CITRIX

Secure Mail

Contents

Visão geral do Secure Mail

June 12, 2019

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 servidor IBM Notes Traveler.

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.

O Secure Mail é compatível com:

- Atualização cumulativa 1 do Exchange Server 2019
- Atualização cumulativa 12 do Exchange Server 2016
- Atualização cumulativa 22 do Exchange Server 2013
- Atualização cumulativa 11 do Exchange Server 2016
- Atualização cumulativa 10 do Exchange Server 2016
- Atualização cumulativa 9 do Exchange Server 2016
- Atualização cumulativa 8 do Exchange Server 2016
- Atualização cumulativa 21 do Exchange Server 2013
- Atualização cumulativa 19 do Exchange Server 2013
- Pacote acumulativo de atualizações 26 do Exchange Server 2010 SP3
- Pacote acumulativo de atualizações 24 do Exchange Server 2010 SP3
- Pacote acumulativo de atualizações 19 do Exchange Server 2010 SP3
- Pacote acumulativo de atualizações 22 do Exchange Server 2010 SP3
- Servidor de email IBM Domino versão 9.0.1 FP10 HF197
- Servidor de email IBM Domino versão 9.0.1 FP9
- IBM Lotus Notes Traveler versão e 9.0.1.21
- IBM Lotus Notes Traveler versão e 9.0.1.9
- 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 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.

Novidades do Secure Mail

June 12, 2019

A versão 19.5.5 do Secure Mail para Android inclui melhorias de desempenho e correções de bugs. Para obter a lista de problemas corrigidos e conhecidos, consulte Problemas conhecidos e resolvidos.

O que há de novo em versões anteriores

Secure Mail 19.5.0

Secure Mail para Android

Gerenciar seus feeds. No Secure Mail para Android, você pode organizar o seu cartão **Feeds** de acordo com os seus requisitos.

Para obter mais informações sobre como gerenciar seus feeds, consulte Gerenciar seus feeds.

Sincronização automática da pasta Rascunhos No Secure Mail para Android, a pasta de rascunhos é sincronizada automaticamente e seus rascunhos ficam disponíveis em todos os seus dispositivos. Para obter detalhes, incluindo um vídeo de demonstração do recurso, consulte Sincronização automática da pasta Rascunhos.

Secure Mail para Android 19.4.6, 19.4.5 e 19.3.5

Estas versões incluem melhorias de desempenho e correções de bugs.

Para obter a lista de problemas corrigidos e conhecidos, consulte Problemas conhecidos e resolvidos.

Secure Mail 19.3.0

A partir desta versão, o Secure Mail inclui suporte para os seguintes servidores:

- Atualização cumulativa 1 do Exchange Server 2019
- Atualização cumulativa 12 do Exchange Server 2016
- Atualização cumulativa 22 do Exchange Server 2013
- Pacote acumulativo de atualizações 26 do Exchange Server 2010 SP3

Para obter mais informações sobre a lista completa de compatibilidade de servidores com o Secure Mail, consulte Visão geral do Secure Mail.

Secure Mail para iOS

Gerenciar seus feeds. No Secure Mail para iOS, agora você pode organizar o seu cartão **Feeds** de acordo com os seus requisitos.

> **Nota:**
>
> Esse recurso não está disponível em iPads.

Para obter mais informações sobre como gerenciar seus feeds, consulte Gerenciar seus feeds.

Secure Mail para iOS e Android

Domínios Internos. Você pode identificar e editar destinatários de email que pertencem a organizações externas. Para usar esse recurso, verifique se você ativou a política de **Domínios Internos** no Citrix Endpoint Management.

Quando você cria, responde ou encaminha um email, os destinatários externos são realçados na lista de mala-direta. O ícone **Contatos** aparece como um aviso no canto inferior esquerdo da tela. Toque no ícone **Contatos** para modificar a lista de mala-direta.

Para obter mais informações sobre domínios internos, consulte Domínios internos.

Melhorias ergonômicas. Os botões de ação foram movidos da parte superior para a parte inferior da tela para facilitar o acesso. Essas alterações são feitas nas telas **Caixa de entrada**, **Calendário** e **Contatos**.

> **Nota:**
>
> Para dispositivos que executam o Android, as alterações são feitas nas telas **Caixa de entrada** e **Calendário**.

Para obter mais informações sobre melhorias ergonômicas, consulte Melhorias ergonômicas.

Secure Mail 19.2.0

Secure Mail para iOS

A versão 19.2.0 do Secure Mail inclui melhorias de desempenho e correções de bugs.

Para obter a lista de problemas corrigidos e conhecidos, consulte Problemas conhecidos e resolvidos.

Secure Mail para Android

- **Melhorias em Contatos.** No Secure Mail para Android, quando você toca em **Contatos** e seleciona um contato, os detalhes do contato aparecem sob a guia **Contato**. Quando você toca na guia **Organização**, os detalhes da hierarquia da organização, como **GERENTE**, **SUBORDINADOS DIRETOS** e **COLEGAS**, aparecem. Quando você toca no ícone Mais no canto superior direito da tela, as seguintes opções são exibidas:

  - **Anexar ao email**
  - **Compartilhar**
  - **Excluir**

  Na guia **Organização**, toque no ícone Mais à direita de **GERENTE**, **SUBORDINADOS DIRETOS** ou **COLEGAS**. Em seguida, crie um convite de calendário ou email. O campo **Para:** do email ou do evento de calendário é preenchido automaticamente com os detalhes de **GERENTE**, **SUBORDINADOS DIRETOS** ou **COLEGAS**.

  Pré-requisitos:

  Certifique-se de que os Serviços Web do Exchange (EWS) estão habilitados no seu Exchange Server.

  Os detalhes do contato aparecem com base nos detalhes organizacionais obtidos do Active Directory. Para que os detalhes corretos apareçam nos seus contatos, verifique se o seu administrador configurou sua hierarquia organizacional no Active Directory.

  > **Nota:**
  >
  > Este recurso não é suportado no servidor IBM Lotus Notes.

- **Política de acesso à rede**. No Secure Mail para Android, uma nova opção chamada **Com túnel - SSO de Web** foi adicionada à política de MDX de Acesso à Rede. A configuração dessa política oferece a flexibilidade de encapsular o tráfego interno por Secure Browse e Secure Ticket Authority (STA) em paralelo. Você também pode permitir conexões do Secure Browse para serviços de autenticação, como NTLM, Okta e Kerberos. Quando você configura inicialmente o STA, é preciso adicionar FQDNs individuais e portas de endereços de serviço à política de serviços de rede em segundo plano. No entanto, se você configurar a opção **Com túnel - SSO de Web**, não será preciso fazer essas configurações.

Para ativar essa política para o Secure Mail para Android no console Citrix Endpoint Management:

1. Baixe e use o arquivo .mdx para Android. Para obter detalhes, consulte as etapas em Como funcionam os aplicativos móveis e MDX.
2. Na política de acesso à rede, clique na opção **Com túnel - SSO de Web**. Para obter mais informações, consulte Acesso à rede do aplicativo

Secure Mail para iOS 19.1.6

Esta versão inclui melhorias de desempenho e correções de bugs.

Secure Mail 19.1.5

A partir desta versão, o Secure Mail inclui suporte para os seguintes servidores:

- Atualização cumulativa 11 do Exchange Server 2016
- Pacote acumulativo de atualizações 24 do Exchange Server 2010 SP3

Para obter mais informações sobre a lista completa de compatibilidade de servidores com o Secure Mail, consulte Visão geral do Secure Mail.

Secure Mail 19.1.0

Secure Mail para iOS

- **Melhorias em Contatos.** No Secure Mail para iOS, quando você toca em **Contatos** e seleciona um contato, os detalhes do contato aparecem sob a guia **Contato**. Quando você toca na guia **Organização**, os detalhes da hierarquia da organização, como **Gerente**, **Subordinados diretos** e **Colegas** aparecem. Quando você toca no ícone Mais no canto superior direito da tela, as seguintes opções são exibidas:

  - Editar
  - Adicionar ao VIP
  - Cancelar

  Na guia **Organização**, você pode tocar no ícone Mais à direita de **Gerente**, **Subordinados diretos** ou **Colegas**. Esta ação permite criar um e-mail ou um evento de calendário. O campo **Para:** do email ou do evento de
  calendário é preenchido automaticamente com os detalhes de **Gerente**, **Subordinados diretos** ou **Colegas**. Você pode redigir e enviar o email.

  Pré-requisitos:

Certifique-se de que os Serviços Web do Exchange (EWS) estão habilitados no seu Exchange Server.

Os detalhes do contato aparecem com base nos detalhes organizacionais (contato do Outlook) obtidos do Active Directory. Para que os detalhes corretos apareçam nos seus contatos, verifique se o seu administrador configurou sua hierarquia organizacional no Active Directory.

> **Nota:**
>
> Este recurso não é suportado no servidor IBM Lotus Notes.

- **Exportar a hora e o local da reunião para o seu calendário nativo.** No Secure Mail para iOS, um novo valor de **Hora e Local da reunião** é adicionado à Política de MDX **Exportar do calendário**. Essa melhoria permite exportar a hora da reunião e a localização dos eventos do calendário do Secure Mail para o seu calendário nativo.
- O Secure Mail para iOS suporta notificações por push em Rich Text em configurações executando o Microsoft Enterprise Mobility + Security (EMS)/Intune com autenticação moderna (O365).

  Para ativar o recurso de notificações por push em rich text, certifique-se de que os seguintes pré-requisitos sejam atendidos:

  - No console Endpoint Management, configure as **Notificações por push** como ON.
  - A **política de acesso à rede** é definida como **Irrestrito**.
  - A política **Controlar notificações de tela de bloqueio** está definida como **Permitir** ou **Remetente do email ou título do evento**.
  - Navegue até **Secure Mail** > **Configurações** > **Notificações** e ative **Notificações por email**.
- Os usuários do Secure Mail podem usar o aplicativo Zoom para participar de reuniões. Para obter informações sobre como configurar as políticas necessárias para usar o aplicativo Zoom, consulte Entrar em reuniões a partir do calendário.
- Esta versão inclui suporte para iPad Pro 11 polegadas e iPad Pro 12,9 polegadas.

Secure Mail para Android

- **Aprimoramento a anexos.** No Secure Mail para Android, a visualização de anexos foi simplificada. Para proporcionar uma experiência melhor, as etapas não essenciais foram removidas e as opções de anexo que existiam nas versões anteriores foram mantidas.

  Você pode exibir anexos no aplicativo Secure Mail. O anexo é aberto diretamente, se puder ser visualizado usando o Secure Mail. Se o anexo não puder ser visualizado usando o Secure Mail, uma lista de aplicativos será exibida. Você pode selecionar o aplicativo necessário para exibir o anexo. Para obter detalhes, consulte Visualizar anexos.

- Os usuários do Secure Mail podem usar o aplicativo Zoom para participar de reuniões. Para obter informações sobre como configurar as políticas necessárias para usar o aplicativo Zoom, consulte Entrar em reuniões a partir do calendário.
- **Exportar a hora e o local da reunião para o seu calendário nativo.** No Secure Mail para iOS, um valor de **Hora e Local da reunião** é adicionado à Política de MDX **Exportar do calendário**. Isso permite exportar a hora da reunião e a localização dos eventos do calendário do Secure Mail para o seu calendário nativo.

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

Secure Mail 18.12.0

A versão 18.12.0 do Secure Mail inclui melhorias de desempenho e correções de bugs.

Para obter a lista de problemas corrigidos e conhecidos, consulte Problemas conhecidos e resolvidos.

Secure Mail 18.11.5

Secure Mail para Android

- **Denunciar e-mails de phishing com cabeçalhos do ActiveSync.** No Secure Mail para Android, quando um usuário denuncia um e-mail de phishing, um arquivo EML é gerado como um anexo correspondente a esse e-mail. Os administradores recebem esse e-mail e podem ver os cabeçalhos do ActiveSync associados ao e-mail denunciado.

  Para ativar esse recurso, um administrador deve configurar a política **Denunciar endereço de email de phishing** e definir **Denunciar mecanismo de phishing** como **Denunciar por anexo**. O administrador define essas configurações no console Citrix Endpoint Management. Para obter detalhes, consulte Denunciar email de phishing (como anexo).
- **Imprimir e-mails e eventos de calendário.** No Secure Mail para Android, você pode imprimir e-mails e eventos de calendário no seu dispositivo Android. Esta funcionalidade de impressão usa o Android Printing Framework. Para obter detalhes, consulte Imprimir e-mails e eventos de calendário.
- **Feeds do seu gerente.** No Secure Mail para Android, você pode visualizar e-mails de seu gerente na tela **Feeds**. Até cinco emails aparecem nos feeds **Do seu gerente**, com base nas configurações de **Período de sincronização de email**. Para ver mais e-mails do seu gerente, toque em **Ver todos**.

  Pré-requisitos:

Certifique-se de que os Serviços Web do Exchange (EWS) estão habilitados no seu Exchange Server.

O cartão do gerente é exibido com base nos detalhes organizacionais (contato do Outlook) obtidos do Active Directory. Para que os detalhes corretos apareçam no feed do gerente, verifique se o seu administrador configurou sua hierarquia organizacional no Active Directory.

> **Nota:**
>
> Este recurso não é suportado no servidor IBM Lotus Notes.

Secure Mail 18.11.1

> Importante:
>
> O seguinte problema foi corrigido no Secure Mail para Android 18.11.1
>
> No Secure Mail para Android com conexões ao IBM Notes Traveler 9.0.1 SP 10, os emails com anexos permanecem na Caixa de saída. [CXM-58962]

Secure Mail 18.11.0

Secure Mail para Android

- **Notificações de subpastas.** No Secure Mail para Android, você pode receber notificações por email de subpastas de sua conta de email. Para obter detalhes, consulte Notificações de subpastas.
- **Atualizações a serviços em segundo plano no Secure Mail para Android.** Para atender ao requisito de Limites de Execução em Segundo Plano do Google Play em dispositivos com Android 8.0 (nível de API 26) ou posterior, atualizamos os serviços em segundo plano do Secure Mail. Para sincronização e notificações de e-mail ininterruptas em seu dispositivo, ative as notificações por push do serviço Firebase Cloud Messaging (FCM). Para obter mais detalhes sobre como habilitar notificações por push baseadas em FCM, consulte Notificações por Push para o Secure Mail

Certifique-se de ativar **Notificações de email** nas configurações do Secure Mail no seu dispositivo. Para obter mais detalhes sobre essa atualização, consulte este artigo do Support Knowledge Center.

Limitações:

- Se você não tiver ativado as notificações por push baseadas em FCM, a sincronização em segundo plano ocorrerá uma vez a cada 15 minutos. Esse intervalo varia dependendo se o aplicativo está sendo executado em segundo plano ou em primeiro plano.
- Quando os usuários atualizam manualmente a hora das configurações do dispositivo, a data no widget de calendário não é atualizada automaticamente.

Secure Mail para iOS

- **Suporte para iOS 12.1.** O Secure Mail para iOS suporta a versão 12.1 do iOS.
- **Aprimoramentos para mensagens de falha de notificação por push em rich text.** No Secure Mail para iOS, mensagens de falha de notificação por push apropriadas são exibidas na central de notificações do dispositivo com base no tipo de falha de notificação. Para obter detalhes, consulte Mensagens de falha na notificação por push no Secure Mail para iOS, consulte Enviar mensagens de falha de notificação por push no Secure Mail para iOS.
- **Feeds do seu gerente.** No Secure Mail para iOS, você pode visualizar e-mails de seu gerente na tela **Feeds**. Até cinco emails aparecem nos feeds **Do seu gerente**, com base nas configurações de **Período de sincronização de email**. Para ver mais e-mails do seu gerente, toque em **Ver todos**.

  Pré-requisitos:

  Certifique-se de que os Serviços Web do Exchange (EWS) estão habilitados no seu Exchange Server.

  O cartão do gerente é exibido com base nos detalhes organizacionais (contato do Outlook) obtidos do Active Directory. Para que os detalhes corretos apareçam no feed do gerente, verifique se o seu administrador configurou sua hierarquia organizacional no Active Directory.

  > **Nota:**
  >
  > Este recurso não é suportado no servidor IBM Lotus Notes.

Secure Mail 18.10.5

- **Integração do Secure Mail com Slack (visualização):** Agora você pode levar sua conversa por e-mail para o aplicativo Slack em dispositivos com iOS ou Android. Para obter detalhes, consulte Integração do Secure Mail com Slack (visualização).
- **Melhorias na pasta Feeds:** No Secure Mail para iOS, os seguintes são aprimoramentos na pasta Feeds existente:
  - Visualize até cinco reuniões futuras no seu cartão de feeds.
  - As próximas reuniões do próximo período de 24 horas aparecem no cartão Feeds e são categorizadas nas Seções **Hoje** e **Amanhã**.

Secure Mail 18.10.0

- **Canais de notificação do Secure Mail para notificações de email e calendário:** Nos dispositivos que executam o Android O ou posterior, você pode usar as configurações do canal de

notificações para gerenciar como suas notificações de e-mail e calendário são tratadas. Esse recurso permite personalizar e gerenciar suas notificações. Para obter detalhes, consulte Canais de notificação.

- **Denunciar email de phishing (como um encaminhamento):**No Secure Mail para iOS, você pode usar o recurso Notificar como phishing para denunciar um email (como um encaminhamento) suspeito de phishing. Você pode encaminhar as mensagens suspeitas para os endereços de email que os administradores configuram na política. Para ativar esse recurso, um administrador deve configurar a política Denunciar endereço de email de phishing e definir **Denunciar mecanismo de phishing** como **Denunciar via Forward**. Para obter detalhes, consulte Denunciar email de phishing como um encaminhamento.

Secure Mail 18.9.0

- Novo esquema de numeração de versão no formato “aa.mm.versão”. Por exemplo, versão **18.9.0**
- **Denunciar email de phishing (como um encaminhamento):**No Secure Mail para Android, você pode usar o recurso Notificar como phishing para denunciar um email (como um encaminhamento) suspeito de phishing. Você pode encaminhar as mensagens suspeitas para os endereços de email que os administradores configuram. Para ativar esse recurso, um administrador deve configurar a política Denunciar endereço de email de phishing e definir Denunciar mecanismo de phishing como **Denunciar via Forward**. Para obter detalhes, consulte Denunciar email de phishing como um encaminhamento.
- **Melhorias nos cartões de feed:** As melhorias a seguir foram feitas na pasta existente **Feeds**, no Secure Mail para Android:
  - Os convites de reunião de todas as pastas sincronizadas automaticamente aparecem no seu cartão de feeds.
  - Visualize até cinco reuniões futuras no seu cartão de feeds.
  - As próximas reuniões agora aparecem com base em um período de 24 horas começando a partir do horário atual. Esses convites para reuniões são categorizados em **Hoje** e **Amanhã**.
    Nas versões anteriores, as próximas reuniões até o final do dia apareceriam nos seus feeds.
- **Exportar eventos de calendário do Secure Mail:**O Secure Mail para Android e iOS permite exportar eventos de calendário do Secure Mail para o aplicativo de calendário nativo do seu dispositivo. Para ativar esse recurso, toque em **Configurações** e arraste o controle deslizante de Exportar eventos de calendário para a direita. Para obter detalhes, consulte Exportar eventos de calendário do Secure Mail.

Secure Mail 10.8.65

- **Disponível com o iOS 12:** No Secure Mail para iOS, oferecemos suporte ao recurso Notificações em Grupo. Com esse recurso, as conversas são agrupadas de um thread de email. Você pode rapidamente ver as notificações agrupadas na tela de bloqueio do seu dispositivo. As configurações de notificação em grupo são ativadas por padrão no dispositivo.
- No Secure Mail para iOS, os botões **Salvar rascunho** e **Excluir rascunho** são maiores. Esse aprimoramento torna mais fácil para os clientes distinguirem uma opção da outra.
- No Secure Mail para iOS, você pode identificar as chamadas recebidas de seus contatos do Secure Mail ativando o ID de chamador do Secure Mail nas **Configurações** do dispositivo. Ao ativar essas configurações, quando você recebe uma chamada, o dispositivo exibe o nome do aplicativo com o ID do Chamador, como "ID do chamador do Secure Mail: Joe Jay". Para obter detalhes, consulte ID de chamador do Secure Mail.

Secure Mail 10.8.60

- Secure Mail suporta Android P.
- O Secure Mail está agora disponível em polonês.
- No Secure Mail para iOS, você pode anexar arquivos ao seu email a partir do aplicativo Arquivos nativo do iOS. Para obter detalhes, consulte Recursos do iOS.

Secure Mail 10.8.55

Não há novos recursos no Secure Mail versão 10.8.55. Quanto aos problemas corrigidos, consulte Problemas conhecidos e resolvidos.

Secure Mail 10.8.50

Melhorias no anexo de fotos. No Secure Mail para iOS, você pode anexar fotos facilmente tocando no novo ícone da **Galeria**. Toque no ícone da **Galeria** e selecione as fotos que deseja anexar ao seu email.

Tela de feeds do Secure Mail. O Secure Mail para iOS e Android apresenta todos os seus e-mails não lidos, convites para reuniões que exigem sua atenção e suas próximas reuniões na tela **Feeds**.

Secure Mail 10.8.45

Sincronização de pastas. No Secure Mail para iOS e Android, toque no ícone **Sincronizar** para atualizar todo o conteúdo do Secure Mail. O ícone **Sincronizar** está presente nas telas deslizantes do

Secure Mail, como Caixas de Correio, Calendários, Contatos e Anexos. Quando você toca no ícone **Sincronizar**, as pastas que você configurou para atualização automática, como caixas de correio, calendários e contatos, são atualizadas. O carimbo data/hora da última sincronização aparece ao lado do ícone **Sincronizar**.

Melhorias no anexo de fotos. No Secure Mail para Android, você pode anexar fotos facilmente tocando no novo ícone da **Galeria**. Toque no ícone da **Galeria** e selecione as fotos que deseja anexar ao seu email.

Secure Mail 10.8.40

Suporte para busca no calendário. No Secure Mail para iOS, você pode pesquisar no calendário por eventos, participantes ou qualquer outro texto.

Secure Mail 10.8.35

A versão do Secure Mail para iOS é 10.8.36.

- **Opções de resposta de notificação.** No Secure Mail para iOS, os usuários podem responder às notificações da reunião, como Aceitar, Recusar e Tentativa. Eles podem responder a notificações de mensagem com Responder e Excluir.
- **Aprimoramentos no botão de voltar do Secure Mail para Android** No Secure Mail para Android, você pode tocar no botão de voltar em seu dispositivo para descartar as opções expandidas do botão de ação flutuante. Se o Botão de Ação Flutuante estiver no estado expandido, se você tocar no botão de voltar no dispositivo, as opções de resposta são ocultadas. Essa ação leva você de volta à exibição de detalhes da mensagem ou do evento.
- **No Secure Mail para Android, os botões de resposta da reunião aparecem no email.** Quando você recebe uma notificação por email sobre convites para a reunião, pode responder ao convite tocando em uma das seguintes opções:
  - Sim
  - Talvez
  - Não

Secure Mail 10.8.25

O Secure Mail para iOS agora suporta S/MIME para credenciais derivadas: Para que esse recurso funcione, você precisa fazer o seguinte:

- Selecione Credencial Derivada como a origem do certificado S/MIME. Para obter detalhes, consulte Credenciais derivadas para o iOS.

- Adicione a propriedade do cliente LDAP Attributes no Citrix Endpoint Management. Use as seguintes informações:
  - **Chave:** SEND_LDAP_ATTRIBUTES
  - **Valor:** `userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme=${ user.samaccountname } ,displayName=${ user.displayName } ,mail=${ user.mail }`

Para ver as etapas para adicionar uma propriedade de cliente, para o XenMobile Server consulte Propriedades do cliente e para o Endpoint Management consulte Propriedades do cliente.

Para obter informações sobre como os dispositivos se registram usando credenciais derivadas, consulte Registro de dispositivos usando credenciais derivadas.

1. No seu console Endpoint Management, navegue até **Configurar > Aplicativos**.
2. Selecione **Secure Mail** e depois clique em **Editar**.
3. Na plataforma iOS, para a origem do certificado S/MIME, selecione**Credencial derivada**.

O **Secure Mail para iOS e Android tem uma nova aparência:** tornamos a navegação do usuário mais simples e eficiente. Nós realinhamos o menu Secure Mail e os botões de ação na forma de uma barra de navegação. Para ver um vídeo que demonstra as alterações de navegação do usuário, veja:

A figura a seguir mostra a nova barra de navegação em dispositivos iOS.

A figura a seguir mostra a nova barra de navegação em dispositivos Android.

O que mudou:

- O ícone do grabber foi removido. Os recursos do Secure Mail, como Correio, Calendário, Contatos e Anexos, agora estão disponíveis como botões na barra de guias do rodapé. A figura a seguir mostra essa alteração.

  > **Nota:**
  >
  > Nos dispositivos Android, a barra de guias do rodapé não fica disponível depois que você abre um item de email. Por exemplo, conforme mostrado na figura a seguir, se você abrir um email ou um evento de calendário, a barra de guias de rodapé não estará disponível.

- O menu **Configurações** está disponível em todos os menus, como Correio, Calendário, Contatos e Anexos. Para ir para **Configurações**, toque no ícone de hambúrguer e, em seguida, toque no botão de configurações disponível na parte inferior direita, conforme mostrado na figura a seguir.
- O ícone **Pesquisar** substitui a barra de pesquisa e está disponível nos modos de exibição da Caixa de entrada, Contatos e Anexos.
- Nos dispositivos iOS, você pode tocar e segurar em um item de correio para selecioná-lo.

- Você pode tocar no botão de ação flutuante **Redigir** para redigir um novo email, conforme mostrado na figura a seguir.
- As seguintes opções de menu estão agora disponíveis no canto superior direito da tela:
  - **Opções de sincronização**: toque no ícone de estouro no canto superior direito e navegue até **Mais opções> Opções de sincronização** para alterar suas preferências de sincronização.

    > **Nota:**
    >
    > Esta opção está disponível apenas em dispositivos Android.

  - **Ícone de pesquisa:** toque para procurar um email.
- **Ícone de visualização de triagem:** toque para ver triagem da conversa.
- **Botão de ação flutuante Responder:** Ao visualizar um email, toque em Encaminhar, Responder a todos ou Responder, conforme mostrado na figura a seguir.
- Ao ver um email, as seguintes opções de menu estão agora disponíveis no canto superior direito da tela:
  - **Sinalização:** toque para sinalizar o email.
  - **Marcar como não lido**: toque para marcar o email como não lido.
  - **Apagar:** toque para apagar o email.
  - **Mais opções:** toque no ícone suspenso para ver outras ações disponíveis, como Mover.

Mudanças na agenda

- No calendário, você pode tocar em um botão de ação flutuante de evento para criar um evento, conforme mostrado na figura a seguir.
- As seguintes opções de menu estão agora disponíveis no canto superior direito da tela:
  - **Hoje:** toque para ver os eventos de hoje.
  - **Pesquisar**: toque para procurar um evento.
  - **Botão de ação flutuante Responder:** Ao visualizar um email, toque em Encaminhar, Responder a todos ou Responder.

Quando você visualiza um evento, as ações de resposta do evento, como Sim, Talvez e Não, são realinhadas e estão disponíveis abaixo dos detalhes do evento.

Mudanças nos Contatos

- Você pode tocar no botão de ação flutuante **Criar novo contato**, como mostrado na figura seguinte.

- A opção de menu **Pesquisar** está agora disponível no canto superior direito da tela. Você pode tocar na opção para procurar um contato.
- Ao ver um contato, as seguintes opções de menu estão agora disponíveis no canto superior direito da tela:

  Em dispositivos Android:

  - **Editar**: toque para editar o contato.
  - **Mais opções:** toque no ícone de edição para ver outras ações disponíveis, como Anexar ao email, Compartilhar e Excluir.

  Em dispositivos iOS:

  - **Editar**: toque para editar o contato.
  - **Compartilhar:** toque no ícone de compartilhamento para ver outras ações disponíveis, como Compartilhar contato e Anexar ao email.

  > **Nota:**
  >
  > Para excluir um contato em dispositivos iOS, selecione o contato, toque em **Editar** e, em seguida, toque em **Excluir** na parte inferior da tela, conforme mostrado na figura a seguir.

Alterações de anexos

As seguintes opções de menu para anexos estão agora disponíveis no canto superior direito da tela:

- **Classificar:** toque no ícone **Classificar** e escolha os filtros apropriados para classificar os anexos.
- **Pesquisar**: toque para procurar um anexo.

Secure Mail 10.8.20

- O Secure Mail para iOS agora aceita o uso de credenciais derivadas para inscrição e autenticação. Para obter mais informações sobre credenciais derivadas, consulte Credenciais derivadas para iOS.
- O Secure Mail dá suporte a notificações por push em rich text. As notificações em rich text garantem que você receba notificações da tela de bloqueio para sua caixa de entrada, mesmo quando o Secure Mail não estiver sendo executado em segundo plano. Este recurso tem suporte em configurações de autenticação baseada em senha e autenticação baseada em cliente. Para obter detalhes, consulte Notificações por push em rich text.

  > **Nota:**
  >
  > Devido à mudança na arquitetura para suportar o recurso de notificações por push em rich

> text, as notificações de e-mail **Apenas VIP** não estão mais disponíveis.

- Agora, o Secure Mail para Android, como para iOS, também oferece suporte a assinaturas em rich text. Você pode usar imagens ou links na sua assinatura de email. Para obter detalhes, consulte Assinaturas em Rich Text.

Secure Mail 10.8.15

- **Agora, o Secure Mail para iOS oferece suporte a assinaturas em rich text.** Você pode usar imagens ou links na sua assinatura de email. Para obter detalhes, consulte Assinaturas em Rich Text.
- **Secure Mail oferece suporte para Android Enterprise, conhecido anteriormente como Android for Work**. Você pode criar um perfil de trabalho separado usando os aplicativos empresariais Android no Secure Mail. Para obter detalhes, consulte Android Enterprise no Secure Mail.
- **O Secure Mail processa recursos incorporados durante a exibição de um email.** Se houver recursos na sua rede interna, como emails com as URLs de imagem que são links internos, o Secure Mail se conecta à rede interna para buscar o conteúdo e processá-lo.
- **Secure Mail dá suporte à autenticação moderna**. A autenticação moderna é uma autenticação baseada no token OAuth com o nome de usuário e senha. Esse suporte inclui suporte para o Office 365 para Active Directory Federation Services (AD FS) internos e externos ou provedor de identidade (IdP).
- **Aprimoramentos no desempenho do repositório de anexos**. Você pode rolar pelo repositório de anexos com muito mais rapidez.

Secure Mail 10.8.10

- **Suporte para imprimir anexos de email**. O Secure Mail para iOS oferece suporte a impressão anexos de email.
- **Autenticação moderna com o Microsoft Office 365**. O Secure Mail para iOS dá suporte à autenticação moderna. A autenticação moderna é uma autenticação baseada no token OAuth com o nome de usuário e senha. Esse suporte inclui suporte para o Office 365 para Active Directory Federation Services (AD FS) externos e internos e provedor de identidade (IdP).

  > **Notas:**
  >
  > - Essa versão não oferece suporte a autenticação moderna com a integração do Endpoint Management com o Microsoft Intune/EMS.
  > - Esta versão inclui autenticação moderna em um cenário onde AD FS está acessível externamente.

  Para obter detalhes, consulte Autenticação moderna usando o Microsoft Office 365.

Problemas conhecidos e resolvidos

June 12, 2019

Problemas conhecidos no Secure Mail para Android versão 19.5.5

No Secure Mail para Android, quando a política de **Acesso à Rede** está definida como **Com túnel - SSO de Web**, você não consegue estabelecer uma HTTPURLConnection. [CXM-66317]

Problemas resolvidos no Secure Mail para Android versão 19.5.5

No Secure Mail para Android, quando você envia um e-mail, os destinatários recebem o e-mail várias vezes. Esse problema ocorre em dispositivos com Android 8 ou versões posteriores. [CXM-66290]

Problemas conhecidos e resolvidos em versões anteriores

Problemas conhecidos na versão 19.5.0

Em dispositivos com iOS, você pode se conectar a redes Wi-Fi fora das redes Wi-Fi permitidas definidas na política de MDX **Redes Wi-Fi permitidas**. Esse problema permite que você abra o Secure Mail e o Secure Web para iOS por meio de redes que não estão listadas na política de MDX. [CXM-66730]

Problemas resolvidos na versão 19.5.0

- No Secure Mail para Android, você não consegue colar endereços de e-mail nos campos **Para:** ou **Cc/Cco:** quando está redigindo um novo e-mail. No entanto, você pode colar endereços de e-mail nos campos **Para:** ou **Cc/Cco:** quando responde a um e-mail. [CXM-64752]
- No Secure Mail para Android, você não consegue salvar as configurações da conta quando registra dispositivos Android Enterprise. [CXM-65138]

Problemas conhecidos e resolvidos no Secure Mail para Android 19.4.6

Não há problemas conhecidos nem resolvidos nesta versão.

Problemas conhecidos na versão 19.4.5

Não há problemas conhecidos nesta versão.

Problemas resolvidos na versão 19.4.5

- No Secure Mail para iOS, quando você envia uma solicitação de reunião no Outlook e a edita no Secure Mail, a reunião não é atualizada no Outlook. Os destinatários também não recebem a atualização. Esse problema também ocorre quando você cria uma solicitação de reunião no Secure Mail e a edita no Secure Mail. [CXM-62511]
- No Secure Mail para iOS, o calendário não sincroniza e aparece o seguinte erro: "Não foi possível sincronizar o calendário". [CXM-62796]
- No Secure Mail para Android, alguns convites de reunião que você cria usando o Outlook não refletem em seu calendário do Secure Mail. [CXM-63552]
- No Secure Mail para Android, as reuniões recorrentes aparecem com atrasado e as atualizações feitas nas reuniões não são sincronizadas corretamente. [CXM-65263]

Problemas conhecidos na versão 19.3.5

Não há problemas conhecidos nesta versão.

Problemas resolvidos na versão 19.3.5

- No Secure Web para iOS, você não consegue colar a URL bitly no navegador. [CXM-56276]
- No Secure Mail para iOS, aparece a seguinte mensagem de erro para cada email recebido: Não é possível obter esta mensagem. Abra o Secure Mail. [CXM-56418]
- No Secure Mail para iOS, quando os usuários abrem o aplicativo e inserem o PIN, eles frequentemente recebem a mensagem de erro "Rede da empresa indisponível". [CXM-59776]
- O Secure Mail para iOS não consegue sincronizar depois de ter mudado para a autenticação multifator. [CXM-62176]

Problemas conhecidos no Secure Mail 19.3.0

Não existem problemas conhecidos nesta versão.

Problemas resolvidos na versão 19.3.0

Secure Mail para iOS

No Secure Mail para iOS, quando há um tempo limite de solicitação devido a uma sessão de rede inválida, o seguinte banner de notificação aparece intermitentemente quando você recebe um email: **O Secure Mail não consegue obter essa mensagem devido a um tempo limite de solicitação**. [CXM-62561]

Secure Mail para Android

- No Secure Mail para Android, não é possível receber notificações do Firebase Cloud Messaging (FCM) de mozaiekwonen.xm.cloud.com. [CXM-62146]
- No Secure Mail para Android, quando você atualiza um evento de calendário, as alterações não sincronizam com o Outlook Office 365. [CXM-62227]
- No Secure Mail para Android, e-mails contendo anexos não são enviados quando a conectividade de rede está fraca ou quando não há conexão. Esses emails permanecem na caixa de saída mesmo depois que a conectividade de rede é restaurada. [CXM-64297]

Problemas conhecidos na versão 19.2.0

No Secure Mail para iOS, quando o certificado tem a opção de transparência de certificado habilitada com grampeamento do Protocolo OCSP (Online Certificate Status Protocol), a configuração do Secure Mail falha no iOS 12.1.1 e versões posteriores.

Problemas resolvidos na versão 19.2.0

Secure Mail para iOS

No Secure Mail para iOS, não é possível copiar o texto do campo de assunto no Secure Mail para o Secure Notes versão 10.8.6.6. [CXM-61060]

Secure Mail para Android

- No Secure Mail para Android, se o texto preditivo estiver ativado em dispositivos Samsung, a última palavra do texto será sublinhada. A última palavra na assinatura é salva com um sublinhado quando você não deixa espaço, e o destinatário também pode vê-la. [CXM-60894]
- No Secure Mail para Android, quando você recebe um resumo de e-mail, as imagens não são mostradas. [CXM-62280]
- O Secure Mail para Android falha na inicialização quando o Portal da Empresa do Intune versão 5.0.4324.0 está instalado. Para obter mais detalhes, consulte este artigo do Support Knowledge Center. [CXM-62516]

Problemas conhecidos e resolvidos no Secure Mail para iOS versão 19.1.6

Não há problemas conhecidos ou resolvidos na versão 19.1.6.

Os seguintes problemas foram resolvidos em versões anteriores:

Problemas conhecidos na versão 19.1.5

Não há problemas conhecidos na versão 19.1.5.

Problemas resolvidos na versão 19.1.5

Os seguintes problemas foram resolvidos na versão 19.1.5:

- No Secure Mail para iOS, aparece a seguinte mensagem de erro para cada email recebido: **Não é possível obter esta mensagem. Abra o Secure Mail** [CXM-56418]
- No Secure Mail para iOS, você frequentemente recebe a seguinte mensagem de erro Rede da empresa indisponível, quando abre o aplicativo e insere o PIN. [CXM-59766]
- Em aplicativos Android preparados, a cadeia UserAgent é anexada várias vezes, fazendo com que o tamanho do cabeçalho aumente. Esse comportamento resulta em um erro e a página não é carregada. [CXM-59869]

Problemas resolvidos na versão 19.1.0

Secure Mail para iOS

- Quando o Secure Mail não consegue se conectar ao Exchange Server, a seguinte mensagem aparece no banner de notificação do e-mail:

  "Não foi possível obter essa mensagem porque sua sessão expirou. Abra o Secure Mail para renovar sua sessão."

  Esse problema foi resolvido e a mensagem é atualizada da seguinte maneira:

  "O Secure Mail não consegue se conectar à rede da sua organização. Entre em contato com seu administrador." [CXM-59128]

- Para usuários que usam caixas de correio O365, executar repetidamente ações de resposta de notificação, como **Sim, Não, Talvez ou Excluir**, faz com que o Office 365 fique limitado e exiba a seguinte mensagem de erro:

  "O servidor está ocupado. Tente novamente". [CXM-60123]

Secure Mail para Android

- No Secure Mail para Android, se você estiver usando o idioma turco, você não pode enviar e-mails para destinatários cujo endereço contém o caractere "I". [CXM-59093]
- No Secure Mail para Android, os usuários não conseguem selecionar e destacar a linha de assunto de um e-mail. [CXM-59185]
- No Secure Mail para Android, o logon falha se a senha contém o caractere €. [CXM-59654]

- No Secure Mail para Android, quando a configuração **Sincronizar com os contatos locais** está habilitada, todos os seus contatos do Secure Mail são exportados para seus contatos nativos. Após a sincronização, os campos de telefone, como celular, trabalho, casa, fax do trabalho e fax residencial, não aparecem na ordem correta. Por exemplo, em seus contatos nativos, o número de fax aparece acima do número do celular. Os usuários não podem alterar essa ordem. [CXM-57994]

Problemas resolvidos na versão 18.12.0

Secure Mail para iOS

- No Secure Mail para iOS, quando você recebe um email no formato Rich Text (RTF), certos tipos de anexos incorporados e o símbolo de anexo não são visíveis. [CXM-59121]
- No Secure Mail para iOS, quando as notificações por push em rich text são habilitadas e você desativa e ativa **Notificações de email**, a opção **Tipo de email** aparece intermitentemente. [CXM-59122]

Secure Mail para Android

- Se você estiver executando o mecanismo de autenticação baseada em cliente em seu ambiente, o Secure Mail não poderá sincronizar automaticamente e-mails intermitentemente. Executar uma sincronização manual obtém apenas alguns e-mails. [CXM-59650]

Problema resolvido na versão 18.11.1

- No Secure Mail para Android com conexões ao IBM Notes Traveler 9.0.1 SP 10, os emails com anexos permanecem na Caixa de saída. [CXM-58962]

Problemas resolvidos na versão 18.11.0

- No Secure Mail para Android, as imagens incorporadas não são visíveis em um email. [CXM-53556]
- O Secure Mail para Android trava ao abrir um e-mail cuja assinatura contém uma URL incorporada, como `file://C:\...jpg`. [CXM-58219]

Problemas resolvidos na versão 18.10.5

Secure Mail para iOS

- Quando a política de MDX Ativar a proteção de dados do iOS está ativada, você recebe a notificação “Você tem um novo email” de forma intermitente. [CXM-55491]
- No iPhone XS, os anexos não podem ser baixados ou enviados e as imagens baixadas não podem ser exibidas. [CXM-57030]

Secure Mail para Android

- Quando os usuários modificam uma reunião recorrente para contas que executam o Exchange ActiveSync versão 16 e posterior, a reunião não é atualizada no Exchange Server. Como resultado, a reunião não é sincronizada entre o Secure Mail e o Outlook. [CXM-57200]

Problemas resolvidos na versão 18.10.0

- No Secure Mail para Android, os usuários não podem exibir imagens em linha que apontam para servidores que não sejam servidores Exchange. [CXM-56736] [CXM-55843]
- No Secure Mail para Android, o número PIN não foi anexado ao número de discagem durante o ingresso em reuniões da Webex. Você tem que digitar manualmente o número PIN. [CXM-56002]
- O Secure Mail para Android trava ao tentar exportar o calendário do Secure Mail, se o seu calendário pessoal não estiver configurado. [CXM-56264]
- No iPhone XS, no Secure Mail para iOS, os anexos não podem ser baixados ou enviados e as imagens baixadas não podem ser exibidas. [CXM-57030]

Problemas resolvidos na versão 18.9.0

Secure Mail para Android

- A estação de trabalho cliente é alterada aleatoriamente com cada solicitação de autenticação do NT LAN Manager (NTLM). [CXM-55177]
- A sincronização do Secure Mail no Android P para de funcionar intermitentemente quando o dispositivo está no modo de economia de bateria. [CXM-55441]
- O Secure Mail trava ao tentar exportar o calendário do Secure Mail, se o seu calendário pessoal não estiver configurado. [CXM-56264]

Problemas resolvidos na versão 10.8.65

Secure Mail para iOS

- Quando o FIPs está habilitado e os usuários executam o Secure Mail para iOS em um dispositivo iOS 11.3, as políticas Recortar e Copiar e Colar MDX não funcionam conforme o esperado. [CXM-53993]

- Ao usar o Secure Mail para iOS em dispositivos compartilhados, novos usuários podem ver os emails de um usuário anterior, mesmo que esse usuário tenha feito logoff. Se o novo usuário tocar em uma pasta para atualizar a exibição, os e-mails dos usuários anteriores não serão mais exibidos. [CXM-55176]

Problemas resolvidos na versão 10.8.60

> Nota:
>
> As versões de 10.8.25 a 10.8.60 do Secure Mail não incluem problemas conhecidos.

- No Secure Mail para iOS em execução nos servidores IBM Lotus Domino, não é possível usar o ícone de pesquisa na sua caixa de entrada. [CXM-53782]
- Quando os usuários registram um dispositivo que está executando o Secure Mail para Android no Intune Company Portal, o Secure Mail para de funcionar. [CXM-54178]
- O Secure Mail para iOS trava ao sincronizar um grande número de pastas de correio do servidor durante um fluxo de FTU. [CXM-54371]
- No Secure Mail para iOS, a visualização de impressão de PDFs aparece menor. [CXM-54482]
- No Secure Mail para Android, múltiplos IDs de email não são preenchidos automaticamente ao responder a emails. [CXM-54811]

Problemas resolvidos na versão 10.8.55

- No Secure Mail para iOS, a exibição Semana do calendário é renderizada incorretamente em um iPad Pro, quando visualizada no modo paisagem. [CXM-53723]

Problemas corrigidos relacionados ao MDX na versão 10.8.55

- No Android, o Secure Mail trava quando os usuários estão desconectados do Secure Hub. [CXM-53930]
- Nos dispositivos iOS, o Secure Web e o Secure Mail 10.8.45 travam na inicialização. [CXM-54089]

Problemas resolvidos na versão 10.8.50

- O Secure Mail para iOS não pode salvar arquivos de vídeo no ShareFile. [CXM-42238]
- Quando você ativa as notificações push no Secure Mail para Android, não recebe notificações de novos emails. Esse problema ocorre de forma intermitente. [CXM-53135]

Problemas resolvidos na versão 10.8.45

O Secure Mail versão 10.8.45 não incluiu problemas resolvidos.

Problemas resolvidos na versão 10.8.40

No Secure Mail para iOS, uma notificação duplicada aparece intermitentemente para cada novo email recebido. [CXM-51473]

Problemas resolvidos na versão 10.8.35

- No Secure Mail para Android, a sincronização automática é interrompida de forma intermitente. Os usuários precisam sincronizar manualmente para que algumas novas mensagens dos servidores do Office 365 apareçam no Secure Mail. [CXM-49354, CXM-52716]
- No Secure Mail para Android, mesmo que você desabilite as notificações por email no Secure Mail para eventos de email e calendário, as notificações ainda serão exibidas e ocorrerá uma notificação sonora. [CXM-50479]
- Quando você cria um evento de dia inteiro usando o Secure Mail para Android, são exibidas datas incorretas no calendário do Outlook. [CXM-50612]
- No Secure Mail para Android, os grupos de contatos pessoais do Exchange não estão sincronizando com o aplicativo. [CXM-51190]
- Quando o SSO é configurado, o Secure Mail para Android SSO para o Exchange não funciona. Os usuários são solicitados a fornecer uma senha para entrar. [CXM-51343]

Problemas resolvidos na versão 10.8.25

- No Secure Mail para Android, ocorre um atraso quando os usuários sincronizam um convite de calendário com o Office 365. O problema ocorre ao criar ou atualizar um convite de calendário. [CXM-49596]
- No Secure Mail para Android, quando os usuários digitam uma única letra no campo cc: e, em seguida, tocam em **Enviar**: o Secure Mail envia a mensagem ao primeiro usuário na lista de usuários usados com freqüência. Em vez disso, deveria aparecer uma notificação que indica que a entrada do campo cc: é inválida. [CXM-50476]
- Nos dispositivos Zebra T51 que executam o Android 7, os usuários não podem instalar o aplicativo Citrix Launcher. [CXM-50621]
- Quando o NetScaler Gateway é configurado com autenticação baseada em certificado: No Secure Mail para iOS, toda vez que os usuários recebem uma nova mensagem, a mensagem “Você tem novo e-mail” é exibida. Em vez disso, a notificação deveria listar o nome do remetente, o assunto e a visualização do corpo da mensagem. [CXM-51075]

Problemas resolvidos na versão 10.8.20

- Se o aplicativo Intune Company Portal estiver instalado em dispositivos Android registrados no modo somente MAM, no Endpoint Management, o Secure Mail tentará redirecionar para a página de login da Microsoft. Aparece a seguinte mensagem de erro: “Nenhuma configuração foi recebida para o aplicativo. Entre em contato com o seu administrador para configurar o aplicativo”. [CXM-48135]
- No Secure Mail para Android, o login falhará se seu nome de usuário ou senha contiverem caracteres especiais como ä, ö, ü ou €. [CXM-48197]
- Nos dispositivos Android, uma reinicialização permite que você deixe de lado a autenticação para acessar o Secure Mail. [CXM-48444]
- No Secure Mail para Android, quando você responde a emails antes que as imagens incorporadas sejam baixadas, os emails ficam presos na sua Caixa de saída. Esse problema ocorre quando a configuração **Mostrar imagens** está ativada nas suas configurações. [CXM-49222]
- No Secure Mail para iOS, se a política de IRM estiver **Ativada** e a classificação de email estiver definida como **Protegida**, você não poderá exibir anexos ao baixar todos os emails. [CXM-49544]

Problemas resolvidos na versão 10.8.10

Secure Mail para iOS

- Após a atualização para o Secure Mail 10.7.25 para iOS, o cabeçalho de mensagem-ID não tem os colchetes (< e >). [CXM-46029]
- No Secure Mail para iOS, depois que os usuários adicionam um convite de calendário do Outlook, algumas vezes o aplicativo trava. Esse problema ocorre quando o convite de calendário contém um Emoji. [CXM-46250]
- No iOS, depois de atualizar os aplicativos móveis de produtividade para 10.7.30, se o Nível de Log for definido como 11 ou mais alto, o Secure Mail fica lento e trava se for deixado aberto. [CXM-46721]
- No Secure Mail para iOS, aparecem notificações duplicadas intermitentemente se a política Controlar notificações de tela de bloqueio estiver definida como **Apenas contagem**. [CXM-47461]

Secure Mail para Android

No Secure Mail para Android, quando os usuários copiam e colam quatro ou mais endereços de email no campo Para:, o aplicativo trava. [CXM-46578]

Problemas conhecidos na versão 19.1.0

Não há problemas conhecidos na versão 19.1.0.

Implantação do Secure Mail

June 12, 2019

Para implantar o Secure Mail com o Citrix Endpoint Management (anteriormente XenMobile), siga estas etapas gerais:

1. Você pode integrar o Secure Mail com um Exchange Server ou servidor IBM Notes Traveler para manter o Secure Mail em sincronia com o Microsoft Exchange ou IBM Notes. Se você usar IBM Notes, configure o servidor IBM Traveler Notes. A configuração usa credenciais do Active Directory para autenticar no servidor do Exchange ou IBM Notes Traveler. Para obter detalhes, consulte Integração do Exchange Server ou servidor IBM Notes Traveler.

   > **Importante:**
   >
   > Você não pode sincronizar email do Secure Mail com o IBM Notes Traveler (anteriormente IBM Lotus Notes Traveler). Essa capacidade de terceiro do Notes não tem suporte atualmente. Como resultado, se você excluir um email de reunião respondido do Secure Mail, o email não é excluído no servidor IBM Notes Traveler. Se os usuários aceitarem um evento de calendário e depois recusarem o evento com um comentário ou agirem em um comentário, o comentário desaparece. [CXM-47936] Para saber mais sobre as limitações conhecidas com o IBM/Lotus Notes, consulte esta postagem no blog Citrix.

2. Você também pode ativar o SSO do Secure Hub. Para fazer isso, você configura as informações da conta do Citrix Files no console Endpoint Management para habilitar o Endpoint Management como um provedor de identidade SAML para o Citrix Files. A configuração usa credenciais do Active Directory para autenticar para o Citrix Files.

   Configurar as informações de conta do Citrix Files no console Endpoint Management é uma instalação única usada para todos os clientes Citrix, clientes Citrix Files e clientes Citrix Files não MDX. Para obter detalhes, consulte Para configurar informações da conta do Citrix Files no console Endpoint Management para SSO..

3. Baixe o arquivo.mdx do Secure Mail a partir do site de downloads da Citrix.
4. Acrescente o Secure Mail ao Endpoint Management e configure as políticas de MDX. Para obter detalhes, consulte Adicionar aplicativos.

> Nota:
>
> a partir de Secure Mail versão 10.6.5, você pode configurar uma nova política de análise do MDX para o Secure Mail para iOS e Android. A Citrix coleta dados analíticos de forma anônima para melhorar a qualidade do produto. A política de nível de detalhes do Google Analytics permite que você especifique se os dados são associados ao seu domínio de empresa ou recolhidos

> de forma anônima. Selecionando **Anônimo**, os usuários impedem que o domínio da empresa seja incluído nos dados que são coletados. Essa nova política substitui uma política anterior do Google Analytics.

Quando a política é definida como anônima, coletamos os seguintes tipos de dados. Não temos nenhuma maneira de vincular esses dados a um determinado usuário ou empresa porque não podemos solicitar informações que permitam identificar o usuário. Nenhuma informação pessoalmente identificável é enviada para o Google.

- Estatísticas de dispositivo, como a versão do sistema operacional, versão do aplicativo e modelo de dispositivo
- Informações de plataforma, como ActiveSync versão e a versão do servidor de Secure Mail
- Pontos de falha para a qualidade do produto, como registros de APNs, sincronização e envio de e-mail, e download de anexos e sincronização de calendário.

Além do domínio da empresa, nenhuma outra informação de identificação é coletada quando a diretiva é definida como **Completa**. O padrão é **Completa**.

Configurando o Secure Mail

March 1, 2019

Os seguintes recursos podem ser configurados e integrados ao Secure Mail:

- Integração do Secure Mail com o Microsoft Intune/EMS
- Autenticação moderna com o Office 365
- Serviços em segundo plano para o Secure Mail
- Integrar Exchange Server ou IBM Notes Traveler Server
- S/MIME para Secure Mail
- SSO para Secure Mail

Integração do Secure Mail com o Microsoft Intune/EMS

February 25, 2019

Com essa integração, você pode gerenciar e entregar o Citrix Secure Mail com mais segurança e os meios para aumentar a produtividade.

O Secure Mail oferece suporte a várias configurações do Intune. Você pode conectar o Secure Mail a caixas de correio locais do Exchange ou do Office 365. Para configurar a integração do Endpoint

Management com o EMS/Intune, consulte Integração do Citrix Endpoint Management com o Microsoft Intune/EMS

O Secure Mail oferece suporte aos seguintes modos de implantação:

- Intune MAM
- Intune MAM e gerenciamento de dispositivo móvel (MDM) Intune
- Intune MAM com Endpoint Management somente MDM
- Intune MAM com Endpoint Management MDM e MAM

Servidores de email suportados

- Exchange Online
- Exchange Server 2016
- Exchange Server 2013

Limitações

O Secure Mail não oferece suporte à autenticação baseada em certificado.

> **Importante:**
>
> Para usar o Secure Mail no modo MDM juntamente com o Citrix Endpoint Management (MDM e MAM), você deve configurar o Secure Hub em seu ambiente.

Para configurar o Secure Mail para Intune

Se o seu ambiente estiver configurado no modo MDM do Citrix Endpoint Management, o Secure Mail preencherá automaticamente os nomes de usuários em uma experiência de FTU.

Para habilitar esse recurso, você deve configurar políticas personalizadas no console do Endpoint Management. Para obter detalhes, consulte a documentação do Endpoint Management, Para configurar o Secure Mail.

Recursos que são incompatíveis com o Intune

Os seguintes recursos do Secure Mail não são compatíveis com a integração do Endpoint Management com o EMS/Intune:

- Secure Ticket Authority (STA)
- Registro de email com o logon único (SSO)
- Notificações por push em rich text

- Citrix Files (anteriormente ShareFile)
- Assinatura e criptografia S/MIME de assinatura
- Gerenciamento de Direitos de Informação da Microsoft
- Secure Browse + servidor interno Não KCD SSO do Exchange

Autenticação moderna com o Microsoft Office 365

June 12, 2019

O Secure Mail oferece suporte à autenticação moderna com o Microsoft Office 365 para os Serviços de Federação do Active Directory (AD FS) ou o Provedor de Identidade (IDP). A autenticação moderna é uma autenticação baseada no token OAuth com o nome de usuário e senha. Usuários do Secure Mail com dispositivos iOS podem aproveitar a autenticação baseada em certificado ao conectar-se com o Office 365. Quando eles fazem login no Secure Mail, os usuários se autenticam usando um certificado de cliente, em vez de digitar suas credenciais.

Antes de prosseguir, faça o seguinte:

1. Ative a autenticação moderna (OAuth) para o Microsoft Office 365.
2. Ative os pontos de extremidade, URLs e intervalos de endereços IP do Office 365 em seu firewall para garantir a conectividade de rede ideal. Para obter detalhes, consulte a documentação da Microsoft sobre URLs e intervalo de endereços IP do Office 365.

Pré-requisitos da política do Citrix Endpoint Management

Ative as seguintes políticas no console Citrix Endpoint Management:

Para dispositivos que executam o iOS:

- **Mecanismo de autenticação do Office 365:** Use esta política para indicar o mecanismo OAuth usado para autenticação durante a configuração de uma conta no Office 365. Essa política possui os seguintes valores que você deve configurar:
  - **Não usar OAuth:** Use esta política para autenticação básica durante a configuração da conta.
  - **Usar OAuth com nome de usuário e senha:** Use esta política para o protocolo OAuth durante a autenticação. Os usuários devem fornecer seu nome de usuário e senha e, opcionalmente, um código de autenticação multifator para o fluxo OAuth.
  - **Usar OAuth com certificado do cliente:** Use esta política se o Office 365 estiver configurado para executar a autenticação baseada em certificado. A configuração padrão é **Não usar OAuth**.

Para dispositivos que executam o Android:

- **Usar autenticação moderna para o O365:** Use esta política para o protocolo OAuth durante a autenticação.
- **Agente de usuário personalizado para autenticação moderna:** Use esta política para alterar a sequência do agente do usuário padrão para autenticação moderna.

Políticas comuns para dispositivos iOS e Android:

- **Nomes de host on-line confiáveis do Exchange:** Use esta política para definir uma lista de nomes de host confiáveis do Exchange Online que usam o mecanismo de OAuth para autenticação ao configurar uma conta. É um formato de lista separada por vírgulas, como server.company.com, server.company.co.uk. Essa lista pode conter um valor padrão ou URLs intuitivas, mas não pode estar vazia. O valor padrão é **outlook.office365.com**.
- **Nomes de host AD FS confiáveis:** Use essa política para definir uma lista de nomes de host confiáveis do AD FS para páginas da Web em que a senha é preenchida durante a autenticação do Office 365 OAuth. Este é um formato separado por vírgulas, como, por exemplo, `sts.companyname.com`, `sts.company.co.uk`. Se a lista estiver vazia, o Secure Mail não insere as senhas automaticamente. O Secure Mail faz a correspondência entre os nomes de host listados com o nome de host da página Web encontrada durante a autenticação do Office 365 e verifica se a página usa o protocolo HTTPS. Por exemplo, quando `sts.company.com` é um nome de host listado e o usuário navega até `https://sts.company.com`, o Secure Mail insere a senha se a página tiver um campo de senha. O valor padrão é `login.microsoftonline.com`.
- **Exchange Server do Secure Mail:** Use esta política para definir o endereço do seu Exchange Server.

Agora o Secure Mail para iOS é ativado com autenticação moderna após as políticas serem atualizadas no dispositivo.

Limitações

- Se você estiver usando a autenticação moderna em seu ambiente, o recurso de notificações por push em rich text para iOS não estará disponível. Para obter detalhes sobre as notificações por push em rich text, consulte Notificações por Push para o Secure Mail.
- Não há suporte para várias contas nas configurações que executam a autenticação baseada em certificado.

Políticas do Secure Mail

As duas tabelas a seguir listam as políticas de Secure Mail necessárias com base em sua infraestrutura do Exchange:

Infraestrutura do Exchange	Mecanismo de autenticação do Office 365 / Usar autenticação moderna para O365	Nomes de host AD FS online confiáveis	Nomes de host online confiáveis do Exchange
No local	O	N/D	N/D
Híbrido*	I	AD FS/IDP	`Outlook.office365.com` ou URL intuitiva
Exchange online	I	AD FS/IDP	`Outlook.office365.com` ou URL intuitiva

Infraestrutura do Exchange	Exchange Server do Secure Mail	Serviços de rede em segundo plano (iOS)	Serviços de rede em segundo plano (Android)
No local	Nome do host local do Exchange	No local	No local
Híbrido*	no local, nomes de host online do Exchange	No local, nome de host local do Exchange	No local, nome de host local do Exchange, AD FS/IDP (somente interno)
Exchange online	`Outlook.office365.com`	Nomes de host online do Exchange	Nome do host local do Exchange, AD FS, IDP

*O Secure Mail suporta uma infraestrutura híbrida do Exchange com caixas de correio migradas.

Se a caixa de correio dos usuários locais for migrada para o Exchange online, o Secure Mail detectará automaticamente essa alteração e solicitará aos usuários uma autenticação moderna sem a necessidade de reconfigurar a conta.

> **Nota:**
>
> Configure os serviços de rede em segundo plano somente se o servidor de email e o AD FS forem internos.

Secure Mail com matriz de suporte OAuth

A tabela a seguir lista a matriz de suporte do Secure Mail OAuth em dispositivos iOS e Android:

Tipo de autenticação	IDP/AD FS externo	IDP/AD FS interno	Azure AD	Intune
Nome de usuário e senha	Sim	Sim	Sim	Sim
Certificado de cliente	Sim	Somente Android	Não	Não

Serviços em segundo plano para o Secure Mail

April 16, 2019

Para acessar seu servidor de e-mail através do Citrix Gateway, você precisa configurar os serviços em segundo plano para o Secure Mail. Quando você adicionar o Secure Mail ao Citrix Endpoint Management (anteriormente, XenMobile), configure os serviços em segundo plano nas configurações das políticas de aplicativos do MDX.

Para configurar serviços em segundo plano para o Secure Mail

1. Conecte-se ao console Endpoint Management usando credenciais de administrador.
2. No console, clique na guia **Configurar**, clique em **Apps**, selecione o aplicativo Secure Mail e clique em **Editar**.
3. Na página **Configurações de política MDX**, na seção **Plataforma**, selecione a plataforma iOS ou Android, conforme necessário.
4. Na seção **Configurações do aplicativo**, configure as políticas.

Políticas de aplicativo MDX para a configuração de serviços em segundo plano

As políticas de aplicativo MDX a seguir afetam a comunicação do Secure Mail com o Citrix Gateway, o servidor Citrix Endpoint Management, os servidores STA (Secure Ticket Authority) e o servidor de email.

Acesso à rede: a política de acesso à rede especifica se o Secure Mail pode usar VPN para acessar serviços de rede em segundo plano ou se todo o tráfego segue sem restrição por essa Internet.

- Se a política de acesso à rede estiver definida como **Com túnel para a rede interna**, apenas as URLs listadas nos serviços de rede em segundo plano passam pelo Citrix Gateway. O restante do tráfego segue sem restrições pela Internet. Por padrão, o acesso ao Secure Mail é **Com túnel para a rede interna**.
- Se a política de acesso à rede estiver definida como **Irrestrito**, todo o tráfego proveniente do Secure Mail é enviado sem restrições pela Internet. A VPN não é usada para acessar serviços em segundo plano.

Secure Mail Exchange Server: defina a política do **Exchange Server do Secure Mail** como o nome de domínio totalmente qualificado (FQDN) para o servidor de email.

Serviço de rede em segundo plano: a política de serviço de rede em segundo plano especifica a lista de servidores de email com acesso permitido por meio do Citrix Gateway. Liste os nomes de host e o número da porta como valores separados por vírgulas. Assegure-se de que não haja espaços à esquerda nem à direita entre os valores. Para endereços de servidor de email, inclua: `hostnameFQDN:portnumber`. Por exemplo: `mail1.example.com:443,mail2.example.com:443` (sem espaço entre a vírgula).

Gateway de serviço de rede em segundo plano: A política Gateway de serviço de rede em segundo plano especifica o Citrix Gateway que o Secure Mail usa para se conectar ao servidor de e-mails. No endereço do Citrix Gateway, inclua: `citrixgatewayFQDN:portnumber`. Por exemplo: `gateway3.example.com:443`.

Expiração de tíquete de serviços em segundo plano: esta política especifica a validade do tíquete de serviço de rede em segundo plano. Quando o Secure Mail se conecta por meio do Citrix Gateway a um servidor de e-mail, o Citrix Endpoint Management emite um token usado para conectar-se ao servidor de e-mail interno. Essa configuração determina a duração até a qual o Secure Mail pode usar esse token. Um novo token para autenticação e conexão com o servidor de email não é necessário se o token estiver ativo. Quando o limite de tempo expirar, os usuários devem fazer logon novamente para gerar um novo token. O valor padrão deste token é 168 horas (7 dias).

Para obter mais informações sobre políticas de aplicativo MDX para serviços em segundo plano, consulte:

- Configurações do aplicativo Secure Mail para Android
- Configurações do aplicativo Secure Mail para iOS

A figura a seguir mostra o fluxo de comunicação e onde essas políticas são aplicáveis.

Os seguintes valores mostram os tipos de conexões do Secure Mail a um servidor de email. Após cada valor há uma lista das configurações de política relacionadas.

Conexão direta a um servidor de email:

Políticas sobre uma conexão direta a um servidor de email:

- Acesso à rede: **Irrestrito**

Se o acesso à rede for irrestrito, as políticas a seguir não serão aplicáveis:

- Serviços de rede em segundo plano: N/A
- Expiração de tíquete de serviços em segundo plano: N/A
- Gateway de serviço de rede em segundo plano: N/A

Conexão a um servidor de email via STA:

Políticas para conexão a um servidor de email via STA:

- Acesso à rede: **Com túnel para a rede interna**
- Serviços de rede em segundo plano: `mail.example.com:443,mail1.example1.com:443`
- Expiração de tíquete de serviços em segundo plano: **168**
- Gateway de serviço de rede em segundo plano: `gateway3.example.com:443`

> Nota:
>
> A Citrix recomenda que você use uma conexão STA para o Secure Mail porque uma conexão STA suporta conexões de sessão de longa duração.

Para obter mais informações sobre STA, consulte este artigo do Citrix Knowledge Center.

Integração do Exchange Server ou servidor IBM Notes Traveler

June 12, 2019

Para manter o Secure Mail em sincronia com os seus servidores de email, integre o Secure Mail com um Exchange Server ou servidor IBM Notes Traveler que reside na sua rede interna ou está por trás do Citrix Gateway.

- Para configurar serviços em segundo plano para o Secure Mail, consulte: Serviços em segundo plano para o Secure Mail.
- Para configurar o servidor IBM Notes Traveler para Secure Mail, consulte: Configuração do servidor IBM Notes Traveler para Secure Mail.

> **Importante:**
>
> Você não pode sincronizar email do Secure Mail com o IBM Notes Traveler (anteriormente IBM Lotus Notes Traveler). Essa capacidade de terceiro do Notes não tem suporte atualmente. Como resultado, se você excluir um email de reunião do Secure Mail, o email não é excluído no servidor IBM Notes Traveler. [CXM-47936]

> Para saber mais sobre as limitações conhecidas com o IBM/Lotus Notes, consulte esta postagem no blog Citrix.

A sincronização também está disponível para Secure Notes e Secure Tasks. Observe, no entanto, que 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.

- Para sincronizar o Secure Notes para iOS, integre-o a um Exchange Server.
- Para sincronizar o Secure Notes e o Secure Tasks para Android, use a conta do Secure Mail para Android.

Quando adicionar o Secure Mail, Secure Notes e Secure Tasks ao Citrix Endpoint Management (anteriormente XenMobile), configure as políticas MDX conforme mencionado em Políticas de aplicativo MDX para a configuração de serviços em segundo plano.

> **Nota:**
>
> O Secure Mail para Android e o Secure Mail para iOS dão suporte ao caminho completo especificado para um servidor Notes Traveler. Por exemplo: `https://mail.example.com/traveler/Microsoft-Server-ActiveSync`.
>
> Não é mais necessário configurar o Domino Directory com o site de substituição de regras para o servidor Traveler.

Configuração do servidor IBM Notes Traveler para Secure Mail

Em ambientes de IBM Notes, você deve configurar o servidor IBM Notes Traveler antes de implantar o Secure Mail. Esta seção mostra uma ilustração de implantação dessa configuração, bem como os requisitos do sistema.

> **Importante:**
>
> Se o seu servidor Notes Traveler usa SSL 3.0, saiba que o SSL 3.0 contém uma vulnerabilidade chamado de ataque de Padding Oracle On Downgraded Legacy Encryption (POODLE), que é um ataque intermediários que afeta qualquer aplicativo que se conecta a um servidor com SSL 3.0. Para resolver as vulnerabilidades introduzidas pelo ataque de POODLE, o Secure Mail desativa as conexões de SSL 3.0 como padrão e usa o TLS 1.0 para se conectar ao servidor. Como resultado, o Secure Mail não pode se conectar a um servidor de Notes Traveler que usa SSL 3.0. Para obter detalhes sobre uma solução recomendada, consulte a seção Configuração de nível de segurança SSL/TLS em Integração do Exchange Server ou servidor IBM Notes Traveler.

Em ambientes de IBM Notes, você deve configurar o servidor IBM Notes Traveler antes de implantar o WorxMail.

O seguinte diagrama mostra o posicionamento na rede dos servidores IBM Notes Traveler e de um servidor de email IBM Domino em uma implantação de exemplo.

Requisitos do sistema

Requisitos de infraestrutura do servidor

- IBM Domino Mail Server 9.0.1
- IBM Notes Traveler 9.0.1

Protocolos de autenticação

- Banco de dados Domino
- Protocolo de autenticação do Lotus Notes
- Protocolo de autenticação de Lightweight Directory

Requisitos de porta

- Exchange: a porta SSL padrão é 443.
- IBM Notes: SSL tem suporte na porta 443. Não-SSL tem suporte, como padrão, na porta 80.

Configuração de nível de segurança SSL/TLS

A Citrix fez modificações no Secure Mail para resolver vulnerabilidades introduzidas pelo ataque de POODLE, conforme descrito na nota “Importante” anterior. Se o seu servidor Notes Traveler usa SSL 3.0, para ativar conexões, a solução alternativa recomendada é usar TLS 1.2 no servidor IBM Notes Traveler 9.0.

A IBM tem um patch para impedir o uso de SSL 3.0 na comunicação de servidor a servidor do Notes Traveler. O patch, lançado em novembro 2014, está incluído como atualizações de correção provisória para as seguintes versões do servidor do Notes Traveler: 9.0.1 IF7, 9.0.0.1 IF8 e 8.5.3 Upgrade Pack 2 IF8 (e serão incluídos em todas as versões futuras). Para obter detalhes sobre o patch, consulte LO82423: DISABLE SSLV3 FOR TRAVELER SERVER TO SERVER COMMUNICATION.

Como uma solução alternativa, ao adicionar o Secure Mail ao Endpoint Management, altere o nível de política de segurança de conexão para **SSLv3 e TLS**. Para obter as informações mais recentes sobre esse problema, consulte SSLv3 Connections Disabled by Default on Secure Mail 10.0.3.

As seguintes tabelas indicam os protocolos a que o Secure Mail dá suporte, de acordo com o sistema operacional, com base no valor de política de nível de segurança de conexão. Seu servidor de email também deve ter a capacidade de negociar o protocolo.

A tabela a seguir mostra os protocolos com suporte para o Secure Mail quando o nível de segurança de conexão é SSLv3 e TLS.

Tipo de sistema operacional	SSLv3	TLS
iOS 9 e versões posteriores	Não	Sim
Anterior a Android M	Sim	Sim
Android M e Android N	Sim	Sim
Android O	Não	Sim

A tabela a seguir mostra os protocolos com suporte para o Secure Mail quando o nível de segurança de conexão é TLS.

Tipo de sistema operacional	SSLv3	TLS
iOS 9 e versões posteriores	Não	Sim
Anterior a Android M	Não	Sim
Android M e Android N	Não	Sim
Android O	Não	Sim

Configuração do servidor de Notes Traveler

As informações a seguir correspondem à configuração de páginas no cliente do IBM Domino Administrator.

- **Security:** Autenticação da Internet está definida como Fewer name variations with higher security. Esta configuração é usada para mapear UID para AD User ID em protocolos de autenticação LDAP.
- **Configurações NOTES.INI:** Adicione **NTS_AS_ENFORCE_POLICY**=**false**. Isso permite que as políticas do Secure Mail sejam administradas pelo Endpoint Management em vez do Traveler. Esta configuração pode entrar em conflito com as implantações de cliente atual, mas simplificarão o gerenciamento do dispositivo nas implantações de Endpoint Management.
- **Protocolos de sincronização:** SyncML no IBM Notes e sincronização de dispositivo móvel não têm suporte do Secure Mail por enquanto. O Secure Mail sincroniza itens de email, calendário e contatos por meio do protocolo Microsoft ActiveSync incorporado em servidores Traveler. Se o SyncML for forçado como o protocolo principal, o Secure Mail não pode se conectar por meio da infraestrutura Traveler.
- **Configuração do Domino Directory - Web Internet Sites:** Substituir a autenticação de sessão em /traveler para desativar autenticação baseada em formulário.

S/MIME para Secure Mail

June 12, 2019

O Secure Mail oferece suporte a Secure/Multipurpose Internet Mail Extensions (S/MIME), permitindo que os usuários assinem e criptografem mensagens para maior segurança. A assinatura garante ao destinatário que o remetente identificado não enviou a mensagem a um impostor. A criptografia garante que apenas os destinatários com um certificado compatível tenham permissão para abrir a mensagem.

Para obter detalhes sobre S/MIME, consulte Microsoft TechNet.

Na tabela a seguir, X indica que o Secure Mail dá suporte a um recurso S/MIME no sistema operacional do dispositivo.

Recurso S/MIME	iOS	Android
Integração de provedores de identidade digital: você pode integrar o Secure Mail com um provedor de identidade digital de terceiros compatível. O provedor de identidade host fornece certificados para um aplicativo de provedor de identidade em dispositivos do usuário. Esse aplicativo envia certificados para o cofre compartilhado do Endpoint Management, uma área de armazenamento segura para dados confidenciais de aplicativos. O Secure Mail obtém certificados do cofre compartilhado. Para obter detalhes, consulte Integração com um provedor de identidade digital.	X	

Recurso S/MIME	iOS	Android
Suporte a credenciais derivadas	O Secure Mail dá suporte ao uso de credenciais derivadas como uma fonte de certificado. Para obter mais informações sobre credenciais derivadas, consulte Credenciais derivadas para iOS.	
Distribuição de certificado por email: A distribuição de certificados por email requer que você crie modelos de certificado e, em seguida, use os modelos para solicitar certificados de usuário. Após instalar e validar os certificados, exporte os certificados de usuário e depois envie-os por email para os usuários. Os usuários então abrem o email no Secure Mail e importam os certificados. Para obter detalhes, consulte Distribuição de certificados por email.	X	X

Recurso S/MIME	iOS	Android
Importação automática de certificados finalidade única: O Secure Mail detecta se um certificado é somente para assinatura ou criptografia e então importa automaticamente o certificado e notifica o usuário. Se um certificado servir para as duas finalidades, os usuários são solicitados para importá-lo.	X	

Integração com um provedor de identidade digital

O seguinte diagrama mostra o caminho que um certificado digital faz a partir do host do provedor de identidade para o Secure Mail. Isso ocorre quanto você integra o Secure Mail com suporte a um provedor de identidade digital de terceiro.

O cofre compartilhado do MDX é uma área de armazenamento para os dados confidenciais do aplicativo, como certificados. Somente o aplicativo habilitado pelo Endpoint Management pode acessar o cofre compartilhado.

Pré-requisitos

Secure Mail oferece suporte para a integração com Entrust IdentityGuard.

Configuração da integração

1. Prepare o aplicativo provedor de identidade e forneça-o aos usuários:
    - Entre em contato com a Entrust para obter o .ipa para preparar.
    - Use o MDX Toolkit para preparar o aplicativo.

      Se você implantar este aplicativo para os usuários que já têm uma versão do aplicativo fora do ambiente do Endpoint Management, use uma ID exclusiva para este aplicativo. Use o mesmo perfil de provisionamento para este aplicativo e o Secure Mail.

- Adicione o aplicativo ao Endpoint Management e publique-o na loja de aplicativos do Endpoint Management.
- Informe aos seus usuários que eles devem instalar o aplicativo provedor de identidade no Secure Hub. Forneça instruções, conforme o necessário, sobre as etapas de pós-instalação.

  Dependendo de como você configurar as políticas de S/MIME para o Secure Mail na próxima etapa o Secure Mail poderá solicitar aos usuários que instalem certificados ou ativar o S/MIME nas configurações do Secure Mail. As etapas para ambos os procedimentos estão em Ativação de S/MIME no Secure Mail para iOS.

2. Ao adicionar o Secure Mail ao Endpoint Management, configure estas políticas:
   - Definir a política de origem de certificado S/MIME como **Cofre compartilhado**. Esta configuração significa que o Secure Mail usa os certificados armazenados no seu cofre compartilhado pelo seu provedor de identidade digital.
   - Para ativar o S/MIME durante a configuração inicial do Secure Mail, configure a política Ativar S/MIME durante a primeira inicialização do Secure Mail. A política determina se o Secure Mail ativa S/MIME quando houver certificados no cofre de dados compartilhado. Se nenhum certificado estiver disponível, o Secure Mail solicita ao usuário para importar certificados. Se a política não estiver ativada, os usuários podem ativar o controle S/MIME nas configurações do Secure Mail. Como padrão, o Secure Mail não ativa o S/MIME, o que significa que os usuários devem ativar o S/MIME através das configurações do Secure Mail.

Uso de credenciais derivadas

Em vez de se integrar a um provedor de identidade digital, você pode permitir o uso de credenciais derivadas.

Ao adicionar o Secure Mail ao Endpoint Management, configure a política de origem de certificado S/MIME para **Credenciais Derivadas**. Para obter mais informações sobre credenciais derivadas, consulte Credenciais derivadas para iOS.

Distribuição de certificados por email

Em vez de integração com um provedor de identidade digital ou usar credenciais derivadas, você pode distribuir certificados para usuários por email. Esta opção requer as seguintes etapas gerais que estão detalhados nesta seção.

1. Use o Gerenciador de Servidor para ativar o registro da web para Serviços de Certificados Microsoft e verificar as configurações de autenticação no IIS.

2. Crie modelos de certificado para assinar e criptografar mensagens de email. Use os modelos para solicitar certificados de usuário.
3. Instale e valide os certificados, exporte os certificados de usuário e depois envie-os por email para os usuários.
4. Os usuários abrem o email do Secure Mail e importam os certificados. Os certificados, portanto, ficam disponíveis somente para o Secure Mail. Eles não serão exibidos no perfil para iOS S/MIME.

Pré-requisitos

As instruções nesta seção são baseadas nos seguintes componentes:

- XenMobile Server 10 e versões posteriores
- Uma versão suportada do Citrix Gateway, anteriormente NetScaler Gateway
- O Secure Mail para iOS (versão mínima 10.8.10); Secure Mail para dispositivos Android (versão mínima 10.8.10)
- Microsoft Windows Server 2008 R2 ou versões posteriores com serviços de certificados Microsoft que atuam como a raiz de autoridade de certificação (CA)
- Microsoft Exchange:
  - Atualização cumulativa 4 do Exchange Server 2016
  - Atualização cumulativa 14 do Exchange Server 2016
  - Exchange Server 2010 SP3 Update Rollup 16

Você deve atender aos pré-requisitos a seguir antes de configurar o controle S/MIME:

- Entregue os certificados raiz e intermediários para os dispositivos móveis manualmente ou por meio de uma política de credenciais de dispositivo no Endpoint Management. Para obter detalhes, consulte Política de dispositivo de credenciais.
- Se você estiver usando certificados de servidor privados para proteger o tráfego do ActiveSync para o Servidor do Exchange, faça o seguinte: instale todos os certificados raiz e intermediários nos dispositivos móveis.

Ativar o registro na web dos serviços de certificado Microsoft

1. Vá até **Ferramentas administrativas** e selecione **Gerenciador de servidor**.
2. Em **Serviços de certificados do Active Directory**, verifique se o **Registro na web da autoridade de certificação** está instalado.
3. Selecione **Adicionar serviços de função** para instalar o Registro na web da autoridade de certificação, se necessário.
4. Assinale **Registro na web de autoridade de certificação** e clique em **Avançar**.

5. Clique em **Fechar** ou **Concluir** quando a instalação for concluída.

Verificação das suas configurações de autenticação no IIS

- Verifique se o site de inscrição na Web usado para solicitar certificados de usuário (por exemplo, `https://ad.domain.com/certsrv/`) está protegido com um certificado de servidor de HTTPS (particular ou público).
- O site de inscrição na web deve ser acessado por HTTPS.

1. Vá até **Ferramentas administrativas** e selecione **Gerenciador de servidor**.
2. Em **Servidor Web (IIS)**, procure em **Serviços de função**. Verifique se a autenticação de mapeamento de certificado de cliente e a autenticação de mapeamento de certificado de cliente IIS estão instalados. Caso não estejam, instale os serviços de função.
3. Vá até **Ferramentas administrativas** e selecione **Gerenciador de Serviços de Informações da Internet (IIS)**.
4. No painel esquerdo da janela do **gerenciador do IIS**, selecione o servidor que está executando a instância de IIS para o registro na web.
5. Clique em **Autenticação**.
6. Certifique-se de que a **Autenticação de certificado de cliente Active Directory** está **Habilitado**.
7. Clique em **Sites > Site padrão para Microsoft Internet Information Services > Associações** no painel direito.
8. Adicione uma associação HTTPS, se ainda não existir.
9. Ir para a página inicial do site da web padrão.
10. Clique em **Configurações de SSL** e clique em **Aceitar para certificados do cliente**.

Criação de novos modelos de certificado

Para assinar e criptografar mensagens de email, a Citrix recomenda que você crie novos certificados nos serviços de certificados do Active Directory da Microsoft. Se você usar o mesmo certificado para as duas finalidades e arquivar o certificado de criptografia, é possível recuperar um certificado de assinatura e permitir assinar por outra pessoa.

O procedimento a seguir duplica os modelos de certificado da Autoridade de Certificação (CA):

- Somente assinatura do Exchange (para assinatura)
- Usuário do Exchange (para criptografia)

1. Abrir o snap-in da Autoridade de Certificação.
2. Expanda a autoridade de certificação e vá para **Modelos de Certificado**.
3. Clique com o botão direito do mouse e, em seguida, clique em **Gerenciar**.

4. Procure o modelo Somente Assinatura do Exchange, clique com o botão direito no modelo e, em seguida, clique em **Duplicar modelo**.
5. Atribua qualquer nome.
6. Assinale a caixa de seleção **Publicar certificado no Active Directory**.

   > **Nota:**
   >
   > Se você não marcar a caixa de seleção **Publicar certificado no Active Directory**, os usuários devem publicar os certificados de usuário (para assinatura e criptografia) manualmente. Eles podem fazer isso por meio de **Cliente de email do Outlook > Central de confiabilidade > Segurança de email > Publicar na GAL (lista de endereços Global)**.

7. Clique na guia **Tratamento de solicitação** e defina os seguintes parâmetros:
   - **Finalidade:** assinatura
   - **Tamanho mínimo da chave:** 2048
   - **Caixa de seleção Permitir que a chave privada seja exportada:**selecionada
   - **Caixa de seleção Registrar requerente sem solicitar entrada do usuário:** selecionada
8. Clique na guia **Segurança**, em **Nomes de usuário ou grupo**, verifique se **Usuários autenticados** (ou outro grupo de segurança de domínio desejado) foi adicionado. Também garanta que em **Permissões para usuários autenticados**, as caixas de seleção **Leitura e Registro** estão selecionadas para **Permitir**.
9. Para todas as outras guias e configurações, deixe as configurações padrão.
10. Em **Modelos de certificado**, clique em **Usuário do Exchange** e, em seguida, repita as etapas de 4 até 9.

    Para o novo modelo de Usuário do Exchange, use as mesmas configurações padrão para o modelo original.

11. Clique na guia **Tratamento de solicitação** e defina os seguintes parâmetros:
    - **Finalidade**: criptografia
    - **Tamanho mínimo da chave:** 2048
    - **Caixa de seleção Permitir que a chave privada seja exportada:**selecionada
    - **Caixa de seleção Registrar requerente sem solicitar entrada do usuário:** selecionada
12. Quando os dois modelos são criados, lembre-se de emitir os dois modelos de certificado. Clique em **Novo** e, em seguida, clique em **Modelo de Certificado a Ser Emitido**.

Solicitação de certificados de usuário

Este procedimento usa “user1” para navegar para a página de inscrição da Web; por exemplo, `https://ad.domain.com/certsrv/`. O procedimento solicita dois novos certificados de usuário para email seguro: um certificado para assinatura e outro para criptografia. Você pode repetir o mesmo procedimento para outros usuários de domínio que exigem o uso de S/MIME por Secure Mail.

A inscrição manual através do site de registro na web (por exemplo, `https://ad.domain.com/certsrv/`) em Serviços de Certificados Microsoft para gerar os certificados de usuário para assinatuta e criptografia. Uma alternativa é configurar inscrição automática através de uma Política de Grupo para o grupo de usuários que usariam este recurso.

1. Em um computador com o Windows, abra o Internet Explorer e vá para o site de inscrição para solicitar um novo certificado de usuário.

   > **Nota:**
   >
   > Faça logon com o nome de usuário de domínio correto para solicitar o certificado.

2. Quando conectado, clique em **Solicitar um certificado**.
3. Clique em **Solicitação de certificado avançado**.
4. Clique em **Criar e enviar uma solicitação a esta autoridade de certificação**.
5. Gere o certificado de usuário para fins de assinatura. Selecione o nome do modelo apropriado nome e digite suas configurações de usuário e, em seguida, próximo a **Solicitar formato**, selecione **PKCS10**.

   A solicitação foi enviada.

6. Clique em **Instalar este certificado**.
7. Confirme se o certificado foi instalado com êxito.
8. Repetir o mesmo procedimento, mas agora para criptografar mensagens de email. Com o mesmo usuário conectado ao Web site de registro, vá para o link Página inicial para solicitar um novo certificado.
9. Selecione o novo modelo para a criptografia e digite as mesmas configurações de usuário que você inseriu na etapa 5.
10. Verifique se você instalou o certificado com êxito e repita o mesmo procedimento para gerar um par de certificados de usuário para outro usuário de domínio. Este exemplo segue o mesmo procedimento e gera um par de certificados para “User2”.

    > **Nota:**

> Esse procedimento usa o mesmo computador com Windows para solicitar o segundo par de certificados para “User2”.

Validação de certificados publicados

1. Para garantir que os certificados estão instalados corretamente no domínio perfil de usuário, vá para **Usuários e computadores do Active Directory > Exibir > Recursos avançados**.
2. Ir para as propriedades do usuário (User1 neste exemplo) e, em seguida, clique na guia **Certificados publicados**. Verifique se ambos os certificados estão disponíveis. Você também pode verificar se cada certificado tem um uso específico.

   A figura apresenta um certificado para criptografar mensagens de email.

   A figura apresenta um certificado para assinar mensagens de email.

   Verifique se o certificado correto criptografado está atribuído ao usuário. Você pode verificar essas informações em **Usuários e computadores do Active Directory > Propriedades de usuário**.

   O modo de funcionamento do Secure Mail é verificando o atributo de objeto de usuário userCertificate por meio de consultas LDAP. Você pode ler o valor na guia **Editor de atributos**. Se este campo está vazio ou tem o certificado de usuário incorreto para criptografia, o Secure Mail não pode criptografar (ou descriptografar) uma mensagem.

Exportação de certificados de usuário

Este procedimento exporta os pares de certificados “User1” e “User2 no formato .PFX (PKCS#12) com a chave privada. Quando exportados, os certificados são enviados por email ao usuário por meio do Outlook Web Access (OWA).

1. Abra o console do MMC e vá para o snap-in de **Certificados - Usuário atual**. Você vê dois pares de certificados “User1” e “User2”.
2. Clique com o botão direito do mouse no certificado e, em seguida, clique em **Todas as Tarefas > Exportar**.
3. Exportar a chave privada selecionando **Sim, exportar a chave privada.**
4. Assinale as caixas de seleção **Incluir todos os certificados no caminho de certificação, se possível** e **Exportar todas as propriedades estendidas**.
5. Quando você exportar o certificado, repita o mesmo procedimento para o restante certificados para usuários.

> **Nota:**
>
> Identifique com clareza qual certificado é o de assinatura e qual é o de criptografia. No exemplo, os certificados estão marcados como userX-sign.pfx and userX-enc.pfx.

Enviando por meio de certificados

Quando todos os certificados tiverem sido exportados no formato PFX, você poderá usar o Outlook Web Access (OWA) para enviá-los por email. O nome de logon neste exemplo é User1 e o email enviado contém ambos os certificados.

Repetir o mesmo procedimento para User2 ou outros usuários no domínio.

Ativação do controle S/MIME do Secure Mail para iOS e Android

Depois que o email tenha sido entregue, a próxima etapa é abrir a mensagem usando Secure Mail e, em seguida, ativar o controle S/MIME com os certificados apropriados para autenticação e criptografia.

Para habilitar o S/MIME com certificados individuais de assinatura e criptografia

1. Abra o Secure Mail e navegue até o e-mail que contém os certificados S/MIME.
2. Toque no certificado de assinatura para baixar e importar.
3. Digite a senha atribuída à chave privada quando o certificado de assinatura foi exportado do servidor.

   Seu certificado foi importado.
4. Toque em **Ativar a assinatura**
5. Alternativamente, você pode navegar para **Configurações** > e **S/MIME** e tocar em S/MIME para ativar o certificado de assinatura.
6. Na tela **Assinatura**, verifique se o certificado de assinatura correto foi importado.
7. Volte para o email e toque no certificado de criptografia para baixar e importar.
8. Digite a senha atribuída à chave privada quando o certificado de criptografia foi exportado do servidor.

   Seu certificado foi importado.
9. Toque em **Ativar a criptografia**

10. Alternativamente, você pode navegar para **Configurações** > e **S/MIME** e tocar em S/MIME para ativar **Criprografar como padrão**.
11. Na tela **Criptografia**, verifique se o certificado de criptografia correto foi importado.

> **Nota:**
>
> a) Se um email é assinado digitalmente com S/MIME, tem anexos e o destinatário não tem o controle S/MIME ativado, os anexos não serão recebidos. Este comportamento é uma limitação Active Sync. Para receber mensagens S/MIME com eficácia, ative S/MIME nas configurações do Secure Mail.
>
> b) A opção **Criptografar como padrão** permite minimizar as etapas necessárias para criptografar seu email.
> Se esse recurso estiver ativado, seu email estará no estado criptografado enquanto estiver sendo redigido.
> Se esse recurso estiver desativado, seu email estará no estado não criptografado ao ser redigido e você precisará tocar no ícone **Bloquear** para criptografá-lo.

Para habilitar o S/MIME com um único certificado de assinatura e criptografia

1. Abra o Secure Mail e navegue até o e-mail que contém o certificado S/MIME.
2. Toque no certificado S/MIME para baixar e importar.
3. Digite a senha atribuída à chave privada quando o certificado foi exportado do servidor.
4. Nas opções de certificado exibidas, toque na opção apropriada para importar certificado de assinatura ou certificado de criptografia.
   Toque em **Abrir certificado** para ver detalhes sobre o certificado.

   Seu certificado foi importado.

   Você pode ver os certificados importados navegando para **Configurações > S/MIME**

Teste do S/MIME para iOS e Android

Depois de executar as etapas listadas na seção anterior, seu destinatário poderá ler seus emails assinados e criptografados.

A imagem a seguir mostra um exemplo de uma mensagem criptografada conforme lida pelo destinatário.

A imagem a seguir mostra um exemplo de verificação de certificado de assinatura confiável.

O Secure Mail pesquisa o domínio do Active Directory em busca de certificados de criptografia pública de destinatários. Se um usuário envia uma mensagem criptografada para um destinatário que não

tem uma chave de criptografia pública válida, a mensagem será enviada sem criptografia. Em uma mensagem de grupo, mesmo se apenas um destinatário não tiver uma chave válida, a mensagem será enviada a todos os destinatários sem criptografia.

Configuração de fontes de certificado público

Para usar certificados públicos do S/MIME, configure a origem de certificado público de S/MIME, endereço do servidor LDAP, DN Base de LDAP e políticas de acesso LDAP anônimo.

Além das políticas do aplicativo, faça o seguinte:

- Se os servidores LDAP são públicos, certifique-se de que o tráfego passa diretamente para os servidores LDAP. Para fazer isso, configure a política de rede para o Secure Mail ser **Com túnel para a rede interna** e configurar o DNS de divisão para o Citrix ADC.
- Se os servidores LDAP em uma rede interna, faça o seguinte:
  - Para iOS, você não configura a política de gateway de serviço de rede em segundo plano. Se você configurar a política, os usuários recebem pedidos de autenticação frequentes.
  - Para o Android, você deve adicionar o **URL do servidor LDAP** na lista da política de Gateway de serviço de rede em segundo plano.

SSO para Secure Mail

April 16, 2019

Você pode configurar o Endpoint Management para registrar usuários automaticamente no Secure Mail quando eles se registram no Secure Hub. Os usuários não têm que digitar mais informações nem executar mais etapas para se registrarem no Secure Mail. Para usuários que se registram no Secure Hub com credenciais por email, este recurso requer que a descoberta automática esteja ativada. Se a descoberta automática não estiver ativada, você pode ativar este recurso para os seguintes modos de registro:

- O endereço do Endpoint Management é passado do Secure Hub para o Secure Mail.
- Os usuários fornecem o endereço do Endpoint Management quando se registram no Secure Hub.

Para ativar o registro automático no Secure Mail

1. Nas propriedades do cliente Endpoint Management, na página **Configurações**, faça o seguinte:

   a. Defina os seguintes valores como **true**:

- ENABLE_PASSCODE_AUTH
- ENABLE_PASSWORD_CACHING
- ENABLE_CREDENTIAL_STORE

b. Adicione esta configuração:

- **Nome de exibição**: SEND_LDAP_ATTRIBUTES
- **Valor**: userPrincipalName=${user.userprincipalname},sAMAccountNAme=${user.samaccountname}, displayName= ${ user.displayName} ,mail= ${ user.mail}

2. Na página **Configurações**, adicione esta configuração à propriedade do servidor:

   MAM_MACRO_SUPPORT definida como **true**

3. Configure estar propriedades do Secure Mail:

   - Defina o mecanismo de autenticação inicial como **Endereço de email do usuário**.
   - Defina as credenciais de autenticação iniciais como **userPrincipalName**.

4. Configure por email AutoDiscovery Service da caixa de correio do Exchange Server do usuário. Para obter suporte, entre em contato com o administrador do Microsoft Exchange. Este artigo pressupõe que você configure o Autodiscovery Service por meio de consultas DNS para um registro de servidor.

Para configurar a política de aplicativo do Secure Mail

Carregue o aplicativo Secure Mail para o Endpoint Management. Carregue o arquivo .mdx associado à versão correta do aplicativo Secure Mail. Em seguida, defina as seguintes configurações de aplicativo no Secure Mail:

1. Em Mecanismo de autenticação inicial, clique em **Endereço de email do usuário**.
2. Em **Credenciais de autenticação inicial**, clique em **userPrincipalName** ou **sAMAccountName**. Sua seleção é baseada no tipo de autenticação configurado com relação ao Exchange Mail Server do usuário.
3. Deixe vazios os campos de domínio de usuário do Exchange Server do Secure Mail e o Domínio de usuário do Secure Mail.
4. Configure outras políticas do aplicativo Secure Mail conforme necessário e verifique as atribuições de grupo de entrega necessários.

A experiência completa do usuário do Secure Mail SSO com provisionamento automático

Você deve atender aos seguintes pré-requisitos.

1. Instale o Secure Hub da Apple App Store (iOS) ou o Google Play Store (Android).
2. Abra o Secure Hub e insira um endereço de email e uma senha para o registro no Endpoint Management.
3. Instale o Secure Mail da Apple App Store (iOS) ou o Google Play Store (Android).
4. Abra o Secure Mail e toque em **OK**. Esta etapa permite que o Secure Hub gerencie o Secure Mail. Ao abrir, o Secure Mail é configurado automaticamente.

O Exchange Server que corresponde ao banco de dados de caixa de correio do usuário é obtido do Autodiscovery Service que você configurou. A consulta do registro SRV de DNS faz uso de endereço de email do usuário obtido do Secure Hub.

Todos os detalhes necessários para a configuração de conta, como o endereço de email, userPrincipalName/sAMAccountName e a senha são obtidos do Secure Hub.

Quando a conta está configurada, os usuários podem exibir detalhes sobre o dispositivo em **Secure Mail** > **Configurações** > **Conta**.

Resolução de problemas

Se qualquer ocorrer com a configuração de SSO, você pode tentar as etapas a seguir.

1. A versão do XenMobile Server deve ser 10.5 ou posterior.
2. O Endpoint Management deve estar configurado para AutoDiscovery Service e o registro de usuário deve estar configurado para uso com um endereço de email.
3. O domínio do Exchange Server deve ser configurado com detecção automática. A consulta para o registro SRV retorna o email esperado detalhes do servidor para os clientes de email do ActiveSync.
4. No caso de um problema com essa funcionalidade, obtenha as seguintes informações e entre em contato com o suporte técnico da Citrix:
    - Faça o download dos logs de diagnóstico do Endpoint Management.
    - Obtenha logs de diagnóstico do Secure Mail com o mais alto nível de log.
    - Obtenha os logs de IIS do diretório C:\inetpub\logs\LogFiles\W3SVC1 do Exchange Server que hospeda o Autodiscovery Service. Para obter mais detalhes sobre o Microsoft AutoDiscovery Service, consulte Autodiscover service in Exchange Server

Considerações de segurança

June 12, 2019

Este artigo discute as considerações de segurança do Secure Mail e configurações específicas que você pode habilitar para ajudar a aumentar a segurança dos dados.

Suporte à proteção de direitos de e-mail Microsoft IRM e AIP

O Secure Mail para Android e iOS dão suporte a mensagens protegidas com o Gerenciamento de Direitos de Informação (IRM) da Microsoft e a solução de Proteção de Informações do Azure (AIP). Esse suporte está sujeito à política de IRM configurada no Citrix Endpoint Management.

Esse recurso permite que as organizações que usam o IRM apliquem proteção ao conteúdo de mensagens. O recurso também permite que os usuários de dispositivos móveis sejam capazes de criar e consumir conteúdo protegido por direitos. Como padrão, o suporte a IRM é **Desativado**. Para ativar o suporte a IRM, defina a política de Gerenciamento de Direitos de Informação como **Ativada**.

Para habilitar o Gerenciamento de Direitos de Informação no Secure Mail

1. Faça logon no Endpoint Management e navegue até **Configurar** > **Aplicativos** e clique em **Adicionar**.
2. Na tela **Adicionar aplicativo**, clique em **MDX**.
3. Na tela **Informações do aplicativo**, insira os detalhes do aplicativo e clique em **Avançar**.
4. Com base no sistema operacional do seu dispositivo, selecione e carregue o arquivo .mdx.
5. Ative o Gerenciamento de Direitos de Informação em **Configurações do aplicativo**.

> Nota:
>
> Ative o Gerenciamento de Direitos de Informação para iOS e Android.

Quando você recebe um email protegido por direitos

Quando os usuários recebem um email com conteúdo protegido, eles veem a seguinte tela:

Para ver detalhes sobre os direitos que o usuário tem, toque em **Detalhes**.

Quando você redige um email protegido por direitos

Quando os usuários redigem um email, eles podem definir perfis de restrição para habilitar a proteção de email.

Para definir restrições ao seu email:

1. Faça login no Secure Mail e toque no ícone **Redigir**.
2. Na tela de redação, toque no ícone **Restrição de email**.
3. Na tela **Perfis de restrição**, toque nas restrições que deseja aplicar ao email e, em seguida, clique de volta.

   As restrições aplicadas aparecem abaixo do campo de assunto.

Algumas organizações podem exigir respeito estrito à política de IRM. Usuários com acesso ao Secure Mail podem tentar ignorar a política de IRM adulterando o Secure Mail, o sistema operacional, ou até mesmo a plataforma de hardware.

Embora o Endpoint Management possa detectar determinados ataques, pense nas seguintes medidas preventivas para aumentar a segurança:

- Revice as orientações de segurança fornecidas pelo fornecedor do dispositivo.
- Configure os dispositivos de acordo, usando os recursos do Endpoint Management ou outros.
- Forneça orientação para seus usuários para o uso apropriado dos recursos de IRM, incluindo o Secure Mail.
- Implante software de segurança adicional para resistir a esse tipo de ataque.

Classificações de segurança de email

O Secure Mail para iOS e Android oferece suporte à marcação de classificação de emails, o que possibilita que os usuários especifiquem segurança (SEC) e marcadores de limitação de disseminação (DLM) ao enviar emails. As marcações SEC são Protected, Confidential e Secret. As DLM são Sensitive, Legal ou Personal. Ao redigir um email, o usuário de Secure Mail pode selecionar uma marcação para indicar o nível de classificação de email, conforme mostrado nas imagens a seguir.

Os destinatários podem exibir a marcação de classificação no assunto do email. Por exemplo:

- Assunto: Planeamento [SEC = PROTECTED, DLM = Sensitive]
- Assunto: Planeamento [DLM = Sensitive]
- Assunto: Planeamento [SEC = UNCLASSIFIED]

Os cabeçalhos de email contêm marcações de classificação como uma extensão de cabeçalho de mensagem de Internet, mostradas em negrito como neste exemplo:

Data: Sex, 01 de maio de 2015 12:34:50 +530

Assunto: Planeamento [SEC = PROTECTED, DLM = Sensitive]

Prioridade: normal

X-prioridade: normal **X-Protective-Marking: VER-2012.3, NS=gov.au,SEC = PROTECTED , DLM = Sensitive,ORIGIN=operations@example.com**

De: operations@example.com

Para: Team <mylist@example.com>

MIME-Version: 1.0 Content-Type: multipart/alternative;boundary="_com.example.email_6428E5E4-9DB3-4133-9F48-155913E39A980"

O Secure Mail somente exibe as marcações de classificação. O aplicativo não executa nenhuma ação com base nessas marcações.

Quando um usuário responde ou encaminha um email com marcações de classificação, os valores SEC e DLM padrão passam para as marcações do email original. O usuário pode escolher uma marcação diferente. O Secure Mail não valida essas alterações em relação ao email original.

Você pode configurar as marcações de classificação através das seguintes políticas de MDX.

- **Classificação de email:** Se o valor for **Ativado**, o Secure Mail dará suporte a marcações de classificação de email para SEC e DLM. As marcações de classificação aparecem em cabeçalhos de email como valores "X-Protective-Marking". Lembre-se de configurar as políticas de classificação de email correspondentes. O valor padrão é **Desativado**.
- **Espaço de nome de classificação de email:** Especifica o espaço de nome de classificação que é necessário no cabeçalho do email pelo padrão de classificação usado. Por exemplo, o espaço de nome "gov.au" aparece no cabeçalho como "NS=gov.au". O valor padrão é vazio.
- **Versão de classificação de email:** Especifica a versão de classificação que é necessária no cabeçalho do email pelo padrão de classificação usado. Por exemplo, a versão "2012.3" aparece no cabeçalho como "VER=2012.3". O valor padrão é vazio.
- **Classificação padrão de email:** Especifica a marcação protetora que o Secure Mail aplica a um email se um usuário não escolher uma marcação. Esse valor deve estar na lista para a política Marcações de classificação de email. O valor padrão é **UNOFFICIAL**.
- **Marcações de classificação de email:** Especifica as marcações de classificação que devem ser disponibilizadas aos usuários. Se a lista estiver vazia, o Secure Mail não inclui uma lista de marcações protetoras. A lista contém pares de marcações valor que são separados por ponto-e-vírgula. Cada par inclui o valor da lista que aparece no Secure Mail e o valor de marcação e é o texto acrescentado ao assunto do email e cabeçalho no Secure Mail. Por exemplo, no par de marcação "UNOFFICIAL,SEC=UNOFFICIAL;", o valor da lista é "UNOFFICIAL" e o valor da marcação é "SEC=UNOFFICIAL".

O valor padrão é uma lista de marcações de classificação que você pode modificar. As marcações a seguir são fornecidas com o Secure Mail.

- UNOFFICIAL,SEC=UNOFFICIAL
- UNCLASSIFIED,SEC=UNCLASSIFIED
- For Official Use Only,DLM=For-Official-Use-Only

- Sensitive,DLM=Sensitive
- Sensitive:Legal,DLM=Sensitive:Legal
- Sensitive:Personal,DLM=Sensitive:Personal
- PROTECTED,SEC=PROTECTED
- PROTECTED+Sensitive,SEC=PROTECTED
- PROTECTED+Sensitive:Legal,SEC=PROTECTED DLM=Sensitive:Legal
- PROTECTED+Sensitive:Personal,SEC=PROTECTED DLM=Sensitive:Personal
- PROTECTED+Sensitive:Cabinet,SEC=PROTECTED,DLM=Sensitive:Cabinet
- CONFIDENTIAL,SEC=CONFIDENTIAL
- CONFIDENTIAL+Sensitive,SEC=CONFIDENTIAL,DLM=Sensitive
- CONFIDENTIAL+Sensitive:Legal,SEC=CONFIDENTIAL DLM=Sensitive:Legal
- CONFIDENTIAL+Sensitive:Personal,SEC=CONFIDENTIAL,DLM=Sensitive:Personal
- CONFIDENTIAL+Sensitive:Cabinet,SEC=CONFIDENTIAL DLM=Sensitive:Cabinet
- SECRET,SEC=SECRET
- SECRET+Sensitive,SEC=SECRET,DLM=Sensitive
- SECRET+Sensitive:Legal,SEC=SECRET,DLM=Sensitive:Legal
- SECRET+Sensitive:Personal,SEC=SECRET,DLM=Sensitive:Personal
- SECRET+Sensitive:Cabinet,SEC=SECRET,DLM=Sensitive:Cabinet
- TOP-SECRET,SEC=TOP-SECRET
- TOP-SECRET+Sensitive,SEC=TOP-SECRET,DLM=Sensitive
- TOP-SECRET+Sensitive:Legal,SEC=TOP-SECRET DLM=Sensitive:Legal
- TOP-SECRET+Sensitive:Personal,SEC=TOP-SECRET DLM=Sensitive:Personal
- TOP-SECRET+Sensitive:Cabinet,SEC=TOP-SECRET DLM=Sensitive:Cabinet

Proteção de dados de iOS

As empresas que devem cumprir os requisitos de proteção de dados da Australian Signals Directorate (ASD) podem usar as novas políticas de **Ativar proteção de dados de iOS** para o Secure Mail e o Secure Web. Por padrão, as políticas estão definidas como **Desativado**.

Quando **Ativar proteção de dados do iOS** estiver **Ativa** para o Secure Web, o Secure Web usa nível de proteção de Classe A para todos os arquivos na área restrita. Para obter detalhes sobre a proteção de dados do Secure Mail, consulte Proteção de dados da Australian Signals Directorate. Se você habilitar esta política, será usada a classe de proteção de dados mais alta, portanto não é necessário especificar a política **Classe de proteção de dados mínima**.

Para alterar a política Ativar proteção de dados de iOS

1. Use o console Endpoint Management para carregar os arquivos MDX do Secure Web e Secure Mail para o Endpoint Management: para um novo aplicativo, navegue até **Configurar > Aplica-**

tivos > Adicionar e clique em **MDX**. Para fazer a atualização, consulte Atualizar aplicativos MDX ou empresariais.

2. No Secure Mail, navegue até as configurações de **Aplicativo**, localize a política **Ativar proteção de dados de iOS** e defina-a como **Ativada**. Os dispositivos que usam versões anteriores do sistema operacional não são afetados quando esta política está ativada.
3. No Secure Web, navegue até as configurações de **Aplicativo**, localize a **política Ativar proteção de dados de iOS** e defina-a como **Ativada**. Os dispositivos que usam versões anteriores do sistema operacional não são afetados quando esta política está ativada.
4. Configure as políticas do aplicativo como faz habitualmente e salve suas configurações para implantar o aplicativo na loja de aplicativos do Endpoint Management.

Proteção de dados da Australian Signals Directorate

O Secure Mail dá suporte à proteção de dados do Australian Signals Directorate para as empresas que precisam atender aos requisitos de segurança de computador da ASD. Como padrão, a política Ativar a proteção de dados do iOS está **Desativada** e o Secure Mail oferece Classe C de proteção ou usa a proteção de dados definida no perfil de provisionamento.

Se a política estiver **Ativada**, o Secure Mail especifica o nível de proteção ao criar e abrir arquivos na área restrita do aplicativo. O Secure Mail define a proteção de dados da Classe A em:

- Itens da caixa de saída
- Fotos da câmera e do rolo de câmera
- Imagens coladas de outros aplicativos
- Anexos de arquivo baixados

O Secure Mail define a proteção de dados da Classe B em:

- Emails armazenados
- Itens de calendário
- Contatos
- Arquivos de política de ActiveSync

A proteção de Classe B permite que um dispositivo bloqueado e possibilita que os downloads sejam concluídos se um dispositivo for bloqueado depois de o download ter iniciado.

Com a proteção de dados ativada, os itens em fila na caixa de saída não são enviados quando um dispositivo está bloqueado porque os arquivos não podem ser abertos. Se o dispositivo for fechado e reiniciar o Secure Mail quando um dispositivo está bloqueado, o Secure Mail não pode sincronizar até que o dispositivo seja desbloqueado e o Secure Mail seja iniciado.

A Citrix recomenda que, se você ativar esta política, deverá ativar o registro em log do Secure Mail somente quando necessário para evitar a criação de arquivos de log com Classe C de proteção de

dados.

Recursos do Android

June 12, 2019

Este artigo aborda os recursos do Android compatíveis com o Secure Mail.

Sincronização automática da pasta Rascunhos

No Secure Mail para Android, a pasta de rascunhos é sincronizada automaticamente e seus rascunhos ficam disponíveis em todos os seus dispositivos.

Esse recurso está disponível em dispositivos com Office 365 ou Exchange Server 2016 e posterior.

> **Nota:**
>
> Se o rascunho do Secure Mail contiver anexos, os anexos não serão sincronizados com o servidor.

O vídeo de um minuto a seguir demonstra como esse recurso funciona:

Gerenciar seus feeds

No Secure Mail para Android, agora você pode organizar o seu cartão **Feed** de acordo com os seus requisitos.

Os aprimoramentos dos feeds incluem as seguintes opções:

- Adicionar até três pastas de e-mail.
- Adicionar cartões para seus colegas e subordinados diretos, ou pastas como VIP e Sinalizadas.
- Busca de cartões ou pastas.
- Reorganizar seus cartões existentes.
- Remover um cartão existente.

Você pode gerenciar seus cartões tocando no botão **Gerenciar Feeds** na exibição de seus **Feeds**.

Alternativamente, você pode tocar na opção **Gerenciar Feeds** em **EMAIL** na sua tela de configurações para gerenciar seus cartões.

Você pode adicionar, reorganizar ou excluir seus cartões de acordo com a sua preferência.

Para adicionar um cartão

1. Toque na guia **Todos os cartões** ou **Todas as pastas**.
2. Toque no ícone **Adicionar** (+) no canto superior direito da tela para selecionar os cartões de sua escolha.
3. Toque em **Concluído**.

Os cartões que você selecionou são adicionados e aparecem em seus feeds.

Para reordenar seus cartões

1. Toque no botão **Gerenciar Feeds**.
2. Nos cartões disponíveis, toque e segure para selecionar um cartão.
3. Mova o cartão para o local desejado.

Para excluir um cartão

1. Toque no botão **Gerenciar Feeds**.
2. Toque no ícone **-** ao lado dos cartões.
3. Toque em **Concluído**.

Os cartões são removidos de seus feeds.

Visualizar anexos

No Secure Mail para Android, visualizar anexos de e-mail e calendário é fácil. O anexo é aberto diretamente no aplicativo ou uma lista de aplicativos compatíveis é exibida. Você pode selecionar o aplicativo necessário para exibir o anexo.

O Secure Mail suporta a visualização de arquivos .txt, arquivos formatados de texto, áudio, vídeo e html, arquivos .zip, imagens, arquivos .eml e formatos de arquivo de contato .vcf.

Pré-requisitos

Assegure que o administrador configure as seguintes políticas de MDX no console Citrix Endpoint Management:

- Política de Troca de documentos (Abrir em) definida como **Irrestrito**.
- Política de Permitir documentos offline definida como **Ilimitado**.

Para obter informações sobre essas políticas, consulte as políticas de MDX em Interação do aplicativo.

Ações ao visualizar anexos

Ao exibir anexos, você pode executar as seguintes ações:

- Selecione uma mensagem existente em suas caixas de correio à qual o arquivo deverá ser anexado.
- Criar uma mensagem à qual anexar o arquivo.
- Salvar um anexo para acesso offline.
- Excluir um anexo de arquivos offline.
- Abrir um anexo usando um aplicativo diferente quando solicitado a fazê-lo .
- Exibir o origem email ou evento de calendário do anexo.

Você pode visualizar anexos:

- Ao exibir mensagem.
- A compor uma nova mensagem.
- Ao encaminhar uma mensagem.

Você também pode visualizar anexos em:

- Pasta **Anexos**.
- Eventos do Calendário.

Anexar arquivos a um email existente ou a um novo email

Você pode anexar arquivos a um email existente ou criar um email para anexar arquivos.

1. Toque na pasta **Anexos** e pressione prolongadamente para selecionar vários anexos ou simplesmente toque em um anexo para selecioná-lo.
2. Toque no ícone **Anexar** na tela. A caixa de correio é exibida.
3. Você pode executar um dos seguintes procedimentos:
    - Para anexar o arquivo a um email existente, selecione uma mensagem existente.
    - Para anexar o arquivo a um novo email, toque em **Nova mensagem**.

Para salvar o anexo para acesso offline

1. Abra o anexo.
2. Toque no ícone **Mais** no canto superior direito da página e em **Salvar para acesso offline**.

Para excluir o anexo dos arquivos offline

1. Abra o anexo.

2. Toque no ícone **Mais** no canto superior direito da página e toque em **Remover dos arquivos offline**.

Para abrir o anexo usando diferentes aplicativos

1. Abra o anexo.
2. Toque no ícone **Mais** no canto superior direito da página e toque em **Abrir com**.
3. Nas opções que aparecem, toque no aplicativo com o qual deseja abrir o anexo.
4. Alternativamente, você pode deslizar para a esquerda para ver a lista de ações que podem ser usadas para exibir ou abrir um anexo.

Para exibir o email ou evento de calendário de origem do anexo

1. Toque no ícone **Anexos** no canto inferior direito da tela.
2. Toque no anexo e, em seguida, toque no ícone **Mais** no canto superior direito da tela.
3. Toque em **Exibir o email original** ou **Exibir o calendário original** para visualizar a origem de um e-mail ou um evento de calendário.

Imprimir e-mails e eventos de calendário

No Secure Mail para Android, você pode imprimir e-mails e eventos de calendário no seu dispositivo Android. Esta funcionalidade de impressão usa o Android Printing Framework.

Pré-requisitos

- Certifique-se de que um administrador definiu a **política Bloquear Impressão** para **Desativada** no console Citrix Endpoint Management. Para obter informações sobre essa política para Android, consulte Política de bloqueio de impressão.
- Se um e-mail estiver protegido pelo IRM, certifique-se de ativar a opção **Permitir que os visualizadores imprimam** no e-mail.

Não é possível imprimir um e-mail ou um evento de calendário se essas políticas estiverem definidas de forma inadequada.

> Nota:
>
> Esse recurso de impressão possui as seguintes limitações conhecidas:
>
> - Imagens incorporadas só serão impressas se você tiver baixado as imagens tocando em

> **Mostrar imagens**. Se você não tocar em **Mostrar imagens**, apenas os espaços reservados das imagens serão impressos.
> - No Secure Mail, os emails de tamanho grande são truncados. Antes de imprimir, toque em **Baixar mensagem completa** para imprimir o e-mail completo. Se a mensagem completa não for baixada, um email truncado será impresso.
> - Nenhum metadado de um email ou evento é adicionado durante a impressão desses itens.

Para imprimir um email

1. Abra o email que você deseja imprimir.
2. Toque no ícone Mais no canto superior esquerdo da tela. São exibidas as seguintes opções:
    - Mover
    - Imprimir

> Nota:
>
> Nos tablets, você pode usar diretamente o ícone de impressão no canto superior esquerdo da tela para imprimir um e-mail.

1. Toque em **Imprimir**. Uma visualização do seu e-mail é exibida.
2. Toque na lista e as seguintes opções serão exibidas:
    - Salvar como PDF
    - Todas as impressoras
3. Toque em **Salvar como PDF** para salvar seu e-mail em um formato PDF.
4. Toque em **Todas as impressoras**. Instale a impressora conforme sua necessidade.
5. Quando a impressora estiver instalada, toque em **Selecionar impressora** para selecionar uma impressora. É exibida a tela **Impressora**.

    > Nota:
    >
    > As opções de impressão variam de acordo com a impressora selecionada. A imagem a seguir é de uma impressora Canon E480 e é usada apenas para fins de representação.

6. Selecione a impressora em que você deseja imprimir. Use as seguintes opções de impressão:
    - Insira manualmente o número de cópias que você deseja imprimir.
    - Selecione o tamanho do papel na lista.
    - Selecione a cor na lista.
    - Escolha a orientação da página conforme necessário.
    - Selecione uma página ou um intervalo de páginas e insira manualmente o intervalo de páginas.

7. Depois de configurar as opções de impressão, toque no ícone Imprimir na tela.

Para imprimir uma imagem incorporada

- Toque em **Mostrar imagens** no email e siga as instruções mencionadas na seção anterior Para imprimir um email.

Imprimir um evento de calendário

1. Navegue até o calendário e toque em um evento.
2. Toque no ícone Imprimir e siga as mesmas instruções como mencionado na seção anterior Para imprimir um email.

Denunciar e-mails de phishing com cabeçalhos do ActiveSync

No Secure Mail para Android, quando um usuário denuncia um e-mail de phishing, um arquivo EML é gerado como um anexo correspondente a esse e-mail. Os administradores recebem esse e-mail e podem ver os cabeçalhos do ActiveSync associados ao e-mail denunciado.

Para ativar esse recurso, um administrador deve configurar a política Denunciar endereço de email de phishing e definir Denunciar mecanismo de phishing como **Denunciar por anexo** no console Citrix Endpoint Management. Para obter detalhes, consulte Denunciar email de phishing (como anexo).

Notificações de subpastas

No Secure Mail para Android, você pode receber notificações por email de subpastas de sua conta de email.

> Nota:
>
> - Certifique-se de que a notificação por push baseada no FCM esteja ativada no console do Endpoint Management para receber notificações de subpastas. Para ver as etapas de configuração de notificações por push baseadas em FCM, consulte Notificações por Push para o Secure Mail.
> - O recurso de notificação de subpasta não está disponível para o Lotus Notes Server.

Para habilitar notificações para subpastas

1. Vá até **Configurações** e, em **Geral**, toque em **Notificações**.

2. Na tela **Notificações**, toque em **Pastas de correio**. Uma lista de subpastas na caixa de entrada é exibida.
3. Toque para selecionar as subpastas das quais você deseja receber notificações. Caixa de Entrada é selecionada por padrão.

> **Nota:**
>
> Ativar notificações para subpastas ativa a sincronização automática.

Para desabilitar as notificações da subpasta, desmarque a caixa de seleção das subpastas das quais você não deseja receber notificações.

Canais de notificação

Nos dispositivos que executam o Android O ou posterior, você pode usar as configurações do canal de notificações para gerenciar como suas notificações de email e calendário são tratadas. Esse recurso permite personalizar e gerenciar suas notificações.

Para configurar notificações para lembretes de email ou calendário, abra o Secure Mail e navegue até **Configurações > Notificações** e selecione a opção de notificação desejada.

Você pode então navegar para **Gerenciar as notificações de email** ou **Gerenciar as notificações de calendário** para gerenciar suas notificações de email ou calendário, respectivamente.

Como alternativa, você pode pressionar prolongadamente o ícone do aplicativo Secure Mail no seu dispositivo, selecionar **Informações do aplicativo** e depois tocar em **Notificações**.

Se a sua configuração Vibrar foi previamente definida como **Apenas no modo silencioso**, ela mudará para a configuração padrão de vibração **Desativada** com esse recurso.

> Nota:
>
> As notificações na tela de bloqueio estão disponíveis com base em como seu administrador configurou a política MDX Controlar notificações de tela de bloqueio.

Anexar arquivos em Android

No Secure Mail versões 10.3.5 e posteriores, os usuários não podem anexar imagens diretamente do aplicativo Galeria se a política Troca de documentos de entrada (Abrir em) está definida como **Restrita**. Se você quiser manter esta política definida como **Restrita**, mas permitir que os usuários adicionem fotos da Galeria, siga estes procedimentos no console Endpoint Management.

1. Defina **Bloquear galeria** como **Desativado**.
2. Obtenha o ID de pacote da Galeria para dispositivos. Alguns exemplos:

- **LG Nexus 5:**
  com.google.android.gallery3d, com.google.android.apps.photos
- **Samsung Galaxy Note 3:**
  com.sec.android.gallery3d, com.sec.android.gallery3d.panorama360view, com.google.android.apps.
- **Sony Expire:**
  com.sonyericsson.album, com.google.android.apps.photos
- **HTC:**
  com.google.android.apps.photos, com.htc.album
- **Huawei:**
  com.android.gallery3d, com.google.android.apps.photos

3. Deixe visível a política oculta InboundDocumentExchangeWhitelist:
   - Baixe o arquivo APK do WorxMail e prepare o arquivo com o MDX Toolkit.
   - Localize o arquivo .mdx no computador e altere o sufixo do arquivo para .zip.
   - Abra o arquivo .zip e localize o arquivo policy_metadata.xml
   - Procure e atere InboundDocumentExchangeWhitelist de `PolicyHidden>**true**</PolicyHidden>` para `<PolicyHidden>**false**</PolicyHidden>`.
   - Salve a política policy_metadata.xml.
   - Selecione todos os arquivos na pasta e compacte-os para criar o arquivo .zip.

     > **Nota:**
     >
     > Não compacte a pasta externa. Selecione todos os arquivos dentro da pasta e compacte os arquivos selecionados.

   - Clique no arquivo compactado resultante.
   - Escolha **Get Info** e mude o sufixo de volta para .mdx.
4. Carregue o arquivo .mdx modificado no console Endpoint Management e adicione a lista de IDs de pacote da Galeria à política Lista branca de troca de documentos recebidos, agora visível.

   As IDs de pacote devem ser separados por vírgula:

   com.sec.android.gallery3d, com.sec.android.gallery3d.panorama360view, com.google.android.apps.photo
5. Salve e implante de Secure Mail.

Os usuários do Android agora podem anexar uma imagem do aplicativo Galeria.

Formatos de arquivo com suporte

Um X indica um formato de arquivo que pode ser anexado, exibido e aberto no Secure Mail.

Formato	iOS	Android
Vídeo: H.263 AMR NB codec_Mp4		X
Vídeo: H.263 AMR NB codec_3gp		X
Vídeo: H.264 AAC codec_3gp	X	X
Vídeo: H.264 AAC codec_mp4	X	X
Vídeo: H.264 Acclc codec_mp4	X	X
GTM recorded_wmv		X
AVI		X
WAV	X	X
MP4	X	X
3GP	X	X
Flac		X
AAC	X	X
M4A	X	X
3GP (AMR-NB)	X	X
MP3	X	X
WAV	X	X
OGG		X
ICO	X	X
JPEG	X	X
PNG	X	X
TIF (apenas de uma página)	X	
BMP	X	X
GIF	X	X
WebP		X
.dot	X	X
PDF	X	
PPT	X	X

Formato	iOS	Android
PPTX	X	X
DOC	X	X
DOCX	X	X
XLS	X	X
XLSM	X	X
XLSX	X	X
TXT	X	X
POT	X	X
HTM	X	X
HTML	X	X
ZIP	X	X
EML	X	X

Várias contas do Exchange para Android

Em **Configurações**, no Secure Mail, você agora pode adicionar várias contas de email do Exchange e alternar entre elas. Este recurso permite monitorar todos os seus emails, contatos e calendários em um local.

Pré-requisitos

É necessário um nome de usuário e a senha para configurar mais contas. Configurações de armazenamento de registro ou credenciais automáticas se aplica somente a primeira configuração de conta no aplicativo. Digite o nome de usuário e senha para todas as contas adicionais.

- Se a primeira conta que você criar for baseada em certificado, você não poderá adicionar mais contas baseadas em certificado.
- Para permitir que mais contas se conectem a um domínio ou ao Exchange Server em uma rede externa, você deve definir o túnel dividido como **ON** no Citrix DC.
- O Secure Mail para iOS oferece suporte somente a servidores de correio Exchange e Office 365.

Para adicionar uma conta de email para Android

1. Abra o Secure Mail, toque no ícone do hambúrguer e depois no ícone de **Configurações**.

2. Em **Contas**, toque em **Adicionar conta**.
3. Na tela **Adicionar conta**, digite as credenciais para a nova conta.

   Opcionalmente, você pode definir os valores para os seguintes parâmetros:

   - **Período de sincronização de email:** Toque para selecionar um valor para o período de sincronização. O valor definido especifica o número de dias de email para o Secure Mail sincronizar. O administrador define o valor padrão.
   - **Tornar esta a conta padrão:** Toque para definir a nova conta como a sua conta padrão. Essa opção é definida como **OFF** por padrão.
4. Toque em **Fazer logon** para criar a conta.

   Você pode ver a nova conta na tela **Configurações** no menu **Contas**.

> **Nota:**
>
> Contas adicionais devem usar a autenticação com base no Active Directory. O Secure Mail não oferece suporte a autenticação baseada em certificado quando são configuradas várias contas.

Para editar uma conta

Você pode editar a senha e a descrição da conta de email para Android.

1. Abra o Secure Mail, toque no ícone do hambúrguer e depois no ícone de **Configurações**.
2. Em **Contas**, toque na conta que você deseja editar.
3. Na tela **Conta**, edite os campos.
4. Toque em **Salvar** para confirmar sua ação ou toque em **Cancelar** para retornar para a tela de **Configurações**.

Para excluir uma conta do Android

1. Abra o Secure Mail, toque no ícone do hambúrguer e depois no ícone de **Configurações**.
2. Em **Contas**, toque na conta que você deseja excluir.
3. Na tela de detalhes de **Conta**, toque em **Excluir conta** na parte inferior da tela ou toque em **Cancelar** para retornar para a tela de **Configurações**.
4. Toque em **EXCLUIR** para confirmar a ação.

> Nota:
>
> Se você excluir a conta padrão, a próxima conta se tornará a conta padrão.

Para definir uma conta padrão para o Android

O Secure Mail usa a conta padrão nas seguintes situações:

- **Composição de emails:** O campo **De:** é preenchido automaticamente com a ID de email da conta padrão.
- **Criação de eventos de calendário:** O campo **Organizador** é preenchido automaticamente com a ID de email da conta padrão.

Quando você adiciona uma ou mais contas de email, a primeira conta criada é a conta padrão. Para alterar a conta padrão, navegue até **Configurações** e, em seguida, toque em **Padrão** sob **Geral**.

Na tela **Conta padrão**, toque na conta que você deseja definir como padrão.

Configurações para várias contas do Exchange para Android

Se você tiver configurado várias contas do Exchange, algumas das configurações do Secure Mail estão disponíveis para cada uma dessas contas individualmente, enquanto que as outras configurações são globais. As seguintes configurações são específicas de conta:

- Padrão
- Notificações
- Ausência Temporária
- Frequência de sincronização da caixa de entrada
- Período de sincronização
- Sincronizar o email
- S/MIME
- Arquivos offline
- Assinatura
- Respostas rápidas
- Sincronizar o calendário
- Sincronizar os contatos
- Sinc. com contatos locais
- Exportar configurações

Essas configurações são exibidas com o ícone >. Toque no ícone > para exibir as contas no seu dispositivo.

Para aplicar a configuração de uma conta específica, expanda um item de configuração tocando em **>** e, em seguida, selecione a conta de email.

Tela de caixas de correio

A tela **Caixas de correio** exibe todas as contas que você configurou e tem os seguintes modos de exibição:

- **Todas as contas:** Contém emails de todas as contas do Exchange que você tiver configurado.
- **Contas individuais:** Contém emails e pastas de uma conta individual. Estas contas são exibidas como uma lista que você pode expandir para exibir as subpastas.

Para visualizar suas caixas de correio, abra o Secure Mail e toque no ícone de hambúrguer. Na tela **Caixas de correio**, toque na conta para expandir as opções.

A exibição **Todas as contas** mostra os seus emails de várias contas coletivamente, e as seguintes ações usam o endereço de email da conta primária ou padrão:

- Nova mensagem
- Novo evento

Para alterar o endereço de email do remetente ao redigir um novo email no modo de exibição **Todas as contas**, toque no endereço padrão no campo **De:** e selecione uma conta diferente das contas de email que aparecem.

> Nota:
>
> Redigir um email no modo de exibição de conversa preenche o campo **De:** automaticamente com o endereço de email à qual a conversa está endereçada.

Contas individuais

A conta padrão ou primária sempre é exibida em primeiro lugar seguida por outras contas em ordem alfabética.

As contas individuais exibem todas as subpastas que você tiver criado.

As seguintes ações são limitadas a contas individuais apenas:

- Mover itens.
- Redação de emails na exibição de conversa.
- Gravação de contatos.

Contatos

Toque no ícone **Contatos** na barra da guia e toque no ícone de hambúrguer no canto superior direito da tela. A tela **Contatos** exibe os itens a seguir:

- **Todos os contatos:** Exibe todos os contatos de várias contas de email. Essa opção só aparece se várias contas de email estiverem configuradas.
- **Conta de e-mail individual:** Exibe os contatos pertencentes à conta de e-mail individual configurada.
- **Categorias:** Exibe as categorias de contato que você pode ter criado ou selecionado na lista predefinida para agrupar contatos.

Para exibir a pasta do contato

> Nota:
>
> Não há suporte para subpastas de contato no Secure Mail para Android. Se tiver criado pastas ou subpastas para seus contatos usando o Microsoft Outlook, você não poderá exibi-los no Secure Mail.

1. Na tela de contatos:
    - Toque em todos os contatos para ver todos os contatos de várias contas de e-mail.
    - Toque na conta de e-mail individual para ver os contatos associados a uma conta de e-mail específica.
2. Toque nas categorias para ver os contatos agrupados em categorias específicas. Você pode optar por agrupar contatos com base em uma categoria criada ou agrupá-los em uma categoria de uma lista predefinida.

Você pode sincronizar contatos pertencentes a uma conta individual com seus contatos locais.

Para sincronizar com contatos locais

1. Abra o Secure Mail.
2. Toque no ícone Configurações e navegue até **Contatos > Sincronizar com contatos locais** e toque em > para expandir o menu.
3. Na tela **Sincronizar os contatos locais**, ative a conta cujos contatos você deseja sincronizar.
4. Toque em **OK**.
5. Quando solicitado para permitir que o Secure Mail tenha acesso aos contatos, toque em **OK**.

Agora você exportou contatos da conta com êxito.
Para desfazer essa ação, vá até **Configurações > Contatos > Sincronizar com os contatos locais** e, em seguida, toque no comutador ao lado da conta para desativar esse recurso. Toque em **OK** para confirmar a ação.

Calendário

O calendário exibe todos os eventos relacionados a várias contas no seu dispositivo. Você pode atribuir cores para contas individuais para diferenciar eventos de calendários relacionado a contas individuais.

> Nota:
>
> Se ativado, o recurso de calendário pessoal sempre será associado à sua conta primária ou padrão.

Para atribuir cores a eventos de calendário

1. Toque no ícone **Calendário** na barra de rodapé e toque no ícone de hambúrguer no canto superior esquerdo.
   A tela **Calendários** exibe todas as contas que você tiver configurado.
2. Toque na cor padrão exibida à direita de uma conta do Exchange.
   A tela cores o exibe as cores disponíveis para aquela conta.
3. Selecione uma cor de sua escolha e, em seguida, toque em **Salvar**.
4. Para retornar à tela anterior, toque em **Cancelar**.
   A cor selecionada é definida para todos os eventos de calendário pertencentes a essa conta do Exchange.

Quando você cria um convite ou evento de calendário, o campo **Organizador** é preenchido automaticamente com o endereço de email da conta padrão. Para alterar a conta de email, toque neste endereço de email e selecione outra conta.

Pesquisa

Você pode realizar uma pesquisa global no modo de exibição **Caixas de correio** ou **Todos os contatos**. Esta ação exibe os resultados apropriados após a pesquisa todas as contas no aplicativo.

Todas as pesquisas realizadas dentro de uma conta individual exibem resultados referentes somente a essa conta.

Android Enterprise no Secure Mail

O Secure Mail e Secure Web para Android são compatíveis com o Android Enterprise, conhecido anteriormente como Android for Work.

Pré-requisitos

- Para poder usar esse recurso, seu dispositivo deve ter o Android 5.0 ou versões posteriores.
- Para implantações no local, a propriedade **afw.accounts** do Endpoint Management deve ser definida como **TRUE**.

Depois que você tiver configurado o Android Enterprise no Endpoint Management, os aplicativos móveis de produtividade estarão disponíveis no seu dispositivo. O ícone do Android Enterprise identifica o aplicativo, como realçado na imagem a seguir.

Recursos que são compatíveis com o Android Enterprise

A tabela a seguir lista os recursos do Secure Mail que são compatíveis com o Android Enterprise.

Recurso	Suporte
Descoberta automática do Exchange Server	X
Secure Ticket Authority (STA)	X
Exportar contatos	X
Gerenciamento de Direitos de Informação da Microsoft	X
Notificações de bloqueio de tela	X
Sincronização de email	X
Classificação de email	X
Assinatura e criptografia S/MIME de assinatura	X
Serviço Firebase Cloud Messaging (FCM)	X
Autenticação moderna (OAuth)	
Várias contas do Exchange	X
Calendário pessoal	
Exportar configurações de email	X
Dispositivos compartilhados	
Endpoint Management integration with Microsoft Intune/EMS	
Office 365	X
LDAP Exchange Server 2010, 2013 e 2016	X
Autenticação baseada em certificados (CBA)	

Recurso	Suporte
GoToMeeting	X
Skype for Business	
Lista de distribuição pessoal	X
Compatibilidade com Citrix Files	X
Registro de email com o logon único	X

A tabela a seguir lista os recursos do Secure Web que são compatíveis com o Android Enterprise.

Recurso	Suporte
Modo Secure Browse	X
Modo VPN completo	X
Todos os recursos do aplicativo	X
Compatibilidade com o Secure Mail	X

Limitações

- Se a política de restrições de dispositivo **Permitir uso da barra de status** estiver **Ativada** para Android Enterprise no modo de perfil de trabalho, o progresso da exportação do calendário e as notificações por push no Secure Mail para Android não serão exibidos na barra de status. No entanto, essas notificações são vistas na tela bloqueada quando permitido. Para obter mais informações, consulte Configurações do Android Enterprise.

Integração do Secure Mail com Slack (visualização)

April 5, 2019

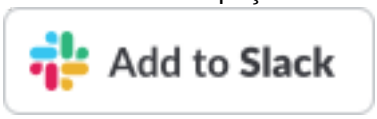
Agora você pode levar sua conversa por e-mail para o aplicativo Slack em dispositivos com iOS ou Android.

Depois de ativar esse recurso, você pode:

- Alternar livremente do email para uma conversa do Slack.
- Criar uma conversa em grupo no Slack com os seus destinatários de email.

- Criar uma mensagem diretamente no Slack com o seu destinatário de email.

Pré-requisitos

- Para administradores:
  - instalar o Secure Mail em seu espaço de trabalho do Slack. Clique no botão **Adicionar ao Slack** abaixo. 

  - Garantir que a política **Ativar Slack** esteja **Ativada**. Para detalhes da política, consulte:
    * Ativar a política do Slack para iOS
    * Ativar a política do Slack para Android
- Para usuários: ter uma conta do Slack e o aplicativo Slack instalado no seu dispositivo.

Para ativar esse recurso no seu dispositivo

1. Abra o Secure Mail e toque no ícone de hambúrguer.
2. Na tela **Caixas de correio**, toque no ícone de configurações na parte inferior direita da tela.
3. Na tela **Configurações**, toque em **Slack**, em **Integrações**.
4. Forneça sua URL de espaço de trabalho e toque em **Continuar**.
5. Forneça suas credenciais e toque em **Fazer logon**.
6. Quando solicitado a autorizar o acesso do Secure Mail às informações, toque em **Autorizar**.

Agora você está conectado ao Slack.

Para usar este recurso

1. Abra qualquer conversa de email no Secure Mail e, em seguida, toque no botão de ação flutuante.
2. Nas opções disponíveis, toque em **Chat no Slack**.
3. A conversa muda para o Slack com os destinatários em seu email.

Tenha em mente o seguinte:

- Nos dispositivos que executam o Secure Mail para iOS ou Android, você pode criar uma conversa do Slack com no máximo oito destinatários do seu email. Se você tiver mais de oito destinatários em seu email, por padrão, o Secure Mail seleciona os oito primeiros destinatários presentes em sua conversa por email.

Notificações e sincronização

June 12, 2019

Este artigo discute sobre a funcionalidade e as configurações de notificação e sincronização de email para o Secure Mail.

Secure Mail para atualização de aplicativos iOS em segundo plano

Se o Secure Mail para iOS estiver configurado para fornecer notificações por meio de atualização de aplicativo iOS em segundo plano (e não APNs), a atualização de email do Secure Mail funciona da seguinte maneira:

- Quando os usuários ativam a **Atualização de aplicativo em segundo plano** no dispositivo usando o menu **Configurações**, e o Secure Mail está em execução em segundo plano, o correio é sincronizado com o servidor. A frequência de sincronização depende de vários fatores.
- Se o usuário desativa **Atualização de aplicativo em segundo plano** o aplicativo nunca recebe emails durante a execução em segundo plano.
- Quando os usuários movem o Secure Mail para o segundo plano, o aplicativo continua a ser executado por um período de tolerância, antes que o aplicativo seja suspenso.
- Ao ser executado em primeiro plano, o Secure Mail mostra a atividade de email em tempo real, independentemente da configuração **Atualização de aplicativo em segundo plano**.

Secure Mail e ActiveSync

O Secure Mail sincroniza com o Exchange Server por meio do protocolo de mensagens do ActiveSync. Essa funcionalidade oferece aos usuários acesso em tempo real aos seus emails do Outlook, contatos, eventos do calendário, caixas de correio geradas automaticamente e pastas criadas pelo usuário.

> **Nota:**
>
> O ActiveSync não dá suporte à sincronização de pastas públicas do Exchange. No Exchange Server 2013, o ActiveSync não sincroniza a pasta Rascunhos.

Para sincronizar pastas criadas pelo usuário, siga estas etapas:

iOS

1. Vá para **Configurações > Atualização automática**.
2. Defina **Atualização automática** como **Ativada**.
3. Toque em **Ativada**. É exibida uma lista de todas as caixas de correio.

4. Toque nas pastas que deseja sincronizar.

Android

1. Vá para a lista de caixas de correio.
2. Toque na caixa de correio que você deseja sincronizar.
3. Toque no ícone de Mais no canto superior direito.
4. Toque em **Opções de sincronização**.
5. Em **Frequência de verificação**, selecione a frequência com que a pasta deve ser sincronizada.

Exportação de contatos no Secure Mail

Os usuários do Secure Mail podem sincronizar continuamente os seus contatos com o catálogo telefônico do telefone, fazer uma exportação de um determinado contato para catálogo de endereços do telefone ou compartilhar um contato como um anexo de vCard.

Para permitir esses recursos, defina a política Export Contacts para Secure Mail no console Endpoint Managementcomo **ON**.

Quando a política está definida como **I**, as seguintes opções são ativadas no Secure Mail:

- **Sync with Local Contacts** nas configurações
- Exportação de contatos
- Compartilhar contatos como anexos de vCard

Quando a política Export Contacts está **OFF**, essas opções não aparecem no aplicativo.

Quando a política está ativada, para sincronizar contatos continuamente do servidor de email para o catálogo de endereços do telefone, os usuários precisam definir **Sync with Local Contacts** como **ON**. Desde que **Sync with Local Contacts** estiver definido como **I**, as atualizações a contatos no Exchange ou Secure Mail provocam uma atualização dos contatos locais.

Por causa das limitações do Android, se alguma conta do Exchange ou Hotmail já estiver definida para sincronização com outros contatos locais, o Secure Mail não consegue sincronizar contatos.

No iOS, os contatos do Secure Mail podem ser exportados e sincronizados com os contatos do telefone, mesmo se os usuários tiverem o Hotmail ou Exchange configurados no dispositivo. Você pode configurar este recurso no Endpoint Management por meio da política Override Native Contacts Check do Secure Mail. Esta política determina se o Secure Mail deve substituir a verificação de contatos de uma conta do Exchange/Hotmail configurado no aplicativo nativo de contatos. Se o valor for **Ativado**, o aplicativo sincroniza contatos no dispositivo, mesmo se o aplicativo nativo de contatos está configurado com a conta do Exchange/Hotmail. Se o valor for **Desativado**, o aplicativo continua a bloquear a sincronização de contatos. O padrão é **Ativado**.

Notificações do Secure Mail

A tabela a seguir contém um resumo de como as notificações são processadas para dispositivos móveis com suporte quando o Secure Mail está sendo executado em primeiro ou em segundo plano.

Com o Secure Mail em execução no primeiro ou segundo plano:	Notificações são manipuladas para o iOS	Notificações são manipuladas para o Android
Primeiro plano	O Secure Mail mantém uma conexão ActiveSync persistente para sincronizar email e atividades do calendário.	O Secure Mail mantém uma conexão ActiveSync persistente para sincronizar email e atividades do calendário.
Segundo plano (ou finalizado)	O Secure Mail recebe notificações por meio da funcionalidade de atualização de aplicativo iOS ou, se configurado, APNs.	O Secure Mail mantém uma conexão ActiveSync persistente.

Para ver detalhes de configuração, consulte Notificações por Push para o Secure Mail para iOS.

Notificações por push em rich text

O Secure Mail dá suporte a notificações por push em rich text. As notificações em rich text garantem que você receba notificações da tela de bloqueio para sua caixa de entrada, mesmo quando o Secure Mail não estiver sendo executado em segundo plano. Este recurso tem suporte em configurações de autenticação baseada em senha e autenticação baseada em cliente.

> **Nota:**
>
> Devido à mudança na arquitetura para suportar esse recurso, o recurso de Notificações de e-mail Apenas VIP não está mais disponível.

Para ativar o recurso de notificações por push em rich text, certifique-se de que os seguintes pré-requisitos sejam atendidos:

- No console Endpoint Management, configure as notificações por push como **ON**.
- A política de acesso à rede está definida como **Irrestrita** ou **Com túnel para a rede interna**. Se a política de acesso à rede estiver definida como **Com túnel para a rede interna**, verifique se o host dos Serviços Web do Exchange (EWS) está configurado na política de serviços de rede em

segundo plano. Se os hosts do EWS e do ActiveSync forem os mesmos, verifique se o host do ActiveSync está configurado na política de serviços de rede em segundo plano.
- A política Controlar notificações de tela de bloqueio está definida como **Permitir** ou **Remetente do email ou título do evento**.
- Navegue até **Secure Mail > Configurações> Notificações** e ative **Notificações por email**.

Este recurso não é suportado se você estiver executando alguma das seguintes configurações:

- Autenticação moderna com o Microsoft Office 365 (Oauth)
- Aplicativos gerenciados pela integração do Endpoint Management com o Microsoft InTune/EMS
- Dispositivos registrados por meio de credenciais derivadas

Razões para a notificação “Você tem novo email” exibida nos dispositivos iOS

A notificação “Você tem novo e-mail” aparece em dispositivos iOS quando o Secure Mail não recebe uma resposta do EWS (Serviços Web do Exchange) no tempo especificado de 30 segundos, necessário para buscar os detalhes da mensagem.

Você também pode ver esse comportamento em seu dispositivo com base em conectividade deficiente de Wi-Fi ou de dados.

Além da resposta de atraso do EWS, o Secure Mail também exibe a notificação “Você tem novo email” nas seguintes situações:

- Quando o Secure Mail não consegue ler as informações necessárias do contêiner seguro. Esse cenário geralmente ocorre após você reiniciar o dispositivo e antes de desbloquear o dispositivo.
- Quando o Secure Mail não consegue se conectar ou configurar um canal seguro com o Citrix Gateway ou o EWS.
- Quando suas credenciais expirarem ou você tiver modificado as credenciais, mas elas ainda não estiverem atualizadas no Secure Mail. A figura a seguir mostra a maneira como a notificação aparece neste cenário.
- Quando o Secure Mail recebe uma resposta inesperada do servidor Exchange para uma solicitação válida do Secure Mail. Para obter detalhes sobre os códigos de resposta do EWS, consulte a documentação do desenvolvedor da Microsoft.

Enviar mensagens de falha de notificação por push no Secure Mail para iOS

No Secure Mail para iOS, mensagens de falha de notificação por push apropriadas são exibidas na central de notificações do dispositivo. Essas notificações aparecem com base no tipo de falha de notificação.

As seguintes mensagens de notificação aparecem com base em diferentes cenários de falha, da seguinte maneira:

- **O Secure Mail não consegue se conectar à rede da sua organização.** Essa notificação aparece quando o Secure Mail não consegue estabelecer uma conexão SOCKS5 com o Citrix Gateway.
- **O Secure Mail não consegue se conectar à rede da sua organização. Entre em contato com seu administrador.** Esta notificação aparece quando o Citrix Gateway está inacessível. Assegure-se de que seu Citrix ADC esteja configurado corretamente e esteja acessível a partir de redes externas.
- **O Secure Mail não consegue se conectar com segurança à rede da sua organização. Entre em contato com seu administrador**. Essa notificação aparece quando o Secure Mail não consegue estabelecer uma conexão SSL com o Citrix Gateway. Certifique-se de que o seu certificado SSL seja válido.
- **O Secure Mail não consegue se conectar com segurança ao seu servidor de e-mail. Entre em contato com seu administrador**. Essa notificação aparece quando o Secure Mail não consegue estabelecer uma conexão SSL com o Exchange Server. Certifique-se de que o certificado SSL no seu Exchange Server seja válido. Se você quiser que o aplicativo se conecte ao Exchange Server apesar de ter um certificado inválido, verifique se você ativou a política MDX Aceitar todos os certificados SSL.
- **O Secure Mail não consegue obter a mensagem devido a um erro no servidor de email. Entre em contato com seu administrador**. Essa notificação aparece quando o Secure Mail não consegue analisar a resposta de EWS do Exchange Server.
- **O Secure Mail não consegue obter a mensagem devido a um tempo limite de solicitação**. Essa notificação aparece quando o Secure Mail não recebe uma resposta do servidor dentro de 30 segundos. Essa notificação pode aparecer devido a dados deficientes ou conexão Wi-Fi no seu dispositivo. Tente novamente depois de esperar alguns minutos.
- **Não é possível obter a mensagem. Abra o Secure Mail**. Essa notificação aparece quando o Secure Mail não consegue ler suas credenciais do contêiner seguro. Essa notificação pode aparecer quando o dispositivo tiver sido reiniciado, mas ainda não estiver desbloqueado. Desbloqueie seu dispositivo para permitir automaticamente o acesso do Secure Mail ao contêiner seguro. Se você ainda estiver recebendo essa notificação, abra o Secure Mail para atualizar automaticamente suas credenciais no contêiner seguro.

Notificações por Push para o Secure Mail

June 12, 2019

O Secure Mail para iOS e o Secure Mail para Android pode receber notificações sobre email e atividades de calendário quando o aplicativo está sendo executado em segundo plano ou está fechado. O Secure Mail para iOS oferece suporte a notificações fornecidas através de atualização de aplicativo em segundo plano ou notificações por push fornecidas através do serviço Apple Push Notification (APNs). O Secure Mail para Android oferece suporte a notificações fornecidas através do serviço Firebase Cloud Messaging (FCM).

Como funcionam as notificações por push

O Secure Mail envia notificações por push para as seguintes atividades da Caixa de entrada:

- **Novo email, solicitações de reuniões, cancelamentos de reuniões, atualizações de reuniões:** Quando o APNs envia notificações para uma caixa de entrada, o Secure Mail atualiza todas as pastas, incluindo o Calendário, de modo que as alterações de reuniões sejam refletidas imediatamente nos calendários dos usuários.
- **Para iOS, o status do Secure Mail muda de lido para não lido e vice-versa.** O ícone do Secure Mail mostra o número de mensagens não lidas e novas na caixa de entrada do Exchange apenas. O ícone do Secure Mail é atualizado depois que os usuários leem os emails em um computador desktop ou laptop.

  Para iOS, o Secure Mail ainda fornece a contagem de emails não lidos da caixa de entrada do período de sincronização. Se a política Controlar notificações de tela de bloqueio está **Ativada**, as notificações por push aparecem na tela de um dispositivo bloqueado depois que o iOS desperta o Secure Mail para executar uma sincronização.

  Durante uma instalação ou atualização, o Secure Mail para iOS avisa aos usuários para que permitam notificações por push. Os usuários também podem permitir notificações por push mais tarde usando as configurações do iOS.

Para fornecer notificações por push para iOS e Android, a Citrix hospeda um serviço de ouvinte no Amazon Web Services (AWS) para executar as seguintes funções:

- Escutar notificações por push de Serviços Web do Exchange (EWS) enviadas por servidores Exchange quando há atividade na caixa de entrada. O Exchange não envia nenhum conteúdo de email para o serviço Citrix.

  Nenhuma informação pessoalmente identificável é armazenada pelo serviço da Citrix. Em vez disso, um token de dispositivo e ID de assinatura identifica o dispositivo específico e pasta de caixa de entrada para ser atualizada dentro do Secure Mail.
- Enviar notificações de APNs, que contêm apenas contagem de indicador de contagem para o Secure Mail em dispositivos iOS.
- Enviar notificações de FCM para o Secure Mail em dispositivos Android.

O serviço de ouvinte da Citrix não prejudica o tráfego de dados de email, que continua a fluir entre dispositivos do usuários e servidores do Exchange por meio do ActiveSync. O serviço de ouvinte, que está configurado para alta disponibilidade e recuperação de desastres, está disponível em três regiões:

- Américas
- Europa, Oriente Médio e África (EMEA)
- Ásia-Pacífico (APAC)

Requisitos do sistema para notificações por push

Caso a sua configuração do Citrix Gateway inclua o Secure Ticket Authority (STA) e o túnel dividido estiver desativado, o Citrix Gateway deve permitir o tráfego (quando encapsulado a partir do Secure Mail) para as seguintes URLs do serviço de ouvinte Citrix:

Região	URL	Endereço IP
Américas	`https://us-east-1.pushreg.xm.citrix.com`	52.7.65.6; 52.7.147.0
EMEA	`https://eu-west-1.pushreg.xm.citrix.com`	54.154.200.233; 54.154.204.192
ÁSIA-PACÍFICO	`https://ap-southeast-1.pushreg.xm.citrix.com`	52.74.236.173; 52.74.25.245

Configuração de Secure Mail para notificações por push

Para configurar notificações por Push da Apple ou FCM para o Secure Mail para distribuição em loja de aplicativos, no console Endpoint Management, defina notificações por Push como **Ativado** e, em seguida, selecione a sua região. A seguinte figura apresenta a configuração para iOS.

Para o Android, a figura a seguir mostra a mesma **configuração de notificação por push** que para o iOS. Além disso, se o EWS estiver hospedado em uma região diferente daquela em que o servidor de email está localizado, defina a configuração de **Nome de host do EWS**. A configuração padrão é vazia. Se você deixar a configuração vazia, o Endpoint Management usará o nome do host do servidor de email.

Configure o Exchange e o Citrix ADC para permitir que o tráfego flua para o serviço de ouvinte.

Configuração do Exchange Server

Permita SSL de saída (pela porta 443) do firewall para o URL do serviço de ouvinte para a região onde o seu Exchange Server está localizado. Por exemplo:

Região	URL	Endereço IP
Américas	https://us-east-1.mailboxlistener.xm.citrix.com	52.6.252.176; 52.4.180.132
EMEA	https://eu-west-1.mailboxlistener.xm.citrix.com	54.77.174.172; 52.17.147.220
ÁSIA-PACÍFICO	https://ap-southeast-1.mailboxlistener.xm.citrix.com	52.74.231.240; 54.169.87.20

Se você tiver um servidor proxy entre Serviços Web do Exchange (EWS) e o dispositivo ouvinte da Citrix, você pode optar por uma das seguintes possibilidades.

- Envie tráfego EWS pelo proxy e, em seguida, para o dispositivo ouvinte.
- Ignore o proxy e roteie o tráfego EWS para o dispositivo ouvinte diretamente.

Para enviar tráfego de EWS através do servidor proxy, configure o arquivo EWS web.config na pasta ClientAccess\exchweb\ews folder, como indicado a seguir.

```
<configuration>
<system.net>
<defaultProxy>
<proxy usesystemdefault=”true” bypassonlocal=”true” />
</defaultProxy>
</system.net>
</configuration>
```

Para obter mais detalhes sobre como configurar proxies, consulte Configuração de proxy.

Para ambientes do Exchange 2013, você deve adicionar a seção `system.net` ao arquivo web.config manualmente. Caso contrário, as configurações descritas neste artigo devem funcionar para Exchange 2013. Para solução de problemas, entre em contato com o administrador do Exchange.

Para ignorar o servidor proxy, configure a lista de ignorar para que permita conexões ao serviço de ouvinte da Citrix.

Quando o Secure Hub é registrado com a autenticação baseada em certificado, você também deve configurar o Exchange Server para autenticação baseada em certificado. Para obter detalhes, consulte este artigo, Conceitos avançados do Endpoint Management.

Configuração do Citrix Gateway

Embora o Exchange Server deva permitir o tráfego para o serviço de ouvinte, o Citrix ADC deve permitir o tráfego para o serviço de registro. Dessa forma, os dispositivos podem se conectar para registrar para notificações por push.

Se o seu EWS e os servidores ActiveSync forem diferentes, configure a política de tráfego do Citrix ADC para permitir o tráfego de EWS.

Solução de problemas

Para solucionar problemas de conexões de saída, verifique os logs de eventos do Exchange, que incluem as entradas de log quando uma solicitação de assinatura ou a notificação para uma assinatura é inválida ou falha. Você também pode executar rastreamentos de Wireshark no Exchange Server para controlar o tráfego de saída para serviço de ouvinte da Citrix.

Para outros problemas, experimente a ferramenta de teste do Secure Mail.

Perguntas frequentes de notificação por push do Secure Mail

Quando o iOS fornece notificações para Secure Mail

Se o Secure Mail estiver sendo executado em primeiro plano, as notificações serão *sempre* entregues para Secure Mail. Esta é a única ocasião em que a Citrix pode garantir que as notificações são entregues. Quando o Secure Mail entra no segundo plano, o indicador de contagem do aplicativo é sempre atualizado. No entanto, as notificações (de tela de bloqueio e de faixa) baseiam-se na atualização do aplicativo em segundo plano – especialmente quando o iOS suspende ou termina o aplicativo – portanto sua ocorrência não é uma certeza. Os seguintes fatores estão fora do controle da Citrix.

Os seguintes casos podem afetar a entrega de notificações:

- A bateria está fraca.
- O Secure Mail não é usado com frequência (raramente aberto no primeiro plano).
- Emails recebidos fora dos horários centrais de uso em que o aplicativo está suspenso por um longo período em segundo plano, por exemplo, entre a meia-noite e 6 da manhã.

As notificações *não são* entregues ao Secure Mail nos seguintes casos:

- Se o usuário fechar o Secure Mail, até que o usuário reabra o aplicativo manualmente.

- Se o sistema tiver terminado o Secure Mail e o aplicativo não tiver sido reiniciado automaticamente.
- Quando o Secure Mail não está ativo.

> **Importante:**
>
> As notificações não podem ser entregues ao Secure Mail quando ele não estiver ativo por vários motivos, incluindo, sem limitação, os casos a seguir:
>
> - Se o dispositivo estiver no modo de baixa energia e o Secure Mail estiver no segundo plano. Este é o tipo mais comum de ocorrência na qual as notificações deixam de ser entregues.
> - Se a atualização de aplicativo em segundo plano do Secure Mail estiver desativada e o Secure Mail estiver em segundo plano. Observe que os usuários controlam esta configuração.
> - Se o dispositivo tiver conectividade de rede deficiente. Essa situação depende totalmente do dispositivo iOS.

Quando o Secure Mail não recebe uma notificação, o Secure Mail não sincroniza novos dados para o dispositivo. Como consequência, ocorrem as seguintes situações:

- O Secure Mail sincroniza dados somente quando os usuários colocam o aplicativo no primeiro plano.
- As notificações de bloqueio de tela param de ocorrer para novos emails. No entanto, os lembretes de calendário ainda aparecem.

Quando o Android envia notificações para Secure Mail

No Android, as notificações são sempre enviadas ao Secure Mail.

Como o FCM afeta as notificações de email que aparecem na tela de bloqueio

As notificações de novos emails que aparecem na tela de bloqueio do dispositivo são geradas com base nos dados que são sincronizados com dispositivo pelo Secure Mail. É importante ressaltar que essas informações não vêm do serviço de ouvinte.

Para mostrar notificações de novos emails, o Secure Mail precisa ter a capacidade de sincronizar dados do Exchange para que o Secure Mail tenha as informações disponíveis para criar as notificações.

Quando você recebe um novo email, é exibida a notificação FCM **Você tem novas mensagens**. Depois que a sincronização de email for terminada em segundo plano, o novo email aparecerá no Secure Mail.

Como a atualização de aplicativo em segundo plano afeta o Secure Mail e APNs

Se o usuário desativa a atualização de aplicativo em segundo plano, ocorrem as seguintes situações:

- O Secure Mail não recebe notificações quando não é o aplicativo em segundo plano.
- O Secure Mail não atualiza a tela de bloqueio com novas notificações de email.

Desabilitar a atualização de aplicativo em segundo plano tem um grande efeito no comportamento do Secure Mail. Como especificado anteriormente, as atualizações do contador baseadas em APNs ainda ocorrem, mas os emails não são sincronizados ao dispositivo nesse modo.

Como o modo de baixa energia afeta o Secure Mail e APNs

O comportamento do sistema com relação ao Secure Mail é o mesmo em modo de baixa energia que quando a atualização de aplicativo em segundo plano está desativada. Em modo de baixa energia, o dispositivo não ativa aplicativos para atualização periódica e não fornece notificações para os aplicativos em segundo plano. Os efeitos colaterais, portanto, são os mesmos que constam da seção "Atualização do aplicativo em segundo plano" acima. Note que no modo de baixa energia as atualizações do contador ainda acontecem com base em notificações de APNs.

Como os APNs afetam as notificações de email que aparecem na tela de bloqueio

As notificações de novos emails que aparecem na tela de bloqueio do dispositivo são geradas com base nos dados que são sincronizados com dispositivo pelo Secure Mail. É importante ressaltar que essas informações não vêm do serviço de ouvinte.

Para mostrar notificações de novos emails, o Secure Mail precisa ter a capacidade de sincronizar dados do Exchange para que o Secure Mail tenha as informações disponíveis para criar as notificações.

Se as notificações de APNs não forem entregues ao Secure Mail em segundo plano, o Secure Mail não detecta as notificações e, portanto, não sincroniza novos dados. Como não existem novos dados disponíveis para o Secure Mail, não são geradas notificações na tela de bloqueio do dispositivo, mesmo que as notificações de APNs não sejam entregues.

Que outros problemas podem causar falha na sincronização em segundo plano comandada por FCM

Vários problemas podem causar falha na sincronização em segundo plano comandada por FCM, entre eles os seguintes:

- Um tíquete de STA inválido.
- Quando o Secure Mail sai do segundo plano, o aplicativo tem 10 segundos para sincronizar todos os dados do servidor.

Se alguma das condições anteriores ocorrer, o Secure Mail não pode sincronizar dados. Como resultado, as notificações não são exibidas na tela de bloqueio.

O que outros problemas podem causar falha na sincronização em segundo plano comandada por APNs

Vários problemas podem causar falha na sincronização em segundo plano comandada por APNs, entre eles os seguintes:

- Um tíquete de STA inválido.
- Uma conexão de rede lenta. Quando o Secure Mail sai do segundo plano, o aplicativo tem 30 segundos para sincronizar todos os dados do servidor.
- Se a política de proteção de dados estiver acionada e o Secure Mail for ativado por uma notificação de APNs, quando o dispositivo está bloqueado, o Secure Mail não pode acessar o armazenamento de dados e a sincronização não ocorre. Observe que isso só se aplica quando o sistema está tentando iniciar o Secure Mail a frio. Se um usuário já tiver iniciado o Secure Mail em algum momento depois de ter desbloqueado o dispositivo, a sincronização comandada por APNs ocorre mesmo se o dispositivo estiver bloqueado.

Se ocorrer alguma das condições precedentes, o Secure Mail não pode sincronizar dados e, portanto, não pode exibir notificações de bloqueio de tela.

De que outros modos o Secure Mail gera notificações de bloqueio de tela quando as notificações não são entregues ou os APNs não estão sendo usados

Se os APNs forem desativados, o Secure Mail ainda é ativado por eventos periódicos de atualização de aplicativo em segundo plano do iOS, partindo-se do pressuposto de que a atualização de aplicativo em segundo plano está ativa e de que o modo de baixa energia está desligado.

Durante esses eventos de ativação, o Secure Mail sincroniza novos emails provindos do Exchange Server. Estes novos emails poderão ser usados para gerar notificações por email na tela de bloqueio. Assim, mesmo quando as notificações de APNs não são entregues ou as APNs estão desativadas, o Secure Mail pode sincronizar dados em segundo plano.

É importante notar que isso ocorre menos em tempo real que quando as APNs estão em uso e quando as notificações de APNs são enviadas para o Secure Mail. Quando o iOS rotei as notificações de APNs para o Secure Mail, o aplicativo sincroniza imediatamente dados provenientes do servidor e as notificações de bloqueio de tela parecem ser em tempo real.

Caso sejam necessárias ativações de atualização de aplicativo em segundo plano, as notificações de bloqueio de tela não ocorrem em tempo real. Nesse caso, o Secure Mail é ativado com uma frequência determinada totalmente pelo iOS. Sendo assim, pode demorar algum tempo entre o momento da chegada de um email a uma caixa de entrada do usuário no Exchange e o momento em que o Secure Mail sincroniza a mensagem de notificação e gera a notificação de tela de bloqueio.

Observe também que o Secure Mail recebe essas ativações periódicas mesmo que as APNs estejam

em uso. Em todos os casos em que a atualização de aplicativo em segundo plano é ativada, o Secure Mail tenta sincronizar dados provenientes do Exchange.

Como o Secure Mail difere de outros aplicativos que mostram o conteúdo na tela de bloqueio

Uma diferença muito importante - e outra que gera confusão - é que o Secure Mail nem sempre mostra novos emails em tempo real na tela de bloqueio do mesmo modo que fazem o Gmail, o Microsoft Outlook e outros aplicativos. O principal motivo dessa diferença é a segurança. Para alinhar com o comportamento dos outros aplicativos, o serviço de ouvinte da Citrix requer as credenciais de usuário para autenticar com o email do Exchange para obter conteúdo e também passar este conteúdo de email por meio do serviço de ouvinte da Citrix, bem como o serviço de APNs da Apple. A abordagem da Citrix relativa às notificações APNs não requer o serviço de ouvinte da Citrix para adquirir ou armazenar a senha dos usuários. O serviço de ouvinte não tem acesso à caixa de correio de usuário ou à senha.

Uma observação sobre o aplicativo de email nativo iOS: o iOS permite que seu próprio aplicativo de email mantenha uma conexão persistente com o servidor de email, o que garante que as notificações são sempre entregues. Aplicativos de terceiros além do email nativo não tem permissão para usar esse recurso.

Comportamento do aplicativo Gmail: A Google é proprietária e controla o aplicativo Gmail e o servidor do Gmail. Isso significa que o Google pode ler o conteúdo da mensagem e incluir o conteúdo da mensagem na carga de notificação de APNs. Quando o iOS recebe esta notificação de APNs do Gmail, o iOS faz o seguinte:

- Atribui ao contador do aplicativo o valor especificado na carga de notificação.
- Exibe a notificação de tela de bloqueio usando o texto da mensagem que está contido na carga de notificação.

Esta é uma diferença crítica: é o iOS, e não no aplicativo Gmail, que exibe a notificação de bloqueio de tela Com base nos dados contidos na carga. Na verdade, o iOS nunca pode ativar o aplicativo Gmail, de modo semelhante à forma como o iOS não pode ativar o Secure Mail quando uma notificação chega. No entanto, como a carga contém o trecho da mensagem, o iOS pode exibir a notificação de tela de bloqueio sem precisar que os dados de email sejam sincronizados com o dispositivo.

No Secure Mail, essa situação é diferente. O Secure Mail precisa primeiro sincronizar dados da mensagem do Exchange para que o aplicativo mostre a notificação de tela de bloqueio.

Comportamento do aplicativo Outlook para iOS: a Microsoft controla o Outlook para iOS. A organização à qual o usuário pertence, no entanto, controla os servidores Exchange dos quais os dados são obtidos. Apesar dessa configuração, o Outlook pode exibir notificações de tela de bloqueio com base nos dados que o Microsoft fornece na notificação de APNs porque o Outlook para iOS faz uso de

um modelo no qual o Microsoft armazena as credenciais do usuário. A Microsoft então acessa Diretamente a caixa de correio do usuário do seu serviço de nuvem e detecta a existência de novos emails.

Se houver novos Emails, o serviço de nuvem da Microsoft gera uma notificação de APNs que contém os nodos dados de email. Esse modelo opera de modo semelhante ao modelo do Gmail em que o iOS simplesmente usar os dados para gerar uma notificação de bloqueio de tela com base naqueles dados. O aplicativo Outlook para iOS não é envolvido no processo.

Nota de segurança importante sobre o Outlook para iOS: Há implicações de segurança importantes na abordagem do Outlook para iOS. As organizações têm de confiar na Microsoft com senhas para seus usuários para que a Microsoft possa ter acesso à caixa de correio do usuário, o que oferece um risco de segurança. Para obter mais informações sobre a forma como a Microsoft gerencia as senhas do usuário, consulte Microsoft TechNet.

Para ver mais perguntas frequentes específicas aos administradores sobre notificações por push, consulte este artigo do Support Knowledge Center. Para ver mais perguntas frequentes específicas a usuários, consulte este artigo do Support Knowledge Center.

Interatividade do Secure Mail com outros aplicativos móveis de produtividade e Citrix Files

June 12, 2019

A interatividade do Secure Mail com outros aplicativos móveis de produtividade e o Citrix Files permite aos usuários acessar, editar, compartilhar e salvar os documentos diretamente, sem sair do ambiente seguro definido pelas políticas da sua organização. Por exemplo, tocar em um link no Secure Mail abre o site no Secure Web. Os usuários podem abrir e editar anexos com o Citrix QuickEdit para Endpoint Management. Anexos são baixados para o espaço do Citrix Files para Endpoint Management do usuário.

Para obter uma lista completa dos recursos do Secure Mail para cada plataforma, consulte Recursos por plataforma.

Teste e resolução de problemas no Secure Mail

June 12, 2019

Quando o Secure Mail não está funcionando corretamente, a causa geralmente são problemas de conexão. Este artigo descreve como evitar problemas de conexão. Este artigo descreve como solucionar os problemas que possam ocorrer.

Teste de conexões ActiveSync, autenticação de usuário e configuração de APNs

Você pode usar o Endpoint Management Analyzer para realizar verificações do serviço de detecção automática do Secure Mail. Ele guia você no download do aplicativo Endpoint Management Exchange ActiveSync Test. A opção de email de teste verifica configurações básicas de conexão ao servidor de email. A ferramenta também ajuda a resolver os problemas de servidores ActiveSync quanto à prontidão para implantação em um ambiente Endpoint Management. Para obter detalhes, consulte Ferramenta Endpoint Management Analyzer.

A opção de teste de email no Analyzer verifica o seguinte.

- As conexões do dispositivo iOS e Android com servidores Microsoft Exchange ou IBM Traveler.
- Autenticação do usuário.
- Configuração de notificação push para iOS, incluindo Exchange Server, Web Services (EWS), Citrix Gateway, certificados APNs e o Secure Mail. Para obter informações sobre a configuração de notificações por push, consulte Notificações por Push para o Secure Mail para iOS.

A ferramenta fornece uma ampla lista de recomendações para corrigir os problemas.

> Nota:
>
> O aplicativo Mail Test, MailTest.ipa, está obsoleto. Em vez disso, acesse a mesma funcionalidade no Endpoint Management Analyzer.

Pré-requisitos para o teste

- Verifique se a política de acesso à rede não está bloqueada.
- Defina a política de bloqueio de composição de email como **Desativada**.

Uso de logs do Secure Mail para resolução de problemas de conexão

Para obter logs do Secure Mail, faça o seguinte.

1. Vá para **Secure Hub > Help > Report Issue**.
2. Selecione **Secure Mail** na lista de aplicativos.

   É aberto um email endereçado ao suporte técnico da sua organização.
3. Preencha a linha de assunto e corpo com algumas palavras que descrevam o problema.
4. Selecione a hora em que aconteceu.
5. Altere essas configurações apenas se a equipe de suporte tiver instruído você a fazer isso.
6. Clique em **Send**.

   A mensagem concluída se abre com arquivos de log anexados.

7. 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 de aplicativo contêm informações sobre o dispositivo e o aplicativo. Verifique se a versão de modelo e plataforma de hardware em uso têm suporte. Verifique se as versões do Secure Mail e MDX Toolkit em uso são as mais recentes e são compatíveis. Para obter detalhes, consulte Requisitos do sistema para o Secure Mail e Compatibilidade do Endpoint Management.

- CtxLog_VPNConfig.xml (iOS) e VpnConfig.xml (Android)

Os logs de configuração de VPN são fornecidos apenas para o Secure Hub. Verifique a versão do Citrix ADC `ServerBuildVersion` para garantir que a versão mais recente do Citrix ADC está em uso. Verifique as configurações `SplitDNS` e `SplitTunnel` da seguinte maneira:

- Se Split DNS estiver definido como **Remote**, **Local** ou **Both**, verifique se você está resolvendo corretamente o servidor de email FQDN por DNS. (Split DNS está disponível para o Secure Hub no Android.)
- Se Split Tunnel estiver definido como **On**, verifique se o servidor de email está listado como um dos aplicativos da Internet acessíveis no back-end.
- CtxLog_AppPolicies.xml (iOS), Policy.xml (Android e Windows Phone)

Os logs de políticas fornecem os valores de todas as políticas de MDX aplicadas ao Secure Mail a partir do momento em que você obteve o log. Para problemas de conexão, verifique os valores das políticas `<BackgroundServices>` e `<BackgroundServicesGateway>`.

- Logs de diagnóstico (na pasta de diagnósticos)

Para obter as configurações iniciais do Secure Mail, o problema mais comum é “A rede da sua empresa não está disponível no momento”. Para usar os logs de diagnóstico para solucionar problemas de conexão da seguinte maneira.

As colunas de chave nos logs de diagnóstico são Timestamp (Carimbo de data/hora), Message Class (Classe de mensagem), e Message (Mensagem). Quando uma mensagem de erro aparece no Secure Mail, anote o horário para que você possa localizar rapidamente as entradas da coluna **Timestamp.**

Para determinar se a conexão do dispositivo ao Citrix Gateway foi bem-sucedida: examine as entradas AG Tunneler. As seguintes mensagens indicam conexão com êxito:

- AG policy Intercepting FQDN:443 for STA tunneling
- New TCP proxy connection to (null):443 established

Para determinar se a conexão do Citrix Gateway ao Endpoint Management foi bem-sucedida (e, portanto, pode validar o tíquete de STA), faça o seguinte: vá para o log de diagnóstico do Secure Hub e

revise as entradas INFO (4) em Message Class com relação à data/hora em que o dispositivo foi registrado. As seguintes mensagens indicam que o Secure Hub obteve um tíquete STA do Endpoint Management:

- Getting STA Ticket.
- Got STA Ticket response.
- STA Ticket – Success obtaining STA ticket for App – Secure Mail.

> Nota:
>
> Durante o processo de registro, o Secure Hub envia uma solicitação de um tíquete de STA para o Endpoint Management. O Endpoint Management envia o tíquete STA para o dispositivo, onde é armazenado e adicionado à lista de tíquetes STA do Endpoint Management.

Para determinar se o Endpoint Management emitiu um tíquete STA para um usuário, verifique o UserAuditLogFile.log, incluído no pacote de suporte. Ele lista, para cada tíquete, o problema, o nome de usuário, dispositivos do usuário e o resultado. Por exemplo:

Data/hora: 2015-06-30T 12:26:34.771-0700

Usuário: user2

Dispositivo: Mozilla/5.0 (iPad; CPU OS 8_1_2 como macOS)

Resultado: Successfully generated STA ticket for user 'user2' for app 'Secure Mail'

Para verificar a comunicação do Citrix Gateway com o servidor de email, verifique se o DNS e a rede estão configurados corretamente. Para fazer isso, use o Secure Web para acessar o Outlook Web Access (OWA). Como o Secure Mail, o Secure Web pode usar um micro túnel VPN para estabelecer uma conexão do Citrix Gateway. O Secure Web atua como um proxy para o recurso interno ou externo que o aplicativo está acessando. Geralmente e em especial em um ambiente do Exchange, o OWA é hospedado no servidor de email.

Para testar a configuração, abra o Secure Web e insira o FQDN da página do OWA. A solicitação segue o mesmo roteiro e resolução DNS que a comunicação entre o Citrix Gateway e o servidor de email. Se a página de OWA abrir, você sabe que o Citrix Gateway está se comunicando com o servidor de email.

Se as verificações anteriores tiverem indicado comunicações com êxito, é uma indicação que o problema não está na instalação da Citrix. Em vez disso, o problema é com os servidores Exchange ou Traveler.

Você pode coletar informações para os seus administradores do servidor Exchange ou Traveler. Primeiro verifique se há problemas nos servidores HTTP do Exchange ou Traveler buscando no log de diagnóstico do Secure Mail log a palavra Error. Se os erros incluírem códigos HTTP e você tiver vários servidores Exchange ou Traveler, investigue cada servidor. O Exchange e o Traveler têm logs de HTTP que mostram solicitações e respostas de dispositivos cliente. O log do Exchange é C:\inetpub\LogFiles\W3SVC1\U_EX.log. O log do Traveler é IBM_TECHNICAL_SUPPORT>HTTHR.log.

Para obter logs de falhas de um dispositivo para Secure Mail para iOS

1. No dispositivo iOS, acesse **Ajustes** > **Privacidade** > **Análise** > **Dados da análise**.
2. Na lista de **Dados**, clique no nome do aplicativo e no carimbo de data/hora relevante. Os logs são exibidos.

Resolução de problemas com email, contatos ou calendário

Você pode solucionar problemas do Secure Mail, como um email ou emails presos na pasta de rascunhos, contatos ausentes ou itens de calendário fora de sincronia. Para solucionar esses problemas, use os logs de caixa de correio do Exchange ActiveSync. Os logs mostram as solicitações de entrada enviadas por dispositivos e as respostas de saída do servidor de email.

Para obter mais detalhes, consulte a postagem Under the Hood: Exchange ActiveSync Mailbox Log Analysis no blog TechNet.

Práticas recomendadas de sincronização ilimitada

Quando os usuários definem seus períodos de sincronização de email como **Todos**, a sincronização é ilimitada. Com a sincronização ilimitada, pressupõe-se que os usuários gerenciem o tamanho da caixa de correio, que é a Caixa de Entrada e todas as subpastas sincronizadas. Aqui estão alguns pontos para levar em consideração para obter o melhor desempenho.

1. Se o tamanho da caixa de correio exceder 18.000 mensagens ou 600 MB no tamanho total, a sincronização de email pode ser mais lenta.
2. Não é recomendável ativar **Carregar anexos em WiFi** com a sincronização ilimitada. Esta opção pode fazer com que o espaço ocupado pelos emails aumente rapidamente e de modo exagerado no dispositivo.
3. Para evitar a sincronização ilimitada como uma opção para os usuários, defina a política de aplicativo **Intervalo de sincronização máximo** com um valor diferente de **Todos**.
4. Não é recomendável definir **Todos** como o **Intervalo de sincronização padrão** para os usuários.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States