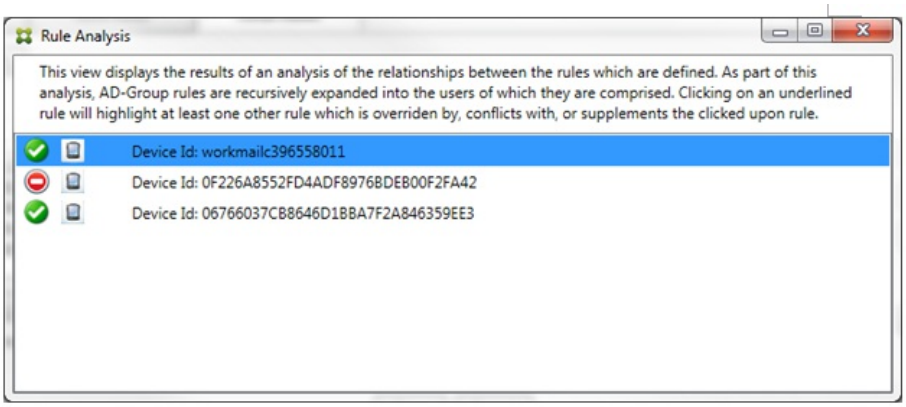
- **Regra predominante**. Uma predominância ocorre quando mais de uma única regra poderia ser aplicada ao mesmo dispositivo. Como as regras são avaliadas por prioridade na lista, as instâncias de regra de menor prioridade que podem ser aplicadas podem nunca ser avaliadas.
- **Regra conflitante**. Um 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 será 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.

A aparência dos tipos de regras na caixa de diálogo Rule Analysis

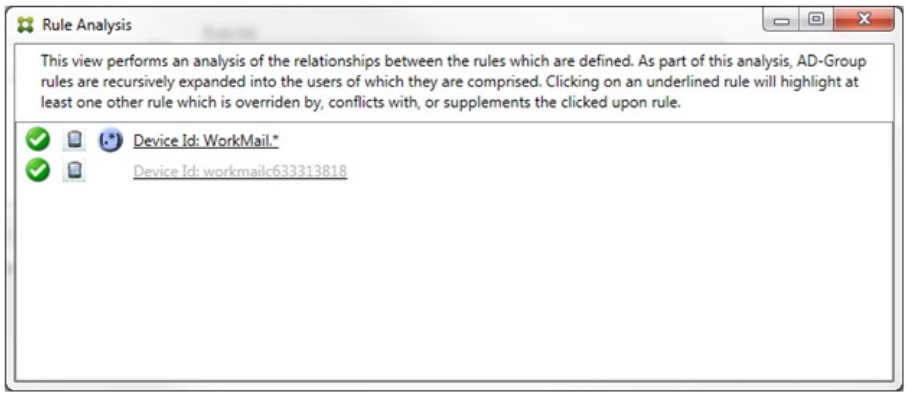
Quando não existirem conflitos, substituições ou suplementos, a caixa de diálogo Rule Analysis não apresentará entradas sublinhadas. Clicar em qualquer um dos itens não terá impacto; por exemplo, os visuais normais de item selecionado ocorrerão.

A janela Análise de regras tem uma caixa de seleção que, quando selecionada, exibe somente as regras que são conflitos, substituições, redundâncias ou suplementos.

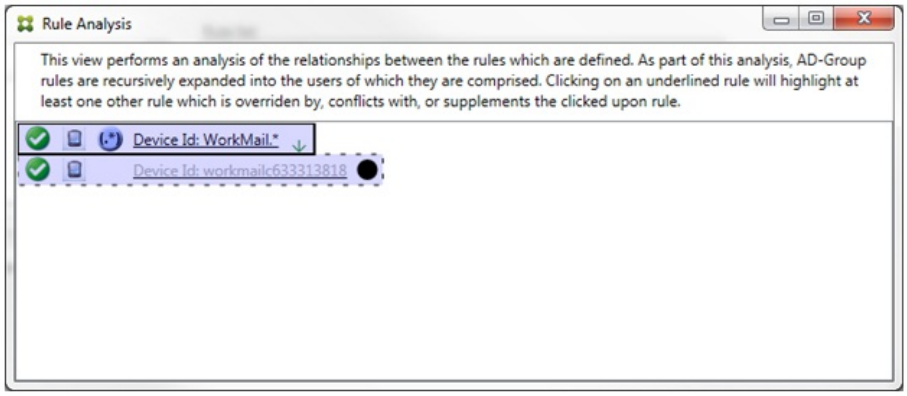
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 será 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 substituída para descobrir qual regra ou regras a substituíram. Sempre que uma regra substituída tiver sido realçada como resultado de a regra ser a regra principal ou auxiliar, um círculo preto será 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:

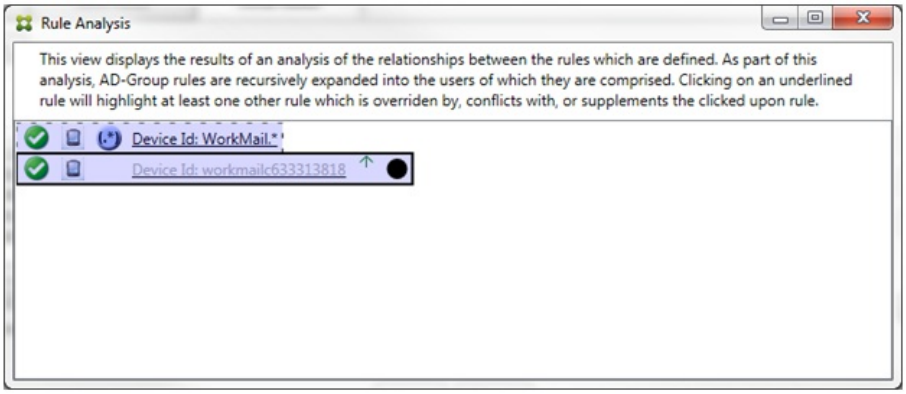


Quando você clica na regra de prioridade mais alta, a caixa de diálogo é exibida da seguinte forma:



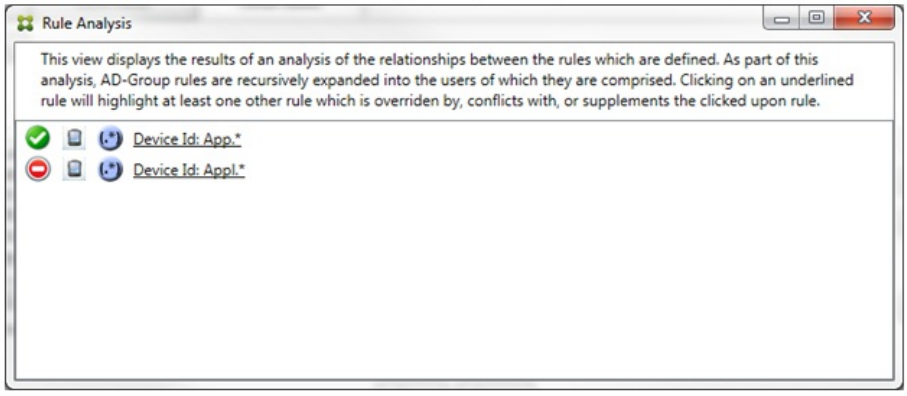
Nesse exemplo, a regra de expressão regular WorkMail.* é a regra principal (indicada pela borda sólida) e a regra normal workmailc633313818 é uma regra auxiliar (indicada pela borda tracejada). O ponto preto ao lado da regra auxiliar é uma indicação visual adicional de que a regra está inativa (nunca será avaliada) devido à regra de expressão regular de prioridade mais alta que a precede. Depois de clicar na regra substituída, a caixa de diálogo é exibida da seguinte forma:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

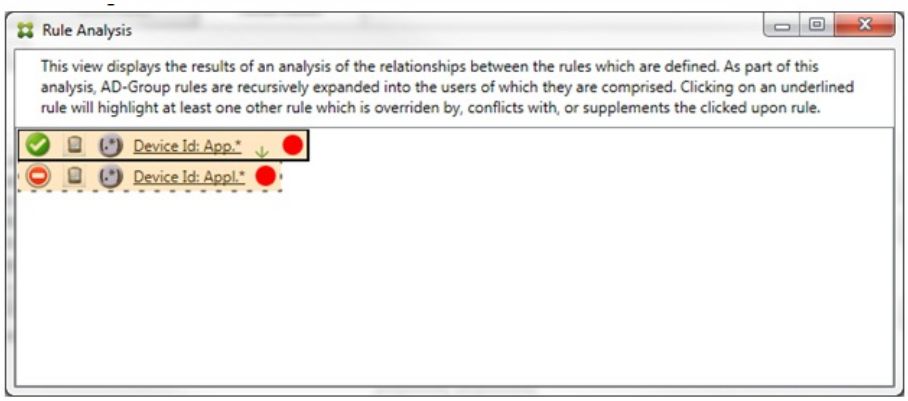


No exemplo anterior, a regra de expressão regular WorkMail.* é a regra auxiliar (indicada pela borda tracejada) e a regra normal workmailc633313818 é uma regra principal (indicada pela borda sólida). Nesse exemplo simples, não há muita diferença. Para um exemplo mais complicado, consulte o exemplo de 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:



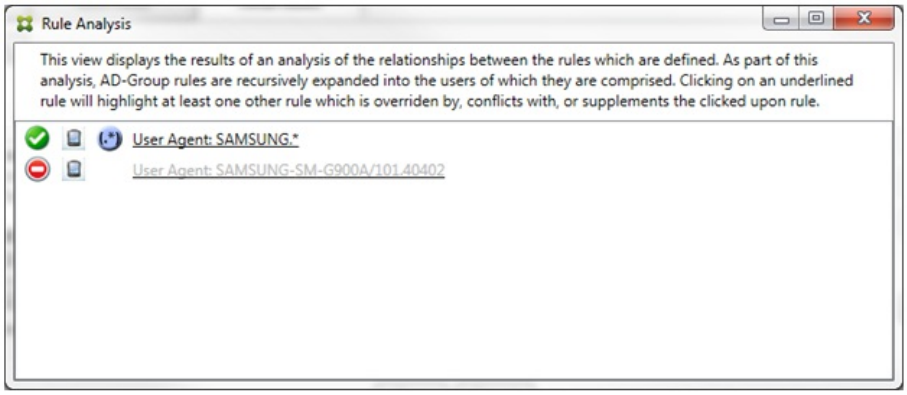
Quando se inspeciona as duas regras de expressão regular, fica evidente que a primeira regra permite todos os dispositivos com um ID de dispositivo que contém "App" e que a segunda regra nega todos os dispositivos com um ID de dispositivo que contém Appl. Além disso, mesmo que a segunda regra negue todos 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:



© 1999-2017 Citrix Systems, Inc. All rights reserved.

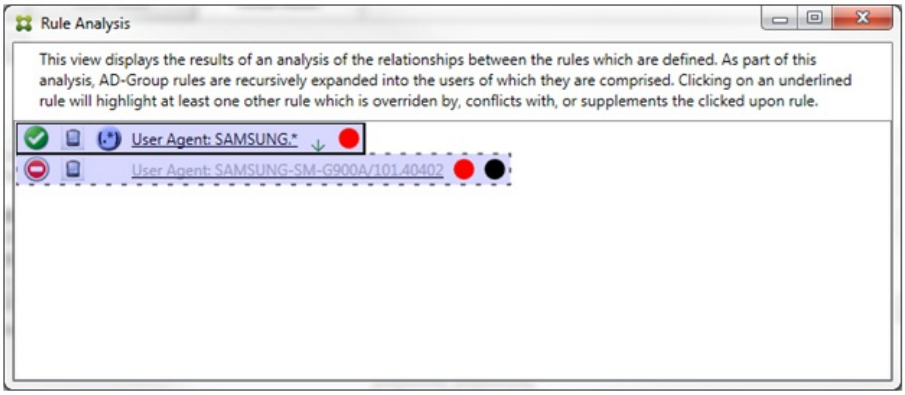
No cenário anterior, tanto a regra principal (a regra de expressão regular App.*) quanto a regra auxiliar (a regra de expressão regular Appl.*) são realçadas em amarelo. Trata-se simplesmente de um aviso visual para alertar para o fato de que você aplicou mais de uma única regra de expressão regular 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 substituição, 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.

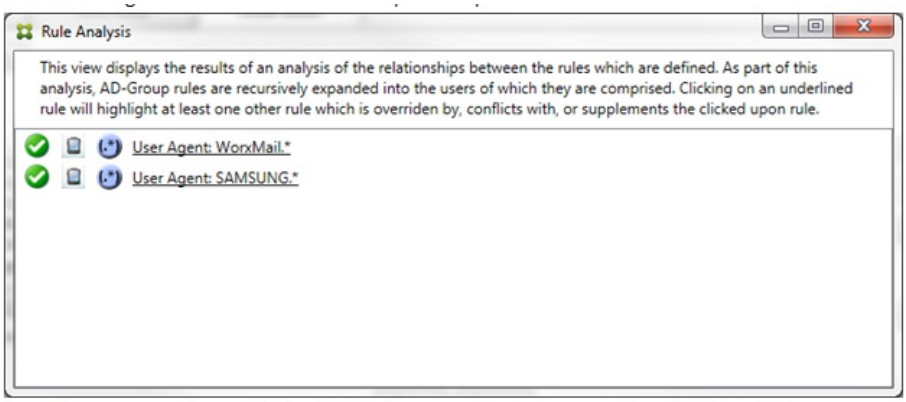
Depois de clicar na regra de expressão regular, a caixa de diálogo é exibida da seguinte forma:



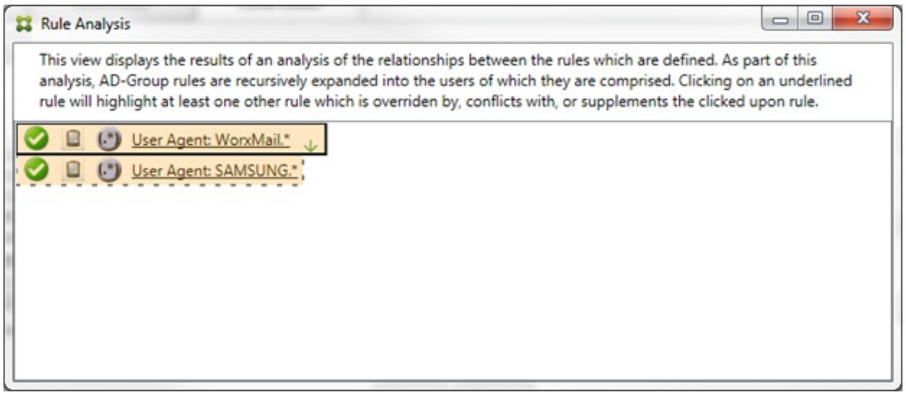
A regra principal (a regra de expressão regular SAMSUNG.*) é seguida por um ponto vermelho para indicar que o estado de acesso dela entra em conflito com uma ou mais regras auxiliares. A regra auxiliar (a regra normal SAMSUNG-SM-G900A/101.40402) é seguida por um ponto vermelho para indicar que o estado de acesso dela entra em conflito com a regra principal, bem como por um ponto preto, como uma indicação adicional de que ela 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:

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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 XenMobile Mail Manager. Depois de clicar na primeira regra, a caixa de diálogo tem a seguinte aparência:

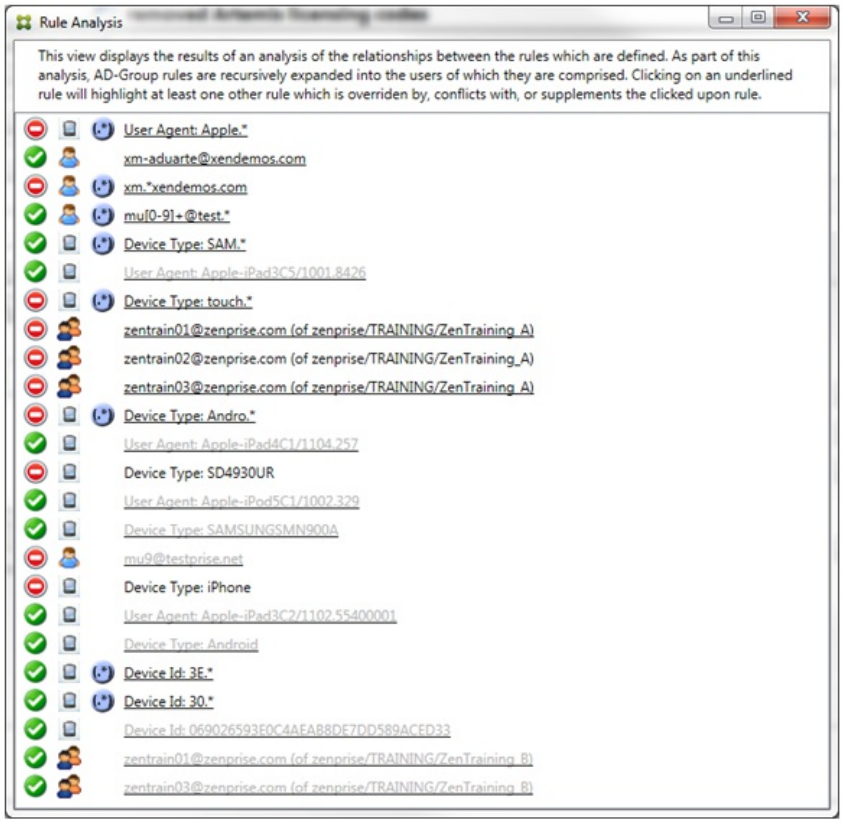


A regra principal (a regra de expressão regular WorkMail.*) é realçada com uma sobreposição amarela para indicar que existe pelo menos uma regra auxiliar adicional que é uma expressão regular. A regra auxiliar (a regra de expressão regular SAMSUNG.*) é realçada com uma sobreposição amarela para indicar que ela e a regra principal são regras de expressão regular aplicadas ao mesmo campo no XenMobile Mail Manager; nesse caso, o campo de ID de dispositivo 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 (.*).

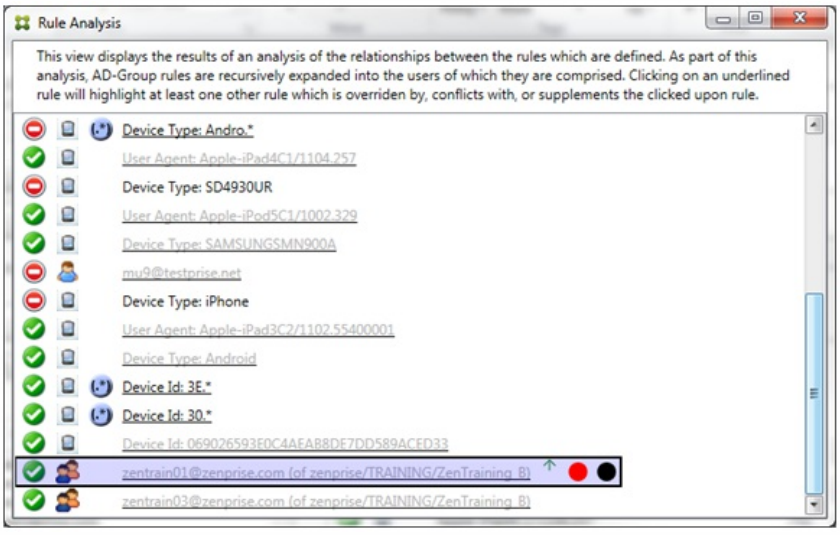
© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.



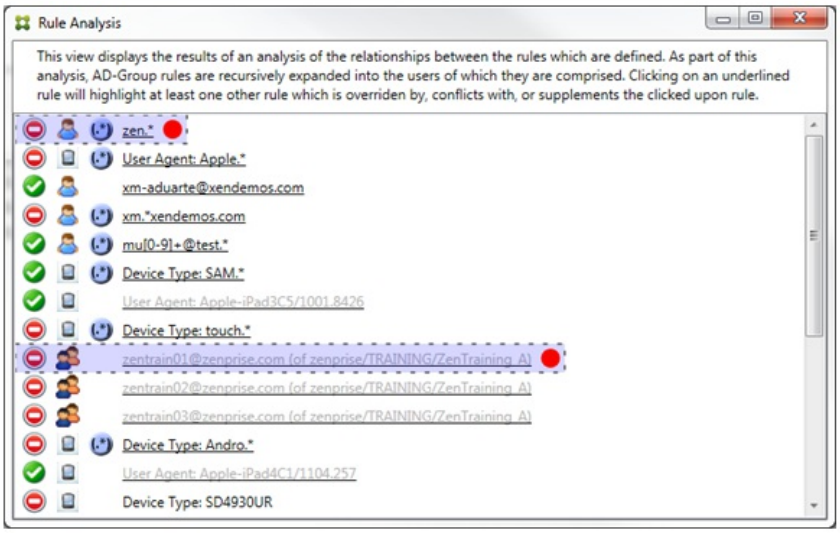
A regra principal (regra AD-group zenprise/treinamento/ZenTraining B, da qual zentrain01@zenprise.com é um membro) apresenta as seguintes características:

- 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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

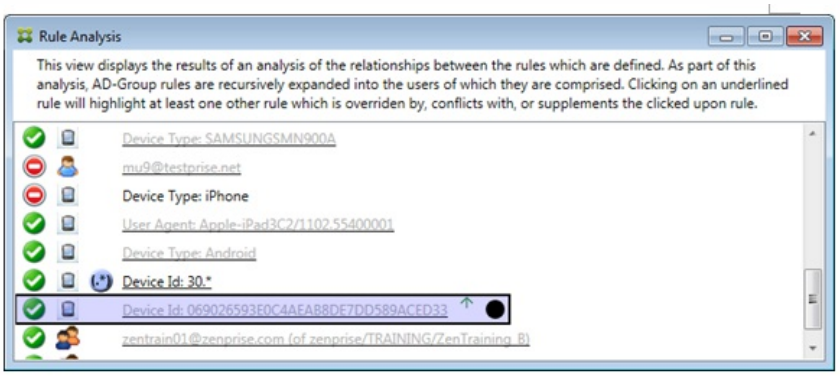
com o respectivo acesso e que a regra principal foi substituída e, portanto, está inativa.

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.

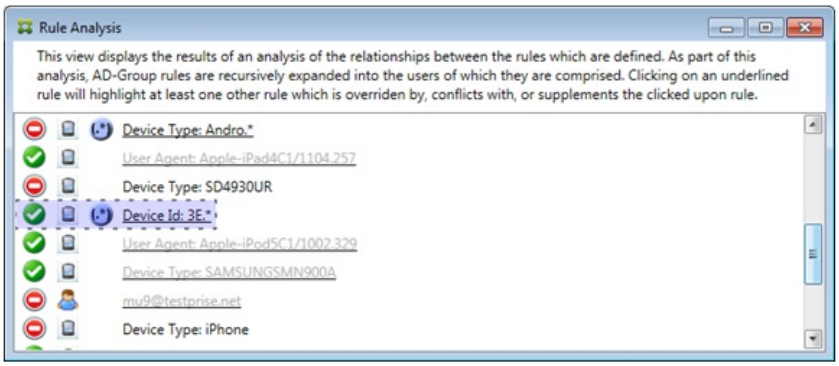
Exemplo 2: Esse exemplo mostra por que o dispositivo com um ID de dispositivo ActiveSync 069026593E0C4AEAB8DE7DD589ACED33 foi substituído:



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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

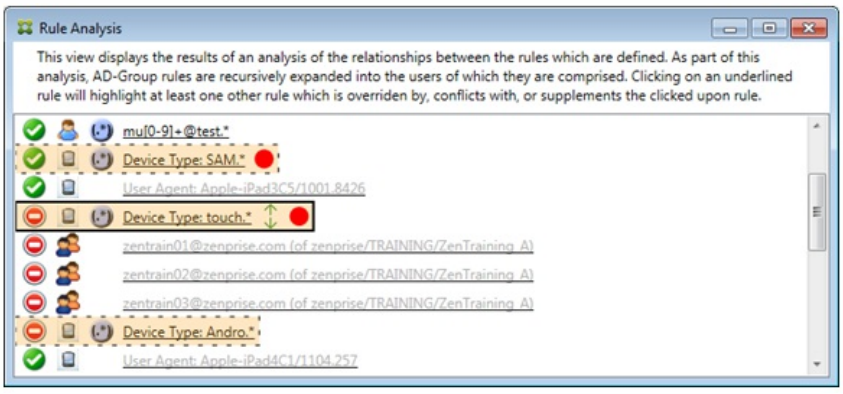


Nesse caso, uma única regra auxiliar substitui a regra principal: a regra de ID de dispositivo ActiveSync de expressão regular governar 3E.*. Como a expressão regular 3E.*corresponderia a 069026593E0C4AEAB8DE7DD589ACED33, a regra principal nunca será avaliada.

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:

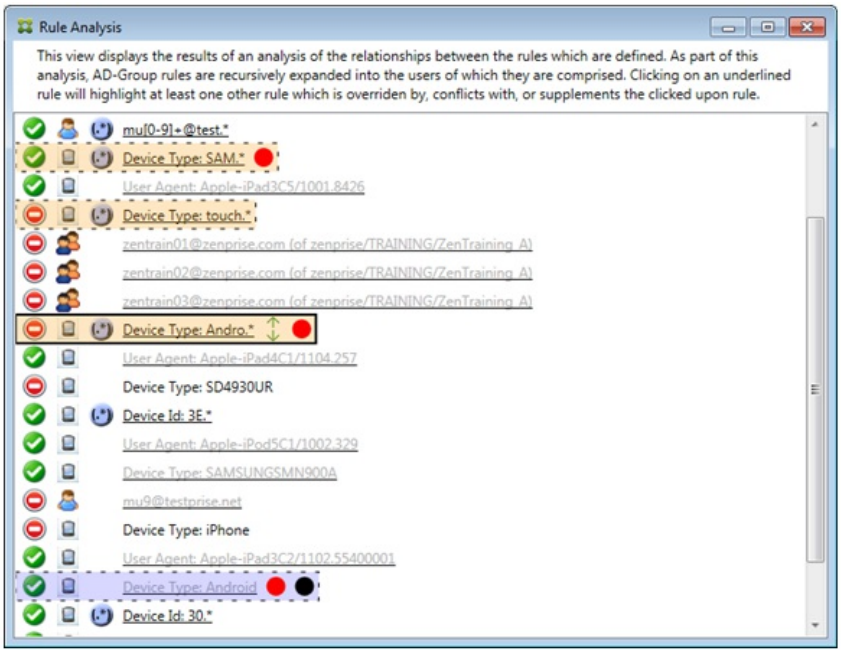
- É indicada por uma borda sólida com uma sobreposição amarela, como um aviso de que há mais de uma única regra de expressão regular em funcionamento em relação a um campo de regra específico; nesse caso, o tipo de dispositivo ActiveSync.
- Duas setas apontam respectivamente para cima e para baixo, indicando 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 são aplicadas de forma suplementar 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 um clique na regra de expressão regular se aplica 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 realçadas.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



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.

   Nesse exemplo, todos os dispositivos que têm um tipo de dispositivo TouchDown têm o 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 instantâneo 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**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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. Nesse exemplo, a escolha é Allow, e o resultado final será 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. Verifique se que a caixa de seleção regular expression está 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 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.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Monitoramento de dispositivo

A guia **Monitor** no XenMobile Mail Manager 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:

- **Dispositivos do ActiveSync**:
  - 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 XenMobile Mail Manager registra erros e outras informações operacionais no respectivo arquivo de log: \log\XmmWindowsService.log. O XenMobile Mail Manager também registra eventos importantes no Log de Eventos do Windows.

Erros Comuns

A seguinte lista inclui os erros comuns:

O serviço do XenMobile Mail Manager 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 do XenMobile Mail Manager 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 Integrada do Windows estiver configurada, a conta de usuário do serviço do XenMobile Mail Manager deve ser um login permitido do SQL. A conta do serviço do XenMobile Mail Manager 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 XenMobile Mail Manager. 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 http://msdn.microsoft.com/pt-br/library/ms733791.aspx para obter detalhes sobre como instalar os certificados.

O XenMobile Mail Manager contém um programa utilitário para testar a conectividade com o serviço do MSP. Execute o programa MspTestServiceClient.exe e defina a URL e as credenciais de 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 serviço XenMobile emite. Observe que, se HTTPS estiver configurado, você deverá especificar o nome de host real do servidor (o nome especificado no certificado SSL).

Nota: quando você estiver usando **Test Connectivity**, verifique se há pelo menos um registro do ActiveSyncDevice ou o teste poderá falhar.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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. Ela pode salvar saída bruta de todos os cdmlets em um arquivo de texto.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile NetScaler Connector

Feb 21, 2018

O XenMobile NetScaler Connector oferece um serviço de autorização de nível de dispositivo dos clientes ActiveSync para o NetScaler 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 XenMobile NetScaler Connector.

Para obter mais informações, consulte ActiveSync Gateway em XenMobile.

Para obter um diagrama detalhado da arquitetura de referência, consulte o artigo do XenMobile Deployment Handbook Reference Architecture for On-Premises Deployments.

Este artigo inclui as seções a seguir:

- Monitoramento do XenMobile NetScaler Connector
- Para simular o tráfego do ActiveSync com o XenMobile NetScaler Connector
- Escolha de filtros para o XenMobile NetScaler Connector
- Para configurar uma conexão ao XenMobile NetScaler Connector
- Para importar uma política do XenMobile
- Configuração do modo de política do XenMobile NetScaler Connector
- Configuração do XenMobile NetScaler Connector
- Escolha de um modelo de segurança para o XenMobile NetScaler Connector
- Gerenciamento do XenMobile NetScaler Connector
- Instalação do XenMobile NetScaler Connector
- Requisitos de sistema do XenMobile NetScaler Connector
- Implantação do XenMobile NetScaler Connector

Monitoramento do XenMobile NetScaler Connector

O utilitário de configuração do XenMobile NetScaler Connector 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 XenMobile NetScaler Connector pelo NetScaler para autorização.

Além disso, para garantir que o serviço web do XenMobile NetScaler Connector esteja em execução, você pode carregar a seguinte URL em um navegador no servidor XenMobile NetScaler Connector http:///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 XenMobile NetScaler Connector

Você pode usar o XenMobile NetScaler Connector para simular como o tráfego do ActiveSync se parecerá em conjunto com suas políticas. No utilitário de configuração do XenMobile NetScaler Connector, selecione a guia **Simulações**. Os resultados mostram como suas políticas serão aplicadas de acordo com as regras que você configurou.

Escolha de filtros para o XenMobile NetScaler Connector

Os filtros do XenMobile NetScaler Connector 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

© 1999-2017 Citrix Systems, Inc. All rights reserved.

atendem aos critérios definidos. Os seguintes filtros estão disponíveis para o XenMobile NetScaler Connector no XenMobile.

- **Aplicativos em lista negra**. Permite ou nega dispositivos com base na Lista de dispositivos definida pelas políticas da lista negra e na presença de aplicativos da lista negra.
- **Somente os aplicativos em lista branca**. Permite ou nega dispositivos com base na Lista de dispositivos definida pelas políticas da lista branca e na não presença de aplicativos da lista branca.
- **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.
- **Dispositivos Android com raiz / 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 sem conformidade**. Permite negar ou permitir dispositivos que atendam aos seus próprios critérios internos de conformidade com TI. Conformidade é uma configuração arbitrária definida pela propriedade do dispositivo chamada Sem conformidade, que é um sinalizador booliano que pode ser Verdadeiro ou Falso. (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 = Verdadeiro** 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 = Falso.** Se um dispositivo atende aos padrões de conformidade e definições de políticas definidos pelo seu departamento de TI, o dispositivo está em conformidade.
- **Senha não compatível**. Cria uma lista de dispositivos de todos os dispositivos que não tenham um código secreto no dispositivo.
- **Status revogado**. Cria uma Lista de Dispositivos de todos os dispositivos revogados e permite ou nega com base no status de revogado.
- **Dispositivos inativos**. Cria uma Lista de Dispositivos de dispositivos que não se comunicaram com o XenMobile dentro de um período de tempo especificado e, portanto, são considerados inativos e permite ou nega os dispositivos apropriadamente.
- 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.
- **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 conexões com base nessa lista. A opção Permissão/negação implícita garante que o status do XenMobile NetScaler Connector na guia Dispositivos esteja ativado e mostre o status do XenMobile NetScaler Connector para seus dispositivos. A opção Permissão/negação implícita também controla todos os outros filtros do XenMobile NetScaler Connector que não foram selecionados. Por exemplo, aplicativos em listas negras serão negados (bloqueados) pelo XenMobile NetScaler Connector, enquanto que todos os outros filtros serão permitidos, pois a opção Permissão/negação implícita está selecionada para Permitir.

Para configurar uma conexão ao XenMobile NetScaler Connector

XenMobile NetScaler Connector se comunica com o XenMobile e outros provedores de configuração remota por meio de serviços da web seguros.

1. No utilitário de configuração do XenMobile NetScaler Connector, 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:////*instanceName*/services/*MagConfigService*. O nome *MagConfigService* diferencia maiúsculas de minúsculas.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 XenMobile NetScaler Connector.
6. Em **Intervalo de linha de base**, especifique um período de tempo para quando um novo conjunto de regras dinâmico atualizado é recebido do Device Manager.
7. Em **Delta interval**, 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 **Config Provider**, 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 XenMobile NetScaler Connector notifique o XenMobile quando um dispositivo estiver bloqueado. Essa opção é necessária se você estiver usando as regras do XenMobile NetScaler Connector 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 XenMobile NetScaler Connector 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 XenMobile NetScaler Configuration, 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 básica de HTTP 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 estabelecida com sucesso, 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 XenMobile NetScaler Connector

O XenMobile NetScaler Connector pode ser executado nos seguintes seis modos:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Permitir todos**. Este modo de política concede acesso para todo o tráfego que passa pelo XenMobile NetScaler Connector. Não são utilizadas outras regras de filtragem.
- **Negar todos**. Este modo de política bloqueia o acesso de todo o tráfego que passa pelo XenMobile NetScaler Connector. 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 XenMobile NetScaler Connector 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 XenMobile NetScaler Connector.
- **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 XenMobile NetScaler Connector 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 XenMobile NetScaler Connector 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 XenMobile NetScaler Connector a permitir ou bloquear o tráfego pelos seguintes critérios:

- **Usuário**. O XenMobile NetScaler Connector 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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

do XenMobile NetScaler Connector mostra os valores que são passados através do XenMobile NetScaler Connector. 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 XenMobile NetScaler Connector.
- **DeviceType**. O XenMobile NetScaler Connector 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 XenMobile NetScaler Connector 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 XenMobile NetScaler Connector 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 e no Device Manager definem regras dinâmicas e podem disparar um filtro dinâmico do XenMobile NetScaler Connector. Os disparadores são baseados na presença de uma violação de política ou configuração de propriedade. Os filtros do XenMobile NetScaler Connector 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 XenMobile NetScaler Connector.

Nota: essas regras dinâmicas devem ser configuradas no console XenMobile.
1. No console XenMobile, clique no ícone de engrenagem no canto superior direito. A página **Configurações** 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 desejar 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 XenMobile NetScaler Connector caso o XenMobile não tenha o identificador do ActiveSync do usuário do dispositivo Android.

Para configurar as políticas personalizadas editando o arquivo XML do XenMobile NetScaler Connector

Você pode visualizar as políticas básicas na configuração padrão na guia **Políticas** do utilitário de configuração do XenMobile NetScaler Connector. Se você quiser criar políticas personalizadas, você pode editar o arquivo de configuração XML do XenMobile NetScaler Connector (config\config.xml).

© 1999-2017 Citrix Systems, Inc. All rights reserved.

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 XenMobile NetScaler Connector

O XenMobile NetScaler Connector usa um arquivo de configuração XML para ditar as ações do XenMobile NetScaler Connector. 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 NetScaler Connector\config\.

Nós GroupRef

Os nós GroupRef definem os nomes de grupos lógicos: por padrão, 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 XenMobile NetScaler Connector

Você pode configurar o XenMobile NetScaler Connector 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 XenMobile NetScaler Connector conecta os grupos periodicamente. O XenMobile pode exportar grupos de usuários e dispositivos permitidos e

© 1999-2017 Citrix Systems, Inc. All rights reserved.

bloqueados para o XenMobile NetScaler Connector.

Os grupos dinâmicos são mantidos por uma fonte externa chamada Gateway Configuration Provider e coletados pelo XenMobile NetScaler Connector periodicamente. O XenMobile pode exportar grupos de usuários e dispositivos permitidos e bloqueados para o XenMobile NetScaler Connector.

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 XenMobile NetScaler Connector

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 integrar o XenMobile NetScaler Connector com 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 XenMobile NetScaler Connector

Você pode usar o XenMobile NetScaler Connector 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 negras ou listas brancas de aplicativos e outras condições de conformidade.

Ao usar o utilitário de configuração XenMobile NetScaler Connector, 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

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

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 XNC

1. Execute XncInstaller.exe com uma conta de administrador.
2. Siga as instruções na tela para concluir a desinstalação.

Para instalar, atualizar ou desinstalar o XenMobile NetScaler Connector

1. Execute o XncInstaller.exe com uma conta de administrador para instalar o XenMobile NetScaler Connector (XNC) ou permitir a atualização ou remoção de um XenMobile NetScaler Connector existente.
2. Siga as instruções na tela para concluir a instalação, atualização ou desinstalação.

Depois de instalar o XenMobile NetScaler Connector, manualmente reinicie o serviço de configuração do XenMobile e o serviço de notificação.

Instalação do XenMobile NetScaler Connector

Você pode instalar o XenMobile NetScaler Connector no seu próprio servidor ou no mesmo servidor no qual você instalou o XenMobile.

Você pode considerar a instalação do XenMobile NetScaler Connector em seu próprio servidor (separado do XenMobile) pelos seguintes motivos:

- Se o seu XenMobile Server estiver hospedado remotamente na nuvem (localização física).
- Se você não quiser que o XenMobile NetScaler Connector seja afetado pelas reinicializações do XenMobile Server(disponibilidade).
- Se você quiser que os recursos do sistema de um servidor sejam inteiramente dedicados ao XenMobile NetScaler Connector (desempenho).

A carga de CPU que o XenMobile NetScaler Connector coloca em um servidor depende da quantidade de dispositivos gerenciados. Um regra geral é provisionar um núcleo de CPU a mais se o XenMobile NetScaler Connector foi implantado no mesmo servidor que o XenMobile. Para um grande número de dispositivos (mais de 50.000), talvez seja necessário fornecer mais núcleos se você não tiver um ambiente em cluster. A espaço de memória do XenMobile NetScaler Connector não é suficientemente significativo para garantir mais memória.

Requisitos de sistema do XenMobile NetScaler Connector

O XenMobile NetScaler Connector se comunica com o NetScaler sobre uma ponte SSL configurada no dispositivo NetScaler. A ponte permite que o dispositivo transmita todo o tráfego seguro diretamente para o XenMobile. O XenMobile NetScaler Connector requer a seguinte configuração mínima do sistema:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Component	Requirement
Computador e processador	Processador 733 MHz Pentium III de 733 MHz ou superior. Processador Pentium III de 2.0 GHz ou superior (recomendado)
NetScaler	Dispositivo NetScaler 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	Microsoft Windows Server 2008 R2, Microsoft Windows Server 2008 SP2, Microsoft Windows Server 2012 R2
Outros dispositivos	Adaptador de rede compatível com o sistema operacional host para comunicação com a rede interna
Tela	Monitor VGA ou resolução superior

O computador host para o XenMobile NetScaler Connector 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 da plataforma para o XenMobile NetScaler Connector, consulte Plataformas de dispositivo suportadas no XenMobile.

Os clientes de email do dispositivo

Nem todos os clientes de email sempre retornam a mesma ID do ActiveSync para um dispositivo. Como o XenMobile NetScaler Connector espera um ID exclusivo do ActiveSync para cada dispositivo, o seguinte é verdadeiro: somente os clientes de email que consistentemente geram o mesmo ID do ActiveSync exclusivo para cada dispositivo são compatíveis. A Citrix testou esses clientes de email e os clientes foram executados sem erros:

- Cliente de email nativo HTC
- Cliente de email nativo Samsung
- Cliente de email nativo iOS
- TouchDown

Implantação do XenMobile NetScaler Connector

O XenMobile NetScaler Connector permite que você use NetScaler para proxy e balanceamento de carga de comunicação do XenMobile Server com dispositivos gerenciados XenMobile. O XenMobile NetScaler Connector se comunica periodicamente com o XenMobile para sincronizar as políticas. O XenMobile NetScaler Connector e o XenMobile podem ser agrupados, em conjunto ou independentemente, e podem ter a carga balanceada pelo NetScaler.
Componentes do XenMobile NetScaler Connector

- **Serviço XenMobile NetScaler Connector**. Esse serviço fornece uma interface de serviço web REST que pode ser invocada pelo NetScaler para determinar se uma solicitação do ActiveSync de um dispositivo está autorizada.
- **Serviço de configuração do XenMobile**. Esse serviço se comunica com o Device Manager para sincronizar as alterações

© 1999-2017 Citrix Systems, Inc. All rights reserved.

da política do Device Manager com o XenMobile NetScaler Connector.

- **Serviço de notificação do XenMobile**. Esse serviço envia notificações de acesso a dispositivo não autorizado para o Device Manager. Desta forma, o Device Manager pode tomar as medidas apropriadas, como notificar o usuário por que o dispositivo foi bloqueado.
- **Utilitário de configuração do XenMobile NetScaler**. Esse aplicativo permite ao administrador configurar e monitorar o XenMobile NetScaler Connector.

Para configurar os endereços de escuta para o XenMobile NetScaler Connector

Para o XenMobile NetScaler Connector receber solicitações do NetScaler para autorizar o tráfego do ActiveSync, faça o seguinte: Especifique a porta em que o XenMobile NetScaler Connector escuta as chamadas de serviço da web do NetScaler.

1. No menu **Iniciar**, selecione o Utilitário de configuração do XenMobile NetScaler.
2. Clique na guia **Serviço da Web** e, em seguida, digite os endereços de escuta para o serviço da web do XenMobile NetScaler Connector. Você pode selecionar **HTTP** ou **HTTPS** ou ambos. Se o XenMobile NetScaler Connector 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 as políticas de controle de acesso do dispositivo no XenMobile NetScaler Connector

Para configurar a política de controle de acesso que deseja aplicar aos seus dispositivos gerenciados, faça o seguinte:

1. No utilitário de configuração do XenMobile NetScaler, 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 **Static + ZDM: Modo de Permissão ou Static + 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 XenMobile NetScaler Connector e NetScaler.

Nota: essa tarefa pressupõe que você já instalou e configurou o XenMobile.

1. No utilitário de configuração do XenMobile NetScaler Connector, 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:////*NomedaInstância*/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 servidor web do XenMobile.
5. Em **Gerenciamento de Host**, insira o nome do servidor no qual você instalou o XenMobile NetScaler Connector.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

6. Em **Intervalo de linha de base**, especifique um período de tempo para quando um novo conjunto de regras dinâmico atualizado é recebido do XenMobile.
7. Em **Tempo limite de solicitação**, especifique o intervalo de tempo limite de solicitação do servidor.
8. Em **Config Provider**, 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. Quando o servidor estiver configurado, clique em **Testar Conectividade** para testar a conexão com o XenMobile Server.
11. Quando a conectividade for estabelecida, clique em **Salvar**.

Implantando o XenMobile NetScaler Connector para escalabilidade e redundância

Se deseja dimensionar sua implantação do XenMobile NetScaler Connector e do XenMobile, você pode instalar instâncias do XenMobile NetScaler Connector em vários Windows Servers, todos apontando para a mesma instância XenMobile e, em seguida, usar o NetScaler para balancear a carga dos servidores.

Há dois modos para a configuração do XenMobile NetScaler Connector:

- No modo não compartilhado, cada instância do XenMobile NetScaler Connector se comunica com 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 XenMobile NetScaler Connector em cada XenMobile Server e o XenMobile NetScaler Connector obteria as políticas da instância do XenMobile local.
- No modo compartilhado, um nó do XenMobile NetScaler Connector 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 XenMobile NetScaler Connector está em uma única pasta (que consiste em alguns arquivos XML). O processo do XenMobile NetScaler Connector 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 XenMobile NetScaler Connector.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Conceitos avançados

Feb 21, 2018

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 pontos decisórios, recomendações, perguntas comuns e casos de uso para o seu ambiente XenMobile de ponta a ponta, consulte o XenMobile Deployment Handbook.

Para fóruns de suporte de comunidade no XenMobile, consulte Citrix Discussions.

Interação do XenMobile no local com o Active Directory

Manual de implantação do XenMobile

Enviar convites para registro em grupo no XenMobile

Configurar um servidor de atestado de integridade de dispositivo no local

Configurar a autenticação baseada em certificado com o EWS para notificações por push do Secure Mail

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Interação do XenMobile no local com o Active Directory

Siddartha Vuppala , **Priyanka Joshi** | Feb 21, 2018

This article explains the interaction between XenMobile Server and Active Directory. XenMobile Server interacts with Active Directory both inline and in the background. The following sections provide more information on the inline and the background operations that involve Active Directory interaction.

> ## Nota
>
> This article is an overview of the interaction and does not cover the granular details. For more information about configuring Active Directory and LDAP in the XenMobile console, see Domain or domain plus security token authentication.

Inline interactions

XenMobile Server communicates with Active Directory by using the LDAP settings that an administrator configures. The settings retrieve information about users and groups. Following are the operations that result in interaction between XenMobile Server and Active Directory.

1. **LDAP configuration.** Configuration of Active Directory itself results in an interaction with Active Directory. XenMobile Server attempts to validate the information by authenticating the information with Active Directory. The server does so by using the internet protocol, port, and service account credentials provided. A successful bind indicates that the connection is configured correctly.
2. **Group-based interactions.**

   a. Search for one or more groups during the Role-Based Access Control (RBAC) and delivery group definition creation. The XenMobile Server administrator inputs a search text string in the XenMobile console. XenMobile Server searches the selected domain for all groups that contain the substring that is provided. Then, XenMobile Server retrieves the objectGUID, sAMAccountName, and Distinguished Name attributes of the groups identified in the search.

   > ## Nota
   >
   > This information is not stored in the XenMobile Server database.

   b. RBAC and deployment group definition add or update. The XenMobile Server administrator selects the Active Directory groups of interest based on the previous search and includes them in the deployment group definition. 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. Group membership information helps determine membership between the group retrieved and existing users or groups in the XenMobile Server database. Changes to group membership result in the RBAC and deployment group derivation for the affected user members, which results in user entitlements.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

> **Nota**
>
> Changes to the deployment group definition can lead to change in app or policy entitlements for affected users.

c. **One-time PIN (OTP) invitations**. The XenMobile Server administrator selects a group from the list of Active Directory groups present in the XenMobile Server database. For this group, all the users, both direct and indirect, are retrieved from Active Directory. OTP invitations are sent to the users who were identified in the preceding step.

> **Nota**
>
> The preceding three interactions imply that group-based interactions are triggered based on XenMobile Server configuration changes. When there are no changes to the configuration, the interactions imply that there are no interactions with Active Directory. They also imply that there are no requirement for background jobs to capture the group side of changes on a periodic basis.

3. **User-based interaction.**

   a. User authentication. User authentication workflow results in two interactions with Active Directory:

   - Used to authenticate the user with the credentials provided.
   - Add or update select user attributes to the XenMobile Server database, including objectGUID, Distinguished Name, sAMAccountName, and direct membership to groups. Changes to group membership result in the re-evaluation of the app, policy, and access entitlements.

   The user can authenticate either from the device or from the XenMobile Server console. In both the scenarios, interaction with Active Directory adheres to the same behavior.

   b. App Store access and refresh. A refresh of the store results in a refresh of user attributes, including direct group memberships. This action allows for a re-evaluation of user entitlements.

   c. Device check-ins. Administrators can configure in the XenMobile console the device check-ins on a periodic basis. Every time a device is checked-in, the corresponding user attributes are refreshed, including direct group memberships. These check-ins allow for a re-evaluation of user entitlements.

   d. OTP invitations by Group. The XenMobile Server administrator selects a group from the list of Active Directory groups present in the XenMobile Server database. User members, both direct and indirect (due to nesting), are retrieved from Active Directory and saved in XenMobile Server database. OTP invitations are sent to the user members identified in the preceding step.

   e. OTP invitations by user. The administrator inputs a search text string within the XenMobile console. XenMobile Server queries Active Directory and returns user records that match the input text string. The administrator then selects the user to send the OTP invitation. XenMobile Server retrieves the user details from Active Directory and updates the same details in the database before sending out the invitation to the user.

Background interactions

One conclusion from inline communication with Active Directory is that group-based interactions are triggered upon select

© 1999-2017 Citrix Systems, Inc. All rights reserved.

changes to the XenMobile Server configuration. When there are no changes to the configuration, it implies that there are no interactions with Active Directory for groups.

This interaction requires background jobs that periodically sync with Active Directory and update relevant changes to the interested groups.

Following are the background jobs that interact with Active Directory.

1. **Group sync job**. The purpose of this job is to query Active Directory, one group at a time, on interested groups for changes to distinguished name or sAMAccountName attributes. The search query to Active Directory uses the objectGUID of the interested group to get the current values of distinguished name and sAMAccountName attributes. Changes in distinguished name or sAMAccountName values for interested groups are updated to the database.

   > **Nota**
   >
   > This job does not update user to group membership information.

2. **Nested group sync job**. This job updates changes in the nesting hierarchy of interested groups. XenMobile Server allows both direct and indirect members of an interested group to get entitlements. The direct membership of the users is updated during user-based inline interactions. Running in the background, this job tracks indirect memberships. Indirect memberships are when a user is a member of a group that is a member of an interested group.

   This job gathers the list of Active Directory groups from XenMobile Server database. These groups are a part of either the deployment group or the RBAC definition. For each group in this list, XenMobile Server gets the members of the group. Members of a group are a list of distinguished names that represent both users and groups. XenMobile Server makes another query back to Active Directory to get only the user members of the interested group. The difference between the two lists gives only the group members for the interested group. Changes in member groups are updated to the database. The same process is repeated for all the groups in the hierarchy.

   Changes to nesting results in processing the affected users for entitlement changes.

3. **Disabled user check**. This job runs only when the XenMobile administrator creates an action to check for disabled users. The job runs within the scope of a group sync job. The job queries Active Directory to check for the disabled status of interested users, one user at a time.

FAQ

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile Deployment

Feb 21, 2018

There's a lot to consider when you're planning a XenMobile deployment. What devices should you choose? How should you manage them? How do you ensure that your network remains secure while still being user friendly? What hardware do you need in place and how do you troubleshoot it? This handbook aims to help answer those questions and more. Throughout the following pages, you'll find use cases and recommendations on topics that cover your deployment concerns, as well as questions you may have never thought to ask.

Keep in mind that a guideline or recommendation might not apply to all environments or use cases. Be sure to set up a test environment before going live with a XenMobile deployment.

The handbook has three main sections:

- **Assess**: Common use cases and questions to consider when planning your deployment.
- **Design & Configure**: Recommendations for designing and configuring your environment
- **Operate & Monitor**: Ensuring the smooth operation of your running environment.

> ## Nota
>
> Some of the sections in this handbook apply to XenMobile on-premises deployments only and some to both on-premises and XenMobile Service (cloud) deployments. A note indicates which deployment applies to the content in each section.

Assess

As with any deployment, assessing your needs should be your first priority. What is your primary need for XenMobile? Do you need to manage every device in your environment or just the apps? Maybe you need to manage both. How secure do you need your XenMobile environment to be? Let's look at common use cases and questions for you to consider when planning your deployment.

- Management modes
- Device requirements
- Security and user experience
- Apps
- User communities
- Email strategy
- XenMobile integration
- Multi-site requirements

Design & Configure

Once you finish assessing your deployment needs, you can make decisions regarding the design and configuration of your environment. Choosing the hardware for your server, setting up policies for apps and devices, and getting users enrolled are just a few of the things you'll need to plan out. This section includes use cases and recommendations for each of these scenarios and more.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

> **Nota**
>
> The following articles in this section apply to XenMobile Service and XenMobile on-premises deployments.

- Integrating with NetScaler and NetScaler Gateway
- SSO and proxy considerations for MDX apps
- Authentication
- Reference architecture for on-premises deployments
- Reference architecture for cloud deployments
- Server properties
- Device and app policies
- User enrollment options
- Tuning XenMobile operations

Operate & Monitor

After your XenMobile environment is up and running, you'll want to monitor it to ensure smooth operation. The monitoring section discusses where you can find the various logs and messages XenMobile and its components generate, as well as how to read those logs. This section also includes a number of common troubleshooting steps you can follow to reduce customer support feedback time.

- App provisioning and deprovisioning
- Dashboard-based operations
- Role-based Access Control and XenMobile support
- Systems monitoring
- Disaster recovery
- Citrix support process

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Management Modes

Feb 21, 2018

For each XenMobile instance (a single server or a cluster of nodes), you can choose whether to manage devices, apps, or both. XenMobile uses the following terms for device and app management modes, sometimes also referred to as deployment modes:

- Mobile device management mode (MDM mode)
- Mobile app management mode (MAM mode)
- MDM+MAM mode (Enterprise mode)

Note: This section applies to XenMobile Service and XenMobile on-premises deployments.

Mobile device management (MDM Mode)

> ### Important
>
> If you configure MDM mode and later change to ENT mode, be sure to use the same (Active Directory) authentication. XenMobile doesn't support changing the authentication mode after user enrollment. For more information, see Upgrade from XenMobile 10 MDM Edition to Enterprise Edition.

With MDM, you can configure, secure, and support mobile devices. MDM enables you to protect devices and data on devices at a system level. You can configure policies, actions, and security functions. For example, you can wipe a device selectively if the device is lost, stolen, or out of compliance. Although app management is not available with MDM mode, you can deliver mobile apps, such as public app store and enterprise apps, in this mode. Following are common use cases for MDM mode:

- MDM is a consideration for corporate-owned devices where device-level management policies or restrictions, such as full wipe, selective wipe, or geo-location are required.
- When customers require management of an actual device, but do not require MDX policies, such as app containerization, controls on app data sharing, or micro VPN.
- When users only need email delivered to their native email clients on their mobile devices, and Exchange ActiveSync or Client Access Server is already externally accessible. In this use case, you can use MDM to configure email delivery.
- When you deploy native enterprise apps (non-MDX), public app store apps, or MDX apps delivered from public stores. Consider that an MDM solution alone might not prevent data leakage of confidential information between apps on the device. Data leakage might occur with copy and paste or Save As operations in Office 365 apps.

Mobile app management (MAM Mode)

MAM protects app data and lets you control app data sharing. MAM also allows for the management of corporate data and resources, separately from personal data. With XenMobile configured for MAM mode, you can use MDX-enabled mobile apps to provide per-app containerization and control. The term MAM mode is also called MAM-only mode. This term distinguishes this mode from a legacy MAM mode.

By leveraging MDX policies, XenMobile provides app-level control over network access (such as micro VPN), app and device interaction, data encryption, and app access.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

MAM mode is often suitable for bring-your-own (BYO) devices because, although the device is unmanaged, corporate data remains protected. MDX has more than 50 MAM-only policies that you can set without needing an MDM control or relying on device passcodes for encryption.

MAM also supports the XenMobile Apps. This support includes secure email delivery to Citrix Secure Mail, data sharing between the secured XenMobile Apps, and secure data storage in ShareFile. For details, see XenMobile Apps.

Note: Worx Mobile Apps are renamed to XenMobile Apps as of the 10.4 release. Most of the individual XenMobile Apps are renamed as well. For details, see About XenMobile Apps.

MAM is often suitable for the following examples:

- You deliver mobile apps, such as MDX apps, managed at the app level.
- You are not required to manage devices at a system level.

MDM+MAM (Enterprise Mode)

MDM+MAM is a hybrid mode, also called Enterprise Mode, which enables all feature sets available in the XenMobile Enterprise Mobility Management (EMM) solution. Configuring XenMobile with MDM+MAM mode enables both MDM and MAM features.

XenMobile lets you specify whether users can choose to opt out of device management or whether you require device management. This flexibility is useful for environments that include a mix of use cases. These environments may or may not require management of a device through MDM policies to access your MAM resources.

MDM+MAM is suitable for the following examples:

- You have a single use case in which both MDM and MAM are required. MDM is required to access your MAM resources.
- Some use cases require MDM while some do not.
- Some use cases require MAM while some do not.

You specify the management mode for XenMobile Server through the Server Mode property. You configure the setting in the XenMobile console. The mode can be MDM, MAM, or ENT (for MDM+MAM).

The XenMobile edition for which you have a license determines the management modes and other features available, as shown in the following table.

XenMobile MDM Edition	**XenMobile Advanced Edition**	**XenMobile Enterprise Edition**
MDM features	MDM features	MDM features
-	MAM features	MAM features
-	MDX Toolkit	MDX Toolkit
Secure Hub	Secure Hub	Secure Hub
-	Secure Mail	Secure Mail

© 1999-2017 Citrix Systems, Inc. All rights reserved.

-	Secure Web	Secure Web
QuickEdit	QuickEdit	QuickEdit
-	Secure Tasks	Secure Tasks
-	-	ShareConnect
-	-	Secure Notes
-	-	ShareFile Enterprise Edition

Device Management and MDM Enrollment

A XenMobile Enterprise environment can include a mixture of use cases, some of which require device management through MDM policies to allow access to MAM resources. Before deploying XenMobile Apps to users, fully assess your use cases and decide whether to require MDM enrollment. If you later decide to change the requirement for MDM enrollment, it is likely that users must re-enroll their devices.

Note: To specify whether you require users to enroll in MDM, use the XenMobile Server property **Enrollment Required** in the XenMobile console (**Settings** > **Server Properties**). That global server property applies to all users and devices for the XenMobile instance. The property applies only when the XenMobile Server Mode is ENT.

Following is a summary of the advantages and disadvantages (along with mitigations) of requiring MDM enrollment in a XenMobile Enterprise mode deployment.

When MDM enrollment is optional

Advantages:

- Users can access MAM resources without putting their devices under MDM management. This option can increase user adoption.
- Ability to secure access to MAM resources to protect enterprise data.
- MDX policies such as **App Passcode** can control app access for each MDX app.
- Configuring NetScaler, XenMobile Server, and per-application time-outs, along with Citrix PIN, provide an extra layer of protection.
- While MDM actions do not apply to the device, some MDX policies are available to deny MAM access. The denial would be based on system settings, such as jailbroken or rooted devices.
- Users can choose whether to enroll their device with MDM during first-time use.

Disadvantages:

- MAM resources are available to devices not enrolled in MDM.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- MDM policies and actions are available only to MDM-enrolled devices.

Mitigation options:

- Have users agree to a company terms and conditions that holds them responsible if they choose to go out of compliance. Have administrators monitor unmanaged devices.
- Manage application access and security by using application timers. Decreased time-out values increase security, but may affect user experience.
- A second XenMobile environment with MDM enrollment required is an option. When considering this option, keep in mind the additional overhead of managing two environments and the additional resources required.

When MDM enrollment is required

Advantages:

- Ability to restrict access to MAM resources only to MDM-managed devices.
- MDM policies and actions can apply to all devices in the environment as desired.
- Users are not able to opt out of enrolling their device.

Disadvantages:

- Requires all users to enroll with MDM.
- Might decrease adoption for users who object to corporate management of their personal devices.

Mitigation options:

- Educate users about what XenMobile actually manages on their devices and what information administrators can access.
- You can use a second XenMobile environment, with a Server Mode of MAM (also called MAM-only mode), for devices that don't need MDM management. When considering this option, keep in mind the additional overhead of managing two environments and the additional resources required.

About MAM and Legacy MAM Modes

XenMobile 10.3.5 introduced a new MAM-only server mode. To distinguish the prior and new MAM modes, the documentation uses these terms. The new mode is called MAM-only or MA, the prior MAM mode is called legacy MAM mode.

MAM-only mode is in effect when the Server Mode property of XenMobile is MAM. Devices register in MAM mode.

Legacy MAM functionality is in effect when the Server Mode property of XenMobile is ENT and users choose to opt out of device management. In that case, devices register in MAM mode. Users who opt out of MDM management continue to receive the legacy MAM functionality.

Note: Previously, setting the Server Mode property to MAM had the same effect as setting it to ENT: Users who opted out of MDM management received the legacy MAM functionality.

The following table summarizes the Server Mode setting to use for a particular license type and desired device mode:

Your licenses are for this	You want devices to register	Set the Server Mode property to

© 1999-2017 Citrix Systems, Inc. All rights reserved.

edition	in this mode	
Enterprise/ Advanced/MDM	MDM mode	MDM
Enterprise/Advanced	MAM mode (also called MAM-only mode)	MAM
Enterprise/Advanced	MDM+MAM mode	ENT (Users who opt out of device management operate under the legacy MAM mode.)

MAM-only mode supports the following features that were previously available only for ENT. These features are not available for Windows Phone.

- **Certificate-based authentication**: MAM-only mode supports certificate-based authentication. Users will experience continued access to their apps even when their Active Directory password expires. If you use certificate-based authentication for MAM devices, you must configure your NetScaler Gateway. By default, in **XenMobile Settings** > **NetScaler Gateway**, Deliver user certificate for authentication is set to **Off**, meaning that user name and password authentication is used. Change that setting to **On** to enable certificate authentication.
- **Self Help Portal**: To enable users to perform their own app lock and app wipe. Those actions apply to all apps on the device. You can configure the App Lock and App Wipe actions in **Configure** > **Actions**.
- **All enrollment modes**: Including High Security, Invitation URL, and Two Factor, configured through **Manage** > **Enrollment Invitations**.
- **Device registration limit for Android and iOS devices**: The Server Property **Number of Devices Per User** has moved to **Configure** > **Enrollment Profiles** and now applies to all server modes.
- **MAM-only APIs**: For MAM-only devices, you can call REST services by using any REST client and the XenMobile REST API to call services that the XenMobile console exposes.
- The MAM-only APIs enable you to:
  - Send an invitation URL and one-time PIN.
  - Issue app lock and wipe on devices.

The following table summarizes the differences between the legacy MAM and MAM-only functionality.

Enrollment Scenarios and Other Features	Legacy MAM (server mode is ENT)	MAM-only mode (server mode is MAM)
Certificate authentication	Not supported.	Supported. For certificate authentication, NetScaler Gateway is required.
Deployment requirement	XenMobile Server does not need to be directly accessible from devices.	XenMobile Server does not need to be directly accessible from devices.
Enrollment option	Use the NetScaler Gateway FQDN or, when using MDM	Use XenMobile Server FQDN.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	FQDN, opt not to enroll.	
Enrollment methods*	User name + Password	User name + Password, High Security, Invitation URL, Invitation URL+PIN, Invitation URL + Password, Two Factor, User name + PIN
App lock and wipe	Supported.	Supported.
Self Help Portal options for app lock and wipe	Not supported.	Supported.
App wipe behavior	Apps remain on the device but are not usable. XenMobile deletes the account on the client only.	Apps remain on the device but are not usable. XenMobile deletes the account on the client only.
Automated actions for MAM-only users.	Event, device property, user property actions are supported. Doesn't support installed app-based automated actions.	Supports event, device property, user property, and some app-based actions, including app wipe and app lock.
Built-in action when an Active Directory user is deleted	Supports app wipe.	Supports app wipe.
Enrollment limit	Supported; configured through an enrollment profile.	Supported; configured through an enrollment profile.
Software inventory	Supported. XenMobile lists apps installed on a device	Not supported.

*__Regarding notifications__: SMTP is the only supported method for sending enrollment invitations.

__Important__: For MAM-only mode, previously enrolled users must re-enroll their devices. Be sure to provide users with the XenMobile Server FQDN they need for enrollment. In MAM-only mode, like the ENT mode, devices enroll using the XenMobile Server FQDN. (In the legacy MAM mode, devices enroll using the NetScaler Gateway FQDN.)

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Device Requirements

Feb 21, 2018

> **Nota**
>
> This section applies to XenMobile Service and XenMobile on-premises deployments.

An important point to consider for any deployment is the device you plan to roll out. On the iOS, Android, and Windows platforms, the options are numerous. For a list of devices that XenMobile supports, see Supported device platforms.

In a bring your own device (BYOD) environment, a mixture of supported platforms is possible. Consider the limitations in the Supported device platform article, however, when informing users about the devices they can enroll. Even if you only allow one or two devices in your environment, XenMobile functions slightly differently on iOS, Android, and Windows devices. Different feature sets are available on each platform.

Also, not all app designs target both tablet and phone form factors. Before you make widespread changes, test the apps to ensure that they fit the device screen you want to roll out.

You can consider enrollment factors as well. Apple and Google offer enterprise enrollment programs. Through the Apple Device Enrollment Program (DEP) and Google Android for Work, you can purchase devices that are preconfigured and ready for employees to use. Even when you don't use these programs, consider whether you want to send invitation links to your users through SMS. You cannot use SMS on tablets.

For more information about enrollment, see User Enrollment Options.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Security and User Experience

Feb 21, 2018

> **Nota**
>
> This section applies to XenMobile Service and XenMobile on-premises deployments.

Security is important to any organization, but you need to strike a balance between security and user experience. On one hand, you may have a very secure environment that is very difficult for users to use. On the other hand, your environment may be so user-friendly that access control is not as strict. The other sections in this virtual handbook cover security features in detail, but the purpose of this article is to give a general overview of the security options available to you and to get you thinking about common security concerns in XenMobile.

Here are some key considerations to keep in mind for each use case:

- Do you want to secure certain apps, the entire device, or both?
- How do you want your users to authenticate their identity? Will you be using LDAP, certificate-based authentication, or a combination of the two?
- How much time should pass before a user's session times out? Keep in mind that there are different time-out values for background services, NetScaler, and for being able to access apps while offline.
- Do you want users to set up a device-level passcode and/or an app-level passcode? How many logon attempts do you want to afford to users? Keep in mind the additional per-app authentication requirements that may be implemented with MAM and how users may perceive them.
- What other restrictions do you want to place on users? Should they be able to access cloud services such as Siri? What can they do with each app you make available to them and what can they not do? Should you deploy corporate WiFi policies to prevent cellular data plans from being eaten up while inside office spaces?

App vs. Device

One of the first things you should consider is whether you should only secure certain apps (mobile app management, or MAM) or if you want to manage the entire device (mobile device management or MDM). Most commonly, if you don't require device-level control, you'll only need to manage mobile apps, especially if your organization supports Bring Your Own Device (BYOD).

With a MAM-only environment, users can access resources made available to them. MAM policies secure and manage the apps themselves.

MDM allows you to secure an entire device, including the ability to take inventory of all the software on a device and prevent enrollment if the device is jailbroken, rooted, or has unsafe software installed. Taking this level of control, however, makes users leery of allowing that much power over their personal devices and may reduce enrollment rates.

It is possible to have MDM required for some devices and not for others, but keep in mind that this choice may involve setting up two dedicated environments, which requires additional resources and upkeep.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Authentication

Authentication is where a great deal of the user experience takes place. If your organization is already running Active Directory, using Active Directory is the simplest way to have your users access the system.

Another big part of the authentication user experience is time-outs. A high security environment may have users log on every time they access the system, but that option may not be ideal for all organizations. For example, having users enter their credentials every time they want to access their email can be very frustrating and may not be necessary.

User Entropy

For added security, you can enable a feature called *user entropy*. Citrix Secure Hub and some other apps often share common data like passwords, PINs, and certificates to ensure everything functions properly. This information is stored in a generic vault within Secure Hub. If you enable user entropy through the **Encrypt Secrets** option, XenMobile creates a new vault called UserEntropy, and moves the information from the generic vault into this new vault. In order for Secure Hub or another app to access the data, users must enter a password or PIN.

Enabling user entropy adds another layer of authentication in a number of places. This means, however, that whenever an app requires access to shared data in the UserEntropy vault—which includes passwords, PINs, and certificates—users need to enter a password or PIN.

You can learn more about user entropy by reading About the MDX Toolkit in the XenMobile documentation. To turn on user entropy, you can find the related settings in the Client properties.

Policies

Both MDX and MDM policies give a great deal of flexibility to organizations, but they can also restrict users. You may want this in some situations, but policies may also make a system unusable. For instance, you may want to block access to cloud applications such as Siri or iCloud that have the potential to send sensitive data where you don't want it going. You can set up a policy to block access to these services, but keep in mind that such a policy may have unintended consequences. The iOS keyboard mic is also reliant on cloud access and you may block access to that feature as well.

Apps

Enterprise Mobility Management (EMM) segments into Mobile Device Management (MDM) and Mobile Application Management (MAM). While MDM enables organizations to secure and control mobile devices, MAM facilitates application delivery and management. With the increasing adoption of BYOD, you can typically implement a MAM solution, such as XenMobile, to assist with application delivery, software licensing, configuration, and application life cycle management. With XenMobile, you can go a step further to secure these apps by configuring specific MAM policies and VPN settings to prevent data leak and other security threats. XenMobile provides organizations with the flexibility to deploy their solution as a MAM-only or a MDM-only environment, or to implement XenMobile as a unified XenMobile Enterprise environment that provides both MDM and MAM functionality within in the same platform.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

In addition to the ability to deliver apps to mobile devices, XenMobile offers app containerization through MDX technology. MDX secures apps through encryption that is separate from device level encryption; you can wipe or lock the app, and the apps are subject to granular policy-based controls. Independent software vendors (ISVs) can apply these controls using the Worx App SDK.

In a corporate environment, users use a variety of mobile apps to aid in their job role. The apps can include apps from the public app store, in-house developed apps, or native apps as well, in some cases. XenMobile categorizes these apps as follows:

Public apps: These apps include free or paid apps available in a public app store, such as iTunes or Google Play. Vendors outside of the organization often make their apps available in public app stores. This option lets their customers download the apps directly from the Internet. You may use numerous public apps in your organization depending on users' needs. Examples of such apps include GoToMeeting, Salesforce, and EpicCare apps.

Citrix does not support downloading app binaries directly from public app stores, and then wrapping them with the MDX Toolkit for enterprise distribution. If you need to wrap third-party applications, work with your app vendor to obtain the app binaries which you can wrap using the MDX Toolkit.

In-house apps: Many organizations have in-house developers who create apps that provide specific functionality and are independently developed and distributed within the organization. In certain cases, some organizations may also have apps that ISVs provide. You can deploy such apps as native apps or you can containerize the apps by using a MAM solution, such as XenMobile. For example, a healthcare organization may create an in-house app that allows physicians to view patient information on mobile devices. An organization can then use the MDX Toolkit to wrap the app in order to secure patient information and enable VPN access to the back-end patient database server.

Web and SaaS apps: These apps include apps accessed from an internal network (web apps) or over a public network (SaaS). XenMobile also allows you to create custom web and SaaS apps using a list of app connectors. These app connectors can facilitate single sign-on (SSO) to existing Web apps. For details, see App connector types. For example, you can use Google Apps SAML for SSO based on Security Assertion Markup Language (SAML) to Google Apps.

XenMobile Apps: These are Citrix-developed apps that are included with the XenMobile license. For details, see About XenMobile Apps. Citrix also offers other business-ready apps that ISVs develop by using the Worx App SDK.

HDX apps: These are Windows-hosted apps that you publish with StoreFront. If you have a Citrix XenApp and XenDesktop environment, you can integrate the apps with XenMobile to make the apps available to the enrolled users.

Depending of the type of mobile apps you plan to deploy and manage with XenMobile, the underlying configuration and architecture will differ. For example, if multiple groups of users with different level of permissions will consume a single app, you may have to create separate delivery groups to deploy two separate versions of the same app. In addition, you must make sure the user group membership is mutually exclusive to avoid policy mismatches on users' devices.

You may also want to manage iOS application licensing by using the Apple Volume Purchase Program (VPP). This option will require you to register for the VPP program and configure XenMobile VPP settings in the XenMobile console to distribute the apps with the VPP licenses. A variety of such use cases makes it important to assess and plan your MAM strategy prior to implementing the XenMobile environment. You can start planning your MAM strategy by defining the following:

Types of apps: List the different types of apps you plan to support and categorize them, such as public, native, XenMobile Apps, Web, in-house, ISV apps, and so on. Also, categorize the apps for different device platforms, such as iOS and Android. This categorization will help with aligning different XenMobile settings that are required for each type of app. For example, certain apps may not qualify for wrapping, or a few apps may require the use of the Worx App SDK to enable special APIs

© 1999-2017 Citrix Systems, Inc. All rights reserved.

for interaction with other apps.

Network requirements: You need to configure apps with specific network access requirements with the appropriate settings. For example, certain apps may need access to your internal network through VPN; some apps may require Internet access to route access via the DMZ. In order to allow such apps to connect to the required network, you have to configure various settings accordingly. Defining per-app network requirements help in finalizing your architectural decisions early on, which will streamline the overall implementation process.

Security requirements: Defining the security requirements that apply to either individual apps or all the apps is critical to ensure that you create the right configurations when you install XenMobile server. Although settings, such as the MDX policies, apply to individual apps, session and authentication settings apply across all apps, and some apps may have specific encryption, containerization, wrapping, encryption, authentication, geo fencing, passcode or data sharing requirements that you will need to outline in advance to simplify your deployment.

Deployment requirements: You may want to use a policy-based deployment to allow only compliant users to download the published apps. For example, you may want certain apps to require that device encryption is enabled or the device is managed, or that the device meets a minimum operating system version. You may also want certain apps to be available only to corporate users. You need to outline such requirements in advance so that you can configure the appropriate deployment rules or actions.

Licensing requirements: You should record app-related licensing requirements. These notes will help you to manage license usage effectively and to decide if you need to configure specific features in XenMobile to facilitate licensing. For example, if you deploy an iOS app, irrespective of whether it is a free or a paid app, Apple enforces licensing requirements on the app by making the users sign into their iTunes account. You can register for Apple VPP to distribute and manage these apps via XenMobile. VPP allows users to download the apps without having to sign into their iTunes account. Additionally, tools, such as Samsung SAFE and Samsung KNOX, have special licensing requirements, which you need to complete prior to deploying those features.

Blacklist/whitelist requirements: There may be apps that you do not want users to install or use at all. Creating a blacklist will define an out of compliance event. You can then set up policies to trigger in case such a thing happens. On the other hand, an app may be acceptable for use but may fall under the blacklist for one reason or another. If this is the case, you can add the app to a whitelist and indicate that the app is acceptable to use but is not required. Also, keep in mind that the apps pre-installed on new devices can include some commonly used apps that are not part of the operating system. This may conflict with your blacklisting strategy.

Use Case

A healthcare organization plans to deploy XenMobile to serve as a MAM solution for their mobile apps. Mobile apps are delivered to corporate and BYOD users. IT decides to deliver and manage the following apps:

- **XenMobile Apps:** iOS and Android apps provided by Citrix.
- **Secure Mail:** Email, calendar, and contact app.
- **Secure Web:** Secure web browser that provides access to the Internet and intranet sites.
- **Secure Notes:** Secure note-taking app with email and calendar integration.
- **ShareFile:** App to access shared data and to share, sync, and edit files.

Public app store:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Secure Hub:** Client used by all mobile devices to communicate with XenMobile. IT pushes security settings, configurations, and mobile apps to mobile devices via the Secure Hub client. Android and iOS devices enroll in XenMobile through Secure Hub.
- **Citrix Receiver:** Mobile app that allows users to open XenApp-hosted applications on mobile devices.
- **GoToMeeting:** An online meeting, desktop sharing, and video conferencing client that lets users meet with other computer users, customers, clients, or colleagues via the Internet in real time.
- **SalesForce1:** Salesforce1 lets users access Salesforce from mobile devices and brings all Chatter, CRM, custom apps, and business processes together in a unified experience for any Salesforce user.
- **RSA SecurID:** Software-based token for two-factor authentication.
- **EpicCare apps:** These apps give healthcare practitioners secure and portable access to patient charts, patient lists, schedules, and messaging.
  - **Haiku:** Mobile app for the iPhone and Android phones.
  - **Canto:** Mobile app for the iPad
  - **Rover:** Mobile apps for iPhone and iPad.

HDX: These apps are delivered via Citrix XenApp.

- **Epic Hyperspace:** Epic client application for electronic health record management.

ISV:

- **Vocera:** HIPAA compliant voice-over IP and messaging mobile app that extends the benefits of Vocera voice technology anytime, anywhere via iPhone and Android smartphones.

In-house apps:

- **HCMail:** App that helps compose encrypted messages, search address books on internal mail servers, and send the encrypted messages to the contacts using an email client.

In-house web apps:

- **PatientRounding:** Web application used to record patient health information by different departments.
- **Outlook Web Access:** Allows the access of email via a web browser.
- **SharePoint:** Used for organization-wide file and data sharing.

The following table lists the basic information required for MAM configuration.

App Name	App Type	MDX Wrapping	iOS	Android
Secure Mail	XenMobile App	No for version 10.4.1 and later	Yes	Yes
Secure Web	XenMobile App	No for version 10.4.1 and later	Yes	Yes
Secure Notes	XenMobile App	No for version 10.4.1 and later	Yes	Yes

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ShareFile	XenMobile App	No for version 10.4.1 and later	Yes	Yes
Secure Hub	Public App	NA	Yes	Yes
Citrix Receiver	Public App	NA	Yes	Yes
GoToMeeting	Public App	NA	Yes	Yes
SalesForce1	Public App	NA	Yes	Yes
RSA SecurID	Public App	NA	Yes	Yes
Epic Haiku	Public App	NA	Yes	Yes
Epic Canto	Public App	NA	Yes	No
Epic Rover	Public App	NA	Yes	No
Epic Hyperspace	HDX App	NA	Yes	Yes
Vocera	ISV App	Yes	Yes	Yes
HCMail	In-House App	Yes	Yes	Yes
PatientRounding	Web App	NA	Yes	Yes
Outlook Web Access	Web App	NA	Yes	Yes
SharePoint	Web App	NA	Yes	Yes

The following tables list specific requirements you can consult when configuring MAM policies in XenMobile.

App Name	VPN Required	Interaction (with apps outside of container)	Interaction (from apps outside of container)	Device Encryption
Secure Mail	Y	Selectively Allowed	Allowed	Not required

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Secure Web	Y	Allowed	Allowed	Not required
Secure Notes	Y	Allowed	Allowed	Not required
ShareFile	Y	Allowed	Allowed	Not required
Secure Hub	Y	N/A	N/A	N/A
Citrix Receiver	Y	N/A	N/A	N/A
GoToMeeting	N	N/A	N/A	N/A
SalesForce1	N	N/A	N/A	N/A
RSA SecurID	N	N/A	N/A	N/A
Epic Haiku	Y	N/A	N/A	N/A
Epic Canto	Y	N/A	N/A	N/A
Epic Rover	Y	N/A	N/A	N/A
Epic Hyperspace	Y	N/A	N/A	N/A
Vocera	Y	Disallowed	Disallowed	Not required
HCMail	Y	Disallowed	Disallowed	Required
PatientRound-ing	Y	N/A	N/A	Required
Outlook Web Access	Y	N/A	N/A	Not required
SharePoint	Y	N/A	N/A	Not required

App Name	Proxy Filtering	Licensing	Geo-fencing	Worx App SDK	Minimum Operating System Version

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Secure Mail	Required	N/A	Selectively Required	N/A	Enforced
Secure Web	Required	N/A	Not required	N/A	Enforced
Secure Notes	Required	N/A	Not required	N/A	Enforced
ShareFile	Required	N/A	Not required	N/A	Enforced
Secure Hub	Not required	VPP	Not required	N/A	Not enforced
Citrix Receiver	Not required	VPP	Not required	N/A	Not enforced
GoToMeeting	Not required	VPP	Not required	N/A	Not enforced
SalesForce1	Not required	VPP	Not required	N/A	Not enforced
RSA SecurID	Not required	VPP	Not required	N/A	Not enforced
Epic Haiku	Not required	VPP	Not required	N/A	Not enforced
Epic Canto	Not required	VPP	Not required	N/A	Not enforced
Epic Rover	Not required	VPP	Not required	N/A	Not enforced
Epic Hyperspace	Not required	N/A	Not required	N/A	Not enforced
Vocera	Required	N/A	Required	Required	Enforced
HCMail	Required	N/A	Required	Required	Enforced
PatientRound-ing	Required	N/A	Not required	N/A	Not enforced
Outlook Web Access	Required	N/A	Not required	N/A	Not enforced
SharePoint	Required	N/A	Not required	N/A	Not enforced

© 1999-2017 Citrix Systems, Inc. All rights reserved.

User Communities

Every organization consists of diverse user communities that operate in different functional roles. These user communities perform different tasks and office functions using various resources that you provide through the users' mobile devices. Users may work from home or in remote offices using mobile devices that you provide, or using their personal mobile devices, which allows them to access tools that are subject to certain security compliance rules.

As more and more user communities start using mobile devices to either simplify or aid in their job role, Enterprise Mobility Management (EMM) becomes critical to prevent data leak and to enforce an organization's security restrictions. In order for efficient and more sophisticated mobile device management, you can categorize your user communities. Doing so simplifies the mapping of users to resources and ensures that the right security policies apply to the right users.

The following example illustrates how the user communities of a healthcare organization are classified for EMM.

Use Case

This example healthcare organization provides technology resources and access to multiple users, including network and affiliate employees and volunteers. The organization has chosen to roll out the EMM solution to non-executive users only.

User roles and functions for this organization can be broken into subgroups including: clinical, non-clinical, and contractors. A selected set of users receive corporate mobile devices, while others can access limited company resources from their personal devices. In order to enforce the right level of security restrictions and prevent data leak, the organization decided that corporate IT manages each enrolled device, Corporate and Bring Your Own Device (BYOD). Additionally, users can only enroll a single device.

The following section provides an overview of the roles and functions of each subgroup:

Clinical:

- Nurses
- Physicians (Doctors, Surgeons, and so on)
- Specialists (Dieticians, phlebotomists, anesthesiologists, radiologists, cardiologists, oncologists, and so on)
- Outside physicians (Non-employee physicians and office workers that work from remote offices)
- Home Health Services (Office and mobile workers performing physician services for patient home visits)
- Research Specialist (Knowledge Workers and Power Users at six Research Institutes performing clinical research to find answers to issues in medicine)
- Education and Training (Nurses, physicians, and specialists in education and training)

Non-Clinical:

- Shared Services (Office workers performing various back office functions including: HR, Payroll, Accounts Payable, Supply Chain Service, and so on)
- Physician Services (Office workers performing a variety of health care management, administrative services, and business process solutions to providers, including: Administrative Services, Analytics and Business Intelligence, Business Systems, Client Services, Finance, Managed Care Administration, Patient Access Solutions, Revenue Cycle Solutions, and so on)
- Support Services (Office workers performing a variety of non-clinical functions including: Benefits Administration, Clinical Integration, Communications, Compensation & Performance Management, Facility & Property Services, HR Technology

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Systems, Information Services, Internal Audit & Process Improvement, and so o.)
- Philanthropic Programs (Office and mobile workers that perform various functions in support of philanthropic programs)

Contractors:

- Manufacturer and vendor partners (Onsite and remotely connected via site-to-site VPN providing various non-clinical support functions)

Based on the preceding information, the organization created the following entities. For more information about delivery groups in XenMobile, see Deploy resources.

Active Directory Organizational Units (OUs) and Groups

For OU **=** XenMobile Resources:

- OU = Clinical; Groups =
  - XM-Nurses
  - XM-Physicians
  - XM-Specialists
  - XM-Outside Physicians
  - XM-Home Health Services
  - XM-Research Specialist
  - XM-Education and Training
- OU = Non-Clinical; Groups =
  - XM-Shared Services
  - XM-Physician Services
  - XM-Support Services
  - XM-Philanthropic Programs

XenMobile Local Users and Groups

For Group= Contractors, Users =

- Vendor1
- Vendor2
- Vendor 3
- ... Vendor 10

XenMobile Delivery Groups

- Clinical-Nurses
- Clinical-Physicians
- Clinical-Specialists
- Clinical-Outside Physicians
- Clinical-Home Health Services
- Clinical-Research Specialist
- Clinical-Education and Training
- Non-Clinical-Shared Services
- Non-Clinical-Physician Services
- Non-Clinical-Support Services

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Non-Clinical-Philanthropic Programs

Delivery Group and User Group mapping

Active Directory Groups	XenMobile Delivery Groups
XM-Nurses	Clinical-Nurses
XM-Physicians	Clinical-Physicians
XM-Specialists	Clinical-Specialists
XM-Outside Physicians	Clinical-Outside Physicians
XM-Home Health Services	Clinical-Home Health Services
XM-Research Specialist	Clinical-Research Specialist
XM-Education and Training	Clinical-Education and Training
XM-Shared Services	Non-Clinical-Shared Services
XM-Physician Services	Non-Clinical-Physician Services
XM-Support Services	Non-Clinical-Support Services
XM-Philanthropic Programs	Non-Clinical-Philanthropic Programs

Delivery Group and Resource mapping

The following tables illustrate the resources assigned to each delivery group in this use case. The first table shows the mobile app assignments; the second table shows the public app, HDX apps, and device management resources.

XenMobile Delivery Groups	Citrix Mobile Apps	Public Mobile Apps	HDX Mobile Apps
Clinical-Nurses	X		
Clinical-Physicians			

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Clinical-Specialists			
Clinical-Outside Physicians	X		
Clinical-Home Health Services	X		
Clinical-Research Specialist	X		
Clinical-Education and Training		X	X
Non-Clinical-Shared Services		X	X
Non-Clinical-Physician Services		X	X
Non-Clinical-Support Services	X	X	X
Non-Clinical-Philanthropic Programs	X	X	X
Contractors	X	X	X

XenMobile Delivery Groups	Public App: RSA SecurID	Public App: EpicCare Haiku	HDX App: Epic Hyperspace	Passcode Policy	Device Restrictions	Automated Actions	WiFi Policy
Clinical-Nurses							X
Clinical-Physicians					X		
Clinical-Specialists							
Clinical-Outside Physicians							
Clinical-Home Health Services							
Clinical-Research Specialist							

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Clinical-Education and Training		X	X				
Non-Clinical-Shared Services		X	X				
Non-Clinical-Physician Services		X	X				
Non-Clinical-Support Services		X	X				

Notes and considerations:

- XenMobile creates a default delivery group named All Users during the initial configuration. If you do not disable this Delivery Group, all Active Directory users will have rights to enroll into XenMobile.
- XenMobile synchronizes Active Directory users and groups on demand using a dynamic connection to the LDAP server.
- If a user is part of a group that is not mapped in XenMobile, that user cannot enroll. Likewise, if a user is a member of multiple groups, XenMobile will only categorize the user as being in the groups mapped to XenMobile.
- In order to make MDM enrollment mandatory, you must set the Enrollment Required option to True in Server Properties in the XenMobile console. For details, see Server Properties.
- You can delete a user group from a XenMobile delivery group by deleting the entry in the SQL Server database, under dbo.userlistgrps.
  Caution: Before you perform this action, create a backup of XenMobile and the database.

About Device Ownership in XenMobile

You can group users according to the owner of a users' device. Device ownership includes corporate-owned devices and user-owned devices, also known as bring your own device (BYOD). You can control how BYOD devices connect to your network in two places in the XenMobile console: in Deployment Rules and through XenMobile server properties on the Settings page. For details about deployment rules, see Configuring Deployment Rules in the XenMobile documentation. For details about server properties, see Server Properties.

By setting server properties, you can require all BYOD users to accept corporate management of their devices before they can access apps, or you can give users access to corporate apps without also managing their devices.

When you set the server setting **wsapi.mdm.required.flag** to **true**, XenMobile manages all BYOD devices, and any user who declines enrollment is denied access to apps. You should consider setting **wsapi.mdm.required.flag** to **true** in environments in which enterprise IT teams need high security along with a positive user experience, which comes from enrolling user devices in XenMobile.

If you leave **wsapi.mdm.required.flag** as **false**, which is the default setting, users can decline enrollment, but may still access apps on their devices through the XenMobile Store. You should consider setting **wsapi.mdm.required.flag** to **false**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

in environments in which privacy, legal, or regulatory constraints require no device management, only enterprise app management.

Users with devices that XenMobile doesn't manage can install apps through the XenMobile Store. Instead of device-level controls, such as selective or full wipe, you control access to the apps through app policies. The policies, depending on the values you set, require the device to check the XenMobile server routinely to confirm that the apps are still allowed to run.

Security Requirements

The amount of security considerations when deploying a XenMobile environment can quickly become overwhelming. There are many interlocking pieces and settings, that you may not know where to begin or what to choose to ensure an acceptable level of protection is available. To make these choices simpler, Citrix provides recommendations for High, Higher, and Highest Security, as outlined in the following table.

Note that security concerns alone should not dictate your deployment mode choice. It is important to also review the requirements of the use case and decide if you can mitigate security concerns before choosing your deployment mode.

High: Using these settings provides an optimal user experience while maintaining a basic level of security acceptable to most organizations.

Higher: These settings strike a stronger balance between security and usability.

Highest: Following these recommendations will provide a very high level of security at the cost of usability and user adoption.

Deployment mode security considerations

The following table specifies the deployment modes for each security level.

High Security	Higher Security	Highest Security
MAM and/or MDM	MDM+MAM	MDM+MAM; plus FIPS

Notes:

- Depending on the use case, a MDM-only or MAM-only deployment could meet security requirements and provide a good user experience.
- If there is no need for app containerization, micro VPN or app specific policies, MDM should be sufficient to manage and secure devices.
- For use cases like BYOD in which all business and security requirements may be satisfied with app containerization only, Citrix recommends MAM-only mode.
- For high security environments (and corporate issued devices), Citrix recommends MDM+MAM to take advantage of all security capabilities available. You should enforce MDM enrollment through a server property in the XenMobile console.
- FIPS options for environments with the highest security needs, such as the federal government.

  If you enable FIPS mode, you must configure SQL Server to encrypt SQL traffic.

NetScaler and NetScaler Gateway security considerations

© 1999-2017 Citrix Systems, Inc. All rights reserved.

The following table specifies the NetScaler and NetScaler Gateway recommendations for each security level.

High Security	Higher Security	Highest Security
NetScaler is recommended. NetScaler Gateway is required for MAM and ENT; recommended for MDM	Standard NetScaler for XenMobile wizard configuration with SSL bridge if XenMobile is in the DMZ; or SSL offload if required to meet security standards when XenMobile server is in the internal network.	SSL Offload with end-to-end encryption

Notes:

- Exposing XenMobile server to the Internet via NAT or existing third-party proxies/load-balancers could be an option for MDM as long as the SSL traffic terminates on XenMobile server, but this choice poses a potential security risk.
- For high security environments, NetScaler with the default XenMobile configuration should meet or exceed security requirements.
- For MDM environments with the highest security needs, SSL termination at the NetScaler provides the ability to inspect traffic at the perimeter, while maintaining end-to-end SSL encryption.
- Options to define SSL/TLS ciphers.
- SSL FIPS NetScaler hardware is also available.
- For more information, see Integrating with NetScaler Gateway and NetScaler.

Enrollment security considerations

The following table specifies the NetScaler and NetScaler Gateway recommendations for each security level.

High Security	Higher Security	Highest Security
Active Directory Group membership only. All users Delivery Group disabled.	Invitation only enrollment mode. Active Directory Group membership only. All users Delivery Group disabled	Enrollment mode tied to Device ID. Active Directory Group membership only. All users Delivery Group disabled

Notes:

- Citrix generally recommends that you restrict enrollment to users in predefined Active Directory groups only. This requires disabling the built-in All users Delivery Group.
- You can use enrollment invitations to restrict enrollment to users with an invitation only.
- You can use one-time PIN (OTP) enrollment invites as a two-factor solution and to control the number of devices a user may enroll.
- For environments with the highest security requirements, you can tie enrollment invitations to a device by SN/UDID/EMEI. A two-factor option is also available to require Active Directory password and OTP. (Note that OTP is not currently an option for Windows devices.)

Device PIN security considerations

The following table specifies the device PIN recommendations for each security level.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

High Security	Higher Security	Highest Security
Recommended. High security is required for device-level encryption. May be enforced with MDM. Can be set as required for MAM-only by using an MDX policy.	Enforced by using MDM and/or MDX policy.	Enforced by using MDM and MDX policy. MDM Complex passcode policy.

Notes:

- Citrix recommends the use of a device PIN.
- You can enforce a device PIN via an MDM policy.
- You can use an MDX policy to make a device PIN a requirement for using managed apps; for example, for BYOD use cases.
- Citrix recommends combining the MDM and MDX policy options for increased security in MDM+MAM environments.
- For environments with the highest security requirements, you can configure complex passcode policies and enforced them with MDM. You can configure automatic actions to notify administrators or issue selective/full device wipes when a device doesn't comply with a passcode policy.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Apps

Feb 21, 2018

Enterprise Mobility Management (EMM) segments into Mobile Device Management (MDM) and Mobile Application Management (MAM). While MDM enables organizations to secure and control mobile devices, MAM facilitates application delivery and management. With the increasing adoption of BYOD, you can typically implement a MAM solution, such as XenMobile, to assist with application delivery, software licensing, configuration, and application life cycle management.

With XenMobile, you can go a step further to secure these apps by configuring specific MAM policies and VPN settings to prevent data leak and other security threats. XenMobile provides organizations with the flexibility to deploy their solution as a MAM-only or a MDM-only environment, or to implement XenMobile as a unified XenMobile Enterprise environment that provides both MDM and MAM functionality within in the same platform.

In addition to the ability to deliver apps to mobile devices, XenMobile offers app containerization through MDX technology. MDX secures apps through encryption that is separate from device level encryption; you can wipe or lock the app, and the apps are subject to granular policy-based controls. Independent software vendors (ISVs) can apply these controls using the Worx App SDK.

In a corporate environment, users use a variety of mobile apps to aid in their job role. The apps can include apps from the public app store, in-house developed apps, or native apps as well, in some cases. XenMobile categorizes these apps as follows:

- **Public apps**: These apps include free or paid apps available in a public app store, such as iTunes or Google Play. Vendors outside of the organization often make their apps available in public app stores. This option lets their customers download the apps directly from the Internet. You may use numerous public apps in your organization depending on users' needs. Examples of such apps include GoToMeeting, Salesforce, and EpicCare apps.

  > Citrix does not support downloading app binaries directly from public app stores, and then wrapping them with the MDX Toolkit for enterprise distribution. If you need to wrap third-party applications, work with your app vendor to obtain the app binaries which you can wrap using the MDX Toolkit.

- **In-house apps**: Many organizations have in-house developers who create apps that provide specific functionality and are independently developed and distributed within the organization. In certain cases, some organizations may also have apps that ISVs provide. You can deploy such apps as native apps or you can containerize the apps by using a MAM solution, such as XenMobile. For example, a healthcare organization may create an in-house app that allows physicians to view patient information on mobile devices. An organization can then use the MDX Toolkit to wrap the app in order to secure patient information and enable VPN access to the back-end patient database server.
- **Web and SaaS apps**: These apps include apps accessed from an internal network (web apps) or over a public network (SaaS). XenMobile also allows you to create custom web and SaaS apps using a list of app connectors. These app connectors can facilitate single sign-on (SSO) to existing Web apps. For details, see App connector types. For example, you can use Google Apps SAML for SSO based on Security Assertion Markup Language (SAML) to Google Apps.
- **Citrix XenMobile Apps**: These are Citrix-developed apps that are included with the XenMobile license. For details, see About XenMobile Apps. Citrix also offers other business-ready apps that ISVs develop by using the Worx App SDK.
- **HDX apps**: These are Windows-hosted apps that you publish with StoreFront. If you have a Citrix XenApp and XenDesktop environment, you can integrate the apps with XenMobile to make the apps available to the enrolled users.

Depending of the type of mobile apps you plan to deploy and manage with XenMobile, the underlying configuration and architecture will differ. For example, if multiple groups of users with different level of permissions will consume a single app, you may have to create separate delivery groups to deploy two separate versions of the same app. In addition, you must make sure the user group membership is mutually exclusive to avoid policy mismatches on users' devices.

You may also want to manage iOS application licensing by using the Apple Volume Purchase Program (VPP). This option will require you to register for the VPP program and configure XenMobile VPP settings in the XenMobile console to distribute the apps with the VPP licenses. A variety of such use cases makes it important to assess and plan your MAM strategy prior to implementing the XenMobile environment. You can start planning your MAM strategy by defining the following:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- **Types of apps** - List the different types of apps you plan to support and categorize them, such as public, native, Worx, Web, in-house, ISV apps, and so on. Also, categorize the apps for different device platforms, such as iOS and Android. This categorization will help with aligning different XenMobile settings that are required for each type of app. For example, certain apps may not qualify for wrapping, or a few apps may require the use of the Worx App SDK to enable special APIs for interaction with other apps.
- **Network requirements** - You need to configure apps with specific network access requirements with the appropriate settings. For example, certain apps may need access to your internal network through VPN; some apps may require Internet access to route access via the DMZ. In order to allow such apps to connect to the required network, you have to configure various settings accordingly. Defining per-app network requirements help in finalizing your architectural decisions early on, which will streamline the overall implementation process.
- **Security requirements** - Defining the security requirements that apply to either individual apps or all the apps is critical to ensure that you create the right configurations when you install XenMobile server. Although settings, such as the MDX policies, apply to individual apps, session and authentication settings apply across all apps, and some apps may have specific encryption, containerization, wrapping, encryption, authentication, geo fencing, passcode or data sharing requirements that you will need to outline in advance to simplify your deployment. For details on security in XenMobile, see Security and User Experience.
- **Deployment requirements** - You may want to use a policy-based deployment to allow only compliant users to download the published apps. For example, you may want certain apps to require that device encryption is enabled or the device is managed, or that the device meets a minimum operating system version. You may also want certain apps to be available only to corporate users. You need to outline such requirements in advance so that you can configure the appropriate deployment rules or actions.
- **Licensing requirements** - You should record app-related licensing requirements. These notes will help you to manage license usage effectively and to decide if you need to configure specific features in XenMobile to facilitate licensing. For example, if you deploy an iOS app, irrespective of whether it is a free or a paid app, Apple enforces licensing requirements on the app by making the users sign into their iTunes account. You can register for Apple VPP to distribute and manage these apps via XenMobile. VPP allows users to download the apps without having to sign into their iTunes account. Additionally, tools, such as Samsung SAFE and Samsung KNOX, have special licensing requirements, which you need to complete prior to deploying those features.
- **Blacklist/whitelist requirements** - There may be apps that you do not want users to install or use at all. Creating a blacklist will define an out of compliance event. You can then set up policies to trigger in case such a thing happens. On the other hand, an app may be acceptable for use but may fall under the blacklist for one reason or another. If this is the case, you can add the app to a whitelist and indicate that the app is acceptable to use but is not required. Also, keep in mind that the apps pre-installed on new devices can include some commonly used apps that are not part of the operating system. This may conflict with your blacklisting strategy.

Use Case

A healthcare organization plans to deploy XenMobile to serve as a MAM solution for their mobile apps. Mobile apps are delivered to corporate and BYOD users. IT decides to deliver and manage the following apps:

XenMobile Apps: iOS and Android apps provided by Citrix. For details, see XenMobile Apps.

Citrix Secure Hub: Client used by all mobile devices to communicate with XenMobile. IT pushes security settings, configurations, and mobile apps to mobile devices via Secure Hub. Android and iOS devices enroll in XenMobile through Secure Hub.

Citrix Receiver: Mobile app that allows users to open XenApp-hosted applications on mobile devices.

GoToMeeting: An online meeting, desktop sharing, and video conferencing client that lets users meet with other computer users, customers, clients, or colleagues via the Internet in real time.

SalesForce1: Salesforce1 lets users access Salesforce from mobile devices and brings all Chatter, CRM, custom apps, and business processes together in a unified experience for any Salesforce user.

RSA SecurID: Software-based token for two-factor authentication.

EpicCare apps: These apps give healthcare practitioners secure and portable access to patient charts, patient lists, schedules, and messaging.

Haiku: Mobile app for the iPhone and Android phones.

Canto: Mobile app for the iPad

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Rover: Mobile apps for iPhone and iPad.

HDX: These apps are delivered via Citrix XenApp.

- **Epic Hyperspace:** Epic client application for electronic health record management.

ISV:

- **Vocera:** HIPAA compliant voice-over IP and messaging mobile app that extends the benefits of Vocera voice technology anytime, anywhere via iPhone and Android smartphones.

In-house apps:

- **HCMail:** App that helps compose encrypted messages, search address books on internal mail servers, and send the encrypted messages to the contacts using an email client.

In-house web apps:

- **PatientRounding:** Web application used to record patient health information by different departments.
- **Outlook Web Access:** Allows the access of email via a web browser.
- **SharePoint:** Used for organization-wide file and data sharing.

The following table lists the basic information required for MAM configuration.

App Name	App Type	MDX Wrapping	iOS	Android
Secure Mail	XenMobile App	No for version 10.4.1 and later	Yes	Yes
Secure Web	XenMobile App	No for version 10.4.1 and later	Yes	Yes
Secure Notes	XenMobile App	No for version 10.4.1 and later	Yes	Yes
ShareFile	XenMobile App	No for version 10.4.1 and later	Yes	Yes
Secure Hub	Public App	N/A	Yes	Yes
Citrix Receiver	Public App	N/A	Yes	Yes
GoToMeeting	Public App	N/A	Yes	Yes
SalesForce1	Public App	N/A	Yes	Yes
RSA SecurID	Public App	N/A	Yes	Yes
Epic Haiku	Public App	N/A	Yes	Yes
Epic Canto	Public App	N/A	Yes	No

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Epic Rover	Public App	N/A	Yes	No
Epic Hyperspace	HDX App	N/A	Yes	Yes
Vocera	ISV App	Yes	Yes	Yes
HCMail	In-House App	Yes	Yes	Yes
PatientRounding	Web App	N/A	Yes	Yes
Outlook Web Access	Web App	N/A	Yes	Yes
SharePoint	Web App	N/A	Yes	Yes

The following table lists specific requirements you can consult configuring MAM policies in XenMobile.

App Name	VPN Required	Interaction (with apps outside of container)	Interaction (from apps outside of container)	Device Encryption	Proxy Filtering	Licensing	Geo-fencing	Worx App SDK	Minimum Operating System Version
Secure Mail	Y	Selectively Allowed	Allowed	Not required	Required	N/A	Selectively Required	N/A	Enforced
Secure Web	Y	Allowed	Allowed	Not required	Required	N/A	Not required	N/A	Enforced
Secure Notes	Y	Allowed	Allowed	Not required	Required	N/A	Not required	N/A	Enforced
ShareFile	Y	Allowed	Allowed	Not required	Required	N/A	Not required	N/A	Enforced
Secure Hub	Y	N/A	N/A	N/A	Not required	VPP	Not required	N/A	Not enforced
Citrix Receiver	Y	N/A	N/A	N/A	Not required	VPP	Not required	N/A	Not enforced
GoToMeeting	N	N/A	N/A	N/A	Not required	VPP	Not required	N/A	Not enforced
SalesForce1	N	N/A	N/A	N/A	Not	VPP	Not	N/A	Not

© 1999-2017 Citrix Systems, Inc. All rights reserved.

					required		required		enforced
RSA SecurID	N	N/A	N/A	N/A	Not required	VPP	Not required	N/A	Not enforced
Epic Haiku	Y	N/A	N/A	N/A	Not required	VPP	Not required	N/A	Not enforced
Epic Canto	Y	N/A	N/A	N/A	Not required	VPP	Not required	N/A	Not enforced
Epic Rover	Y	N/A	N/A	N/A	Not required	VPP	Not required	N/A	Not enforced
Epic Hyperspace	Y	N/A	N/A	N/A	Not required	N/A	Not required	N/A	Not enforced
Vocera	Y	Disallowed	Disallowed	Not required	Required	N/A	Required	Required	Enforced
HCMail	Y	Disallowed	Disallowed	Required	Required	N/A	Required	Required	Enforced
PatientRound-ing	Y	N/A	N/A	Required	Required	N/A	Not required	N/A	Not enforced
Outlook Web Access	Y	N/A	N/A	Not required	Required	N/A	Not required	N/A	Not enforced
SharePoint	Y	N/A	N/A	Not required	Required	N/A	Not required	N/A	Not enforced

© 1999-2017 Citrix Systems, Inc. All rights reserved.

User Communities

Feb 21, 2018

Every organization consists of diverse user communities that operate in different functional roles. These user communities perform different tasks and office functions using various resources that you provide through user mobile devices. Users might work from home or in remote offices using mobile devices that you provide. Or, users might use personal mobile devices, which allows them to access tools that are subject to certain security compliance rules.

With more user communities using mobile devices, Enterprise Mobility Management (EMM) becomes critical to prevent data leak and to enforce organizational security restrictions. In order for efficient and more sophisticated mobile device management, you can categorize your user communities. Doing so simplifies the mapping of users to resources and ensures that the right security policies apply to the right users.

Categorizing user communities can include use of the following components:

- Active Directory Organizational Units (OUs) and Groups

  Users added to specific Active Directory security groups can receive policies and resources such as apps. Removing users from the Active Directory security groups removes access to previously allowed XenMobile resources.

- XenMobile local users and groups

  For users who don't have an account in Active Directory, you can create the users as local XenMobile users. You can add local users to delivery groups and provision resources to them in the same manner as Active Directory users.

- XenMobile delivery groups

  If multiple groups of users with different level of permissions are to consume a single app, you might need to create separate delivery groups. With separate delivery groups, you can deploy two separate versions of the same app.

- Delivery group and user group mapping

  Delivery group to Active Directory group mappings can be either one-to-one, or one-to-many. Assign base policies and apps to a one-to-many delivery group mapping. Assign function-specific policies and apps to one-to-one delivery group mappings.

- Delivery Group and Resource Mapping of Apps

  Assign specific apps to each delivery group.

- Delivery Group and Resource Mapping of MDM Resources

  Assign apps and specific device management resources to each delivery group. For example, configure a delivery group with any mix of the following: Types of apps (public, HDX, and so on), specific apps per app type, and resources such as device policies and automated actions.

The following example illustrates how the user communities of a healthcare organization are classified for EMM.

Use Case

This example healthcare organization provides technology resources and access to multiple users, including network and affiliate employees and volunteers. The organization has chosen to roll out the EMM solution to non-executive users only.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

You can divide user roles and functions for this organization into subgroups including: clinical, non-clinical, and contractors. A selected set of users receive corporate mobile devices, while others can access limited company resources from their personal devices (BYOD). To enforce the appropriate level of security restrictions and prevent data leak, the organization decided that corporate IT manages each enrolled device. Also, users can only enroll a single device.

The following section provides an overview of the roles and functions of each subgroup:

Clinical:

- Nurses
- Physicians (Doctors, Surgeons, and so on)
- Specialists (Dieticians, phlebotomists, anesthesiologists, radiologists, cardiologists, oncologists, and so on)
- Outside physicians (Non-employee physicians and office workers that work from remote offices)
- Home Health Services (Office and mobile workers performing physician services for patient home visits)
- Research Specialist (Knowledge Workers and Power Users at six Research Institutes performing clinical research to find answers to issues in medicine)
- Education and Training (Nurses, physicians, and specialists in education and training)

Non-Clinical:

- Shared Services (Office workers performing various back-office functions including: HR, Payroll, Accounts Payable, Supply Chain Service, and so on)
- Physician Services (Office workers performing various health care management, administrative services, and business process solutions to providers, including: Administrative Services, Analytics and Business Intelligence, Business Systems, Client Services, Finance, Managed Care Administration, Patient Access Solutions, Revenue Cycle Solutions, and so on)
- Support Services (Office workers performing various non-clinical functions including: Benefits Administration, Clinical Integration, Communications, Compensation & Performance Management, Facility & Property Services, HR Technology Systems, Information Services, Internal Audit & Process Improvement, and so on.)
- Philanthropic Programs (Office and mobile workers that perform various functions in support of philanthropic programs)

Contractors:

- Manufacturer and vendor partners (Onsite and remotely connected via site-to-site VPN providing various non-clinical support functions)

Based on the preceding information, the organization created the following entities. For more information about delivery groups in XenMobile, see Deploy resources in the XenMobile product documentation.

Active Directory Organizational Units (OUs) and Groups

For OU = XenMobile Resources

- OU = Clinical; Groups =
  - XM-Nurses
  - XM-Physicians
  - XM-Specialists
  - XM-Outside Physicians
  - XM-Home Health Services
  - XM-Research Specialist
  - XM-Education and Training
- OU = Non-Clinical; Groups =

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- XM-Shared Services
- XM-Physician Services
- XM-Support Services
- XM-Philanthropic Programs

XenMobile Local Users and Groups

For Group= Contractors, Users =

- Vendor1
- Vendor2
- Vendor 3
- ... Vendor 10

XenMobile Delivery Groups

- Clinical-Nurses
- Clinical-Physicians
- Clinical-Specialists
- Clinical-Outside Physicians
- Clinical-Home Health Services
- Clinical-Research Specialist
- Clinical-Education and Training
- Non-Clinical-Shared Services
- Non-Clinical-Physician Services
- Non-Clinical-Support Services
- Non-Clinical-Philanthropic Programs

Delivery Group and User Group mapping

Active Directory Groups	**XenMobile Delivery Groups**
XM-Nurses	Clinical-Nurses
XM-Physicians	Clinical-Physicians
XM-Specialists	Clinical-Specialists
XM-Outside Physicians	Clinical-Outside Physicians
XM-Home Health Services	Clinical-Home Health Services
XM-Research Specialist	Clinical-Research Specialist
XM-Education and Training	Clinical-Education and Training

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XM-Shared Services	Non-Clinical-Shared Services
XM-Physician Services	Non-Clinical-Physician Services
XM-Support Services	Non-Clinical-Support Services
XM-Philanthropic Programs	Non-Clinical-Philanthropic Programs

Delivery Group and Resource Mapping of Apps

	Secure Mail	**Secure Web**	**Secure Notes**	**ShareFile**	**Receiver**	**SalesForce1**	**RSA SecurID**	**EpicCare Haiku**	**Epic Hyperspace**
Clinical-Nurses	X	X	X	X					
Clinical-Physicians									
Clinical-Specialists									
Clinical-Outside Physicians	X		X	X					
Clinical-Home Health Services	X		X	X					
Clinical-Research Specialist	X		X	X					
Clinical-Education and Training								X	X
Non-Clinical-Shared								X	X

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Services									
Non-Clinical-Physician Services								X	X
Non-Clinical-Support Services	X		X	X				X	X
Non-Clinical-Philanthropic Programs	X		X	X				X	X
Contractors	X		X	X	X	X		X	X

Delivery Group and Resource Mapping of MDM Resources

	MDM: Passcode policy	**MDM: Device Restrictions**	**MDM: Automated Actions**	**MDM: WiFi policy**
Clinical-Nurses				X
Clinical-Physicians		X		
Clinical-Specialists				
Clinical-Outside Physicians				
Clinical-Home Health Services				
Clinical-Research Specialist				
Clinical-Education and Training				
Non-Clinical-Shared Services				
Non-Clinical-Physician Services				

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Non-Clinical-Support Services				
Non-Clinical-Philanthropic Programs				
Contractors				X

Notes and considerations:

- XenMobile creates a default delivery group named All Users during the initial configuration. If you do not disable this Delivery Group, all Active Directory users have rights to enroll into XenMobile.
- XenMobile synchronizes Active Directory users and groups on demand using a dynamic connection to the LDAP server.
- If a user is part of a group that is not mapped in XenMobile, that user cannot enroll. Likewise, if a user is a member of multiple groups, XenMobile only categorizes the user as being in the groups mapped to XenMobile.
- To make MDM enrollment mandatory, set the **Enrollment Required** option to **True** in **Server Properties** in the XenMobile console. For details, see Server Properties.
- To delete a user group from a XenMobile delivery group, delete the entry in the SQL Server database, under dbo.userlistgrps.
  Caution: Before you perform this action, create a backup of XenMobile and the database.

About Device Ownership in XenMobile

You can group users according to the owner of a user device. Device ownership includes corporate-owned devices and user-owned devices, also known as bring your own device (BYOD). You can control how BYOD devices connect to your network in two places in the XenMobile console: in Deployment Rules and through XenMobile server properties on the **Settings** page. For details about deployment rules, see Deploy resources in the XenMobile documentation. For details about server properties, see Server Properties in this handbook.

By setting server properties, you can require all BYOD users to accept corporate management of their devices before they can access apps. Or, you can give users access to corporate apps without also managing their devices.

When you set the server property **wsapi.mdm.required.flag** to **true**, XenMobile manages all BYOD devices, and any user who declines enrollment is denied access to apps. Consider setting **wsapi.mdm.required.flag** to **true** in environments in which enterprise IT teams need high security plus a positive user experience during enrolling.

If you leave **wsapi.mdm.required.flag** as **false**, which is the default setting, users can decline enrollment. However, they can access apps on their devices through the XenMobile Store. Consider setting **wsapi.mdm.required.flag** to **false** in environments in which privacy, legal, or regulatory constraints require no device management, only enterprise app management.

Users with devices that XenMobile doesn't manage can install apps through the XenMobile Store. Instead of device-level controls, such as selective or full wipe, you control access to the apps through app policies. Some policy settings require the device to check the XenMobile server routinely to confirm that the apps are still allowed to run.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Email Strategy

Feb 21, 2018

Secure access to email from mobile devices is one of the main drivers behind any organization's mobility management initiative. Deciding on the proper email strategy is often a key component of any XenMobile design. XenMobile offers several options to accommodate different use cases, based on security, user experience, and integration requirements. This article covers the typical design decision process and considerations for choosing the right solution, from client selection to mail traffic flow.

Choosing Your Email Clients

Client selection is generally at the top of the list for the overall email strategy design. You can choose from several clients: Citrix Secure Mail, native mail that is included with a particular mobile platform operating system, or other third-party clients available through the public app stores. Depending on your needs, you can possibly support the user communities with a single (standard) client or you may need to use a combination of clients.

The following table outlines design considerations for the different client options available:

Topic	**Secure Mail**	**Native (for example, iOS Mail)**	**Third-party mail (for example, TouchDown)**
Minimum XenMobile Edition	Advanced	MDM	MDM
Configuration	Exchange account profiles configured via an MDX policy.	Exchange account profiles configured via an MDM policy. Android support is limited to: SAFE/KNOX, HTC, and Android for Work. All other clients are considered third-party clients.	Generally requires manual configuration by the user. Configuration of Exchange account profiles via an MDM policy for TouchDown only.
Security	Secure by design, providing the highest security. Uses MDX policies with added data encryption levels. Secure Mail is a fully managed app via an MDX policy. Added layer of authentication with Citrix PIN.	Based on vendor/app feature set. Provides higher security. Uses device encryption settings (with no security via MDX policies). Relies on device-level authentication for access to the app.	Based on vendor/app feature set. Provides high security.
Integration	Allows interaction with managed (MDX) apps by default. Open web URLs with Citrix Secure Web. Save files to	Can only interact with other unmanaged (non-MDX) apps by default.	Can only interact with other unmanaged (non-MDX) apps by default.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

	and attach files from ShareFile. Directly join and dial in to GoToMeeting.		
Deployment/ Licensing	You can push Secure Mail through MDM, directly from public app stores. Included with XenMobile Advanced and Enterprise licensing.	Client app included with platform operating system. No additional licensing requirements.	Can push via MDM, as an enterprise app or directly from public app stores. Associated licensing model/costs based on app vendor.
Support	Single vendor support for the client and EMM solution (Citrix). Embedded support contact info in Secure Hub/app debug logging capabilities. One client to support.	Vendor defined support (Apple/Google). May need to support different clients based on device platform.	Vendor-defined support. One client to support, assuming that the third-party client is supported on all managed device platforms.

Mail traffic flow and filtering considerations

This section discusses the three main scenarios and design considerations regarding the flow of mail (ActiveSync) traffic in the context of XenMobile.

Scenario 1: Exposed Exchange

Environments that support external clients commonly have Exchange ActiveSync services exposed to the internet. Mobile ActiveSync clients connect through this externally facing path through a reverse proxy (for example, NetScaler) or through an edge server. This option is required for the use of native or third-party mail clients, making these clients the popular choice for this scenario. Although not a common practice, you can also use the Secure Mail client in this scenario. By doing so, you benefit from the security features offered by the use of MDX policies and management of the app.

Scenario 2: Tunneled via NetScaler (micro VPN and STA)

This scenario is the default when using the Secure Mail client, due to its micro VPN capabilities. In this case, the Secure Mail client establishes a secure connection to ActiveSync via NetScaler Gateway. In essence, you can consider Secure Mail to be the client connecting directly to ActiveSync from the internal network. Citrix customers often standardize on Secure Mail as the mobile ActiveSync client of choice. That decision is part of an initiative to avoid exposing ActiveSync services to the internet on an exposed Exchange Server, as described in the first scenario.

Only managed (MDX wrapped) apps can use the micro VPN function. Therefore, this scenario does not apply to native clients. Even though it may be possible to wrap third-party clients with the MDX Toolkit, this practice is not common. The use of device-level VPN clients to allow tunneled access for native or third-party clients has proven to be cumbersome and not a viable solution.

Scenario 3: Cloud-hosted Exchange services

Cloud-hosted Exchange services, such as Microsoft Office 365, are becoming more popular. In the context of XenMobile, this scenario may be treated in the same way as the first scenario, because the ActiveSync service is also exposed to the

© 1999-2017 Citrix Systems, Inc. All rights reserved.

internet. In this case, cloud service provider requirements dictate client choices. The choices generally include support for most ActiveSync clients, such as Secure Mail and other native or third-party clients.

XenMobile can add value in three areas for this scenario:

- Client wrapping with MDX policies and app management with Secure Mail
- Client configuration with the use of an MDM policy on supported clients (native, such as TouchDown)
- ActiveSync filtering options with the use of XenMobile Mail Manager

Mail traffic filtering considerations

As with most services exposed to the internet, you must secure the path and provide filtering for authorized access. The XenMobile solution includes two components designed specifically to provide ActiveSync filtering capabilities for native and third-party clients: XenMobile NetScaler Connector and XenMobile Mail Manager.

XenMobile NetScaler Connector

The use of XenMobile NetScaler Connector provides ActiveSync filtering at the perimeter, by using NetScaler as a proxy for ActiveSync traffic. As a result, the filtering component sits in the path of mail traffic flow, intercepting mail as it enters or leaves the environment. XenMobile NetScaler Connector acts an intermediary between NetScaler and the XenMobile Server. When a device communicates with Exchange through the ActiveSync virtual server on the NetScaler, NetScaler performs an HTTP callout to the XenMobile NetScaler Connector service. That service then checks the device status with XenMobile. Based on the status of the device, XenMobile NetScaler Connector replies to NetScaler to either allow or deny the connection. You may also configure static rules to filter access based on user, agent, and device type or ID.

This setup allows Exchange ActiveSync services to be exposed to the internet with an added layer of security to prevent unauthorized access. Design considerations include the following:

- Windows Server: The XenMobile NetScaler Connector component requires a Windows Server.
- Filtering rule set: XenMobile NetScaler Connector is designed for filtering based on device state and information, rather than user information. Although you may configure static rules to filter by user ID, no options exist for filtering based on Active Directory group membership, for example. If there is a requirement for Active Directory group filtering, you can use XenMobile Mail Manager instead.
- NetScaler scalability: Given the requirement to proxy ActiveSync traffic via NetScaler: Proper sizing of the NetScaler instance is critical to support the added workload of all ActiveSync SSL connections.
- NetScaler Integrated Caching: The XenMobile NetScaler Connector configuration on the NetScaler uses the Integrated Caching function to cache responses from XenMobile NetScaler Connector. As a result of that configuration, NetScaler doesn't need to issue a request to XenMobile NetScaler Connector for every ActiveSync transaction in a given session. That configuration is also critical for adequate performance and scale. Integrated Caching is available with the NetScaler Platinum Edition or you can license the feature separately for Enterprise Editions.
- Custom filtering policies: You might need to create custom NetScaler policies to restrict certain ActiveSync clients outside of the standard native mobile clients. This configuration requires knowledge on ActiveSync HTTP requests and NetScaler responder policy creation.
- Secure Mail clients: Secure Mail has micro VPN capabilities which eliminate the need for filtering at the perimeter. The Secure Mail client would generally be treated as an internal (trusted) ActiveSync client when connected through the NetScaler Gateway. If support for both native and third-party (with XenMobile NetScaler Connector) and Secure Mail clients is required: Citrix recommends that Secure Mail traffic does not flow via the NetScaler virtual server used for XenMobile NetScaler Connector. You can accomplish this traffic flow via DNS and keep the XenMobile NetScaler Connector policy from affecting Secure Mail clients.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

For a diagram of XenMobile NetScaler Connector in a XenMobile deployment, see Reference Architecture for On-Premises Deployments.

XenMobile Mail Manager

XenMobile Mail Manager is a XenMobile component that provides ActiveSync filtering at the Exchange service level. As a result, filtering only occurs once the mail reaches the exchange service, rather than when it enters the XenMobile environment. Mail Manager uses PowerShell to query Exchange ActiveSync for device partnership information and control access through device quarantine actions. Those action take devices in and out of quarantine based on XenMobile Mail Manager rule criteria. Similar to XenMobile NetScaler Connector, XenMobile Mail Manager checks the device status with XenMobile to filter access based on device compliance. You may also configure static rules to filter access based on device type or ID, agent version, and Active Directory group membership.

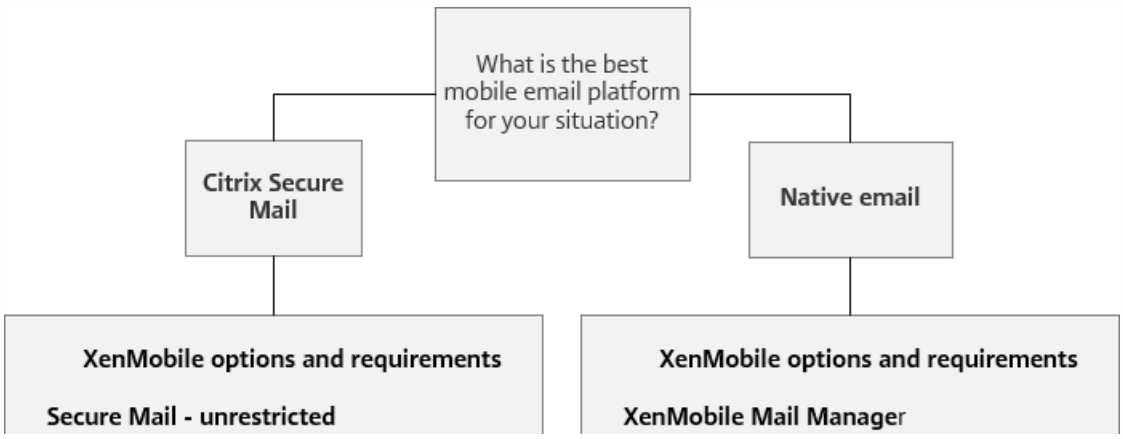
This solution does not require the use of NetScaler. You can deploy XenMobile Mail Manager without changes routing for the existing ActiveSync traffic. Design considerations include:

- Windows Server: The XenMobile Mail Manager component requires you to deploy Windows Server.
- Filtering rule set: Just like XenMobile NetScaler Connector, XenMobile Mail Manager includes filtering rules to evaluate device state. Additionally, XenMobile Mail Manager also supports static rules to filter based on Active Directory group membership.
- Exchange integration: XenMobile Mail Manager requires direct access to the Exchange Client Access Server (CAS) hosting the ActiveSync role and control over device quarantine actions. This requirement might present a challenge depending on the environment architecture and security posture. It is critical that you evaluate this technical requirement up front.
- Other ActiveSync clients: Because XenMobile Mail Manager is filtering at the ActiveSync service level, consider other ActiveSync clients outside the XenMobile environment. You can configure XenMobile Mail Manager static rules to avoid unintended impact to other ActiveSync clients.
- Extended Exchange functions: Through direct integration with Exchange ActiveSync, XenMobile Mail Manager provides the ability for XenMobile to perform an Exchange ActiveSync wipe on a mobile device. XenMobile Mail Manager also allows XenMobile to access information about Blackberry devices and to perform other control operations.

For a diagram of XenMobile Mail Manager in a XenMobile deployment, see Reference Architecture for On-Premises Deployments.

Email Platform Decision Tree

The following figure helps you distinguish the pros and cons between using native email or Secure Mail solutions in your XenMobile deployment. Each choice allows for associated XenMobile options and requirements to enable server, network, and database access. The pros and cons include details on security, policy, and user interface considerations.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Email traffic bypasses NetScaler Gateway
- MDX policies secure the app
- Exchange ActiveSync/CAS is exposed to the Internet

Secure Mail – tunneled to the internal network
- Email traffic leverages NetScaler Gateway
- Uses XenMobile as a STA server (optional)
- MDX policies secure the app

- Requires existing path to Exchange ActiveSync/Client Access Server (CAS)
- Requires XenMobile Mail Manager server

XenMobile NetScaler Connector
- Can leverage internal-only Exchange access
- Requires XenMobile NetScaler Connector server and NetScaler

Native ActiveSync
- Existing Exchange ActiveSync/CAS infrastructure
- Exchange ActiveSync/CAS must be externally accessible

Pros for each option

WorxMail – unrestricted
- Better battery life on device
- Secured with MDX policies
- Supports client certificate authentication for security
- Integration with Citrix Secure apps
- Standard user interface across platforms

WorxMail – tunneled to the internal network
- Best battery life on device (with STA)
- Secured with MDX policies
- Support for client certificates
- Full control of app access
- Integration with Citrix Secure apps
- Exchange ActiveSync/CAS is not exposed to the Internet
- Standard user interface across platforms

Pros for each option

XenMobile Mail Manager
- Ability to use native mail client
- Supports Microsoft Office 365
- Blacklist/whitelist access policies
- Can perform Exchange ActiveSync/CAS commands (full wipe, reset password, and so on)
- Can connect to BlackBerry BES and perform basic device controls
- Can filter Exchange ActiveSync access to non-MDM managed devices

XenMobile NetScaler Connector
- Ability to use devices-native mail client
- Rule-based allow and deny modes
- Uses NetScaler as a reverse proxy
- More secure than XenMobile Mail Manager and external access to Exchange ActiveSync/CAS

Native ActiveSync
- Ability to use native mail client
- Basic Exchange ActiveSync/CAS device management capabilities

Cons for each option

Secure Mail – unrestricted
- Exchange ActiveSync/CAS exposed to the Internet
- Must account for user adoption

Secure Mail – tunneled to the internal network
- Additional overhead to the NetScaler
- Must account for user adoption
- User must have an active session with Secure Hub to receive email updates
- Highly secure

Cons for each option

XenMobile Mail Manager
- Mail client not secured with MDX policies
- Requires Windows Server
- Requires PowerShell to schedule/invoke policies
- Limited control over devices
- May require Touchdown for some Android devices

XenMobile NetScaler Connector
- Mail client not secured with MDX policies
- Requires Windows Server

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Requires user education for adoption

- Requires NetScaler
- May require Touchdown for some Android devices

Native ActiveSync

- Mail client not secured with MDX policies
- Exposed Exchange ActiveSync/CAS
- Limited control over which devices/users can connect

© 1999-2017 Citrix Systems, Inc. All rights reserved.

XenMobile Integration

Feb 21, 2018

This article covers what to consider when planning how XenMobile is to integrate with your existing network and solutions. For example, if you're already using NetScaler for XenApp and XenDesktop:

- Should you use the existing NetScaler instance or a new, dedicated instance?
- Do you want to integrate with XenMobile the HDX apps that are published using StoreFront?
- Do you plan to use ShareFile with XenMobile?
- Do you have a Network Access Control solution that you want to integrate into XenMobile?
- Do you deploy web proxies for all outbound traffic from your network?

NetScaler and NetScaler Gateway

NetScaler Gateway required mandatory for XenMobile ENT and MAM modes. NetScaler Gateway provides a micro VPN path for access to all corporate resources and provides strong multi-factor authentication support. NetScaler load balancing is required for all XenMobile Server device modes:

- If you have multiple XenMobile Servers.
- Or, if the XenMobile Server is inside your DMZ or internal network (and therefore traffic flows from devices to NetScaler to XenMobile).

You can use existing NetScaler instances or set up new ones for XenMobile. The following sections note the advantages and disadvantages of using existing or new, dedicated NetScaler instances.

Shared NetScaler MPX with a NetScaler Gateway VIP created for XenMobile

Advantages:

- Uses a common NetScaler instance for all Citrix remote connections: XenApp, full VPN, and clientless VPN.
- Uses the existing NetScaler configurations, such as for certificate authentication and for accessing services like DNS, LDAP, and NTP.
- Uses a single NetScaler platform license.

Disadvantages:

- It is more difficult to plan for scale when you handle two very different use cases on the same NetScaler.
- Sometimes you need a specific NetScaler version for a XenApp use case. That same version might have known issues for XenMobile. Or XenMobile might have known issues for the NetScaler version.
- If a NetScaler Gateway exists, you cannot run the NetScaler for XenMobile wizard a second time to create the NetScaler configuration for XenMobile.
- Except when Platinum licenses are used for NetScaler Gateway 11.1 or later: User access licenses installed on NetScaler and required for VPN connectivity are pooled. Because those licenses are available to all NetScaler virtual servers, services other than XenMobile can potentially consume them.

Dedicated NetScaler VPX/MPX instance

Advantages:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix recommends using a dedicated instance of NetScaler.

- Easier to plan for scale and separates XenMobile traffic from a NetScaler instance that might already be resource constrained.
- Avoids issues when XenMobile and XenApp need different NetScaler software versions. The recommendation generally is to use the latest compatible NetScaler version and build for XenMobile.
- Allows XenMobile configuration of NetScaler through the built-in NetScaler for XenMobile wizard.
- Virtual and physical separation of services.
- Except when Platinum licenses are used for NetScaler Gateway 11.1 or later: The user access licenses required for XenMobile are only available to XenMobile services on the NetScaler.

Disadvantages:

- Requires setup of extra services on NetScaler to support XenMobile configuration.
- Requires another NetScaler platform license. License each NetScaler instance for NetScaler Gateway.

For information about what to consider when integrating NetScaler and NetScaler Gateway with each XenMobile server mode, see Integrating with NetScaler and NetScaler Gateway.

StoreFront

If you have a Citrix XenApp and XenDesktop environment, you can integrate HDX applications with XenMobile using StoreFront. When you integrate HDX apps with XenMobile:

- The apps are available to users who are enrolled with XenMobile.
- The apps display in the XenMobile Store along with other mobile apps.
- XenMobile uses the legacy PNAgent (services) site on StoreFront.
- When Citrix Receiver is installed on a device, HDX apps start using the Receiver.

StoreFront has a limitation of one services site per StoreFront instance. Suppose that you have multiple stores and want to segment it from other production usage. In that case, Citrix generally recommends that you consider a new StoreFront Instance and services site for XenMobile.

Considerations include:

- Are there any different authentication requirements for StoreFront? The StoreFront services site requires Active Directory credentials for logon. Customers only using certificate-based authentication cannot enumerate applications through XenMobile using the same NetScaler Gateway.
- Use the same store or create a new one?
- Use the same or a different StoreFront server?

The following sections note the advantages and disadvantages of using separate or combined storefronts for Receiver and XenMobile Apps.

Integrate your existing StoreFront instance with XenMobile server

Advantages:

- Same store: No additional configuration of StoreFront is required for XenMobile, assuming that you use the same NetScaler VIP for HDX access. Suppose that you choose to use the same store and want to direct Receiver access to a new NetScaler VIP. In that case, add the appropriate NetScaler Gateway configuration to StoreFront.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Same StoreFront server: Uses the existing StoreFront installation and configuration.

Disadvantages:

- Same store: Any reconfiguration of StoreFront to support XenApp and XenDesktop workloads may adversely affect XenMobile as well.
- Same StoreFront server: In large environments, consider the additional load from XenMobile usage of PNAgent for app enumeration and start-up.

Use a new, dedicated StoreFront instance for integration with XenMobile server

Advantages:

- New store: Any configuration changes of the StoreFront store for XenMobile should not affect existing XenApp and XenDesktop workloads.
- New StoreFront server: Server configuration changes should not affect XenApp and XenDesktop workflow. Additionally, load outside of XenMobile usage of PNAgent for app enumeration and launch should not affect scalability.

Disadvantages:

- New store: StoreFront store configuration.
- New StoreFront server: Requires new StoreFront installation and configuration.

For more information, see XenApp and XenDesktop through Citrix Secure Hub in the XenMobile documentation.

ShareFile

ShareFile enables users to access and sync all of their data from any device. With ShareFile, users can securely share data with people both inside and outside the organization. If you integrate ShareFile with XenMobile Advanced Edition or Enterprise Edition, XenMobile can provide ShareFile with:

- Single sign-on authentication for XenMobile App users.
- Active Directory-based user account provisioning.
- Comprehensive access control policies.

Mobile users can benefit from the full ShareFile Enterprise feature set.
Alternatively, you can configure XenMobile to integrate only with StorageZone Connectors. Through StorageZone Connectors, ShareFile provides access to:

- Ddocuments and folders
- Network file shares
- In SharePoint sites: Site collections and document libraries.

Connected file shares can include the same network home drives used in Citrix XenDesktop and XenApp environments. You use the XenMobile console to configure the integration with ShareFile Enterprise or StorageZones Connectors. For more information, see ShareFile use with XenMobile.

The following sections note the questions to ask when making design decisions for ShareFile.

Integrate with ShareFile Enterprise or only StorageZone Connectors

Questions to ask:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Do you need to store data in Citrix-managed StorageZones?
- Do you want to provide users with file sharing and sync capabilities?
- Do you want to enable users to access files on the ShareFile website? Or to access Office 365 content and Personal Cloud connectors from mobile devices?

Design decision:

- If the answer to any of those questions is "yes," integrate with ShareFile Enterprise.
- An integration with only StorageZone Connectors gives iOS users secure mobile access to existing on-premises storage repositories, such as SharePoint sites and network file shares. In this configuration, you don't set up a ShareFile subdomain, provision users to ShareFile, or host ShareFile data. Using StorageZones Connectors with XenMobile complies with security restrictions against leaking user information outside of the corporate network.

ShareFile StorageZones Controller server location

Questions to ask:

- Do you require on-premises storage or features such as StorageZone Connectors?
- If using on-premises features of ShareFile, where will the ShareFile StorageZones Controllers sit in the network?

Design decision:

- Determine whether to locate the StorageZones Controller servers in the ShareFile cloud, in your on-premises single-tenant storage system, or in supported third-party cloud storage.
- StorageZones Controllers require some internet access to communicate with the Citrix ShareFile Control Plane. You can connect in several ways, including direct access, NAT/PAT configurations, or proxy configurations.

StorageZone Connectors

Questions to ask:

- What are the CIFS share paths?
- What are the SharePoint URLs?

Design decision:

- Determine if on-premises StorageZones Controllers are required to access those locations.
- Due to StorageZone Connector communication with internal resources such as file repositories, CIFS shares, and SharePoint: Citrix recommends that StorageZones Controllers reside in the internal network behind DMZ firewalls and fronted by NetScaler.

SAML integration with XenMobile Enterprise

Questions to ask:

- Is Active Directory authentication required for ShareFile?
- Does first time use of the ShareFile app for XenMobile require SSO?
- Is there a standard IdP in your current environment?
- How many domains are required to use SAML?
- Are there multiple email aliases for Active Directory users?

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Are there any Active Directory domain migrations in progress or scheduled soon?

Design decision:

XenMobile Enterprise environments may choose to use SAML as the authentication mechanism for ShareFile. The authentication options are:

- Use XenMobile server as the Identity Provider (IdP) for SAML

  This option can provide excellent user experience and automate ShareFile account creation, as well as enable mobile app SSO features.

- XenMobile server is enhanced for this process: It does not require the synchronization of Active Directory.
- Use the ShareFile User Management Tool for user provisioning.
- Use a supported third-party vendor as the IdP for SAML

If you have an existing and supported IdP and don't require mobile app SSO capabilities, this option might be the best fit for you. This option also requires the use of the ShareFile User Management Tool for account provisioning.

Using third-party IdP solutions such as ADFS may also provide SSO capabilities on the Windows client side. Be sure to evaluate use cases before choosing your ShareFile SAML IdP.

Additionally, to satisfy both use cases, you can Configure and ADFS and XenMobile as a Dual IdP.

Mobile apps

Questions to ask:

- Which ShareFile mobile app do you plan to use (public, MDM, MDX)?

Design decision:

- You distribute XenMobile apps from the Apple App Store and Google Play Store. With that public app store distribution, you obtain wrapped apps from the Citrix downloads page.
- If security is low and you don't require containerization, the public ShareFile application may not be suitable. In an MDM-only environment, you can deliver the MDM version of the ShareFile app using XenMobile in MDM mode.
- For more information, see Apps and Citrix ShareFile for XenMobile.

Security, policies, and access control

Questions to ask:

- What restrictions do you require for desktop, web, and mobile users?
- What standard access control settings do you want for users?
- What file retention policy do you plan to use?

Design decision:

- ShareFile lets you manage employee permissions and device security. For information, see Employee Permissions and Managing Devices and Apps.
- Some ShareFile device security settings and MDX policies control the same features. In those cases, XenMobile policies take precedence, followed by the ShareFile device security settings. Examples: If you disable external apps in ShareFile,

© 1999-2017 Citrix Systems, Inc. All rights reserved.

but enable them in XenMobile, the external apps get disabled in ShareFile. You can configure the apps so that XenMobile doesn't require a PIN/passcode, but the ShareFile app requires a PIN/passcode.

Standard vs. Restricted StorageZones

Questions to ask:

- Do you require Restricted StorageZones?

Design decision:

- A standard StorageZone is intended for non-sensitive data and enables employees to share data with non-employees. This option supports workflows that involve sharing data outside of your domain.
- A restricted StorageZone protects sensitive data: Only authenticated domain users can access the data stored in the zone.

Web Proxies

The most likely scenario for routing XenMobile traffic through an HTTP(S)/SOCKS proxy is as follows: When the subnet that the XenMobile server resides in doesn't have outbound Internet access to the required Apple, Google, or Microsoft IP addresses. You can specify proxy server settings in XenMobile to route all Internet traffic to the proxy server. For more information, see Enable proxy servers.

The following table describes the advantages and disadvantages of the most common proxy used with XenMobile.

Option	Advantages	Disadvantages
Use an HTTP(S)/ SOCKS Proxy with XenMobile server.	In cases where policies do not permit outbound Internet connections from the XenMobile server subnet: You can configure an HTTP(S) or SOCKS proxy to provide Internet connectivity.	If the proxy server fails, APNs (iOS) or Google Cloud Messaging (Android) connectivity breaks. As a result, device notifications fail for all iOS and Android devices.
Use an HTTP(S) Proxy with Secure Web.	You can monitor HTTP/HTTPS traffic to ensure that Internet activity complies with your organization's standards.	This configuration requires all Secure Web Internet traffic to tunnel back to the corporate network before they are sent back out to the Internet. If your Internet connection constrains browsing: This configuration could affect Internet browsing performance.

Your NetScaler session profile configuration for split tunneling affects the traffic as follows.

When NetScaler Split Tunneling is **off**:

- If the MDX **Network access** policy is **Tunneled to the internal network:** All traffic is forced to use the micro VPN or clientless VPN (cVPN) tunnel back to the NetScaler Gateway.
- Configure NetScaler traffic policies/profiles for the proxy server and bind them to the NetScaler Gateway VIP.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Important: Be sure to exclude Secure Hub cVPN traffic from the proxy.

- For more information, see XenMobile Secure Hub Traffic Through Proxy Server in Secure Browse Mode.

When **NetScaler Split Tunneling** is **on**:

- When apps are configured with the MDX **Network access** policy set to **Tunneled to the internal network**: The apps first attempt to get the web resource directly. If the web resource is not publicly available, those apps then fall back to NetScaler Gateway.
- Configure NetScaler traffic policies and profiles for the proxy server. Then, bind those policies and profiles to the NetScaler Gateway VIP.

  Important: Be sure to exclude Secure Hub cVPN traffic from the proxy.

Your NetScaler session profile configuration for **Split DNS** (under **Client experience**) functions similarly to Split Tunneling.

With **Split DNS** enabled and set to **Both**:

- The client first attempts to resolve the FQDN locally and then falls back to NetScaler for DNS resolution during failure.

With **Split DNS** set to **Remote**:

- DNS resolution occurs only on NetScaler.

With **Split DNS** set to **Local**:

- The client attempts to resolve the FQDN locally. NetScaler isn't used for DNS resolution.

Access Control

Enterprises can now manage mobile devices inside and outside of networks. Enterprise Mobility Management solutions such as XenMobile are great at providing security and controls for mobile devices, independent of location. However, when coupled with a Network Access Control (NAC) solution, you can add QoS and more fine-grained control to devices that are internal to your network. That combination enables you to extend the XenMobile device security assessment through your NAC solution. Your NAC solution then can use the XenMobile security assessment to facilitate and handle authentication decisions. Citrix has validated NAC integration with XenMobile for Cisco Identity Services Engine (ISE) or ForeScout. Citrix doesn't guarantee integration for other NAC solutions.

Advantages of a NAC solution integration with XenMobile include the following:

- Better security, compliance, and control for all endpoints on an enterprise network.
- A NAC solution can:
  - Detect devices at the instant they attempt to connect to your network.
  - Query XenMobile for device attributes.
  - Then use that information to determine whether to allow, block, limit, or redirect those devices. Those decisions depend on the security policies you choose to enforce.
- A NAC solution provides IT administrators with a view of unmanaged and non-compliant devices.

For a description of the NAC compliance filters supported by XenMobile, see Network Access Control.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Multi-Site Requirements

Feb 21, 2018

You can architect and configure XenMobile deployments that include multiple sites for high availability and disaster recovery. This article provides an overview of the high availability and disaster recovered models used in XenMobile deployments.

High Availability

- For XenMobile cluster nodes, NetScaler handles the load balancing.
- XenMobile server nodes operate in an active/active configuration.
- Additional XenMobile server nodes are added to a high availability cluster as capacity is required. One node can handle up to approximately 8,500 user devices (see Scalability and performance for additional detail).
- Citrix recommends configuring "n+1" XenMobile servers: one server for every 8,500 user devices and one extra server for redundancy.
- Citrix recommends high availability for all NetScaler instances wherever possible to allow the configurations to sync with a second NetScaler.
- The standard NetScaler high availability pair operates in an active/passive configuration.

A typical high availability XenMobile deployment typically includes:

- Two NetScaler instances (VPX or MPX). If the NetScaler SDX platform is used, high availability should also be considered.
- Two or more XenMobile servers configured with the same database settings.

Disaster Recovery

You can configure XenMobile for disaster recovery across two data centers with one active data center and one passive data center. NetScaler and Global Server Load Balancing (GSLB) are used to create an active/active data path so that the user experience is that of an active/active setup.

For disaster recovery, a XenMobile deployment includes:

- Two data centers; each contains one or more NetScaler instances, XenMobile servers, and SQL Server databases.
- A GSLB server to direct traffic to the data centers. The GSLB server is configured for both the XenMobile enrollment URL and NetScaler Gateway URL handling traffic to the site.
- When you use the NetScaler for XenMobile wizard to configure NetScaler Gateway, by default, the GSLB is not enabled to resolve traffic to the XenMobile enrollment server and traffic to the NetScaler Gateway, en route to the MAM load-balancing server; as a result, additional steps are required. For more information on preparing for and implementing these steps, see Disaster Recovery.
- Clustered SQL Servers of Always On Availability Groups.
- Latency between the XenMobile servers and SQL Server must be less than 5 ms.

> ### Nota
>
> The disaster recovery methods described in this handbook provide only automated disaster recovery for the access layer. You must manually start all XenMobile server nodes and the SQL Server database at the failover site before devices can connect the XenMobile server.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Integrating with NetScaler Gateway and NetScaler

Feb 21, 2018

When integrated with XenMobile, NetScaler Gateway provides an authentication mechanism for remote device access to the internal network for MAM devices. The integration enables XenMobile Apps to connect to corporate servers in the intranet through a micro VPN created from the apps on the mobile device to NetScaler Gateway.

NetScaler load balancing is required for all XenMobile server device modes if you have multiple XenMobile servers or if the XenMobile server is inside your DMZ or internal network (and therefore traffic flows from devices to NetScaler to XenMobile).

Integration requirements for XenMobile Server modes

The integration requirements for NetScaler Gateway and NetScaler differ based on the XenMobile Server modes: MAM, MDM, and ENT.

MAM

With XenMobile Server in MAM mode:

- **NetScaler Gateway** is required. NetScaler Gateway provides a micro VPN path for access to all corporate resources and provides strong multi-factor authentication support.
- **NetScaler** is recommended for load balancing.

  Citrix recommends that you deploy XenMobile in a high availability configuration, which requires a load balancer in front of XenMobile. For details, see About MAM and Legacy MAM Modes.

MDM

With XenMobile Server in MDM mode:

- NetScaler Gateway isn't required. For MDM deployments, Citrix recommends NetScaler Gateway for mobile device VPN.
- NetScaler is recommended for security and load balancing.

  Citrix recommends that you deploy a NetScaler appliance in front of XenMobile server, for security and load balancing. For standard deployments with XenMobile server in the DMZ, Citrix recommends the NetScaler for XenMobile wizard along with XenMobile server load balancing in SSL Bridge mode. You can also consider SSL Offload for deployments where XenMobile server resides in the internal network rather than the DMZ and/or where security requires such configurations.

  While you might consider exposing XenMobile server to the Internet via NAT or existing third-party proxies or load-balancers for MDM provided that the SSL traffic terminates on XenMobile server (SSL Bridge), Citrix does not recommend that approach due to the potential security risk.

  For high security environments, NetScaler with the default XenMobile configuration should meet or exceed security requirements.

  For MDM environments with the highest security needs, SSL termination at the NetScaler provides the ability to inspect traffic at the perimeter, while maintaining end-to-end SSL encryption. For more information, see Security Requirements. NetScaler offers options to define SSL/TLS ciphers and SSL FIPS NetScaler hardware.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ENT (MAM+MDM)

With XenMobile Server in ENT mode:

- NetScaler Gateway is required. NetScaler Gateway provides a micro VPN path for access to all corporate resources and provides strong multi-factor authentication support.

  When the XenMobile server mode is ENT and a user opts out of MDM enrollment, the device operates in the legacy MAM mode. In the legacy MAM mode, devices enroll using the NetScaler Gateway FQDN. For details, see About MAM and Legacy MAM Modes.

- NetScaler is recommended for load balancing. For more information, see the NetScaler point above under "MDM."

> **Important**
>
> Be aware that for initial enrollment, the traffic from user devices authenticates on the XenMobile server whether you configure load balancing virtual servers to SSL Offload or SSL Bridge.

Design Decisions

The following sections summarize the many design decisions to consider when planning a NetScaler Gateway integration with XenMobile.

Licensing and edition

Decision detail:

- What edition of NetScaler will you use?
- Have you applied Platform licenses to NetScaler?
- If you require MAM functionality, have you applied the NetScaler Universal Access Licenses?

Design guidance:

Ensure that you apply the proper licenses to the NetScaler Gateway. If you are using XenMobile NetScaler Connector, integrated caching might be required; therefore, you must ensure that the appropriate NetScaler Edition is in place.

The license requirements to enable NetScaler features are as follows.

- XenMobile MDM load balancing requires a NetScaler standard platform license at a minimum.
- ShareFile load balancing with StorageZones Controller requires a NetScaler standard platform license at a minimum.
- The XenMobile Enterprise edition includes the required NetScaler Gateway Universal licenses for MAM.
- Exchange load balancing requires a NetScaler Platinum platform license or a NetScaler Enterprise platform license with the addition of an Integrated Caching license.

NetScaler version for XenMobile

Decision detail:

- What version is the NetScaler running in the XenMobile environment?

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Will a separate instance be required?

Design guidance:

Citrix recommends using a dedicated instance of NetScaler for your NetScaler Gateway virtual server. Be sure that the minimum required NetScaler version and build is in use for the XenMobile environment. It is usually best to use the latest compatible NetScaler version and build for XenMobile. If upgrading NetScaler Gateway would affect your existing environments, a second dedicated instance for XenMobile might be appropriate.

If you plan to share a NetScaler instance for XenMobile and other apps that use VPN connections, be sure that you have enough VPN licenses for both. Keep in mind that XenMobile test and production environments cannot share a NetScaler instance.

Certificates

Decision detail:

- Do you require a higher degree of security for enrollments and access to the XenMobile environment?
- Is LDAP not an option?

Design guidance:

The default configuration for XenMobile is user name and password authentication. To add another layer of security for enrollment and access to XenMobile environment, consider using certificate-based authentication. You can use certificates with LDAP for two-factor authentication, providing a higher degree of security without needing an RSA server.

If you don't allow LDAP and use smart cards or similar methods, configuring certificates allows you to represent a smart card to XenMobile. Users then enroll using a unique PIN that XenMobile generates for them. After a user has access, XenMobile creates and deploys the certificate subsequently used to authenticate to the XenMobile environment.

XenMobile supports Certificate Revocation List (CRL) only for a third party Certificate Authority. If you have a Microsoft CA configured, XenMobile uses NetScaler to manage revocation. When you configure client certificate-based authentication, consider whether you need to configure the NetScaler Certificate Revocation List (CRL) setting, **Enable CRL Auto Refresh**. This step ensures that the user of a device in MAM-only mode can't authenticate using an existing certificate on the device; XenMobile re-issues a new certificate, because it doesn't restrict a user from generating a user certificate if one is revoked. This setting increases the security of PKI entities when the CRL checks for expired PKI entities.

Networking topology

Decision detail:

- What NetScaler topology is required?

Design guidance:

Citrix recommends using a NetScaler instance for XenMobile. However, if you don't want traffic going from the inside network out to the DMZ, you might consider setting up an additional instance of NetScaler, so that you're using one NetScaler instance for internal users and one for external users. Be aware that when users switch between the internal and external networks, DNS record caching can result in an increase in logon prompts in Secure Hub.

Note that XenMobile does not currently support NetScaler Gateway double hop.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Dedicated or shared NetScaler Gateway VIPs

Decision detail:

- Do you currently use NetScaler Gateway for XenApp and XenDesktop?
- Will XenMobile leverage the same NetScaler Gateway as XenApp and XenDesktop?
- What are the authentication requirements for both traffic flows?

Design guidance:

When your Citrix environment includes XenMobile, plus XenApp and XenDesktop, you can use the same NetScaler instance and NetScaler Gateway virtual server for both. Due to potential versioning conflicts and environment isolation, a dedicated NetScaler instance and NetScaler Gateway are recommend for each XenMobile environment. However, if a dedicated NetScaler instance is not an option, Citrix recommends using a dedicated NetScaler Gateway vServer rather than a vServer shared between XenMobile and XenApp and XenDesktop, to separate the traffic flows for Secure Hub.

If you use LDAP authentication, Receiver and Secure Hub can authenticate to the same NetScaler Gateway with no issues. If you use certificate-based authentication, XenMobile pushes a certificate in the MDX container and Secure Hub uses the certificate to authenticate with NetScaler Gateway. Receiver is separate from Secure Hub and can't use the same certificate as Secure Hub to authenticate to the same NetScaler Gateway.

You might consider this work around, which allows you to use the same FQDN for two NetScaler Gateway VIPs. You can create two NetScaler Gateway VIPs with the same IP address, but the one for Secure Hub uses the standard 443 port and the one for XenApp and XenDesktop (which deploy Receiver) uses port 444. Then, one FQDN resolves to the same IP address. For this work around, you might need to configure StoreFront to return an ICA file for port 444, instead of the default, port 443. This workaround doesn't require users to enter a port number.

NetScaler Gateway time-outs

Decision detail:

- How do you want to configure the NetScaler Gateway time-outs for XenMobile traffic?

Design guidance:

NetScaler Gateway includes the settings Session time-out and Forced time-out. For details, see Recommended Configurations in this handbook. Keep in mind that there are different time-out values for background services, NetScaler, and for accessing applications while offline.

XenMobile load balancer IP address for MAM

Decision detail:

- Are you using internal or external IP addresses for VIPs?

Design guidance:

In environments where you can use public IP addresses for NetScaler Gateway VIPs, assigning the XenMobile load balancing VIP and address in this manner will cause enrollment failures.

Ensure that the load balancing VIP uses an internal IP to avoid enrollment failures in this scenario. This virtual IP address

© 1999-2017 Citrix Systems, Inc. All rights reserved.

must follow the RFC 1918 standard of private IP addresses. If you use a non-private IP address for this virtual server, NetScaler will not be able to contact the XenMobile server successfully during the authentication process. For details, see http://support.citrix.com/article/CTX200430.

MDM load balancing mechanism

Decision detail:

- How will the XenMobile servers be load balanced by NetScaler Gateway?

Design guidance:

Use SSL Bridge if XenMobile is in the DMZ. Use SSL Offload, if required to meet security standards, when XenMobile server is in the internal network.

- When you load balance XenMobile server with NetScaler VIPs in SSL Bridge mode, Internet traffic flows directly to XenMobile server, where connections terminate. SSL Bridge mode is the simplest mode to set up and troubleshoot.
- When you load balance XenMobile server with NetScaler VIPs in SSL Offload mode, Internet traffic flows directly to NetScaler, where connections terminate. NetScaler then establishes new sessions from NetScaler to XenMobile server. SSL Offload mode involves additional complexity during setup and troubleshooting.

Service port for MDM load balancing with SSL Offload

Decision detail:

- If you will use SSL Offload mode for Load Balancing, What port will the back-end service use?

Design guidance:

For SSL Offload, choose port 80 or 8443 as follows:

- Leverage port 80 back to XenMobile server, for true offloading.
- End-to-end encryption, that is, re-encryption of traffic, isn't supported. For details, see the Citrix support article, Supported Architectures Between NetScaler and XenMobile Server.

Enrollment FQDN

Decision detail:

- What will be the FQDN for enrollment and XenMobile instance/load balancing VIP?

Design guidance:

Initial configuration of the first XenMobile server in a cluster requires that you enter the XenMobile server FQDN. That FQDN must match your MDM VIP URL and your Internal MAM LB VIP URL. (An internal NetScaler address record resolves the MAM LB VIP.) For details, see "Enrollment FQDN for each deployment type" later in this article.

In addition, you must use the same certificate as the XenMobile SSL listener certificate, Internal MAM LB VIP certificate, and MDM VIP certificate (if using SSL Offload for MDM VIP).

Important: After you configure the enrollment FQDN, you cannot change it. A new enrollment FQDN will require a new SQL Server database and XenMobile server re-build.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Secure Web traffic

Decision detail:

- Will you restrict Secure Web to internal web browsing only?
- Will you enable Secure Web for both internal and external web browsing?

Design guidance:

If you will use Secure Web for internal web browsing only, NetScaler Gateway configuration is straightforward, assuming that Secure Web can reach all internal sites by default; you might need to configure firewalls and proxy servers.

If you will use Secure Web for both internal and external browsing, you must enable the SNIP to have outbound internet access. Because IT generally views enrolled devices (using the MDX container) as an extension of the corporate network, IT typically wants Secure Web connections to come back to NetScaler, go through a proxy server, and then go out to Internet. By default, Secure Web access tunnels to the internal network, which means that Secure Web uses a per-application VPN tunnel back to the internal network for all network access and NetScaler uses split tunnel settings.

For a discussion of Secure Web connections, see Configuring User Connections in the XenMobile Apps documentation.

Push Notifications for Secure Mail

Decision detail:

- Will you use push notifications?

Design guidance for iOS:

If your NetScaler Gateway configuration includes Secure Ticket Authority (STA) and split tunneling is off, NetScaler Gateway must allow traffic from Secure Mail to the Citrix listener service URLs specified in Push Notifications for Secure Mail for iOS.

Design guidance for Android:

As an alternative to the MDX policy, Active poll period, you can use Google Cloud Messaging (GCM) to control how and when Android devices need to connect to XenMobile. With GCM configured, any security action or deploy command triggers a push notification to Secure Hub to prompt the user to reconnect to the XenMobile server.

HDX STAs

Decision detail:

- What STAs to use if you will integrate HDX application access?

Design guidance:

HDX STAs must match the STAs in StoreFront and must be valid for the XenApp/XenDesktop farm.

ShareFile

Decision detail:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Will you use ShareFile StorageZone Controllers in the environment?
- What ShareFile VIP URL will you use?

Design guidance:

If you will include ShareFile StorageZone Controllers in your environment, ensure that you correctly configure the following: ShareFile Content Switch VIP (used by the ShareFile Control Plane to communicate with the StorageZone Controller servers), ShareFile Load Balancing VIPs, and all required policies and profiles. For information, see Configure NetScaler for StorageZones Controller in the Citrix StorageZones documentation.

SAML IdP

Decision detail:

- If SAML is required for ShareFile, do you want to use XenMobile as the SAML IdP?

Design guidance:

The recommended best practice is to integrate ShareFile with XenMobile Advanced Edition or XenMobile Enterprise Edition, a simpler alternative to configuring SAML-based federation. When you use ShareFile with those XenMobile editions, XenMobile provides ShareFile with single sign-on (SSO) authentication of XenMobile Apps users, user account provisioning based on Active Directory, and comprehensive access control policies. The XenMobile console enables you to perform ShareFile configuration and to monitor service levels and license usage.

Note that there are two types of ShareFile clients: ShareFile Worx clients (also referred to as wrapped ShareFile) and ShareFile mobile clients (also referred to as unwrapped ShareFile). To understand the differences, see How ShareFile Worx Clients Differ from ShareFile Mobile Clients.

You can configure XenMobile and ShareFile to use SAML to provide SSO access to ShareFile mobile apps you wrap with the MDX toolkit, as well as to non-wrapped ShareFile clients, such as the web site, Outlook plugin, or sync clients.

If you want to use XenMobile as the SAML IdP for ShareFile, ensure that the proper configurations are in place. For details, see SAML for SSO with ShareFile.

ShareConnect direct connections

Decision detail:

- Will users access a host computer from a computer or mobile device running ShareConnect using direct connections?

Design guidance:

ShareConnect enables users to connect securely to their computers through iPads, Android tablets, and Android phones to access their files and applications. For direct connections, XenMobile uses NetScaler Gateway to provide secure access to resources outside of the local network. For configuration details, see ShareConnect.

Enrollment FQDN for each deployment type

Deployment type	Enrollment FQDN
Enterprise (MDM+MAM) with mandatory MDM enrollment	XenMobile server FQDN

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Enterprise (MDM+MAM) with optional MDM enrollment	XenMobile server FQDN or NetScaler Gateway FQDN
MDM only	XenMobile server FQDN
MAM-only (legacy)	NetScaler Gateway FQDN
MAM-only (for XenMobile 10.3.5 and higher)	XenMobile server FQDN

Deployment Summary

The XenMobile product documentation includes a Flowchart for Deploying XenMobile with NetScaler Gateway along with links to related articles, such as system requirements, gathering required information, configuring XenMobile for NetScaler Gateway, and using the NetScaler for XenMobile wizard to configure XenMobile connections.

Citrix recommends that you use the NetScaler for XenMobile wizard to ensure proper configuration. Be aware that you can use the wizard only one time. If you have multiple XenMobile instances, such as for test, development, and production environments, you must configure NetScaler for the additional environments manually. When you have a working environment, take note of the settings before attempting to configure NetScaler manually for XenMobile.

The key decision you make when using the wizard is whether to use HTTPS or HTTP for communication to the XenMobile server. HTTPS provides secure back-end communication, as traffic between NetScaler and XenMobile is encrypted; the re-encryption impacts XenMobile server performance. HTTP provides better XenMobile server performance; traffic between NetScaler and XenMobile is not encrypted. The following tables show the HTTP and HTTPS port requirements for NetScaler and XenMobile server.

HTTPS

Citrix typically recommends SSL Bridge for NetScaler MDM virtual server configurations. For NetScaler SSL Offload use with MDM virtual servers, XenMobile supports only port 80 as the backend service.

Deployment type	NetScaler load balancing method	SSL re-encryption	XenMobile server port
MDM	SSL Bridge	N/A	443, 8443
MAM	SSL Offload	Enabled	8443
Enterprise	MDM: SSL Bridge	N/A	443, 8443
Enterprise	MAM: SSL Offload	Enabled	8443

HTTP

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Deployment type	NetScaler load balancing method	SSL re-encryption	XenMobile server port
MDM	SSL Offload	Not supported	80
MAM	SSL Offload	Enabled	8443
Enterprise	MDM: SSL Offload	Not supported	80
Enterprise	MAM: SSL Offload	Enabled	8443

For diagrams of NetScaler Gateway in XenMobile deployments, see Reference Architecture for On-Premises Deployments and Reference Architecture for Cloud Deployments.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

SSO and Proxy Considerations for MDX Apps

Feb 21, 2018

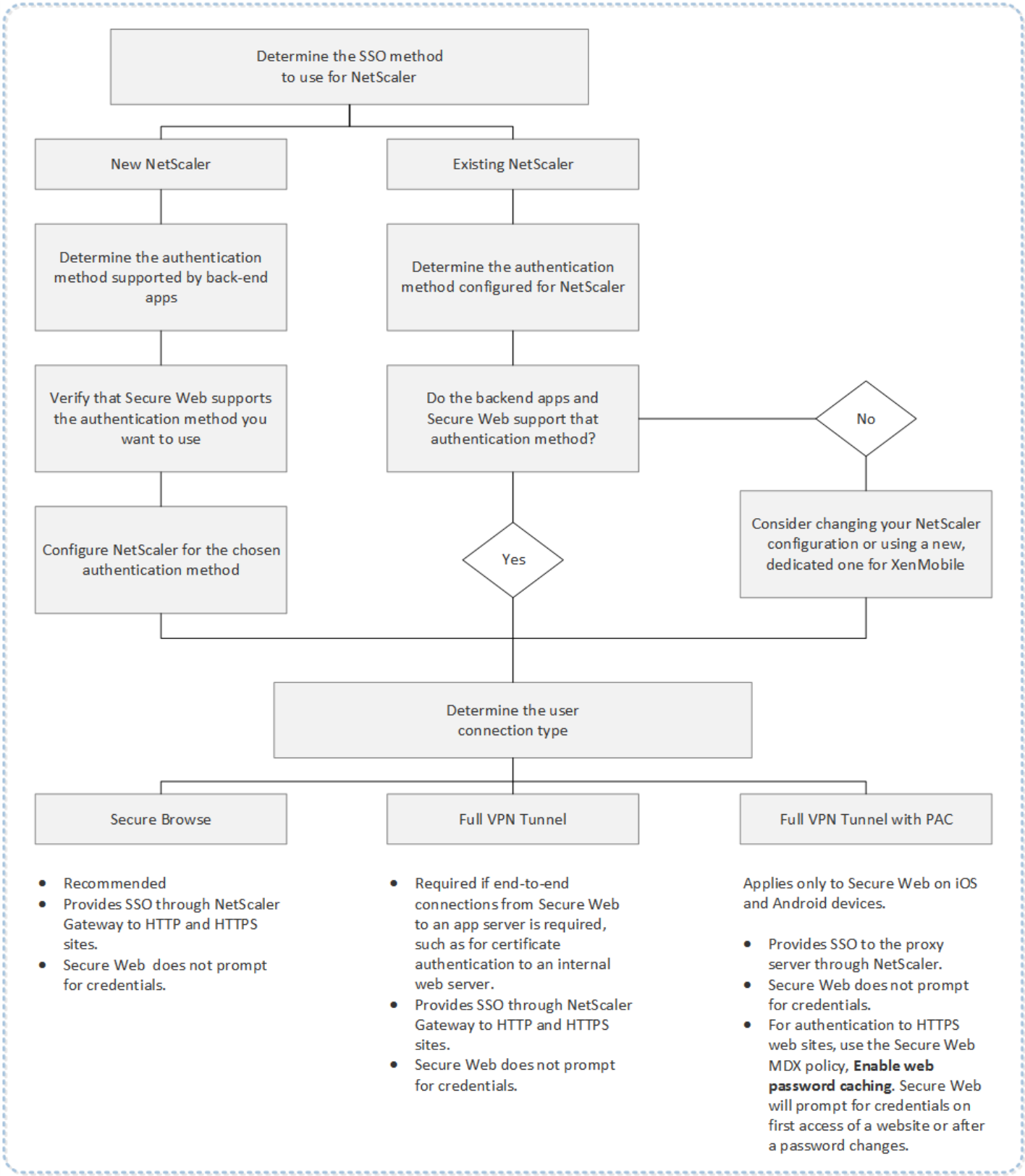
XenMobile integration with NetScaler enables you to provide users with single sign-on (SSO) to all backend HTTP/HTTPS resources. Depending on your SSO authentication requirements, you can configure user connections for an MDX app to use either of these options:

- Secure Browse, which is a type of clientless VPN
- Full VPN Tunnel

If NetScaler isn't the best way to provide SSO in your environment, you can set up an MDX app with policy-based local password caching. This article explores the various SSO and proxy options, with a focus on Secure Web. The concepts apply to other MDX apps.

The following flow chart summarizes the decision flow for SSO and user connections.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



NetScaler Authentication Methods

This section provides general information about the authentication methods supported by NetScaler.

SAML authentication

© 1999-2017 Citrix Systems, Inc. All rights reserved.

When you configure NetScaler for Security Assertion Markup Language (SAML), users can connect to web apps that support the SAML protocol for single sign-on. NetScaler Gateway supports the identity provider (IdP) single sign-on for SAML web apps.

Required configuration:

- Configure SAML SSO in the NetScaler Traffic profile.
- Configure the SAML iDP for the requested service.

NTLM authentication

If SSO to web apps is enabled in the session profile, NetScaler performs NTLM authentication automatically.

Required configuration:

- Enable SSO in the NetScaler Session or Traffic profile.

Kerberos impersonation

XenMobile supports Kerberos for Secure Web only. When you configure NetScaler for Kerberos SSO, NetScaler uses impersonation when a user password is available to NetScaler. Impersonation means that NetScaler uses user credentials to get the ticket required to gain access to services, such as Secure Web.

Required configuration:

- Configure the NetScaler "Worx" Session policy to allow it to identify the Kerberos Realm from your connection.
- Configure a Kerberos Constrained Delegation (KCD) account on NetScaler. Configure that account with no password and bind it to a traffic policy on your XenMobile gateway.
- For those and other configuration details, see the Citrix blog: WorxWeb and Kerberos Impersonation SSO.

Kerberos Constrained Delegation

XenMobile supports Kerberos for Secure Web only. When you configure NetScaler for Kerberos SSO, NetScaler uses constrained delegation when a user password is not available to NetScaler.

With constrained delegation, NetScaler uses a specified administrator account to get tickets on behalf of users and services.

Required configuration:

- Configure a KCD account in Active Directory with the required permissions and a KDC account on NetScaler.
- Enable SSO in the NetScaler Traffic profile.
- Configure the back-end website for Kerberos authentication.
- For those and other configuration details, see the Citrix blog, Configuring Kerberos Single Sign-on for WorxWeb.

Form Fill Authentication

When you configure NetScaler for Form-based single sign-on, users can log on one time to access all protected apps in your network. This authentication method applies to apps that use Secure Browse or Full VPN modes.

Required configuration:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Configure Form-based SSO in the NetScaler Traffic profile.

Digest HTTP authentication

If you enable SSO to web apps in the session profile, NetScaler performs digest HTTP authentication automatically. This authentication method applies to apps that use Secure Browse or Full VPN modes.

Required configuration:

- Enable SSO in the NetScaler Session or Traffic profile.

Basic HTTP authentication

If you enable SSO to web apps in the session profile, NetScaler performs basic HTTP authentication automatically. This authentication method applies to apps that use Secure Browse or Full VPN modes.

Required configuration:

- Enable SSO in the NetScaler Session or Traffic profile.

Secure Browse, Full VPN Tunnel, or Full VPN Tunnel with PAC

The following sections describe the user connection types for Secure Web. For more information, see this Secure Web article in the Citrix documentation, Configuring User Connections.

Full VPN Tunnel

Connections that tunnel to the internal network can use a full VPN tunnel. Use the Secure Web Preferred VPN mode policy to configure full VPN tunnel. Citrix recommends Full VPN tunnel for connections that use client certificates or end-to-end SSL to a resource in the internal network. Full VPN tunnel handles any protocol over TCP. You can use full VPN tunnel with Windows, Mac, iOS, and Android devices.

In Full VPN Tunnel mode, NetScaler does not have visibility inside an HTTPS session.

Secure Browse

Connections that tunnel to the internal network can use a variation of a clientless VPN, referred to as Secure Browse. Secure Browse is the default configuration specified for the Secure Web **Preferred VPN mode** policy. Citrix recommends Secure Browse for connections that require single sign-on (SSO).

In Secure Browse mode, NetScaler breaks the HTTPS session into two parts:

- From the client to NetScaler
- From NetScaler to the back-end resource server.

In this manner, NetScaler has full visibility into all transactions between the client and server, enabling it to provide SSO.

You can also configure proxy servers for Secure Web when used in secure browse mode. For details, see the blog XenMobile WorxWeb Traffic Through Proxy Server in Secure Browse Mode.

Full VPN Tunnel with PAC

© 1999-2017 Citrix Systems, Inc. All rights reserved.

You can use a Proxy Automatic Configuration (PAC) file with a full VPN tunnel deployment for Secure Web on iOS and Android devices. XenMobile supports proxy authentication provided by NetScaler. A PAC file contains rules that define how web browsers select a proxy to access a given URL. PAC file rules can specify handling for both internal and external sites. Secure Web parses PAC file rules and sends the proxy server information to NetScaler Gateway. NetScaler Gateway is unaware of the PAC file or proxy server.

For authentication to HTTPS web sites: The Secure Web MDX policy, **Enable web password caching**, enables Secure Web to authenticate and provide SSO to the proxy server through MDX.

NetScaler Split Tunneling

When planning your SSO and proxy configuration, you must also decide whether to use NetScaler split tunneling. Citrix recommends that you use NetScaler split tunneling only if needed. This section provides a high-level look at how split tunneling works: NetScaler determines the traffic path based on its routing table. When NetScaler split tunneling is on, Secure Hub distinguishes internal (protected) network traffic from Internet traffic. Secure Hub makes that determination based on the DNS suffix and Intranet applications. Secure Hub then tunnels only the internal network traffic through the VPN tunnel. When NetScaler split tunneling is off, all traffic goes through the VPN tunnel.

- If you prefer to monitor all the traffic due to security considerations, turn off NetScaler split tunneling. As a result, all traffic goes through the VPN tunnel.
- If you use Full VPN Tunnel with PAC, you must disable NetScaler Gateway split tunneling. If split tunneling is on and you configure a PAC file, the PAC file rules override the NetScaler split tunneling rules. A proxy server configured in a traffic policy does not override NetScaler split tunneling rules.

By default, the **Network access** policy is set to **Tunneled to the internal network** for Secure Web. With that configuration, MDX apps use NetScaler split tunnel settings. The **Network access** policy default differs for some other XenMobile Apps.

NetScaler Gateway also has a micro VPN reverse split tunnel mode. This configuration supports an exclusion list of IP addresses that aren't tunneled to the NetScaler. Instead, those addresses are sent by using the device internet connection. For more information about reverse split tunneling, see Configuring Split Tunneling in the NetScaler Gateway documentation.

XenMobile includes a **Reverse split tunnel exclusion list.** To prevent certain websites from tunneling through NetScaler Gateway: Add a comma-separated list of fully qualified domain names (FQDN) or DNS suffixes that connect by using the local area network (LAN) instead. This list applies only to Secure Browse mode with NetScaler Gateway configured for reverse split tunneling.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Authentication

Feb 21, 2018

In a XenMobile deployment, several considerations come into play when deciding how to configure authentication. This section will help you understand the various factors that affect authentication by discussing the following:

- The main MDX policies, XenMobile client properties and NetScaler Gateway settings involved with authentication.
- The ways these policies, client properties, and settings interact.
- The tradeoffs of each choice.

This article also includes three examples of recommended configurations for increasing degrees of security.

Broadly speaking, stronger security results in a less-optimal user experience, because users have to authenticate more often. How you balance those concerns depends on your organization's needs and priorities. By reviewing the three recommended configurations, you should gain a greater understanding of the interplay of authentication measures available to you, and how to best deploy your own XenMobile environment.

Authentication Modes

Online authentication: Allows users into the XenMobile network. Requires an Internet connection.

Offline authentication: Happens on the device. Users unlock the secure vault and have offline access to items, such as downloaded mail, cached websites, and notes.

Methods of Authentication

Single Factor

LDAP: You can configure a connection in XenMobile to one or more directories, such as Active Directory that are compliant with the Lightweight Directory Access Protocol (LDAP). This is a commonly used method to provide single sign-on (SSO) for company environments. You might opt for Citrix PIN with Active Directory password caching to improve the user experience with LDAP while still providing the security of complex passwords on enrollment, password expiration, and account lockout.

For more details, see Domain or domain plus STA in the XenMobile documentation.

Client certificate: XenMobile can integrate with industry-standard certificate authorities to use certificates as the sole method of online authentication. XenMobile provides this certificate after user enrollment, which requires either a one-time password, invitation URL, or LDAP credentials. When using a client certificate as the primary method of authentication, a Citrix PIN is required in client certificate-only environments to secure the certificate on the device.

XenMobile supports Certificate Revocation List (CRL) only for a third-party Certificate Authority. If you have a Microsoft CA configured, XenMobile uses NetScaler to manage revocation. When you configure client certificate-based authentication, consider whether you need to configure the NetScaler Certificate Revocation List (CRL) setting, Enable CRL Auto Refresh. This step ensures that the user of a device in MAM-only mode can't authenticate using an existing certificate on the device; XenMobile re-issues a new certificate, because it doesn't restrict a user from generating a user certificate if one is revoked. This setting increases the security of PKI entities when the CRL checks for expired PKI entities.

For a diagram that shows the deployment needed if you plan to use certificate-based authentication for users or if you need to use your enterprise Certificate Authority (CA) for issuing device certificates, see Reference Architecture for On-Premises Deployments.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Two Factor

LDAP + Client Certificate: In the XenMobile environment, this configuration is the best combination of security and user experience, with the best SSO possibilities coupled with security provided by two-factor authentication at NetScaler. Using both LDAP and client certificate provides security with both something users know (their Active Directory passwords) and something they have (client certificates on their devices). Secure Mail (and some other XenMobile Apps) can automatically configure and provide a seamless first-time user experience with client certificate authentication, with a properly configured Exchange client access server environment. For optimal usability, you can combine this option with Citrix PIN and Active Directory password caching.

LDAP + Token: This configuration allows for the classic configuration of LDAP credentials, plus a one-time password, using the RADIUS protocol. For optimal usability, you can combine this option with Citrix PIN and Active Directory password caching.

Important Policies, Settings and Client Properties Involved in Authentication

The following policies, settings, and client properties come into play with the following three recommended configurations:

MDX policies

App passcode: If **On**, a Citrix PIN or passcode is required to unlock the app when it starts or resumes after a period of inactivity. Default is **On**.

To configure the inactivity timer for all apps, set the INACTIVITY_TIMER value in minutes in the XenMobile console in **Client Properties** on the **Settings** tab. The default is 15 minutes. To disable the inactivity timer, so that a PIN or passcode prompt appears only when the app starts, set the value to zero.

Note: If you select Secure offline for the Encryption keys policy, this policy is automatically enabled.

Online session required: If **On**, the user must have a connection to the enterprise network and an active session in order to access the app on the device. If **Off**, an active session is not required to access the app on the device. Default is **Off**.

Maximum offline period (hours): Defines the maximum period an app can run without reconfirming app entitlement and refreshing policies from XenMobile. When you set the Maximum offline period, if Secure Hub for iOS has a valid NetScaler Gateway token, the app retrieves new policies for MDX apps from XenMobile without any interruption to users. If Secure Hub does not have a valid NetScaler token, users must authenticate through Secure Hub in order for app policies to update. The NetScaler token may become invalid due to a NetScaler Gateway session inactivity or a forced session time-out policy. When users sign on to Secure Hub again, they can continue running the app.

Users are reminded to sign on at 30, 15, and 5 minutes before the period expires. After expiration, the app is locked until users sign on. Default is **72 hours (3 days)**. Minimum period is 1 hour.

Note: Keep in mind that in a scenario in which users travel often and may use international roaming, the default of 72 hours (3 days) may be too short.

Background services ticket expiration: The time period that a background network service ticket remains valid. When Secure Mail connects through NetScaler Gateway to an Exchange Server running ActiveSync, XenMobile issues a token that Secure Mail uses to connect to the internal Exchange Server. This property setting determines the duration that Secure Mail can use the token without requiring a new token for authentication and the connection to the Exchange Server. When the time limit expires, users must log on again to generate a new token. Default is **168 hours (7 days)**. When this time-out expires, mail notifications will discontinue.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Online session required grace period: Determines how many minutes a user can use the app offline before the Online session required policy prevents them from further use (until the online session is validated). Default is 0 (no grace period).

For more information about MDX Toolkit authentication policies, see XenMobile MDX Policies for iOS and XenMobile MDX Policies for Android.

XenMobile client properties

Note: Client properties are a global setting that apply to all devices that connect to XenMobile.

Citrix PIN: For a simple sign-on experience, you might choose to enable the Citrix PIN. With the PIN, users do not have to enter other credentials repeatedly, such as their Active Directory user names and passwords. You can configure the Citrix PIN as a standalone offline authentication only, or combine the PIN with Active Directory password caching to streamline authentication for optimal usability. You configure the Citrix PIN in **Settings** > **Client** > **Client Properties** in the XenMobile console.

Following is a summary of a few important properties. For more information, see Client properties in the XenMobile documentation.

ENABLE_PASSCODE_AUTH

Display name: Enable Citrix PIN Authentication

This key allows you to turn on Citrix PIN functionality. With the Citrix PIN or passcode, users are prompted to define a PIN to use instead of their Active Directory password. You should enable this setting if **ENABLE_PASSWORD_CACHING** is enabled or if XenMobile is using certificate authentication.

Possible values: **true** or **false**

Default value: **false**

ENABLE_PASSWORD_CACHING

Display name: Enable User Password Caching

This key lets you allow the users' Active Directory password to be cached locally on the mobile device. When you set this key to true, users are prompted to set a Citrix PIN or passcode. The ENABLE_PASSCODE_AUTH key must be set to true when you set this key to **true**.

Possible values: **true** or **false**

Default value: **false**

PASSCODE_STRENGTH

Display name: PIN Strength Requirement

This key defines the strength of the Citrix PIN or passcode. When you change this setting, users are prompted to set a new Citrix PIN or passcode the next time they are prompted to authenticate.

Possible values: **Low**, **Medium**, or **Strong**

Default value: **Medium**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

INACTIVITY_TIMER

Display name: Inactivity timer

This key defines the time in minutes that users can leave their devices inactive and then access an app without being prompted for a Citrix PIN or passcode. To enable this setting for an MDX app, you must set the App Passcode setting to **On**. If the App Passcode setting is set to **Off**, users are redirected to Secure Hub to perform a full authentication. When you change this setting, the value takes effect the next time users are prompted to authenticate. The default is 15 minutes.

ENABLE_TOUCH_ID_AUTH

Display name: Enable Touch ID Authentication

Allows the use of the fingerprint reader (in iOS only) for offline authentication. Online authentication will still require the primary authentication method.

ENCRYPT_SECRETS_USING_PASSCODE

Display name: Encrypt secrets using Passcode

This key lets sensitive data be stored on the mobile device in a secret vault instead of in a platform-based native store, such as the iOS keychain. This configuration key enables strong encryption of key artifacts, but also adds user entropy (a user-generated random PIN code that only the user knows).

Possible values: **true** or **false**

Default value: **false**

NetScaler Settings

Session time-out: If you enable this setting, NetScaler Gateway disconnects the session if NetScaler detects no network activity for the specified interval. This setting is enforced for users who connect with the NetScaler Gateway Plug-in, Citrix Receiver, Secure Hub, or through a web browser. Default is **1440 minutes**. If you set this value to zero, the setting is disabled.

Forced time-out: If you enable this setting, NetScaler Gateway disconnects the session after the time-out interval elapses no matter what the user is doing. When the time-out interval elapses, there is no action the user can take to prevent the disconnection. This setting is enforced for users who connect with the NetScaler Gateway Plug-in, Citrix Receiver, Secure Hub, or through a web browser. If Secure Mail is using STA, a special NetScaler mode, the Forced time-out setting does not apply to Secure Mail sessions. Default is **1440 minutes**. If you leave this value blank, the setting is disabled.

For more information about time-out settings in NetScaler Gateway, see Configuring Time-Out Settings in the NetScaler documentation.

For more information on the scenarios that prompt users to authenticate with XenMobile by entering credentials on their devices, see Authentication Prompt Scenarios in the XenMobile Apps documentation.

Default Configuration Settings

These settings are the defaults provided by the NetScaler for XenMobile wizard, by the MDX Toolkit, and in the XenMobile

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

console.

Setting	Where to Find the Setting	Default Setting
Session time-out	NetScaler Gateway	1440 minutes
Force time-out	NetScaler Gateway	1440 minutes
Maximum offline period	MDX Policies	72 hours
Background services ticket expiration	MDX Policies	168 hours (7 days)
Online session required	MDX Policies	Off
Online session required grace period	MDX Policies	0
App passcode	MDX Policies	On
Encrypt secrets using passcode	XenMobile client properties	false
Enable Citrix PIN Authentication	XenMobile client properties	false
PIN Strength Requirement	XenMobile client properties	Medium
PIN Type	XenMobile client properties	Numeric
Enable User Password Caching	XenMobile client properties	false
Inactivity Timer	XenMobile client properties	15
Enable Touch ID Authentication	XenMobile client properties	false

Recommended Configurations

This section gives examples of three XenMobile configurations that range from lowest security and optimal user experience, to the highest security and more intrusive user experience. These examples should provide you with helpful reference points to determine where on the scale you want to place your own configuration. Be aware that modifying these settings may require you to alter other settings as well. For instance, the maximum offline period should always be less than the session time-out.

High Security

This configuration, the most convenient to users, provides base-level security.

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
Session time-out	NetScaler Gateway	10080	Users enter their Secure Hub credentials only when online authentication is required - every 7 days

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
Force time-out	NetScaler Gateway	No value	Sessions will be extended if there's any activity.
Maximum offline period	MDX Policies	167	Requires policy refresh every week (every 7 days). The hour difference is to allow for refresh ahead of session time-out.
Background services ticket expiration	MDX Policies	240	Time out for STA, which allows for long-lived sessions without a NetScaler Gateway session token. In the case of Secure Mail, making the STA time-out longer than the session time-out avoids having mail notifications stop without prompting the user if they don't open the app before the session expires.
Online session required	MDX Policies	Off	Ensures a valid network connection and NetScaler Gateway session to use apps.
Online session required grace period	MDX Policies	0	No grace period (if you enabled Online Session required).
App passcode	MDX Policies	On	Require passcode for application.
Encrypt secrets using passcode	XenMobile client properties	false	Do not require user entropy to encrypt the vault.
Enable Citrix PIN Authentication	XenMobile client properties	true	Enable Citrix PIN for simplified authentication experience.
PIN Strength Requirement	XenMobile client properties	Low	No password complexity requirements
PIN Type	XenMobile client properties	Numeric	PIN is a numeric sequence.
Enable Password Caching	XenMobile client properties	true	The user PIN caches and protects the Active Directory password.
Inactivity Timer	XenMobile client properties	90	If user does not use MDX apps or Secure Hub for this period of time, prompt for offline authentication.
Enable Touch ID Authentication	XenMobile client properties	true	Enables Touch ID for offline authentication use cases in iOS.

Higher Security

© 1999-2017 Citrix Systems, Inc. All rights reserved.

A more middle-of-the-road approach, this configuration requires users to authenticate more often - every 3 days, at most, instead of 7 - and stronger security. The increased number of authentications lock the container more often, ensuring data security when devices aren't in use.

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
Session time-out	NetScaler Gateway	4320	Users enter their Secure Hub credentials only when online authentication is required - every 3 days
Force time-out	NetScaler Gateway	No value	Sessions will be extended if there's any activity.
Maximum offline period	MDX Policies	71	Requires policy refresh every 3 days. The hour difference is to allow for refresh ahead of session time-out.
Background services ticket expiration	MDX Policies	168 hours	Time out for STA, which allows for long-lived sessions without a NetScaler Gateway session token. In the case of Secure Mail, making the STA time-out longer than the session time-out avoids having mail notifications stop without prompting the user if they don't open the app before the session expires.
Online session required	MDX Policies	Off	Ensures a valid network connection and NetScaler Gateway session to use apps.
Online session required grace period	MDX Policies	0	No grace period (if you enabled Online Session required).
App passcode	MDX Policies	On	Require passcode for application.
Encrypt secrets using passcode	XenMobile client properties	false	Do not require user entropy to encrypt the vault.
Enable Citrix PIN Authentication	XenMobile client properties	true	Enable Citrix PIN for simplified authentication experience.
PIN Strength Requirement	XenMobile client properties	Medium	Enforces medium password complexity rules.
PIN Type	XenMobile client properties	Numeric	PIN is a numeric sequence.
Enable Password	XenMobile client	true	The user PIN caches and protects the Active Directory password.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
Inactivity Timer	XenMobile client properties	30	If user does not use MDX apps or Secure Hub for this period of time, prompt for offline authentication.
Enable Touch ID Authentication	XenMobile client properties	true	Enables Touch ID for offline authentication use cases in iOS.

Highest Security

This configuration offers the highest level of security but contains significant usability trade-offs.

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
Session time-out	NetScaler Gateway	1440	Users enter their Secure Hub credentials only when online authentication is required-every 24 hours.
Force time-out	NetScaler Gateway	1440	Online authentication will be strictly required every 24 hours. Activity doesn't extend session life.
Maximum offline period	MDX Policies	23	Requires policy refresh every day.
Background services ticket expiration	MDX Policies	72 hours	Time out for STA, which allows for long-lived sessions without a NetScaler Gateway session token. In the case of Secure Mail, making the STA time-out longer than the session time-out avoids having mail notifications stop without prompting the user if they don't open the app before the session expires.
Online session required	MDX Policies	Off	Ensures a valid network connection and NetScaler Gateway session to use apps.
Online session required grace period	MDX Policies	0	No grace period (if you enabled Online Session required).
App passcode	MDX Policies	On	Require passcode for application.
Encrypt secrets using passcode	XenMobile client properties	true	A key derived from user entropy protects the vault.
Enable Citrix PIN Authentication	XenMobile client properties	true	Enable Citrix PIN for simplified authentication experience.
PIN Strength	XenMobile		

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
PIN Type	XenMobile client properties	Alphanumeric	PIN is an alphanumeric sequence.
Enable Password Caching	XenMobile client properties	false	Active Directory password is not cached and Citrix PIN will be used for offline authentications.
Inactivity Timer	XenMobile client properties	15	If user does not use MDX apps or Secure Hub for this period of time, prompt for offline authentication.
Enable Touch ID Authentication	XenMobile client properties	false	Disables Touch ID for offline authentication use cases in iOS.

Using Step-Up Authentication

Some apps may require enhanced authentication (for example, a secondary authentication factor, such as a token or aggressive session time-outs). You control this authentication method through an MDX policy. The method also requires a separate virtual server to control the authentication methods (on either the same or on separate NetScaler appliances).

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
Alternate NetScaler Gateway	MDX Policies	Requires the FQDN and port of the secondary NetScaler appliance.	Allows for enhanced authentication controlled by the secondary NetScaler appliance authentication and session policies.

If a user opens an app that logs on to the alternate NetScaler Gateway instance, all other apps will use that NetScaler Gateway instance for communicating with the internal network. The session will only switch back to the lower security NetScaler Gateway instance when the session times out from the NetScaler Gateway instance with enhanced security.

Using Online Session Required

For certain applications, such as Secure Web, you may want to ensure that users run an app only when they have an authenticated session and while the device is connected to a network. This policy enforces that option and allows for a grace period so users can finish their work.

Setting	Where to Find the Setting	Recommended Setting	Behavior Impact
Online session required	MDX Policies	On	Ensures device is online and has a valid authentication token.
Online session required			Allows a 15-minute grace period before the user can no

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Setting	**Where to Find the Setting**	**Recommended Setting**	**Behavior Impact**

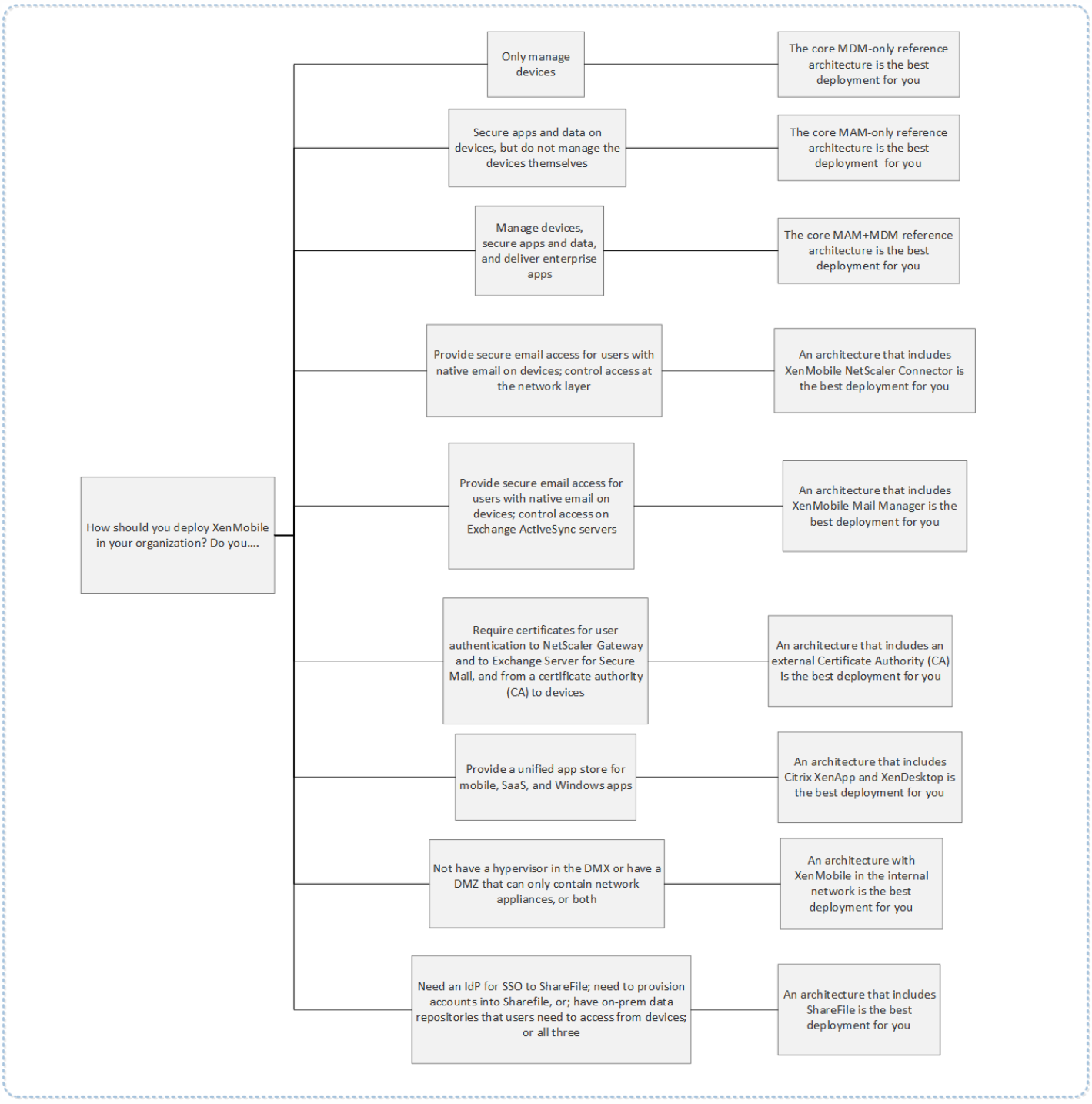
© 1999-2017 Citrix Systems, Inc. All rights reserved.

Reference Architecture for On-Premises Deployments

Feb 21, 2018

The figures in this article illustrate the reference architectures for the XenMobile deployment on premises. The deployment scenarios include MDM-only, MAM-only, and MDM+MAM as the core architectures, as well as those that include components, such as the SNMP Manager, XenMobile NetScaler Connector, XenMobile Mail Manager, and XenApp and XenDesktop. The figures show the minimal components required for XenMobile.

Use this chart as a general guide for your deployment decisions.

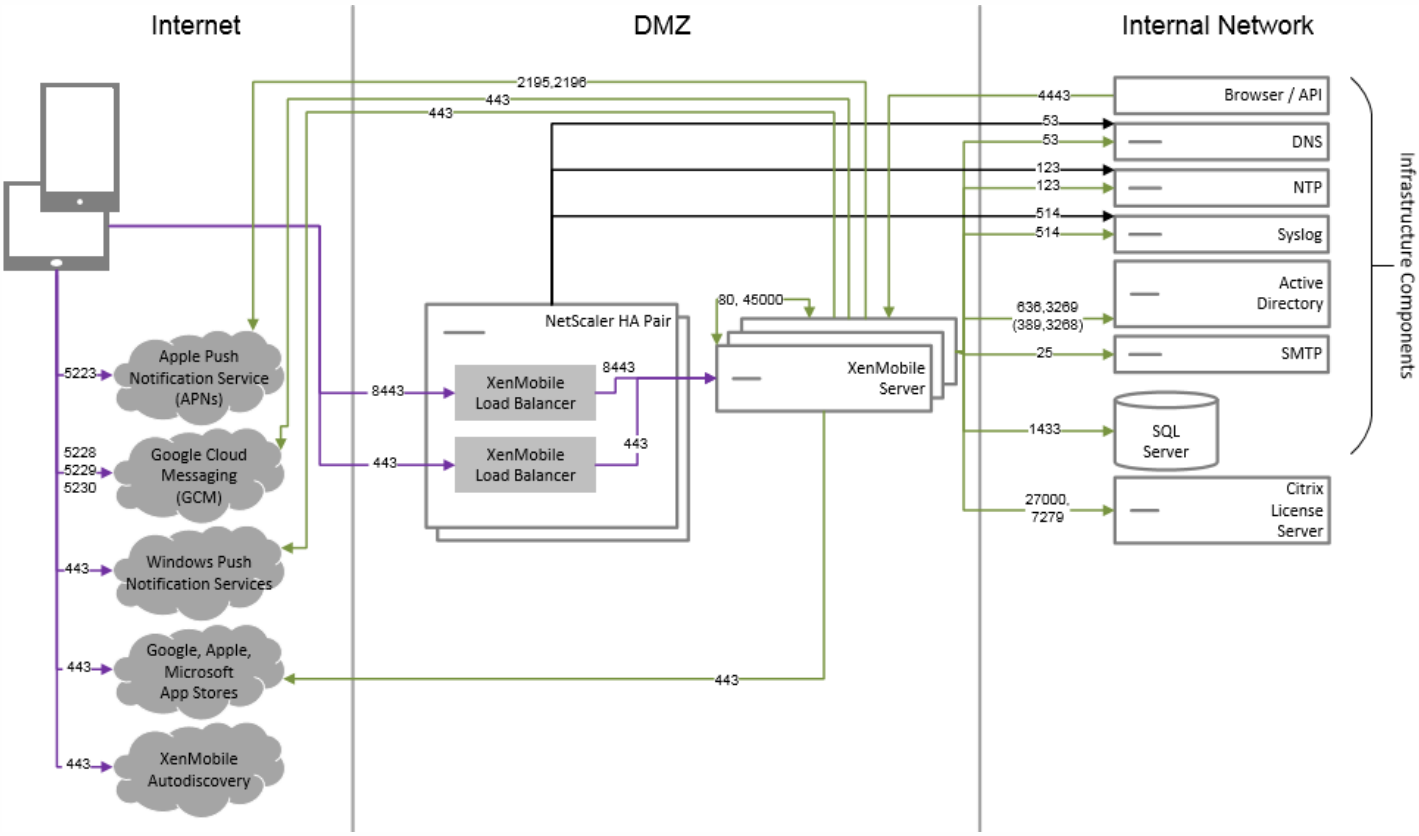


© 1999-2017 Citrix Systems, Inc. All rights reserved.

In the figures, the numbers on the connectors represent ports that you must open to allow connections between the components. For a complete list of ports, see Port requirements in the XenMobile documentation.

Core MDM-Only Reference Architecture

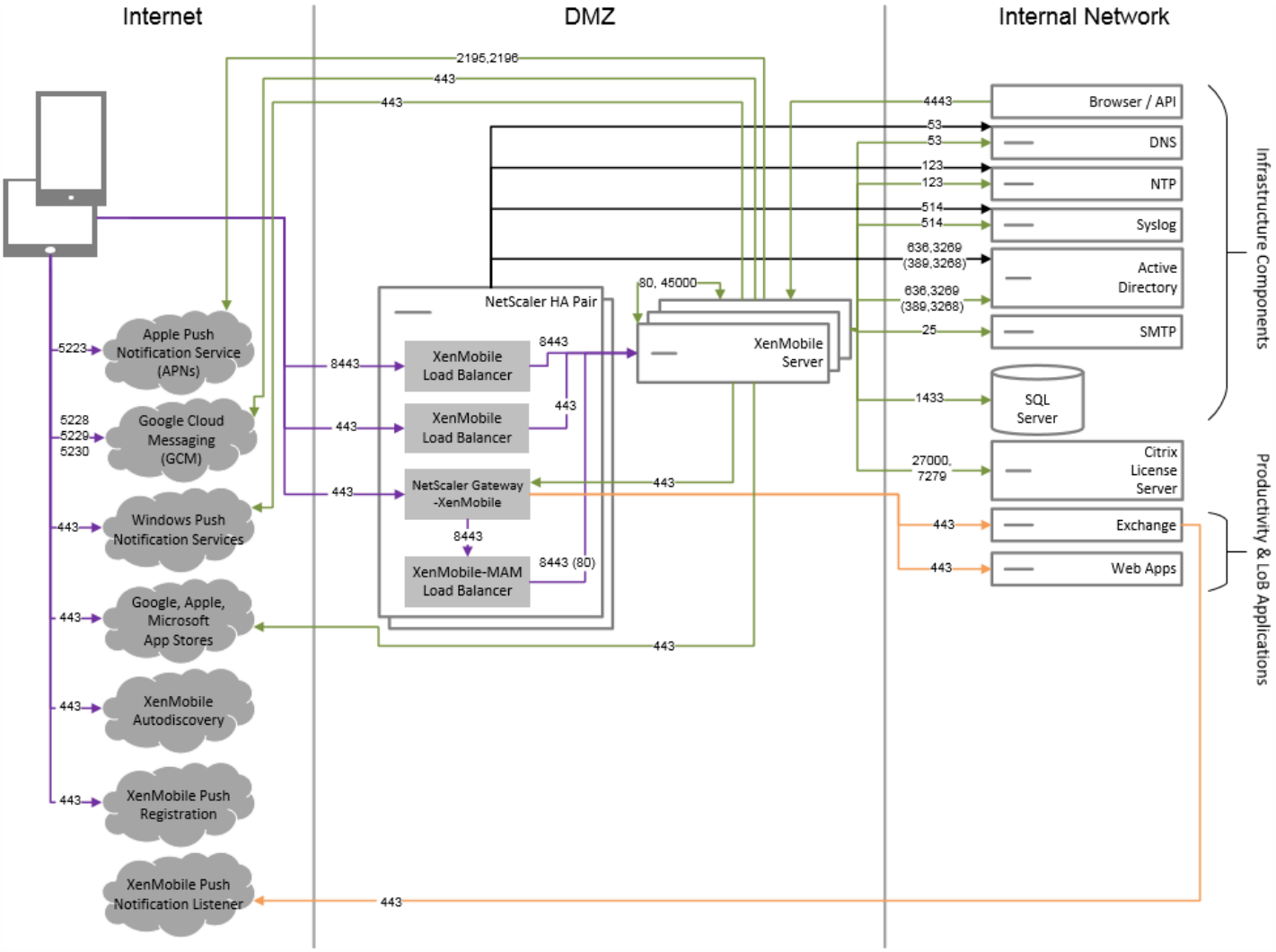
Deploy this architecture if you plan to use only the MDM features of XenMobile. For example, you need to manage a corporate-issued device through MDM in order to deploy device policies, apps and to retrieve asset inventories and be able to carry out actions on devices, such as a device wipe.



Core MAM-Only Reference Architecture

Deploy this architecture if you plan to use only the MAM features of XenMobile without having devices enroll for MDM. For example, you want to secure apps and data on BYO mobile devices; you want to deliver enterprise mobile apps and be able to lock apps and wipe their data. The devices cannot be MDM enrolled.

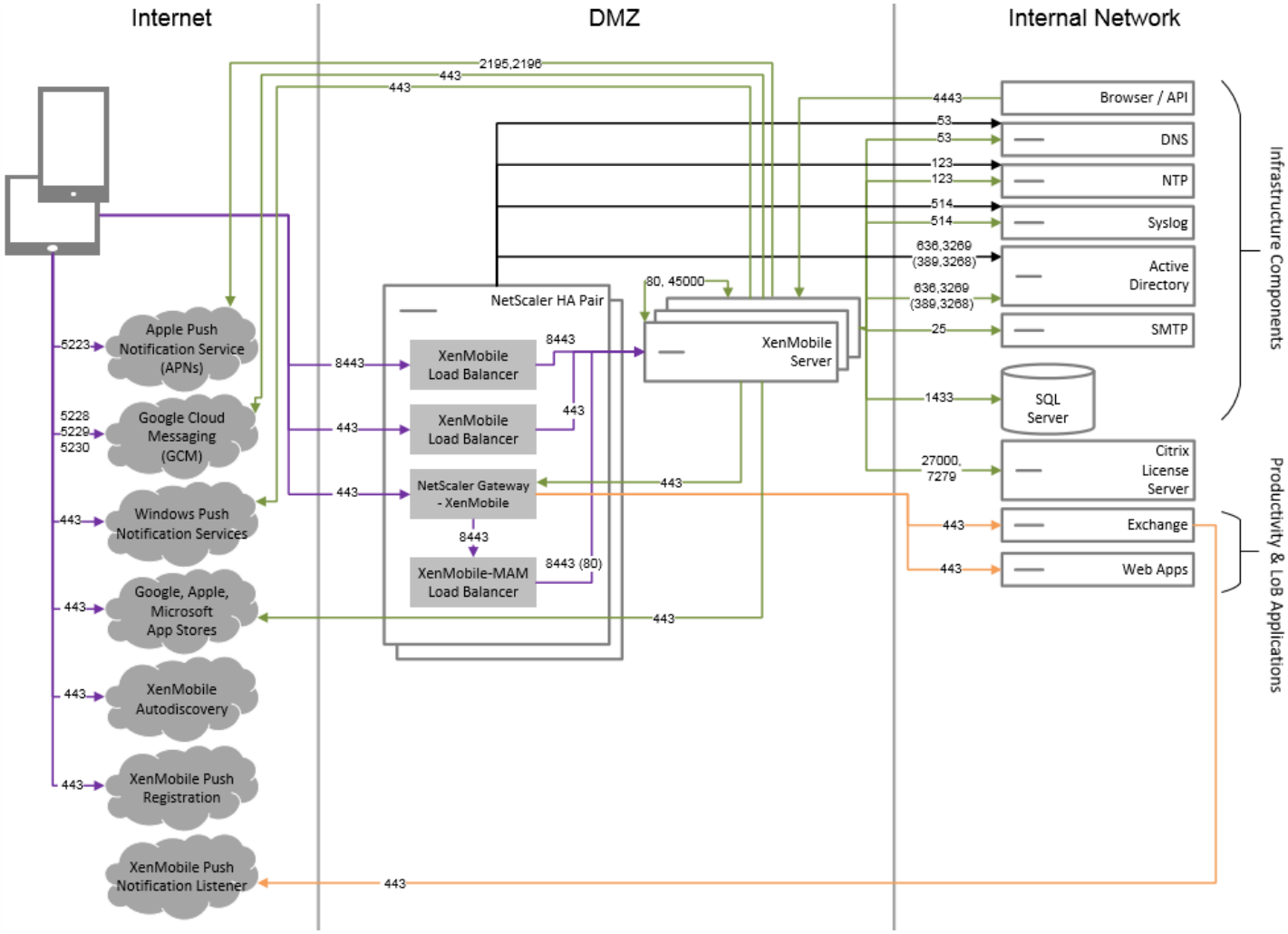
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Core MAM+MDM Reference Architecture

Deploy this architecture if you plan to use MDM+MAM features of XenMobile. For example, you want to manage a corporate-issued device via MDM; you want to deploy device policies and apps, retrieve an asset inventory and be able to wipe devices. You also want to deliver enterprise mobile apps and be able to lock apps and wipe the data on devices.

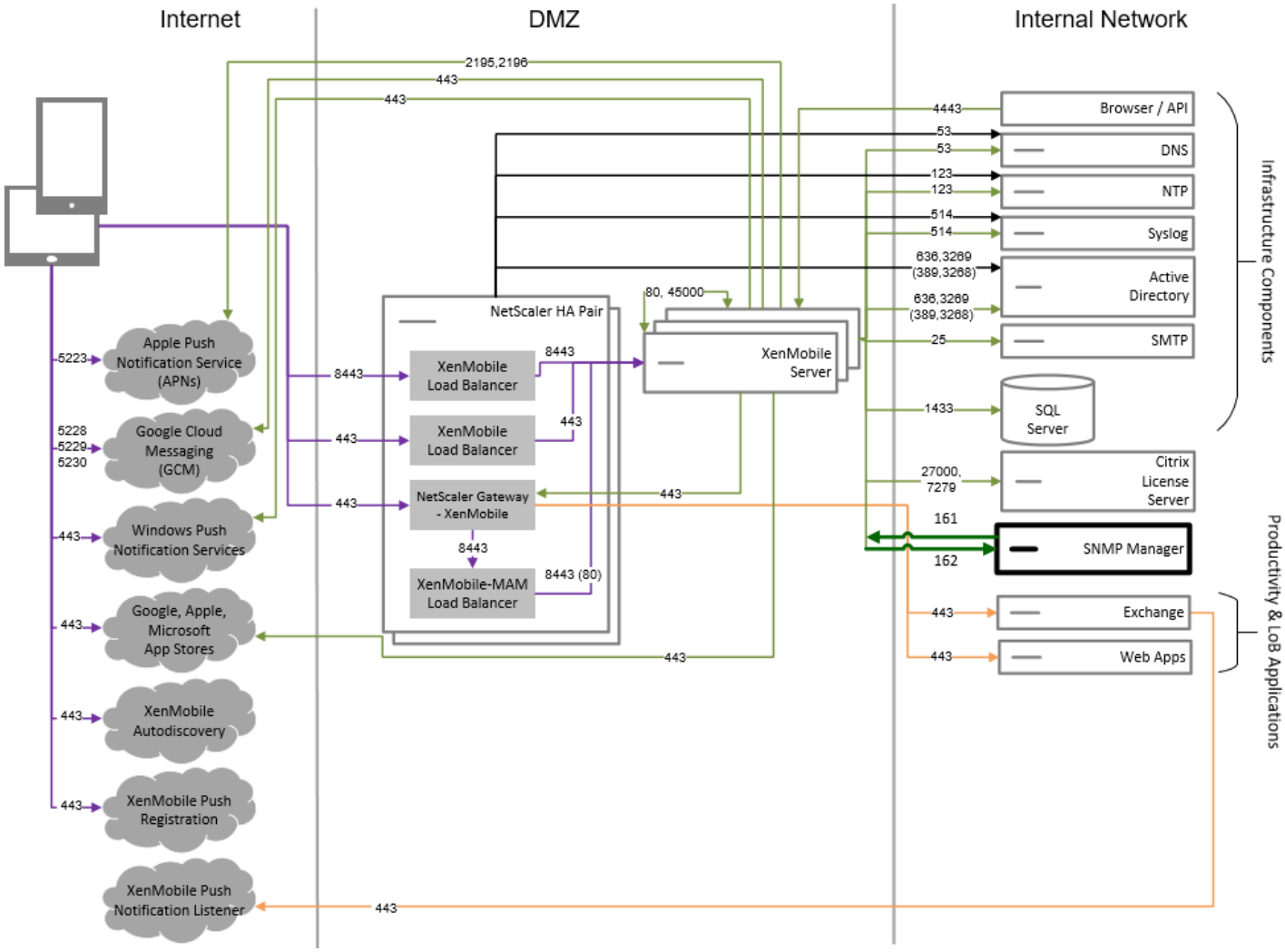
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Reference Architecture with SNMP

Deploy this architecture if you plan to enable SNMP monitoring with XenMobile. For example, you want to allow monitoring systems to query and obtain information on your XenMobile nodes. For details, see SNMP monitoring.

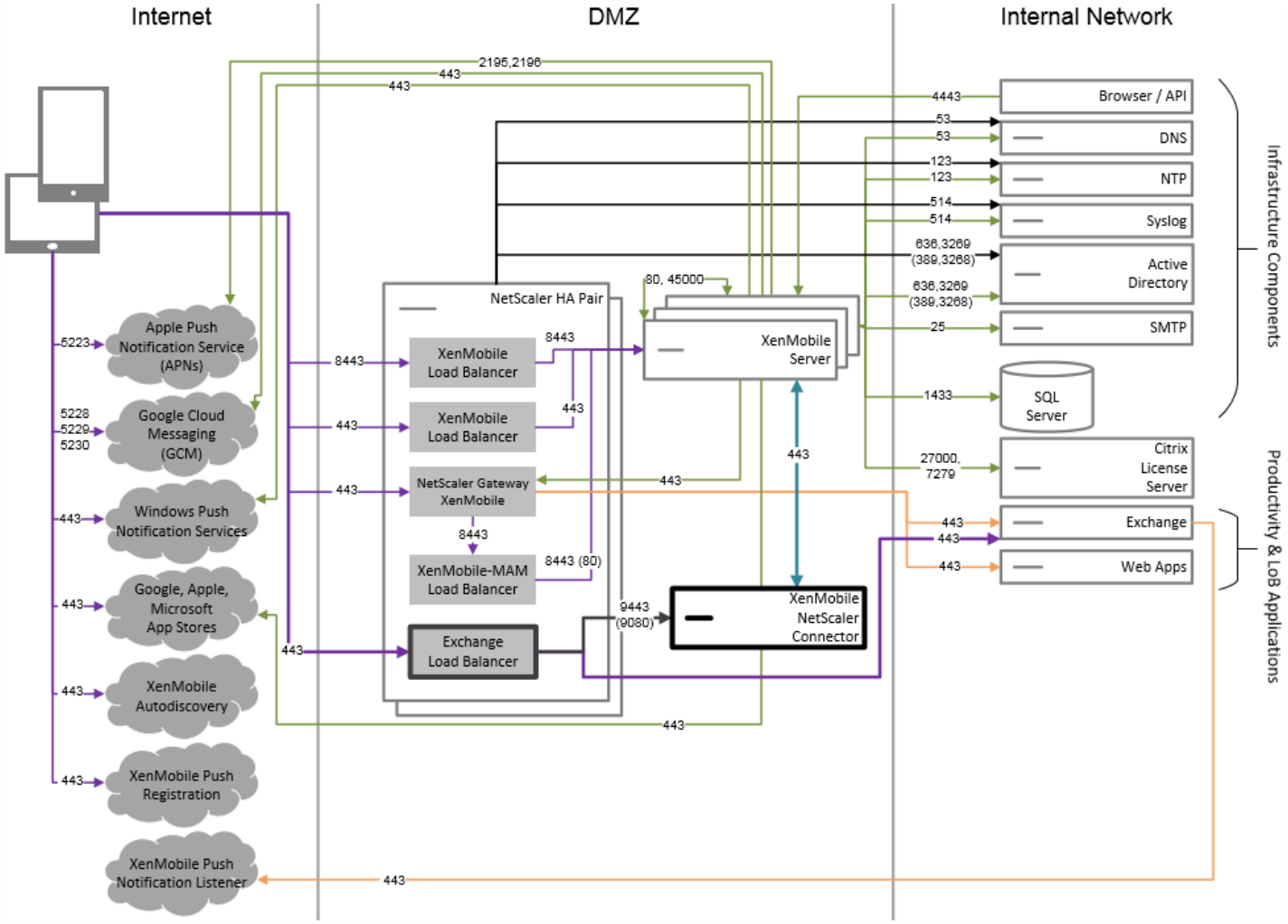
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Reference Architecture with XenMobile NetScaler Connector

Deploy this architecture if you plan to use XenMobile NetScaler Connector with XenMobile. For example, you need to provide secure email access to users who use native mobile email apps. These users will continue accessing email via a native app or you may transition them over time to Citrix Secure Mail. Access control needs to occur at the network layer before traffic hits the Exchange Active Sync servers. Even though the diagram shows XenMobile NetScaler Connector deployed in a MDM and MAM architecture, you can also deploy XenMobile NetScaler Connector in the same manner as part of an MDM-only architecture.

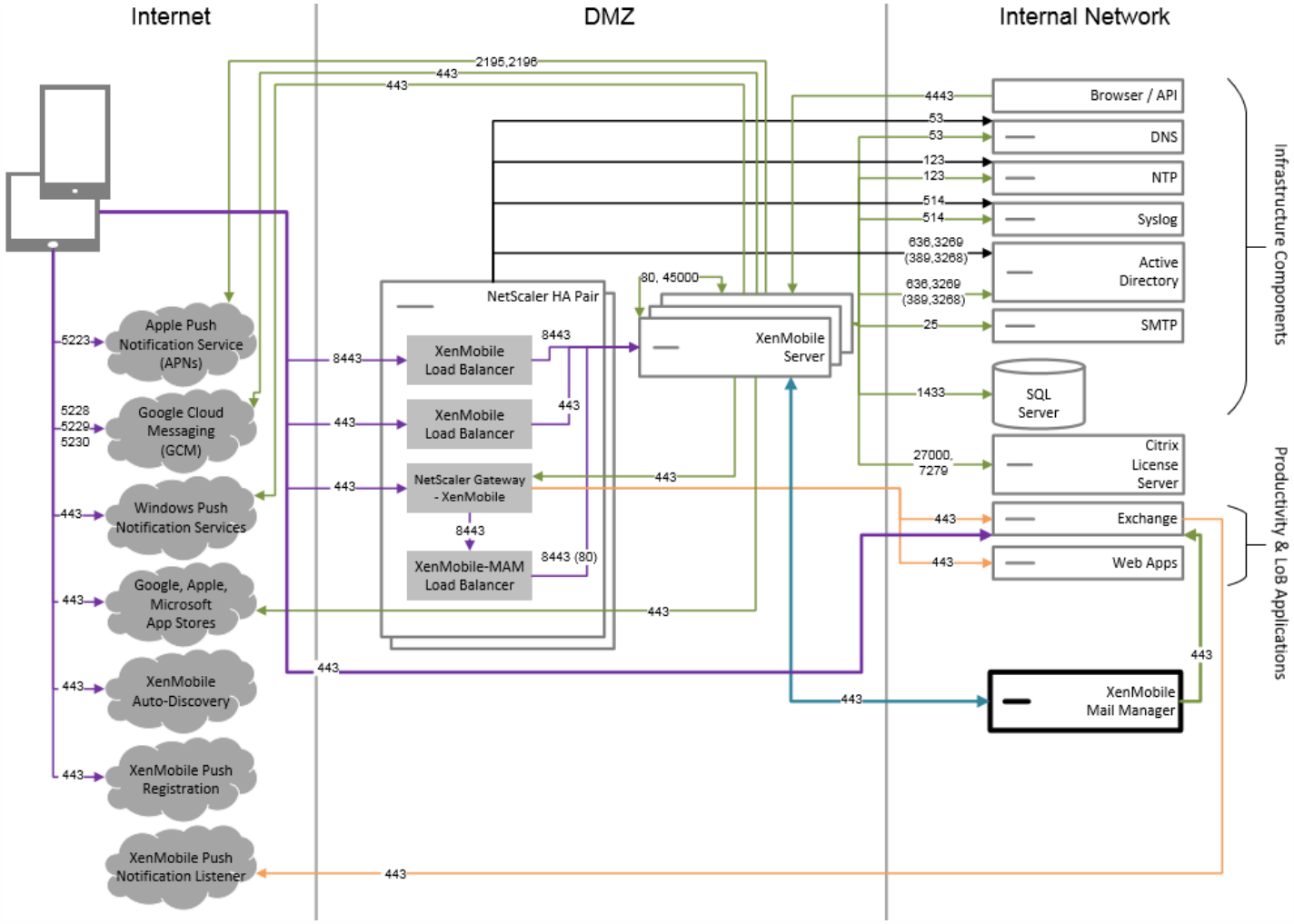
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Reference Architecture with XenMobile Mail Manager

Deploy this architecture if you plan to use XenMobile Mail Manager with XenMobile. For example, you want to provide secure email access to users who use native mobile email apps. These users will continue accessing email via a native app or you may transition users over time to Secure Mail. You can achieve access control on the Exchange ActiveSync servers. Although the diagram shows XenMobile Mail Manager deployed in a MDM and MAM architecture, you can also deploy XenMobile Mail Manager in the same manner as part of an MDM-only architecture.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



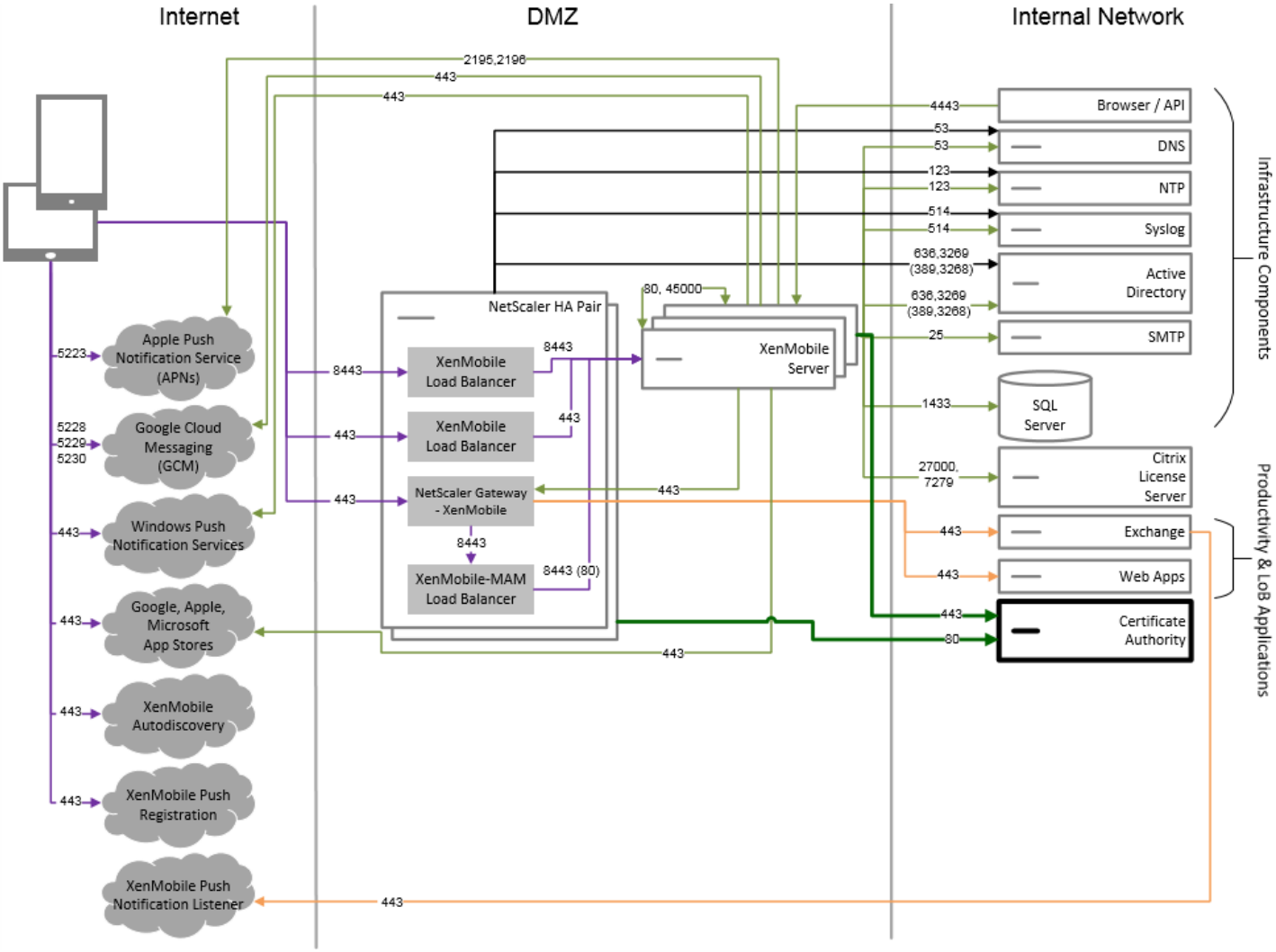
Reference Architecture with External Certificate Authority

A deployment that includes an external certificate authority is recommended to meet one or more of the following requirements:

- You require user certificates for user authentication to NetScaler Gateway (for intranet access).
- You require Secure Mail users to authenticate to Exchange Server by using a user certificate.
- You need to push certificates issued by your corporate Certificate Authority to mobile devices for WiFi access, for example.

Although the diagram shows an external certificate authority deployed in an MDM+MAM architecture, you can also deploy an external Certificate Authority in the same manner as part of an MDM-only or MAM-only architecture.

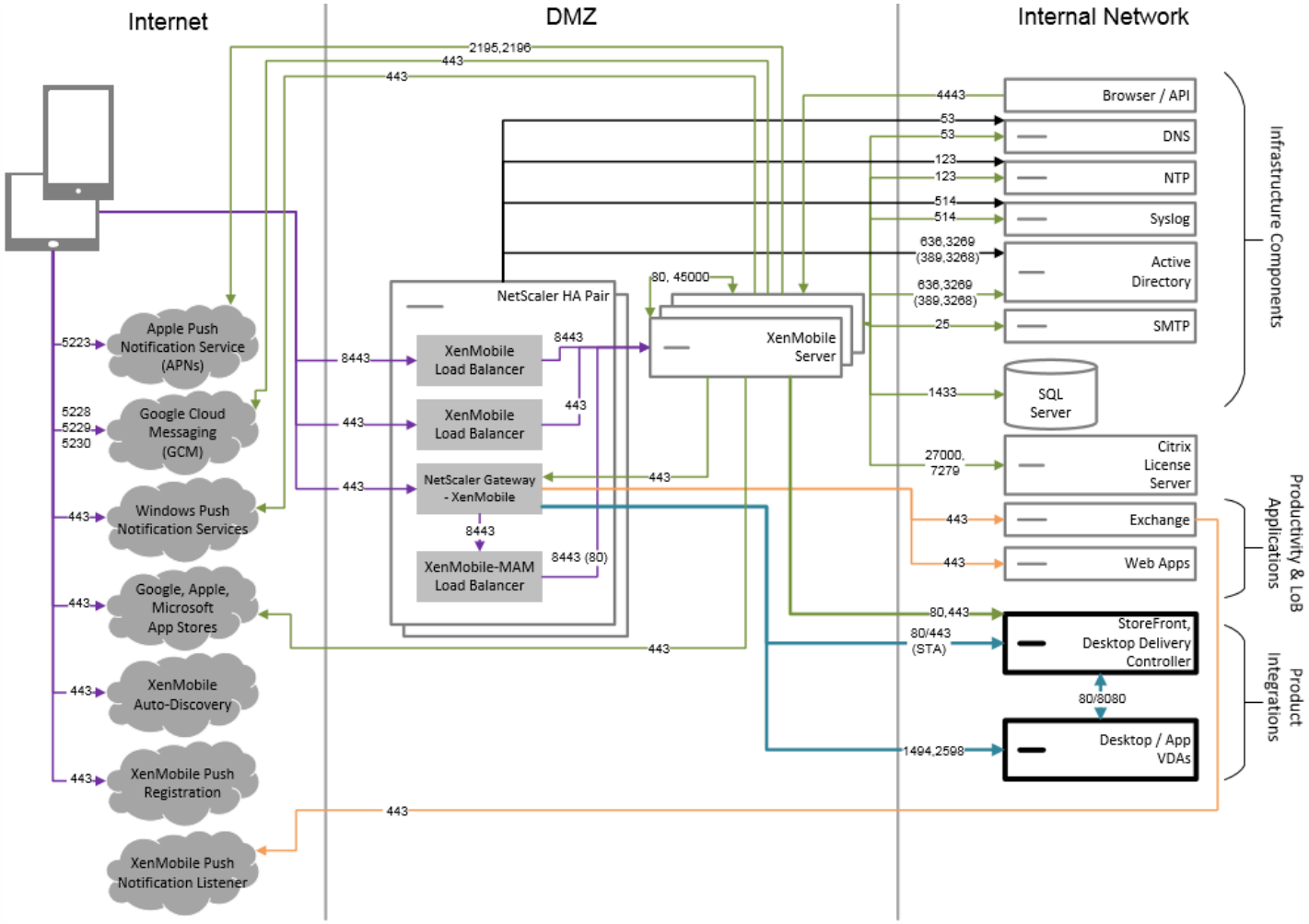
© 1999-2017 Citrix Systems, Inc. All rights reserved.



Reference Architecture with XenApp and XenDesktop

Deploy this architecture if you plan to integrate XenApp and XenDesktop with XenMobile. For example, you need to provide a unified app store to mobile users for all types of applications (mobile, SaaS and Windows). Although the diagram shows XenDesktop deployed in a MDM and MAM architecture, you can also deploy XenDesktop in the same manner as part of a MAM-only architecture.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

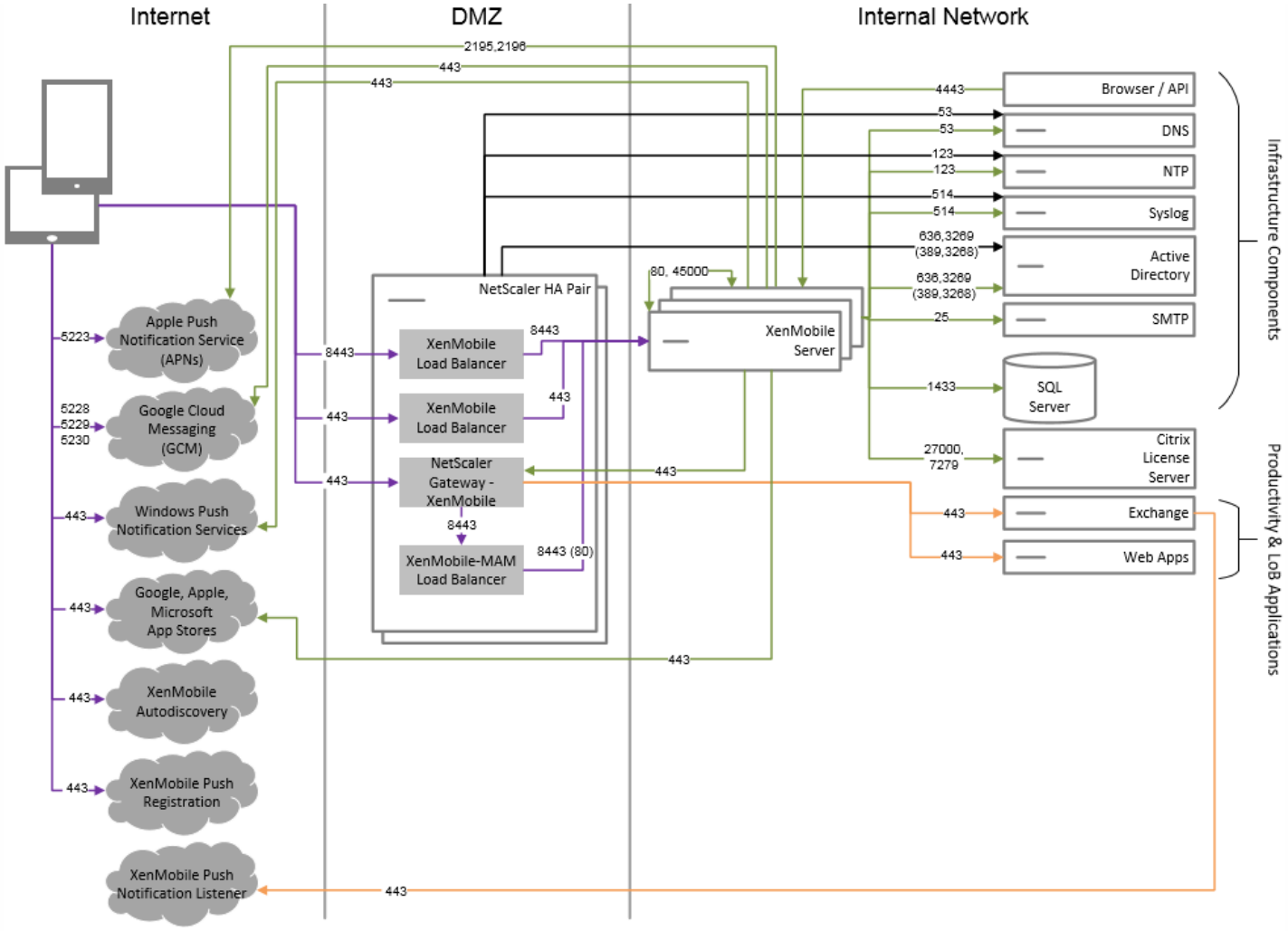


Reference Architecture with XenMobile in the Internal Network

You can deploy an architecture with XenMobile in the internal network to meet one or more of the following requirements:

- You do not have or are not allowed to have a hypervisor in the DMZ.
- Your DMZ can only contain network appliances.
- Your security requirements require the use of SSL Offload.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



Reference Architecture with ShareFile

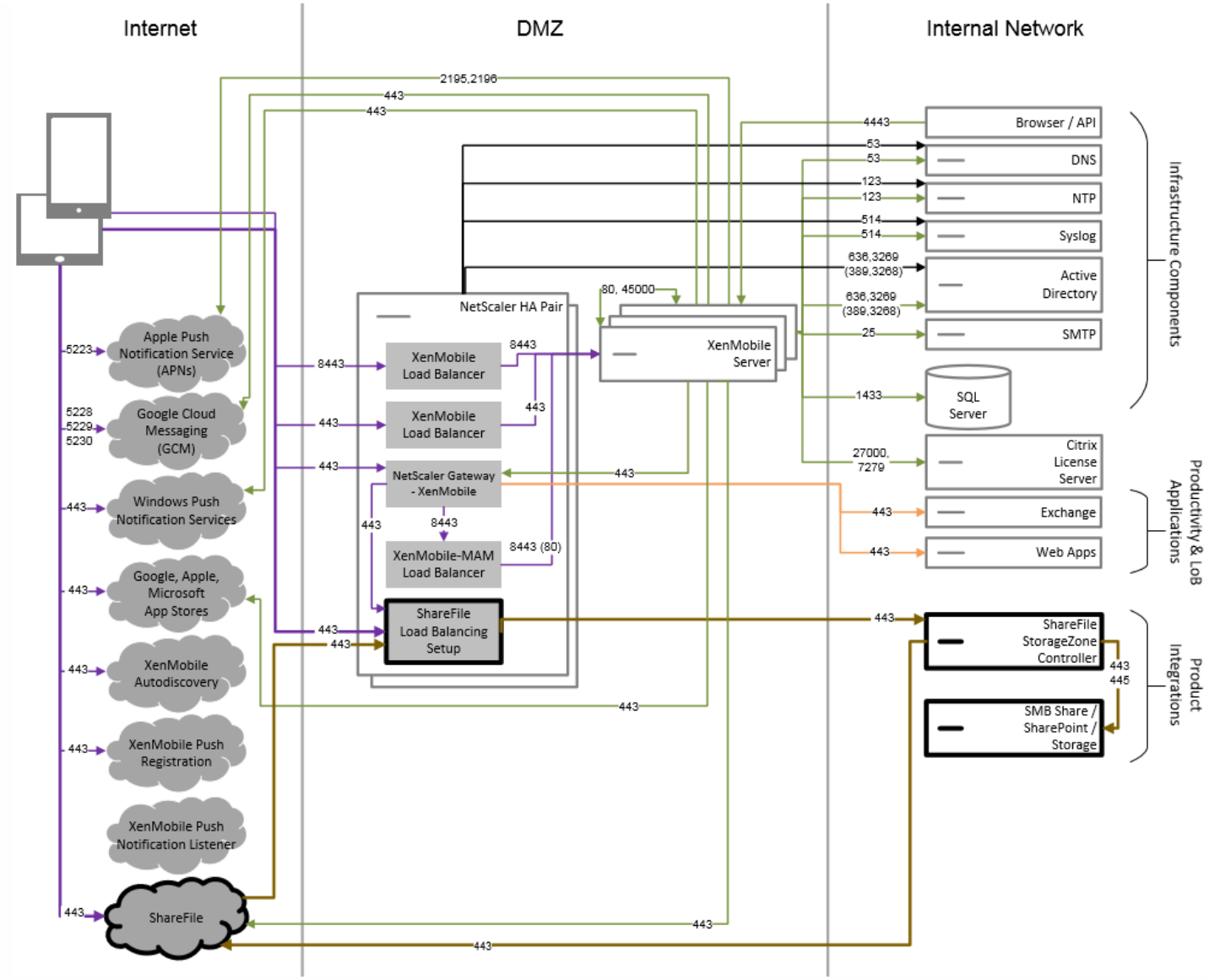
Deploy this architecture if you want to integrate ShareFile Enterprise or only StorageZone Connectors with XenMobile. ShareFile Enterprise integration enables you to meet one or more of the following requirements:

- You need an IDP to give users single sign-on (SSO) to ShareFile.com.
- You need a way to provision accounts into ShareFile.com.
- You have on-premises data repositories that need to be accessed from mobile devices.

An integration with only StorageZone Connectors gives users secure mobile access to existing on-premises storage repositories, such as SharePoint sites and network file shares. In this configuration, you don't need to set up a ShareFile subdomain, provision users to ShareFile, or host ShareFile data.

Although the diagram shows ShareFile deployed in a MDM+MAM architecture, you can also deploy ShareFile in the same manner as part of a MAM-only architecture.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Reference Architecture for Cloud Deployments

Mar 08, 2018

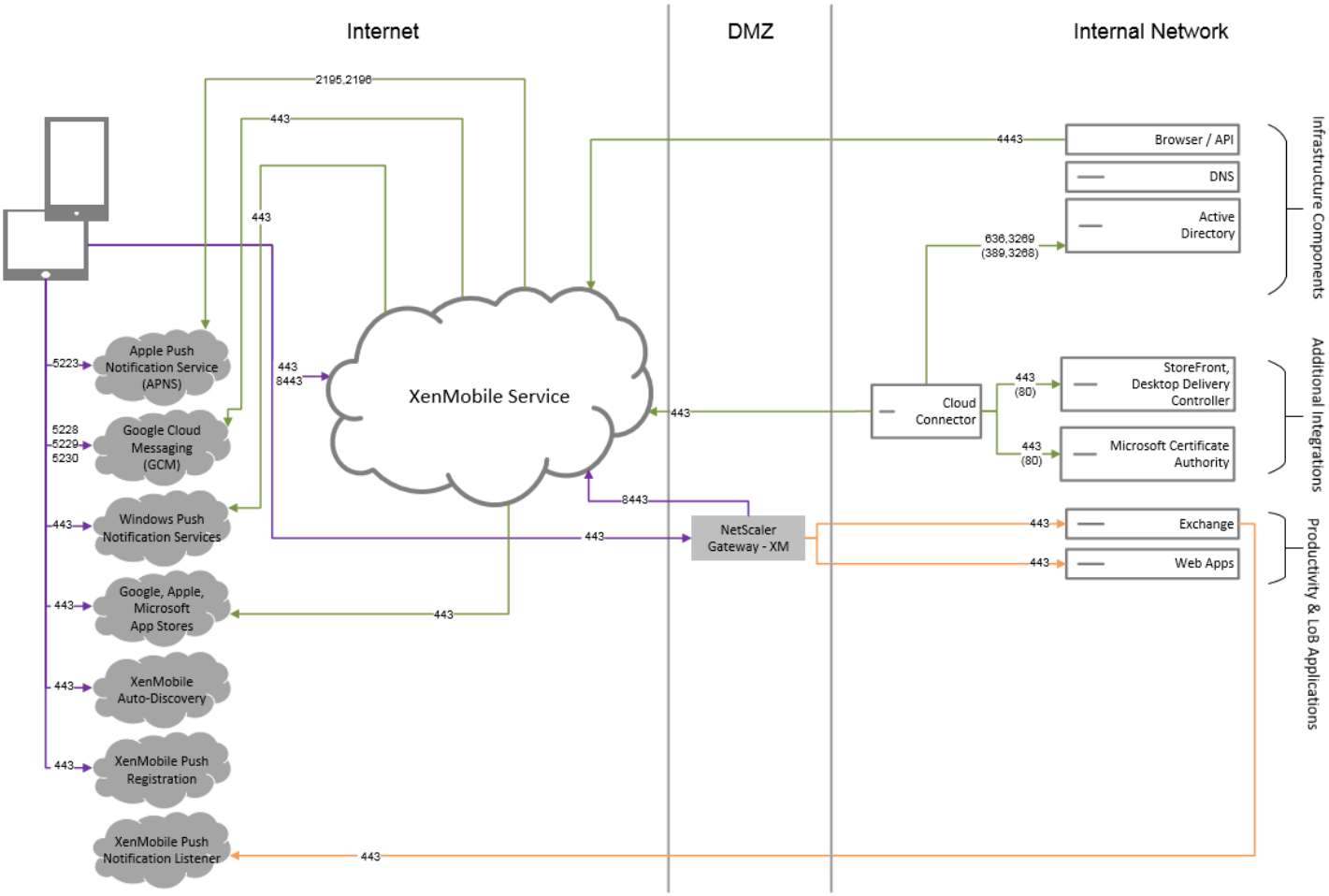
Nota

This article applies to XenMobile Service deployments only.

For the latest information about XenMobile Service architecture and port requirements, see About XenMobile Service and System requirements.

The diagram in this article shows how XenMobile Service integrates with your data center. The other component integrations, such as ShareFile, Certificate Authority, and XenApp and XenDesktop, are available as shown in the preceding core architectures. For details, see Reference Architecture for On-Premises Deployments.

Use of Cloud Connector eliminates the need to set up complex networking or infrastructure configuration, such as VPNs or IPsec tunnels. If you require a micro VPN, you must use an on-premises NetScaler with Cloud Connector. The following diagram shows NetScaler Gateway hosted on your site.



© 1999-2017 Citrix Systems, Inc. All rights reserved.

Server Properties

Feb 21, 2018

Server properties are global properties that apply to operations, users, and devices across an entire XenMobile instance. Citrix recommends that you evaluate for your environment the server properties covered in this article. Be sure to consult with Citrix before changing other server properties.

Be aware that a change to some server properties requires a restart of each XenMobile server node. XenMobile notifies you when a restart is required.

Server Property	**Notes**
Block Enrollment of Rooted Android and Jailbroken iOS Devices	When this property is **True**, XenMobile blocks enrollments for rooted Android devices and jailbroken iOS devices. Default is **True**. Recommended setting is **True** for all security levels.
Enrollment required	This property, which applies only when the XenMobile Server Mode is ENT, specifies whether you require users to enroll in MDM. The property applies to all users and devices for the XenMobile instance. Requiring enrollment provides a higher level of security; however, that decision depends on whether you want to require MDM. By default, enrollment is not required. When this property is **False**, users can decline enrollment, but may still access apps on their devices through the XenMobile Store. When this property is **True**, any user who declines enrollment is denied access to apps. If you change this property after users enroll, the users must re-enroll. For a discussion about whether to require MDM enrollment, see Device Management and MDM Enrollment.
XenMobile MDM Self Help Portal console max inactive interval (minutes) **Note**: This property name reflects the older XenMobile versions. The property controls the XenMobile console max inactive interval.	The number of minutes after which XenMobile logs an inactive user out of the XenMobile console. A time-out of 0 means an inactive user remains logged in. Default is **30**.
Inactivity Timeout in Minutes	The number of minutes after which XenMobile logs out an inactive user who used the XenMobile server Public API to access the XenMobile console or any third-party app. A time-out value of **0** means an inactive user remains logged in. For third-party apps that access the API, remaining logged in is typically necessary. Default is **5**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

iOS Device Management Enrollment Install Root CA if Required	When this property is **True**, XenMobile checks if the user has the root CA installed on the device and, if the root certificate is missing, installs it. A third-party public certificate trusted by iOS is required. Default is **True**. If you are using trusted certificates and the iOS device trusts the issuer, setting this property to False improves the MDM user enrollment experience because Secure Hub doesn't prompt the user to install another certificate and enter their PIN. However, we don't recommend setting the property to **False** if you are using a self-signed SSL Listener certificate on the XenMobile server.
VPP baseline interval	The **VPP baseline interval** sets the minimum interval that XenMobile re-imports VPP licenses from Apple. Refreshing license information ensures that XenMobile reflects all changes, such as when you manually delete an imported app from VPP. By default, XenMobile refreshes the VPP license baseline a minimum of every **720** minutes. If you have a large number of VPP licenses installed (for example, more than 50,000), Citrix recommends that you increase the baseline interval to reduce the frequency and overhead of importing licenses. If you expect frequent VPP license changes from Apple, Citrix recommends that you lower the value to keep XenMobile updated with the changes. The minimum interval between two baselines is 60 minutes. Because the cron job runs in the background every 60 minutes, if the VPP baseline interval is 60 minutes, the interval between baselines could be delayed up to 119 minutes.

Some server properties help improve performance and stability. For details, see Tuning XenMobile Operations.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Device and App Policies

Feb 21, 2018

> **Nota**
>
> This section applies to XenMobile Service and XenMobile on-premises deployments.

XenMobile device and app policies enable you to optimize a balance between factors, such as:

- Enterprise security
- Corporate data and asset protection
- User privacy
- Productive and positive user experiences

The optimum balance between those factors can vary. For example, highly regulated organizations, such as finance, require stricter security controls than other industries, such as education and retail, in which user productivity is a primary consideration.

You can centrally control and configure policies based on users' identity, device, location, and connectivity type to restrict malicious usage of corporate content. In the event a device is lost or stolen, you can disable, lock, or wipe business applications and data remotely. The overall result is a solution that increases employee satisfaction and productivity, while ensuring security and administrative control.

The primary focus of this article is the many device and app policies related to security.

Policies That Address Security Risks

XenMobile device and app policies address many situations that may pose a security risk, such as the following:

- When users try to access apps and data from untrusted devices and unpredictable locations.
- When users pass data from device to device.
- When an unauthorized user tries to access data.
- When a user who has left the company had used their own device (BYOD).
- When a user misplaces a device.
- When users need to access the network securely at all times.
- When users have their own device managed and you need to separate work data from personal data.
- When a device is idle and requires verification of user credentials again.
- When users copy and paste sensitive content into unprotected email systems.
- When users receive email attachments or web links with sensitive data on a device that holds both personal and company accounts.

Those situations relate to two main areas of concern when protecting company data, which are when data is:

- At rest
- In transit

© 1999-2017 Citrix Systems, Inc. All rights reserved.

How XenMobile Protects Data at Rest

Data stored on mobile devices is referred to as data at rest. The mobile application management (MAM) capabilities in XenMobile enable complete management, security, and control over XenMobile Apps, MDX-enabled apps, and their associated data. The Worx App SDK, which enables apps for XenMobile deployment, leverages Citrix MDX app container technology to separate corporate apps and data from personal apps and data on the user's mobile device. This allows you to secure any custom developed, third-party, or BYO mobile app with comprehensive policy-based controls.

In addition to an extensive MDX policy library, XenMobile also includes app-level encryption. XenMobile separately encrypts data stored within any MDX-enabled app without requiring a device PIN code and without requiring that you manage the device to enforce the policy.

Policies and the Worx App SDK enable you to:

- Separate business and personal apps and data in a secure mobile container.
- Secure apps with encryption and other mobile Data Loss Prevention (DLP) technologies.

MDX policies provide many operational controls, so you can enable seamless integration between MDX-wrapped apps, while also controlling all communication. In this way, you can enforce policies, such as ensuring that data only is accessible by MDX-enabled apps.

Beyond device and app policy control, the best way to safeguard data at rest is encryption. XenMobile adds a layer of encryption to any data stored in an MDX-enabled app, giving you policy control over features such as public file encryption, private file encryption, and encryption exclusions. The Worx App SDK uses FIPS 140-2 compliant AES 256- bit encryption with keys stored in a protected Citrix Secret Vault.

How XenMobile Protects Data in Transit

Data on the move between your user's mobile devices and your internal network is referred to as data in transit. MDX app container technology provides application-specific VPN access to your internal network through NetScaler Gateway.

Consider the situation where an employee wants to access the following resources residing in the secure enterprise network from a mobile device: the corporate email server, an SSL-enabled web application hosted on the corporate intranet, and documents stored on a file server or Microsoft SharePoint. MDX enables access to all these enterprise resources from mobile devices through an application-specific micro VPN. Each device has its own dedicated micro VPN tunnel.

Micro VPN functionality does not require a device-wide VPN, which can compromise security on untrusted mobile devices. As a result, the internal network is not exposed to malware or attacks that could infect the entire corporate system. Corporate mobile apps and personal mobile apps are able to coexist on one device.

To offer even stronger levels of security, you can configure MDX-enabled apps with an Alternate NetScaler Gateway policy, used for authentication and for micro VPN sessions with an app. You can use an Alternate NetScaler Gateway with the Online session required policy to force apps to reauthenticate to the specific gateway. Such gateways would typically have different (higher assurance) authentication requirements and traffic management policies.

In addition to security features, micro VPN also offers data optimization techniques, including compression algorithms to

© 1999-2017 Citrix Systems, Inc. All rights reserved.

ensure that only minimal data is transferred and that the transfer is done in the quickest time possible, thereby improving user experience, which is a key success factor in mobile project success.

You should reevaluate your device policies periodically, such as in these situations:

- When a new version of XenMobile includes new or updated policies due to the release of device operating system updates.
- When you add a new device type. Although many policies are common to all devices, each device has a set of policies specific to its operating system. As a result, you may find differences between iOS, Android, and Windows devices, and even between different manufacturers' devices running Android.
- To keep XenMobile operation in sync with enterprise or industry changes, such as new corporate security policies or compliance regulations.
- When a new version of MDX Toolkit includes new or updated policies.
- When you add or update an app.
- When you need to integrate new workflows for your users as a result of new apps or new requirements.

App Policies and Use Case Scenarios

Although you can choose which apps are available through Secure Hub, you might also want to define how those apps interact with XenMobile. If you want users to authenticate after a certain time period passes or you want to provide users offline access to their information, you do so through app policies. The following list includes some of the policies and discusses how you might use them. For a list of all MDX policies per platform, see MDX Policies at a Glance.

Authentication policies

Device passcode

Why use this policy: Enable the Device passcode policy to enforce that a user can access an MDX app only if the device has a device PIN enabled. This feature, for iOS 9 devices, ensures use of iOS encryption at the device level and for the MDX container.

User example: Enabling this policy means that the user must set a PIN code on their iOS device before they can access the MDX app.

App passcode

Why use this policy: Enable the App passcode policy to have Secure Hub prompt a user to authenticate to the managed app before they can open the app and access data. The user might authenticate with their Active Directory password, Citrix PIN, or iOS TouchID, depending what you configure under Client Properties in your XenMobile Server Settings. You can set an inactivity timer in Client Properties so that, with continued use, Secure Hub doesn't prompt the user to authenticate to the managed app again until the timer expires.

The app passcode differs from a device passcode in that, with a device passcode policy pushed to a device, Secure Hub prompts the user to configure a passcode or PIN, which they must unlock before they can gain access to their device when they turn on the device or when the inactivity timer expires. For more information, see Authentication in XenMobile.

User example: When opening the Citrix Secure Web application on the device, the user must enter their Citrix PIN before they can browse web sites if the inactivity period is expired.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Online session required

Why use this policy: If an application requires access to a web app (web service) to run, enable this policy so that XenMobile prompts the user to connect to the enterprise network or have an active session before using the app.

User example: When a user attempts to open an MDX app that has the Online session required policy enabled, they can't use the app until they connected to the network using a cellular or wifi service.

Maximum offline period

Why use this policy: Use this policy as an additional security option, to ensure that users can't run an app offline for long time periods without reconfirming app entitlement and refreshing policies from XenMobile.

User example: If you configure an MDX app with a Maximum offline period, the user can open and use the app offline until the offline timer period expires. At that point, the user must connect back to the network via cellular or wifi service and reauthenticate, if prompted.

Miscellaneous Access policies

App update grace period (hours)

Why use this policy: The app update grace period is the time available to the user before they must update an app that has a newer version released in the XenMobile Store. At the point of expiry, the user must update the app before they can gain access to the data in the app. When setting this value, keep in mind the needs of your mobile workforce, particularly those who might experience long periods offline when travelling internationally.

User example: You load a new version of Secure Mail in the XenMobile Store and then set an app update grace period of 6 hours. All Secure Mail users will see a message asking them to update their Secure Mail app, until the 6 hours expires. When the 6 hours expires, Secure Hub routes users to the XenMobile Store.

Active poll period (minutes)

Why use this policy: The active poll period is the interval at which XenMobile checks apps for when to perform security actions, such as App Lock and App Wipe.

User example: If you set the Active poll period policy to 60 minutes, when you send the App Lock command from XenMobile to the device, the lock occurs within 60 minutes of when the last poll took place.

Encryption policies

Why use these policies: XenMobile includes a secret vault with a strong encryption layer that Secure Hub and other XenMobile Apps use to persist their sensitive data, such as passwords and encryption keys, on the device without depending on the platform native keystores. As a result, if the device becomes compromised in any way, corporate data remains encrypted in the MDX container and XenMobile obfuscates the data before transferring it outside of the container.

User example: If the device owner did not set a device PIN or the device PIN becomes compromised, the corporate data inside the Secure Hub container remains secure.

App Interaction Policies

Why use these policies: Use App Interaction policies to control the flow of documents and data from MDX apps to other apps on the device. For example, you can prevent a user from moving data to their personal apps outside of the

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

container or from pasting data from outside of the container into the containerized apps.

User example: You set an App interaction policy to Restricted, which means a user can copy text from Secure Mail to Secure Web but can't copy that data to their personal Safari or Chrome browser that is outside the container. In addition, a user can open an attached document from Secure Mail into ShareFile or Quick Edit but can't open the attached document in their own personal file viewing apps that are outside the container.

App Restrictions policies

Why use these policies: Use App Restriction policies to control what features users can access from an MDX app while it is open. This helps to ensure that no malicious activity can take place while the app is running. The App Restriction policies vary slightly between iOS and Android. For example, in iOS you can block access to iCloud while the MDX app is running. In Android, you can stop NFC use while the MDX app is running.

User example: If you enable the App Restriction policy to block dictation on iOS in an MDX app, the user can't use the dictate function on the iOS keyboard while the MDX app is running. Thus, data users dictate isn't passed to the unsecure third-party cloud dictation service. When the user opens their personal app outside of the container, the dictate option remains available to the user for their personal communications.

App Network Access policies

Why use these policies: Use the App Network Access policies to provide access from an MDX app in the container on the device to data sitting inside your corporate network. For the Network access policy, set the **Tunneled to the internal network** option to automate a micro VPN from the MDX app through the NetScaler to a back-end web service or datastore.

User example: When a user opens an MDX app, such as Secure Web, that has tunneling enabled, the browser opens and launches an intranet site without the user needing to start a VPN. The Secure Web app automatically accesses the internal site using micro VPN technology.

App Geolocation and Geofencing policies

Why use these policies: The policies that control app geolocation and geofencing include center point Longitude, center point Latitude, and Radius. Those policies contain access to the data in the MDX apps to a specific geographical area. The policies define a geographic area by a radius of latitude and longitude coordinates. If a user attempts to use an app outside of the defined radius, the app remains locked and the user cannot access the app data.

User example: A user can access merger and acquisition data while they are in their office location. When they move outside of their office location, this sensitive data becomes inaccessible.

Secure Mail App policies

Background network services

Why use this policy: Background network services in Secure Mail leverage Secure Ticket Authority (STA), which is effectively a SOCKS5 proxy to connect through NetScaler Gateway. STA supports long-lived connections and provides better battery life compared to micro VPN. Thus, STA is ideal for mail that connects constantly. Citrix recommends that you configure these settings for Secure Mail. The NetScaler for XenMobile wizard automatically sets up STA for Secure Mail.

User example: When STA isn't enabled and an Android user opens Secure Mail, they are prompted to open a VPN, which remains open on the device. When STA is enabled and the Android user opens Secure Mail, Secure Mail

© 1999-2017 Citrix Systems, Inc. All rights reserved.

connects seamlessly with no VPN required.

Default sync interval

Why use this policy: This setting specifies the default days of email that synchronize to Secure Mail when the user accesses Secure Mail for the first time. Be aware that 2 weeks of email takes longer to sync than 3 days and prolongs the setup process for the user.

User example: If the default sync interval is set to 3 days when the user first sets up Secure Mail, they can see any emails in their Inbox that they received from the present to 3 days in the past. If a user wants to see emails that are older than 3 days, they can do a search. Secure Mail then shows the older emails stored on the server. After installing Secure Mail, each user can change this setting to better suit their needs.

Device Policies and Use Case Behavior

Device policies, sometimes referred to as MDM policies, determine how XenMobile works with devices. Although many policies are common to all devices, each device has a set of policies specific to its operating system. The following list includes some of the device policies and discusses how you might use them. For a list of all device policies, see the articles under Device policies.

App inventory policy

Why use this policy: Deploy the App inventory policy to a device if you need to see the apps installed by a user. If you don't deploy the App inventory policy, you can see only the apps that a user installed from the XenMobile Store and not any personally installed applications. You must use this policy if you want to blacklist certain apps from running on corporate devices.

User example: A user with an MDM-managed device cannot disable this functionality. The user's personally installed applications are visible to XenMobile administrators.

App lock policy

Why use this policy: The App Lock policy, for Android, allows you to blacklist or whitelist apps. For example, by whitelisting apps you can configure a kiosk device. Typically, you deploy the App lock policy only to corporate owned devices, because it limits the apps that users can install. You can set an override password to provide user access to blocked apps.

User example: Suppose that you deploy an App lock policy that blocks the Angry Birds app. The user can install the Angry Birds app from Google Play, yet when they open the app a message advises them that their administrator blocked the app.

Connection scheduling policy

Why use this policy: You must use the Connection scheduling policy so that Android and Windows Mobile devices can connect back to XenMobile for MDM management, app push, and policy deployment. If you do not deploy this policy and have not enabled Google Firebase Cloud Messaging (FCM), devices will not connect back to XenMobile. It is important to deploy this policy in the base package for enrolling devices. The Scheduling options are as follows:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Always - Keeps the connection alive permanently. Citrix recommends this option for optimized security. When you choose **Always**, also use the Connection timer policy to ensure that the connection is not draining the battery. By keeping the connection alive, you can push security commands like wipe or lock to the device on-demand. You must also select the Deployment Schedule option **Deploy for always-on connection** in each policy you deploy to the device.

Never - Connects manually. Citrix does not recommend this option for production deployments because the **Never** option prevents you from deploying security policies to devices; thus, users never receive any new apps or policies.

Every - Connects at the designated interval. When this option is in effect and you send a security policy, such as a lock or a wipe, XenMobile processes the policy on the device the next time the device connects.

Define schedule - When enabled, XenMobile attempts to reconnect the user's device to the XenMobile server after a network connection loss and monitors the connection by transmitting control packets at regular intervals within the timeframe you define.

User example: You want to deploy a passcode policy to enrolled devices. The scheduling policy ensures that the devices connect back to the server at a regular interval to collect the new policy.

Credentials Policy

Why use this policy: Often used in conjunction with a WiFi policy, the Credentials policy lets you deploy certificates for authentication to internal resources that require certificate authentication.

User example: You deploy a WiFi policy that configures a wireless network on the device. The WiFi network requires a certificate for authentication. The Credentials policy deploys a certificate that is then stored in the operating system keystore. The user can then select the certificate when connected to the internal resource.

Exchange policy

Why use this policy: With XenMobile, you have two options to deliver Microsoft Exchange ActiveSync email.

Secure Mail app - Deliver email by using the Secure Mail app that you distribute from the public app store or the XenMobile Store.

Native emal app - Use the Exchange policy to enable ActiveSync email for the native email client on the device. With the Exchange policy for native email, you can use macros to populate the user data from their Active Directory attributes, such as ${user.username} to populate the user name and ${user.domain} to populate the user domain.

User example: When you push the Exchange policy, you send Exchange Server details to the device. Secure Hub then prompts the user to authenticate and email begins to sync.

Location policy

Why use this policy: The Location policy lets you geolocate devices on a map, if the device has GPS enabled for Secure Hub. After you deploy this policy and then send a locate command from the XenMobile server, the device responds back with the location coordinates.

User example: When you deploy the location policy and GPS is enabled on the device, if users misplace their device, they can log on to the XenMobile Self Help Portal and choose the locate option to see the location of their device

© 1999-2017 Citrix Systems, Inc. All rights reserved.

on a map. Note that the user makes the choice to allow Secure Hub to use location services. You cannot enforce the use of location services when users enroll a device themselves. Another consideration for using this policy is the effect on battery life.

Passcode policy

Why use this policy: The passcode policy allows you to enforce a PIN code or password on a managed device. This passcode policy allows you to set the complexity and time-outs for the passcode on the device.

User example: When you deploy a passcode policy to a managed device, Secure Hub prompts the user to configure a passcode or PIN, which they must unlock before they can gain access to their device when they turn on the device or when the inactivity timer expires.

Profile removal policy

Why use this policy: Suppose that you deploy a policy to a group of users and later need to remove that policy from a subset of the users. You can remove the policy for selected users by creating a Profile removal policy and using deployment rules to deploy the Profile removal policy only to specified user names.

User example: When you deploy a Profile removal policy to user devices, users might not notice the change. For example, if the Profile removal policy removes a restriction that disabled the device camera, the user won't know that camera use is now allowed. Consider letting users know when changes affect their user experience.

Restrictions policy

Why use this policy: The restriction policy gives you many options to lock down and control features and functionality on the managed device. You can enable hundreds of restriction options for supported devices, from disabling the camera or microphone on a device to enforcing roaming rules and access to third-party services like app stores.

User example: If you deploy a restriction to an iOS device, the user may not be able to access iCloud or the iTunes store.

Terms and conditions policy

Why use this policy: You might need to advise users of the legal implications of having their device managed. In addition, you may want to ensure that users are aware of the security risks when corporate data is pushed to the device. The custom Terms and Conditions document allows you to publish rules and notices before the user enrolls.

User example: A user sees the Terms and Conditions information during the enrollment process. If they decline to accept the conditions stated, the enrollment process ends and they cannot access corporate data. You can generate a report to provide to HR/Legal/Compliance teams to show who accepted or declined the terms.

VPN policy

Why use this policy: Use the VPN policy to provide access to backend systems using older VPN Gateway technology. The policy supports a number of VPN providers, including Cisco AnyConnect, Juniper, as well as Citrix VPN. It is also possible to link this policy to a CA and enabled VPN on-demand, if the VPN gateway supports this option.

User example: With the VPN policy enabled, a user's device opens a VPN connection when the user accesses an

© 1999-2017 Citrix Systems, Inc. All rights reserved.

internal domain.

Webclip policy

Why use this policy: Use the Webclip policy if you want to push to devices an icon that opens directly to a website. A webclip contains a link to a website and can include a custom icon. On a device a webclip looks like an app icon.

User example: A user can click on a webclip icon to open an internet site that provides services they need to access. Using a web link is more convenient than needing to open a browser app and type a link address.

WiFi policy

Why use this policy: The WiFi policy lets you deploy WiFi network details, such as the SSID, authentication data, and configuration data, to a managed device.

User example: When you deploy the WiFi policy, the device automatically connects to the WiFi network and authenticates the user so they can gain access to the network.

Windows Information Protection policy

Why use this policy: Use the Windows Information Protection (WIP) policy to protect against the potential leakage of enterprise data. You can specify the apps that require Windows Information Protection at the enforcement level you set. For example, you can block any inappropriate data sharing or warn about in appropriate data sharing and allow users to override the policy. You can run WIP silently while logging and permitting inappropriate data sharing

User example: Suppose that you configure the WIP policy to block inappropriate data sharing. If a user copies or saves a protected file to a non-protected location, a message similar to the following appears: You can't place work protected content in this location.

XenMobile Store policy

Why use this policy: The XenMobile Store is a unified app store where administrators can publish all the corporate apps and data resources needed by their users. An administrator can add Web apps, SaaS apps, MDX wrapped apps, Citrix productivity apps, native mobile apps such as .ipa or .apk files, iTunes and Google play apps, web links, and XenApp and XenDesktop apps published using Citrix StoreFront.

User example: After a user enrolls their device into XenMobile, they access the XenMobile Store through the Citrix Secure Hub app. The user can then see all the corporate apps and services available to them. Users can click on an app to install it, access the data, rate and review the app, and download app updates from the XenMobile Store.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

User Enrollment Options

Feb 21, 2018

Note: This section applies to XenMobile Service and XenMobile on-premises deployments.

You can have users enroll their devices in XenMobile in a number of ways. Before considering the specifics, you must decide if the devices in your environment will enroll in Enterprise mode (MDM+MAM), MDM mode, or MAM mode (also referred to as MAM-only mode). For more information about the management modes, see Management Modes.

At the highest level, there are four enrollment options:

- **Enrollment Invitation**: Send an enrollment invitation or invitation link to users.
- **Self Help Portal**: Set up a portal that users can visit to download Secure Hub and enroll their devices or send themselves an enrollment invitation.
- **Manual Enrollment**: Send out an email, handbook, or some other communication letting users know that the system is up and that they can enroll. Users then download Secure Hub and enroll their devices manually.
- **Enterprise**: Another option for device enrollment is through the Apple Device Enrollment Program (DEP) and Google Android for Work. Through each of these programs, you can purchase devices that are pre-configured and ready for employees to use. For more information, see Apple Device Enrollment Program (DEP) and Google Android for Work.

Enrollment Invitation

You can email an enrollment invitation to users with iOS, macOS, or Android devices. You can also send an installation link through SMTP or SMS to users with iOS, macOS, Android, or Windows devices. For more information, see Enroll devices.

If you choose to use the enrollment invitation method: You can choose from up to seven enrollment modes (depending on platform), and you can use any combination of the modes. You can enable or disable the modes from the XenMobile Settings page, and you can select a default from Username + Password, Two Factor, and Username + PIN. For information on each enrollment mode, see To configure enrollment modes in the XenMobile documentation.

If you choose certificate-based, consider excluding Username + Password traditional authentication from the allowed options, because this mode may expose a weak onboarding vector into your environment and potentially void the mandated security quality.

Invitations serve many purposes. The most common use of invitations is to notify users that the system is available, and that they can enroll. Invitation URLs are unique; once a user uses an invitation URL, the URL cannot be used again. You can use this property to limit the users or devices enrolling to your system.

You can set up XenMobile so that iOS users provide credentials during enrollment in one of the following ways:

- Users type their credentials during enrollment.
- Users insert a smart card from a derived credentials provider into a reader attached to their desktop. For information about derived credentials, see Derived credentials for iOS.

In the XenMobile console, you can also choose the option for Enrollment Profiles, through which you can control the number of devices specific users can enroll, based on Active Directory groups. For instance, if you want to allow your Finance division only one device per user, you can configure that scenario through enrollment profiles.

Be aware of the extra costs and pitfalls of certain enrollment options. If you want to send invitations using SMS, you need

© 1999-2017 Citrix Systems, Inc. All rights reserved.

to set up an additional infrastructure. For more information on this option, see Notifications in the XenMobile documentation.

In addition, if you plan to send invitations by email, ensure that users have a way of accessing email outside of Secure Hub. You may use one-time password (OTP) enrollment modes as an alternative to Active Directory passwords for MDM enrollment. Note that OTP is available on iOS and Android devices only and is not currently available on Windows devices.

Self Help Portal

Users can request an enrollment invitation through the Self Help Portal. The default mode is Username + Password, but you can also change that requirement to Two Factor or Username + PIN. For information about setting up the Self Help Portal, see To configure enrollment modes and the Self Help Portal in the XenMobile documentation.

Manual Enrollment

With manual enrollment, users connect to XenMobile either through autodiscovery or by entering the server information. With autodiscovery, users log on to the server with only their email address or Active Directory credentials in User Principal Name format. Without autodiscovery, they must enter the server address and their Active Directory credentials. For more information about setting up autodiscovery, see XenMobile Autodiscovery Service in the XenMobile documentation.

You can facilitate manual enrollment in a number of ways. You can create a guide, distribute it to users, and have them enroll themselves. You can have your IT department manually enroll groups of users in certain time slots. You can use any similar method where users must enter their credentials and/or server information.

User Onboarding

After you have your environment set up, you need to decide how to get users into your environment. An earlier section in this article discusses the specifics of user enrollment modes. This section discusses the way you reach out to users.

Open Enrollment vs. Selective Invitation

When onboarding users, you can allow enrollment through two basic methods: You can allow open enrollment in which, by default, any user with LDAP credentials and the XenMobile environment information can enroll. Or, you can limit the number of users by only allowing users with invitations to enroll. You can also limit open enrollment by Active Directory group.

With the invitation method, you can also limit the number of devices a user can enroll. In most situations, open enrollment is acceptable, but there are a few things to consider:

- If you are rolling out a MAM environment, you can easily limit enrollment through Active Directory group membership.
- With an MDM environment, the only way to limit enrollment is to limit the number of devices that can enroll based on Active Directory group membership. If you only allow corporate devices in your environment, this shouldn't be an issue. You may want to consider this method, however, in a BYOD workplace where you want to limit the number of devices in your environment.
- You also want to keep in mind whether you have user or device licenses. With user licenses, each user can have multiple devices and only one license is consumed. With device licenses, each device enrolled consumes one license.

Selective invitation is typically performed less often because it requires a bit more work than open enrollment. In order for users to enroll their devices in your environment, you must send an invitation unique to each user. For information on how to send an enrollment invite, see Sending an enrollment invitation in the XenMobile documentation.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

You'll need to send an invite for each user or group whom you want enrolled in your environment, which can take a long time depending on the size of your organization. It is possible to use Active Directory groups to create invitations in batches, but you must carry out this approach in waves.

First Contact with Users

When you have decided whether you want to use open enrollment or selective invitation and have set up those environments, you'll need to make users aware of their enrollment options.

If you use the selective invitation method, email and SMS messages are a part of the process. You can send emails through the XenMobile console for open enrollment as well. For details, see Sending an enrollment invitation in the XenMobile documentation.

In either case, keep in mind that for email, you need an SMTP server. For text messages, you need an SMS server. These may be extra costs to consider when making your decision. In addition, before you select a method, consider how you expect new users to access information, like email. If you want all users to access their email through XenMobile, sending them an invitation email would be problematic.

You may also send communication by another means outside of XenMobile for an open enrollment environment, as long as you include all the relevant information, such as where users can get the Secure Hub app and what method they should use to enroll. If you have autodiscovery turned off, you need to tell them the XenMobile server address as well. To learn more about autodiscovery, see XenMobile Autodiscovery Service in the XenMobile documentation.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Tuning XenMobile Operations

Feb 27, 2018

The performance and stability of XenMobile operations involves many settings across XenMobile and depends on your NetScaler and SQL Server database configuration. This article focuses on the settings that are most often configure, related to the tuning and optimization of XenMobile. Citrix recommends that you evaluate each of the settings in this article before deploying XenMobile.

> ## Important
>
> These guidelines assume that the XenMobile server CPU and RAM is adequate for the number of devices. For more information about scalability, see Scalability and performance in the XenMobile documentation.

The following server properties globally apply to operations, users, and devices across an entire XenMobile instance. Be aware that a change to some server properties requires a restart of each XenMobile server node. XenMobile notifies you when a restart is required.

These tuning guidelines apply to both clustered and non-clustered environments.

hibernate.c3p0.idle_test_period

- This XenMobile server property, a Custom Key, determines the idle time in seconds before a connection is automatically validated. Configure the key as follows. Default is **30**.

  Key: **Custom Key**
  Key: **hibernate.c3p0. idle_test_period**
  Value: **30**
  Display name: **hibernate.c3p0. idle_test_period**
  Description: **Hibernate idle test period**

hibernate.c3p0.max_size:

- This Custom Key determines the maximum number of connections that XenMobile can open to the SQL Server database. XenMobile uses the value you specify for this custom key as an upper limit. The connections open only if you need them. Base your settings on the capacity of your database server.

  Note the following equation in a clustered configuration. Your c3p0 connection multiplied by the number of nodes equals your actual maximum number of connections that XenMobile can open to the SQL Server database.

  In clustered and non-clustered configuration, setting the value too high with an undersized SQL Server can cause resource issues on the SQL side during peak load. Setting the value too low means you might not be able to take advantage of the SQL resources available.

  Configure the key as follows. Default is **1000**.

Key: **hibernate.c3p0.max_size**
Value: **1000**
Display name: **hibernate.c3p0.max_size**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Description: DB connections to SQL

hibernate.c3p0.min_size:

- This Custom Key determines the minimum number of connections that XenMobile opens to the SQL Server database. Configure the key as follows. Default is **100**.

  Key: **hibernate.c3p0.min_size**
  Value: **100**
  Display name: **hibernate.c3p0.min_size**
  Description: DB connections to SQL

hibernate.c3p0.timeout:

- This Custom Key determines the idle time-out. If you use database cluster failover, Citrix recommends that you add this Custom Key and set it to reduce the idle time-out. Default is **120**.

  Key: **Custom Key**
  Key: **hibernate.c3p0.timeout**
  Value: **120**
  Display name: **hibernate.c3p0.timeout**
  Description: Database idle timeout

Push Services Heartbeat Interval

- This setting determines how frequently an iOS device checks if an APNs notification is not delivered in the interim. Increasing the APNs heartbeat frequency can optimize database communications. Too large a value can add unnecessary load. This setting applies only to iOS. Default is **20** hours.

  If you have a large number of iOS devices in your environment, the heartbeat interval can lead to higher load than necessary. Security actions, such as selective wipe, lock, full wipe, and so on do not rely on this heartbeat, as an APNs notification is sent to the device when these actions are executed. This value governs how quickly a policy updates after Active Directory Group membership changes. As such, it is often suitable to increase this value to something between 12 and 20 hours to reduce load.

iOS MDM APNS Connection Pool Size

- An APNs connection pool that is too small can negatively affect APNs activity performance when you have more than 100 devices. Performance issues include slower deployment of apps and policies to devices and slower device registration. Recommended setting is **10** or up to the maximum number of APNs servers for your geographic location. Default is **10**.

auth.ldap.connect.timeout; auth.ldap.read.timeout

- To compensate for slow LDAP responses, Citrix recommends that you add server properties for the following Custom Keys.

  Key: **Custom Key**
  Key: **auth.ldap.connect.timeout**
  Value: **60000**
  Display name: **auth.ldap.connect.timeout**
  Description: **LDAP connection timeout**

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Key: **Custom Key**
Key: **auth.ldap.read.timeout**
Value: **60000**
Display name: **auth.ldap.read.timeout**
Description: **LDAP read timeout**

Other Server Optimizations

Server Property	Default Setting	Why Change This Setting?
Background Deployment	1440 minutes	The frequency for background policy deployments, in minutes. Applies only to always-on connections for Android devices. Increasing the frequency of policy deployments reduces server load. Recommended setting is **1440** (24 hours).
Background Hardware Inventory	1440 minutes	The frequency for background hardware inventory, in minutes. Applies only to always-on connections for Android devices. Increasing the frequency of hardware inventory reduces server load. Recommended setting is **1440** (24 hours).
Interval for check deleted Active Directory user	15 minutes	The standard sync time for Active Directory is **15** minutes. The value **0** prevents XenMobile from checking for deleted Active Directory users. Recommended setting is **15** minutes.
MaxNumberOfWorker	3	The number of threads used when importing a large number of VPP licenses. Defaults to **3**. If you need further optimization, you can increase the number of threads. However, be aware that with a larger number of threads, such as 6, a VPP import results in very high CPU usage.

Optimizing Deployment Scheduling for Android Devices

You can schedule deployments for Android devices using the Google Firebase Cloud Messaging (FCM, previously named Google Cloud Messaging) or XenMobile settings.

If using FCM to schedule deployments

Enabling FCM for your XenMobile environment allows for near real-time notifications to Android devices, similar to APNs for iOS devices. With FCM configured, when XenMobile needs to connect to a device for a policy update, selective wipe, and so on, the XenMobile server sends a notification message to the FCM server to forward the request to the client device. After the device receives the notification from FCM, the device connects back to XenMobile for further instructions. Keep in mind that this method relies on third-party servers (Google) and therefore is subject to service interruptions outside the control of your IT department or Citrix Support.

For information on how to register with the FCM service, refer to XenMobile and Firebase Cloud Messaging (FCM) Configuration.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

If using FCM for Android, be aware of the following XenMobile server properties. The properties still use the prior acronym for Google Cloud Messaging, GCM.

- **GCM API Key**: The key created in the Google Developers Console.
- **GCM Sender ID**: The Project Number in the Google Developers Console.
- **GCM Registration ID TTL**: The delay, in days, before renewing the device FCM registration ID. Defaults to **10**.
- **GCM Heartbeat Interval**: Defaults to **6** hours.

If using XenMobile settings to schedule deployments

To schedule deployments to Android devices, use these XenMobile settings:

- Set the **Connection Scheduling Policy** (a XenMobile device policy) to **Always**, which keeps the connection alive permanently. This enables you to deploy policies to delivery groups immediately. The open connection also enables the background services defined in the server properties **Background Deployment** and **Background Hardware Inventory** to occur per those property settings.
- Select the **Deployment Schedule** option **Deploy for always-on connection** in each policy deployed to the device.

> ## Nota
>
> For Android devices, setting the **Deployment condition** to **Only when previous deployment has failed** helps with device usage, because some devices overwrite the policy and some devices reset the policy. If a device resets the policy, XenMobile might prompt users for credentials every time a policy that requires authentication is re-deployed. Enabling this feature also helps with server load and prevents the success reported from bouncing between failed and success when XenMobile pushes the policy every time the device connects.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

App Provisioning and Deprovisioning

Feb 21, 2018

Application provisioning revolves around mobile app lifecycle management, which mainly consists of wrapping, configuring, delivering, and managing mobile apps within a XenMobile environment. In some instances, developing or modifying application code may also be part of the provisioning process. XenMobile is equipped with various tools and processes that you can use for app provisioning.

Before you read this article on app provisioning, it is recommended that you read the articles on Apps and User Communities. When you have finalized the type of apps your organization plans to deliver to users, you can then outline the process for managing the apps throughout their lifecycle.

Consider the following points when defining your app provisioning process:

- **App profiling**: Your organization may start with a limited number of apps; however, the number of apps you manage could rapidly increase as user adoption rates increase and your environment grows. You should define specific app profiles right from the beginning in order to make app provisioning easy to manage. App profiling helps you categorize apps into logical groups from a nontechnical perspective. For example, you can create app profiles based on the following factors:
  - Version: App version for tracking
  - Instances: Multiple instances that are deployed for different set of users, for example, with different levels of access
  - Platform: iOS, Android, or Windows
  - Target Audience: Standard users, departments, C-level executives
  - Ownership: Department that owns the app
  - Type: MDX, Public, Web and SaaS, or Web links
  - Upgrade Cycle: How often the app is upgraded
  - Licensing: Licensing requirements and ownership
  - MDX Policies: Wrapped or unwrapped with MDX security policies
  - Network Access: Type of access, such as secure browse or full VPN

Example:

Factor	Secure Mail	Secure Mail	In-House	Epic Rover
Version	10.1	10.1	X.x	X.x
Instance	VIP	Physicians	Clinical	Clinical
Platform	iOS	iOS	iOS	iOS
Target Users	VIP Users	Physicians	Clinical Users	Clinical Users
Ownership	IT	IT	IT	IT

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Type	MDX	MDX	Native	Public
Upgrade Cycle	Quarterly	Quarterly	Yearly	N/A
Licensing	N/A	N/A	N/A	VPP
MDX Policies	Yes	Yes	Yes	No
Network Access	VPN	VPN	VPN	Public

- **App versioning**: Maintaining and tracking app versions is a critical part of the provisioning process. Versioning is usually transparent to users. They only receive notifications when a new version of the app is available for download. From your perspective, reviewing and testing each app version in a non-production capacity is also critical in order to avoid production impact.

It is also important to evaluate if a specific upgrade is actually required. App upgrades are usually of two types: One is a minor upgrade, such as a fix to a specific bug; the second is a major release, which introduces significant changes and improvements to the app. In either case, you should carefully review the release notes of the app to evaluate if the upgrade is necessary.

- **App signing and wrapping**: With XenMobile, you can use MDX policies with managed apps to secure the corporate data through app wrapping. For more information about the MDX Toolkit for app wrapping, see MDX Toolkit in the XenMobile documentation. The app provisioning process for a wrapped app is significantly different from the provisioning process for a standard non-wrapped app.
- **App security**: You define security requirements of individual apps or app profiles as part of the provisioning process. You can map security requirements to specific MDM or MAM policies prior to deploying the apps, which greatly simplifies and expedites app deployment. You may deploy certain apps differently, or you may need to make architectural changes to your XenMobile environment depending on the type of security compliance that the apps require. For example, you may want the device to be encrypted in order to allow the use of a critical business intelligence app, or a certain app may require end-to-end SSL encryption or geo-fencing.
- **App delivery**: XenMobile allows you to deliver apps as MDM apps or as MAM apps. The MDM apps appear in the XenMobile Store. This store allows you to conveniently deliver public or native apps to users without controlling the app apart from enforcing device level restrictions. On the other hand, the MAM mode of delivering apps allows full control over app delivery and over the app itself. Delivering the apps in MAM mode is more suitable in most cases in which you have an on-premises XenMobile deployment with app management requirements along with MDM. When you deliver apps in MAM mode, the mobile device must be enrolled either into XME (MDM+MAM) or MAM-only mode.
- **Application maintenance**:
  - Perform an initial audit: You should keep track of the app version that is present in your production environment, as well as the last upgrade cycle. Make note of specific features or bug fixes that required the upgrade to take place.
  - Establish baselines: You should maintain a list of the latest stable release of each app. This app version should be fall back in case unexpected issues occur post upgrade. You should also device a rollback plan. You should test app upgrades in a test environment prior to your production deployment; if possible, you should deploy the upgrade to a subset of production users first and then to the entire user base.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

- Subscribe to Citrix software update notifications and any third-party software vendor notifications: This is critical in order to keep up to date with the latest release of the apps. In some cases, an early access release (EAR) build may also be available for testing ahead of time.
- Devise a strategy to notify users: You should define a strategy to notify users when app upgrades are available. Prepare users with training prior to deployment. You may send multiple notifications prior to updating the apps. Depending on the app, the best notification method might be email notifications or web sites.

App lifecycle management represents the completed lifecycle of an app from its initial deployment through the retirement of the app. The lifecycle of an app can be broken down into these five phases:

1. Requirements for specifications: Start with business case and user requirements.
2. Development: Validate that the app meets business needs.
3. Testing: Identify test users, issues, and bugs.
4. Deployment: Deploy the app to production users.
5. Maintenance: Update app version. Deploy the app in a test environment before updating the app in a production environment.

Application Lifecycle Example Using Secure Mail

1. Requirements for specifications: As a security requirement, you require a mail app that is containerized and supports MDX security policies.
2. Development: Validate that the app meets business needs. You must be able to apply MDX policy controls to the app.
3. Testing: Assign Secure Mail to a test users group and deploy the corresponding MDX file from the XenMobile Server. The test users validate that they can successfully send and receive email, and have calendar and contact access. The test users also report issues and identify bugs. Based on the test users' feedback you optimize Secure Mail configuration for production use.
4. Deployment: When the testing phase is complete, you assign Secure Mail to production users and deploy the corresponding MDX file from XenMobile Server.
5. Maintenance: A new update to Secure Mail is available. You download the new MDX file from Citrix downloads and replace the existing MDX file on the XenMobile Server. Instruct the users to perform the update. Note: Citrix recommends that you complete and test this process in a test environment before uploading the app to a XenMobile production environment and deploying the app to users.

For more information, see Wrapping iOS Mobile Apps and Wrapping Android Mobile Apps in the XenMobile documentation.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Dashboard-Based Operations

Feb 21, 2018

You can view information at a glance by accessing your XenMobile console dashboard. With this information, you can see issues and successes quickly by using widgets.

The dashboard is usually the screen that appears when you first sign on to the XenMobile console. To access the dashboard from elsewhere in the console, click **Analyze**. Click **Customize** on the dashboard to edit the layout of the page and to edit the widgets that appear.

- **My Dashboards**: You can save up to four dashboards. You can edit these dashboards separately and view each one by selecting the saved dashboard.
- **Layout Style**: In this row, you can select how many widgets appear on your dashboard and how the widgets are laid out.
- **Widget Selection**: You can choose which information appears on your dashboard.
  - **Notifications**: Mark the check box above the numbers on the left to add a Notifications bar above your widgets. This bar shows the number of compliant devices, inactive devices, and devices wiped or enrolled in the last 24 hours.
  - **Devices By Platform**: Displays the number of managed and unmanaged devices by platform.
  - **Devices By Carrier**: Displays the number of managed and unmanaged devices by carrier. Click each bar to see a breakdown by platform.
  - **Managed Devices By Platform**: Displays the number of managed devices by platform.
  - **Unmanaged Devices By Platform**: Displays the number of unmanaged devices by platform. Devices that appear in this chart may have an agent installed on them, but have had their privileges revoked or have been wiped.
  - **Devices By ActiveSync Gateway Status**: Displays the number of devices grouped by ActiveSync Gateway status. The information shows Blocked, Allowed, or Unknown status. You can click each bar to break down the data by platform.
  - **Devices By Ownership**: Displays the number of devices grouped by ownership status. The information shows corporate-owned, employee-owned, or unknown ownership status.
  - **Android TouchDown License Status**: Displays the number of devices that have a TouchDown license.
  - **Failed Delivery Group Deployments**: Displays the total number of failed deployments per package. Only packages that have failed deployments appear.
  - **Devices By Blocked Reason**: Displays the number of devices blocked by ActiveSync
  - **Installed Apps**: By using this widget, you can type an app name, and a graph displays information about that app.
  - **VPP Apps License Usage**: Displays license usage statistics for Apple Volume Purchase Program apps.

Use Cases

Some examples for the many ways you can use dashboard widgets to monitor your environment are as follows.

- You have deployed XenMobile Apps and are receiving support tickets regarding XenMobile Apps failing to install on devices. Use the **Out of Compliance Devices** and **Installed Apps** widgets to see the devices that do not have XenMobile Apps installed.
- You'd like to monitor inactive devices so that you can remove the devices from your environment and reclaim licenses. Use the **Inactive Devices** widget to track this statistic.
- You are receiving support tickets concerning data not being synced properly. You may want to use the **Devices by ActiveSync Gateway Status** and **Devices By Blocked Reason** widgets to determine whether the issue is ActiveSync related.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Reporting

After your environment is setup and users enroll, you can run reports to learn about your deployment. XenMobile comes with a number of reports built in to help you get a better picture of the devices running on your environment. For details, see Reports in the XenMobile documentation.

Important: Although it is possible to use SQL Server to create custom reports, Citrix does not recommend this method. Using the SQL Server database in this manner may have unforeseen consequences in your XenMobile deployment. If you do decide to pursue this method of reporting, ensure that SQL queries are run using a read-only account.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Role-Based Access Control and XenMobile Support

Feb 21, 2018

XenMobile uses role-based access control (RBAC) to restrict user and group access to XenMobile system functions, such as the XenMobile console, Self Help Portal, Remote Support, and public API. This article describes the roles built in to XenMobile and includes considerations for deciding on a support model for XenMobile that leverages RBAC.

Built-In Roles

You can change the access granted to the following built-in roles and you can add roles. For the full set of access and feature permissions associated with each role and their default setting, download Role-Based Access Control Defaults from the XenMobile documentation. For a definition of each feature, see Configure roles with RBAC in the XenMobile documentation.

Roles	Default Access Granted	Considerations
Admin	Full system access except to the Self-Help Portal and Remote Support. By default, administrators can perform some support tasks, such as check connectivity and create support bundles.	Do some or all of your administrators need access to the Self-Help Portal or Remote Support? If so, you can edit the Admin role or add Admin roles. To restrict access further for some administrators or administrator groups, add roles based on the Admin template and edit the permissions.
Device Provisioning	Access to the XenMobile console to perform basic administration on Windows CE devices: add, change, and remove devices; use the Settings page.	The Device Provisioning role applies only to Windows CE devices.
Support	Access to Remote Support.	For on-premises XenMobile Server deployments: Remote support enables your help desk representatives to take remote control of managed Windows CE and Android mobile devices. Screen cast is supported on Samsung KNOX devices only. Remote support isn't available to XenMobile Service customers and isn't supported for clustered on-premises XenMobile Server deployments.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

User	Access to the Self-Help Portal, which lets authenticated users generate enrollment links. The links allow them to enroll their devices or send themselves an enrollment invitation. Restricted access to the XenMobile console: device features (such as wipe, lock/unlock device; lock/unlock container; see location and set geographic restrictions; ring the device; reset container password); add, remove, and send enrollment invitations.	The User role enables you to enable users to help themselves. To support shared devices, create a user role for shared device enrollment.

Considerations for a XenMobile Support Model

The support models that you can adopt can vary widely and might involve third parties who handle level 1 and 2 support while employees handle level 3 and 4 support. Regardless of how you distribute the support load, keep in mind the considerations in this section specific to your XenMobile deployment and user base.

Do users have corporate-owned or BYO devices?
The primary question that influences support is who owns the user devices in your XenMobile environment. If your users have corporate-owned devices, you might offer a lower level of support, as a way to lock down the devices. In that case, you might provide a help desk that assists users with device issues and how to use the devices. Depending on the types of devices you need to support, consider how you might use the RBAC Device Provisioning and Support roles for your help desk.

If your users have BYO devices, your organization might expect users to find their own sources for device support. In that case, the support your organization provides is more of an administrative role focused around XenMobile-specific issues.

What is your support model for desktops?
Consider whether your support model for desktops is appropriate for other corporate-owned devices. Can you use the same support organization? What additional training will they need?

Do you want to give users access to the XenMobile Self Help Portal?
Although some organizations prefer not to grant users access to XenMobile, giving users some self-support capabilities can ease the load on your support organization. If the default User role for RBAC includes permissions that you don't want to grant, consider creating a new role with only the permissions you want to include. You can create as many roles as needed to meet your requirements.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Systems Monitoring

Feb 21, 2018

To ensure optimal uptime for app access and connectivity, you should monitor the following core components in the XenMobile environment:

XenMobile server

XenMobile server generates and stores logs on local storage that you can also export to a systems log (syslogs) server. You can configure log settings to specify size constraints, log level, or you can create custom loggers to filter specific events. You can look at XenMobile server logs from the XenMobile console at any time. You can also export information in the logs via the syslog server to your production Splunk logging servers.

The following list describes the different types of log files available in XenMobile:

Debug log file: Contains debug level information about core web services of XenMobile, including error messages and server-related actions.

Message format:

<date> <timestamp> <loglevel> <class name (including the package)> - <id> <log message>

- where <id> is a unique identifier like sessionID.
- where <log message> is the message supplied by the application.

Admin audit log file - Contains audit information about activity on the XenMobile console.

Note: The same format is used for both admin audit and user audit logs.

Message format:

With the exception of required Date and Timestamp values, all other attributes are optional. Optional fields are represented with " " in the message.

<date> <timestamp> "<username/id>" "<sessionid>" "<deviceid>" "<clientip>" "<action>" "<status>"

"<application name>" "<app user id>" "<user agent>" "<details>"

The following table lists the available admin audit log events:

Admin Audit Log Messages	
Event	**Status**
Login	success/failure
Logout	success/failure
Getadmin	success/failure

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Event	Status
Get application	success/failure
Add application	success/failure
Update application	success/failure
Delete application	success/failure
Bind application	success/failure
Unbind application	success/failure
Disable application	success/failure
Enable application	success/failure
Get category	success/failure
Add category	success/failure
Update category	success/failure
Delete category	success/failure
Add certificate	success/failure
Delete certificate	success/failure
Active certificate	success/failure
Self-sign certificate	success/failure
CSR certificate	success/failure
Export certificate	success/failure
Delete certificate chain	success/failure
Add certificate chain	success/failure
Get connector	success/failure
Add connector	success/failure
Delete connector	success/failure
Update connector	success/failure
Get device	success/failure

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Event	Status
Unlock device	success/failure
Wipe device	success/failure
Unwipe device	success/failure
Delete device	success/failure
Get role	success/failure
Add role	success/failure
Update role	success/failure
Delete role	success/failure
Bind role	success/failure
Unbind role	success/failure
Update config settings	success/failure
Update workflow email	success/failure
Add workflow	success/failure
Delete workflow	success/failure
Add Active Directory	success/failure
Update Active Directory	success/failure
Add masteruserlist	success/failure
Update masteruserlist	success/failure
Update DNS	success/failure
Update Network	success/failure
Update log server	success/failure
Transfer log from log server	success/failure
Update syslog	success/failure
Update receiver updates	success/failure
Update time server	success/failure
Update trust	success/failure

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Event	Status
Add service record	success/failure
Update service record	success/failure
Update receiver email	success/failure
Upload patch	success/failure
Import snapshot	success/failure
Fetch app store app details	success/failure
Update MDM	success/failure
Delete MDM	success/failure
Add HDX	success/failure
Update HDX	success/failure
Delete HDX	success/failure
Add Branding	success/failure
Delete Branding	success/failure
Update SSL offload	success/failure
Add account property	success/failure
Delete account property	success/failure
Update account property	success/failure
Add beacon	success/failure

User audit log file: Contains information related to the user activity from enrolled devices.

Note: The same format is used for both user audit and admin audit logs.

Message format:

With the exception of required Date and Timestamp values, all other attributes are optional. Optional fields are represented with " " in the message. For example,

<date> <timestamp> " <username/id>" "<sessionid>" "<deviceid>" "<clientip>" "<action>" "<status>" " <application name>" " <app user id>" "<user agent>" "<details>"

The following table lists the available user audit log events:

© 1999-2017 Citrix Systems, Inc. All rights reserved.

User Audit Log Messages	
Event	**Status**
Login	success/failure
Session time-out	success/failure
Subscribe	success/failure
Unsubscribe	success/failure
Pre-launch	success/failure
AGEE SSO	success/failure
SAML Token for ShareFile	success/failure
Device registration	success/failure
Device check	lock/wipe
Device update	success/failure
Token refresh	success/failure
Secret saved	success/failure
Secret retrieved	success/failure
User initiated change password	success/failure
Mobile client download	success/failure
Logout	success/failure
Discovery Service	success/failure
Endpoint Service	success/failure
MDM Functions	
REGHIVE	success/failure
Cab inventory	success/failure
Cab	success/failure

© 1999-2017 Citrix Systems, Inc. All rights reserved.

MDM Functions	
Cab shell install	success/failure
Cab create folder	success/failure
Cab file get	success/failure
File create folder	success/failure
File get	success/failure
File sent	success/failure
Script create folder	success/failure
Script get	success/failure
Script sent	success/failure
Script shell execution	success/failure
Script auto execution	success/failure
APK inventory	success/failure
APK	success/failure
APK shell install	success/failure
APK auto install	success/failure
APK create folder	success/failure
APK file get	success/failure
APK App	success/failure
EXT App	success/failure
List get	success/failure
List sent	success/failure
Locate device	success/failure
CFG	success/failure
Unlock	success/failure
SharePoint wipe	success/failure
SharePoint Configuration	success/failure

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Remove profile	success/failure
MDM Functions	
Remove application	success/failure
Remove unmanaged application	success/failure
Remove unmanaged profile	success/failure
IPA App	success/failure
EXT App	success/failure
Apply redemption code	success/failure
Apply settings	success/failure
Enable tracking device	success/failure
App management policy	success/failure
SD card wipe	success/failure
Encrypted email attachment	success/failure
Branding	success/failure
Secure browser	success/failure
Container browser	success/failure
Container unlock	success/failure
Container password reset	success/failure
AG client auth creds	success/failure

NetScaler also monitors the XenMobile web service state, which is configured with intelligent monitoring probes to simulate HTTP requests to each XenMobile server cluster node. The probes determine whether the service is online and then respond based on the response received. In the event that a node does not respond as expected, NetScaler marks the server as down. In addition, NetScaler takes the node out of the load-balancing pool and logs the event for use in generating alerts through the NetScaler monitoring solution.

You can also use standard hypervisor monitoring tools to monitor the XenMobile virtual machines and to provide relevant alerts regarding CPU, memory, and storage utilization metrics.

SQL Server and database

SQL Server and database performance directly affects XenMobile services. The XenMobile instance requires access to the database at all times and goes offline (for example, stops responding) in the event of an outage to the SQL infrastructure. The XenMobile console may continue to function for a while following any disk space issues with SQL Server. To ensure maximum database uptime and adequate performance for the XenMobile workload, you should proactively monitor the

© 1999-2017 Citrix Systems, Inc. All rights reserved.

state of your SQL Servers following Microsoft recommendations. Additionally, you should adjust resource allocation for CPU, memory, and storage to guarantee service level agreements as your XenMobile environment continues to grow.

NetScaler

NetScaler provides the ability to log metrics to internal storage or to send logs to an external logging server. You can configure the syslog server to export NetScaler logs to your production Splunk logging servers. The following logging levels are available in NetScaler:

- Emergency
- Alert
- Critical
- Error
- Warning
- Information

The log files are also stored in NetScaler storage in the /var/log/ns.log directory and named newnslog. NetScaler rolls over and compresses the files by using the GZIP algorithm. Log file names are newnslog.xx.gz, where xx represents a running number.

NetScaler also supports SNMP traps and alerts as a monitoring option. The following table lists the SNMP traps recommended for the environment.

NetScaler SNMP traps	
Configuration	**Setting**
cpuUtilization 1.3.6.1.4.1.5951.1.1.0.3	This trap indicates that the CPU utilization has exceeded the high threshold.
averageCpuUtilization 1.3.6.1.4.1.5951.1.1.0.51	This trap indicates that the average CPU usage in the multi-processor NetScaler system has exceeded the high threshold.
memoryUtilization 1.3.6.1.4.1.5951.1.1.0.13	This trap is sent when the memory utilization of the system exceeds the threshold value.
netScalerLoginFailure 1.3.6.1.4.1.5951.1.1.0.55	This trap is sent when a logon attempt to NetScaler fails.
diskUsageHigh 1.3.6.1.4.1.5951.1.1.0.64	This trap indicates that disk usage has gone high.
haSyncFailure 1.3.6.1.4.1.5951.1.1.0.69	This trap indicates that configuration synchronization has failed on the secondary instance.
haNoHeartbeats 1.3.6.1.4.1.5951.1.1.0.70	This trap indicates that high availability heartbeats are not received from the secondary instance.
haBadSecState	This trap indicates that the secondary instance is in DOWN/UNKNOWN/STAY SECONDARY state.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuration	Setting
haPropFailure 1.3.6.1.4.1.5951.1.1.0.85	This trap indicates that configuration propagation has failed on the secondary instance.
ipConflict 1.3.6.1.4.1.5951.1.1.0.86	This trap indicates that an IP address conflict is present with another device in the network.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Disaster Recovery

Feb 21, 2018

You can architect and configure XenMobile deployments that include multiple sites for disaster recovery using an active-passive failover strategy.

The recommended disaster recovery strategy discuss in this article consists of:

- A single XenMobile active site in the datacenter of one geographical location serving all the enterprises users globally, known as the primary site.
- A second XenMobile site in the datacenter of a second geographical location, known as the disaster recovery site. This disaster recovery site provides active-passive site failover in if a site-wide datacenter failure occurs in the primary site. The primary site includes XenMobile, SQL database, NetScaler infrastructure in order to facilitate failover and provide users with access to XenMobile via the event of connectivity failure to the primary site.

The XenMobile servers at the disaster recovery site remains offline during normal operations and is brought online during only disaster recovery scenarios, where complete site failover from the primary site to the disaster recovery site is required. The SQL Servers at the disaster recovery site must be active and ready to service connections before you start the XenMobile servers at the disaster recovery site.

This disaster recovery strategy relies on manual failover of the NetScaler access tier by means of DNS changes for routing MDM and MAM connections to the disaster recovery site in the event of an outage.

> **Nota**
>
> To use this architecture, you must have a process in place for asynchronous backups of the databases and some way of ensuring high availability for the SQL infrastructure.

Disaster Recovery Failover Process

1. If you are testing your disaster recovery failover process, shut down XenMobile servers in the primary site to simulate site failure.
2. Change public DNS records for the XenMobile servers to point to the disaster recovery site's external IP addresses.
3. Change internal DNS record for the SQL Server to point to the disaster recovery site's SQL Server IP address.
4. Bring XenMobile SQL databases online at the disaster recovery site. Ensure that the SQL Server and database is active and ready to service connections from the XenMobile servers local to the site.
5. Turn on the XenMobile servers on the disaster recovery site.

XenMobile Server Update Process

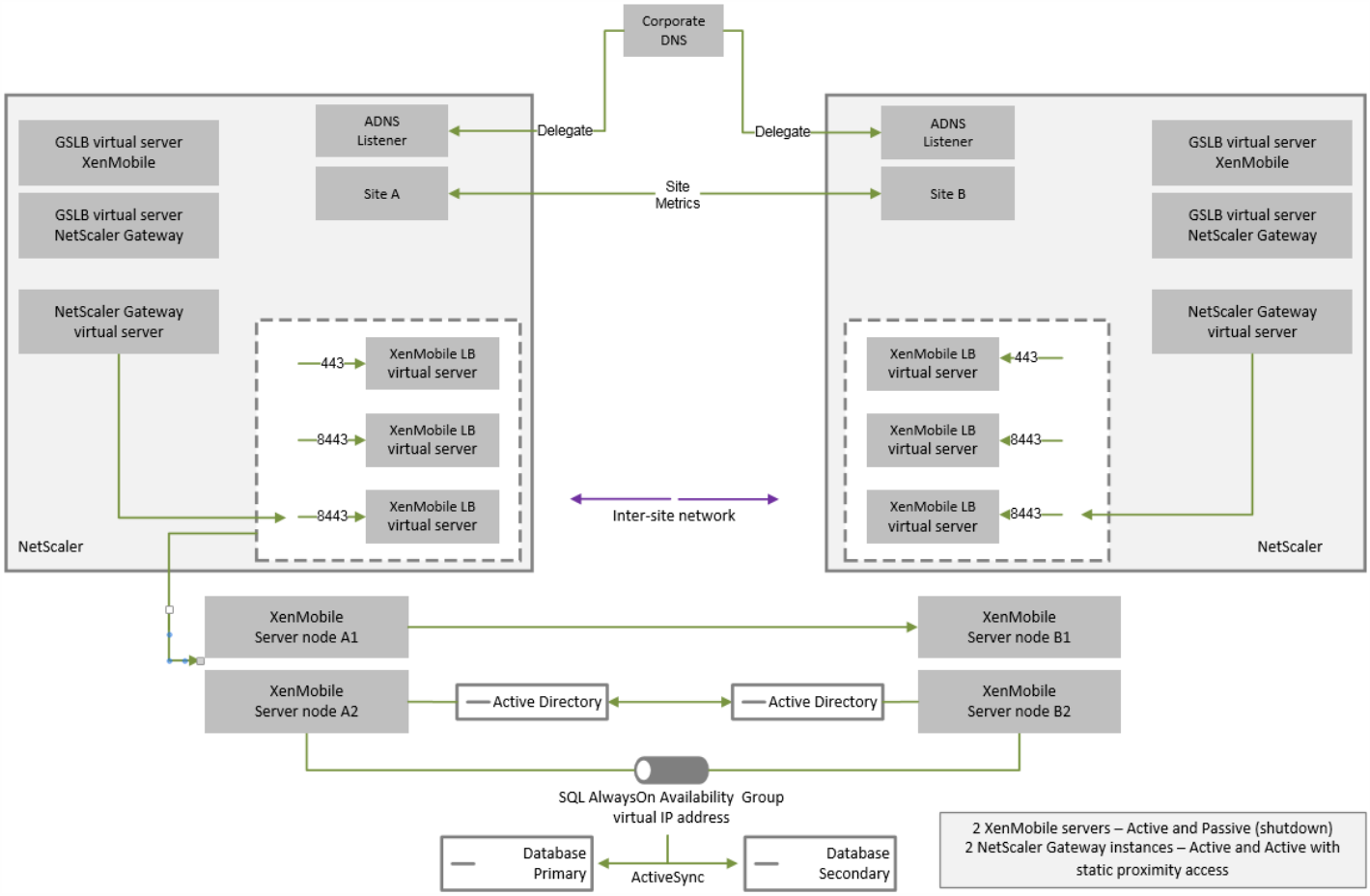
Follow these steps any time you update XenMobile with patches and releases, in order to keep the code of the primary and disaster recovery servers uniform.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

1. Ensure that XenMobile servers in primary site have been patched or upgraded.
2. Ensure that DNS record for the SQL Server is resolving to the active SQL Server database in the primary site.
3. Bring the disaster recovery site's XenMobile servers online. The servers connect to the primary site's database across the WAN during the upgrade process only.
4. Apply required patches and updates to all disaster recovery site's XenMobile servers.
5. Restart the XenMobile servers and confirm that the patch or upgrade is successful.

Disaster Recovery Reference Architecture Diagram

The following diagram shows the high-level architecture for a disaster recovery deployment of XenMobile.



GSLB for Disaster Recovery

A key element of this architecture is the use of Global Server Load Balancing (GSLB) to direct traffic to the correct data center.

By default, the NetScaler for XenMobile wizard configures NetScaler Gateway in a way that does not enable the use of GSLB for disaster recovery. Therefore, you must take additional steps.

How GSLB Works

GSLB is at its core a form of DNS. Participating NetScaler appliances act as authoritative DNS servers and resolve DNS

© 1999-2017 Citrix Systems, Inc. All rights reserved.

records to the correct IP address (typically the VIP that is supposed to receive traffic). The NetScaler appliance checks the system health before responding to a DNS query directing traffic to that system.

When a record is resolved, GSLB's role in resolving the traffic is complete. The client communicates directly with the target virtual IP (VIP) address. DNS client behavior plays an important part on controlling how and when a record expires. This is largely outside the boundaries of the NetScaler system. As such, GSLB is subject to the same limitations as DNS name resolution. Clients cache responses; thus, load balancing in this way isn't as real-time as is traditional load balancing.

The GSLB configuration on NetScaler, including sites, services, and monitors, exist in order to provide the correct DNS name resolution.

The actual configuration for publishing servers (in this scenario, the configuration that the NetScaler for XenMobile wizard creates) is not affected by the GSLB. GSLB is a separate service on the NetScaler.

Challenges with Domain Delegation When Using GSLB with XenMobile

The NetScaler for XenMobile wizard configures NetScaler Gateway for XenMobile. This wizard generates three load balancing virtual servers and a NetScaler Gateway virtual server.

Two of the load balancing virtual servers handle MDM traffic, on port 443 and 8443. NetScaler Gateway receives MAM traffic and forwards it to the third server, the MAM load balancing virtual server, on port 8443. All traffic to the MAM load balancing virtual server is passed through NetScaler Gateway.

The MAM load balancing virtual server requires the same SSL certificate as the XenMobile servers and uses the same FQDN as used to enroll devices. The MAM load balancing server also uses the same port (8443) as one of the MDM load balancing servers. To enable traffic to be resolved, the NetScaler for XenMobile wizard creates a local DNS record on NetScaler Gateway. The DNS record matches the FQDN used to enroll devices.

This configuration is effective when the XenMobile server URL is not a GSLB domain URL. If a GSLB domain URL is used as the XenMobile server URL, as is required for disaster recovery, the local DNS record prevents NetScaler Gateway from resolving traffic to the MDM load balancing servers.

Using the CNAME Method for GSLB Disaster Recovery

To address the challenges presented by the default configuration created by the NetScaler for XenMobile wizard, you can create a CNAME record for the XenMobile server FQDN in the parent domain (company.com) and point a record in the delegated subzone (gslb.company.com) for which NetScaler is authoritative. Doing so allows for the creation of the static DNS A record for the MAM load balancing VIP address required to resolve traffic.

1. On the external DNS, create a CNAME for the XenMobile server FQDN that points to the GSLB domain FQDN on NetScaler GSLB. You need two GSLB domains: one for MDM traffic and another for MAM (NetScaler Gateway) traffic.

Example: CNAME = xms.company.com IN CNAME xms.gslb.comany.com

2. On the NetScaler Gateway instance of each site, create a GSLB virtual server with a FQDN that is what the CNAME record is pointing to.

Example: bind gslb vserver xms-gslb -domainName xms.gslb.company.com

When using the NetScaler for XenMobile wizard to deploy NetScaler Gateway, use the XenMobile server URL when configuring the MAM load balancing server. This creates a static DNS A record for the XenMobile server URL.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

3. Test with clients enrolling on Secure Hub using the XenMobile server URL (xms.company.com).

This example uses the following FQDNs:

- xms.company.com is the URL that is used by the MDM traffic and is used by devices enrolling, which is configured in this example by using the NetScaler for XenMobile wizard.
- xms.gslb.company.com is the GSLB domain FQDN for the XenMobile server.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Citrix Support Process

Feb 21, 2018

You can turn Citrix Technical Support Services to help with issues related to Citrix products. The group offers workarounds and resolutions and works hand in hand with development teams to offer solutions.

Citrix Consulting Services or Citrix Education Services offer help related to product training, advice on product usage, configuration, installation, or environment design and architecture.

Citrix Consulting helps with Citrix product-related projects, including proof of concepts, economic impact assessment, infrastructure health checks, design requirements analysis, architecture design verification, integration, and operational process development.

Citrix Education offers best-in-class IT training and certification on Citrix Virtualization, Cloud, and networking technologies.

Citrix recommends that you take full advantage of the Citrix Self-Help Resources and recommendations before creating a support case. For instance, there are several places where you can access articles and bulletins written by Citrix technical experts, see product documentation for Citrix solutions and technologies, or read straight talk from Citrix executives, product teams, and technical experts. See the Knowledge Center, Product documentation, and Blogs pages respectively.

For more interactive assistance, you can participate in discussion forums where you can ask questions and get real-world answers from other customers, share ideas, opinions, technical information, and best practices within user groups and interest groups, or interact with Citrix Support engineers who monitor Citrix Support social networking sites. See the Support Forums, Citrix Community, and Citrix Support on Twitter pages respectively.

You also have access to training and certification courses to build your skills. See Citrix Education.

Citrix Insight Services provides a simple, online troubleshooting platform and health-checker for your Citrix environment. Available for XenMobile, XenDesktop, XenServer, XenApp, and NetScaler. See Analysis Tool.

To seek technical support, you can create a support case either by phone or via the web. You can use the web for low- and medium-severity issues and use the phone option for high-severity issues. For information on contacting support for XenMobile issues, see How to Contact Support.

If you seek a highly trained single point of contact with extensive experience delivering Citrix solutions, Citrix Services offers a Technical Relationship Manager. For more information about Citrix services offering and benefits, see Citrix Worldwide Services.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Sending group enrollment invitations in XenMobile

John Bartel III , | Feb 21, 2018

You can send enrollment invitations to groups in XenMobile. You can send invitations to your nested groups as well. When setting up the group invitation, you can specify one or multiple device platforms. You can also tag devices so that you can, for example, distinguish corporate-owned devices from employee-owned devices. Then, you set the authentication type for user devices.

> **Nota**
>
> If you plan to use custom notification templates, you must set up the templates before you configure enrollment modes. For more information about notification templates, see Creating or Updating Notification Templates.

For more information on basic configurations on user accounts, roles, and enrollment modes and invitations, see User accounts, roles, and enrollment.

General steps

1. Within the XenMobile console, navigate to **Manage** > **Enrollment Invitations.**
2. Click **Add** toward the upper left of the screen and then click **Add Invitation.**
3. Click **Group** from the **Recipient** menu.

   This step lets you choose one or multiple platforms. If you have a mix of different operating system platforms within your company, choose all platforms. Only clear the platform selection if you are sure that no users are using the particular platform.
4. You can choose to tag devices during the invite process. Choose **Corporate** or **Employee**.

   Tagging makes it easy to separate corporate-owned devices and employee-owned devices.
5. In the **Domain** list, choose the domain in which the group exists.
6. In the **Group** list, select the Active Directory group you want to send the invites to.
7. The **Enrollment mode** allows you to set the type of authentication you prefer for users.
   - User name + Password
   - High Security
   - Invitation URL
   - Invitation URL + PIN
   - Invitation URL + Password
   - Two Factor
   - User name + PIN
8. For the **Agent Download, Enrollment URL**, **Enrollment PIN,** and **Enrollment Confirmation** templates, choose the custom notification template that you have created in the past. Or, choose the default that is listed.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

If you plan to use custom notification templates, you must set up the templates before you configure enrollment modes. For more information about notification templates, see Creating or Updating Notification Templates.

For these notification templates, use your configured SMTP server setup within XenMobile. Set your SMTP information first before proceeding.

> ## Nota
>
> You will note **Expire after** and **Maximum Attempts** options. These options change based on the **Enrollment mode** option that you choose. You cannot change these options.

9. Select ON for **Send invitation** and then click **Save and Send** to complete the process.

Nested group support

You can use nested groups to send invites. Typically, nested groups are used in large-scale environments where groups with similar permissions are bound to each other.

Navigate to **Settings** > **LDAP** and then enable the **Support nested group** option.

Troubleshooting and known limitations

Issue: Invites are being sent out to users even though they have been removed from an Active Directory group.

Solution: Depending on how large your Active Directory environment is, it could take up to six hours for changes to propagate to all servers. If a user or nested group is removed recently, XenMobile may still consider those users as a part of the group.

Therefore, it's best to wait up to six hours before sending out another group invite to your group.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuring an on-premises Device Health Attestation server

Sanket Mishra , | Mar 12, 2018

You can enable Device Health Attestation (DHA) for Windows 10 mobile devices through an on-premises Windows server. To enable DHA on-premises, you first configure a DHA server.

After you configure the DHA server, you create a XenMobile Server policy to enable the on-premises DHA service. For information on creating this policy, see Device Health Attestation device policy.

Prerequisites for a DHA server

- A server running Windows Server Technical Preview 5 or later, installed using the Desktop Experience installation option.
- One or more Windows 10 client devices. These devices must be have TPM 1.2 or 2.0 running the latest version of Windows.
- These certificates:
  - **DHA SSL certificate.** An x.509 SSL certificate that chains to an enterprise trusted root with an exportable private key. This certificate protects DHA data communications in transit including server to server (DHA service and MDM server) and server to client (DHA service and a Windows 10 device) communications.
  - **DHA signing certificate.** An x.509 certificate that chains to an enterprise trusted root with an exportable private key. The DHA service uses this certificate for digital signing.
  - **DHA encryption certificate.** An x.509 certificate that chains to an enterprise trusted root with an exportable private key. The DHA service also uses this certificate for encryption.
- Choose one of these certificate validation modes:
  - **EKCert.** EKCert validation mode is optimized for devices in organizations that are not connected to the Internet. Devices connecting to a DHA service running in EKCert validation mode do not have direct access to the Internet.
  - **AIKCert.** AIKCert Validation Mode is optimized for operational environments that do have access to the Internet. Devices connecting to a DHA service running in AIKCert validation mode must have direct access to the Internet and are able to get an AIK certificate from Microsoft.

Add the DHA server role to the Windows server

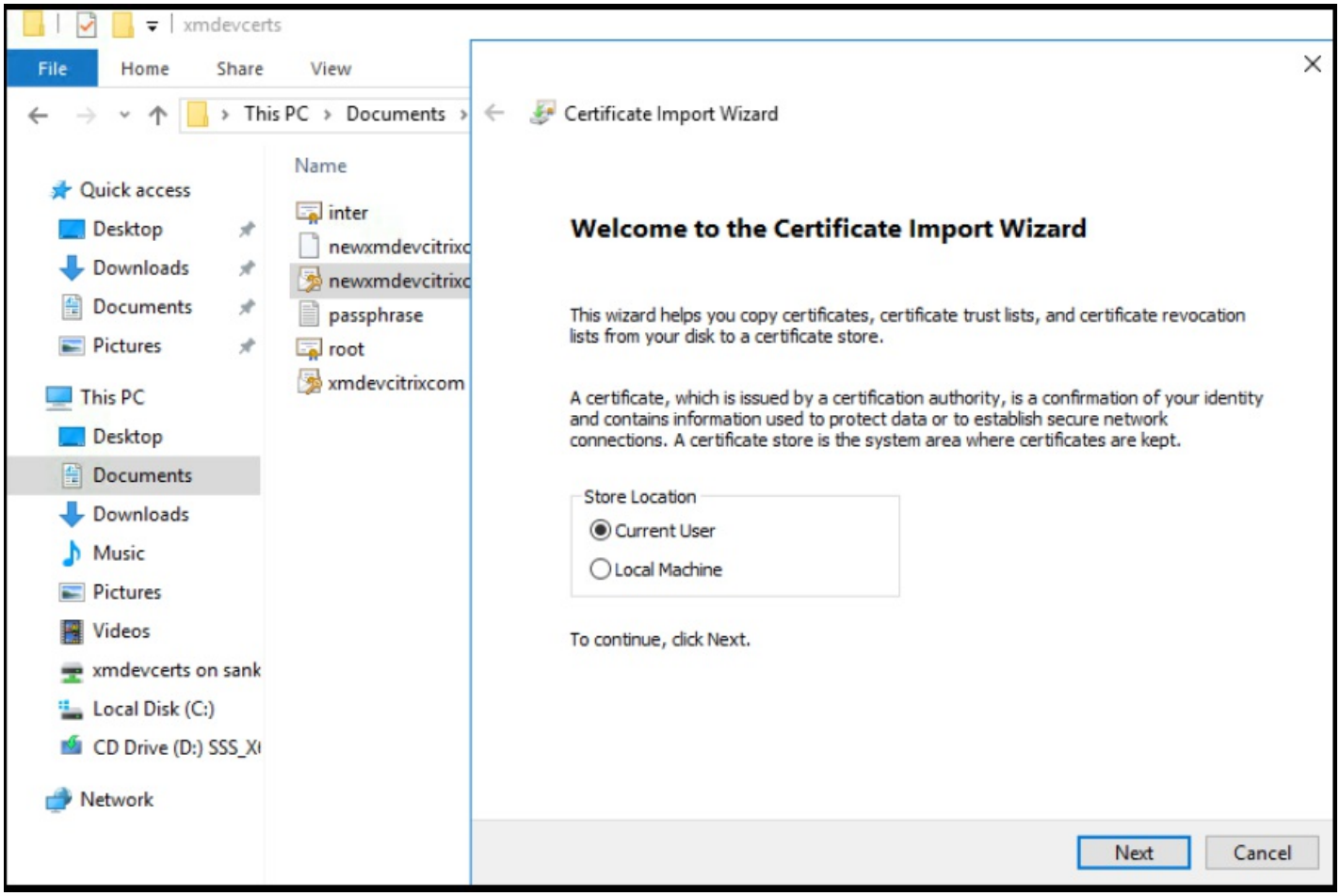
1. On the Windows server, if the Server Manager is not already open, click **Start** and then click **Server Manager**.
2. Click **Add roles and features**.
3. On the **Before you begin** page, click **Next**.
4. On the **Select installation type** page, click **Role-based or feature-based installation**, and then click **Next**.
5. On the **Select destination server** page, click **Select a server from the server pool**, select the server, and then click **Next**.
6. On the **Select server role**s page, select the Device Health Attestation check box.
7. Optional: Click **Add Features** to install other required role services and features.
8. Click **Next**.
9. On the **Select feature**s page, click **Next**.
10. On the **Web Server Role (IIS)** page, click **Next**.

 © 1999-2017 Citrix Systems, Inc. All rights reserved.

11. On the **Select role services** page, click **Next**.
12. On the **Device Health Attestation Service** page, click **Next**.
13. On the **Confirm installation selections** page, click **Install**.
14. When the installation is done, click **Close**.

Add the SSL certificate to the certificate store of the server

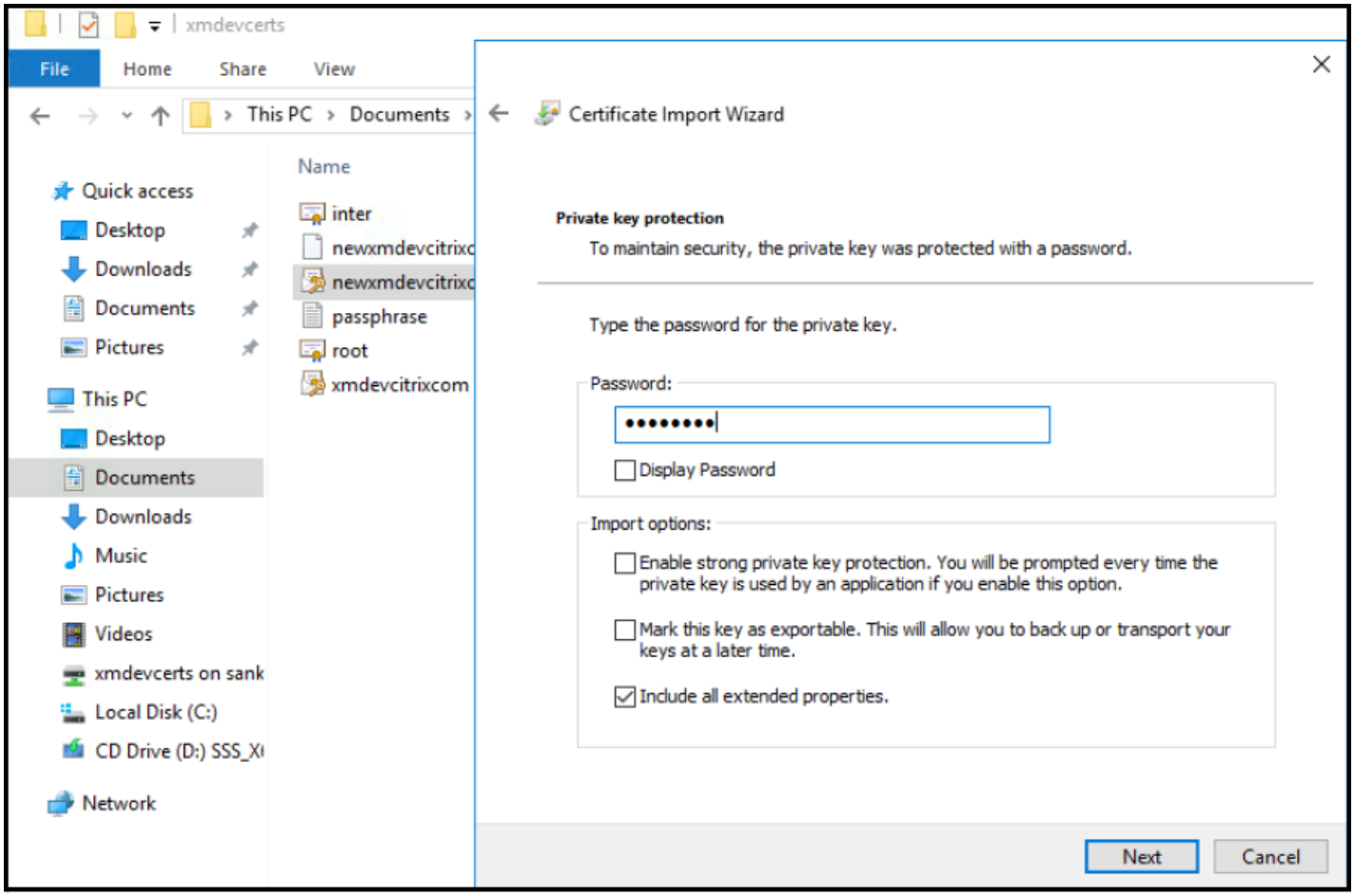
1. Go to the SSL certificate file and select it.
2. Select **Current user** as the store location and click **Next**.



3. Type the password for the private key.

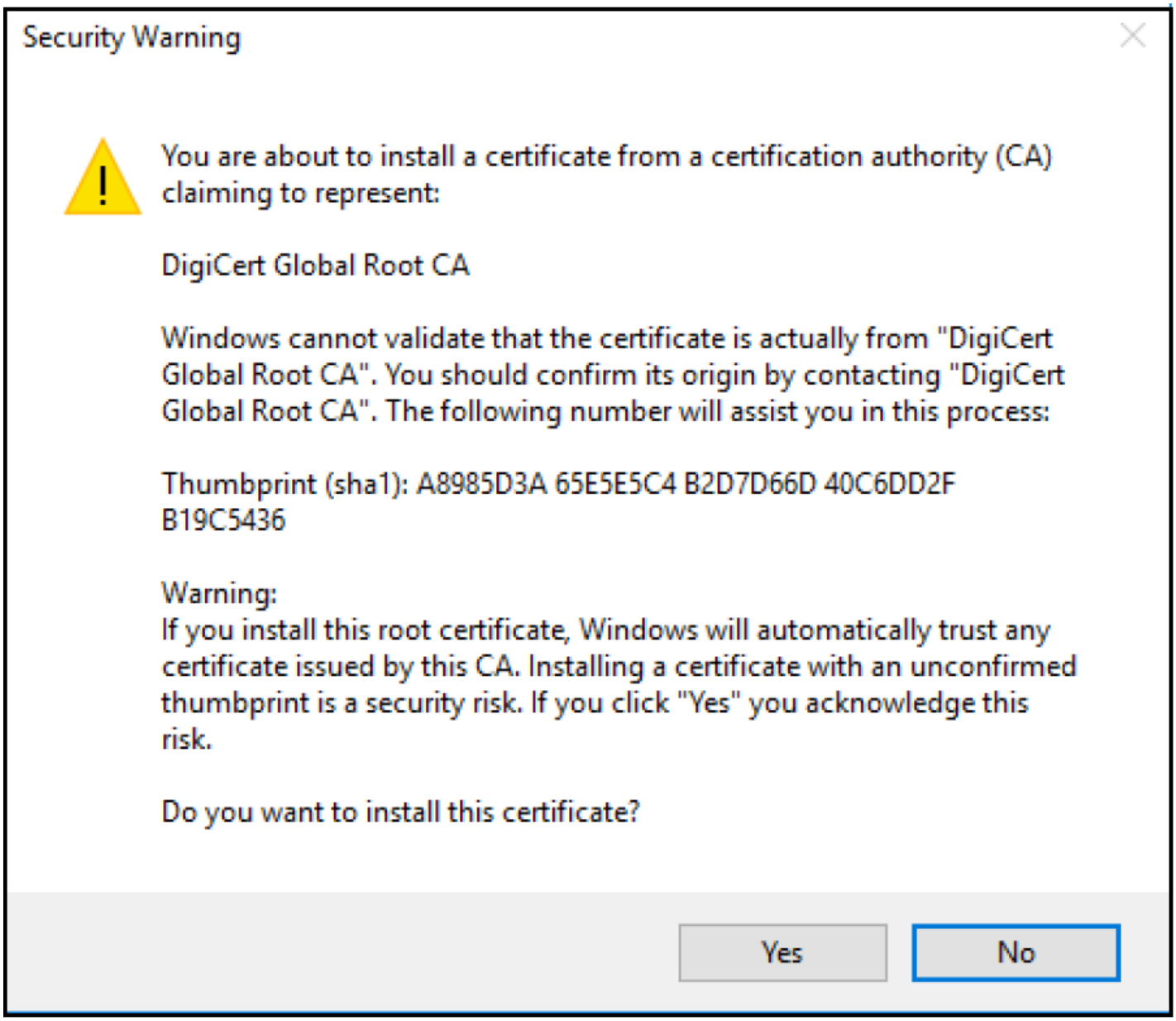
4. Ensure the import option **Include all extended properties** is selected. Click **Next**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



5. When this window appears, click **Yes**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



6. Confirm that the certificate is installed:

a. Open a Command Prompt window.

b. Type **mmc** and press the Enter key. To view certificates in the local machine store, you must be in the Administrator role.

c. On the File menu, click **Add/Remove Snap In**.

d. Click **Add**.

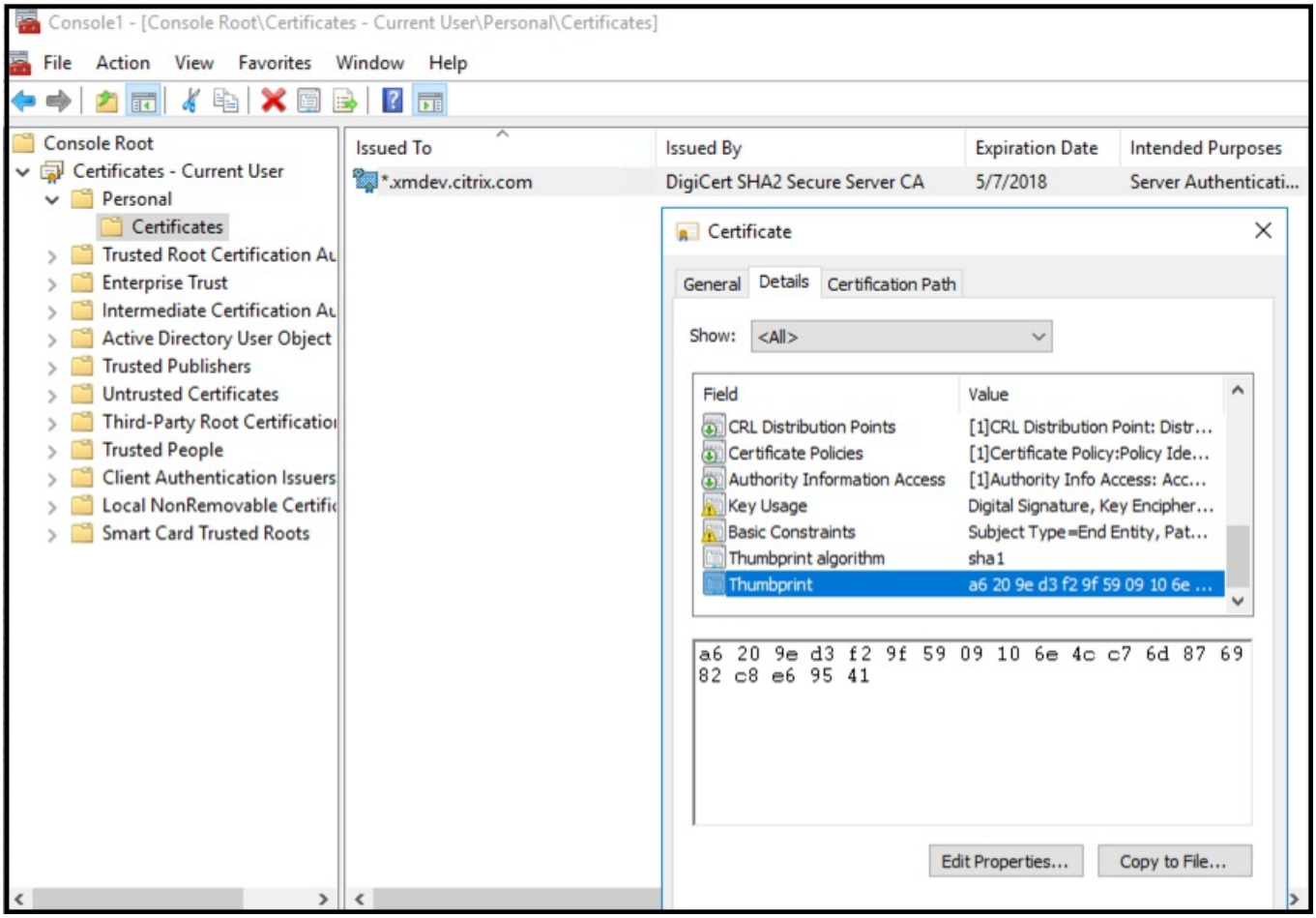
e. In the Add Standalone Snap-in dialog box, select **Certificates**.

f. Click **Add**.

g. In the Certificates snap-in dialog box, select **My User account.** (If you are signed in as service account holder, select **Service account**.)

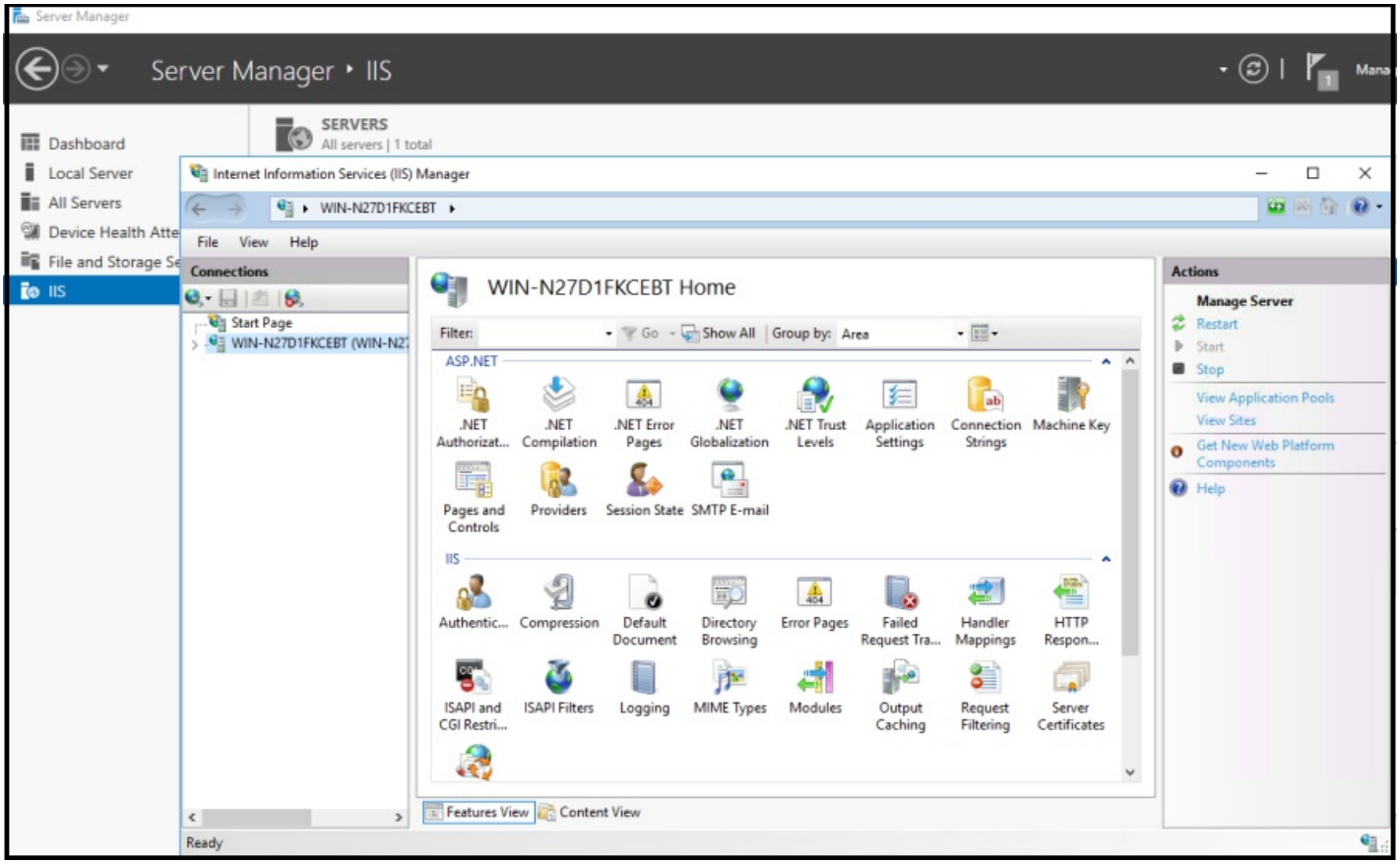
© 1999-2017 Citrix Systems, Inc. All rights reserved.

h. In the Select Computer dialog box, click **Finish**.

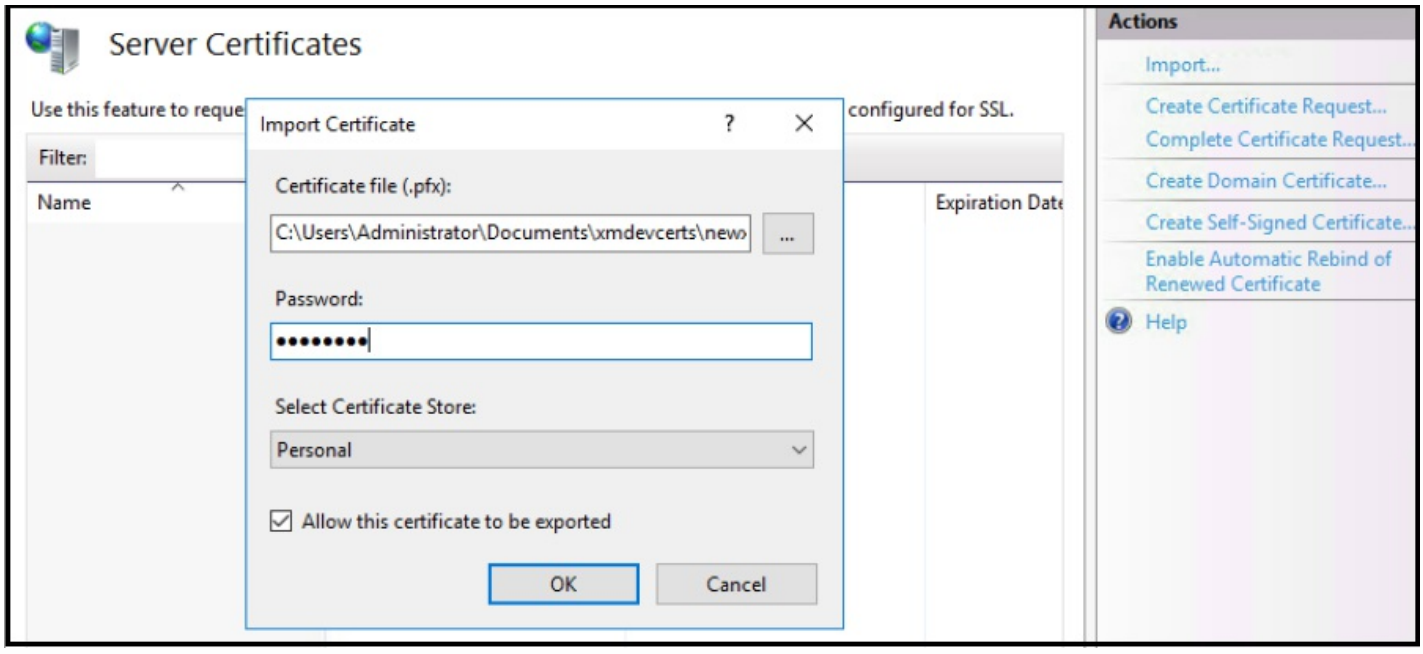


7. Go to **Server Manager > IIS** and select **Server Certificates** from the list of icons.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



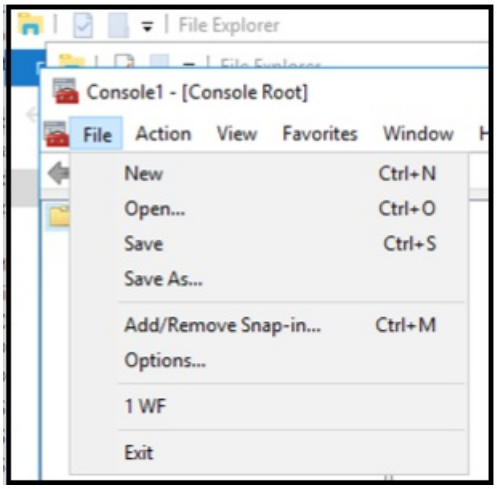
8. From the Action menu, select **Import ...** to import the SSL certificate.



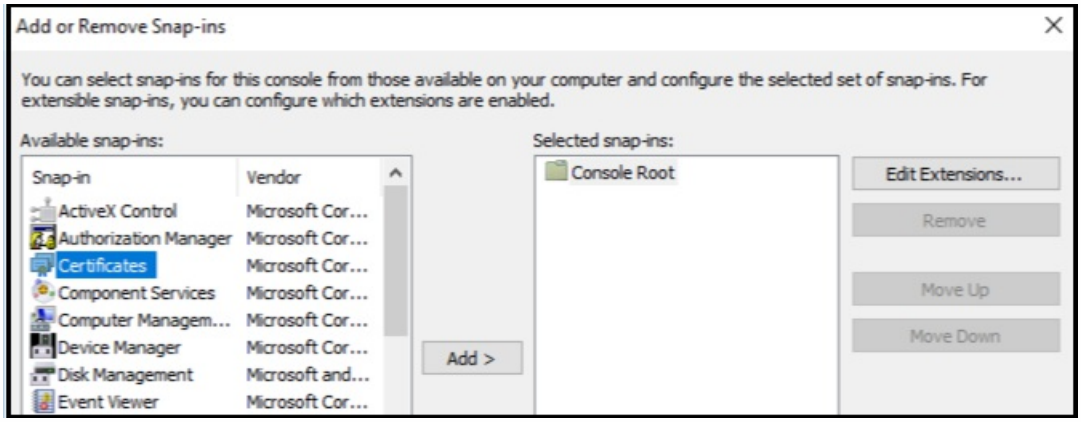
Retrieve and save the thumbprint of the certificate

1. In the File Explorer search bar, type **mmc**.
2. In the Console Root window, click **File > Add/Remove Snap-in...**.

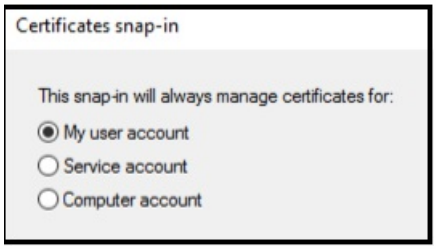
© 1999-2017 Citrix Systems, Inc. All rights reserved.



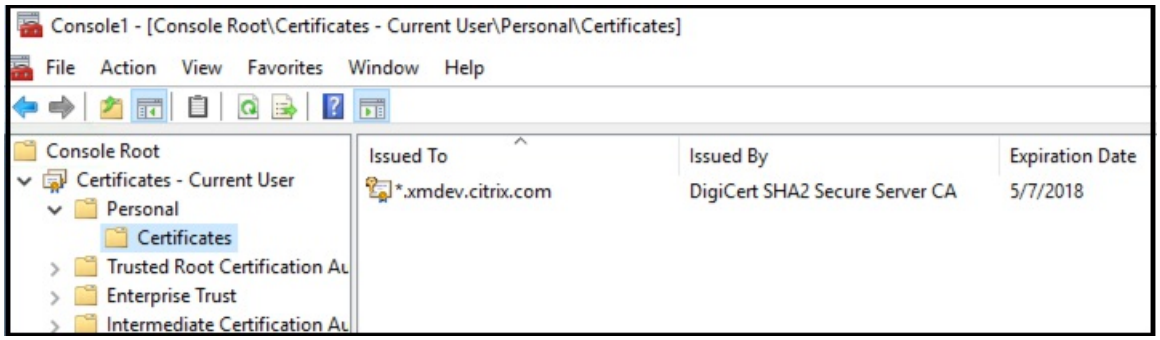
3. Select the certificate from available snap-in and add it to selected snap-ins.



4. Select **My user account**.

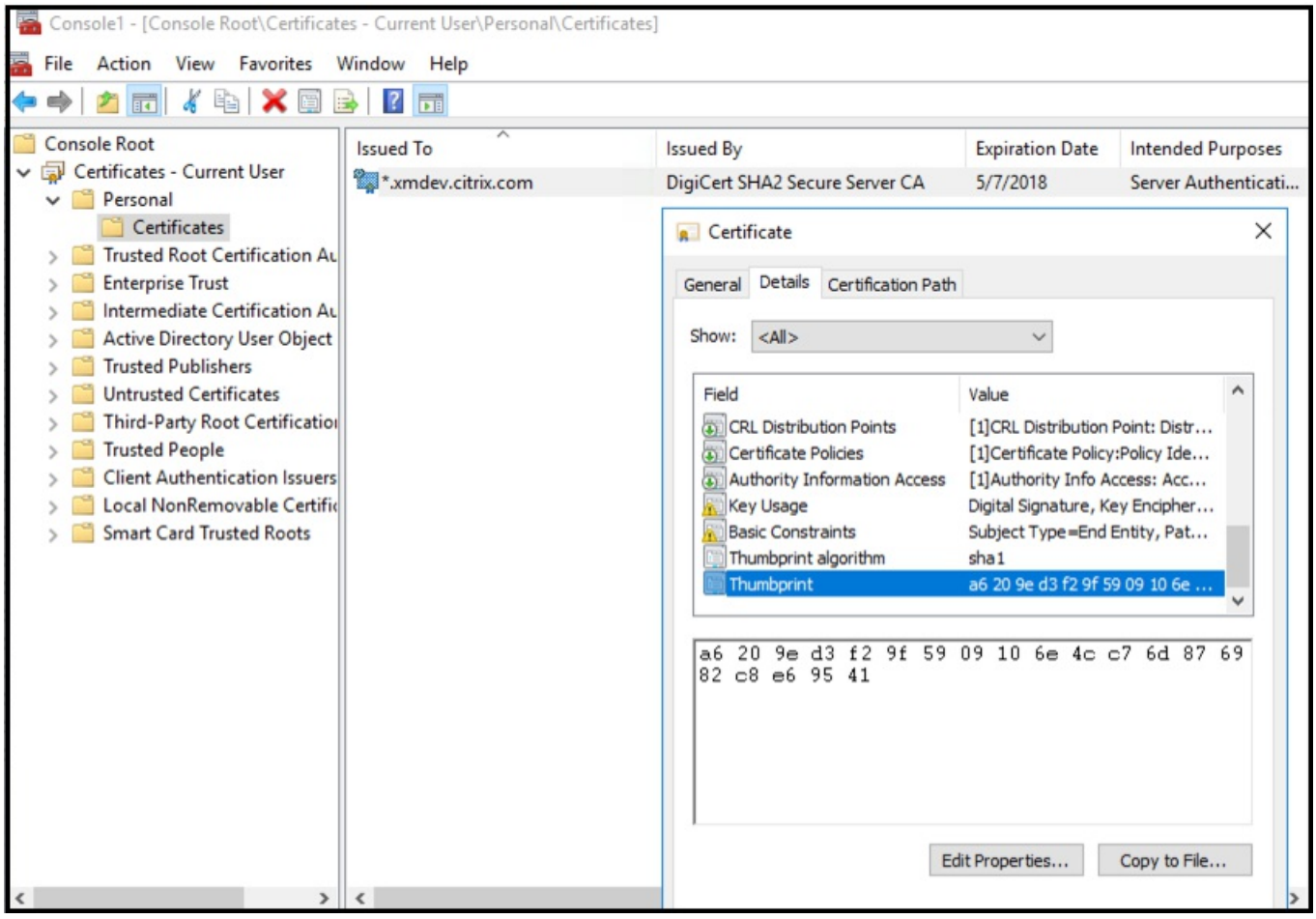


5. Select the certificate and click **OK**.



6. Double-click on the certificate and select the **Details** tab. Scroll down to see the certificate thumbprint.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



7. Copy the thumbprint to a file. Remove the spaces when using the thumbprint in PowerShell commands.

Install the signing and encryption certificates

Run these PowerShell commands certificates on the Windows server to install the signing and encryption:

```
$key = Get-ChildItem Cert:\LocalMachine\My | Where-Object {$_.Thumbprint -like "ReplaceWithThumbprint"}

$keyname = $key.PrivateKey.CspKeyContainerInfo.UniqueKeyContainerName

$keypath = $env:ProgramData + "\Microsoft\Crypto\RSA\MachineKeys\" + $keyname icacls $keypath /grant IIS_IUSRS`:R
```

Extract the TPM roots certificate and install the trusted certificate package

Run these commands on the Windows server:

```
mkdir .\TrustedTpm

expand -F:* .\TrustedTpm.cab .\TrustedTpm
```


© 1999-2017 Citrix Systems, Inc. All rights reserved.

cd .\TrustedTpm

.\setup.cmd

Configure the DHA service

Run this command on the Windows server to configure the DHA service:

Install-DeviceHealthAttestation -EncryptionCertificateThumbprint <*ReplaceWithThumbprint*>

-SigningCertificateThumbprint <*ReplaceWithThumbprint*>

-SslCertificateStoreName My -SslCertificateThumbprint <*ReplaceWithThumbprint*>

-SupportedAuthenticationSchema "AikCertificate"

Run these commands on the Windows server to set up the certificate chain policy for the DHA service:

$policy = Get-DHASCertificateChainPolicy

$policy.RevocationMode = "NoCheck"

Set-DHASCertificateChainPolicy -CertificateChainPolicy $policy

Respond to these prompts, as follows:

Confirm

Are you sure you want to perform this action?

Performing the operation "Install-DeviceHealthAttestation" on target "WIN-N27D1FKCEBT".

[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help (default is "Y"): A

Adding SSL binding to website 'Default Web Site'.

Add SSL binding?

[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

Adding application pool 'DeviceHealthAttestation_AppPool' to IIS.

Add application pool?

[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

Adding web application 'DeviceHealthAttestation' to website 'Default Web Site'.

Add web application?

[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

Adding firewall rule 'Device Health Attestation Service' to allow inbound connections on port(s) '443'.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Add firewall rule?

[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

Setting initial configuration for Device Health Attestation Service.

Set initial configuration?

[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

Registering User Access Logging.

Register User Access Logging?

[Y] Yes [N] No [S] Suspend [?] Help (default is "Y"): Y

Check the configuration

To check whether the DHASActiveSigningCertificate is active, run this command on the server:

Get-DHASActiveSigningCertificate

If the certificate is active, the certificate type (Signing) and thumbprint is displayed.

To check whether the DHASActiveSigningCertificate is active, run this command on the server:

Set-DHASActiveEncryptionCertificate -Thumbprint "*ReplaceWithThumbprint*" -Force

Get-DHASActiveEncryptionCertificate

If the certificate is active, the thumbprint is displayed.

To perform a final check, go to this URL:

https://*dha.myserver.com*/DeviceHeathAttestation/ValidateHealthCertificate/v1

If the DHA service is running, “Method not allowed” is displayed.

© 1999-2017 Citrix Systems, Inc. All rights reserved.

Configuring certificate-based authentication with EWS for Secure Mail push notifications

Vijay Kumar Kunchakuri , | Feb 21, 2018

To make sure that Secure Mail push notifications work, you must configure Exchange Server for certificate-based authentication. This requirement is especially necessary when Secure Hub is enrolled in XenMobile with certificate-based authentication.

You need to configure the Active Sync and Exchange Web Services (EWS) virtual directory on the Exchange Mail Server with certificate-based authentication.

Unless you complete these configurations, the subscription to Secure Mail push notifications fails and no badge updates occur in Secure Mail.

This article describes the steps to configure certificate-based authentication. The configurations are specifically against the EWS virtual directory on Exchange Server.

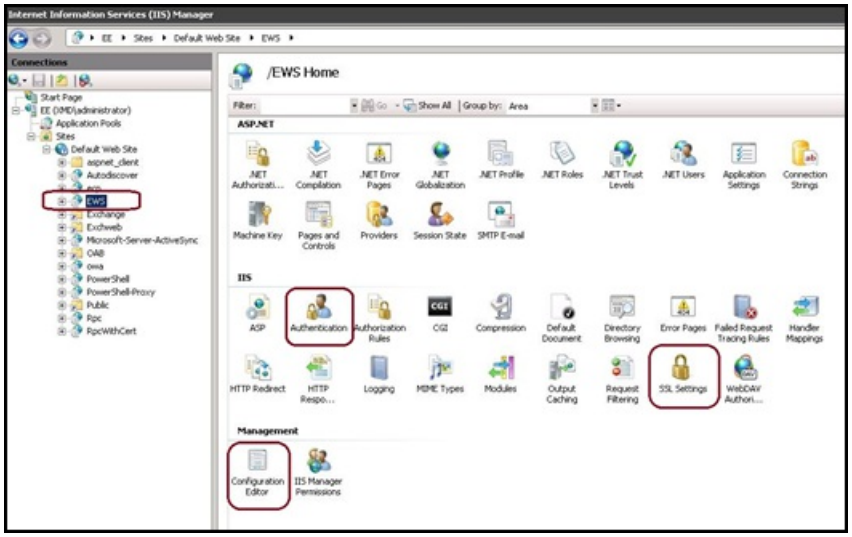
To get started with the configuration, do the following:

1. Log on to the server or servers where the EWS virtual directory is installed.

2. Open the IIS Manager Console.

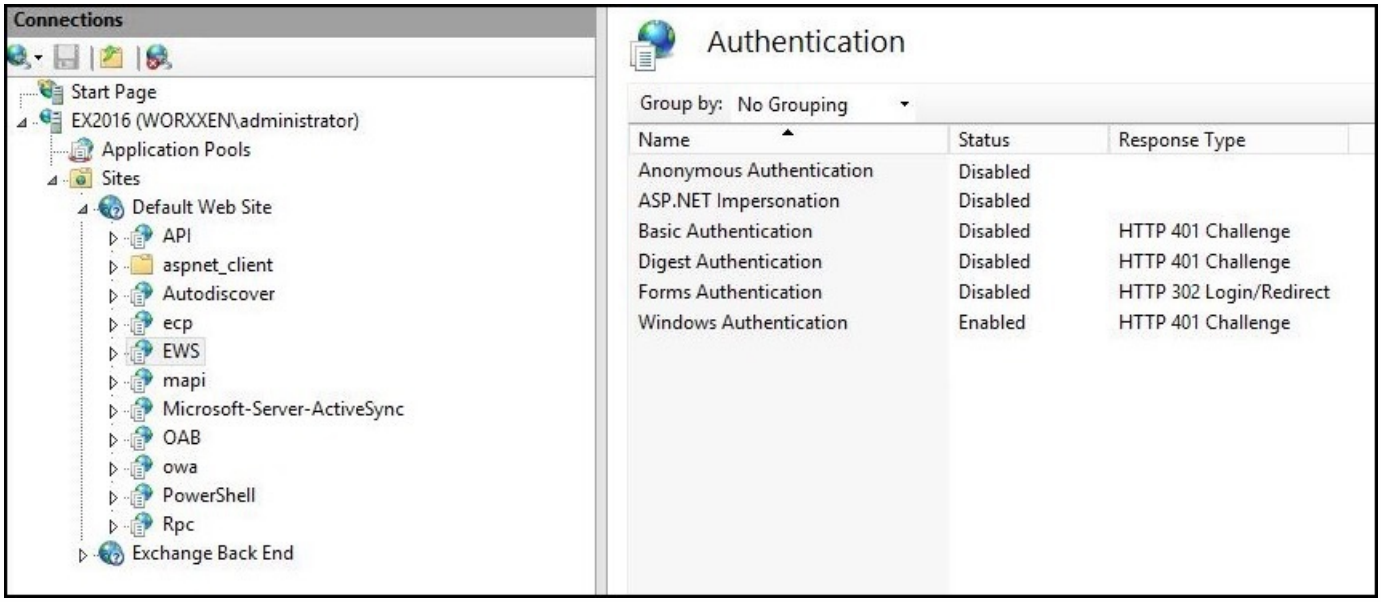
3. Under the **Default Web Site**, click the EWS virtual directory.

The Authentication, SSL, Configuration Editor snap-ins are on the right side of the IIS Manager Console



4. Ensure that the **Authentication** settings for EWS are configured as shown in the following figure.

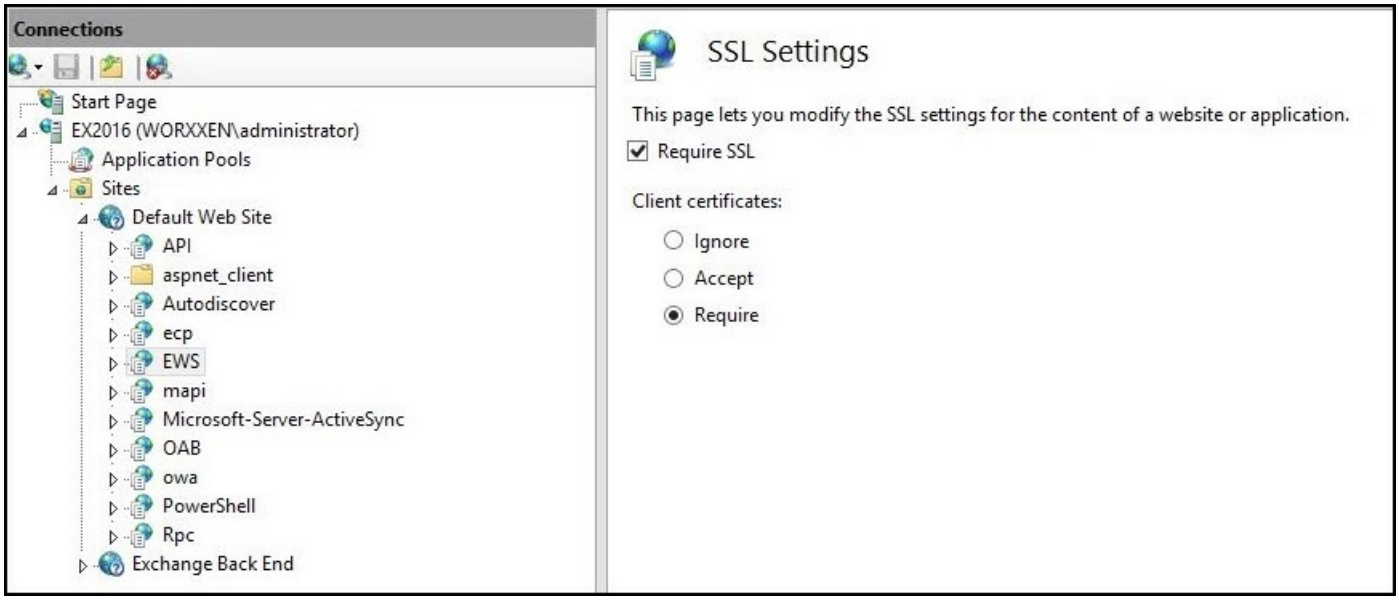
 © 1999-2017 Citrix Systems, Inc. All rights reserved.



5. Configure the **SSL Settings** for the EWS virtual directory.

   a. Select the **Require SSL** check box.

   b. Under **Client Certificates,** click **Require.** You can set this option to **Accept** if other EWS mail clients connect with username/password as credentials to authenticate and connect to the Exchange Server.

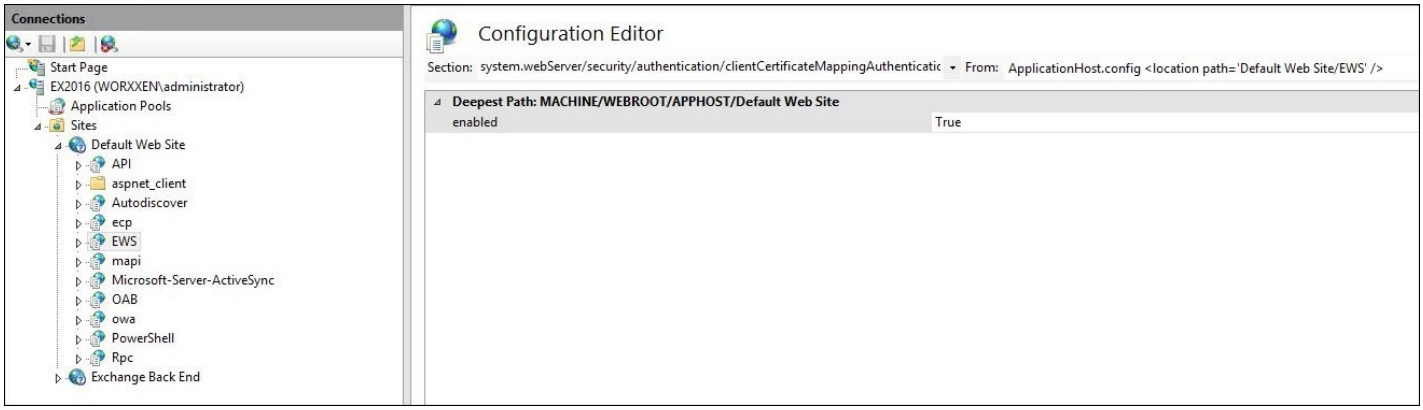


6. Click **Configuration Editor** and in the **Section** drop-down list, navigate to the following section:

system.webServer/security/authentication/clientCertificateMappingAuthentication

7. Set the **enabled** value to **True**.

© 1999-2017 Citrix Systems, Inc. All rights reserved.



8. Click **Configuration Editor** and in the **Section** drop-down list, navigate to the following section:

system.webServer/serverRuntime

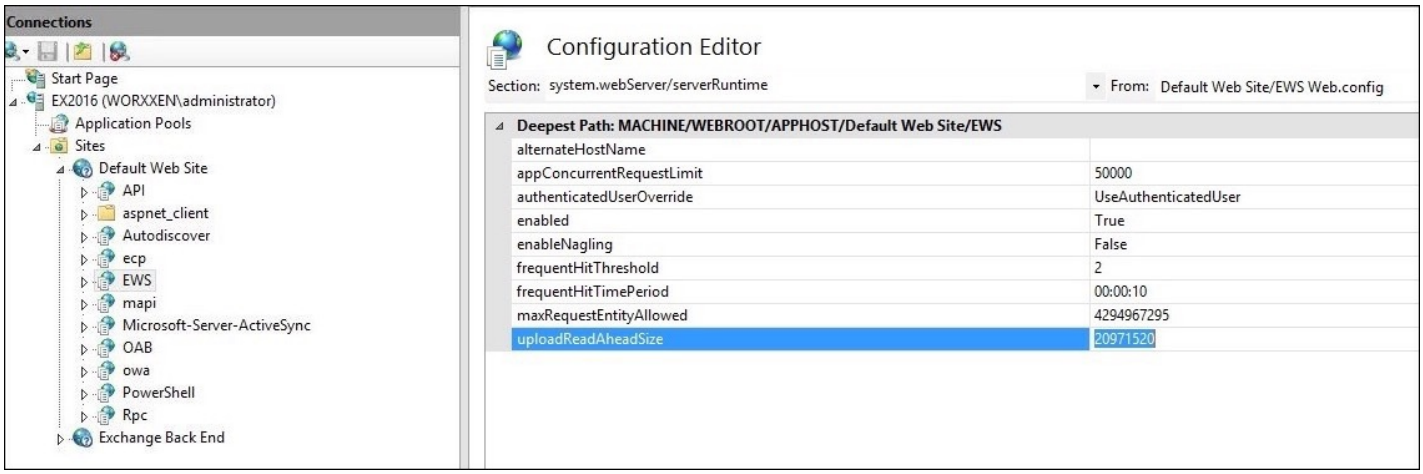
9. Set the **uploadReadAheadSize** value to **10485760** (10 MB) or **20971520** (20 MB) or to a value as required by your organization.

Important: If you don't set this value correctly, certificate-based authentication while subscribing to EWS push notifications may fail with an error code of 413.

Note: Do not set this value to **0.**

For more information, see the following third-party resources:

- Microsoft IIS server runtime
- Butsch Client Management Blog



For more information about troubleshooting Secure Mail issues with iOS push notifications, see this Citrix Support Knowledge Center article.

Related information

- Push notifications for Secure Mail for iOS

© 1999-2017 Citrix Systems, Inc. All rights reserved.