Aplicativos móveis de produtividade

Contents

Cronograma de lançamento dos aplicativos móveis de produtividade

December 9, 2021

O lançamento dos aplicativos móveis de produtividade da Citrix ocorre em períodos de duas semanas. Embora as datas exatas possam se alterar, você poderá planejar antecipadamente com base nessa frequência. Também queremos que seja mais fácil para você gerenciar as atualizações e implantações de aplicativo.

Sobre o processo das fases de lançamento do Secure Mail e Secure Web

Quando há novas versões disponíveis do Secure Mail e do Secure Web, as versões são lançadas em fases, da seguinte maneira:

- Para usuários de iOS e Android, as atualizações do Secure Mail e do Secure Web estão disponíveis na App Store e na loja de aplicativos Google Play para uma porcentagem crescente de usuários ao longo de uma semana (sete dias).
- Os novos downloads do Secure Mail e do Secure Web para iOS recebem a nova versão dentro dessa semana. Os novos downloads do Secure Mail e do Secure Web para Android continuarão com a versão anterior da semana, até o lançamento da nova versão atingir 100% de todos os usuários.
- Para os usuários, alguns recursos são lançados em fases graduais.

Pré-requisitos para o gerenciamento de sinalizador de recursos

Se ocorrer um problema com o Secure Hub ou Secure Mail na produção, podemos desabilitar um recurso dentro do código do aplicativo afetado. Para fazer isso, usamos sinalizadores de recurso e um serviço de terceiros chamado LaunchDarkly. Você não precisa fazer as configurações para ativar o tráfego para LaunchDarkly, exceto quando você tiver um firewall ou proxy que bloqueie o tráfego de saída. Nesse caso, você ativa o tráfego para LaunchDarkly via URLs específicos ou endereços IP, dependendo dos requisitos de sua política. Para obter detalhes sobre suporte no MDX desde os aplicativos móveis de produtividade 10.6.15 para a exclusão de domínios de encapsulamento, consulte a Documentação do MDX Toolkit. Para ver as Perguntas Frequentes sobre sinalizadores de recurso e o LaunchDarkly, consulte este artigo do Knowledge Center de suporte.

> **Nota:**
> Para receber um aviso prévio dos recursos do Citrix Endpoint Management que estão sendo descontinuados, consulte as Substituições.

Suporte para aplicativos móveis de produtividade

February 27, 2024

Os usuários que têm atualizações automáticas ativadas recebem a versão mais recente da loja de aplicativos A versão mais recente dos aplicativos móveis de produtividade é a seguinte:

- 23.10.0 (Secure Web para Android)
- 23.9.0 (Secure Mail e Secure Web para iOS)
- 23.8.2 (Secure Mail para Android)

A Citrix oferece suporte a atualizações das duas últimas versões dos aplicativos móveis de produtividade. As duas últimas versões dos aplicativos móveis de produtividade são as seguintes:

- 23.8.1 (Secure Mail para Android)
- 23.8.0 (Secure Web para Android)
- 23.7.0 (Secure Mail para Android e Secure Mail para iOS)
- 23.5.0 (Secure Mail para iOS e Secure Web para Android)
- 23.2.0 (Secure Web para iOS)
- 22.9.1 (Secure Web para iOS)

> **Importante:**
>
> A criptografia MDX atingiu o fim da vida útil (EOL) em 1º de setembro de 2020. Para dispositivos registrados na administração de dispositivos (DA) legados:
>
> - Se você não usa criptografia MDX, nenhuma ação é necessária.
> - Se você usa criptografia MDX, migre seus dispositivos Android para o Android Enterprise. Os dispositivos com Android 10 devem se registrar ou se registrar novamente usando o Android Enterprise. Isso inclui dispositivos Android no modo somente MAM. Consulte Migrar do Device Administration para o Android Enterprise para obter detalhes.

Sistemas operacionais compatíveis

Os aplicativos móveis de produtividade oferecem suporte aos seguintes sistemas operacionais:

Nome do produto	Sistema operacional	Versão mínima de implantação	Versão mais recente disponível
Secure Hub	Android	7.x	14.x
	iOS	12.x	17.x

Nome do produto	Sistema operacional	Versão mínima de implantação	Versão mais recente disponível
Secure Mail	Android	8.x	14.x
	iOS	13.x	17.x
Secure Web	Android	8.x	14.x
	iOS	13.x	17.x

As versões mais recentes dos Aplicativos móveis de produtividade são compatíveis com a versão mais recente, além das duas versões anteriores do Citrix Endpoint Management. Para obter mais informações sobre os sistemas operacionais compatíveis com o Citrix Endpoint Management, consulte Sistemas operacionais compatíveis de dispositivos.

A versão mais recente dos Aplicativos móveis de produtividade requer a versão mais recente do Secure Hub. Certifique-se de manter o Secure Hub atualizado.

> **Nota:**
>
> a qualquer momento, a Citrix oferece suporte somente à versão mais recente e às duas versões anteriores (N, N-1 e N-2) dos sistemas operacionais Android e iOS.

Outras considerações e limitações

Para receber um aviso prévio dos recursos do Citrix Endpoint Management que estão sendo descontinuados, consulte as Substituições.

Secure Mail

- O Endpoint Management atualmente não dá suporte ao NetScaler 12.0.41.16 por causa de um problema com o Secure Ticket Authority (STA) e o Secure Mail. O problema foi corrigido no NetScaler 12.0 compilação 41.22.
- O suporte no Secure Mail para o Exchange 2007 e Lotus Notes 8.5.3 atingiu o fim da vida útil (EOL) em 30 de setembro de 2017.
- Para obter o melhor desempenho ao enviar anexos do Citrix Files, as versões mais recentes do Citrix Files são recomendadas. O Citrix Files não é suportado pelo Windows.
- Em ambientes IBM Notes, você deve configurar o servidor IBM Domino Traveler, versão 9.0. Para obter detalhes, consulte Integração do Exchange Server ou servidor IBM Notes Traveler.

> **Nota:**
>
> - O Citrix Files for XenMobile atingiu o EOL em 1º de julho de 2023. Para obter mais informações, consulte EOL e aplicativos obsoletos

Secure Web

Instale a versão mais recente do Android WebView nos dispositivos. Os usuários podem baixar o Android WebView na Google Play Store.

QuickEdit

O QuickEdit permanece disponível como um aplicativo móvel de produtividade. O status de fim da vida útil (EOL) não foi aplicado em 1º de setembro de 2018, como comunicado anteriormente.

Citrix Content Collaboration para Endpoint Management

Os usuários acessam o Citrix Content Collaboration para Endpoint Management nas lojas de aplicativos públicas após a versão 6.5.

ShareConnect

O ShareConnect atingiu o fim da vida útil (EOL) em 30 de junho de 2020. Para obter detalhes, consulte EOL e aplicativos obsoletos.

Citrix Secure Notes e Citrix Secure Tasks

O Citrix Secure Notes e o Citrix Secure Tasks atingiram o status de fim da vida útil (EOL) em 31 de dezembro de 2018. Para obter detalhes, consulte EOL e aplicativos obsoletos.

Tarefas e considerações do administrador

October 31, 2022

Este artigo discute as tarefas e considerações relevantes para administradores de aplicativos móveis de produtividade.

Gerenciamento de sinalização de recurso

Se ocorrer um problema com o aplicativo móvel de produtividade na produção, podemos desabilitar um recurso afetado dentro do código do aplicativo. Podemos desabilitar o recurso no Secure Hub, Secure Mail e Secure Web para iOS e Android. Para fazer isso, usamos sinalizadores de recurso e um serviço de terceiros chamado LaunchDarkly. Você não precisa fazer as configurações para ativar o tráfego para LaunchDarkly, exceto quando você tiver um firewall ou proxy que bloqueie o tráfego de saída. Nesse caso, você ativa o tráfego para LaunchDarkly via URLs específicos ou endereços IP, dependendo dos requisitos de sua política. Para obter detalhes sobre suporte no MDX para a exclusão de domínios de encapsulamento, consulte a Documentação do MDX Toolkit.

Você pode ativar o tráfego e a comunicação com o LaunchDarkly das seguintes maneiras:

Habilitar o tráfego para as seguintes URLs

- `events.launchdarkly.com`
- `stream.launchdarkly.com`
- `clientstream.launchdarkly.com`
- `firehose.launchdarkly.com`

Criar uma lista de permissão por domínio

Anteriormente, oferecíamos uma lista de endereços IP para usar quando suas políticas internas exigissem que apenas endereços IP fossem listados. Agora, como a Citrix fez melhorias de infraestrutura, estamos eliminando os endereços IP públicos a partir de 16 de julho de 2018. Recomendamos que você crie uma lista de permissão por domínio, se possível.

Listar endereços IP em uma lista de permissão

Se você precisar acrescentar os endereços IP à lista de permissão, consulte a Lista de IPs públicos do LaunchDarkly para obter uma lista de todos os intervalos de endereços IP atuais. Você pode usar essa lista para garantir que suas configurações de firewall sejam atualizadas automaticamente, de acordo com as atualizações da infraestrutura. Para obter detalhes sobre o status atual das alterações de infraestrutura, consulte LaunchDarkly Statuspage.

> Nota:
>
> Os aplicativos da loja pública requerem uma instalação nova na primeira vez que você os implanta. Não é possível atualizar a partir da versão empresarial atual preparada do aplicativo para a versão da loja pública.

> Com distribuição em loja de aplicativos pública, você não precisa assinar e preparar aplicativos desenvolvidos pela Citrix com o MDX Toolkit. No entanto, você pode usar o MDX Toolkit para preparar os aplicativos de terceiros ou empresariais.

Requisitos do sistema LaunchDarkly

- Endpoint Management 10.7 ou posterior.
- Verifique se os aplicativos podem se comunicar com os seguintes serviços se o túnel dividido do Citrix ADC estiver definido como **Desativado**:
  - Serviço LaunchDarkly
  - Serviço de ouvinte APNs

Lojas de aplicativos com suporte

Os aplicativos móveis de produtividade estão disponíveis na loja de aplicativos da Apple e no Google Play.

Na China, onde o Google Play não está disponível, o Secure Hub para Android está disponível nas seguintes lojas de aplicativos:

- https://shouji.baidu.com
- https://apk.hiapk.com
- https://apk.91.com

Ativar a distribuição em loja de aplicativos pública

1. Baixe os arquivos .mdx da loja pública para iOS e Android na página de downloads do Endpoint Management.
2. Carregue os arquivos .mdx para o console Endpoint Management. As versões da loja pública dos aplicativos móveis de produtividade ainda são carregadas como aplicativos MDX. Não carregue os aplicativos como aplicativos de armazenamento público no servidor. Para informações sobre as etapas, consulte Adicionar aplicativos.
3. Altere as políticas de seus padrões com base nas suas políticas de segurança (opcional).
4. Envie os aplicativos como aplicativos necessários (opcional). Esta etapa requer que seu ambiente seja habilitado para gerenciamento de dispositivos móveis.
5. Instale aplicativos no dispositivo da App Store, do Google Play ou da loja de aplicativos do Endpoint Management.
   - No Android, o usuário é direcionado à Play Store para instalar o aplicativo. No iOS, em implantações com o MDM, o aplicativo é instalado sem que o usuário vá até a loja de aplicativos.

- Quando o aplicativo é instalado a partir da App Store ou Play Store, ocorre a seguinte ação. O aplicativo muda para um aplicativo gerenciado desde que o arquivo .mdx correspondente tenha sido carregado para o servidor. Ao fazer a transição para um aplicativo gerenciado, o aplicativo pede um PIN da Citrix. Quando os usuários inserem o PIN da Citrix, o Secure Mail exibe a tela de configuração de conta.

6. Os aplicativos estão acessíveis somente se você estiver registrado no Secure Hub e o arquivo .mdx correspondente estiver no servidor. Se alguma das condições não for atendida, os usuários podem instalar o aplicativo, mas o uso do aplicativo é bloqueado.

Se você atualmente usa aplicativos do Citrix Ready Marketplace que estão em lojas de aplicativos públicas, você já está familiarizado com o processo de implantação. Os aplicativos móveis de produtividade adotam a mesma abordagem que muitos ISVs utilizam atualmente. Incorpore o SDK do MDX no aplicativo para tornar o aplicativo apto para loja de aplicativos pública.

> Nota:
>
> As versões de loja pública do aplicativo Citrix Files para iOS e Android agora são universais. O aplicativo Citrix Files é o mesmo para telefones e tablets.

Notificação por push da Apple

Para obter informações sobre a configuração de notificações por push, consulte Configuração de Secure Mail para notificações por push.

Perguntas frequentes da loja de aplicativos pública

- Posso implantar várias cópias do aplicativo de loja pública em diferentes grupos de usuários? Por exemplo, eu queiro implantar políticas diferentes para diferentes grupos de usuários.

  Carregue um arquivo .mdx diferente para cada grupo de usuários. No entanto, nesse caso, um único usuário não pode pertencer a mais de um grupo. Se os usuários pertencerem a mais de um grupo, várias cópias do mesmo aplicativo são atribuídas àquele usuário. Mais de uma cópia de um aplicativo de loja pública não pode ser implantada no mesmo dispositivo porque a ID de aplicativo não pode ser alterado.

- Posso enviar por push aplicativos de loja pública conforme seja necessário?

  Sim. O envio de aplicativos por push requer MDM; não tem suporte com implantações de apenas MAM.

- Atualizo as políticas de tráfego ou regras do Exchange Server que são baseadas em agente de usuário?

Cadeias de caracteres para as políticas baseadas em agentes e regras por plataforma como apresentado a seguir.

> Importante:
>
> O Secure Notes e o Secure Tasks atingiram o status de Fim da Vida Útil (EOL) em 31 de dezembro de 2018. Para obter detalhes, consulte EOL e aplicativos obsoletos.

Android

Aplicativo	Servidor	Cadeia de agente do usuário
Citrix Secure Mail	Exchange	WorxMail
	Lotus Notes Traveler	Apple - iPhone WorxMail
Citrix Secure Web		WorxMail
Citrix Secure Tasks	Exchange	WorxMail
Citrix Secure Notes	Exchange	WorxMail
	Citrix Files	Secure Notes

iOS

Aplicativo	Servidor	Cadeia de agente do usuário
Citrix Secure Mail	Exchange	WorxMail
	Lotus Notes Traveler	Apple - iPhone WorxMail
Citrix Secure Web		com.citrix.browser
Citrix Secure Tasks	Exchange	WorxTasks
Citrix Secure Notes	Exchange	WorxNotes
	Citrix Files	Secure Notes

- Posso impedir atualizações do aplicativo?

  Não. Quando uma atualização é colocada na loja de aplicativos pública, todos os usuários que têm atualizações automáticas ativadas recebem a atualização.

- Posso impor atualizações de aplicativo?

Sim, as atualizações são impostas por meio da política de período de cortesia de atualização. Essa política é definida quando o novo arquivo .mdx correspondente à versão atualizada do aplicativo é carregado no Endpoint Management.

- Como faço para testar aplicativos antes da atualização atingir os usuários se eu não puder controlar os prazos da atualização?

  Semelhante ao processo para o Secure Hub, os aplicativos estão disponíveis para teste no TestFlight para iOS durante o período EAR. No Android, os aplicativos estão disponíveis por meio do programa beta Google Play durante o período EAR. Você pode testar as atualizações de aplicativos durante esse período.

- O que acontece se eu não atualizar o novo arquivo .mdx antes de a atualização automática atingir os dispositivos de usuário?

  O aplicativo atualizado permanece compatível com o antigo arquivo .mdx. Os novos recursos que dependem de uma nova política não são ativados.

- O aplicativo fará a transição para gerenciado se o Secure Hub estiver instalado ou o aplicativo precisa ser registrado?

  Os usuários devem estar registrados no Secure Hub para que a loja de aplicativos pública o ative como um aplicativo gerenciado pelo (com segurança pelo MDX) e ele seja utilizável. Se o Secure Hub estiver instalado, mas não registrado, o usuário não pode usar o aplicativo de loja pública.

- Preciso de uma conta de desenvolvedor Apple Enterprise para os aplicativos de loja pública?

  Não. Como a Citrix agora manterá os certificados e perfis de provisionamento para os aplicativos móveis de produtividade, não é necessário ter uma conta de desenvolvedor Apple Enterprise para implantar esses aplicativos aos usuários.

- O fim de distribuição empresarial se aplica a qualquer aplicativo preparado que eu tiver implantado?

  Não, aplica-se somente aos aplicativos móveis de produtividade: Secure Mail, Secure Web e Citrix Content Collaboration para Endpoint Management, QuickEdit e ShareConnect. Os aplicativos empresariais preparados que você implantou que foram desenvolvidos internamente ou por terceiros podem continuar a usar preparação empresarial. O MDX Toolkit continuará a oferecer suporte à preparação empresarial para desenvolvedores de aplicativos.

- Quando eu instalo um aplicativo do Google Play, recebo um erro do Android com código de erro 505.

  > Nota:
  >
  > O suporte para Android 5.x terminou em 31 de dezembro de 2018.

  Este é um problema conhecido com o Google Play e Android das versões 5.x. Se o erro ocorrer,

há alguns procedimentos que você pode executar para limpar dados obsoletos no dispositivo que estão impedindo a instalação do aplicativo:

1. Reinicie o dispositivo.
2. Limpe o cache e os dados do Google Play por meio das configurações do dispositivo.
3. Como último recurso, remova e adicione de volta a conta do Google ao seu dispositivo.

Para obter mais informações, pesquise neste site usando as seguintes palavras-chave: "Fix Google Play Store Error 505 in Android: Unknown Error Code"

- Embora o aplicativo no Google Play tenha sido liberado para produção e não haja uma nova versão beta disponível, por que aparece Beta após o nome do aplicativo no Google Play?

  Se você faz parte do nosso programa de versão de acesso antecipado, você sempre verá Beta ao lado do nome do aplicativo. Esse nome simplesmente notifica os usuários sobre o seu nível de acesso para um aplicativo específico. O nome Beta indica que os usuários têm a versão mais recente do aplicativo disponível. A versão mais recente pode ser a última publicada para produção ou como beta.

- Após instalar e abrir o aplicativo, os usuários veem a mensagem Aplicativo não autorizado, ainda que o arquivo .mdx esteja no console Endpoint Management.

  Esse problema pode acontecer se os usuários instalarem o aplicativo diretamente da App Store ou do Google Play e se o Secure Hub não tiver sido atualizado. O Secure Hub deve ser atualizado quando o temporizador de inatividade expirar. As políticas são atualizadas quando os usuários abrem o Secure Hub e autenticam novamente. O aplicativo será autorizado na próxima vez em que os usuários abrirem o aplicativo.

- É necessário um código de acesso para usar o aplicativo? Eu vejo uma tela que me pede para inserir um código de acesso quando instalo o aplicativo da App Store ou Play Store.

  Se for exibida uma tela que solicita o código de acesso, isso indica que você não está registrado no Endpoint Management através do Secure Hub. Registre com o Secure Hub e verifique se o arquivo .mdx foi implantado no servidor. Também verifique se é possível usar o aplicativo. O código de acesso está limitado ao uso interno da Citrix. Os aplicativos exigem uma implantação de Endpoint Management para que sejam ativados.

- Posso implantar aplicativos de loja pública do iOS via VPP ou DEP?

  O Endpoint Management é otimizado para distribuição por VPP de aplicativos de loja pública que não são habilitados para MDX. Embora você possa distribuir os aplicativos da loja pública do Endpoint Management com VPP, a implantação não é ideal, até que façamos aprimoramentos adicionais ao Endpoint Management e à loja do Secure Hub para resolver as limitações. Para obter uma lista de problemas conhecidos com a implantação de aplicativos da loja pública do

Endpoint Management por meio de VPP, além de possíveis soluções alternativas, consulte este artigo do Citrix Knowledge Center.

Políticas de MDX para aplicativos móveis de produtividade

As políticas de MDX permitem que você ajuste as configurações que o Endpoint Management impõe. As políticas abrangem autenticação, segurança de dispositivo, requisitos de rede e de acesso, criptografia, interação de aplicativos, restrições de aplicativos e muito mais. Muitas políticas de MDX se aplicam a todos os aplicativos móveis de produtividade. Algumas políticas são específicas do aplicativo.

Os arquivos de política são fornecidos como arquivos .mdx para as versões de loja pública dos aplicativos móveis de produtividade. Você também pode configurar as políticas no console Endpoint Management ao adicionar um aplicativo.

Para obter descrições completas das políticas de MDX, consulte os seguintes artigos nesta seção:

- Resumo das políticas de MDX para aplicativos móveis de produtividade
- Políticas de MDX para aplicativos móveis de produtividade para Android
- Políticas de MDX para aplicativos móveis de produtividade para iOS

As seções a seguir descrevem as políticas de MDX relacionadas a conexões de usuário.

Modo duplo no Secure Mail para Android

Um SDK de gerenciamento de aplicativo móvel (MAM) está disponível para substituir áreas de funcionalidade MDX que não são cobertas pelas plataformas iOS e Android. A tecnologia de preparação MDX está programada para atingir o fim da vida útil (EOL) em setembro de 2021. Para continuar gerenciando seus aplicativos empresariais, você deve incorporar o SDK MAM.

A partir da versão 20.8.0, os aplicativos Android são lançados com o MDX e o MAM SDK para se preparar para a estratégia MDX EOL mencionada anteriormente. O modo duplo MDX destina-se a fornecer uma maneira de fazer a transição para novos SDKs MAM a partir do MDX Toolkit atual. O uso do modo duplo permite que você:

- Continue gerenciando aplicativos usando o MDX Toolkit (agora chamado MDX Legado no console Endpoint Management)
- Gerencie aplicativos que incorporam o novo MAM SDK.

> **Nota:**
>
> Quando você usa o MAM SDK, não é necessário preparar aplicativos.

Não há etapas adicionais necessárias depois que você alternar para o MAM SDK.

Para obter mais detalhes sobre o SDK MAM, consulte os seguintes artigos:

- Visão geral do MAM SDK
- Seção Citrix Developer sobre o gerenciamento de dispositivo
- Postagem no blog Citrix
- Baixe o SDK quando você fizer logon nos downloads da Citrix

Pré-requisitos

Para uma implantação bem-sucedida do recurso de modo duplo, assegure o seguinte:

- Atualize o Citrix Endpoint Management para as versões 10.12 RP2 e posteriores ou 10.11 RP5 e posteriores.
- Atualize seus aplicativos móveis para a versão 20.8.0 ou posterior.
- Atualize o arquivo de políticas para a versão 20.8.0 ou posterior.
- Se a sua organização usa aplicativos de terceiros, certifique-se de incorporar o SDK MAM em seus aplicativos de terceiros antes de mudar para a opção SDK MAM em seus aplicativos móveis de produtividade Citrix. Todos os seus aplicativos gerenciados devem ser movidos para o SDK MAM de uma só vez.

> **Nota:**
>
> O SDK MAM é compatível com todos os clientes baseados em nuvem.

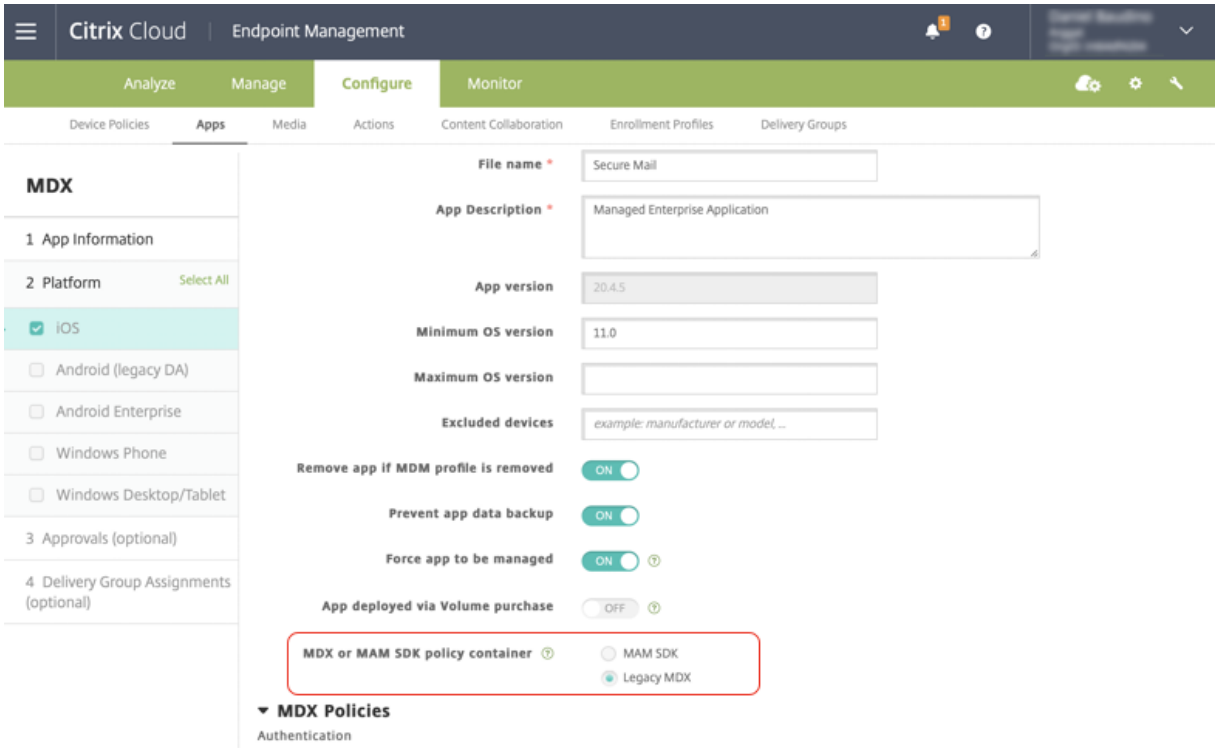
Limitações

- O SDK MAM suporta apenas aplicativos publicados na plataforma Android Enterprise em sua implantação do Citrix Endpoint Management. Para os aplicativos recém-publicados, a criptografia padrão é a criptografia baseada em plataforma.
- O SDK MAM suporta apenas criptografia baseada em plataforma, não criptografia MDX.
- Se você não atualizar o Citrix Endpoint Management e os arquivos da política estiverem sendo executados na versão 20.8.0 e posterior nos aplicativos móveis, serão criadas entradas duplicadas da política de Rede no Secure Mail.

Quando você configura o Secure Mail no Citrix Endpoint Management, o recurso de modo duplo permite que você continue gerenciando aplicativos usando o MDX Toolkit (agora MDX herdado) ou alterne para o novo MAM SDK para gerenciamento de aplicativos. A Citrix recomenda que você alterne para o MAM SDK, pois os SDKs MAM são mais modulares e têm o objetivo de permitir que você use apenas um subconjunto da funcionalidade de MDX que a sua organização usa.

Você tem as seguintes opções de configurações de política no **Contêiner de política MDX ou MAM SDK**:

- **MAM SDK**
- **MDX herdado**



Na política de **Contêiner de política MDX ou MAM SDK**, você só pode alterar sua opção de **MDX herdado** para **MAM SDK**. A opção de alternar do **MAM SDK** para o **MDX herdado** não é permitida, e você precisa republicar o aplicativo. O valor padrão é **MDX herdado**. Certifique-se de definir o mesmo modo de política para o Secure Mail e o Secure Web em execução no mesmo dispositivo. Não é possível ter dois modos diferentes em execução no mesmo dispositivo.

Conexões de usuário à rede interna

As conexões que fazem túnel para a rede interna podem usar um Túnel de VPN completo ou uma variação de uma VPN sem cliente, conhecida como Com túnel —SSO de Web. A Política de modo VPN preferencial controla esse comportamento. Por padrão, as conexões usam Com túnel —SSO de Web, que é recomendado para conexões que exigem SSO. A configuração do túnel VPN completo é recomendada para conexões que usam certificados de cliente ou SSL de ponta a ponta a um recurso na rede interna. A configuração manipula qualquer protocolo por TCP e pode ser usada com computadores Windows e Mac e com dispositivos iOS e Android.

A política Permitir comutação de modo VPN permite a comutação automática entre os modos Túnel VPN completo e Com túnel –SSO de Web, conforme necessário. Como padrão, esta política está De-

sativada. Quando esta política está ativada, uma solicitação de rede que falhar devido a uma solicitação de autenticação que não possa ser processado no modo VPN preferida é repetida no modo alternativo. Por exemplo, desafios do servidor para certificados de cliente podem ser acomodados pelo modo túnel VPN completo, mas não pelo modo Com túnel —SSO de Web. Da mesma forma, os desafios de autenticação HTTP têm maior probabilidade de serem atendidos pelo SSO ao usar o modo Com túnel —SSO de Web.

Restrições de acesso à rede

A política de Acesso à rede especifica se são colocadas restrições no acesso à rede. Como padrão, o acesso ao Secure Mail é irrestrito, o que significa que não há restrições colocadas no acesso à rede. Os aplicativos têm acesso irrestrito a redes a que o dispositivo está conectado. Como padrão, o acesso ao Secure Web é com túnel para a rede interna, o que significa que é usado um túnel de VPN por aplicativo para rede interna para todo o acesso à rede e são utilizadas configurações de túnel dividido do Citrix ADC. Você também pode especificar acesso bloqueado para que o aplicativo funcione como se o dispositivo não tivesse conexão de rede.

Não bloqueie a política de acesso à rede se você quiser permitir recursos como AirPrint e iCloud, além de APIs do Facebook e Twitter.

A política Acesso à rede interage com a política Serviços de rede em segundo plano. Para obter detalhes, consulte Integração do Exchange Server ou servidor IBM Notes Traveler.

Propriedades do cliente Endpoint Management

As propriedades do cliente contêm informações que são fornecidas diretamente para o Secure Hub em dispositivos de usuários. As propriedades do cliente estão localizadas no console Endpoint Management em **Configurações > Cliente > Propriedades do cliente**.

As propriedades do cliente são usadas para configurar configurações como as seguintes:

Armazenamento em cache de senha do usuário

O armazenamento de senha do usuário em cache permite aos usuários que a senha do Active Directory seja armazenada em cache localmente no dispositivo móvel. Se você ativar o armazenamento em cache da senha do usuário, os usuários são solicitados a criar um PIN da Citrix ou código secreto.

Timer de inatividade

O timer de inatividade define o tempo, em minutos, durante o qual os usuários podem deixar o dispositivo inativo e, em seguida, podem acessar um aplicativo sem que lhes seja solicitado um PIN da

Citrix ou código secreto. Para ativar esta configuração em um aplicativo de MDX, você deve definir a Política de código secreto de aplicativo como **Ativada**. Se a Política de código secreto de aplicativo estiver **Desativada**, os usuários são redirecionados para o Secure Hub para executar uma autenticação completa. Quando você altera essa configuração, o valor entra em vigor na próxima vez em que houver solicitação para que os usuários se autentiquem.

Autenticação do PIN da Citrix

O PIN da Citrix simplifica o processo de autenticação do usuário. O PIN é usado para proteger um certificado de cliente ou salvar credenciais do Active Directory localmente no dispositivo. Se você definir as configurações do PIN, o logon do usuário acontece da seguinte maneira:

1. Quando os usuários iniciam o Secure Hub pela primeira vez, eles recebem um aviso para inserir um PIN, que armazena em cache as credenciais do Active Directory.
2. Na próxima vez que os usuários iniciam um aplicativo móvel de produtividade, como o Secure Mail, eles inserem o PIN e se conectam.

Você deve usar as propriedades de cliente para ativar a autenticação por PIN, especificar o tipo de PIN e especificar a força, comprimento do PIN e alterar os requisitos.

Autenticação por impressão digital ou por Touch ID

A autenticação por impressão digital, também conhecida como autenticação por Touch ID, para dispositivos iOS é uma alternativa ao PIN Citrix. O recurso é útil quando aplicativos preparados, exceto o Secure Hub, precisam de autenticação offline, como quando o timer de inatividade expira. Você pode ativar o recurso nos seguintes cenários de autenticação:

- PIN da Citrix + configuração de certificado de cliente
- PIN da Citrix + senha de AD armazenada em cache
- PIN da Citrix + configuração de certificado do e configuração da senha de AD armazenada em cache
- PIN da Citrix está desativado

Se a autenticação por impressão digital falhar ou se um usuário cancelar o aviso de autenticação por impressão digital, os aplicativos preparados voltam para autenticação de PIN da Citrix ou de senha do AD.

Requisitos de autenticação por impressão digital

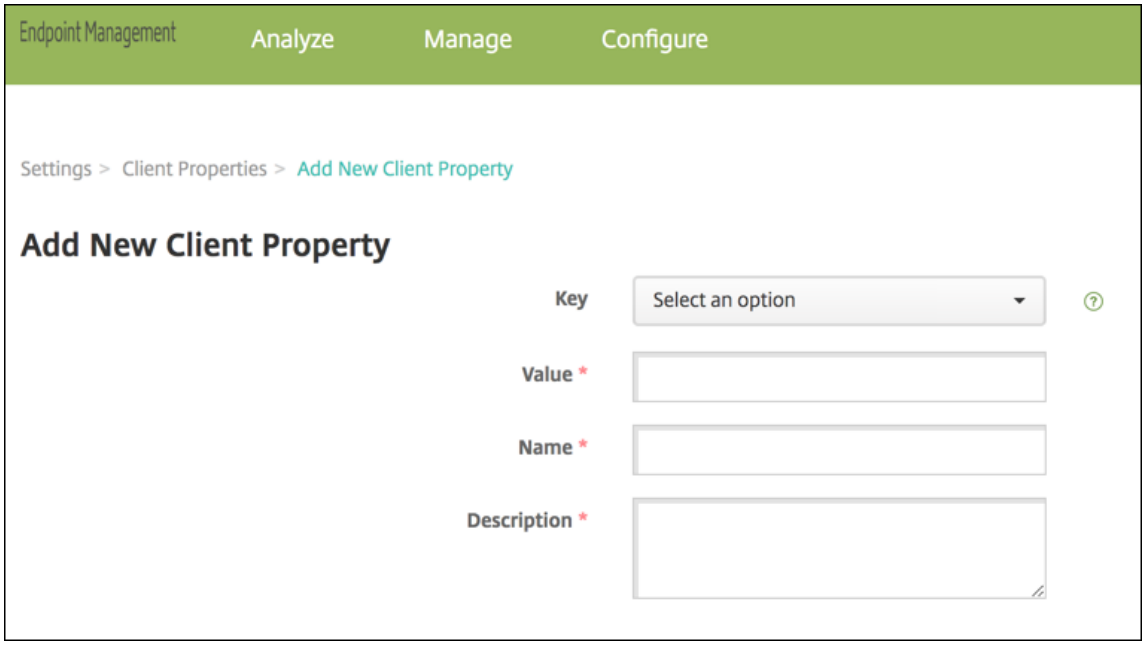
- Dispositivos iOS (mínimo de versão 8.1) que dão suporte a autenticação por impressão digital, devendo ter pelo menos uma impressão digital configurada.

- A entropia de usuário deve estar desativada.

Autenticação de impressão digital

> Importante:
>
> Se a entropia de usuário estiver ativada, a propriedade Ativar Autenticação de Touch ID é ignorada. O recurso de entropia de usuário é ativado por meio da chave Criptografar segredos usando o código secreto.

1. No console Endpoint Management vá até **Configurações > Cliente > Propriedades do cliente**.
2. Clique em **Add**.



3. Adicione a chave **ENABLE_TOUCH_ID_AUTH**, defina o **Valor** como **True** e defina o nome da política como **Ativar Autenticação por impressão digital**.

Depois de configurar a autenticação por impressão digital, os usuários não precisam registrar seus dispositivos de novo.

Para obter mais informações sobre a criptografia de segredos usando uma chave de código secreto e as propriedades do cliente em geral, consulte o artigo do Endpoint Management sobre Propriedades do cliente.

Google Analytics

O Citrix Secure Mail usa o Google Analytics para coletar estatísticas do aplicativo e dados analíticos sobre informações de uso para melhorar a qualidade do produto. A Citrix não coleta nem armazena

nenhuma outra informação pessoal do usuário.

Desativar o Google Analytics

Os administradores podem desativar o Google Analytics configurando a propriedade personalizada do cliente **DISABLE_GA**. Para desativar o Google Analytics, faça o seguinte:

1. Faça logon no console Citrix Endpoint Management e navegue para **Configurações** > **Propriedades do cliente** > **Adicionar nova propriedade de cliente**.
2. Adicione o valor **DISABLE_GA** ao campo **Chave**.
3. Defina o valor da propriedade do cliente como **true**.

> **Nota:**
>
> Se você não configurar o valor **DISABLE_GA** no console Citrix Endpoint Management, os dados do Google Analytics ficam ativos.

Recursos por plataforma

June 6, 2024

As tabelas a seguir resumem os recursos dos aplicativos móveis de produtividade Citrix. **X** indica que o recurso está disponível para a plataforma. Para conhecer os recursos no QuickEdit, consulte o Citrix QuickEdit.

Citrix Secure Hub

Recurso	iOS	Android
Logon para autenticar	X	X
Monitoração de aderência à política	X	X
Acesso a aplicativos e áreas de trabalho	X	X
Aplicativos HDX e áreas de trabalho	X	X
Criar e enviar logs de problemas	X	X

Recurso	iOS	Android
Anexação de capturas de tela para logs	X	X
Contato com o suporte técnico de dentro do aplicativo	X	X
Contato com a Citrix de dentro do aplicativo	X	X
Coleta e a análise de panes	X	X
Autenticação offline	X	X
Enviar logs com Citrix Secure Mail	X	X
Google Analytics	X	X
Modo de retrato e paisagem	X	X
Guia integrado para confiar em aplicativos	X	X
Quando registrado com email, registro automático no Secure Mail (MAM somente)	X	X
Autenticação offline de Touch ID	X	X
Registrar com credenciais derivadas	X	
Autenticação biométrica		X
Uso da loja de aplicativos do Workspace	X	X

Citrix Secure Mail

Recurso	iOS	Android
Produtividade de email		
Minimizar rascunhos	X	X
Desfazer envio de emails		X
Gerenciamento de criptografia	X	X

Recurso	iOS	Android
Widget para agenda do Calendário		X
Imagem do contato no Secure Mail	X	X
Suporte para emails responsivos	X	X
Sincronização automática da pasta Rascunhos	X	X
Sincronização de anexos na pasta **Rascunhos**		X
Enviar e receber, responder, responder para todos, encaminhar emails	X	X
Criar, editar e excluir rascunhos	X	X
Sinalizar email	X	X
Marcar como não lida	X	X
Exibir todas as pastas e subpastas	X	X
Salvamento automático de rascunhos quando o aplicativo é colocado em segundo plano	X	X
Email para nota com o Citrix Secure Notes. **Importante:** o Secure Notes atingiu o status de Fim da Vida Útil (EOL) em 31 de dezembro de 2018. Para obter detalhes, consulte EOL e aplicativos obsoletos.	X	X
Pesquisar email (local e servidor)	X	X
Selecionar período de sincronização de email (até 1 mês ou Todos os emails)	X	X
Exibir emails não lidos	X	X
Exibição/reprodução de imagens, vídeo e áudio	X	X

Recurso	iOS	Android
Vários anexos	X	X
Responder e encaminhar anexos	X	X
Anexar arquivos do Citrix Files	X	X
Anexar arquivos de conectores e zonas restritas do Citrix Files	X	X
Repositório de anexos	X	X
Edição de texto com formatação	X	X
Notificação por email com assunto, visualização em tela de bloqueio	X	X
Responder e excluir mensagens e convites na tela de notificação	X	
Anexar ou tirar fotos	X	X
Selecionar várias mensagens	X	X
Baixar anexos	X	X
Carregar imagens incorporadas	X	X
Classificação rápida	X	X
Enviar e receber, abrir e salvar anexos em arquivos .zip	X	X
Modos de retrato e paisagem	X; Pelos modos de exibição de lista de mensagens, mensagens lidas, composição, calendário e contatos	X: Pelos modos de exibição de leitura de email e composição apenas
Texto colado retém a formatação	X	X
SMS de contatos	X	X
FaceTime de contatos	X	
Mensagens não enviadas devido a problemas de conectividade ou a caixa de correio completa armazenados na Caixa de Saída	X	X

Recurso	iOS	Android
Destaque de pastas recentes		X
Puxar para baixo para atualizar emails	X	X
Carimbo de data e hora de última atualização	X	X
Deslizar para a esquerda para ações de mensagens	X	X
Suporte ao Microsoft Exchange e IBM Notes Traveler	X	X
Toque para atualizar email, calendário e contatos	X	X
Respeito às configurações de acessibilidade/tamanho de fonte em exibições de email	X	X
Assinatura e criptografia S/MIME de assinatura	X	X
Importação de certificado S/MIME por email	X	X
S/MIME, integração de Intercede	X	
S/MIME, integração de Entrust	X	
Proteção IRM Microsoft para o corpo da mensagem	X	X
Notificações por push	X	X
Notificações por push para a Caixa de Entrada atualizam automaticamente todas as pastas, incluindo o calendário	X	
Abrir documentos do Office 365	X	X
Ações de toque 3D	X	
Ícones contextuais na tela de bloqueio	X	X
Pastas de pesquisa	X	X
Pasta de email VIP	X	X
Suporte de tipo dinâmico	X	X

Recurso	iOS	Android
Manter pastas expandidas	X	X
Marcadores de classificação de mensagem	X	X
Verificação ortográfica	X	
Anexar a última foto tirada	X	X
Visualização da URL	X	X
Abrir links do Citrix Files no Citrix Files	X	X
Suporte para arquivos `.pass`	X	
Selecionar vários emails no modo de pesquisa	X	X
Inserir imagens em linha	X	X
Atualizar para o Exchange ActiveSync (EAS) versão 16	X	X
Impedir que os usuários usem domínios desconhecidos ou pessoais	X	
Suporte para telas de dispositivo super largas		X
Configurar várias contas do Exchange	X	X
Deslizar para a esquerda ou para a direita para mais ações	X	X
Criptografar respostas ou encaminhamentos de emails criptografados	X	
Impressão de emails e imagens incorporadas	X	
Use Visualização das linhas nas configurações para configurar quantas linhas do corpo de um email são exibidas como visualização no modo de exibição de caixas de correio.	X	

Recurso	iOS	Android
Suporte para emails responsivos	X	X
Visualização de anexos dentro do aplicativo (MS Office ou imagens).	X	X
Grupos de contatos pessoais	X	X
Migrar nomes de usuário (UPN) para endereços de email	X	X
Relatar emails de phishing	X	X
Autenticação moderna (OAuth)	X	X
Imprimir anexos	X	
Android Enterprise (Android for Work)	X	
Assinaturas em Rich Text	X	
Notificações por push em rich text	X	
Feeds	X	X
Melhorias no anexo de fotos	X	X
Notificações em grupo	X	
Integração do Slack (visualização)	X	X
Gerenciar feeds	X	
Domínios internos	X	X
Gerenciar seus feeds	X	X
Integração do MS Teams	X	X
Opção de autodiagnóstico (**solução de problemas**)		X
Modo duplo (MAM SDK)	X	X
Ferramenta de autodiagnóstico		X
Calendário		
Visualizar e importar arquivos ICS como eventos de calendário		X

Recurso	iOS	Android
Arrastar e soltar eventos do calendário	X	X
Modos de exibição de dia, semana, mês e agenda	X	X
Lembretes detalhados na tela de bloqueio	X	X
Sincronizar por seis meses	X	X
Definir eventos como particulares	X	X
Rolar para a hora antes do primeiro evento	X	
Opções de atualização manual	X	X
Definir lembretes	X	X
Toque para mapear endereços	X	X
Números das semanas	X	X
Suporte de tipo dinâmico	X	X
Marcadores de classificação de segurança	X	X
Toques longos em endereços	X	
Definir dia inicial da semana de trabalho	X	X
Concentrar o foco na semana da data selecionada	X	
Data atual sempre realçada	X	X
Anexos de calendário do repositório de anexos	X	X
Suporte ao calendário pessoal	X	X
Exibição entra em conflito com os eventos de calendário pessoal		X
Imprimir eventos de calendário	X	
Toque em números de telefone e endereços da web em uma linha de assunto do calendário	X	

Recurso	iOS	Android
Pesquisar no calendário	X	
Reuniões		
Responder, responder a todos, encaminhar reuniões	X	X
Modo de exibição de organizador de respostas a convites	X	X
Modo de exibição de organizador de disponibilidade de convidados com disponibilidade sugerida	X	X
Toque para ingressar em reuniões online. **Nota:** para WebEx e Lync, você deve configurar políticas no Citrix Endpoint Management para habilitar estes aplicativos.	X	X
Toque para ingressar em conferências de áudio	X	X
Agendar reunião online, áudio, conferência em novo convite	X	X
Adicionar links do ShareFile para novos convites	X	X
Encaminhar convites com anexos	X	X
Toque para enviar email de ‘‘vou me atrasar’’	X	X
Toque para responder ao organizador da reunião	X	X
Toque para responder a todos os convites para a reunião	X	X
Toque para responder a todos os convidados para a reunião	X	X
Toque para responder a todos os convidados com anexos	X	X
Discar para entrar em GoToMeeting	X	X

Recurso	iOS	Android
Responder ao convite de tela de bloqueio de tela ou notificação	X	X
Discar para entrar em reuniões de WebEx ou Lync	X	X
Ocultar eventos recusados	X	X
Exibir mais de 3 eventos simultâneos	X	X
Exibição rápida de status de convidado	X	X
Excluir, responder, responder a todos, adicionar comentários sobre eventos cancelados	X	X
Mostrar nome do organizador em convites encaminhados	X	X
Dispositivos compartilhados	X	X
Entrar em reuniões do Skype for Business	X	X
Responder às notificações de reunião, como Aceitar, Recusar e Tentativa.	X	X
Responder a notificações de mensagem com Responder e Excluir	X	
Contatos		
Criar pastas em **Contatos**		X
Sincronização de contato bidirecional	X	X
Informações detalhadas de contato (busca GAL)	X	X
Exportação e sincronização de contatos do Secure Mail com os contatos locais	X	X
Contatos: Favoritos e Categoria		X
Controlar quais campos de contato são exportados	X	X

Recurso	iOS	Android
Detalhes de contato não Secure Mail	X	X
Suporte de tipo dinâmico	X	X
Marcar contatos como VIPs	X	X
Compartilhar contatos com `.vcards`	X	X
Exibir contatos com pressionamento longo		X
Exportar contatos, mesmo que exista conta de email nativa	X	X
Exibir pastas e subpastas	X	
Configurações definidas no dispositivo		
Suporte a iMessage	X	
Opções avançadas para notificações de controle	X	X
Controle de notificação de bloqueio de tela	X	X
Sons de notificação de email e calendário	X	X
Atualização automática de pastas	X	X
Configurar notificações de fora do escritório internas e externas	X	X
Perguntar antes de excluir	X	X
Exibições de conversa encadeada ou cronológicas	X	X
Carregar anexos em Wi-Fi	X	X
Atribuir valor padrão aos anexos em Wi-Fi	X	X
Definir período de sincronização de email	X	X
Sincronização ilimitada/sincronizar todos os emails		X

Recurso	iOS	Android
Definir assinatura de email	X	X
Lista de contatos por nome ou sobrenome	X	X
Avanço automático	X	X
Usar o fuso horário local		X
Modelos de resposta rápida		X
Enviar frequência de configuração de email		X
Exportação/importação de configurações	X	X
Toque no botão Voltar no dispositivo para descartar as opções do botão de ação flutuante		X
Microsoft Teams	X	X

Citrix Secure Web

Recurso	iOS	Android
Usar dois aplicativos simultaneamente com Multitarefa	X	
Baixar arquivos	X	X
Adicionar favoritos	X	X
Limpar os nomes de usuário e senhas salvas	X	X
Excluir cache/histórico/cookies	X	X
Bloquear pop-ups	X	X
Salvar páginas offline	X	X
Pesquisar na barra de endereços	X	X
Abrir itens baixados de notificações	X	X

Recurso	iOS	Android
Senhas salvas automaticamente	X	X
Suporte a proxy		
Proxies empresariais	X	X
Listas de permissão e listas de bloqueio de URL	X	X
Histórico	X	X
Página inicial padrão	X	X
Guias	X	X
Enviar indicadores	X	X
Bloco de captura de tela		X
Pesquisar na página atual	X	X
Ações de toque 3D	X	
Dispositivos compartilhados	X	X
Proteção contra violação de arquivos com dispositivos compartilhados	X	
Exportação/importação de configurações	X	X
Modo de retrato e paisagem	X	X
Android Enterprise (Android for Work)		X
Puxe para atualizar o conteúdo na tela	X	X
Secure Web como navegador padrão		X

Citrix Secure Hub

June 6, 2024

O Citrix Secure Hub é a plataforma de lançamento dos aplicativos móveis de produtividade. Os

usuários registram seus dispositivos no Secure Hub para obter acesso à loja de aplicativos. Na loja de aplicativos, eles podem adicionar aplicativos móveis de produtividade desenvolvidos pela Citrix e aplicativos de terceiros.

Você pode baixar o Secure Hub e outros componentes da Página de downloads do Citrix Endpoint Management.

Quanto ao Secure Hub e outros requisitos de sistema de aplicativos móveis de produtividade, consulte os Requisitos do sistema.

Para obter as mais recentes informações sobre aplicativos móveis de produtividade, consulte Anúncios recentes.

As seções a seguir listam os novos recursos nas versões atual e anteriores do Secure Hub.

> **Observação:**
>
> O suporte para as versões Android 6.x e iOS 11.x do Secure Hub foi encerrado em outubro de 2023.

O que há de novo na versão atual

Secure Hub para iOS 24.5.0

Compatível com o Return to Service do iOS 17

O Secure Hub oferece suporte ao recurso Return to Service no iOS 17, que fornece uma experiência de Gerenciamento de Dispositivos Móveis (MDM) mais eficiente e segura. Anteriormente, era necessária uma configuração manual para configurá-lo para um novo usuário após a limpeza do dispositivo. Agora, o recurso Return to Service automatiza esse processo, seja reaproveitando um dispositivo da empresa ou integrando um dispositivo pessoal (BYOD) às políticas de segurança corretas.

Com o recurso Return to Service, o servidor do MDM pode enviar um comando de apagamento que inclui detalhes de Wi-Fi e um perfil de registro de MDM padrão para o dispositivo do usuário. Em seguida, o dispositivo limpa automaticamente todos os dados do usuário, se conecta à rede Wi-Fi especificada e se inscreve novamente no servidor do MDM usando o perfil de registro fornecido.

O que há de novo em versões anteriores

Secure Hub para Android 24.3.0

Compatível com o Samsung Knox Enhanced Attestation v3 O Secure Hub agora oferece suporte ao Samsung Enhanced Attestation v3, aproveitando o atestado Knox para fortalecer as medidas de segurança dos dispositivos Samsung gerenciados pelo Citrix Endpoint Management. Esse protocolo

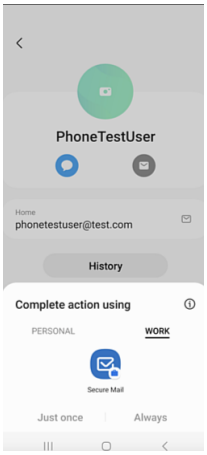
de atestado avançado verifica a integridade e o status de segurança dos dispositivos, garantindo que eles não estejam enraizados e estejam executando o firmware autorizado. O recurso fornece uma camada essencial de proteção contra ameaças à segurança e garante a adesão às políticas de segurança da empresa.

Secure Hub para Android 23.12.0

Segurança aprimorada com o Samsung Knox A adição da política de dispositivos Knox Platform for Enterprise Key no Citrix Endpoint Management aprimora significativamente os recursos de segurança do Secure Hub em dispositivos Samsung. Essa política permite que você forneça as informações de licença necessárias do Samsung Knox Platform for Enterprise (KPE) e use as licenças do KPE para aprimorar a segurança do seu dispositivo Samsung. O Samsung Knox garante que os dados corporativos permaneçam protegidos, ao mesmo tempo em que mantém a facilidade de gerenciamento e uma experiência de usuário tranquila.

Para obter mais informações, consulte a Política de dispositivos Knox Platform for Enterprise Key.

Acessar o Secure Mail no perfil pessoal do usuário Agora, os usuários podem acessar e usar o Secure Mail em seu perfil de trabalho a partir de seu perfil pessoal. Quando os usuários clicam em um endereço de email em seu catálogo de endereços de perfil pessoal, eles têm a opção de usar o Secure Mail em seu perfil de trabalho. Esse recurso oferece conveniência, permitindo que os usuários enviem um email a partir de seu perfil pessoal. Esse recurso é aplicável em dispositivos BYOD ou WPCOD.



Secure Hub para iOS 24.1.0

Esta versão aborda alguns problemas para ajudar a melhorar o desempenho geral e a estabilidade.

Secure Hub para Android 23.12.0

Adicionar uma dica sobre o PIN de autenticação na página de logon A partir da versão 23.12.0, você pode adicionar uma dica sobre o PIN de autenticação na página de logon. Esse recurso é opcional e se aplica a dispositivos registrados para autenticação de dois fatores. A dica permite que você saiba como acessar o PIN.

Você pode configurar uma dica como texto ou link. O texto da dica oferece informações concisas sobre o PIN, enquanto o link fornece informações detalhadas sobre como acessar o PIN. Para obter mais informações sobre como configurar uma dica, consulte Configurar dica por meio do console Citrix Endpoint Management.

A autenticação do nFactor oferece suporte ao recurso de logon único A partir do Secure Hub para Android versão 23.12.0, o registro ou login do nFactor for Mobile Application Management (MAM) oferece suporte ao recurso de logon único (SSO). Esse recurso permite que as credenciais de logon inseridas anteriormente passem pelo processo de registro ou login do MAM, eliminando a necessidade de os usuários inseri-las manualmente novamente. Para obter mais informações sobre a propriedade SSO do nFactor, consulte a Referência de propriedades do cliente na documentação do Citrix Endpoint Management.

Permite limpeza total no modo de inicialização direta Anteriormente, era necessário desbloquear o dispositivo para executar um comando de limpeza completa em um dispositivo reinicializado. Agora, você pode executar um comando de limpeza completa no modo de inicialização direta, mesmo se o dispositivo estiver bloqueado. Esse recurso é útil do ponto de vista da segurança, especialmente quando o dispositivo está na posse de uma pessoa não autorizada. Para obter mais informações sobre o comando de limpeza completa, consulte as ações de segurança na documentação do Citrix Endpoint Management.

A velocidade de carregamento da App Store do Secure Hub foi otimizada A App Store no Secure Hub agora carrega mais rápido do que antes, permitindo que os usuários a acessem mais rapidamente.

Secure Hub para iOS 23.11.0

Adicionar uma dica sobre o PIN de autenticação na página de logon A partir da versão 23.11.0, você pode adicionar uma dica sobre o PIN de autenticação na página de logon. Esse recurso é opcional e se aplica a dispositivos registrados para autenticação de dois fatores. A dica permite que você saiba como acessar o PIN.

Você pode configurar uma dica como texto ou link. O texto da dica oferece informações concisas sobre o PIN, enquanto o link fornece informações detalhadas sobre como acessar o PIN. Para obter mais informações sobre como configurar uma dica, consulte o artigo Configurar dica por meio do console Citrix Endpoint Management.

A autenticação do nFactor oferece suporte ao recurso de logon único A partir do Secure Hub para iOS versão 23.11.0, o registro ou logon do nFactor for Mobile Application Management (MAM) oferece suporte ao recurso de logon único (SSO). Esse recurso permite que as credenciais de logon inseridas anteriormente passem pelo processo de registro ou logon do MAM, eliminando a necessidade de os usuários inseri-las manualmente novamente.

Para obter mais informações sobre a propriedade SSO do nFactor, consulte a Referência de propriedades do cliente na documentação do Citrix Endpoint Management.

Secure Hub 23.10.0

Secure Hub para Android

O Secure Hub para Android 23.10.0 é compatível com o Android 14. A atualização para a versão 23.10.0 do Secure Hub garante suporte contínuo para dispositivos atualizados para o Android 14.

Secure Hub 23.9.0

Secure Hub para Android

Esta versão aborda áreas que melhoram o desempenho geral e a estabilidade.

Secure Hub 23.8.1

Secure Hub para iOS Esta versão aborda alguns problemas para ajudar a melhorar o desempenho geral e a estabilidade.

Secure Hub 23.8.0

Secure Hub para iOS Esta versão aborda alguns problemas para ajudar a melhorar o desempenho geral e a estabilidade.

Secure Hub 23.7.0

Secure Hub para Android

API Play Integrity Em breve, a API SafetyNet Attestation será preterida pelo Google de acordo com o cronograma de descontinuação e migrada para a API Play Integrity sugerida.

Para obter mais informações, consulte API Play Integrity no documento do Citrix Endpoint Management.

Para obter detalhes sobre a substituição, consulte as Substituições e remoções no documento do Citrix Endpoint Management.

Para ler sobre o recurso Android SafetyNet, consulte SafetyNet

Secure Hub 23.4.0

Secure Hub para iOS

Experiência de usuário aprimorada A partir da versão 23.4.0, o Secure Hub para iOS aprimora as seguintes experiências do usuário:

- Experiência na loja:

  Anteriormente, a página Meus aplicativos aparecia primeiro. Na versão 23.4.0, a página da Loja aparece primeiro.

  Anteriormente, a loja do Secure Hub executava a ação de recarga sempre que o usuário clicava na opção Loja.

  Na versão 23.4.0, a experiência do usuário foi aprimorada. Agora, o aplicativo é recarregado quando o usuário inicia o aplicativo pela primeira vez, reinicia o aplicativo ou desliza a tela para baixo.

- Interface do usuário: anteriormente, a opção Fazer logoff era posicionada na parte inferior esquerda da tela. Na versão 23.4.0, a opção Fazer logoff faz parte do menu principal e fica acima da opção Sobre.
- Hiperlinks: anteriormente, os hiperlinks na página de detalhes do aplicativo apareciam como texto sem formatação. Na versão 23.4.0, os hiperlinks são clicáveis e têm uma formatação sublinhada para indicar links.

Experiência de transição de MDX para MAM SDK A partir da versão 23.4.0, a experiência de transição do MDX herdado para o MAM SDK foi aprimorada para aplicativos iOS de modo duplo. Esse recurso melhora a experiência do usuário ao usar aplicativos móveis de produtividade, reduzindo as mensagens de alerta e migrando para o Secure Hub.

Usar o PIN da Citrix para desbloquear aplicativos Anteriormente, o usuário final digitava a senha do dispositivo para desbloquear aplicativos baseados em Gerenciamento de Aplicativo Móvel (MAM).

A partir da versão 23.4.0, o usuário final pode inserir o PIN da Citrix como senha para desbloquear o aplicativo baseado em MAM. Os administradores podem configurar a complexidade da senha usando as propriedades do cliente no servidor CEM.

Sempre que o aplicativo ficar inativo por mais tempo do que o permitido, os usuários finais podem inserir o PIN da Citrix para desbloquear o aplicativo, dependendo da configuração definida pelos administradores.

No Secure Hub para Android, há uma propriedade de cliente separada para configurar como lidar com o timer de inatividade em aplicativos MAM. Para obter mais informações, consulte Timer de inatividade para Android separado.

Secure Hub 23.4.1

Secure Hub para Android Esta versão aborda alguns problemas para ajudar a melhorar o desempenho geral e a estabilidade.

Secure Hub 23.4.0

Secure Hub para Android Esta versão aborda alguns problemas para ajudar a melhorar o desempenho geral e a estabilidade.

Secure Hub 23.2.0

Secure Hub para Android

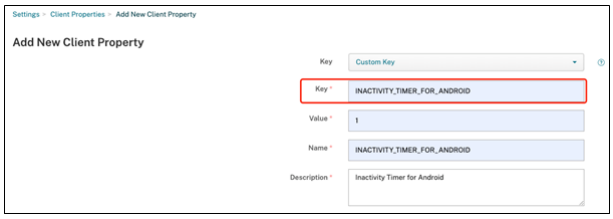
> **Nota:**
>
> - Nenhum dado analítico é coletado dos usuários da União Europeia (UE), Espaço Econômico Europeu (EEE), Suíça e Reino Unido.

VPN MDX em modo de túnel completo O MDX Micro VPN (modo de túnel completo) foi preterido.

Para obter mais informações, consulte Substituição na documentação do Citrix Endpoint Management.

Timer de inatividade para Android separado Anteriormente, a propriedade do cliente **Timer de inatividade** era comum no Secure Hub para Android e iOS.

A partir da versão 23.2.0, um administrador de TI pode usar a nova propriedade do cliente **Inactivity_Timer_For_Android** para separar o timer de inatividade do iOS. Um administrador de TI pode definir o **Valor** de **Inactivity_Timer_For_Android** como 0 para desativar o timer de inatividade do Android de forma independente. Dessa forma, todos os aplicativos no perfil de trabalho, incluindo o Secure Hub, desafiam somente o PIN de trabalho.



Para obter mais informações sobre como adicionar e modificar uma propriedade de cliente, consulte Propriedades do cliente na documentação do XenMobile.

Secure Hub 22.11.0

Secure Hub para Android Esta versão inclui correções de bugs.

Secure Hub 22.9.0

Secure Hub para Android Esta versão inclui:

- Complexidade do código secreto do dispositivo (Android 12+)
- Suporte para SDK 31
- Correções de bugs

Complexidade do código secreto do dispositivo (Android 12+) A complexidade do código secreto é preferível a um requisito de senha personalizada. O nível de complexidade do código secreto é um dos níveis predefinidos. Portanto, o usuário final não consegue definir uma senha com um nível de complexidade menor.

A complexidade do código secreto para dispositivos com Android 12+ é a seguinte:

- **Aplique a complexidade do código secreto:** exige uma senha com um nível de complexidade definido pela plataforma, em vez de um requisito de senha personalizada. Somente para dispositivos com Android 12+ e usando o Secure Hub 22.9 ou posterior.
- **Nível de complexidade:** níveis predefinidos de complexidade da senha.
  - **Nenhum:** não é necessária uma senha.

- **Baixo:** as senhas podem ser:
  - Um padrão
  - Um PIN com no mínimo quatro números
- **Médio:** as senhas podem ser:
  - Um PIN sem sequências repetidas (4444) ou sequências ordenadas (1234) e um mínimo de quatro números
  - Alfabéticas, com um mínimo de quatro caracteres
  - Alfanuméricas, com um mínimo de quatro caracteres
- **Alto:** as senhas podem ser:
  - Um PIN sem sequências repetidas (4444) ou sequências ordenadas (1234) e um mínimo de oito números
  - Alfabéticas, com um mínimo de seis caracteres
  - Alfanuméricas, com um mínimo de seis caracteres

> **Notas:**
>
> - Para dispositivos BYOD, as configurações de código secreto, como Tamanho mínimo, Caracteres obrigatórios, Reconhecimento biométrico e Regras avançadas, não se aplicam ao Android 12+. Em vez disso, use a complexidade do código secreto.
> - Se a complexidade do código secreto para o perfil de trabalho estiver ativada, a complexidade do código secreto para o lado do dispositivo também deverá estar ativada.

Para obter mais informações, consulte Configurações do Android Enterprise na documentação do Citrix Endpoint Management.

Secure Hub 22.7.0

Secure Hub para Android Esta versão inclui correções de bugs.

Secure Hub 22.6.0

Secure Hub para Android Esta versão inclui correções de bugs.

Secure Hub 22.5.0

Secure Hub para iOS Esta versão inclui correções de bugs.

Secure Hub 22.4.0

Secure Hub para Android Esta versão inclui correções de bugs.

Secure Hub 22.2.0

Secure Hub para iOS Esta versão inclui correções de bugs.

Secure Hub para Android Esta versão inclui correções de bugs.

Secure Hub 21.11.0

Secure Hub para Android

Suporte para Perfil de trabalho para dispositivos de propriedade da empresa Em dispositivos Android Enterprise, agora você pode registrar o Secure Hub no modo Perfil de trabalho em dispositivos de propriedade da empresa. Esse recurso está disponível em dispositivos com Android 11 ou posterior. Os dispositivos previamente registrados no modo COPE (propriedade da empresa, habilitado pessoalmente) migram automaticamente para o modo Perfil de trabalho para dispositivos de propriedade da empresa quando o dispositivo é atualizado do Android 10 para o Android 11 ou posterior.

Secure Hub 21.10.0

Secure Hub para iOS Esta versão inclui correções de bugs.

Secure Hub para Android **Suporte para Android 12**. A partir desta versão, o Secure Hub é compatível com dispositivos que executam o Android 12.

Secure Hub 21.8.0

Secure Hub para iOS Esta versão inclui correções de bugs.

Secure Hub 21.7.1

Secure Hub para Android **Suporte para Android 12 em dispositivos já registrados.** Se você estiver pensando em atualizar para o Android 12, certifique-se de atualizar o Secure Hub para a versão 21.7.1 primeiro. O Secure Hub 21.7.1 é a versão mínima necessária para atualizar para o Android 12. Essa versão garante a atualização descomplicada do Android 11 para o Android 12 para usuários já registrados.

> **Nota:**
>
> Se o Secure Hub não for atualizado para a versão 21.7.1 antes de você atualizar para o Android 12, o dispositivo exigirá um novo registro ou uma redefinição de fábrica para recuperar a funcionalidade anterior.
>
> A Citrix está comprometida em fornecer suporte de Dia 1 para o Android 12 e adicionará mais atualizações às versões subsequentes do Secure Hub para oferecer suporte total ao Android 12.

Secure Hub 21.7.0

Secure Hub para iOS Esta versão inclui correções de bugs.

Secure Hub para Android Esta versão inclui correções de bugs.

Secure Hub 21.6.0

Secure Hub para iOS Esta versão inclui correções de bugs.

Secure Hub para Android Esta versão inclui correções de bugs.

Secure Hub 21.5.1

Secure Hub para iOS Esta versão inclui correções de bugs.

Secure Hub para Android Esta versão inclui correções de bugs.

Secure Hub 21.5.0

Secure Hub para iOS Nesta versão, os aplicativos com MDX Toolkit versão 19.8.0 ou anterior não funcionarão mais. Certifique-se de preparar seus aplicativos com o MDX Toolkit mais recente para retomar a funcionalidade adequada.

Secure Hub 21.4.0

Aprimoramento de cores no Secure Hub. O Secure Hub está em conformidade com as atualizações de cores da marca Citrix.

Secure Hub 21.3.2

Secure Hub para iOS Esta versão inclui correções de bugs.

Secure Hub 21.3.0

Esta versão inclui correções de bugs.

Secure Hub 21.2.0

Secure Hub para Android Esta versão inclui correções de bugs.

Secure Hub 21.1.0

Secure Hub para iOS Esta versão inclui correções de bugs.

Secure Hub para Android Esta versão inclui correções de bugs.

Secure Hub 20.12.0

Secure Hub para iOS Esta versão inclui correções de bugs.

Secure Hub para Android O Secure Hub para Android suporta o modo de inicialização direta. Para obter mais informações sobre o modo de inicialização direta, consulte a documentação do Android em *Developer.android.com.*

Secure Hub 20.11.0

Secure Hub para Android O Secure Hub oferece suporte aos requisitos atuais de API de destino do Google Play para Android 10.

Secure Hub 20.10.5

Esta versão inclui correções de bugs.

Secure Hub 20.9.0

Secure Hub para iOS O Secure Hub para iOS suporta iOS 14.

Secure Hub para Android Esta versão inclui correções de bugs.

Secure Hub 20.7.5

Secure Hub para Android

- O Secure Hub para Android suporta o Android 11.
- **Transição do Secure Hub 32 bits para 64 bits para aplicativos**. Na versão 20.7.5 do Secure Hub, o suporte se encerra para a arquitetura de 32 bits para aplicativos, e o Secure Hub foi atualizado para 64 bits. A Citrix recomenda que os clientes atualizem da versão 20.6.5 para a 20.7.5. Se os usuários ignorarem a atualização para o Secure Hub versão 20.6.5 e, em vez disso, atualizarem diretamente da 20.1.5 para a 20.7.5, eles precisarão autenticar novamente. A reautenticação envolve inserir credenciais e redefinir o PIN do Secure Hub. O Secure Hub versão 20.6.5 está disponível na Google Play Store.
- **Instale atualizações a partir da App Store.** No Secure Hub para Android, se houver atualizações disponíveis para aplicativos, o aplicativo será realçado e o recurso **Atualizações disponíveis** aparecerá na tela da App Store.

  Ao tocar em **Atualizações disponíveis**, você navega até a loja que mostra a lista de aplicativos com atualizações pendentes. Toque em **Detalhes** no aplicativo para instalar as atualizações. Quando o aplicativo for atualizado, a seta para baixo em **Detalhes** mudará para uma marca de seleção.

Secure Hub 20.6.5

Secure Hub para Android **Transição de 32 bits para 64 bits para aplicativos.** A versão 20.6.5 do Secure Hub é a versão final que suporta uma arquitetura de 32 bits para aplicativos móveis Android. Nas versões subsequentes, o Secure Hub oferece suporte à arquitetura de 64 bits. A Citrix recomenda que os usuários atualizem para o Secure Hub versão 20.6.5, para que assim os usuários possam atualizar para versões posteriores sem reautenticação. Se os usuários ignorarem a atualização para o Secure Hub versão 20.6.5 e, em vez disso, atualizarem diretamente para 20.7.5, eles precisarão autenticar novamente. A reautenticação envolve inserir credenciais e redefinir o PIN do Secure Hub.

> **Nota:**
>
> A versão 20.6.5 não bloqueia o registro de dispositivos que executam o Android 10 no modo de administrador do dispositivo.

Secure Hub para iOS **Ativar um proxy configurado em dispositivos iOS.** O Secure Hub para iOS requer que você habilite uma nova propriedade de cliente, `ALLOW_CLIENTSIDE_PROXY`, se quiser

permitir que os usuários usem servidores proxy configurados em **Ajustes > Wi-Fi**. Para obter mais informações, consulte `ALLOW_CLIENTSIDE_PROXY` na referência de propriedades de cliente.

Secure Hub 20.3.0

> **Nota:**
>
> O suporte para as versões Android 6.x e iOS 11.x do Secure Hub, Secure Mail, Secure Web e aplicativo Citrix Workspace termina em junho de 2020.

Secure Hub para iOS

- **Extensão de rede desativada.** Devido a alterações recentes nas Diretrizes de Revisão da App Store, a partir da versão 20.3.0, o Secure Hub não dará suporte à Extensão de Rede (NE) em dispositivos com iOS. A NE não tem impacto nos aplicativos móveis de produtividade desenvolvidos pela Citrix. No entanto, a remoção da NE tem um certo impacto em aplicativos MDX preparados empresarialmente e implantados. Os usuários finais podem experimentar mudanças extras no Secure Hub durante a sincronização de componentes, como tokens de autorização, timers e tentativas de PIN. Para obter mais informações, consulte https://support.citrix.com/article/CTX270296.

> **Nota:**
>
> Novos usuários não são solicitados a instalar a VPN.

- **Suporte para perfis de registro aprimorado.** O Secure Hub oferece suporte aos recursos de perfil de registro aprimorado anunciados para o Citrix Endpoint Management no suporte para perfil de registro.

Secure Hub 20.2.0

Secure Hub para iOS Esta versão inclui correções de bugs.

Secure Hub 20.1.5

Esta versão inclui:

- Atualização à formatação e exibição da política de privacidade do usuário. Esta atualização de recurso altera o fluxo de registro do Secure Hub.
- Correções de bugs.

Secure Hub 19.12.5

Esta versão inclui correções de bugs.

Secure Hub 19.11.5

Esta versão inclui correções de bugs.

Secure Hub 19.10.5

Secure Hub para Android **Registrar o Secure Hub no modo COPE.** Em dispositivos Android Enterprise, registre o Secure Hub no modo COPE (Propriedade da empresa, habilitado pessoalmente) quando o Citrix Endpoint Management estiver configurado no perfil de registro COPE.

Secure Hub 19.10.0

Esta versão inclui correções de bugs.

Secure Hub 19.9.5

Secure Hub para iOS Esta versão inclui correções de bugs.

Secure Hub para Android **Suporte para gerenciar recursos do keyguard para o perfil de trabalho Android Enterprise e dispositivos totalmente gerenciados.** O Android keyguard gerencia as telas de bloqueio de dispositivo e de Work Challenge. Use a política de dispositivo de Gerenciamento de Keyguard no Citrix Endpoint Management para controlar o gerenciamento de keyguard em dispositivos de perfil de trabalho e o gerenciamento de keyguard em dispositivos totalmente gerenciados e dedicados. Com o gerenciamento de keyguard, você pode especificar os recursos disponíveis para os usuários, como agentes de confiança e câmera segura, antes que eles desbloqueiem a tela de keyguard. Ou, você pode optar por desativar todos os recursos de proteção do teclado.

Para obter mais informações sobre as configurações do recurso e como configurar a política de dispositivo, consulte a política de gerenciamento de proteção do teclado.

Secure Hub 19.9.0

Secure Hub para iOS O Secure Hub para iOS suporta iOS 13.

Secure Hub para Android Esta versão inclui correções de bugs.

Secure Hub para Android 19.8.5

Esta versão inclui correções de bugs.

Secure Hub 19.8.0

Secure Hub para iOS Esta versão inclui melhorias de desempenho e correções de bugs.

Secure Hub para Android **Suporte para Android Q.** Esta versão inclui suporte para Android Q. Antes de atualizar para a plataforma Android Q, consulte Migrar do Device Administration para o Android Enterprise para obter informações sobre como a substituição de APIs do Google Device Administration afeta os dispositivos que executam o Android Q. Consulte também o blog, Citrix Endpoint Management e Android Enterprise –uma temporada de mudanças.

Secure Hub 19.7.5

Secure Hub para iOS Esta versão inclui melhorias de desempenho e correções de bugs.

Secure Hub para Android **Suporte para Samsung Knox SDK 3.x.** O Secure Hub para Android dá suporte a Samsung Knox SDK 3.x. Para obter mais informações sobre como migrar para o Samsung Knox 3.x, consulte a documentação do desenvolvedor do Samsung Knox. Esta versão também inclui suporte para os novos espaços de nome Samsung Knox. Para obter mais informações sobre alterações aos espaços de nome antigos do Samsung Knox, consulte Changes to old Samsung Knox namespaces.

> **Nota:**
>
> O Secure Hub para Android não dá suporte ao Samsung Knox 3.x em dispositivos com Android 5.

Secure Hub 19.3.5 a 19.6.6

Estas versões incluem melhorias de desempenho e correções de bugs.

Secure Hub 19.3.0

Suporte para Samsung Knox Platform for Enterprise. O Secure Hub para Android suporta o Knox Platform for Enterprise (KPE) em dispositivos Android Enterprise.

Secure Hub 19.2.0

Esta versão inclui melhorias de desempenho e correções de bugs.

Secure Hub 19.1.5

O Secure Hub para Android Enterprise agora oferece suporte às seguintes políticas:

- **Política de dispositivo WiFi.** A política de dispositivo Wi-Fi agora suporta o Android Enterprise. Para obter mais informações sobre esta política, consulte a Política de dispositivo Wi-Fi.
- **Política de dispositivo de XML personalizado.** A política de dispositivo XML personalizada agora suporta o Android Enterprise. Para obter mais informações sobre esta política, consulte a Política de dispositivo XML personalizado.
- **Política de dispositivo de arquivo.** Você pode adicionar arquivos de script no Citrix Endpoint Management para executar funções em dispositivos Android Enterprise. Para obter mais informações sobre esta política, consulte a Política de dispositivo de arquivos.

Secure Hub 19.1.0

O Secure Hub oferece aprimoramento de fontes, cores e outras melhorias na interface do usuário. Esse aprimoramento fornece uma experiência melhor ao usuário, alinhando-se com a estética da marca Citrix utilizada em nosso conjunto completo de aplicativos móveis de produtividade.

Secure Hub 18.12.0

Esta versão inclui melhorias de desempenho e correções de bugs.

Secure Hub 18.11.5

- **Configurações de política do dispositivo de restrições para Android Enterprise.** As novas configurações da política de dispositivos Restrições permitem que os usuários acessem esses recursos em dispositivos Android Enterprise: barra de status, proteção de tela de bloqueio, gerenciamento de conta, compartilhamento de localização e manutenção da tela do dispositivo ativada em dispositivos Android Enterprise. Para obter informações, consulte Política de dispositivo Restrições.

O Secure Hub 18.10.5 a 18.11.0 inclui aprimoramentos de desempenho e correções de bugs.

Secure Hub 18.10.0

- **Suporte para o modo Samsung DeX:** o Samsung DeX permite que os usuários conectem dispositivos habilitados para KNOX a um monitor externo para usar aplicativos, revisar documentos e assistir a vídeos em uma interface semelhante a um PC. Para obter informações sobre os requisitos do dispositivo Samsung DeX e configurar o Samsung DeX, consulte How Samsung DeX work.

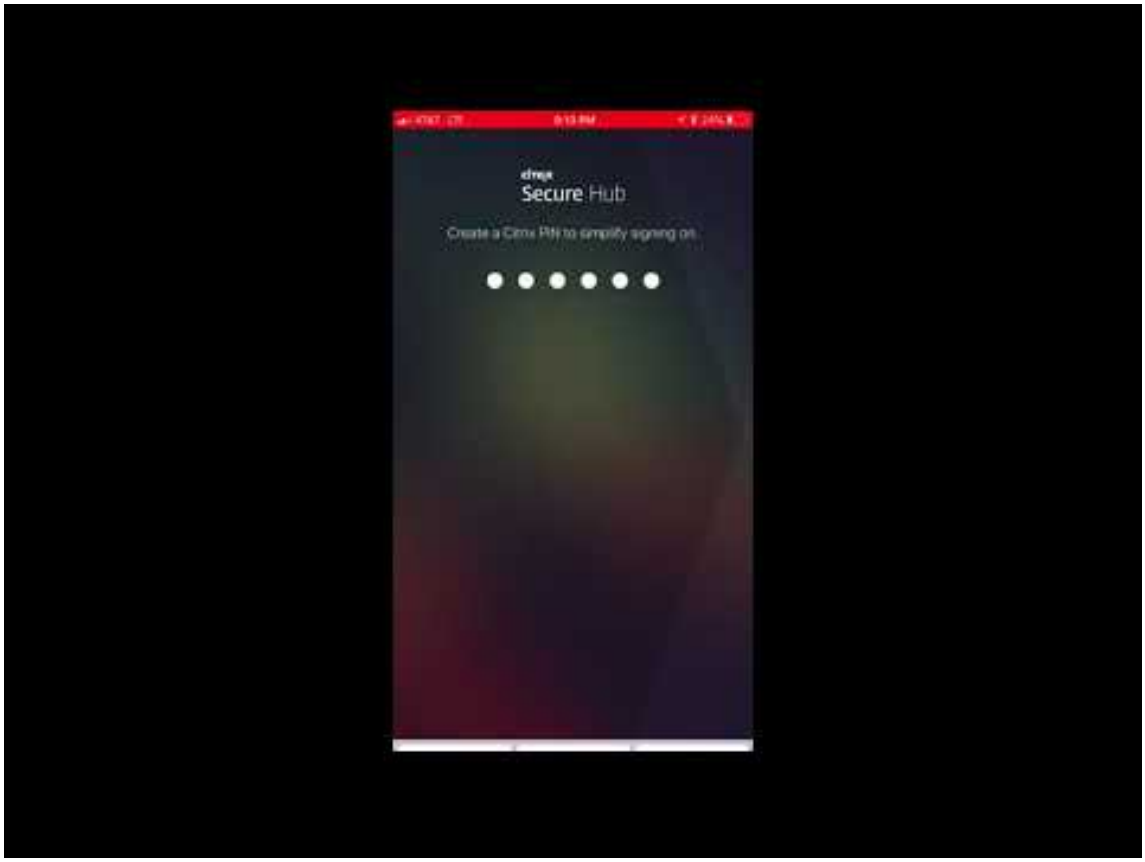
  Para configurar os recursos do modo Samsung DeX no Citrix Endpoint Management, atualize a política de dispositivo Restrições para o Samsung Knox. Para obter informações, consulte **Configurações do Samsung KNOX** em Política de dispositivo Restrições.
- **Suporte para Android SafetyNet:** você pode configurar o Endpoint Management para usar o recurso **Android SafetyNet** para avaliar a compatibilidade e a segurança de dispositivos Android que têm o Secure Hub instalado. Os resultados podem ser usados para acionar ações automatizadas nos dispositivos. Para obter informações, consulte Android SafetyNet.
- **Prevenir o uso da câmera em dispositivos Android Enterprise:** a nova configuração **Permitir o uso da câmera** da política de dispositivo Restrições permite impedir que os usuários usem a câmera em seus dispositivos Android Enterprise. Para obter informações, consulte Política de dispositivo Restrições.

Secure Hub 10.8.60 a 18.9.0

Estas versões incluem melhorias de desempenho e correções de bugs.

Secure Hub 10.8.60

- Suporte para o idioma polonês.
- Suporte para Android P.
- Suporte para o uso da loja de aplicativos do Workspace.
  Ao abrir o Secure Hub, os usuários não verão mais a loja de aplicativos do Secure Hub. O botão **Adicionar aplicativos** leva os usuários para a loja de aplicativos do Workspace. O vídeo a seguir mostra um dispositivo iOS executando uma inscrição no Citrix Endpoint Management usando o aplicativo Citrix Workspace.



> Importante:
>
> Este recurso está disponível apenas para novos clientes. Atualmente, não oferecemos suporte à migração para clientes existentes.

Para usar esse recurso, configure o seguinte:

- Ative as políticas de Senha em cache e Autenticação de senha. Para obter mais informações sobre como configurar as políticas, consulte Resumo das políticas de MDX para aplicativos móveis de produtividade.
- Configurar a autenticação do Active Directory como AD ou AD+Cert. Damos suporte a esses dois modos. Para obter mais informações sobre como configurar a autenticação, consulte Autenticação de domínio ou de domínio mais token de segurança.
- Habilite a integração do Workspace para o Endpoint Management. Para obter mais informações sobre a integração do espaço de trabalho, consulte Configurar espaços de trabalho.

> **Importante:**
>
> Depois que esse recurso é ativado, o SSO do Citrix Files ocorre por meio do Workspace e não pelo Endpoint Management (anteriormente, XenMobile). Recomendamos que você

> desative a integração de Citrix Files no console Endpoint Management antes de habilitar a integração do Workspace.

Secure Hub 10.8.55

- A capacidade de transmitir um nome de usuário e senha para o portal Google zero-touch e Samsung Knox Mobile Environment (KME) usando a configuração JSON. Para mais detalhes, consulte o registro em massa do Samsung Knox.
- Quando você ativa certificate pinning, os usuários não podem se registrar no Endpoint Management com um certificado autoassinado. Se os usuários tentarem se registrar ao Endpoint Management com um certificado autoassinado, eles serão avisados de que o certificado não é confiável.

Secure Hub 10.8.25: Secure Hub para Android inclui suporte para dispositivos Android P.

> **Nota:**
>
> Antes de atualizar para a plataforma Android P: certifique-se de que sua infraestrutura de servidor está em conformidade com os certificados de segurança que tenham um nome de host correspondente na extensão subjectAltName (SAN). Para confirmar um nome de host, o servidor deve apresentar um certificado com uma SAN correspondente. Os certificados que não contêm uma SAN correspondente ao nome de host não são mais confiáveis. Para obter detalhes, consulte a documentação do desenvolvedor do Android.

Atualização do Secure Hub para iOS em 19 de março de 2018: O Secure Hub versão 10.8.6 para iOS está disponível para corrigir um problema com a política de aplicativo VPP. Para obter detalhes, consulte este artigo do Citrix Knowledge Center.

Secure Hub 10.8.5: suporte no Secure Hub para Android para o modo COSU para o Android Work (Android for Work). Para obter mais detalhes, consulte Documentação do Citrix Endpoint Management.

Administração do Secure Hub

Você executa a maioria das tarefas administrativas relacionadas ao Secure Hub durante a configuração inicial do Endpoint Management. Para tornar o Secure Hub disponível para os usuários, para iOS e Android, carregue o Secure Hub no iOS App Store e no Google Play Store.

O Secure Hub também atualiza a maioria das políticas de MDX armazenadas no Endpoint Management para os aplicativos instalados quando uma sessão de usuário do Citrix Gateway se renova após autenticação usando o Citrix Gateway.

> **Importante:**
>
> Alterações a qualquer uma dessas políticas exigem que um usuário exclua e reinstale o aplicativo para aplicar a atualização de política: Grupo de Segurança, Ativar criptografia e o Exchange Server do Secure Mail.

PIN da Citrix

Você pode configurar o Secure Hub para usar o PIN da Citrix, um recurso de segurança ativado no console Endpoint Management em **Configurações** > **Propriedades do cliente**. A configuração requer que os usuários de dispositivos móveis registrados façam logon no Secure Hub e ativem os aplicativos MDX incluídos usando um número de identificação pessoal (PIN).

O recurso de PIN da Citrix simplifica a experiência de autenticação do usuário ao fazer logon nos aplicativos seguros preparados. Os usuários não precisam inserir outra credencial, como o nome de usuário e a senha do Active Directory, repetidamente.

Os usuários que fazem logon no Secure Hub pela primeira vez precisam inserir seu nome de usuário e senha do Active Directory. Durante o logon, o Secure Hub salva as credenciais do Active Directory ou um certificado de cliente no dispositivo do usuário e, em seguida, solicita ao usuário para inserir um PIN. Quando o usuário faz logon novamente, ele digita o PIN para acessar seus aplicativos Citrix e o Store com segurança, até que o próximo período de tempo limite de ociosidade termine para a sessão de usuário ativa. Propriedades de cliente correlatas permitem criptografar segredos usando o PIN, especificar o tipo de código secreto para PIN e especificar os requisitos de força e comprimento do PIN. Para obter detalhes, consulte Propriedades do cliente.

Quando a autenticação da impressão digital (Touch ID) está ativada, os usuários podem fazer logon usando impressão digital quando for necessária a autenticação offline devido à inatividade de aplicativo. Os usuários ainda têm que inserir um PIN quando fizerem logon ao Secure Hub pela primeira vez ou ao reiniciar o dispositivo, e depois que o tempo limite de inatividade expirar. Para obter informações sobre como habilitar a autenticação de impressão digital, consulte Autenticação por impressão digital ou por Touch ID.

Certificate pinning

O Secure Hub para iOS e Android oferecem suporte a certificate pinning SSL. Esse recurso garante que o certificado assinado por sua empresa seja usado quando clientes Citrix se comunicam com o Endpoint Management, evitando conexões de clientes com o Endpoint Management quando a instalação de um certificado raiz no dispositivo comprometer a sessão SSL. Quando o Secure Hub detecta alterações no servidor chave pública, o Secure Hub nega a conexão.

A partir do Android N, o sistema operacional não permite mais autoridades de certificação (AC) adicionadas pelo usuário. A Citrix recomenda o uso de uma Autoridade de Certificação raiz pública no lugar de uma autoridade de certificação adicionada pelo usuário.

Os usuários que fizerem a atualização para Android N podem ter problemas se usarem autoridades de certificação privadas ou autoassinadas. As conexões em dispositivos Android N são interrompidas nos seguintes cenários:

- Autoridades de certificação privadas/autoassinadas e a opção Required Trusted CA for Endpoint Management está definida como **ON.** Para obter detalhes, consulte Gerenciamento de dispositivos.
- Autoridades de certificação privadas/autoassinadas e o Endpoint Management AutoDiscovery Service (ADS) não estão acessíveis. Devido a questões de segurança, quando ADS não está acessível, a opção Required Trusted CA é **ativada** mesmo que tenha sido definida como **desativada** inicialmente.

Antes de registrar dispositivos ou atualizar o Secure Hub, considere ativar a certificate pinning. A opção está **desativada** por padrão e é gerenciada pelo ADS. Quando você ativa certificate pinning, os usuários não podem se registrar no Endpoint Management com um certificado autoassinado. Se os usuários tentarem se registrar com um certificado autoassinado, eles serão avisados de que o certificado não é confiável. O registro falhará se os usuários não aceitarem o certificado.

Para usar certificate pinning, solicite que a Citrix carregue certificados no seu servidor Citrix ADS. Abra um caso de suporte técnico usando o Citrix Support portal. Lembre-se de não enviar a chave privada para a Citrix. Em seguida, forneça as seguintes informações:

- O domínio que contém as contas com que os usuários se registram.
- O nome de domínio totalmente qualificado (FQDN) do Endpoint Management.
- O nome da instância do Endpoint Management. Por padrão, o nome da instância é zdm e ela diferencia maiúsculas de minúsculas.
- Tipo de ID de usuário, que pode ser UPN ou Email. Como padrão, o tipo é UPN.
- A porta usada para registro de iOS se você tiver alterado o número de porta da porta padrão 8443.
- A porta através da qual o Endpoint Management aceita conexões se você tiver alterado o valor do número de porta padrão 443.
- O URL completo do seu Citrix Gateway.
- Opcionalmente, um endereço de email para o seu administrador.
- Os certificados formatados com PEM que você deseja adicionar ao domínio, que devem ser certificados públicos e não a chave privada.
- Como lidar com os certificados de servidor existentes: remover o certificado de servidor antigo imediatamente (porque está comprometido) ou continuar a dar suporte ao certificado de servidor antigo até que expire.

O caso do suporte técnico caso é atualizado quando seus detalhes e o certificado tiverem sido adicionados aos servidores Citrix.

Certificado + autenticação de senha de uso único

Você pode configurar o Citrix ADC para que o Secure Hub autentique usando um certificado além de um token de segurança que atua como uma senha de uso único. Essa opção fornece uma configuração de alta segurança que não deixa rastros do Active Directory nos dispositivos.

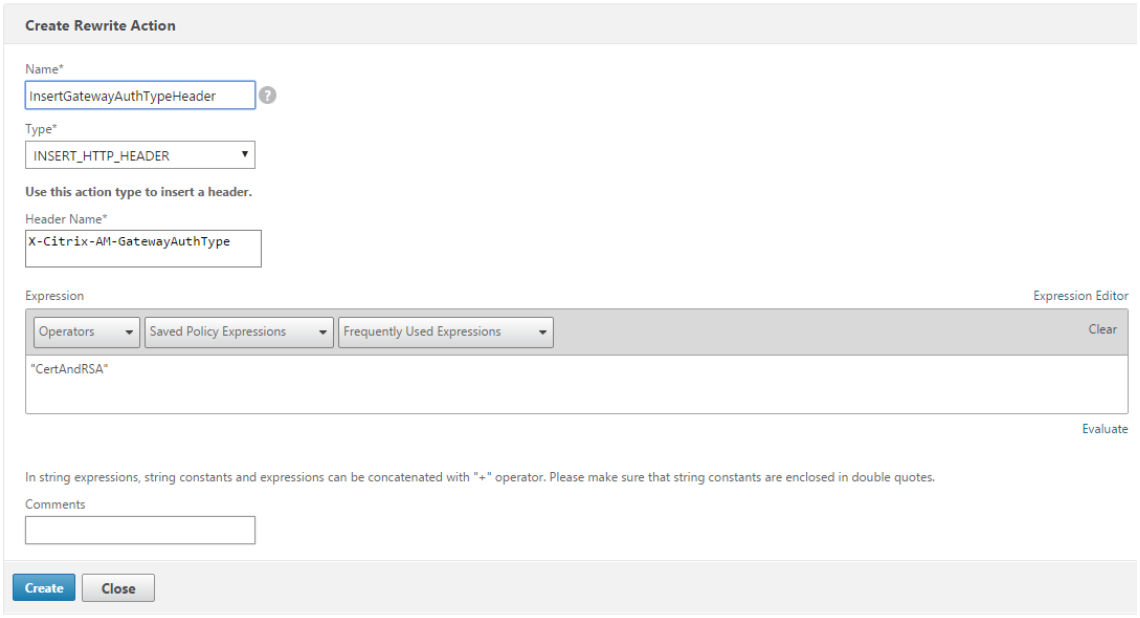
Para ativar o Secure Hub para usar o tipo de autenticação Certificado + Senha de uso único, faça o seguinte: adicione uma ação de regravação e uma política de regravação no Citrix ADC que insira um cabeçalho de resposta personalizado do formulário **X-Citrix-AM-GatewayAuthType: CertAndRSA** para indicar o tipo de logon Citrix Gateway.

Em geral, o Secure Hub usa o tipo de logon do Citrix Gateway configurado no console Endpoint Management. No entanto, essas informações não estão disponíveis para o Secure Hub até que o Secure Hub conclua o logon pela primeira vez. Portanto, o cabeçalho personalizado é obrigatório.

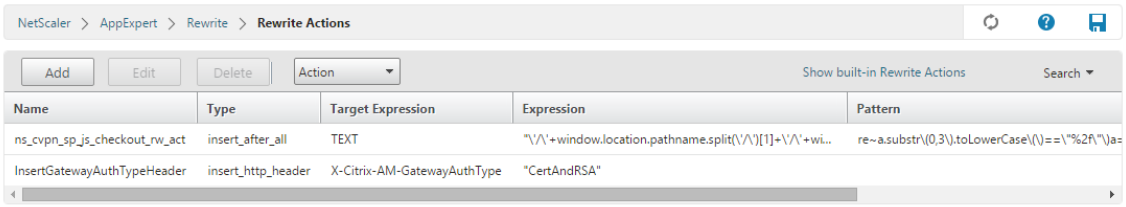
> **Nota:**
>
> Se diferentes tipos de logon forem definidos no Endpoint Management e no Citrix ADC, a configuração do Citrix ADC substituirá. Para obter informações, consulte Citrix Gateway e Endpoint Management.

1. No Citrix ADC, navegue para **Configuration > AppExpert > Rewrite > Actions**.
2. Clique em **Add**.

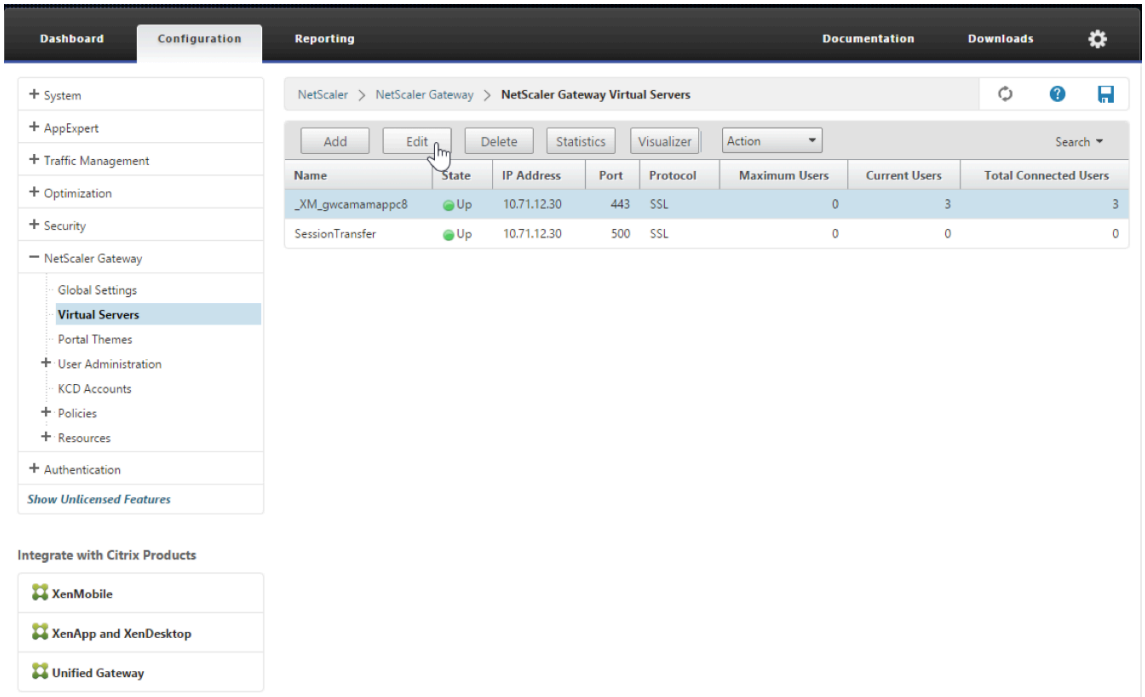
   É exibida a tela **Create Rewrite Action**.
3. Preencha cada campo conforme mostrado na figura a seguir e, em seguida, clique em **Create**.



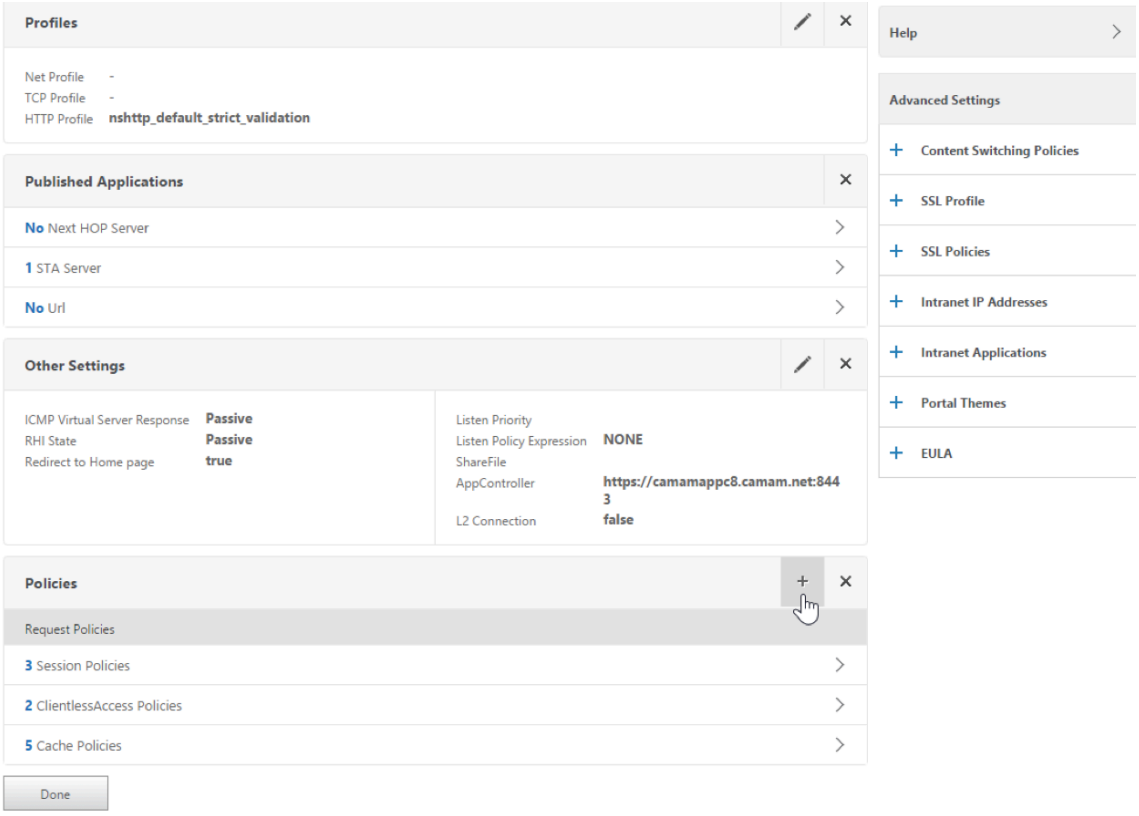
O resultado é exibido na tela principal **Rewrite Actions**.



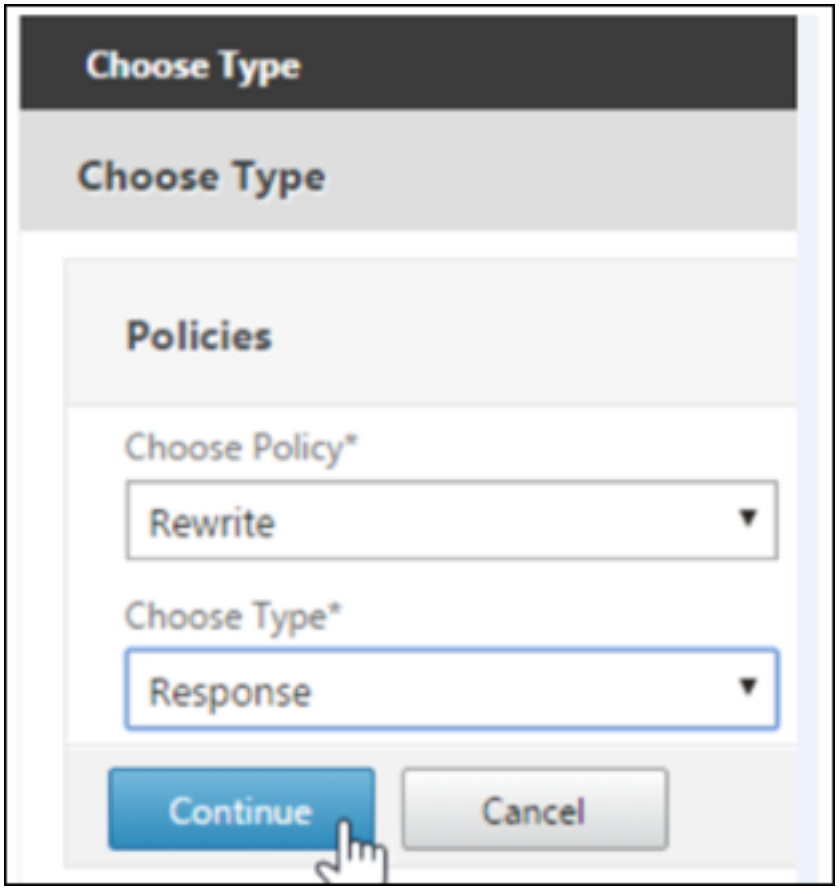
4. Vincule a ação de regravar ao servidor virtual como uma política de regravação. Vá para **Configuration > NetScaler Gateway > Virtual Servers** e selecione seu servidor virtual.



5. Clique em **Edit**.
6. Na tela **Virtual Servers configuration**, role até **Policies**.
7. Clique em **+** para adicionar uma política.

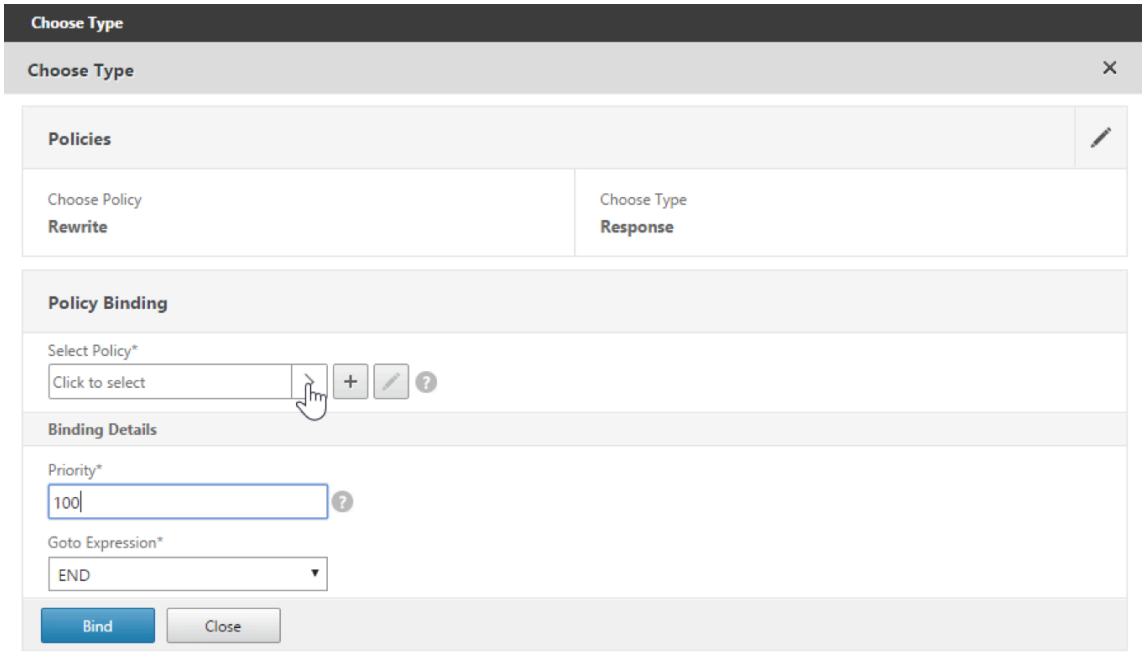


8. No campo **Choose Policy**, selecione **Rewrite**.
9. No campo **Choose Type**, selecione **Response**.



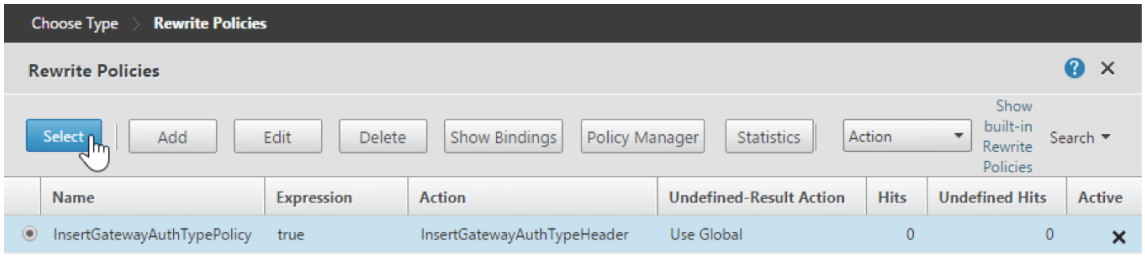
10. Clique em **Continue**.

    A seção **Policy Binding** se expande.

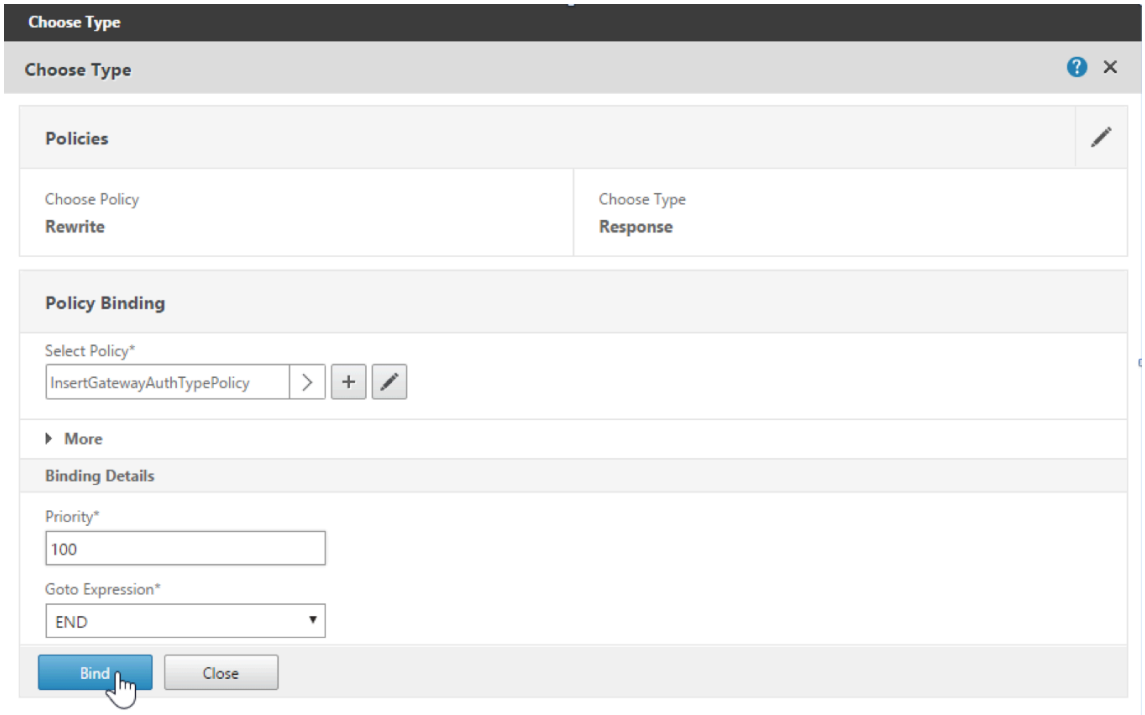


11. Clique em **Select Policy**.

    É exibida uma tela com políticas disponíveis.

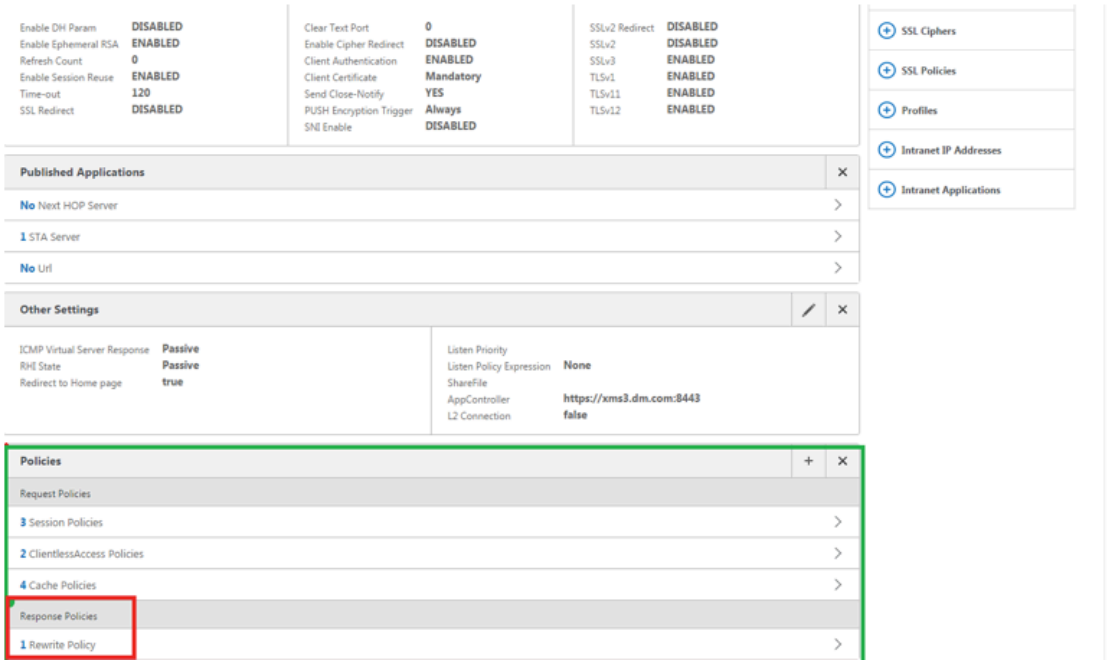


12. Clique na linha da política que você criou e clique em **Select**. A tela **Policy Binding** aparece novamente, com a sua política selecionada preenchida.

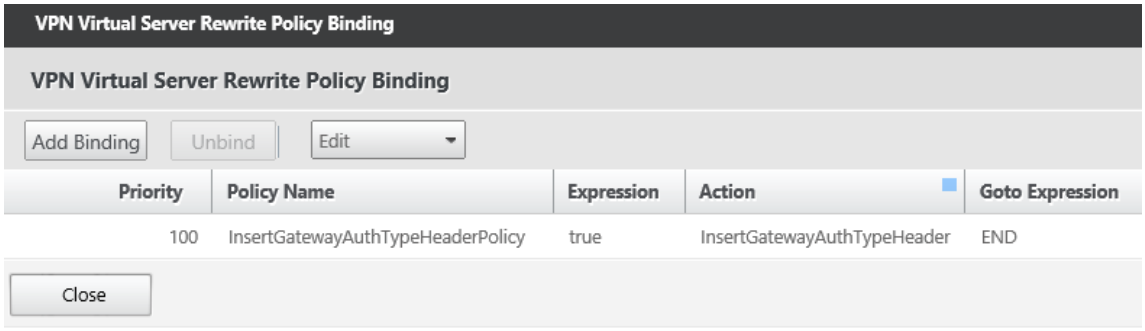


13. Clique em **Bind**.

    Se a associação for bem-sucedida, é exibida a principal tela de configuração com a política de reescrever concluída exibida.



14. Para exibir os detalhes da política, clique em **Rewrite Policy**.



Requisito de porta para conectividade ADS para dispositivos Android A configuração de porta garante que dispositivos Android que se conectam do Secure Hub possam acessar o Citrix ADS de dentro da rede corporativa. A capacidade de acessar ADS é importante ao baixar as atualizações de segurança disponibilizadas por meio do ADS. As conexões ADS podem não ser compatíveis com o servidor proxy. Nesse cenário, permita que a conexão do ADS ignore o servidor proxy.

> **Importante:**
>
> O Secure Hub para Android e iOS exige que você permita que dispositivos Android acessem o ADS. Para obter detalhes, consulte os Requisitos de porta na documentação do Citrix Endpoint Management. Essa comunicação é na porta de saída 443. É altamente provável que o ambiente existente tenha sido projetado para permitir isso. Recomenda-se aos clientes que não possam garantir essa comunicação que não atualizem para o Secure Hub 10.2. Se tiver alguma dúvida, entre em contato com o Atendimento ao Cliente Citrix.

Pré-requisitos:

- Colete os certificados do Endpoint Management e do Citrix ADC. Os certificados precisam estar no formato PEM e devem ser um certificado público e não a chave privada.
- Entre em contato com o suporte da Citrix e faça uma solicitação para permitir a certificate pinning. Durante este processo, você será solicitado a fornecer seus certificados.

As melhorias da nova certificate pinning exigem que os dispositivos se conectem ao ADS antes de o dispositivo se registrar. Esse pré-requisito garante que as informações de segurança mais recentes estejam disponíveis ao Secure Hub para o ambiente no qual o dispositivo está se registrando. Se os dispositivos não puderem alcançar o ADS, o Secure Hub não permitirá o registro do dispositivo. Portanto, a abertura de acesso a ADS na rede interna é crítica para possibilitar que os dispositivos se registrem.

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

FQDN	Endereço IP	Porta	Uso de IP e porta
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: observe que o Secure Hub versão 10.6.15 e posterior usa ads.xm.cloud.com.	34.194.83.188	443	Secure Hub - ADS Communication
ads.xm.cloud.com: observe que o Secure Hub versão 10.6.15 e posterior usa ads.xm.cloud.com.	34.193.202.23	443	Secure Hub - ADS Communication

Se a certificate pinning estiver ativada:

- O Secure Hub fixa o certificado corporativo durante o registro do dispositivo.
- Durante uma atualização, o Secure Hub descarta os certificados fixados e, em seguida, fixa o certificado do servidor na primeira conexão para usuários registrados.

  > **Nota:**
  >
  > Se você ativar a certificate pinning após uma atualização, os usuários devem fazer novo registro.

- A renovação do certificado não exige o processo de novo registro, se a chave pública de certificado não tiver sido alterada.

A certificate pinning dá suporte a certificados de folha, mas não certificados intermediários ou certificados de emissor. A certificate pinning se aplica a servidores Citrix, como, por exemplo, Endpoint Management e Citrix Gateway, e não a servidores de terceiros.

Desabilitar a opção Excluir conta

Você pode desativar a opção **Excluir conta** no Secure Hub em ambientes em que o Auto Discovery Service (ADS) está ativado.

Execute as seguintes etapas para desativar a opção **Excluir conta**:

1. Configure o ADS para o seu domínio.
2. Abra o **AutoDiscovery Service Information** no Citrix Endpoint Management e defina o valor de `displayReenrollLink` como **False**.
   Por padrão, esse valor é **True**.
3. Se o dispositivo estiver registrado no modo MDM+MAM (ENT), faça logoff e faça login novamente para que as alterações entrem em vigor.
   Se o dispositivo estiver registrado em outros modos, você deve registrar novamente o dispositivo.

Usando o Secure Hub

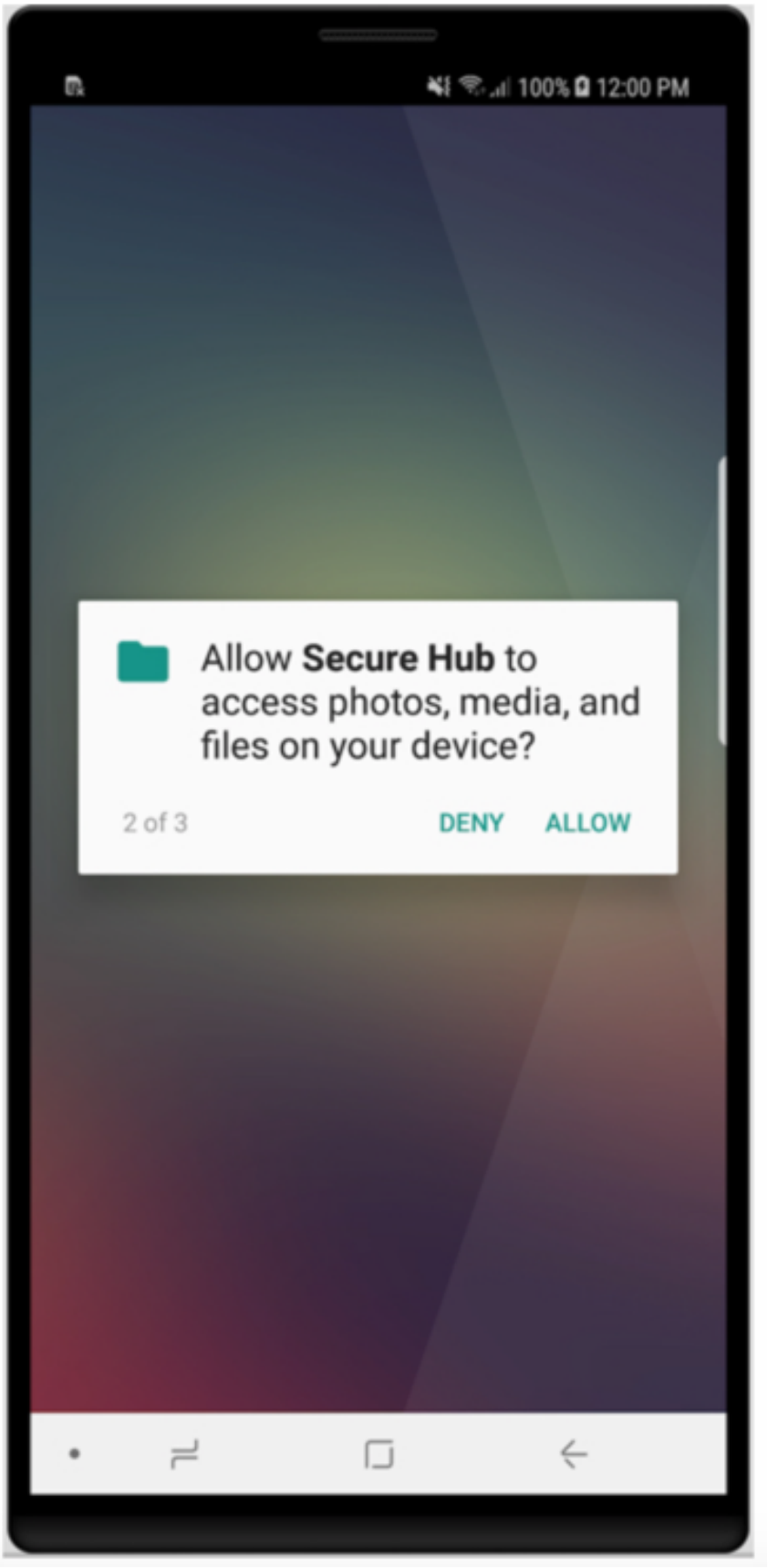
Os usuários começam com o download do Secure Hub para seus dispositivos a partir das lojas de aplicativos Apple ou Android.

Quando o Secure Hub é aberto, os usuários digitam as credenciais fornecidas pela sua empresa para registrar seus dispositivos no Secure Hub. Para obter mais informações sobre o registro de dispositivos, consulte Contas de usuários, funções e registro.

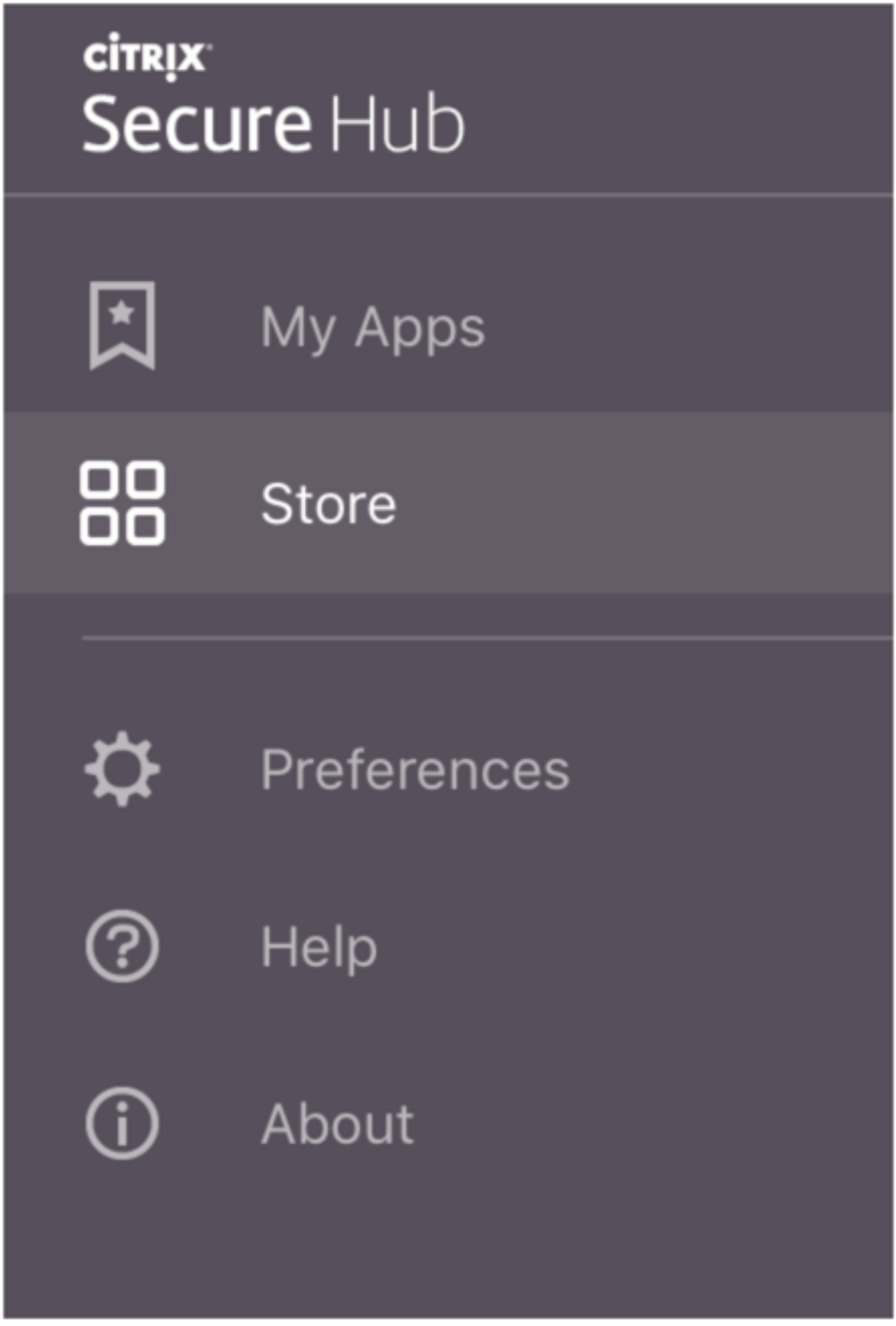
No Secure Hub para Android, durante a instalação inicial e registro, aparece a seguinte mensagem: Permitir que o Secure Hub acesse fotos, mídia e arquivos em seu dispositivo?

Esta mensagem vem do sistema operacional Android e não da Citrix. Quando você toca em **Allow**, a Citrix e os administradores que administram o Secure Hub não veem seus dados pessoais em nenhum momento. Se, no entanto, você realizar uma sessão de suporte remoto com seu administrador, o administrador pode visualizar seus arquivos pessoais dentro da sessão.

Depois de registrados, os usuários veem os aplicativos e áreas de trabalho que você enviou nas respectivas guias **My Apps**. Os usuários podem adicionar mais aplicativos do Store. Nos telefones o link do Store está sob o ícone de **configurações** tipo hambúrguer no canto superior esquerdo.



Em tablets, o Store é uma guia separada.



Quando usuários com iPhones com iOS 9 ou posterior instalam aplicativos móveis de produtividade da loja, eles veem uma mensagem. A mensagem afirma que o desenvolvedor corporativo, Citrix, não é confiável nesse iPhone. A mensagem observa que o aplicativo não está disponível para uso até que o desenvolvedor seja confiável. Quando esta mensagem é exibida, o Secure Hub avisa aos usuários para exibir um guia que os orienta pelo processo de confiar nos aplicativos empresariais Citrix para seu iPhone.

Registro automático no Secure Mail

Para as implantações somente MAM, você pode configurar o Endpoint Management para que os usuários com dispositivos Android ou iOS que se registrarem no Secure Hub com credenciais de email sejam automaticamente registrados no Secure Mail. Os usuários não têm que digitar mais informações nem executar mais etapas para se registrarem no Secure Mail.

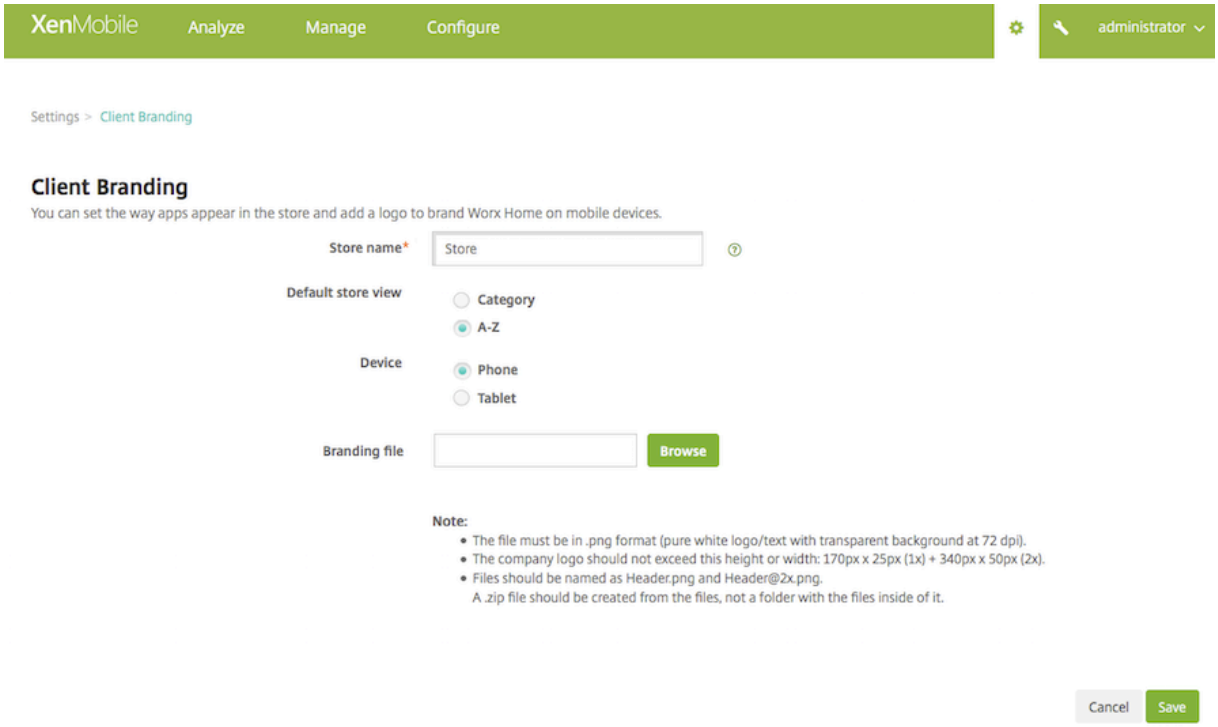
Ao ser usado pela primeira vez, o Secure Mail obtém do Secure Hub o endereço de email do usuário, o domínio e o ID de usuário. O Secure Mail usa o endereço de email no AutoDiscovery. O Exchange Server é identificado com o uso do domínio e ID de usuário, o que permite que o Secure Mail autentique o usuário automaticamente. O usuário é solicitado a inserir uma senha se a política estiver configurada para não passar pela senha. O usuário não é, no entanto, obrigado a inserir mais informações.

Para ativar esse recurso, crie três propriedades:

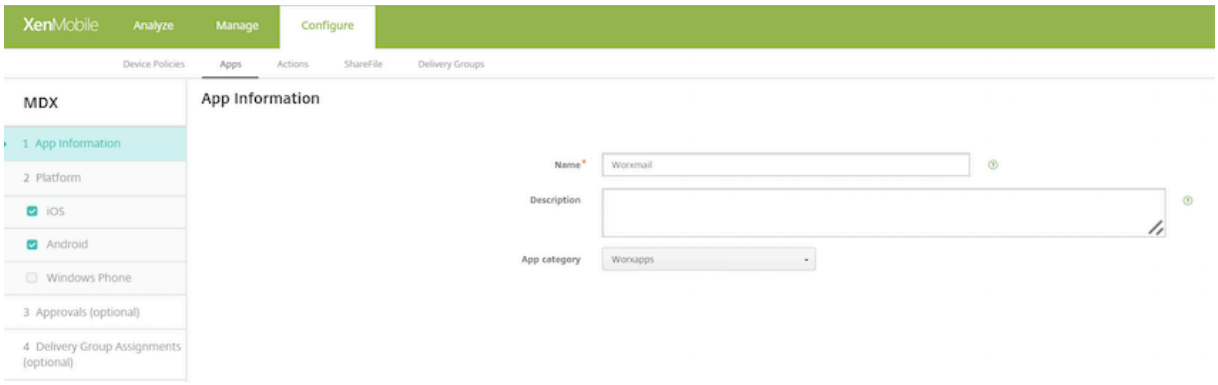
- A propriedade do servidor MAM_MACRO_SUPPORT. Para obter instruções, consulte Propriedades do servidor.
- As propriedades de cliente ENABLE_CREDENTIAL_STORE e SEND_LDAP_ATTRIBUTES. Para obter instruções, consulte Propriedades do cliente.

Loja personalizada

Se você deseja personalizar sua Store, vá para **Settings > Client Branding** para alterar o nome, adicionar um logotipo e especificar como os aplicativos serão exibidos.



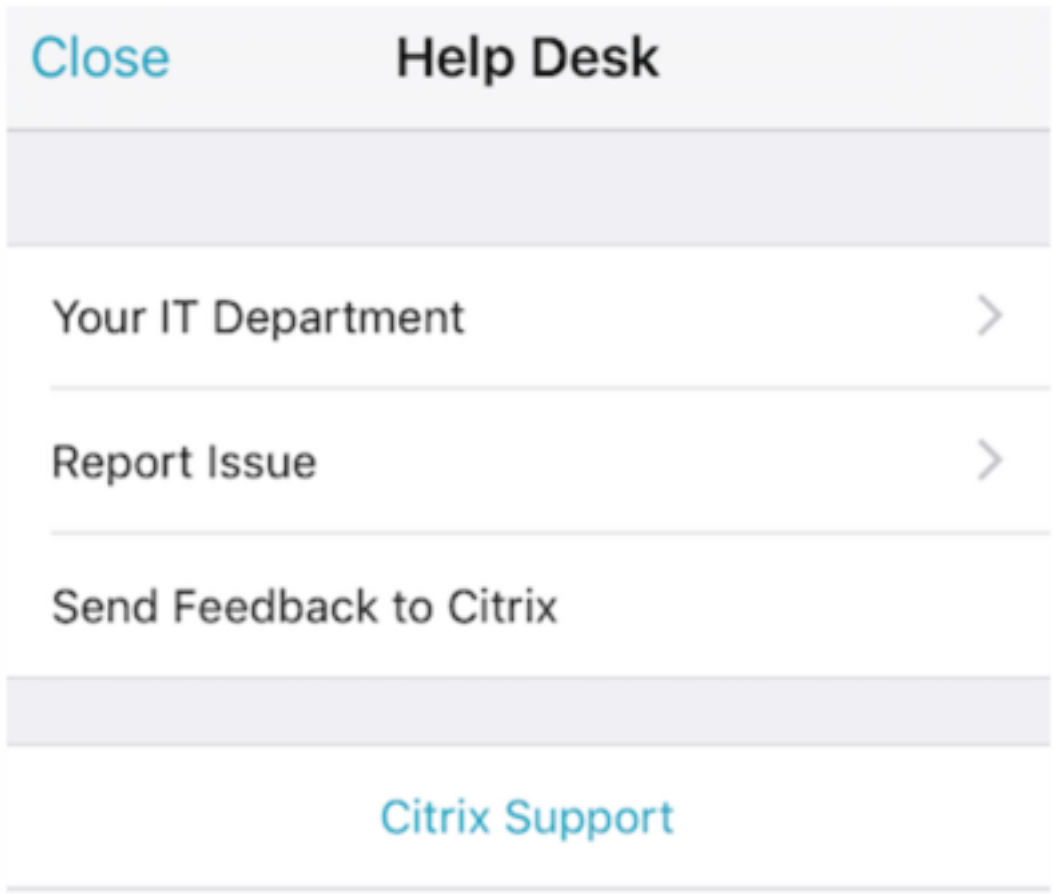
Você pode editar as descrições do aplicativo no console Endpoint Management. Clique em **Configure** e em **Apps**. Selecione o aplicativo na tabela e clique em **Edit**. Selecione as plataformas para o aplicativo com a descrição que você está editando e digite o texto na caixa **Description**.



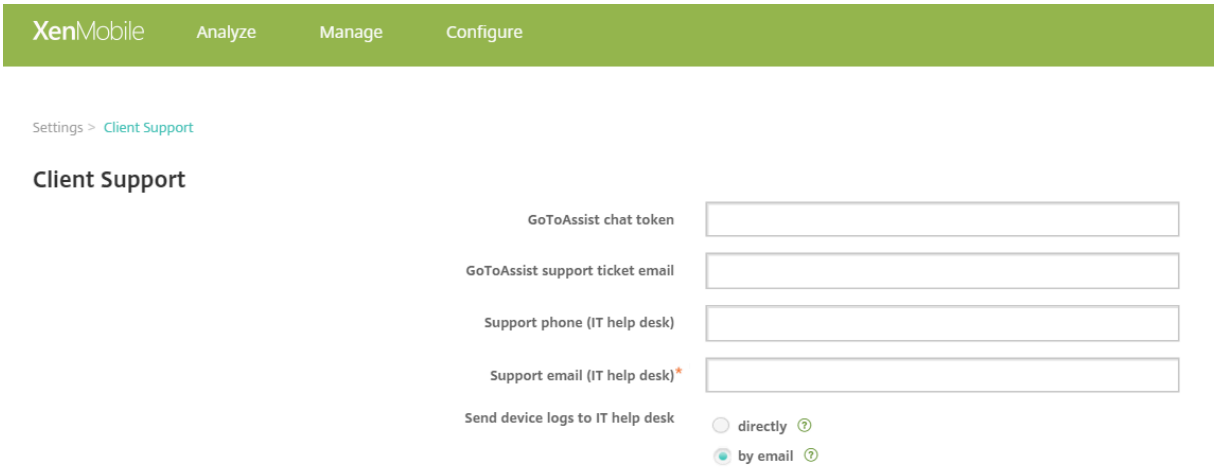
No Store, os usuários poderão procurar somente os aplicativos e áreas de trabalho que você tiver configurado e protegido no Endpoint Management. Para adicionar o aplicativo, os usuários devem tocar em **Details** e depois em **Add**.

Opções configuradas de Help

O Secure Hub também oferece aos usuários várias formas de obter ajuda. Em tablets, tocar o ponto de interrogação no canto superior direito abre as opções de ajuda. Em telefones, os usuários devem tocar no ícone de hambúrguer no canto superior esquerdo e depois tocar em **Help**.



Your IT Department mostra o telefone e o email do suporte técnico de sua empresa, que os usuários podem acessar diretamente do aplicativo. Você pode inserir números de telefone e endereços de email no console Endpoint Management. Clique no ícone de engrenagem no canto superior direito. A página **Configurações** é exibida. Clique em **More** e em **Client Support**. É exibida a tela em que você insere as informações.



Report Issue mostra uma lista de aplicativos. Os usuários devem selecionar o aplicativo que apresenta o problema. O Secure Hub gera automaticamente os logs e abre uma mensagem em Secure Mail com os logs anexados como um arquivo zip. Os usuários podem adicionar linhas de assunto e descrição do problema. Eles também podem anexar uma captura de tela.

Send Feedback to Citrix abre uma mensagem no Secure Mail com um endereço de suporte da Citrix preenchido. No corpo da mensagem, o usuário pode fornecer sugestões para melhorar o Secure Mail. Se o Secure Mail não estiver instalado no dispositivo, o programa de e-mail nativo abre.

Os usuários também podem tocar em **Citrix Support**, o que abre o Citrix Knowledge Center. Ali eles podem pesquisar artigos de suporte para todos os produtos da Citrix.

Em **Preferences**, os usuários podem encontrar informações sobre suas contas e dispositivos.

Políticas de localização

O Secure Hub também fornece políticas de localização geográfica e rastreio geográfico se, por exemplo, você desejar garantir que um dispositivo pertencente à empresa não invade um determinado perímetro geográfico. Para obter detalhes, consulte Location device policy.

Coleta e a análise de panes

O Secure Hub coleta automaticamente e analisa informações de falhas para que você possa ver o que levou a uma determinada falha. O software Crashlytics suporta essa função.

Para obter mais recursos disponíveis para iOS e Android, consulte a matriz Recursos por plataforma do Citrix Secure Hub.

Gerar logs do lado do dispositivo do Secure Hub

Esta seção explica como gerar os logs do lado do dispositivo do Secure Hub e configurar o nível de depuração correto neles.

Para obter os logs do Secure Mail, faça o seguinte.

1. Vá para **Secure Hub > Help > Report Issue**. Selecione Secure Mail na lista de aplicativos. É aberto um email endereçado ao suporte técnico da sua organização.
2. Altere essas configurações apenas se a equipe de suporte tiver instruído você a fazer isso. Sempre confirme se as configurações estão definidas corretamente.
3. Retorne ao Secure Mail e reproduza o problema. Anote a hora em que o problema começou a ser reproduzido e a hora em que o problema ocorre ou a mensagem de erro exibida.

4. Retorne para **Secure Hub > Help > Report Issue**. Selecione Secure Mail na lista de aplicativos. É aberto um email endereçado ao suporte técnico da sua organização.
5. Preencha a linha de assunto e corpo com algumas palavras que descrevam o problema. Inclua os carimbos de data/hora coletados na etapa 3 e clique em **Send**.
   A mensagem concluída se abre com arquivos de log anexados.
6. Clique em **Send** novamente.

   Os arquivos zip enviados de logs incluem o seguinte:

   - CtxLog_AppInfo.txt (iOS), Device_And_AppInfo.txt (Android), logx.txt e WH_logx.txt (Windows Phone)

   Os logs de informações dos aplicativos contêm informações sobre o dispositivo e o aplicativo.

Visão geral do Secure Mail

June 6, 2024

O Citrix Secure Mail permite que os usuários gerenciem seus emails, calendários e contatos em seus celulares e tablets. Para manter a continuidade de contas do Microsoft Outlook ou IBM Notes, o Secure Mail sincroniza com o Microsoft Exchange Server e o IBM Notes Traveler Server.

Como parte da família de aplicativos Citrix, o Secure Mail oferece o benefício da compatibilidade de logon único (SSO) com o Citrix Secure Hub. Depois que os usuários fazem logon no Secure Hub, eles podem se mover facilmente para o Secure Mail sem precisar reinserir seus nomes de usuário e senhas. Você pode configurar o Secure Mail para ser enviado a dispositivos de usuários automaticamente quando os dispositivos se registram no Secure Hub ou os usuários podem adicionar o aplicativo do Store.

> **Nota:**
>
> O suporte para o Exchange Server 2010 terminou em 13 de outubro de 2020.

O Secure Mail é compatível com:

- Atualização cumulativa 14 do Exchange Server 2019
- Atualização cumulativa 13 do Exchange Server 2019
- Atualização cumulativa 12 do Exchange Server 2019
- Atualização cumulativa 11 do Exchange Server 2019
- Atualização cumulativa 10 do Exchange Server 2019
- Atualização cumulativa 9 do Exchange Server 2019
- Atualização cumulativa 8 do Exchange Server 2019

- Atualização cumulativa 7 do Exchange Server 2019
- Atualização cumulativa 6 do Exchange Server 2019
- Atualização cumulativa 23 do Exchange Server 2016
- Atualização cumulativa 22 do Exchange Server 2016
- Atualização cumulativa 21 do Exchange Server 2016
- Atualização cumulativa 20 do Exchange Server 2016
- Atualização cumulativa 19 do Exchange Server 2016
- Atualização cumulativa 18 do Exchange Server 2016
- Atualização cumulativa 17 do Exchange Server 2016
- Atualização cumulativa 23 do Exchange Server 2013
- Atualização cumulativa 22 do Exchange Server 2013
- Atualização cumulativa 21 do Exchange Server 2013
- HCL Domino versão 12.0.2 FP2
- HCL Traveler versão 12.0.2.1 Compilação 202302010413_30
- HCL Domino 11 (anteriormente Lotus Notes)
- HCL Domino 10.0.1 (anteriormente Lotus Notes)
- HCL Domino 9.0.1 FP10 HF197 (anteriormente Lotus Notes)
- HCL Domino 10.0.1.0 compilação 201811191126_20 (anteriormente Lotus Notes)
- HCL Domino 9.0.1.21 (anteriormente Lotus Notes)
- Microsoft Office 365 (Exchange on-line)

Para começar, baixe o Secure Mail e outros componentes do Endpoint Management em Downloads do Citrix Endpoint Management.

Quanto ao Secure Mail e outros requisitos de sistema de aplicativos móveis, consulte os Requisitos do sistema.

Para obter informações sobre as notificações no Secure Mail para iOS e Android quando o aplicativo está sendo executado em segundo plano ou fechado, consulte Notificações por Push para o Secure Mail.

Para os recursos do iOS suportados no Secure Mail, consulte Recursos do iOS para Secure Mail.

Para os recursos do Android suportados no Secure Mail, consulte Recursos do Android para Secure Mail.

Para os recursos do iOS e Android suportados no Secure Mail, consulte Recursos do iOS e Android para Secure Mail.

Para obter a documentação de ajuda do usuário, consulte a página Citrix Secure Mail no Centro de Ajuda ao Usuário Citrix.

Citrix Secure Web

July 19, 2023

O Citrix Secure Web é um navegador da Web móvel compatível com HTML5 que permite o acesso seguro a sites internos e externos. Você pode configurar o Secure Web para ser enviado a dispositivos de usuários automaticamente quando os dispositivos são registrados no Secure Hub. Como alternativa, você pode adicionar o aplicativo a partir da loja de aplicativos do Endpoint Management.

Quanto ao Secure Web e outros requisitos de sistema de aplicativos móveis de produtividade, consulte os Requisitos do sistema.

Integrar e fornecer o Secure Web

> **Nota:**
>
> O MDX Toolkit 10.7.10 é a versão final compatível com a preparação dos aplicativos móveis de produtividade. Os usuários obtêm os aplicativos móveis de produtividade da versão 10.7.5 e versões posteriores da loja de aplicativos pública.

Para integrar e fornecer o Secure Web, siga estas etapas gerais:

1. Para ativar o logon único (SSO) na rede interna, configure o Citrix Gateway.

   Para o tráfego HTTP, o Citrix ADC pode fornecer SSO para todos os tipos de autenticação proxy com suporte pelo Citrix ADC. Para o tráfego HTTPS, a política de cache de senha da Web permite ao Secure Web autenticar e fornecer SSO para o servidor proxy por meio de MDX. O MDX dá suporte apenas a autenticação basic, digest e NTLM proxy. A senha é armazenada em cache usando MDX e armazenada no cofre compartilhado do Endpoint Management, uma área de armazenamento segura para os dados confidenciais de aplicativo. Para obter detalhes sobre a configuração do Citrix Gateway, consulte Citrix Gateway.
2. Baixar o Secure Web.
3. Determine como você deseja configurar conexões de usuário para a rede interna.
4. Adicione o Secure Web ao Endpoint Management usando as mesmas etapas que para outros aplicativos MDX e configure as políticas de MDX. Para obter detalhes sobre as políticas específicas para o Secure Web, veja “Sobre as políticas do Secure Web”mais adiante neste artigo.

Configurando conexões de usuário

O Secure Web oferece suporte para as seguintes configurações para conexões de usuário:

- **Com túnel —SSO de Web:** As conexões que fazem túnel para a rede interna podem usar uma variação de uma VPN sem cliente, conhecida como Com túnel —SSO de Web. Esta é a configuração padrão especificada para a política de **modo VPN preferencial**. Com túnel —SSO de Web é recomendado para conexões que exigem logon único (SSO).
- **Túnel VPN completo:** Conexões que fazem túnel para a rede interna podem usar um túnel VPN, configurado pela política de modo **VPN preferencial**. Túnel VPN completo é recomendado para conexões que usam certificados de cliente ou SSL de ponta a ponta a um recurso na rede interna. O Secure Web, no entanto, não é um aplicativo que pode ler certificados de cliente armazenados em um dispositivo móvel. Alguns aplicativos corporativos preparados de terceiros que estejam instalados podem oferecer esse recurso. O túnel VPN completo manipula qualquer protocolo por TCP e pode ser usado com computadores Windows e Mac, além de dispositivos iOS e Android.
- A política **Permitir comutação de modo VPN** permite a comutação automática entre os modos Túnel VPN completo e Com túnel –SSO de Web, conforme necessário. Como padrão, esta política está Desativada. Quando esta política está ativada, uma solicitação de rede que falhar devido a uma solicitação de autenticação que não possa ser processado no modo VPN preferida é repetida no modo alternativo. Por exemplo, o modo de túnel VPN completo acomoda desafios do servidor para certificados de cliente, mas não o modo Com túnel —SSO de Web. Da mesma forma, os desafios de autenticação HTTP têm maior probabilidade de serem atendidos pelo SSO ao usar o modo Com túnel —SSO de Web.

A tabela a seguir indica se o Secure Web pede as credenciais de um usuário, com base na configuração de site e tipo:

Modo de conexão	Tipo de Site	Senha em cache	SSO configurado para o Citrix Gateway	Secure Web solicita credenciais no primeiro acesso de um site	Secure Web solicita credenciais no acesso subsequente do site	Secure Web solicita credenciais após a alteração da senha
Com túnel – SSO de Web	HTTP	Não	Sim	Não	Não	Não
Com túnel – SSO de Web	HTTPS	Não	Sim	Não	Não	Não
VPN completa	HTTP	Não	Sim	Não	Não	Não

Modo de conexão	Tipo de Site	Senha em cache	SSO configurado para o Citrix Gateway	Secure Web solicita credenciais no primeiro acesso de um site	Secure Web solicita credenciais no acesso subsequente do site	Secure Web solicita credenciais após a alteração da senha
VPN completa	HTTPS	Sim. Se a política Secure Web MDX Enable web password caching está definida como On.	Não	Sim. É necessário para armazenar em cache as credenciais no Secure Web.	Não	Sim

Políticas do Secure Web

Ao adicionar o Secure Web, leve em consideração essas políticas de MDX que são específicas para o Secure Web. Para todos os dispositivos móveis com suporte:

Websites permitidos ou bloqueados

O Secure Web normalmente não filtra links da Web. Você pode usar essa política para configurar uma lista específica de sites permitidos ou bloqueados. Você pode configurar padrões de URL para restringir os sites que o navegador pode abrir, formatado como uma lista de itens separados por vírgula. Um sinal de mais (+) ou menos (-) precede cada padrão na lista. O navegador compara uma URL conforme com os padrões na ordem listada antes que uma correspondência seja encontrada. Quando uma ocorrência é encontrada, o prefixo determina a ação a executar da seguinte maneira:

- Um prefixo menos instrui o navegador para bloquear o URL. Nesse caso, o URL é tratado como se o endereço do servidor não pudesse ser resolvido.
- Um prefixo de mais (+) permite que o URL seja processado normalmente.
- Se nem + ou - for fornecido com o padrão, fica presumido + (permitir).
- Se o URL não corresponder a nenhum padrão na lista, o URL é permitido

Para bloquear todas as outras URLs, encerre a lista com sinal de menos seguido por um asterisco (-*). Por exemplo:

- O valor da política `+http://*.mycorp.com/*,-http://*,+https://*,+ftp://*,-*` permite URLs de HTTP no domínio `mycorp.com`, mas os bloqueia nos demais lugares, permite URLs de HTTPS e FTP em qualquer lugar, e bloqueia todos os outros URLs.
- O valor da política `+http://*.training.lab/*,+https://*.training.lab/*,-*` permite que os usuários abram qualquer site no domínio Training.lab (intranet) via HTTP ou HTTPS. No entanto, não é possível abrir URLs públicos, como Facebook, Google e Hotmail, independentemente do protocolo.

O valor padrão é vazia (todas os URLs são permitidos).

Bloquear pop-ups

Os pop-ups são novas guias que os sites abrem sem a sua permissão. Esta política determina se o Secure Web permite pop-ups. Se o valor for Ativado, o Secure Web impedirá que os sites abram pop-ups. O valor padrão é Desativado.

Indicadores pré-carregados

Define um conjunto de indicadores para o navegador Secure Web. A política é uma lista separada por vírgulas de tuplas que incluem um nome de pasta, o nome amigável e o endereço da Web. Cada tripleto deve ter o formato de pasta, nome, url em que a pasta e o nome podem ser, opcionalmente, colocados entre aspas duplas (“).

Por exemplo, os valores da política `,"Mycorp, Inc. home page",https://www.mycorp.com, "MyCorp Links",Account logon,https://www.mycorp.com/Accounts "MyCorp Links/Investor Relations","Contact us",https://www.mycorp.com/IR/Contactus.aspx` definem três marcadores. O primeiro é um link primário (sem nome de pasta) intitulado “Mycorp, Inc. home page”. O segundo link é colocado em uma pasta chamada “MyCorp Links”e intitulado “Account logon”. O terceiro é colocado na subpasta “Investor Relations” da pasta “MyCorp Links”e exibido como “Contact us”.

O valor padrão é vazio.

URL da página inicial

Define o site que o Secure Web carrega quando iniciado. O valor padrão é vazio (página inicial padrão).

Apenas para dispositivos Android e iOS com suporte:

Interface do usuário de navegador

Determina o comportamento dos controles da interface do usuário do navegador para o Secure Web. Normalmente, todos os controles de navegação estão disponíveis. Estes incluem avançar, retroceder, barra de endereços e os controles para atualizar/parar. Você pode configurar esta política para restringir o uso e a visibilidade de alguns desses controles. O valor padrão é Todos os controles visíveis.

Opções

- Todos os controles visíveis. Todos os controles estão visíveis e os usuários não são impedidos de usá-los.
- Barra de endereços de somente leitura. Todos os controles estão visíveis, mas os usuários não podem editar o campo de endereço do navegador.
- Ocultar barra de endereços. Oculta a barra de endereços, mas não outros controles.
- Ocultar todos os controles. Suprime toda a barra de ferramentas para fornecer uma experiência de navegação sem molduras.

Ativar armazenamento em cache de senha da web

Quando os usuários do Secure Web digitam credenciais ao acessas ou solicitar um recurso da Web, esta política determina se o Secure Web armazena silenciosamente em cache a senha no dispositivo. Esta política se aplica a senhas inseridas nos diálogos de autenticação e não para senhas inseridas em formulários da Web.

Se o valor for **Ativado**, o Secure Web armazena em cache todas as senhas que os usuários digitarem ao solicitar um recurso da Web. Se o valor for **Desativado**, o Secure Web não armazena em cache as senhas e remove as senhas existentes armazenadas em cache. O valor padrão é **Desativado**.

Esta política é ativada somente quando você também define a política de VPN preferida como Túnel VPN completo para este aplicativo.

Servidores proxy

Você também pode configurar servidores proxy para o Secure Web quando usado no modo Com túnel —SSO de Web. Para obter detalhes, consulte esta postagem no blog.

Sufixos DNS

Em Android, se os sufixos DNS não estiverem configurados, a VPN poderá falhar. Para obter detalhes sobre a configuração de sufixos DNS, consulte Suporte a consultas de DNS usando sufixos DNS para

dispositivos Android.

Preparação de sites de intranet para o Secure Web

Esta seção é para desenvolvedores de sites que necessitam preparar um site da intranet para uso com o Secure Web para Android e iOS. Sites de Intranet feitos para navegadores de desktop requerem alterações para funcionar corretamente em dispositivos Android e iOS.

Secure Web utiliza o Android WebView e o iOS WkWebView para oferecer suporte à tecnologia da Web. Algumas das tecnologias com suporte pelo Secure Web são:

- AngularJS
- ASP .NET
- JavaScript
- jQuery
- WebGL

Algumas das tecnologias sem suporte pelo Secure Web são:

- Flash
- Java

A tabela a seguir mostra recursos de renderização HTML e tecnologias com suporte para o Secure Web. X indica que o recurso está disponível para uma plataforma, navegador e combinação de componentes.

Tecnologia	iOS Secure Web	Android 6.x/7.x Secure Web
Mecanismo de JavaScript	JavaScriptCore	V8
Armazenamento local	X	X
AppCache	X	X
IndexedDB		X
SPDY	X	
WebP		X
srcet	X	X
WebGL		X
requestAnimationFrame API		X
Navigation Timing API		X
Resource Timing API		X

As tecnologias funcionam do mesmo modo nos diferentes dispositivos, no entanto, o Secure Web retorna cadeias de caracteres de agente diferentes para dispositivos diferentes. Para determinar a versão do navegador usada para o Secure Web, você pode ver a sua sequência de caracteres de e agente de usuário. No Secure Web, navegue até https://whatsmyuseragent.com/.

Solução de problemas de sites da Intranet

Para solucionar problemas de renderização quando o site de intranet é exibido no Secure Web, compare como o site é exibido no Secure Web e em um navegador compatível de terceiros.

Para iOS, os navegadores de terceiros compatíveis para teste são o Chrome e o Dolphin.

Para o Android, o navegador de terceiro compatível para teste é o Dolphin.

> **Nota:**
>
> Chrome é um navegador nativo no Android. Não o use para a comparação.

No OS, verifique se os navegadores têm suporte a VPN no nível de dispositivo. Você pode configurar a VPN no dispositivo navegando para **Configurações > VPN > Adicionar configuração de VPN**.

Você também pode usar o aplicativo de cliente VPN disponíveis na App Store, como Citrix VPN, Cisco AnyConnect, or Pulse Secure.

- Se uma página da Web é renderizada do mesmo modo nos dois navegadores, o problema é no seu site. Atualize seu site e verifique se ela funciona bem para o sistema operacional.
- Se o problema em uma página da Web aparecer somente no Secure Web, entre em contato com o suporte da Citrix para abrir um tíquete de suporte. Forneça as etapas de solução de problemas, incluindo o navegador e os tipos de sistema operacional testados. Se o Secure Web para iOS tiver problemas de exibição, inclua um arquivo da web da página como descrito nas seguintes etapas. Isso ajuda a Citrix resolver o problema de com mais rapidez.

Para criar um arquivo web

Usando o Safari no macOS 10.9 ou posterior, você pode salvar uma página da Web como um arquivo da Web arquivado (chamado de lista de leitura). O arquivo da Web arquivado inclui todos os arquivos vinculados, como imagens, CSS e JavaScript.

1. No Safari, esvazie a pasta de Lista de Leitura: no **Finder**, clique no menu **Ir** na barra **Menu**, selecione **Ir para a pasta**, digite o nome do caminho ~/Library/Safari/ReadingListArchives/ e, em seguida, exclua todas as pastas contidas nesse local.
2. Na barra **Menu**, vá para **Safari > Preferências > Avançado** e ative **Mostrar menu Desenvolvedor** na barra de menus.

3. Na barra **Menu**, vá para **Desenvolvedor > Agente do Usuário** e insira o agente de usuário do Secure Web: (Mozilla/5.0 (iPad; CPU OS 8_3, como macOS) AppleWebKit/600.1.4 (KHTML, como Gecko) Mobile/12F69 Secure Web/ 10.1.0(build 1.4.0) Safari/8536.25).
4. No Safari, abra o site que você deseja salvar como lista de leitura (arquivo da Web arquivado).
5. Na barra **Menu**, vá até **Favoritos > Adicionar à lista de leitura**. O arquivamento ocorre em segundo plano e pode levar alguns minutos.
6. Localize a lista de leitura arquivada: na barra **Menu**, vá até **Visualizar > Mostrar Barra Lateral da Lista de Leitura**.
7. Verifique o arquivo:
   - Desative a conectividade de rede para o seu Mac.
   - Abrir o site a partir da lista de leitura.

     O site renderiza completamente.
8. Compactar o arquivo arquivado: no **Finder**, clique no menu **Ir** na barra **Menu**, escolha **Ir para a pasta** e digite o nome do caminho ~/Library/Safari/ReadingListArchives/. Agora, compacte a pasta que tem uma cadeia de caracteres hexadecimais aleatória como um nome de arquivo. Você pode enviar esse arquivo para o Suporte Citrix quando abrir um tíquete de suporte.

Recursos do Secure Web

O Secure Web usa tecnologias de troca de dados móveis para criar um túnel VPN para que os usuários acessem sites internos e externos e todos os outros sites. Isso inclui sites com informações confidenciais em um ambiente protegido pelas políticas da sua organização.

A integração do Secure Web com o Secure Mail e o Citrix Files oferece uma experiência de usuário excelente no contêiner seguro do Endpoint Management. Veja a seguir alguns exemplos de recursos de integração:

- Quando os usuários tocam em links **Mailto**, uma nova mensagem de email é aberta no Citrix Secure Mail sem a necessidade de mais nenhuma autenticação.
- No iOS, os usuários podem abrir um link no Secure Web de um aplicativo de email nativo, inserindo **ctxmobilebrowser://** na frente do URL. Por exemplo, para abrir `example.com` de um aplicativo de email nativo, use o URL ctxmobilebrowser://example.com.
- Quando os usuários clicam em um link de intranet contido em uma mensagem de email, o Secure Web vai para aquele site sem que seja necessária nenhuma autenticação adicional.
- Os usuários podem carregar arquivos para o Citrix Files que eles baixam da Web no Secure Web.

Os usuários do Secure Web também podem executar as seguintes ações:

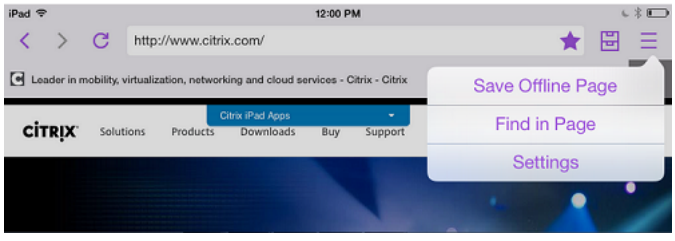
- Bloquear pop-ups.

> **Nota:**
>
> Grande parte da memória do Secure Web é usada para exibir pop-ups, portanto, o desempenho muitas vezes pode ser melhorado com o bloqueio de pop-ups em Configurações.

- Marcar seus sites favoritos.
- Baixar arquivos.
- Salvar páginas offline.
- Senhas de salvamento automático.
- Excluir cache/histórico/cookies.
- Desabilitar cookies e armazenamento local de HTML5.
- Compartilhar dispositivos com outros usuários de modo seguro.
- Pesquisar na barra de endereços.
- Permitir que aplicativos da Web sejam executados com o Secure Web para acessar a respectiva localização.
- Exportação e importação de configurações.
- Abrir arquivos diretamente no Citrix Files sem a necessidade de fazer o download de arquivos. Para habilitar esse recurso, adicione **ctx-sf**: à política URLs permitidas no Endpoint Management.
- No iOS, use Ações de toque 3D para abrir uma nova guia e acessar páginas offline, sites favoritos e downloads diretamente da tela inicial.
- No iOS, baixar arquivos de qualquer tamanho e abri-los no Citrix Files ou em outros aplicativos.

  > **Nota:**
  >
  > Se o Secure Web for colocado em segundo plano, o download é interrompido.

- Pesquisar um termo no modo de exibição de página atual usando **Find in Page**.



O Secure Web também tem suporte de texto dinâmico. O aplicativo exibe a fonte definida pelos usuários em seus dispositivos.

> **Nota:**
>
> - O Citrix Files for XenMobile atingiu o EOL em 1º de julho de 2023. Para obter mais informações, consulte EOL e aplicativos obsoletos

Citrix Content Collaboration para Endpoint Management

July 19, 2023

Os clientes do Citrix Content Collaboration para Endpoint Management são versões compatíveis com MDX dos clientes móveis do Citrix Files. Esses clientes fornecem acesso seguro e integrado a dados em outros aplicativos preparados com MDX. Os clientes do Citrix Content Collaboration para Endpoint Management também se beneficiam dos recursos MDX, como micro VPN, logon único (SSO) com Secure Hub e autenticação de dois fatores.

O Citrix Files é um serviço de sincronização de arquivos e compartilhamento empresarial que permite que os usuários troquem documentos entre si com facilidade e segurança. O Citrix Files oferece aos usuários várias opções de acesso, incluindo clientes móveis do Citrix Files, como Citrix Files para telefones Android e Citrix Files para iPad.

Você pode integrar o Citrix Files ao Endpoint Management para fornecer o conjunto completo de recursos do Citrix Files ou fornecer acesso apenas aos StorageZone Connectors. Por padrão, o console Citrix Endpoint Management permite a configuração apenas do Citrix Files. Para configurar o Endpoint Management para uso com os StorageZone Connectors, consulte Usar Citrix Content Collaboration com Endpoint Management na documentação do Citrix Endpoint Management.

Você usa o Endpoint Management, o Citrix Files, o StorageZones Controller e o Citrix ADC da seguinte forma para implantar e gerenciar clientes do Citrix Content Collaboration para Endpoint Management:

- Quando o Endpoint Management é configurado com o Citrix Files, o Endpoint Management atua como um provedor de identidade SAML (IdP) e implementa os clientes do Citrix Content Collaboration para Endpoint Management. O Citrix Files gerencia os dados do Citrix Files. Nenhum dado do Citrix Files percorre o Endpoint Management.
- Quando o Endpoint Management é configurado com o Citrix Files ou com os StorageZones Connectors, o StorageZones Controller fornece conectividade a dados em compartilhamentos de rede e no SharePoint. Os usuários acessam seus dados armazenados por meio dos aplicativos móveis de produtividade do Citrix Files. Os usuários podem editar documentos do Microsoft Office, visualizar e fazer anotações em arquivos Adobe PDF em dispositivos móveis.

- O Citrix ADC gerencia solicitações de usuários externos, protegendo suas conexões, solicitações de balanceamento de carga e lidando com a comutação de conteúdo para StorageZones Connectors.

Para baixar os clientes do Citrix Content Collaboration para Endpoint Management, consulte a página de downloads do Citrix.com.

Quanto ao Citrix Content Collaboration para Endpoint Management e outros requisitos de sistema de aplicativos móveis de produtividade, consulte Suporte para aplicativos móveis de produtividade.

Como os clientes do Citrix Content Collaboration para Endpoint Management diferem dos clientes móveis do Citrix Files

A seguir, descrevemos as diferenças entre os clientes do Citrix Content Collaboration para Endpoint Management e os clientes móveis do Citrix Files.

O acesso do usuário

Clientes do Citrix Content Collaboration para Endpoint Management:

Os usuários obtêm e abrem os clientes do Citrix Content Collaboration para Endpoint Management do Secure Hub.

Clientes móveis do Citrix Files:

Os usuários obtêm clientes móveis do Citrix Files em lojas de aplicativos.

SSO

Clientes do Citrix Content Collaboration para Endpoint Management:

Para integração do Endpoint Management com o Citrix Files: você pode configurar o Endpoint Management como um IdP SAML para o Citrix Files. Nessa configuração, o Secure Hub obtém um token SAML para o cliente do Citrix Content Collaboration para Endpoint Management, usando o Endpoint Management como o IdP SAML. Um usuário que inicia o cliente do Citrix Content Collaboration para Endpoint Management, mas não está conectado ao Secure Hub, é solicitado a fazer logon no Secure Hub. O usuário não tem que saber o domínio do Citrix Files ou as informações da conta.

Clientes móveis do Citrix Files:

Você pode configurar o Endpoint Management e o Citrix Gateway como um IdP SAML para Citrix Files. Nessa configuração, um usuário que faz logon no Citrix Files usando um navegador da Web ou outros clientes do Citrix Files é redirecionado para o ambiente do Endpoint Management para autenticação do usuário. Após a autenticação bem-sucedida pelo Endpoint Management, o usuário recebe um token de SAML válido para o logon em sua conta do Citrix Files.

Micro VPN

Clientes do Citrix Content Collaboration para Endpoint Management:

Os usuários remotos podem se conectar usando uma conexão VPN ou micro VPN por meio do Citrix Gateway para acessar aplicativos e áreas de trabalho na rede interna. Este recurso, disponível através da integração do Citrix ADC com o Endpoint Management, é transparente para os usuários.

Clientes móveis do Citrix Files:

Não aplicável.

Autenticação de dois fatores

Clientes do Citrix Content Collaboration para Endpoint Management:

A integração do Citrix ADC com o Endpoint Management também oferece suporte à autenticação usando uma combinação de autenticação de certificado de cliente e outro tipo de autenticação, como LDAP ou RADIUS.

Clientes móveis do Citrix Files:

Não aplicável.

Permissões de pasta

Clientes do Citrix Content Collaboration para Endpoint Management e clientes móveis do Citrix Files:

Para integração do Endpoint Management com o Citrix Files: determinado por Citrix Files.

Proteção de acesso a documento

Clientes do Citrix Content Collaboration para Endpoint Management:

Os usuários podem abrir anexos recebidos no Secure Mail ou baixados por qualquer aplicativo MDX preparado. Somente aplicativos preparados com MDX aparecem quando o usuário executa uma ação de Abrir em. Os dados provenientes de um aplicativo não preparado não estão disponíveis para um cliente do Citrix Content Collaboration para Endpoint Management. Os usuários do Secure Mail podem anexar arquivos do repositório do Citrix Files sem precisar baixar o arquivo para o dispositivo. Se um usuário tiver o Citrix Files preparado e não preparado em um dispositivo, o cliente preparado do Citrix Files não poderá acessar os arquivos da conta pessoal do Citrix Files do usuário. O cliente do Citrix Files preparado pode acessar apenas o subdomínio do Citrix Files configurado no Endpoint Management.

Clientes móveis do Citrix Files:

Os usuários podem abrir anexos de qualquer aplicativo.

Acesso à conta do Citrix Files

Clientes do Citrix Content Collaboration para Endpoint Management:

Para integração do Endpoint Management com o Citrix Files: para acessar uma conta pessoal do Citrix Files ou uma conta do Citrix Files de terceiros, os usuários devem usar uma versão não-MDX do Citrix Files no dispositivo.

Clientes móveis do Citrix Files:

Para integração do Endpoint Management com o Citrix Files: disponível a partir dos clientes do Citrix Files.

Políticas de dispositivo

Clientes do Citrix Content Collaboration para Endpoint Management e clientes móveis do Citrix Files:

As políticas de dispositivo Endpoint Management e Citrix Files aplicam-se aos clientes do Citrix Content Collaboration para Endpoint Management. Por exemplo, no console Endpoint Management, você pode executar o apagamento de um dispositivo. No console Citrix Files, você pode apagar remotamente o aplicativo Citrix Files.

Políticas de MDX

Clientes do Citrix Content Collaboration para Endpoint Management:

As políticas de MDX permitem que você defina as configurações no Citrix Endpoint Management que a loja de aplicativos do Endpoint Management impõe. Políticas disponíveis apenas por meio de MDX incluem a capacidade de bloquear a câmera, microfone, email, criação de emails, captura de tela e operações de recortar, copiar e colar na área de transferência.

Clientes móveis do Citrix Files:

Não aplicável.

Criptografia de dados

Clientes do Citrix Content Collaboration para Endpoint Management e clientes móveis do Citrix Files:

Criptografa todos os dados armazenados usando AES-256 e protege os dados em trânsito com SSL 3.0 e um mínimo de criptografia de 128 bits.

Disponibilidade

Clientes do Citrix Content Collaboration para Endpoint Management:

Os clientes do Citrix Content Collaboration para Endpoint Management estão incluídos nas edições Endpoint Management Advanced e Enterprise.

Clientes móveis do Citrix Files:

Todas as edições do Endpoint Management incluem todos os recursos do Citrix Files. Você pode integrar o Endpoint Management com o conjunto completo de recursos do Citrix Files ou apenas com StorageZones Connectors.

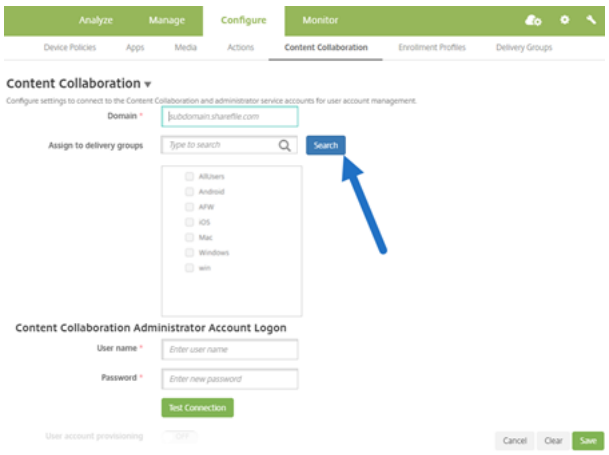
Integração e fornecimento de clientes do Citrix Content Collaboration para Endpoint Management

Para integrar e fornecer clientes do Citrix Content Collaboration para Endpoint Management, siga estas etapas gerais:

1. Habilite o Endpoint Management como um IdP SAML para Citrix Files, para fornecer SSO de clientes do Citrix Files para o Citrix Files. Para isso, você deve configurar informações da conta do Citrix Files no Endpoint Management. Para obter mais informações, consulte a seção "Para configurar informações da conta do Citrix Files no Endpoint Management para SSO".

   > **Importante:**
   >
   > Para usar o Endpoint Management como um IdP SAML para clientes não-MDX do Citrix Files, como o aplicativo Web Citrix Files e os clientes Citrix Files Sync, é necessária configuração extra. Para obter detalhes, consulte este artigo no site de suporte do Citrix Files:
   >
   > Citrix Files (ShareFile) Single Sign-On SSO. O artigo contém um link para download do guia de configuração do Endpoint Management.

2. Baixe os clientes do Citrix Files.
3. Adicione os clientes do Citrix Files ao Endpoint Management. Para obter detalhes, consulte "Para adicionar Citrix Files ao Endpoint Management"mais adiante neste artigo.
4. Validar a sua configuração. Para obter detalhes, consulte "Para validar clientes do Citrix Files" mais adiante neste artigo.



Sobre as configurações:

- O domínio é o subdomínio do Citrix Files que deve ser usado para os clientes.
- Somente os usuários que pertencem aos DGs selecionados têm acesso SSO ao Citrix Files a partir dos clientes.

  Se um usuário em um DG não tiver uma conta do Citrix Files, o Endpoint Management provisionará o usuário no Citrix Files quando você adicionar o cliente do Citrix Files ao Endpoint Management.
- As informações de logon de conta do administrador do Citrix Files são usadas pelo Endpoint Management para salvar as configurações de SAML no plano de controle do Citrix Files.

> **Importante:**
>
> A configuração que permite SSO dos clientes do Citrix Files para o Citrix Files não autentica os usuários para compartilhamentos de rede ou bibliotecas de documentos do SharePoint. O acesso a essas fontes de dados de conector requer a autenticação para o domínio do Active Directory no qual residem os compartilhamentos de rede ou os servidores SharePoint.

Para configurar informações da conta do Citrix Files no Endpoint Management para SSO

Para habilitar o SSO a partir do Secure Hub para aplicativos móveis de produtividade, você especifica a conta do Citrix Files e as informações da conta de serviço do administrador do Citrix Files no console Endpoint Management. Com essa configuração, o Endpoint Management atua como um IdP SAML para o Citrix Files, para clientes do aplicativo móvel de produtividade, clientes do Citrix Files e clientes não-MDX do Citrix Files. Quando um usuário inicia um cliente de aplicativo móvel de produtividade, o Secure Hub obtém um token SAML para o usuário a partir do Endpoint Management e o envia ao cliente do Citrix Files.

No console do Endpoint Management, clique em **Configure** > **Content Collaboration**, que é o antigo nome do Citrix Files.

Para adicionar clientes do Citrix Content Collaboration para Endpoint Management ao Endpoint Management

Quando você adiciona clientes do Citrix Content Collaboration para Endpoint Management ao Endpoint Management, é possível ativar o acesso SSO às fontes de dados do Connector a partir dos clientes do Citrix Content Collaboration para Endpoint Management. Para fazer isso, configure a política de Acesso à rede e a política de modo VPN preferencial como descrito nesta seção.

Pré-requisitos

- O Endpoint Management deve ser capaz de acessar o seu subdomínio do Citrix Files. Para testar a conexão, execute um ping no subdomínio do Citrix Files a partir do servidor do Endpoint Management.
- O fuso horário configurado para a sua conta do Citrix Files e para o hipervisor que está executando o Endpoint Management deve ser o mesmo. Se o fuso horário for diferente, as solicitações de SSO podem falhar porque o token de SAML não pode acessar o Citrix Files no limite de tempo esperado. Para configurar o servidor NTP para o Endpoint Management, use a interface de linha de comando do Endpoint Management.

  > **Nota:**
  >
  > O host Hyper-V define o tempo em um computador virtual Linux com o fuso horário local e não UTC.

- Faça login na conta de ShareFile como administrador e verifique as configurações de SAML SSO em **Settings** > **Admin Settings** > **Security** > **Login & Security Policy** > **Single sign-on / SAML 2.0 Configuration**.
- Baixe os clientes do Citrix Content Collaboration para Endpoint Management.

Etapas:

1. No console Endpoint Management, clique em **Configure > Apps** e depois clique em **Add**.
2. Clique em **MDX**.
3. Digite um nome em **Name** e, se desejar, uma descrição em **Description** e categoria de aplicativo em **App category** para o aplicativo.
4. Clique em **Next** e carregue o arquivo .mdx para o cliente do Citrix Content Collaboration para Endpoint Management.
5. Clique em **Next** para configurar as informações sobre o aplicativo e as políticas.

   A configuração que permite SSO dos clientes do Citrix Content Collaboration para Endpoint Management para o Citrix Files não autentica os usuários para compartilhamentos de rede ou bibliotecas de documentos do SharePoint.

6. Para ativar o SSO entre a micro VPN do Secure Hub e o StorageZones Controller, defina a seguinte configuração de política:

   - Defina a política de Acesso à rede como **Com túnel para a rede interna**.

     Nesse modo, a estrutura MDX intercepta todo o tráfego de rede do cliente Citrix Content Collaboration para Endpoint Management. Em seguida, o tráfego de rede é redirecionado através do Citrix Gateway usando uma micro VPN específica do aplicativo.

   - Defina a política de modo VPN preferido como **Com túnel –SSO de Web**.

     Nesse modo de criação de túneis, o framework MDX termina o tráfego SSL/HTTP a partir de um aplicativo MDX, o qual, depois, inicia novas 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.

7. Conclua as Aprovações e Atribuições de Grupo de Entrega (DG) conforme necessário.

Somente os usuários que pertencem aos DGs selecionados terão acesso SSO ao Citrix Files a partir dos clientes do Citrix Content Collaboration para Endpoint Management. Se um usuário em um DG não tiver uma conta do Citrix Files, o Endpoint Management provisionará o usuário no Citrix Files quando você adicionar o cliente do Citrix Content Collaboration para Endpoint Management ao Endpoint Management.

Para validar clientes do Citrix Content Collaboration para Endpoint Management

1. Depois de concluir a configuração descrita neste artigo, inicie o cliente do Citrix Content Collaboration para Endpoint Management. O Citrix Files não solicita que você faça logon.
2. No Secure Mail, crie um email e adicione um anexo do Citrix Files. A página inicial do Citrix Files abre, sem solicitar que você faça logon.

> **Nota:**
>
> - O Citrix Files for XenMobile atingiu o EOL em 1º de julho de 2023. Para obter mais informações, consulte EOL e aplicativos obsoletos

EOL e aplicativos obsoletos

June 6, 2024

Os aplicativos a seguir atingiram o fim da vida útil (EOL) ou estão prestes a atingir o status EOL. Quando uma versão do produto atinge EOL, você pode usar o produto nos termos de seu contrato de licença de

produto, mas as opções de suporte disponíveis são limitadas. Informações não atualizadas aparecem no Knowledge Center ou 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.

> **Nota:**
>
> Para receber um aviso prévio dos recursos do Citrix Endpoint Management que estão sendo descontinuados, consulte as Substituições.

Citrix Files for XenMobile (MDX): o Citrix Files for XenMobile atingiu o fim da vida útil em 1º de julho de 2023.

Recomendamos que os clientes usem o Citrix Files disponível na Apple App Store e no Google Play. Eles está pronto para o MAM SDK.

Secure Mail para Intune SDK (iOS e Android): o Secure Mail atingiu o fim da vida útil em 30 de abril de 2023.

Citrix Files para Intune: descontinuado em 31 de dezembro de 2020.

Incentivamos você a explorar as opções para aproveitar os recursos da plataforma para agrupar em contêineres o aplicativo Citrix Files comum (disponível nas lojas de aplicativos) via Android Enterprise (com Perfil de trabalho) e registro de usuário do iOS.

ShareConnect: o ShareConnect atingiu o fim da vida útil em 30 de junho de 2020.

Secure Notes: a data de ciclo de vida de fim de vida útil (EOL) foi 31 de dezembro de 2018.

Se você precisar dos recursos do Secure Notes e Secure Tasks, recomendamos o Notate for Citrix, um aplicativo de terceiros que você pode proteger com políticas MDX.

Se os usuários do Secure Notes e do Secure Tasks armazenarem dados no Outlook, eles poderão acessar os dados no Notate. Se os usuários armazenassem dados no ShareFile, agora Citrix Files, os dados não eram migrados.

Os usuários podem continuar executando o Secure Notes além da data de EOL, até que o sistema operacional da plataforma interrompa o suporte à interface de usuário. No entanto, não recomendamos que você use um produto não suportado.

Secure Tasks: a data de ciclo de vida de fim de vida útil (EOL) foi 31 de dezembro de 2018.

Secure Forms: a data de ciclo de vida de fim de vida útil (EOL) foi 31 de março de 2018. Os clientes são incentivados a fazer a transição para Citrix ShareFile Workflows incluídos nas contas Citrix Files Platinum e Premium. Para obter detalhes, consulte Citrix ShareFile Workflows.

ScanDirect: o ScanDirect atingiu o fim da vida útil em 1º de setembro de 2018.

Ativar a interação segura com aplicativos do Office 365

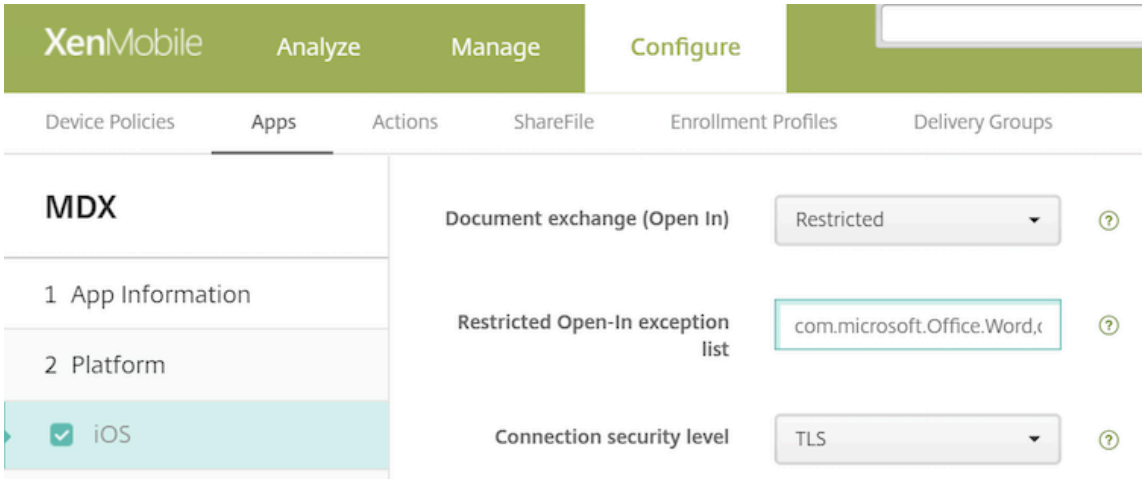
December 9, 2021

O Citrix Secure Mail, Citrix Secure Web e Citrix Files oferecem a opção de abrir o contêiner do MDX para permitir que os usuários transfiram documentos e dados para aplicativos do Microsoft Office 365. Você gerencia essa capacidade para plataformas iOS e Android através das políticas de "abrir em"no console Endpoint Management.

Uma vez abertos em um aplicativo Microsoft, os dados não estão mais seguros nem criptografados no contêiner do MDX. Leve em consideração as implicações de segurança antes de ativar esse recurso. Principalmente os clientes preocupados com a prevenção contra perda de dados ou que estão sujeitos a HIPAA ou outros requisitos estritos de segurança devem ponderar os prós e contras de abrir o contêiner.

Ativar o Office 365 no iOS

1. Baixe as versões mais recentes de aplicativos do Secure Mail, Secure Web ou Citrix Files da página de downloads do Endpoint Management.
2. Carregue os arquivos para o console Endpoint Management.
3. Localize a **política de troca de documentos (Abrir Em)** e defina-a como **Restrita**. Na **Lista restrita de exceção de Abrir em**, o Microsoft Word, Excel, PowerPoint, OneNote e Outlook são listados automaticamente. Por exemple: com.microsoft.Office.Word, com.microsoft.Office.Excel, com.microsoft.Office.Powerpoint, com.microsoft.onenote, com.microsoft.onenoteiPad, com.microsoft.Office.Outlook



Em ambientes MSM, estão disponíveis mais controles para dispositivos iOS.

Você pode carregar aplicativos do iTunes para o console Endpoint Management e enviar os arquivos para os dispositivos. Se você escolher esta opção, defina as seguintes políticas como **ATIVAS**:

- Remova o aplicativo se o perfil MDM for removido
- Evitar o backup de dados do aplicativo
- Forçar aplicativo a ser gerenciado (observe que uma limpeza seletiva remove o aplicativo e todos os dados)

Para evitar que os documentos e dados saiam dos aplicativos Microsoft para aplicativos não gerenciados, vá até **Configurar > Dispositivos > Restrições > iOS** no console Endpoint Management e em seguida defina **Documentos de aplicativos gerenciados em aplicativos não gerenciados** e **Documentos de aplicativos não gerenciados em aplicativos gerenciados** como **O**.

Ativar o Office 365 no Android

1. Baixe as versões mais recentes de aplicativos do Secure Mail, Secure Web ou Citrix Files da página de downloads do Endpoint Management.
2. Carregue os arquivos para o console Endpoint Management.
3. Role até a política **Document exchange (Open In)** e depois selecione **Restricted**.
4. Na **Restricted Open-in exception list**, acrescente os seguintes IDs de pacote:

   ```
   { package=com.microsoft.office.word } { package=com.microsoft.office.powerpoint } { package=com.microsoft.office.excel }
   ```

5. Configure outras políticas de aplicativo como faz habitualmente e salve os aplicativos.

Os usuários devem salvar arquivos do Secure Mail, Secure Web ou Citrix Files em seus dispositivos e abrir os arquivos com um aplicativo do Office 365.

Tanto no iOS como no Android os usuários podem abrir e editar os seguintes tipos de arquivos em seus dispositivos:

Formatos de arquivo com suporte

Para os formatos de arquivo com suporte, consulte a Documentação do Microsoft Office.