



Secure Mail

Contents

Visão geral do Secure Mail	3
Novidades do Secure Mail	4
Problemas conhecidos e resolvidos	80
Implantação do Secure Mail	81
Configurando o Secure Mail	83
Integração do Secure Mail com o Microsoft Intune/EMS	83
Autenticação moderna com o Microsoft Office 365	85
Serviços em segundo plano para o Secure Mail	88
Integração do Exchange Server ou servidor IBM Notes Traveler	93
S/MIME para Secure Mail	97
SSO para Secure Mail	145
Considerações de segurança	147
Recursos do iOS	159
Recursos do Android	181
Recursos do iOS e Android para Secure Mail	217
Integração do Secure Mail com Slack	274
Notificações e sincronização	289
Notificações por Push para o Secure Mail	291
Notificações por Push em rich text para o Secure Mail para iOS	299
Interatividade do Secure Mail com outros aplicativos móveis de produtividade e Citrix Files	306
Teste e resolução de problemas no Secure Mail	306

Visão geral do Secure Mail

July 25, 2022

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

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

Nota:

O suporte para o Exchange Server 2010 terminou em 13 de outubro de 2020.

O Secure Mail é compatível com:

- Atualização cumulativa 11 do Exchange Server 2019
- Atualização cumulativa 10 do Exchange Server 2019
- Atualização cumulativa 9 do Exchange Server 2019
- Atualização cumulativa 8 do Exchange Server 2019
- Atualização cumulativa 7 do Exchange Server 2019
- Atualização cumulativa 6 do Exchange Server 2019
- Atualização cumulativa 23 do Exchange Server 2016
- Atualização cumulativa 22 do Exchange Server 2016
- Atualização cumulativa 21 do Exchange Server 2016
- Atualização cumulativa 20 do Exchange Server 2016
- Atualização cumulativa 19 do Exchange Server 2016
- Atualização cumulativa 18 do Exchange Server 2016
- Atualização cumulativa 17 do Exchange Server 2016
- Atualização cumulativa 23 do Exchange Server 2013
- Atualização cumulativa 22 do Exchange Server 2013
- Atualização cumulativa 21 do Exchange Server 2013
- HCL Domino 11 (anteriormente Lotus Notes)
- HCL Domino 10.0.1 (anteriormente Lotus Notes)
- HCL Domino 9.0.1 FP10 HF197 (anteriormente Lotus Notes)
- HCL Domino 10.0.1.0 compilação 201811191126_20 (anteriormente Lotus Notes)
- HCL Domino 9.0.1.21 (anteriormente Lotus Notes)
- Microsoft Office 365 (Exchange on-line)

Para começar, baixe o Secure Mail e outros componentes do Endpoint Management em [Downloads do Citrix Endpoint Management](#).

Quanto ao Secure Mail e outros requisitos de sistema de aplicativos móveis, consulte os [Requisitos do sistema](#).

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

Para os recursos do iOS suportados no Secure Mail, consulte [Recursos do iOS para Secure Mail](#).

Para os recursos do Android suportados no Secure Mail, consulte [Recursos do Android para Secure Mail](#).

Para os recursos do iOS e Android suportados no Secure Mail, consulte [Recursos do iOS e Android para Secure Mail](#).

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

Novidades do Secure Mail

September 13, 2022

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

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

Nota:

O Secure Hub, Secure Mail, Secure Web e o aplicativo Citrix Workspace não são compatíveis com o Android 6.x e iOS 11.x a partir de junho de 2020.

O que há de novo na versão atual

Secure Mail 22.9.0

Secure Mail para iOS

O Secure Mail agora oferece suporte ao iOS 16.

O que há de novo em versões anteriores

Secure Mail 22.6.2

Secure Mail para iOS

Esta versão inclui correções de bugs.

Secure Mail 22.6.0

A partir desta versão em diante, o Secure Mail inclui suporte para a Atualização cumulativa 23 do Exchange Server 2016

Secure Mail para iOS

Esta versão inclui correções de bugs.

Secure Mail para Android

Esta versão inclui correções de bugs.

Secure Mail 22.3.0

Secure Mail para iOS

Suporte para HCL Domino 11. A partir desta versão, o Secure Mail para iOS inclui suporte para HCL Domino 11 (anteriormente Lotus Notes).

Google Analytics. O Citrix Secure Mail usa o Google Analytics para coletar estatísticas do aplicativo e dados analíticos sobre informações de uso para melhorar a qualidade do produto. A Citrix não coleta nem armazena nenhuma outra informação pessoal do usuário. Para obter mais informações sobre como desativar o Google Analytics do Secure Mail, consulte [Desativar o Google Analytics](#).

Secure Mail para Android

Suporte para HCL Domino 11. A partir desta versão, o Secure Mail para Android inclui suporte para HCL Domino 11 (anteriormente Lotus Notes).

Google Analytics. O Citrix Secure Mail usa o Google Analytics para coletar estatísticas do aplicativo e dados analíticos sobre informações de uso para melhorar a qualidade do produto. A Citrix não coleta nem armazena nenhuma outra informação pessoal do usuário. Para obter mais informações sobre como desativar o Google Analytics do Secure Mail, consulte [Desativar o Google Analytics](#).

Secure Mail 22.2.0

Secure Mail para iOS

A opção de gerenciar seus feeds foi preterida na versão 21.5.0. Com esta versão, somente os seguintes cartões de feed padrão aparecem no Secure Mail para iOS:

- Não lida(s)
- Convites para reuniões
- Próximas reuniões
- Do seu gerente

Se você tem esse recurso habilitado e configurado no momento, as preferências são substituídas pelos cartões padrão.

Secure Mail para Android

A opção de gerenciar seus feeds foi preterida na versão 21.5.0. Com esta versão, somente os seguintes cartões de feed padrão aparecem no Secure Mail para iOS:

- Não lida(s)
- Convites para reuniões
- Próximas reuniões
- Do seu gerente

Se você tem esse recurso habilitado e configurado no momento, as preferências são substituídas pelos cartões padrão.

Secure Mail 21.12.0

Secure Mail para iOS

Suporte para agente de usuário personalizado. A partir desta versão, você pode usar agentes de usuário personalizados para autenticação com o Microsoft Office 365 para Serviços de Federação do Active Directory (AD FS) ou Provedor de Identidade (IdP). Para usar esse recurso, você deve habilitar e configurar a política de **Agente de usuário personalizado para autenticação moderna** no console Citrix Endpoint Management.

Secure Mail para Android

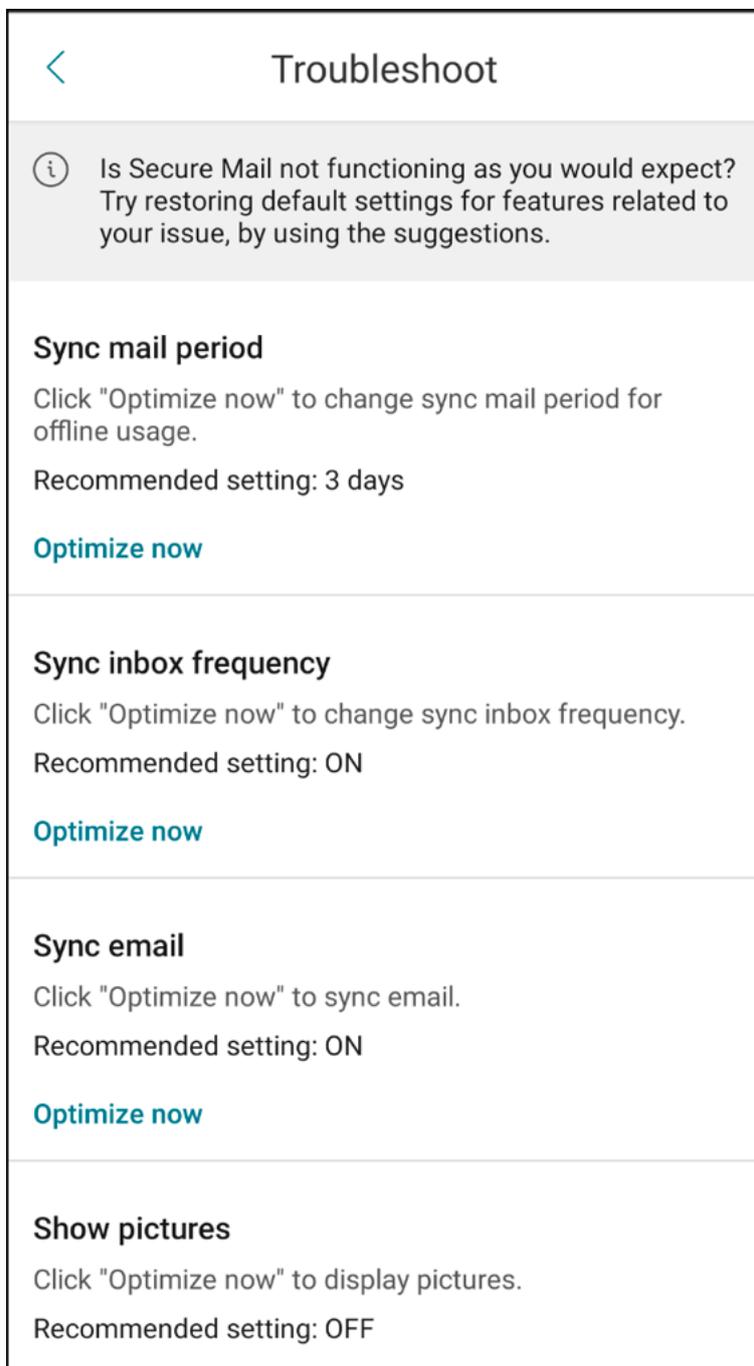
Esta versão inclui correções de bugs.

Secure Mail 21.11.0

Secure Mail para Android

Ferramenta de autodiagnóstico

Agora você pode solucionar qualquer problema que possa ter no Secure Mail para Android. Use o botão **Solucionar problemas** na opção de menu **Suporte** nas configurações do aplicativo. Para corrigir os problemas, abra o Secure Mail e navegue até **Configurações > Solucionar problemas**.

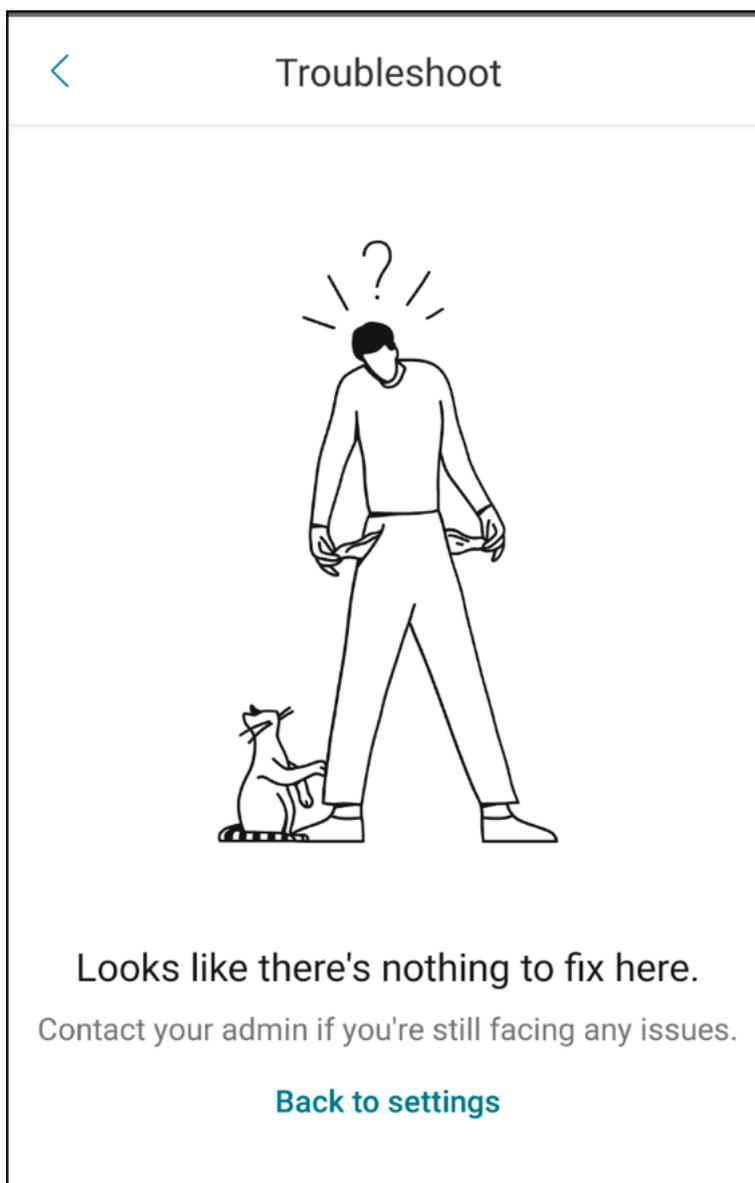


Os seguintes itens de menu parecem solucionar problemas:

- Limpar as preferências padrão de aplicativo

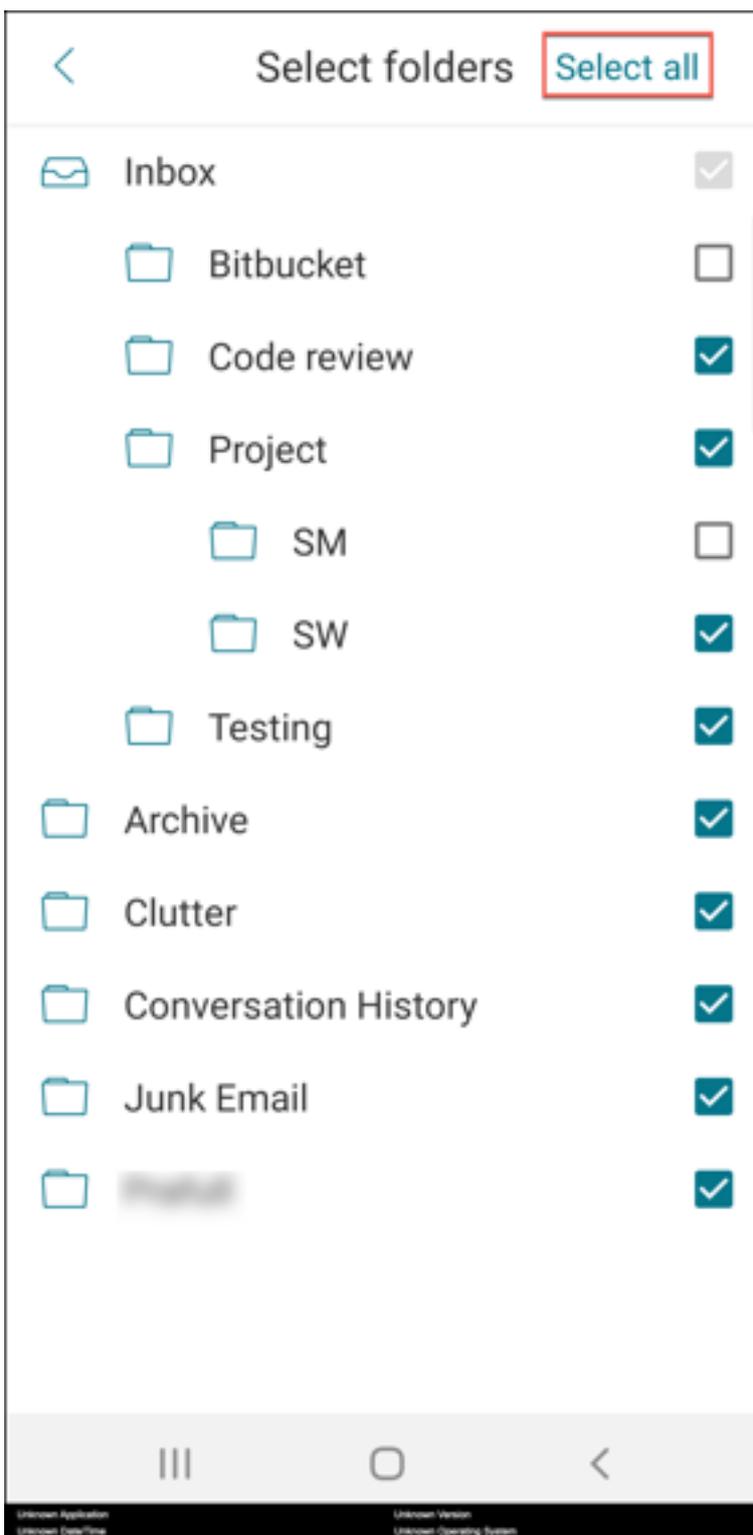
- Tempo do lembrete padrão
- Ignorar otimizações de bateria
- Gerenciar as notificações de calendário
- Gerenciar as notificações de email
- Mostrar imagens
- Sincronizar o calendário
- Sincronizar os contatos
- Sincronizar o email
- Frequência de sincronização da caixa de entrada
- Período de sincronização

Se todas essas configurações forem restauradas para os padrões e você ainda estiver enfrentando problemas com o Secure Mail, entre em contato com o administrador.

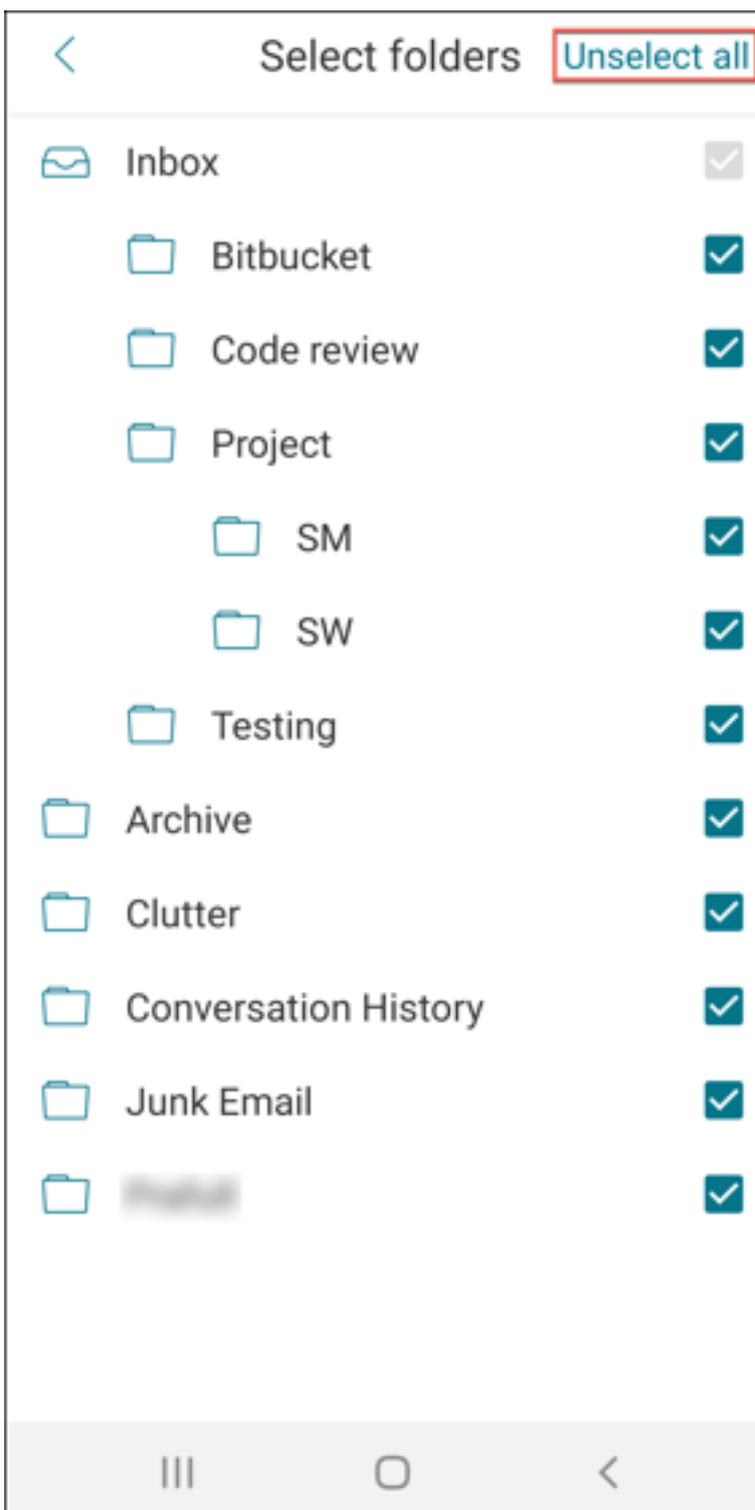


Melhorias na notificação de subpastas

Agora você pode receber notificações de todas as suas subpastas clicando na opção **Selecionar tudo** na tela **Selecionar pastas** navegando para **Configurações > Notificações > Pastas de correio**.



Você pode clicar em **Desmarcar tudo** para parar de receber notificações de todas as subpastas.



Secure Mail 21.10.5

A partir desta versão em diante, o Secure Mail inclui suporte para a Atualização cumulativa 11 do Exchange Server 2019 e Atualização cumulativa 22 do Exchange Server 2016.

Secure Mail para iOS

Esta versão inclui correções de bugs.

Secure Mail para Android

Esta versão inclui correções de bugs.

Nota:

O suporte para o Android 7 termina para o Secure Mail em outubro de 2021.

Secure Mail 21.10.0

Secure Mail para Android

- **Suporte para Android 12.** A partir desta versão, o Secure Mail é compatível com dispositivos que executam o Android 12.
- O Secure Mail atende aos requisitos atuais da API de destino do Google Play (API de nível 30) para Android 11.

Secure Mail 21.9.1

Secure Mail para Android

Esta versão inclui correções de bugs.

Secure Mail 21.9.0

Secure Mail para iOS

Esta versão inclui correções de bugs.

Secure Mail para Android

Esta versão inclui correções de bugs.

Secure Mail 21.8.5

Secure Mail para Android

Suporte para Android 12 Beta 4 em dispositivos já registrados. O Secure Mail agora oferece suporte ao Android 12 Beta 4. Se você estiver pensando em atualizar para o Android 12 Beta 4, certifique-se de atualizar o Secure Hub para a versão 21.7.1 primeiro. O Secure Hub 21.7.1 é a versão mínima necessária para atualizar para o Android 12 Beta 4. Essa versão garante a atualização descomplicada do Android 11 para o Android 12 Beta 4 para usuários já registrados.

Nota:

A Citrix está comprometida em fornecer suporte de Dia 1 para o Android 12. As versões subsequentes do Secure Mail recebem atualizações adicionais para oferecer suporte total ao Android 12.

Secure Mail 21.8.0

Secure Mail para iOS

Detecção automática baseada em e-mail do Exchange Server em ambientes híbridos

No Secure Mail para iOS, você pode configurar a sua conta do Microsoft 365 Exchange usando o seu endereço de e-mail, o que garante uma experiência de login tranquila para Exchange Servers híbridos. Esse recurso também está disponível para Exchange Servers locais.

Nota:

Certifique-se de habilitar o recurso de detecção automática para o Exchange Server.

Notificações por push avançadas em configurações executando a autenticação moderna com o Microsoft Office 365

Com esta versão, o Secure Mail suporta notificações por push quando a política de acesso à rede é definida como **Com túnel - SSO de Web** e o nome do host do Exchange Web Services (EWS) está incluído na **Lista de exclusão**. Se os hosts EWS e ActiveSync forem os mesmos, certifique-se de que o host ActiveSync esteja incluído na política de **Lista de exclusão**.

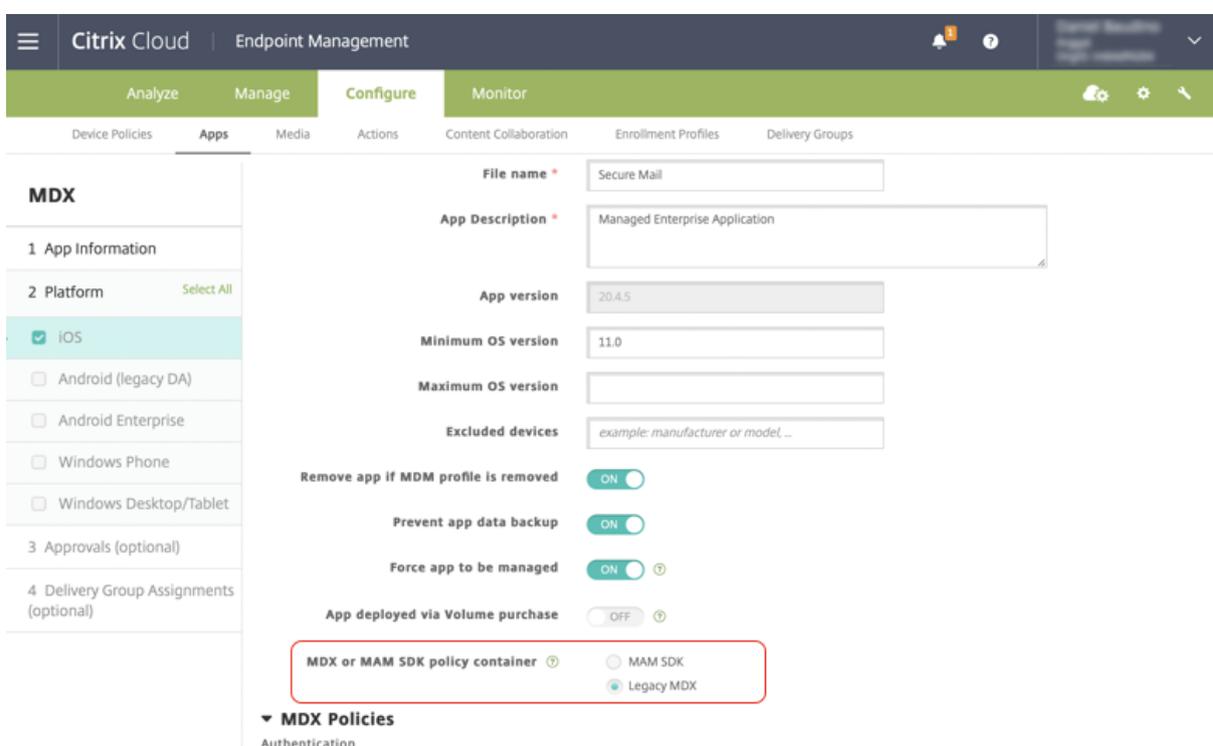
Modo duplo para Secure Mail

O SDK de gerenciamento de aplicativo móvel (MAM) está disponível para substituir áreas de funcionalidade MDX que não são cobertas pela plataforma iOS. A tecnologia de preparação MDX está programada para atingir o fim da vida útil (EOL) em março de 2022.

O Citrix Secure Mail é lançado com as estruturas MDX e MAM SDK para se preparar para o fim da vida útil (EOL) de MDX, programado para março de 2022. Para continuar gerenciando seus aplicativos empresariais, você deve incorporar o SDK MAM. A Citrix recomenda que você mude para o **MAM SDK**. A funcionalidade de modo duplo destina-se a fornecer uma maneira de fazer a transição do aplicativo Secure Mail para o novo modelo de MAM SDK.

A funcionalidade de modo duplo permite que você continue gerenciando aplicativos usando MDX (agora **MDX herdado**) ou mude para o novo **MAM SDK**. Você tem as seguintes opções de configurações de política no **Contêiner de política MDX ou MAM SDK**:

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



Na política de **Contêiner de política MDX ou MAM SDK**, você pode alterar sua opção de **MDX herdado** para **MAM SDK**.

É recomendável que você não mude de **MAM SDK** para **MDX herdado**, pois isso exige que você reinstale o aplicativo. O valor padrão é **MDX herdado**. Certifique-se de definir o mesmo modo de política para o Secure Mail e o Secure Web em execução em um dispositivo. Não é possível ter dois modos diferentes em execução no mesmo dispositivo.

Quando você seleciona o modo **MAM SDK**, os aplicativos mudam automaticamente para a estrutura MAM SDK e as políticas de dispositivo são atualizadas sem nenhuma ação adicional dos administradores.

Nota:

Quando você muda da estrutura de **MDX herdado** para **MAM SDK**, a política de **Acesso à rede** deve ser modificada para **Com túnel — SSO de Web** ou **Irrestrita**

Pré-requisitos

Para uma implantação bem-sucedida do recurso de modo duplo, certifique-se de que os seguintes requisitos sejam atendidos:

- Atualize o Citrix Endpoint Management para as versões 10.12 RP2, ou posteriores, ou 10.11 RP5, ou posteriores.
- Atualize seus aplicativos móveis para a versão 21.8.0 ou posterior.
- Se a sua organização usa aplicativos de terceiros, certifique-se de incorporar o MAM SDK em seus aplicativos de terceiros antes de mudar para a estrutura MAM SDK. Todos os seus aplicativos gerenciados devem ser movidos para o MAM SDK de uma só vez.

Limitações

- O SDK MAM suporta apenas criptografia baseada em plataforma, não criptografia MDX.
- Entradas de política duplicadas aparecerão se você não atualizar o Citrix Endpoint Management para a versão 10.12 RP2 ou posterior, ou 10.11 RP5 ou posterior. As entradas duplicadas são criadas se os arquivos de política estiverem sendo executados na versão 21.8.0 ou posterior.
- Quando você muda para o modo MAM SDK de gerenciamento de aplicativo, alguns recursos não são suportados ou não estão disponíveis. Além disso, a interoperação entre aplicativos em diferentes modos não é suportada para ações como Abrir e Copiar/Colar. Por exemplo, você não pode copiar o conteúdo de um aplicativo gerenciado no modo **MDX herdado** para um aplicativo gerenciado no modo **MAM SDK** ou vice-versa. Consulte a tabela a seguir para ver os recursos que não estão disponíveis no modo MAM SDK:

Recurso	MDX herdado	MAM SDK
Dispositivos compartilhados	Sim	Não
Intune	Sim	Não
Cofre de certificado compartilhado SMIME	Sim	Não
Credenciais derivadas	Sim	Não
Encapsulamento UIWebView	Sim	Não

Recurso	MDX herdado	MAM SDK
VPN completa	Sim	Não

- As políticas a seguir estão preteridas e não estão disponíveis no modo MAM SDK:
 - Domínios do Secure Web permitidos
 - Redes Wi-Fi permitidas
 - Citrix Gateway alternativo
 - Etiqueta de certificado
 - Relatório Citrix
 - Notificação explícita de logoff
 - sessão micro VPN necessária
 - período de tolerância para sessão micro VPN obrigatória (minutos)
 - Tamanho máximo do cache de arquivo de relatório
 - Exigir Wi-Fi
 - Enviar relatórios apenas por Wi-Fi
 - Token de upload

Nota:

Se você estiver usando um certificado de cliente para autenticação em servidores internos, a certificação do cliente deve ser a mesma usada no Access Gateway.

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

- [Visão geral do MAM SDK](#)
- Documentação do Citrix Developer sobre [integração de aplicativos móveis](#)
- [Postagem no blog Citrix](#)
- Baixe o SDK quando você fizer logon nos [downloads da Citrix](#)

Secure Mail para Android

Esta versão inclui correções de bugs.

Secure Mail 21.7.0

Secure Mail para iOS

Esta versão inclui correções de bugs.

Secure Mail para Android

Esta versão inclui correções de bugs.

Secure Mail 21.6.0

Secure Mail para iOS

A partir desta versão, as seguintes opções de política de **Acesso à rede** não são mais suportadas:

- **Usar as configurações anteriores**
- **Com túnel - VPN completa**
- **Com túnel - VPN completa e SSO de web**

Se estiver usando as políticas **Com túnel - VPN completa** ou **Com túnel - VPN completa e SSO de web**, você deverá mudar para a política **Com túnel - SSO de web**. Seus e-mails não conseguem sincronizar se você continuar a usar as políticas preteridas.

Nota:

Para usar o Secure Ticket Authority (STA), a política de **Acesso à rede** deve ser definida como **Com túnel - SSO de Web**.

Secure Mail para Android

Suporte para autodiagnóstico usando a opção de **Solução de problemas**. Esse recurso permite que você examine se as preferências e configurações básicas, cruciais para o funcionamento correto do aplicativo, estão definidas como padrão ou não. Se você estiver enfrentando algum erro em relação a determinadas configurações do Secure Mail, use esse recurso para solucionar problemas do aplicativo.

Para acessar esse recurso, abra as configurações do aplicativo e toque em **Solucionar problemas** em **Suporte**. As seguintes opções de menu aparecem para você revisar e editar:

- Período de sincronização
- Frequência de sincronização da caixa de entrada
- Sincronizar o email
- Mostrar imagens
- Tempo do lembrete padrão
- Sincronizar o calendário
- Sincronizar os contatos

Para restaurar uma configuração para seu valor padrão, toque em **APLICAR ALTERAÇÃO**. Para restaurar todas as configurações para seus valores padrão, toque em **APLICAR ALTERAÇÕES A TODOS**.

Secure Mail 21.5.0

A partir desta versão em diante, o Secure Mail inclui suporte para a Atualização cumulativa 9 do Exchange Server 2019 e Atualização cumulativa 20 do Exchange Server 2016.

Secure Mail para iOS

- **Crie reuniões do Microsoft Teams em eventos do calendário do Secure Mail.** No Secure Mail para iOS, você pode criar convites para reuniões do Microsoft Teams enquanto cria eventos de calendário. Para criar uma reunião do Microsoft Teams, ative o botão de alternância **Reunião do Microsoft Teams**. O link do convite da reunião e os detalhes são enviados automaticamente com os detalhes do evento. Para obter mais informações, consulte [Criar reuniões do Microsoft Teams em eventos do Calendário do Secure Mail](#)
- Desta versão em diante, as seguintes opções de política de **Acesso à rede** estão preteridas e não são mais suportadas a partir da versão 21.6.0:
 - **Usar as configurações anteriores**
 - **Com túnel - VPN completa**
 - **Com túnel - VPN completa e SSO de web**

Se estiver usando as políticas **Com túnel - VPN completa** ou **Com túnel - VPN completa e SSO de web**, você deverá mudar para a política **Com túnel - SSO de web**. Seus e-mails não conseguem sincronizar se você continuar a usar as políticas preteridas.

Nota:

Se você está usando **Com túnel - VPN completa** e o Secure Ticket Authority (STA) está configurado, a tela de autenticação moderna não carrega.

Secure Mail para Android

- Com esta versão, a política diversa de **Desativar obrigatoriedade de atualização** não está mais disponível no console Citrix Endpoint Management. Seu aplicativo atualiza automaticamente para a versão mais recente disponível na Play Store.
- No Secure Mail para Android, a opção **Gerenciar feeds** está preterida com esta versão. Se você tem esse recurso habilitado e configurado no momento, continuará a ver os feeds com base nas suas configurações preferidas na janela **Feeds**. Se você for um novo usuário ou se tiver removido anteriormente todos os cartões de feed, os seguintes cartões de feed padrão estarão disponíveis:
 - Não lida(s)
 - Convites para reuniões
 - Próximas reuniões

- Do seu gerente

Secure Mail 21.4.5

Secure Mail para Android

Suporte a descoberta automática baseado em e-mail. No Secure Mail para Android, você pode configurar sua conta do Microsoft O365 Exchange usando seu endereço de e-mail, o que garante uma experiência de login descomplicada. Esse recurso também está disponível para os usuários no local, se o AutoDiscovery estiver ativado no ambiente híbrido

Nota:

Este recurso é suportado apenas na Atualização cumulativa 3 do Exchange Server 2016 e posterior.

Secure Mail 21.4.0

Secure Mail para iOS

Esta versão inclui correções de bugs.

Secure Mail 21.3.5

Secure Mail para Android

Esta versão inclui correções de bugs.

Secure Mail 21.3.0

Secure Mail para iOS

Destino de implantação para o Secure Mail iOS alterado para iOS 12.2. O SDK do aplicativo Microsoft Intune para iOS versão 14.1.3 exige que os aplicativos de destino tenham uma versão mínima de implantação do iOS como iOS 12.2. O destino de implantação do Secure Mail é atualizado para o iOS 12.2 para estar em conformidade com esse requisito.

Secure Mail para Android

Crie reuniões do Microsoft Teams em eventos do calendário do Secure Mail. No Secure Mail para Android, você pode criar convites para reuniões do Microsoft Teams enquanto cria eventos de calendário.

Para criar uma reunião do Microsoft Teams, ative o botão de alternância **Reunião do Microsoft Teams**. O link do convite da reunião e os detalhes são enviados automaticamente com os detalhes do evento.

Para obter mais informações, consulte [Criar reuniões do Microsoft Teams em eventos do Calendário do Secure Mail](#)

Secure Mail 21.2.0

A partir desta versão em diante, o Secure Mail inclui suporte para a Atualização cumulativa 8 do Exchange Server 2019 e Atualização cumulativa 19 do Exchange Server 2016.

Secure Mail para iOS

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

Secure Mail para Android

- **Aprimoramento de cores no Secure Mail.** O Secure Mail está em conformidade com as atualizações de cores da marca Citrix.
- **Suporte para o Microsoft Intune.** O Secure Mail para Android suporta a versão mais recente do Microsoft Intune 7.2.2.
- **Funcionamento uniforme em dispositivos dobráveis.** O Secure Mail para Android inclui correções para o funcionamento constante em dispositivos dobráveis.

Secure Mail 21.1.5

Secure Mail para iOS

Esta versão inclui correções de bugs.

Secure Mail 21.1.0

Esta versão inclui correções de bugs.

Secure Mail 20.12.0

Secure Mail para iOS

Esta versão inclui correções de bugs.

Secure Mail 20.11.0

Nota:

O suporte para o Exchange Server 2010 terminou em 13 de outubro de 2020.

Secure Mail 20.10.5**Secure Mail para iOS**

Esta versão inclui correções de bugs.

Secure Mail para Android

Suporte para bibliotecas AndroidX. De acordo com a recomendação do Google, o Secure Mail suporta as bibliotecas do **AndroidX**, que são um substituto para as bibliotecas empacotadas do **android.support**.

Secure Mail 20.10.0

A partir desta versão em diante, o Secure Mail inclui suporte para a Atualização cumulativa 7 do Exchange Server 2019 e Atualização cumulativa 18 do Exchange Server 2016.

Secure Mail para iOS

Participe das reuniões do Microsoft Teams no Secure Mail. No Secure Mail para iOS, você pode participar de reuniões do Microsoft Teams diretamente dos convites no Calendário. Se o aplicativo Microsoft Teams estiver instalado, o aplicativo é aberto e você entra na reunião. Quando o aplicativo não estiver instalado, você vê uma opção para ir à App Store para instalar o Microsoft Teams. Para reuniões no formato <https://teams.microsoft.com/l/meetup-join/meetinglink>, o aplicativo abre e você entra diretamente na reunião.

Nota:

Certifique-se de que seu administrador inclua `+^msteams:` na política URLs permitidas. Para obter detalhes, consulte [Interação de aplicativo \(URL de saída\)](#).

Secure Mail para Android

- **Participe das reuniões do Microsoft Teams no Secure Mail.** No Secure Mail para Android, você pode participar de reuniões do Microsoft Teams diretamente dos convites no Calendário. Se o aplicativo Microsoft Teams estiver instalado, o aplicativo é aberto e você entra na reunião. Quando o aplicativo não estiver instalado, você vê uma opção para ir ao Google Play para instalar o Microsoft Teams. Para reuniões no formato <https://teams.microsoft.com/l/meetup-join/>meetinglink>, o aplicativo abre e você entra diretamente na reunião.

Nota:

Certifique-se de que seu administrador inclua { `action=android.intent.action.VIEW` `scheme=msteams` `package=com.microsoft.teams` } na política Lista restrita de exceção de Abrir em. Para obter detalhes, consulte [Interação do aplicativo](#).

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

Secure Mail 20.9.5

Secure Mail para Android

Esta versão inclui correções de bugs.

Secure Mail 20.9.0

Suporte para computação em nuvem do Azure Governamental O Secure Mail para iOS e Android oferece suporte à Computação em Nuvem Governamental (GCC) Alta para autenticação moderna (OAuth) no locatário do Azure Active Directory. O Secure Mail é registrado como um ponto de extremidade no GCC High, para atender aos requisitos obrigatórios da Microsoft para todo o serviço GCC High. Para obter detalhes, consulte [O que há de novo no Azure Active Directory no Microsoft 365 Governamental](#).

Com essa alteração, você é roteado para o GCC High no locatário do Azure Active Directory para autenticação. E é necessário que o administrador dê permissões para o Secure Mail no locatário do Azure Active Directory.

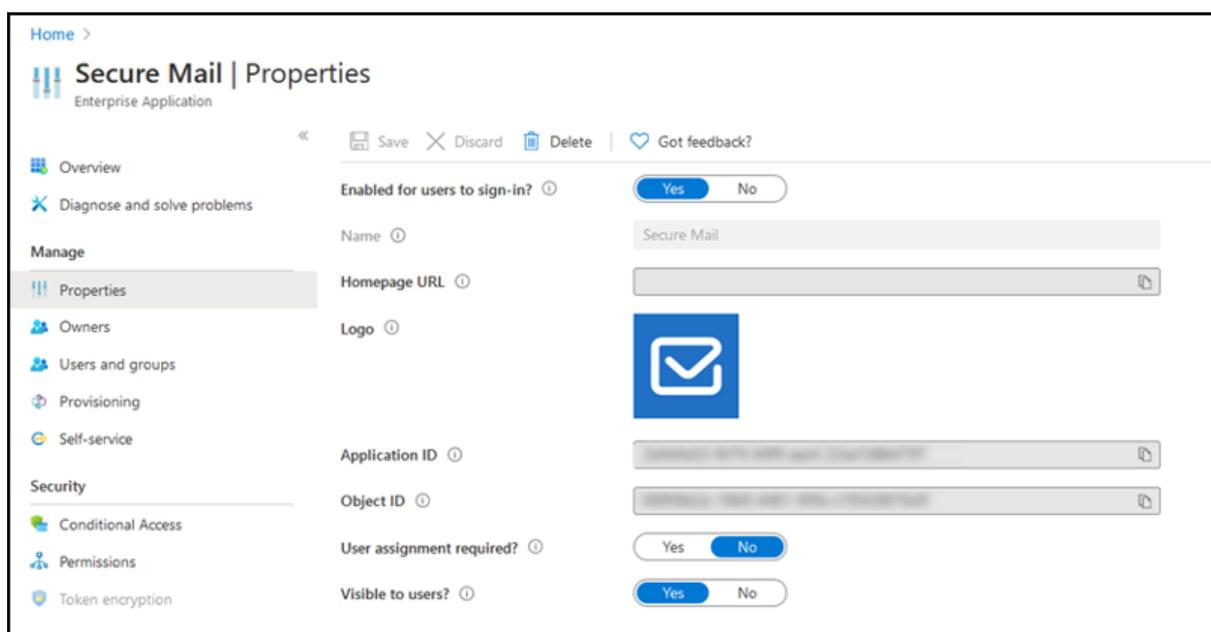
Pré-requisitos

Certifique-se de que o administrador global do Azure Active Directory execute o seguinte:

- Baixe a versão mais recente do Secure Mail em seu dispositivo.
- Configure sua conta do Exchange no aplicativo Secure Mail e dê permissão de aplicativo no Azure Active Directory para que todos os usuários entrem. Veja a tela a seguir.

Nota:

Estas etapas são específicas apenas para os administradores globais como um requisito único. Uma vez que o aplicativo tenha acesso, você pode simplesmente atualizar a partir da App Store.



Depois de atualizar

Após uma atualização, é exibido um aviso de reautenticação após a expiração do token refresh, que o redireciona para o GCC High no Azure Active Directory. Valide o fluxo de trabalho precedente para garantir que a solicitação de autorização seja enviada para o GCC High no Azure Active Directory.

Você pode validar o fluxo de trabalho de uma das seguintes maneiras:

- O Secure Mail com o nome de aplicativo **Secure Mail-GCC High** aparece na página de login no seu locatário do Azure Active Directory.
- Verifique os logs do Secure Mail para confirmar se os redirecionamentos ocorrem via <https://login.microsoftonline.us> após a reautenticação.

Secure Mail 20.8.5

Secure Mail para Android

O Secure Mail para Android suporta o Android 11.

Secure Mail 20.8.0

A partir desta versão em diante, o Secure Mail inclui suporte para a Atualização cumulativa 6 do Exchange Server 2019 e Atualização cumulativa 17 do Exchange Server 2016.

Secure Mail para Android

Modo duplo para Secure Mail. Um SDK de gerenciamento de aplicativo móvel (MAM) está disponível para substituir áreas de funcionalidade MDX que não são cobertas pelas plataformas iOS e Android. A tecnologia de preparação MDX está programada para atingir o fim da vida útil (EOL) em março de 2022. Para continuar gerenciando seus aplicativos empresariais, você deve incorporar o SDK MAM.

A partir da versão 20.8.0, os aplicativos Android são lançados com o MDX e o MAM SDK para se preparar para a estratégia MDX EOL mencionada anteriormente. O modo duplo MDX destina-se a fornecer uma maneira de fazer a transição para novos SDKs MAM a partir do MDX Toolkit legado. O uso do modo duplo permite que você continue gerenciando aplicativos usando o MDX Toolkit (agora MDX herdado) ou alterne para o novo SDK MAM para gerenciamento de aplicativos.

Depois que você mudar para o SDK MAM para gerenciamento de aplicativos, a Citrix implementará outras alterações, o que não requer nenhuma ação dos administradores.

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

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

Pré-requisitos

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

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

Nota:

O SDK MAM é compatível com todos os clientes baseados em nuvem.

Limitações

- O SDK MAM suporta apenas aplicativos publicados na plataforma Android Enterprise em sua implantação do Citrix Endpoint Management. Para os aplicativos recém-publicados, a criptografia padrão é a criptografia baseada em plataforma.
- O SDK MAM suporta apenas criptografia baseada em plataforma, não criptografia MDX.

- Se você não atualizar o Citrix Endpoint Management e os arquivos da política estiverem sendo executados na versão 20.8.0 e posterior nos aplicativos móveis, serão exibidas entradas duplicadas da política de Rede no Secure Mail.

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

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

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

The screenshot displays the Citrix Cloud Endpoint Management interface for configuring an application. The 'Configure' tab is active, and the 'App Information' section is expanded. The 'MDX or MAM SDK policy container' option is highlighted with a red box, showing 'MAM SDK' selected and 'Legacy MDX' unselected. Other configuration options include:

- File name: Secure Mail
- App Description: Managed Enterprise Application
- App version: 20.4.5
- Minimum OS version: 11.0
- Maximum OS version: (empty)
- Excluded devices: example: manufacturer or model...
- Remove app if MDM profile is removed: ON
- Prevent app data backup: ON
- Force app to be managed: ON
- App deployed via Volume purchase: OFF

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

Secure Mail para iOS

Otimização de sincronização para caixa de correio No Secure Mail para iOS, a sincronização da

Caixa de correio foi aprimorada para proporcionar uma melhor experiência do usuário. O **Calendário** e os **Contatos** são sincronizados mais rapidamente. Emails com mais de 3 semanas são truncados para reduzir o tempo de sincronização. Você pode exibir o email completo ao abri-lo.

Secure Mail 20.7.5

Nota:

O suporte para Android 6.x terminou em 30 de junho de 2020.

Para obter as mais recentes informações sobre aplicativos móveis de produtividade, consulte o artigo [Anúncios recentes](#).

Secure Mail 20.7.0

Esta versão inclui correções de bugs.

Secure Mail 20.6.5

Esta versão inclui correções de bugs.

Secure Mail 20.6.0

Esta versão inclui correções de bugs.

Secure Mail 20.5.0

Esta versão inclui correções de bugs.

Secure Mail 20.4.5

Secure Mail para Android

A partir desta versão em diante, o Secure Mail inclui suporte para a Atualização cumulativa 5 do Exchange Server 2019 e Atualização cumulativa 16 do Exchange Server 2016

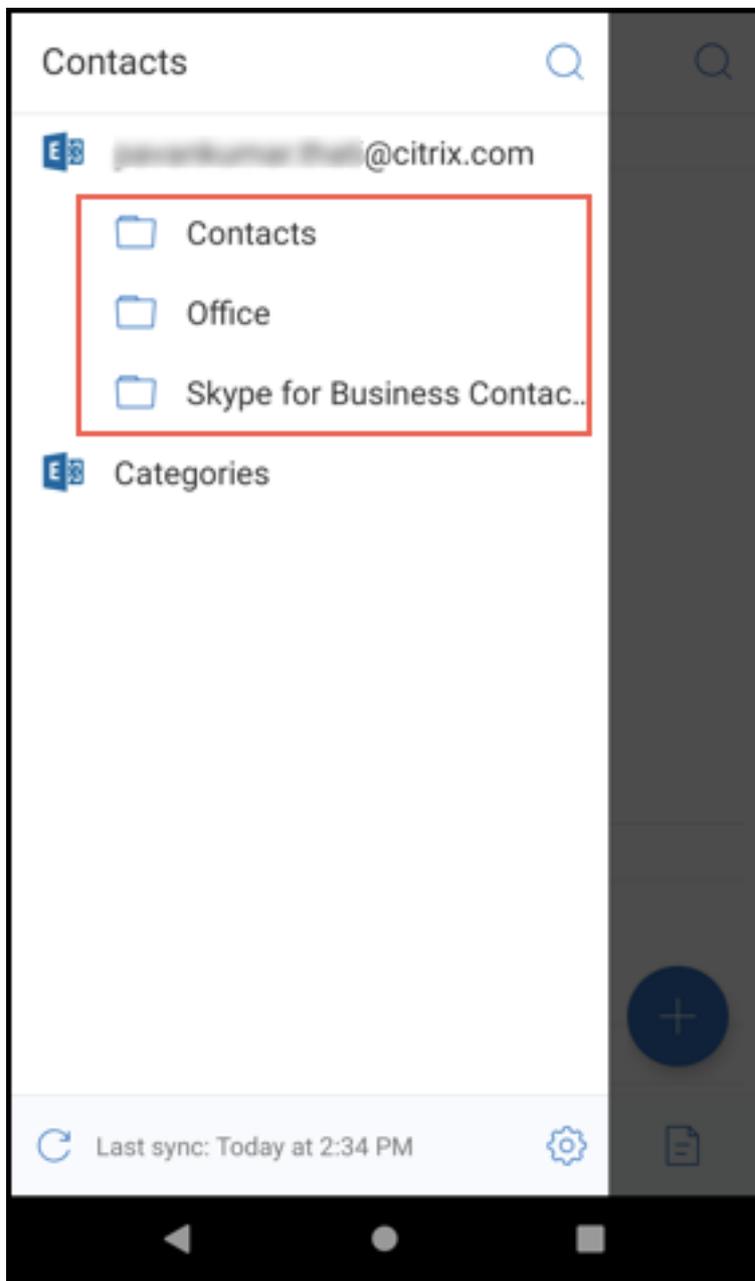
Secure Mail 20.4.0

A partir desta versão em diante, o Secure Mail inclui suporte para a Atualização cumulativa 15 do Exchange Server 2016 e Atualização cumulativa 23 do Exchange Server 2013

Secure Mail 20.3.0

Secure Mail para Android

Criar pastas em Contatos. No Secure Mail para Android, você pode adicionar, editar e excluir pastas na seção **Contatos** da sua conta de email.



Secure Mail para iOS

Esta versão inclui correções de bugs.

Secure Mail 20.2.0

Secure Mail para Android

Minimizar rascunhos

No Secure Mail para Android, você pode minimizar um rascunho enquanto estiver redigindo um e-mail e navegar dentro do aplicativo. Para obter a documentação de ajuda do usuário sobre esse recurso, consulte o artigo [Minimizar um rascunho de e-mail](#) no Centro de Ajuda ao Usuário Citrix.

Secure Mail 20.1.5

Secure Mail para iOS

A partir desta versão em diante, o Secure Mail inclui suporte para a Atualização cumulativa 4 do Exchange Server 2019.

Secure Mail para Android

- **Sincronização de contato bidirecional.** No Secure Mail para Android, você pode criar, editar e excluir contatos do Secure Mail da sua lista de contatos local.
- **Suporte para arquivos ICS.** No Secure Mail para Android, você pode visualizar os arquivos ICS que você recebe como anexos e importá-los para o seu calendário como Eventos.
- A partir desta versão em diante, o Secure Mail inclui suporte para a Atualização cumulativa 4 do Exchange Server 2019.

Secure Mail 20.1.0

A partir desta versão em diante, o Secure Mail inclui suporte para a Atualização cumulativa 14 do Exchange Server 2016

Secure Mail 19.12.5

Secure Mail para iOS

Esta versão inclui correções de bugs.

Secure Mail para Android

Desfazer o envio de emails. No Secure Mail para Android, você pode desfazer o envio de um email. Depois de tocar no botão **Enviar**, você recebe uma mensagem de notificação do sistema que permite

desfazer a ação de envio. Toque em **Desfazer** para reverter a ação de envio e editar a mensagem, os destinatários do email, anexar ou remover anexos ou descartar o email.

Sincronização de anexos na pasta Rascunhos. No Secure Mail para Android, quando a pasta **Rascunhos** é sincronizada, os anexos também são sincronizados e ficam disponíveis em todos os seus dispositivos. Esse recurso está disponível em dispositivos que executam o Exchange ActiveSync versão 16 ou posterior.

Secure Mail 19.11.5

Secure Mail para iOS

Imagem do contato no Secure Mail. No Secure Mail para iOS, visualize a imagem de um contato quando você adicionar destinatários a e-mails ou convites de reunião. Para obter a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Mostrar fotos de seus contatos](#).

Secure Mail para Android

Visualização dentro do aplicativo de arquivos PDF. No Secure Mail para Android, você pode visualizar arquivos PDF dentro do aplicativo, juntamente com indicadores e anotações. Também está disponível a visualização aprimorada de outros anexos do Microsoft Office.

Secure Mail para iOS 19.10.6

Esta versão inclui correções de bugs.

Secure Mail 19.10.5

Secure Mail para iOS

Minimizar rascunhos. No Secure Mail para iOS, você pode minimizar um rascunho enquanto estiver redigindo um e-mail e navegar dentro do aplicativo. Esse recurso está disponível em dispositivos que executam o iOS 13 e posterior. Para obter a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Minimizar um rascunho de e-mail](#).

Secure Mail para Android

Esta versão inclui correções de bugs.

Secure Mail 19.10.0

Use a política do Office 365 Exchange Server para definir o endereço do servidor do Office 365.

No Secure Mail iOS e Android, uma nova política chamada **Office 365 Exchange Server** é adicionada à seção **Suporte de OAuth para Office 365**. Com essa política, você pode definir o nome do host para a caixa de correio do Office 365 presente na nuvem. Essa política também habilita o suporte do Office 365 para agências governamentais. O nome do host é um valor único, como *outlook.office365.com*. O valor padrão é *outlook.office365.com*.

O Secure Mail iOS e Android suportam o gerenciamento de criptografia. O gerenciamento de criptografia permite que você use a segurança moderna da plataforma de dispositivos, ao mesmo tempo que garante que o dispositivo permaneça em um estado adequado para usar a segurança da plataforma de forma eficaz. Usando o gerenciamento de criptografia, você elimina a redundância de criptografia de dados local, uma vez que a criptografia do sistema de arquivos é fornecida pela plataforma iOS ou Android. Para habilitar esse recurso, um administrador deve configurar a política MDX de **Tipo de criptografia** como **Criptografia de plataforma com imposição de conformidade** no console Citrix Endpoint Management.

Para usar o recurso de gerenciamento de criptografia, no console Citrix Endpoint Management, defina a política de **Tipo de criptografia** como **Criptografia de plataforma com imposição de conformidade**. Isso habilita o gerenciamento de criptografia, e todos os dados dos aplicativos criptografados existentes nos dispositivos dos usuários fazem a transição para um estado, que é criptografado pelo dispositivo e não pelo MDX. Durante essa transição, o aplicativo é pausado para uma migração de dados única. Após a migração bem-sucedida, a responsabilidade pela criptografia de dados armazenados localmente é transferida do MDX para a plataforma do dispositivo. O MDX continua a verificar a conformidade do dispositivo após cada inicialização do aplicativo. Esse recurso funciona em ambientes MDM + MAM e apenas MAM.

Quando você define a política de **Tipo de criptografia** como **Criptografia de plataforma com imposição de conformidade**, a nova política substitui a sua criptografia MDX existente.

Para obter detalhes sobre as políticas MDX de gerenciamento de criptografia para Secure Mail, consulte a seção **Criptografia** em:

- [Políticas de MDX para aplicativos móveis de produtividade para Android](#)
- [Políticas de MDX para aplicativos móveis de produtividade para iOS](#)

Quando um dispositivo fica abaixo dos requisitos mínimos de conformidade, a política de **Comportamento do dispositivo não compatível** permite que você selecione qual ação será executada:

- **Permitir aplicativo** — Permite que o aplicativo seja executado normalmente.
- **Permitir aplicativo após aviso** — Avisa ao usuário que um aplicativo não atende aos requisitos mínimos de conformidade e permite que o aplicativo seja executado. Este é o valor padrão.
- **Bloquear aplicativo** — Bloqueia a execução do aplicativo.

Dispositivos que executam o iOS

Os critérios a seguir determinam se um dispositivo atende aos requisitos mínimos de conformidade para dispositivos com iOS:

- iOS 10 - Um aplicativo está executando uma versão do sistema operacional que é maior ou igual à versão especificada.
- Acesso ao depurador - Um aplicativo não tem a depuração habilitada.
- Dispositivo com jailbroken - Um aplicativo não está sendo executado em um dispositivo com jailbroken.
- Código secreto do dispositivo - O código secreto do dispositivo está **ON**.
- Compartilhamento de dados - O compartilhamento de dados não está habilitado para o aplicativo.

Dispositivos que executam o Android

Os critérios a seguir determinam se um dispositivo atende aos requisitos mínimos de conformidade para dispositivos com Android:

- Android SDK 24 (Android 7 Nougat) - um aplicativo está executando uma versão do sistema operacional que é maior ou igual à versão especificada.
- Acesso ao depurador - Um aplicativo não tem a depuração habilitada.
- Dispositivos com root - Um aplicativo não está sendo executado em um dispositivo com root.
- Bloqueio do dispositivo - O código secreto do dispositivo está **ON**.
- Dispositivo criptografado - Um aplicativo está sendo executado em um dispositivo criptografado.

Secure Mail 19.9.5

Secure Mail para iOS

Suporte para arquivos ICS. No Secure Mail para iOS, você pode importar os arquivos ICS recebidos como anexos para o seu calendário como um evento.

Secure Mail para Android

Esta versão inclui correções de bugs.

Secure Mail 19.9.0

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

- Atualização cumulativa 13 do Exchange Server 2016

- IBM Lotus Notes Traveler versão 10.0.1.0 compilação 201811191126_20
- Servidor de email IBM Domino versão 10.0.1

Secure Mail para iOS

- O Secure Mail para iOS suporta iOS 13.
- **Denunciar e-mails de phishing com cabeçalhos MIME.** No Secure Mail para iOS, 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 MIME 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 um e-mail de phishing como um anexo](#).
- **Suporte para emails responsivos.** O Secure Mail para iOS foi otimizado para entregar e-mails responsivos. Anteriormente, o conteúdo de e-mail com grandes tabelas ou imagens era renderizado incorretamente. Este recurso fornece conteúdo de e-mail mais legível em todos os dispositivos suportados, independentemente do formato e tamanho do e-mail.
- **Arrastar e soltar eventos de calendário.** No Secure Mail para iOS, você pode alterar a hora de um evento de calendário existindo arrastando e soltando o evento. Arraste o evento e solte-o no intervalo de tempo desejado, no mesmo dia ou em outros dias, para atualizar.
- **Avanço automático.** No Secure Mail para iOS, quando você exclui uma mensagem em **Conversas**, você pode escolher para qual mensagem retornar. Para usar esse recurso, navegue até **Configurações > Avanço automático**. Em seguida, selecione sua preferência nas opções disponíveis. Para obter a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Excluir e avançar automaticamente para um e-mail em Conversas](#).
- **Suporte para WKWebView.** O Secure Mail para iOS suporta WKWebView. Esse recurso melhora a maneira como os e-mail e eventos de calendário do Secure Mail são renderizados no seu dispositivo.

Secure Mail para Android

A partir desta versão, o Secure Mail para Android só é suportado em dispositivos que executam o Android 6 ou posterior.

Secure Mail para Android 19.8.5

Esta versão inclui correções de bugs.

Secure Mail 19.8.0

Secure Mail para iOS

Esta versão inclui melhorias de desempenho e correções de bugs.

Secure Mail para Android

- Suporte para Android Q.
- **Suporte para aplicativos de 64 bits para o Google Play.** O Secure Mail para Android suporta arquiteturas de 64 bits.
- **Melhorias na IU Puxe para Atualizar no Secure Mail para Android.** Para mantermos a conformidade com as diretrizes de Material Design, fizemos pequenas melhorias no recurso **Puxe para atualizar**. O carimbo de data/hora de sincronização está disponível na parte inferior da tela quando você toca no ícone do hambúrguer.

Secure Mail 19.7.5

Secure Mail para iOS

- **Sincronização automática da pasta Rascunhos** No Secure Mail para iOS, a pasta de rascunhos é sincronizada automaticamente e seus rascunhos ficam disponíveis em todos os seus dispositivos. Esse recurso está disponível em configurações que executam o Exchange ActiveSync v16 ou posterior. Para obter a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Sincronização automática da pasta Rascunhos](#).
- **O Secure Mail para Android oferece suporte a logon único quando você usa o Microsoft Intune no modo MDM + MAM.** Para poder usar esse recurso, confirme que o aplicativo Microsoft Authenticator está instalado no seu dispositivo. Para obter mais informações sobre como instalar o aplicativo Microsoft Authenticator, consulte **Download and install the Microsoft Authenticator** em *Docs.microsoft.com*.

Secure Mail para Android

Nota:

A Citrix recomenda que você atualize para o Secure Mail versão 19.7.5 antes de atualizar seu sistema operacional para o Android Q.

- **Use a política para encapsulamento com o SSO da Web para configurações executando a autenticação moderna com o Microsoft Office 365.** No Secure Mail para Android, uma nova política chamada **Usar o SSO da Web para encapsulamento** é adicionada. Com essa política, você pode encapsular o tráfego OAuth para passar por Com túnel – SSO de Web. Para isso:
 - Defina a política **Usar o SSO da Web para encapsulamento** como **Ativado**.

- Na política de acesso à rede, selecione a opção **Com túnel - SSO de Web**.
- Exclua os nomes de host relacionados ao OAuth da política de **Serviços em segundo plano**.
- **O Secure Mail para Android oferece suporte ao logon único quando você está usando o Microsoft Intune no modo MDM + MAM.** Para poder usar esse recurso, verifique se o aplicativo Portal da Empresa do Intune está instalado em seu dispositivo. Depois de fazer login no aplicativo Portal da Empresa do Intune, você poderá usar o SSO no modo MDM + MAM sem precisar autenticar novamente no Secure Mail usando suas credenciais.

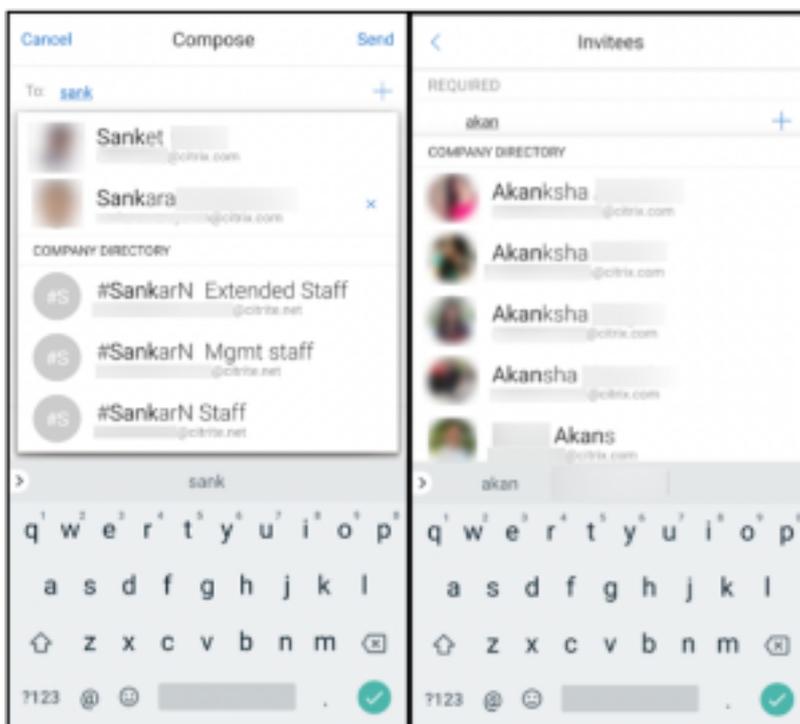
Secure Mail 19.6.5

Secure Mail para iOS

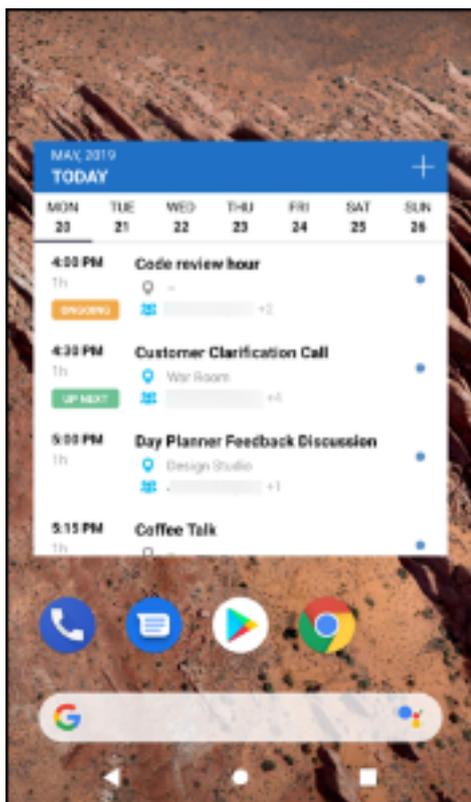
A versão 19.6.5 do Secure Mail para iOS inclui melhorias de desempenho e correções de bugs. Para obter a lista de problemas corrigidos e conhecidos, consulte [Problemas conhecidos e corrigidos](#).

Secure Mail para Android

- **Arrastar e soltar eventos de calendário.** No Secure Mail para Android, você pode alterar a hora de um evento de calendário existente arrastando e soltando o evento. Para obter a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Alterar o horário de um evento de calendário](#).
- **Suporte para emails responsivos.** O Secure Mail para Android foi otimizado para entregar e-mails responsivos. Anteriormente, o conteúdo de e-mail com grandes tabelas ou imagens era renderizado incorretamente. Este recurso fornece conteúdo de e-mail mais legível em todos os dispositivos suportados, independentemente do formato e tamanho do e-mail.
- **Imagem do contato no Secure Mail.** No Secure Mail para Android, visualize a imagem do contato quando você adicionar destinatários a e-mails ou convites de reunião. A imagem do contato é exibida ao lado do nome. Se houver várias pessoas com o mesmo nome, a imagem ajuda a identificar o destinatário correto quando você adiciona destinatários a e-mails ou convites de reunião. Para procurar contatos que não estão salvos localmente, insira um mínimo de quatro caracteres do nome do destinatário para exibir a imagem.



- **Widget para a agenda do Calendário.** No Secure Mail para Android, a agenda do **Calendário** está disponível como um widget. Neste widget, você pode visualizar os próximos eventos no **Calendário** para uma semana. Esse recurso permite que você crie um evento de **Calendário**, visualize um evento existente e edite os detalhes. A política **Bloquear captura de tela** não se aplica ao widget encontrado na tela inicial. No entanto, você pode desativar o widget usando a política **Permitir widget de agenda do calendário**.



Secure Mail 19.5.5

Secure Mail para Android

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 corrigidos](#).

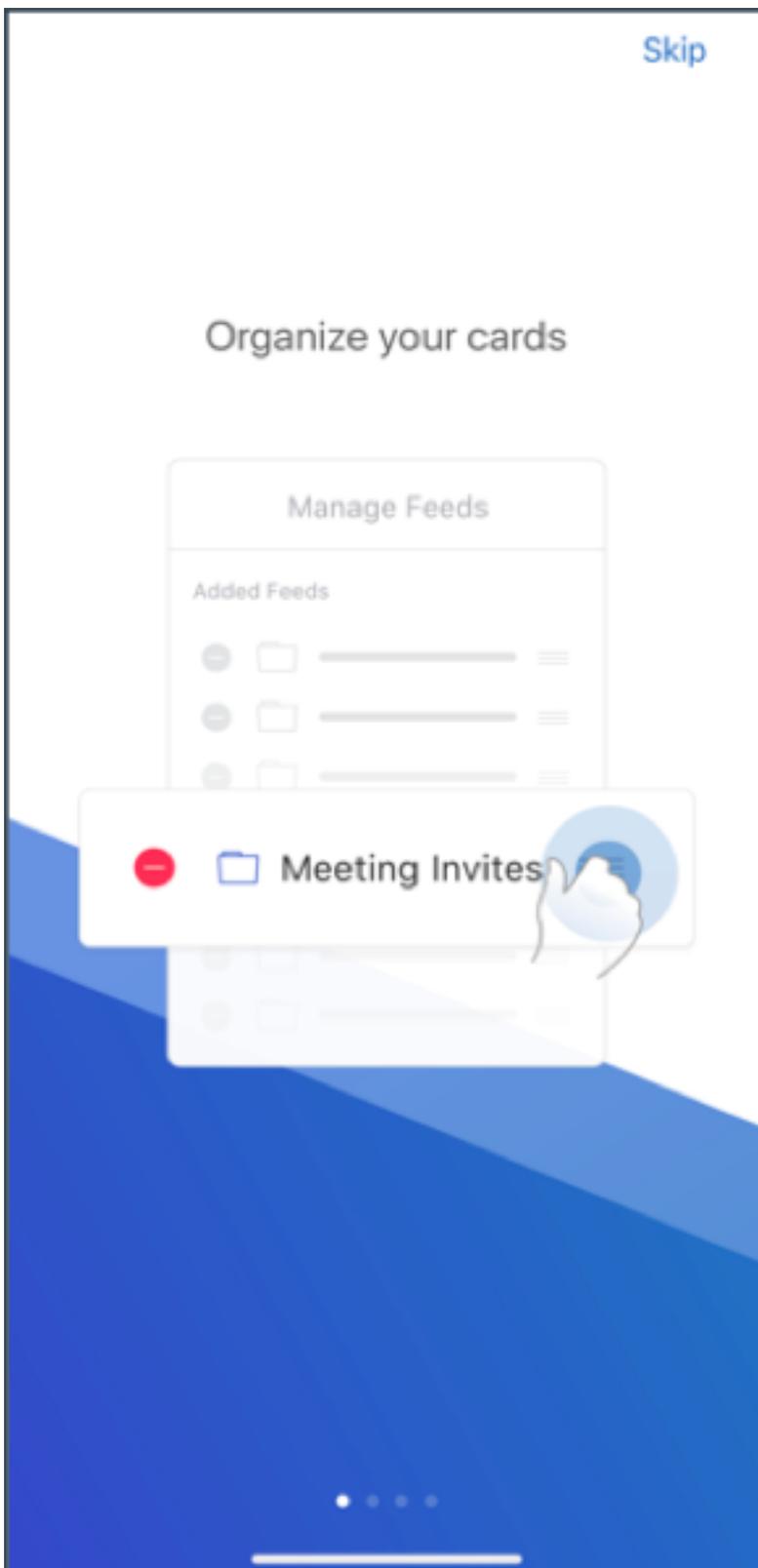
Secure Mail para iOS

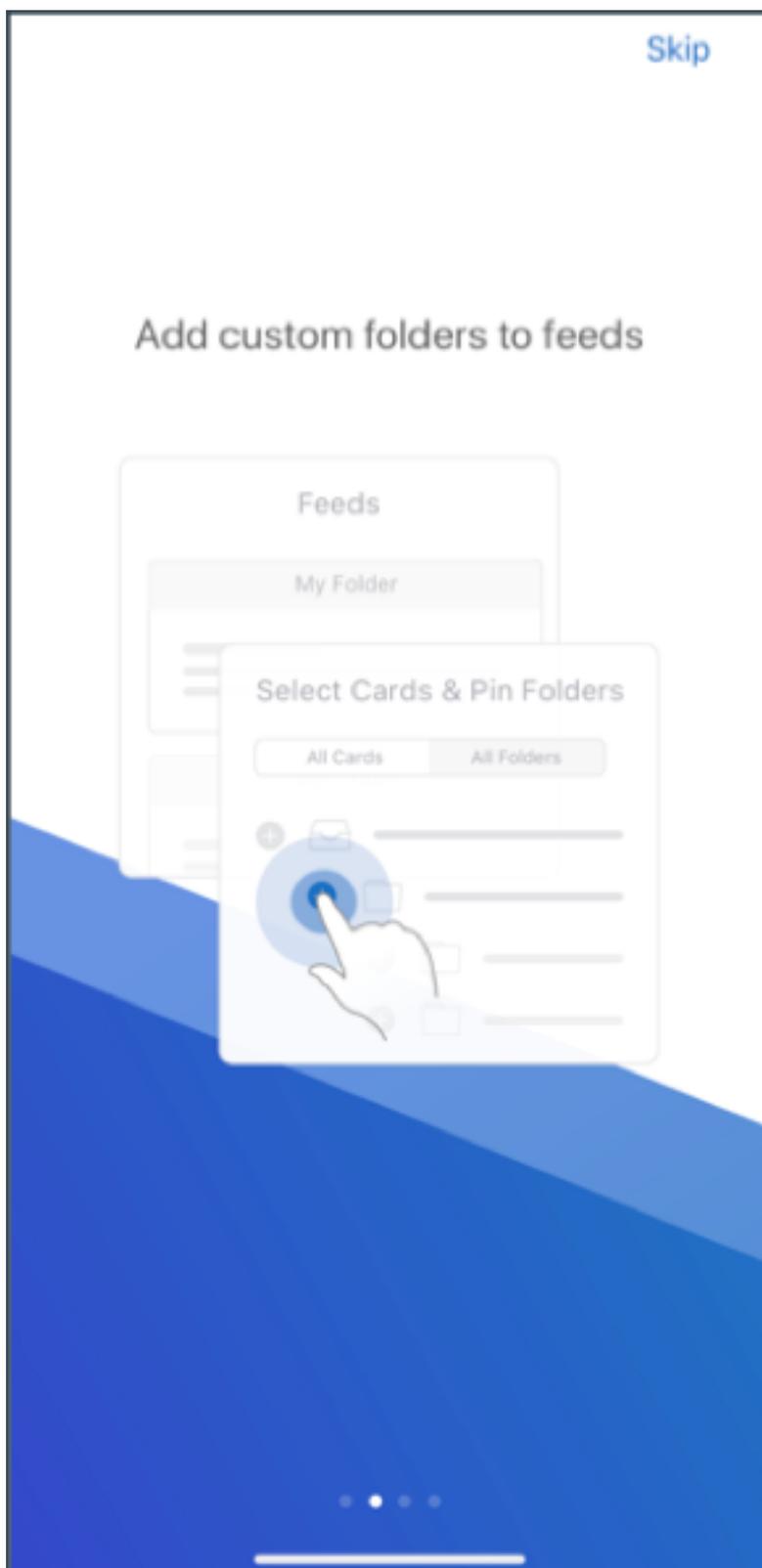
- O Secure Mail para Android oferece suporte a logon único quando você usa o Microsoft Intune no modo MDM + MAM. Para poder usar esse recurso, confirme que o aplicativo Microsoft Authenticator está instalado no seu dispositivo. O aplicativo Microsoft Authenticator está disponível nas lojas de aplicativos.
- **Suporte para Slack EMM:** o Slack EMM é para clientes Slack com o Enterprise Mobility Management (EMM) habilitado. O Secure Mail para iOS suporta o aplicativo **Slack EMM**, que permite que os administradores escolham a integração do Secure Mail com o aplicativo **Slack** ou com o aplicativo **Slack EMM**.

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 a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [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 corrigidos](#).

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

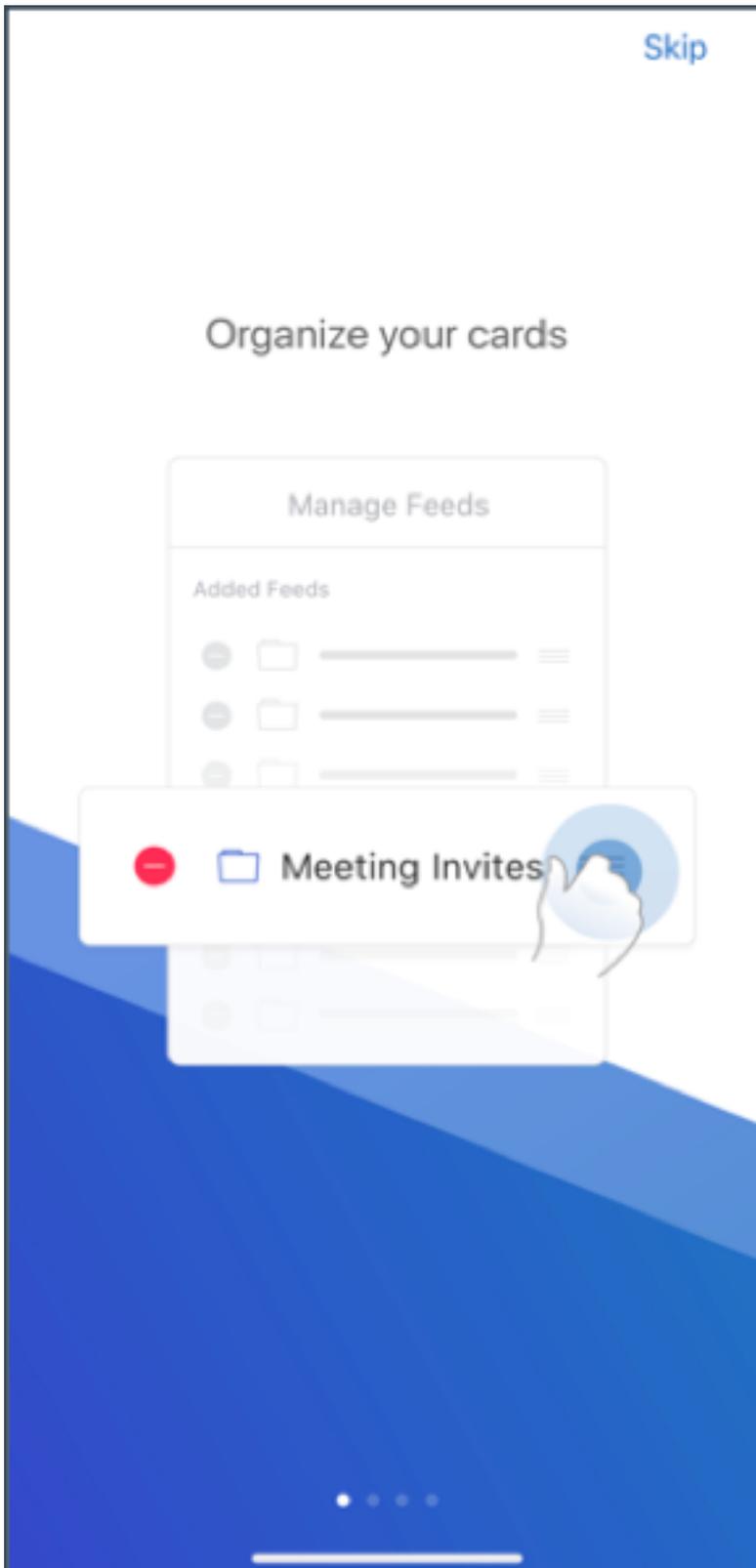
Para obter mais informações sobre a lista completa de compatibilidade de servidores com o Secure Mail, consulte [Visão geral do Secure Mail](#).

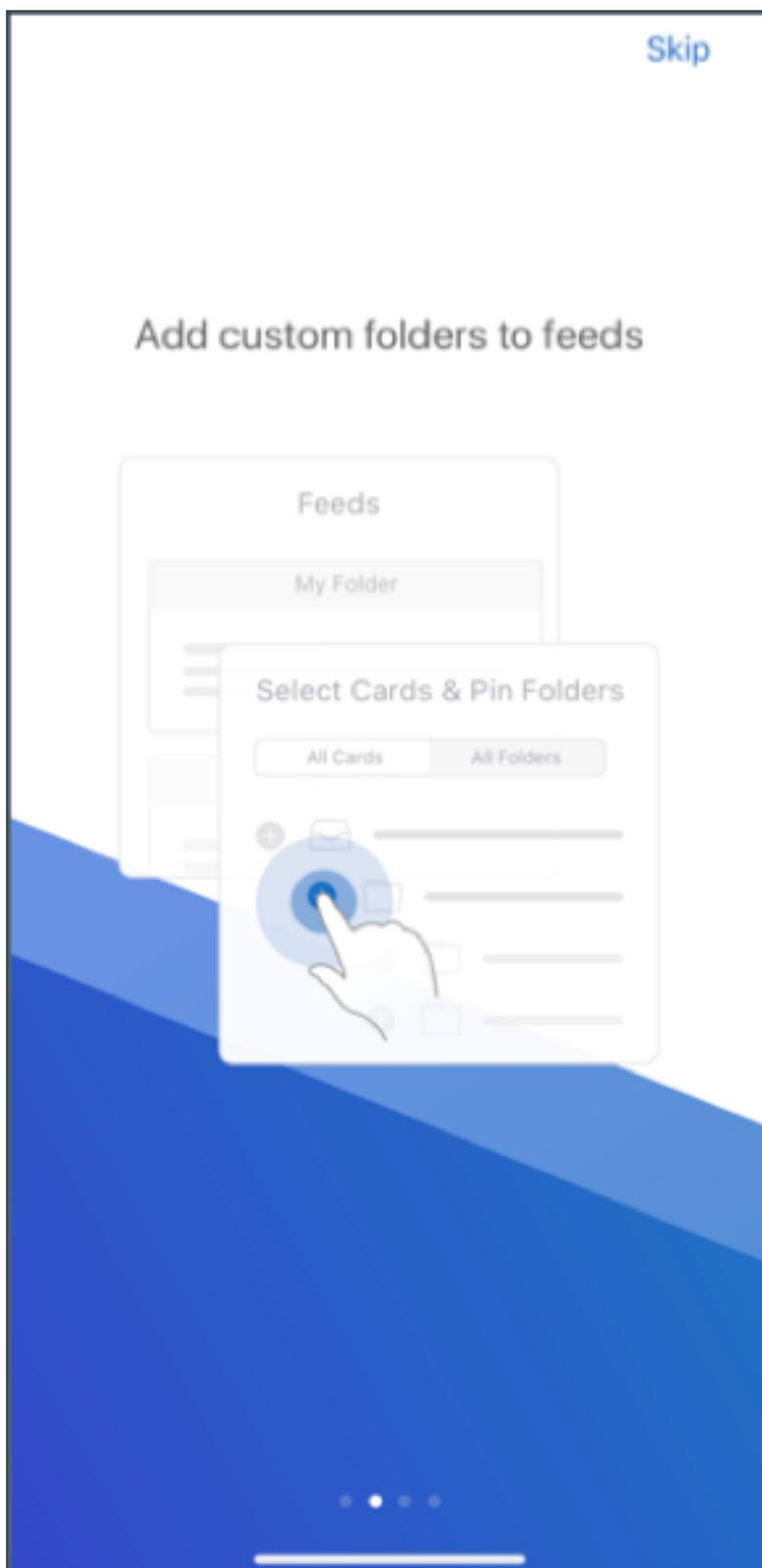
Secure Mail para iOS

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.



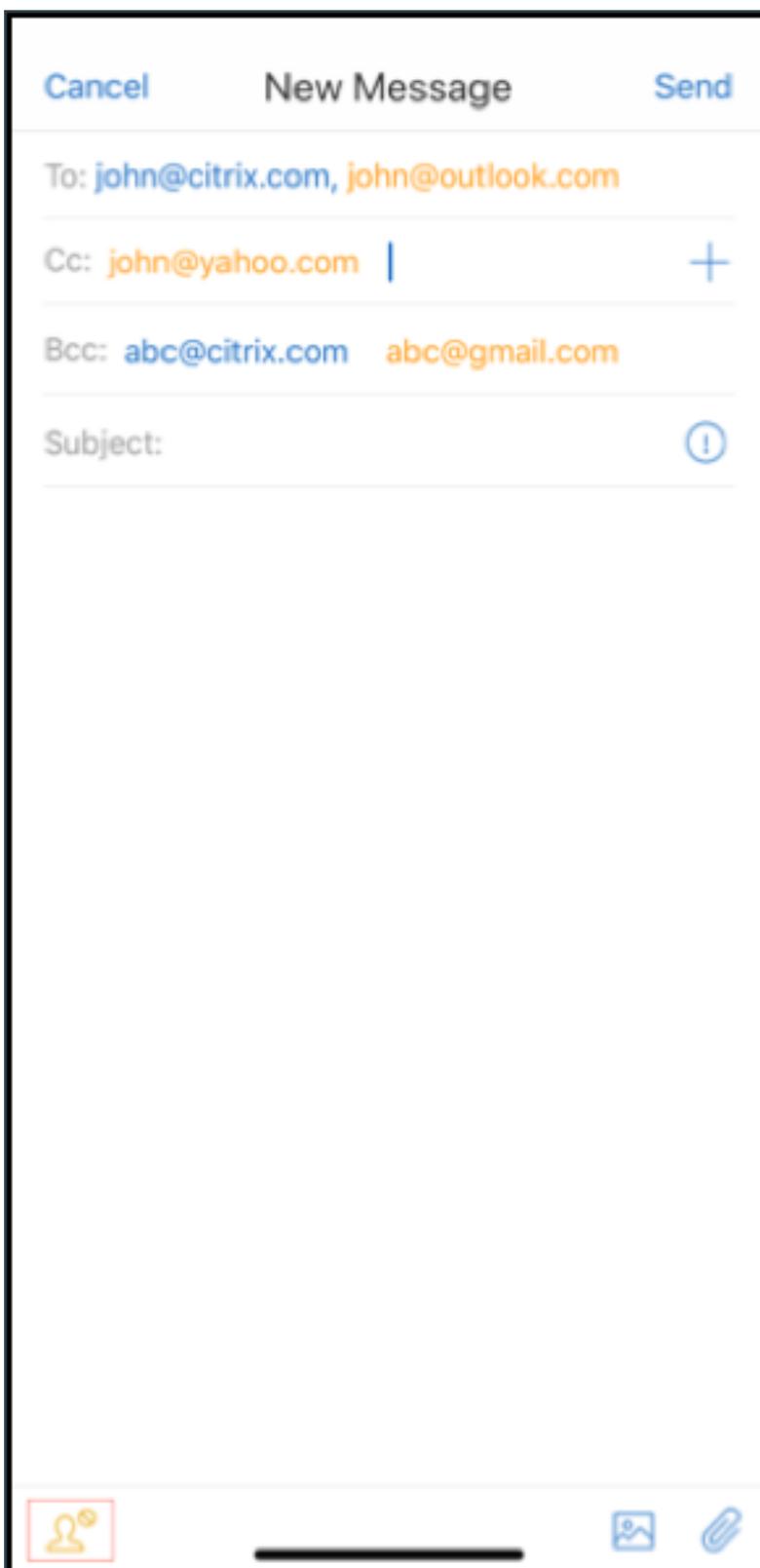


Para obter mais informações sobre como gerenciar seus feeds, consulte [Gerenciar seus feeds](#).

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.

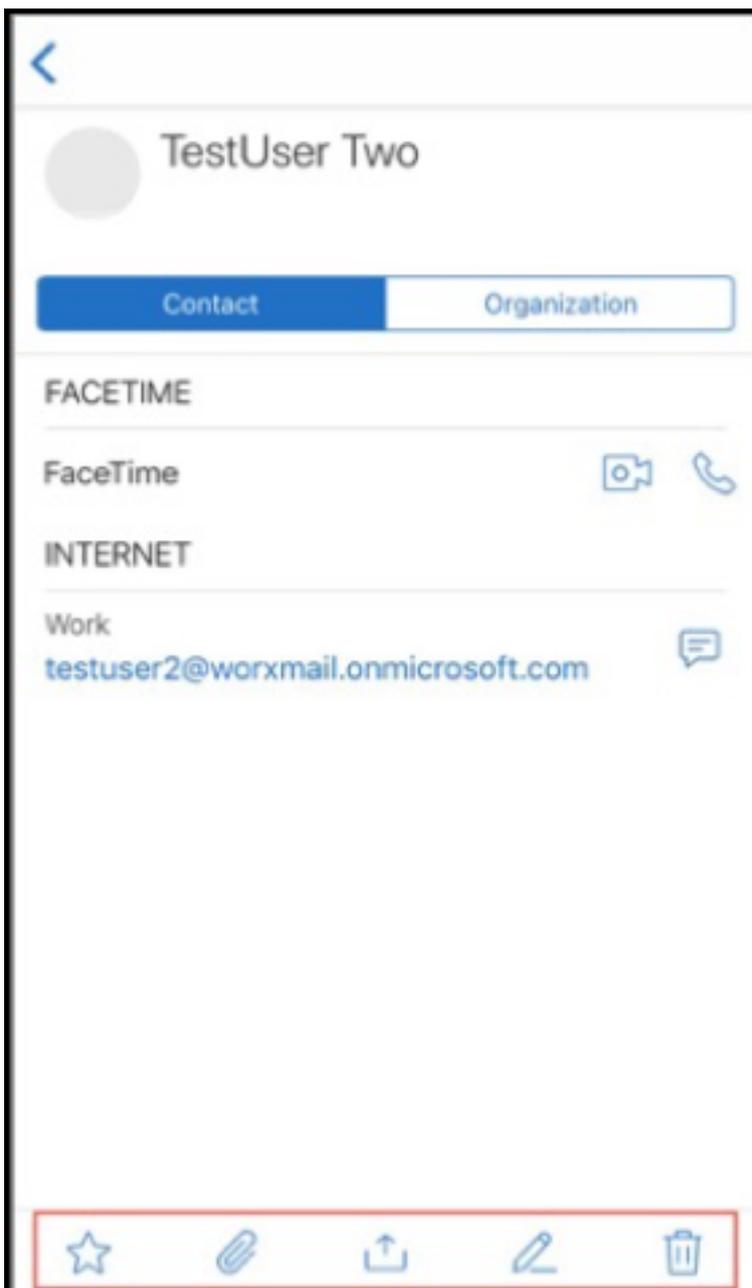


Para obter mais informações sobre domínios internos, consulte [Domínios internos](#).

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

Esta versão inclui melhorias de desempenho e correções de bugs.

Para obter a lista de problemas corrigidos e conhecidos, consulte [Problemas conhecidos e corrigidos](#).

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**
 - **Delete**

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 usando Com túnel - SSO de Web e Secure Ticket Authority (STA) em paralelo. Você também pode permitir conexões Com túnel - SSO de Web 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 sobre como [Adicionar um aplicativo 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 Android, 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

Esta versão inclui melhorias de desempenho e correções de bugs.

Para obter a lista de problemas corrigidos e conhecidos, consulte [Problemas conhecidos e corrigidos](#).

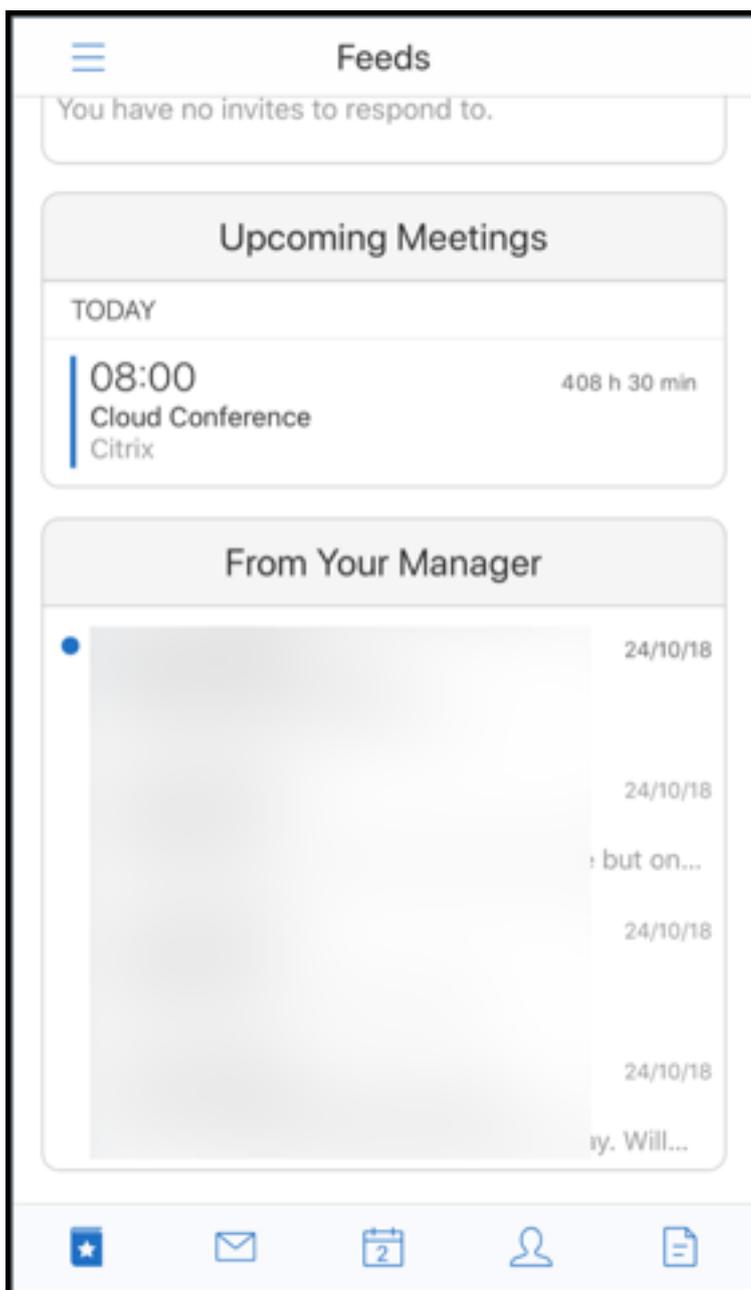
Secure Mail 18.11.5

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 sobre como configurar políticas MDX para o Secure Mail, consulte [Políticas de MDX para aplicativos móveis de produtividade](#).

- **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 push baseadas em FCM, consulte [Notificações por push para 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 Knowledge Center de suporte](#).

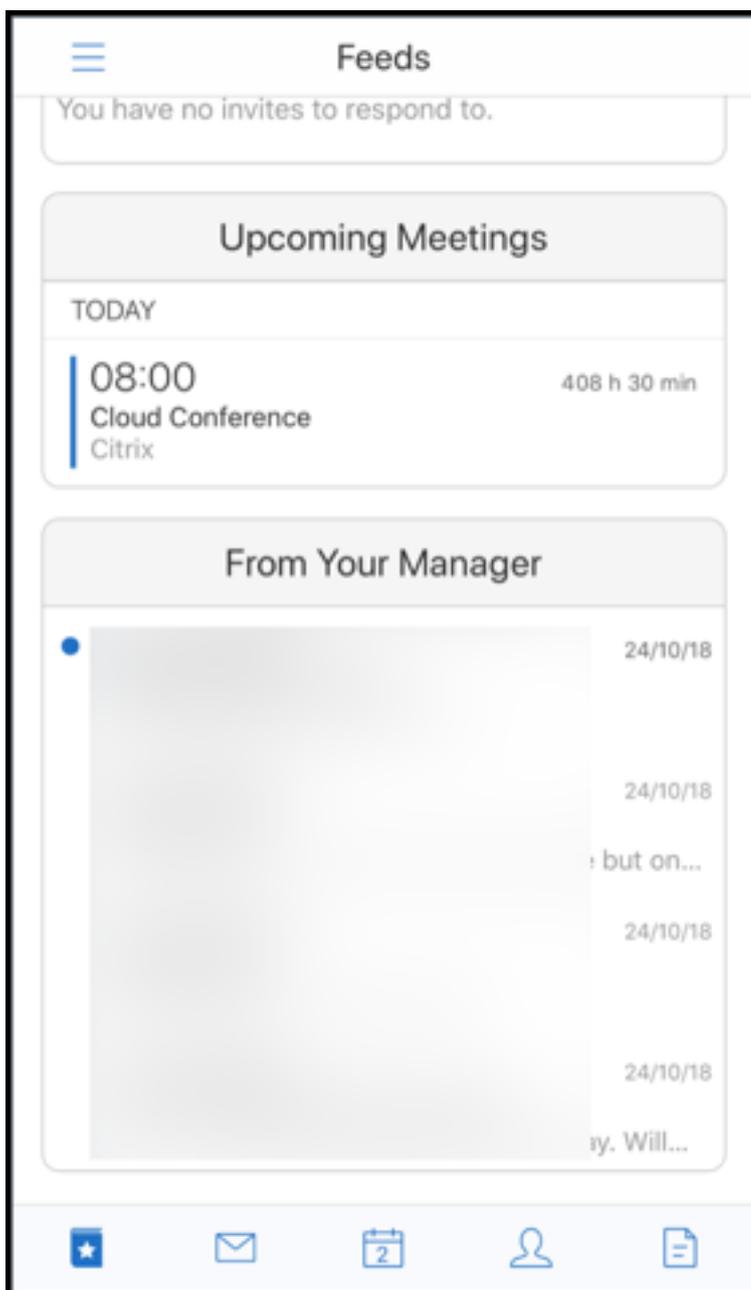
Limitações:

- 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 as Mensagens de falha na notificação por push no Secure Mail para iOS, consulte [Mensagens de falha na 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 (Preview):** 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 a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Denunciar um e-mail de phishing](#).

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 a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Denunciar um e-mail de phishing](#).
- **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, identifique as chamadas recebidas de seus contatos 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 do 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 Files nativo do iOS. Para detalhes, consulte [Recursos do iOS](#).

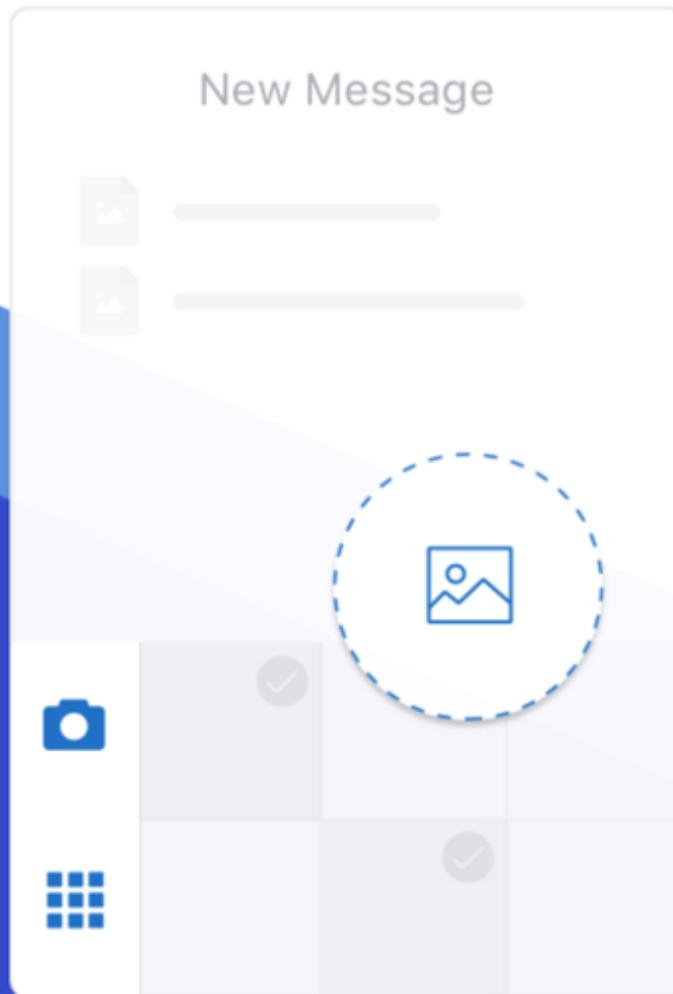
Secure Mail 10.8.55

Não há novos recursos no Secure Mail versão 10.8.55. Quanto aos problemas corrigidos, consulte [Problemas conhecidos e corrigidos](#).

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.

Attach multiple photos more easily



[Enter Secure Mail](#)

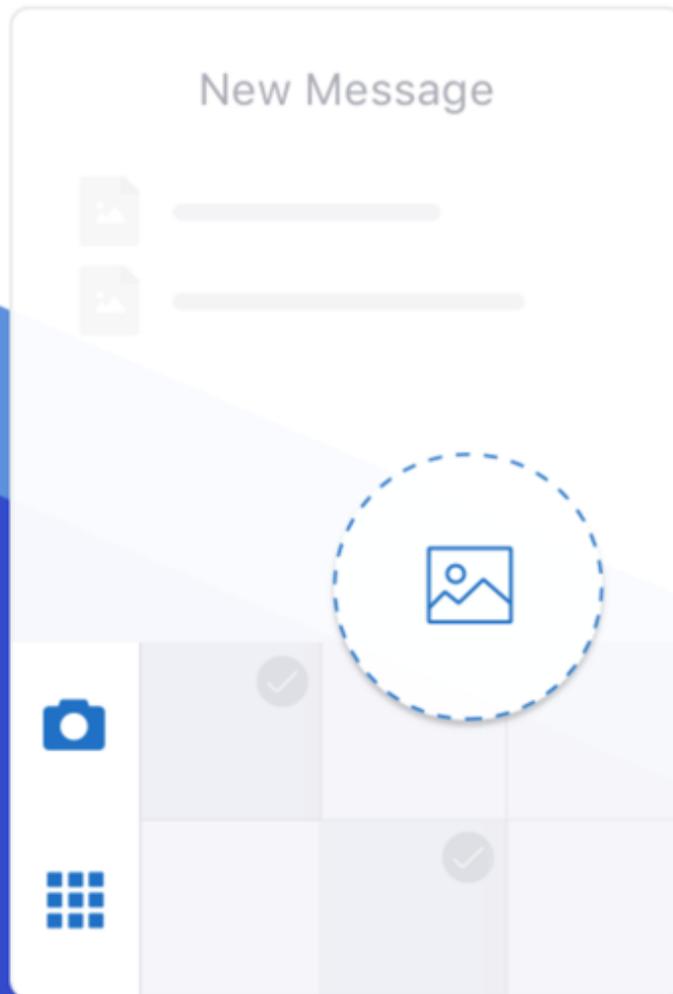
Tela de feeds do Secure Mail. O Secure Mail para iOS e Android apresenta todos os seus e-mails não lidos, convites para reuniões que exigem sua atenção e suas próximas reuniões na tela **Feeds**.

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.

Attach multiple photos more easily



[Enter Secure Mail](#)

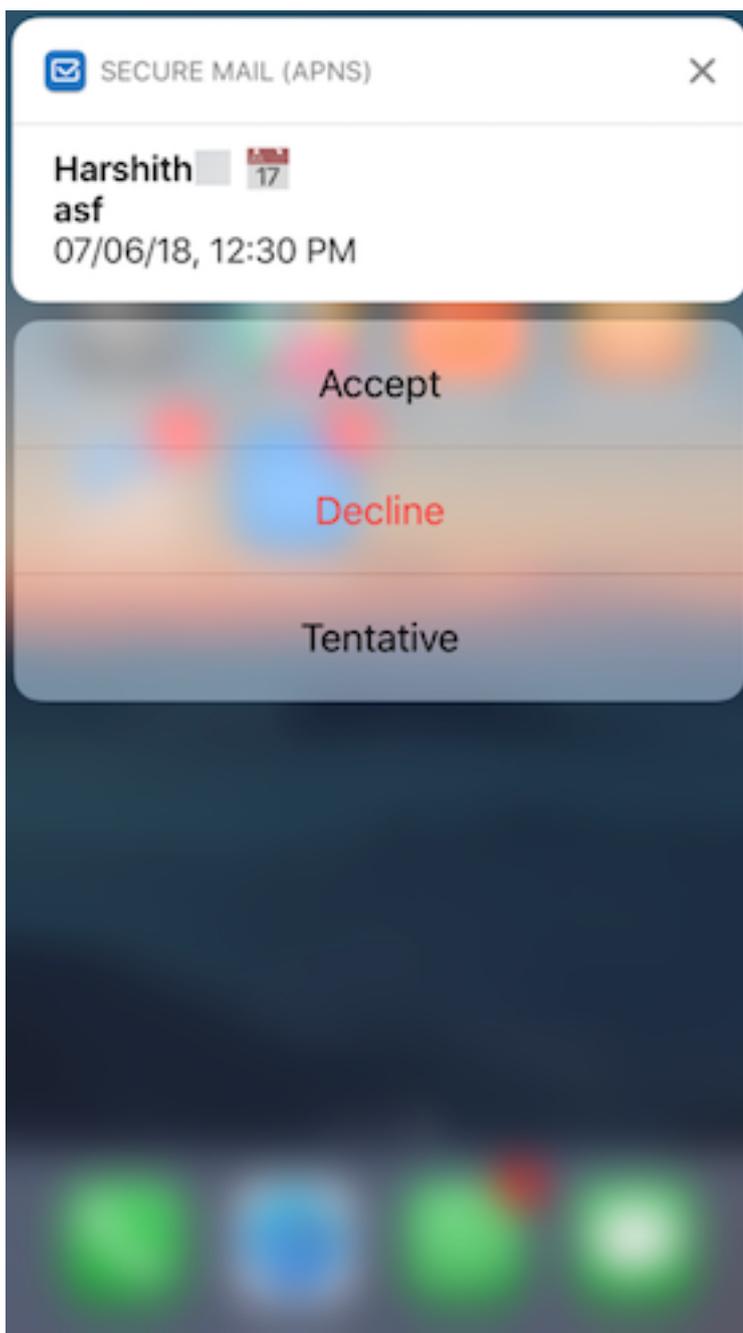
Secure Mail 10.8.40

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

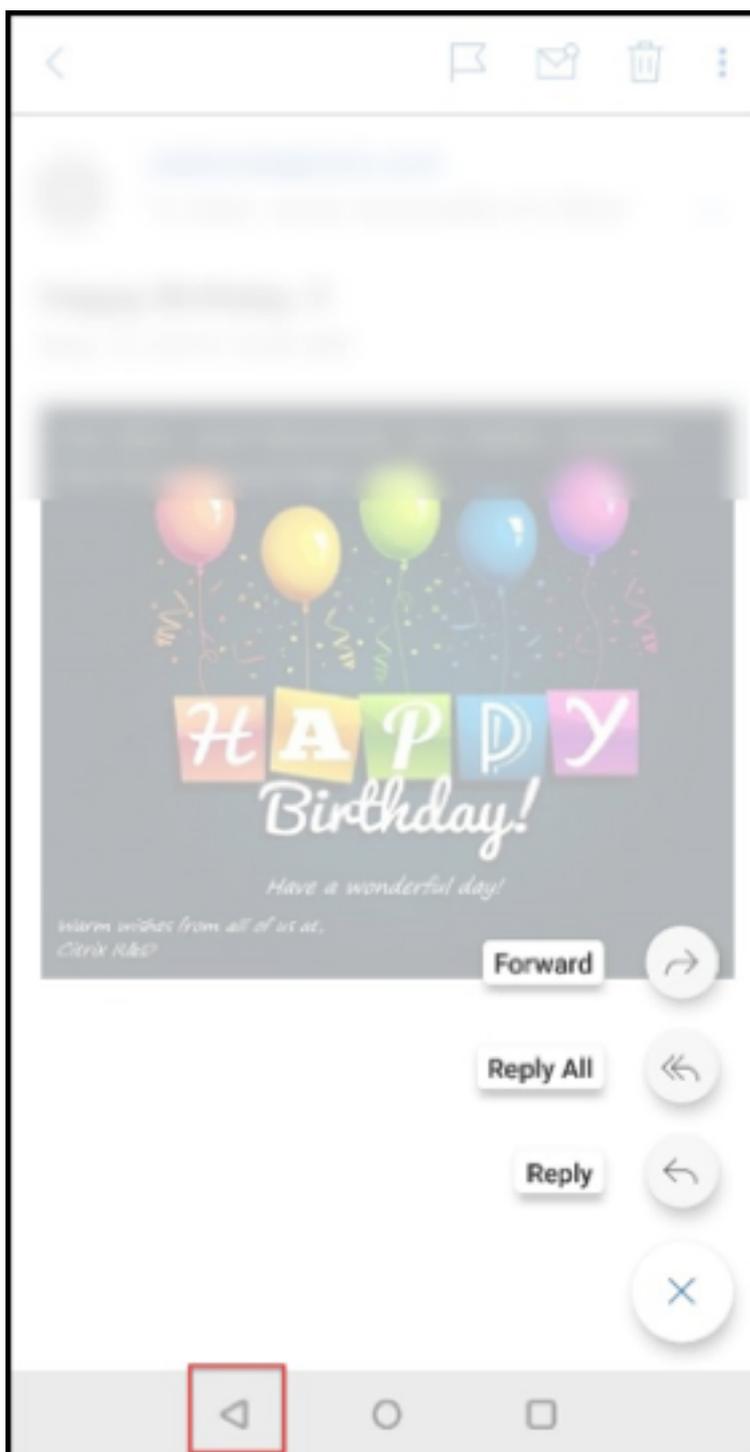
Secure Mail 10.8.35

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.

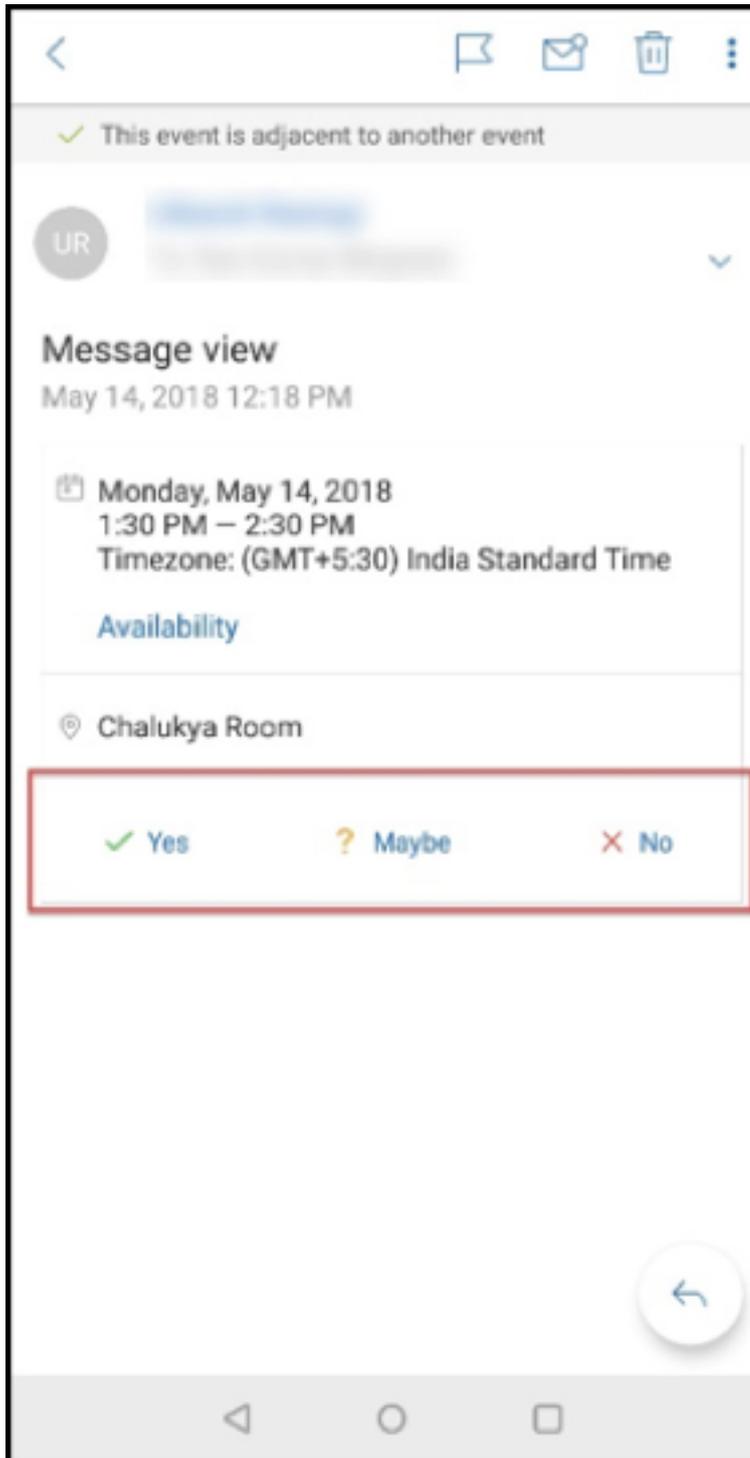


- **Aprimoramentos no botão de voltar do Secure Mail para Android** No Secure Mail para Android, você pode tocar no botão de voltar em seu dispositivo para descartar as opções expandidas do botão de ação flutuante. Se o Botão de Ação Flutuante estiver no estado expandido, se você tocar no botão de voltar 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

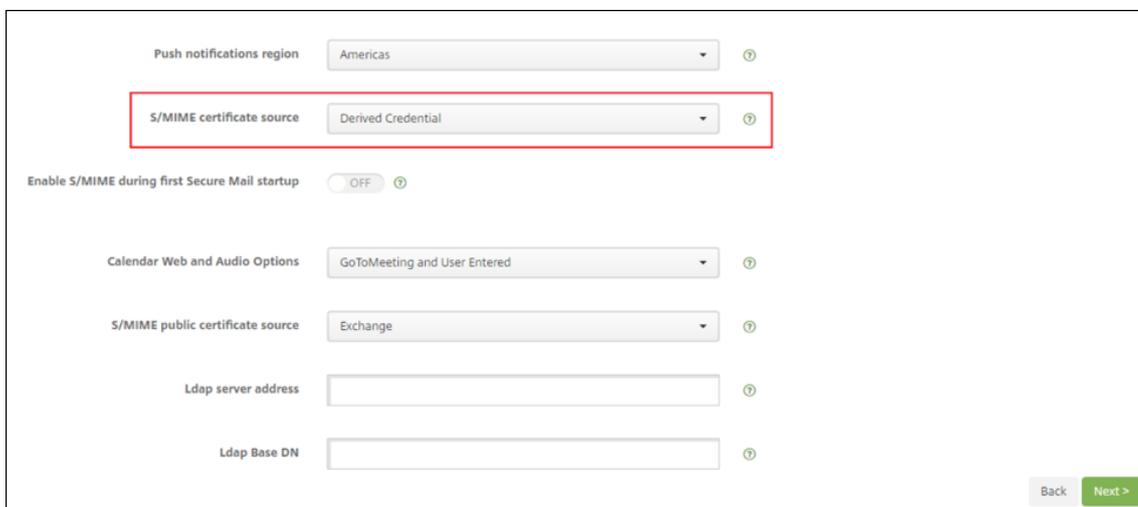
O Secure Mail para iOS agora suporta S/MIME para credenciais derivadas: Para que esse recurso funcione, você precisa fazer o seguinte:

- Selecione Credencial Derivada como a origem do certificado S/MIME. Para obter detalhes, consulte [Credenciais derivadas para 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 estas [Propriedades do cliente](#), e para o Endpoint Management consulte estas [Propriedades do cliente](#).

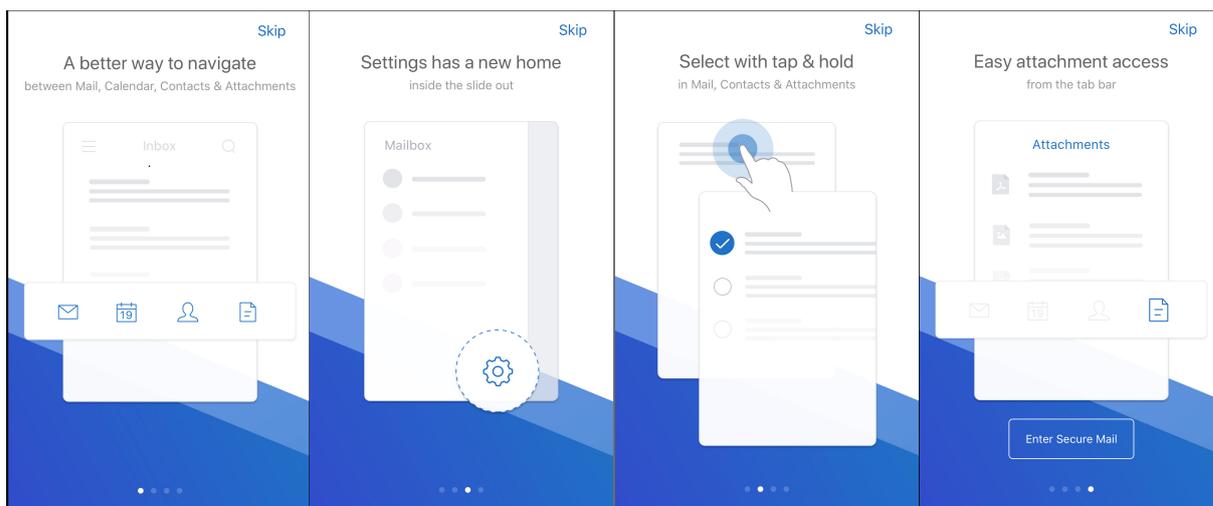
Para obter informações sobre como os dispositivos se registram usando credenciais derivadas, consulte [Registrar dispositivos usando credenciais derivadas](#).

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**.

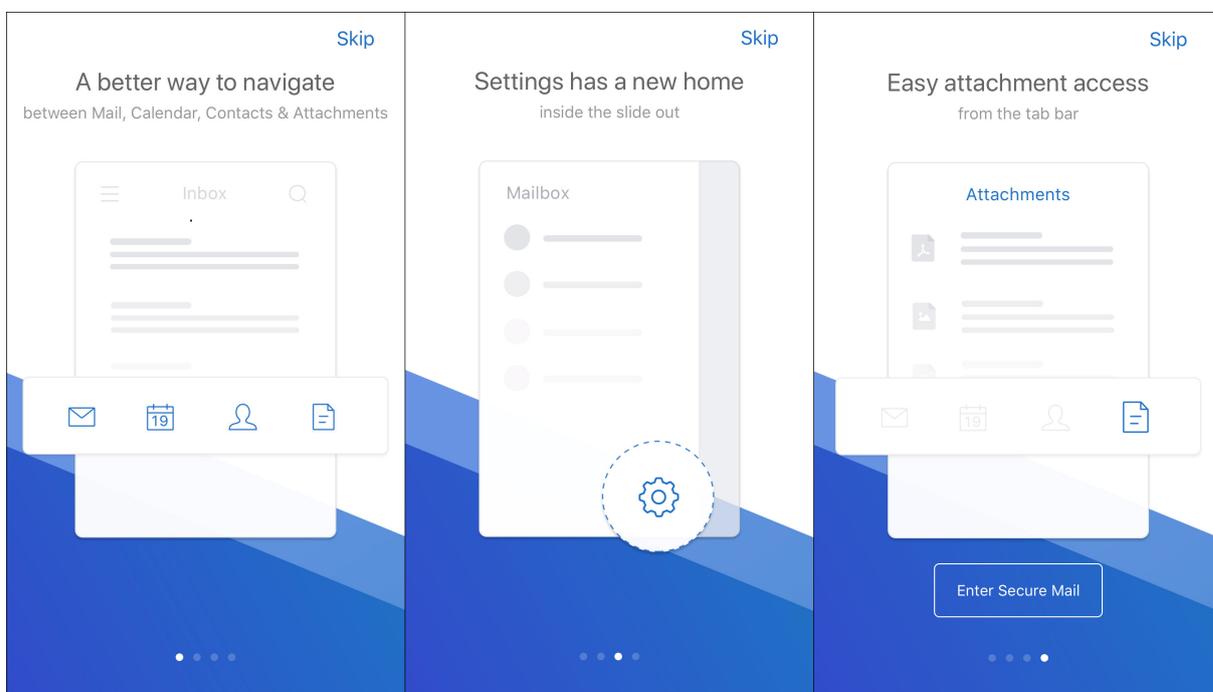


O Secure Mail para iOS e Android tem uma nova aparência: tornamos a navegação do usuário mais simples e eficiente. Nós realinhamos o menu e os botões de ação na forma de uma barra de navegação.

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

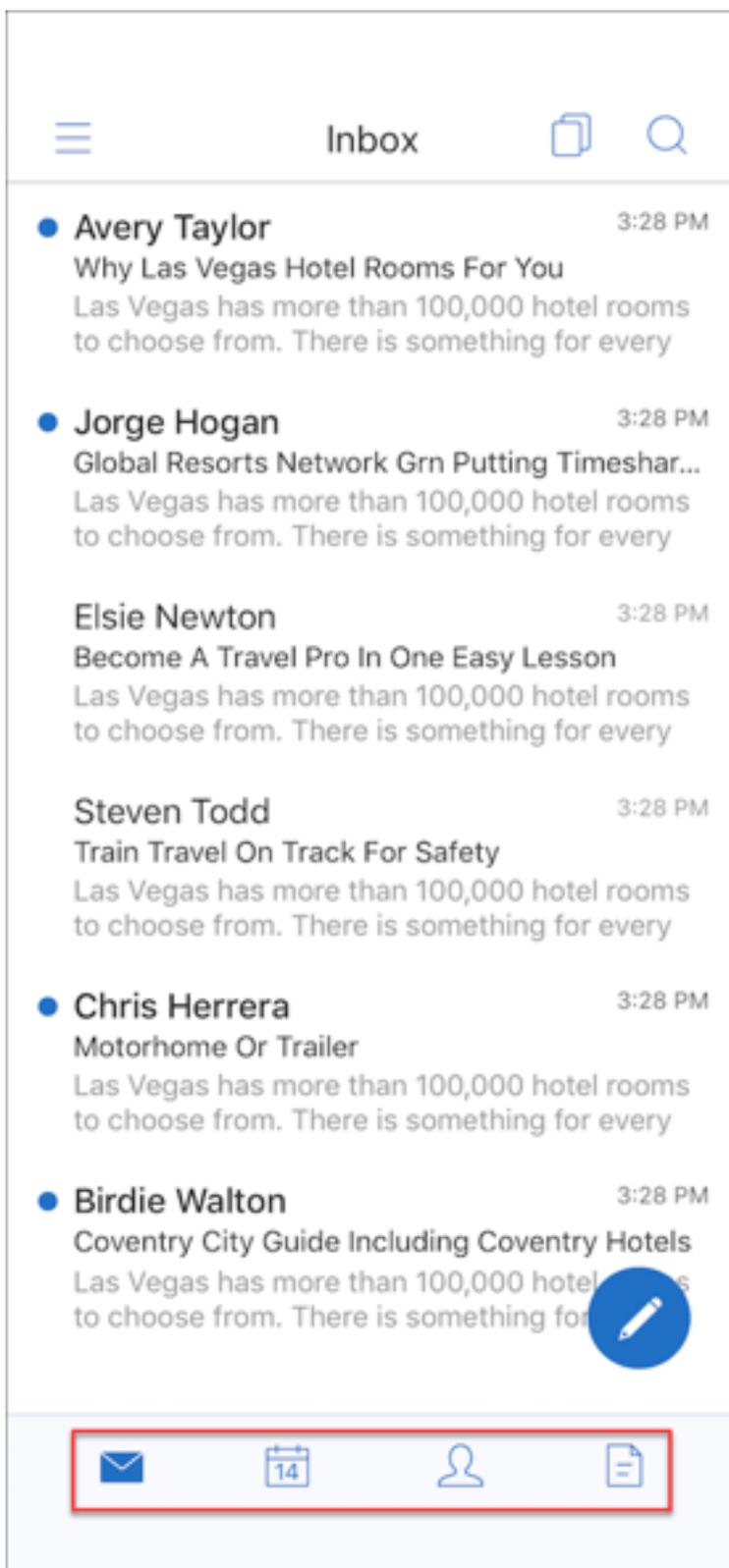


A figura a seguir mostra a nova barra de navegação em dispositivos Android.



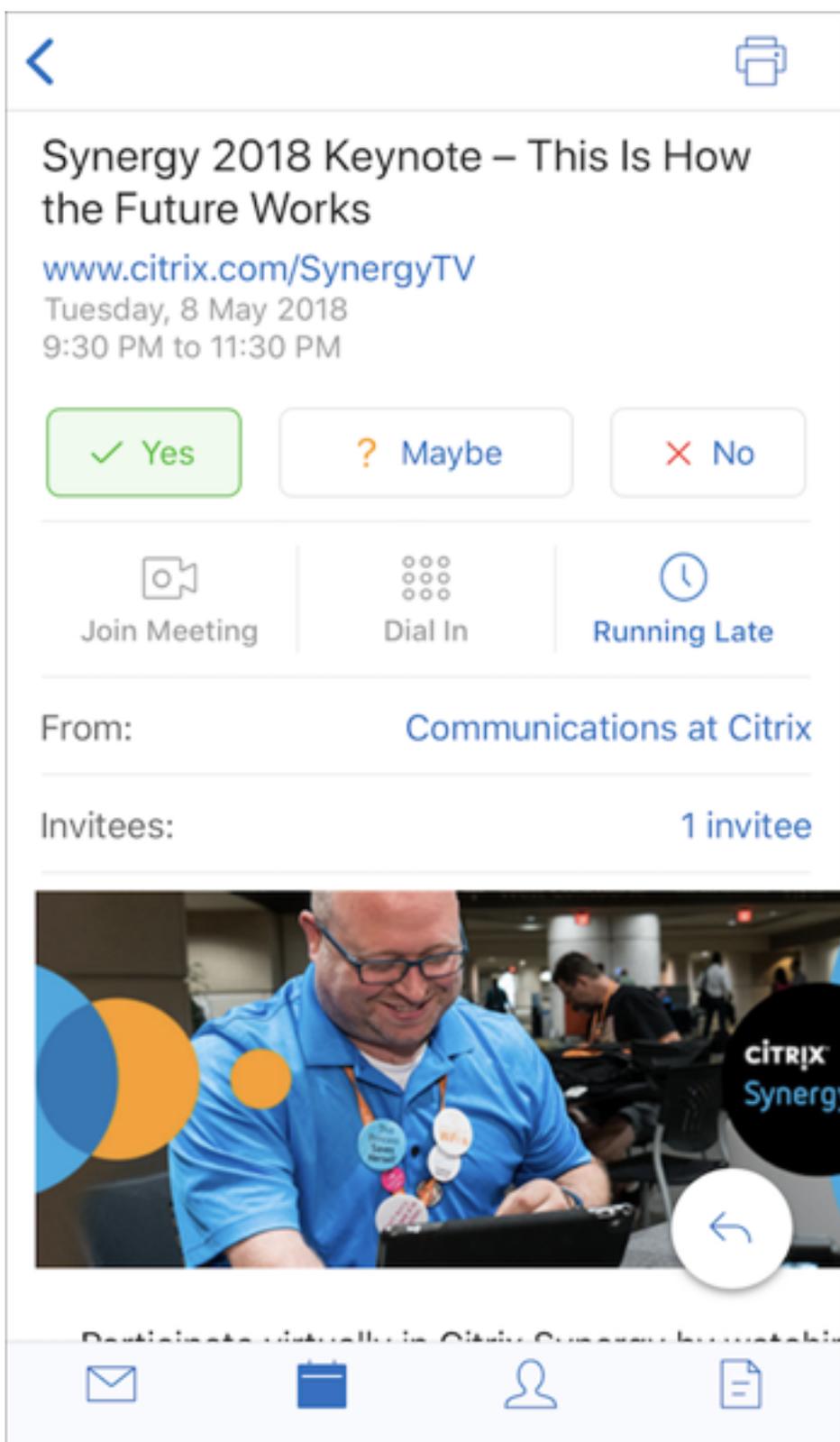
O que mudou:

- 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.



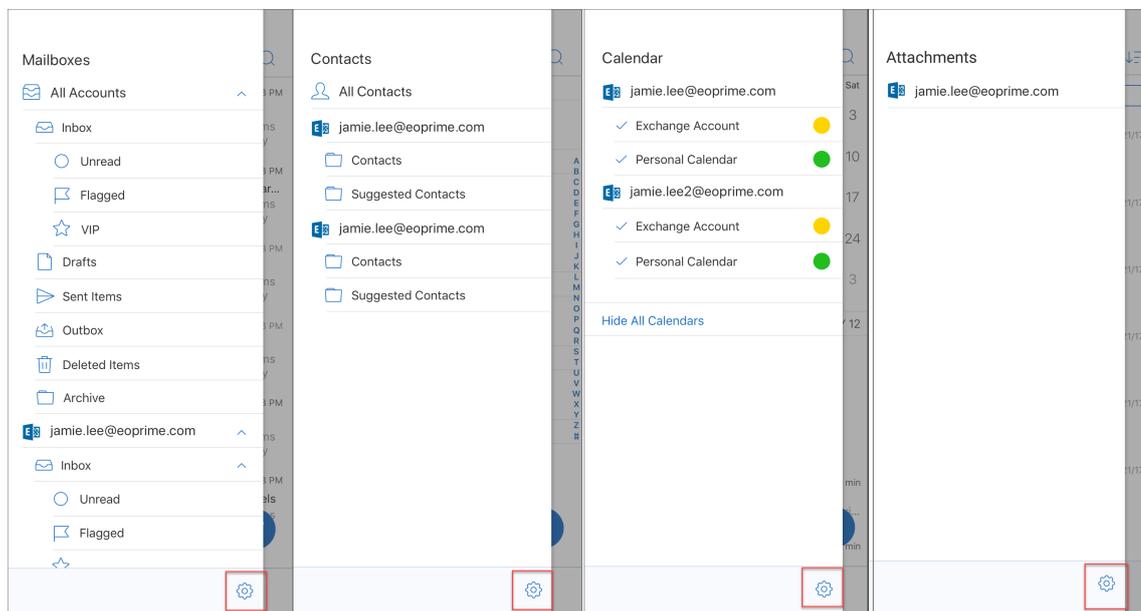
Nota:

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.

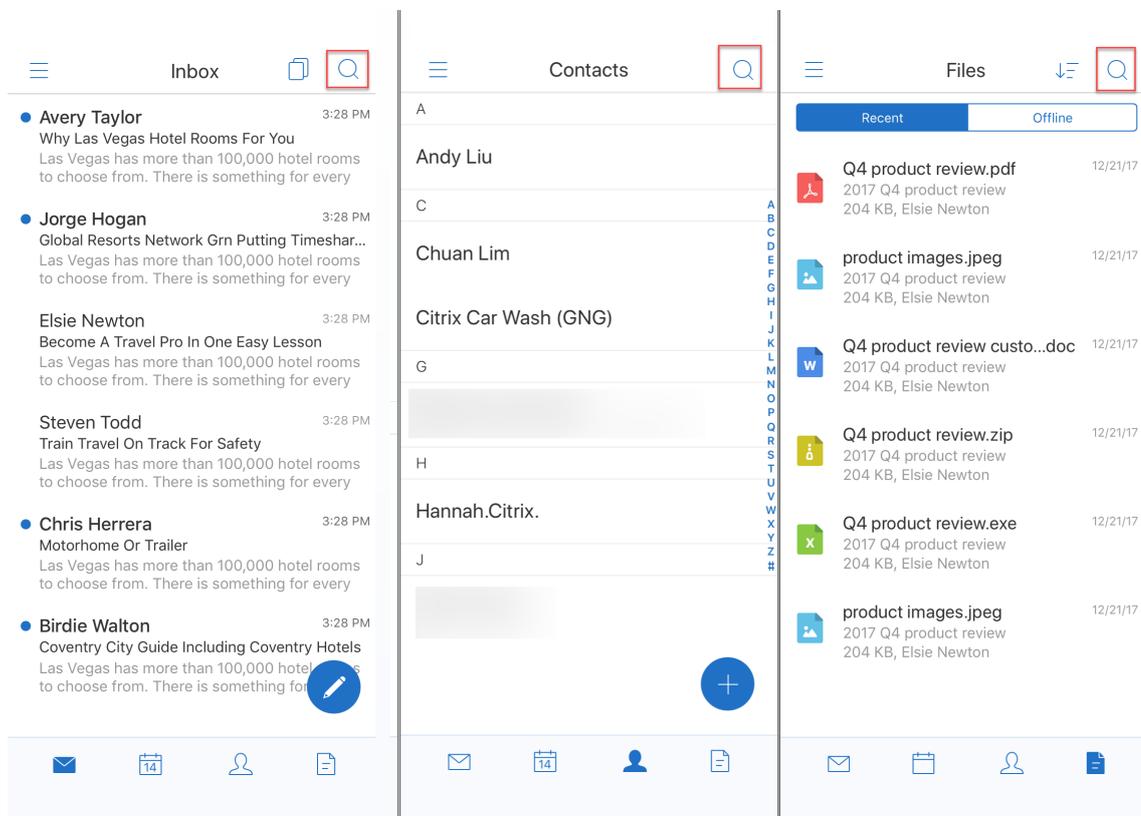


- O menu **Configurações** está disponível em todos os menus, como Correio, Calendário, Contatos e Anexos. Para ir para **Configurações**, toque no ícone de hambúrguer e, em seguida, toque

no botão de configurações disponível na parte inferior direita, conforme mostrado na figura a seguir.

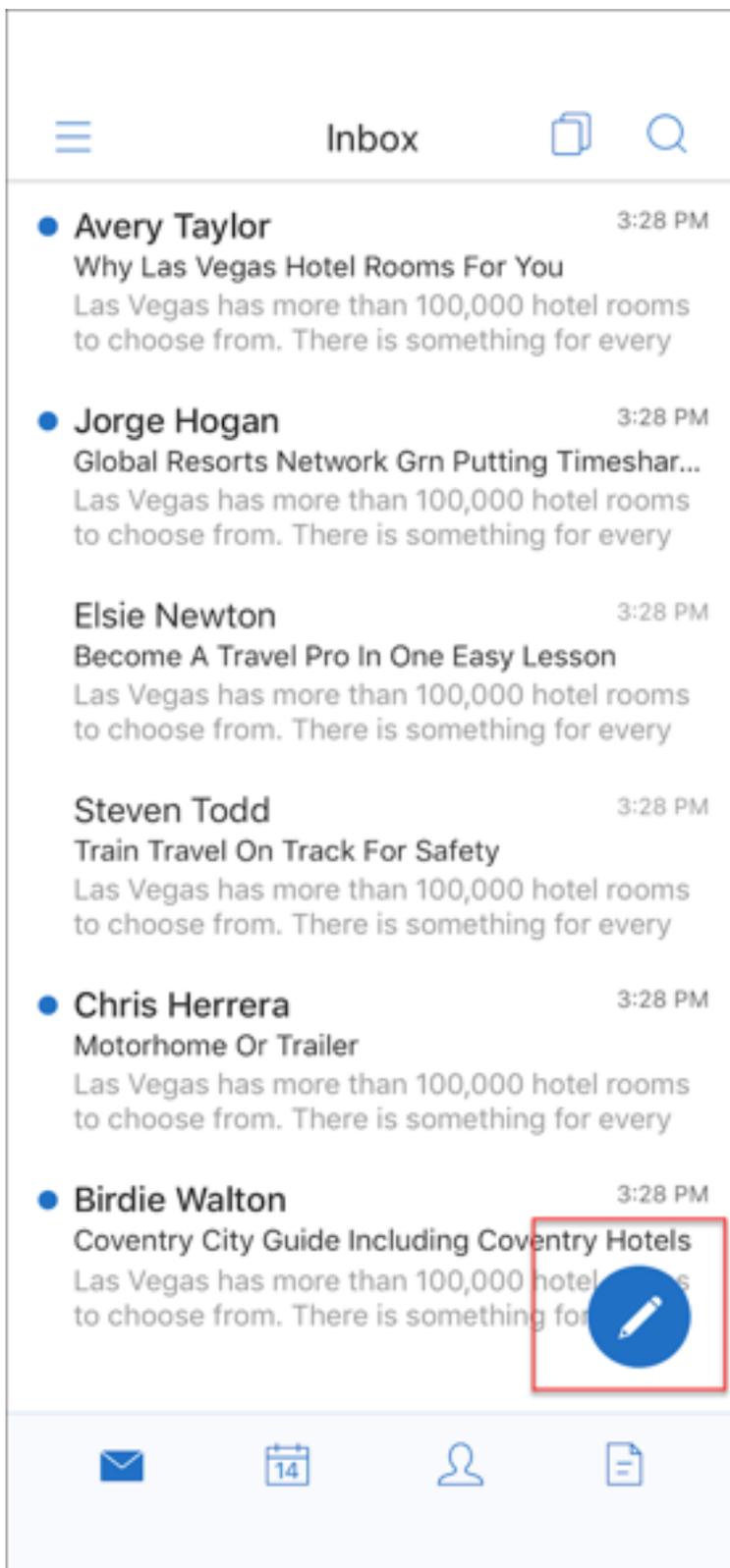


- O ícone **Pesquisar** substitui a barra de pesquisa e está disponível nos modos de exibição da Caixa de entrada, Contatos e Anexos.

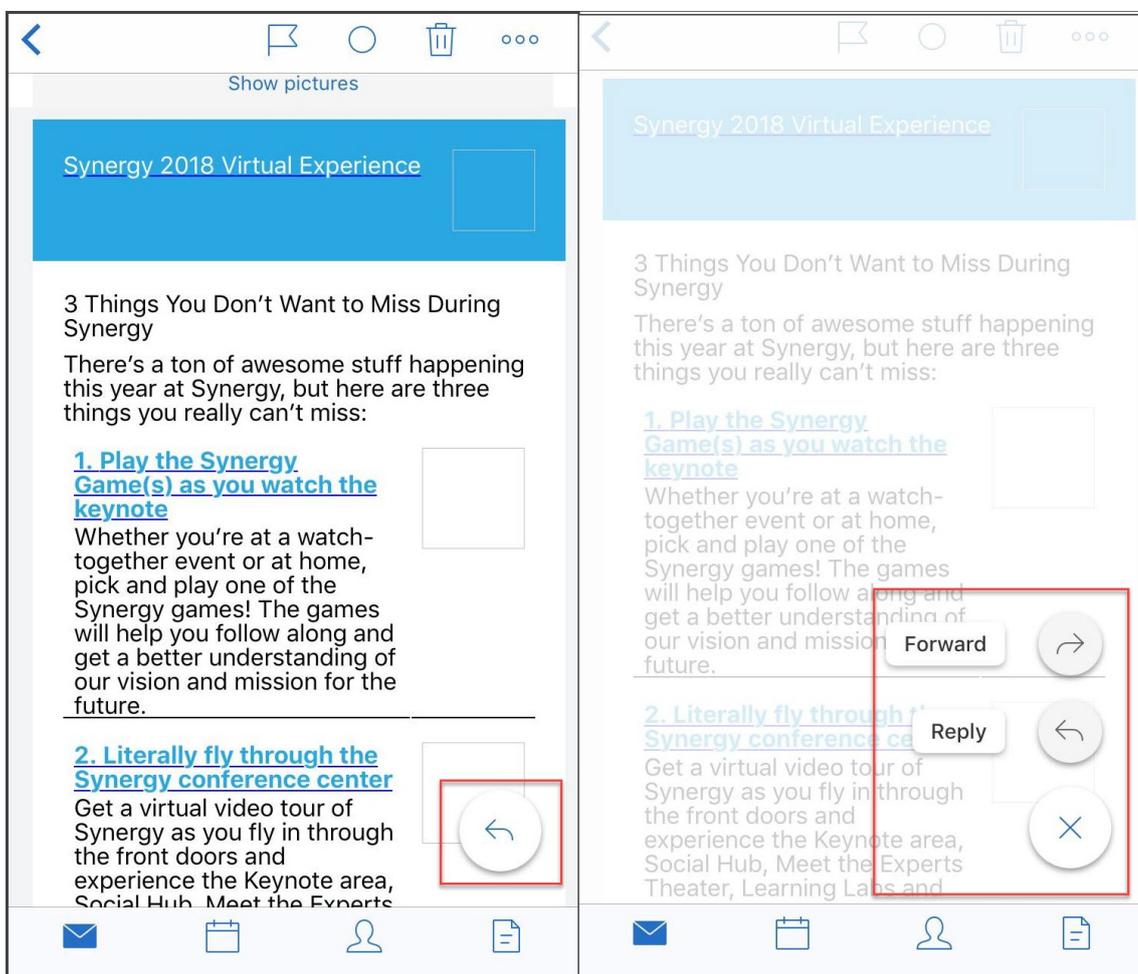


- Nos dispositivos iOS, você pode tocar e segurar em um item de correio para selecioná-lo.

- 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.

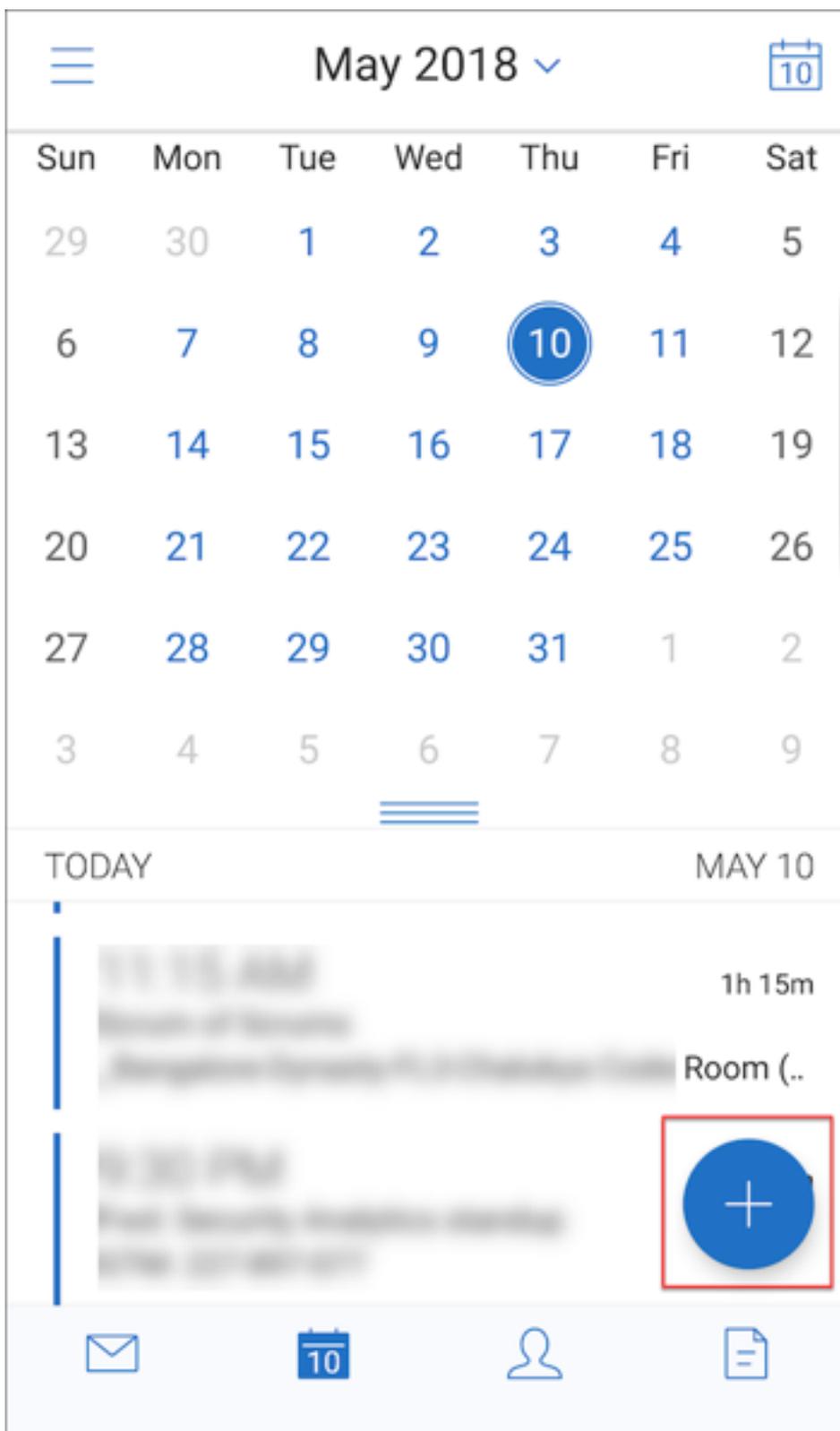


- Ao ver um email, as seguintes opções de menu estão agora disponíveis no canto superior direito da tela:
 - **Sinalização:** toque para sinalizar o email.
 - **Marcar como não lido:** toque para marcar o email como não lido.

- **Apagar:** toque para apagar o email.
- **Mais opções:** toque no ícone suspenso para ver outras ações disponíveis, como Mover.

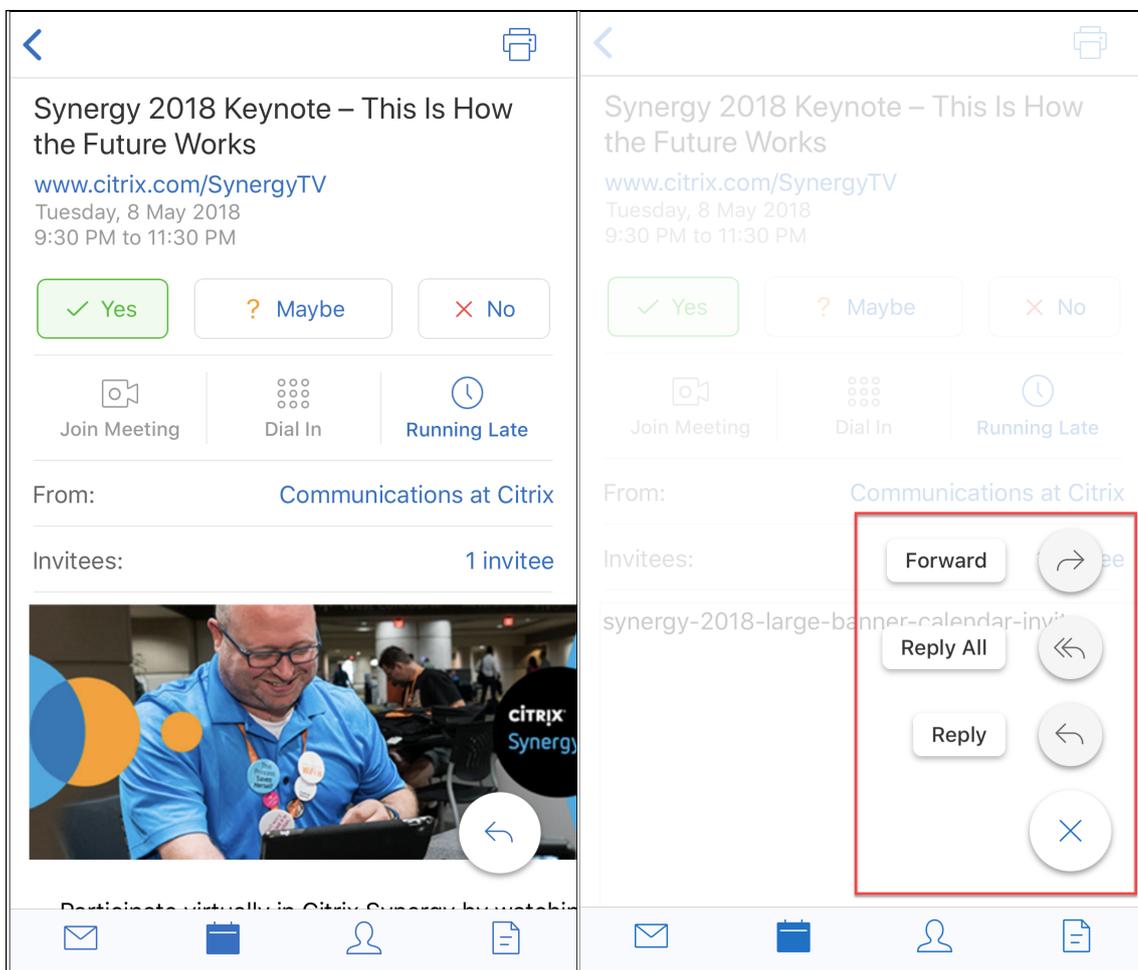
Mudanças na agenda

- 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.

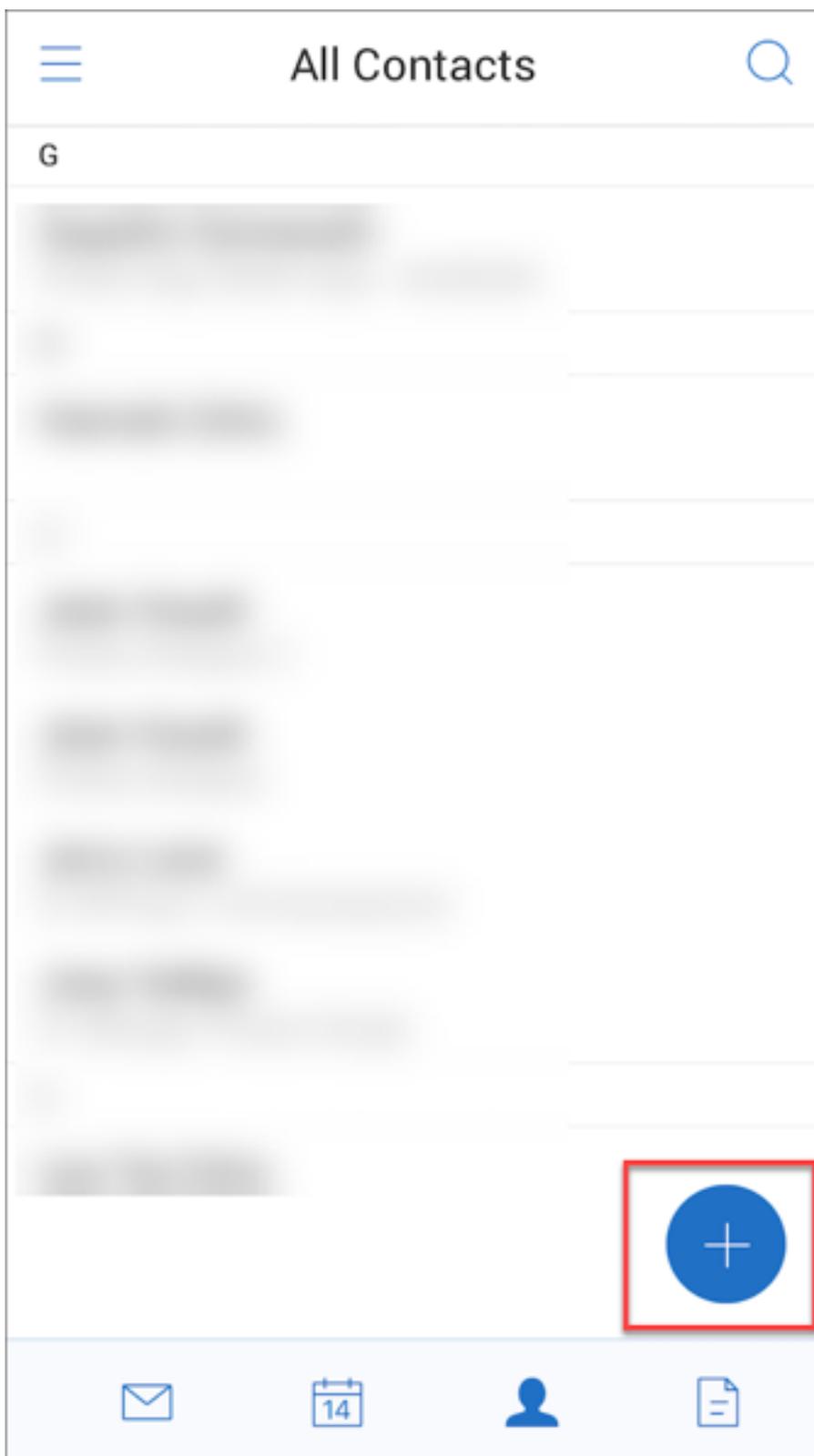
- **Pesquisar:** toque para procurar um evento.
- **Botão de ação flutuante Responder:** Ao visualizar um email, toque em Encaminhar, Responder a todos ou Responder.



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.

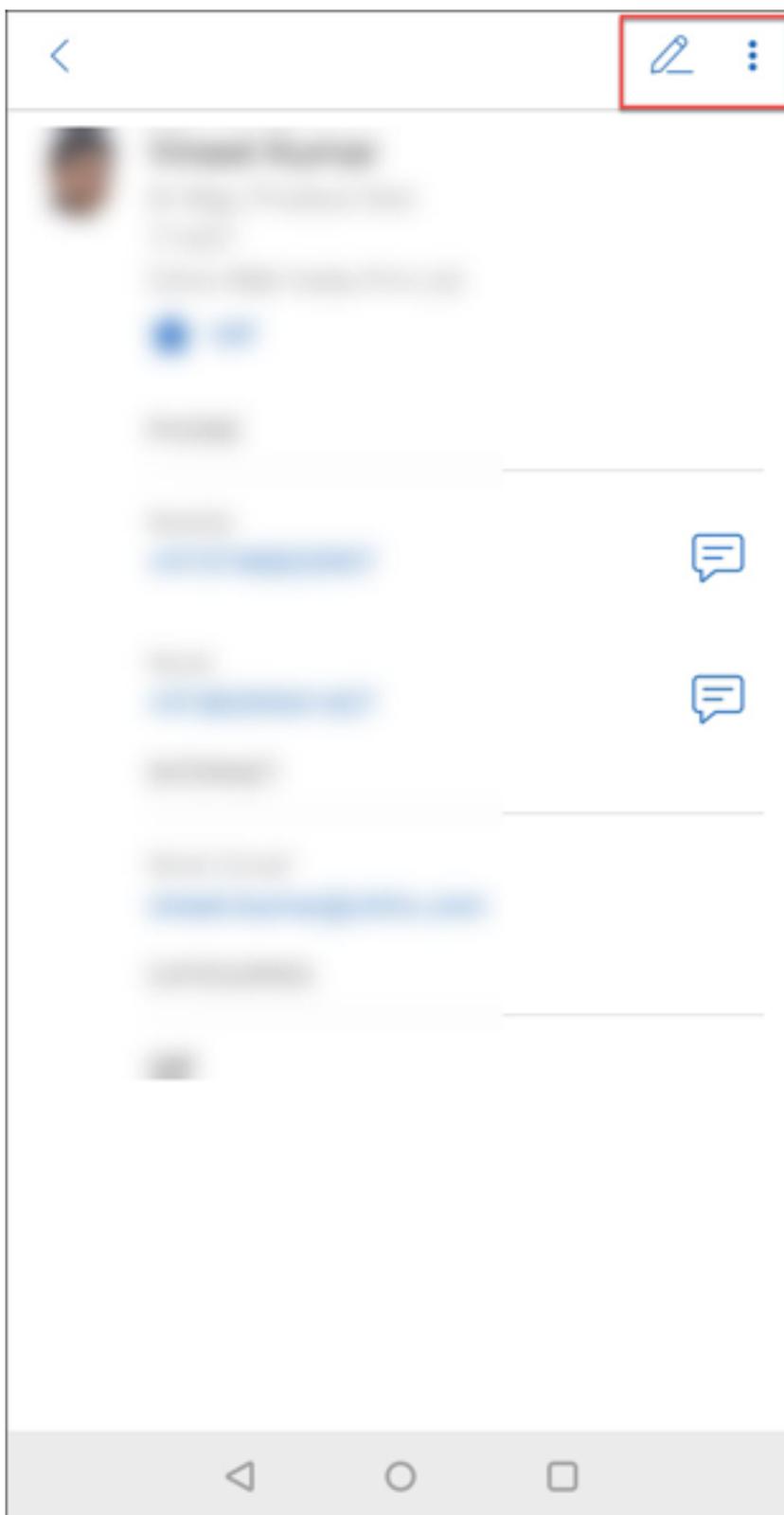


- A opção de menu **Pesquisar** está agora disponível no canto superior direito da tela. Você pode tocar na opção para procurar um contato.

- Ao ver um contato, as seguintes opções de menu estão agora disponíveis no canto superior direito da tela:

Em dispositivos Android:

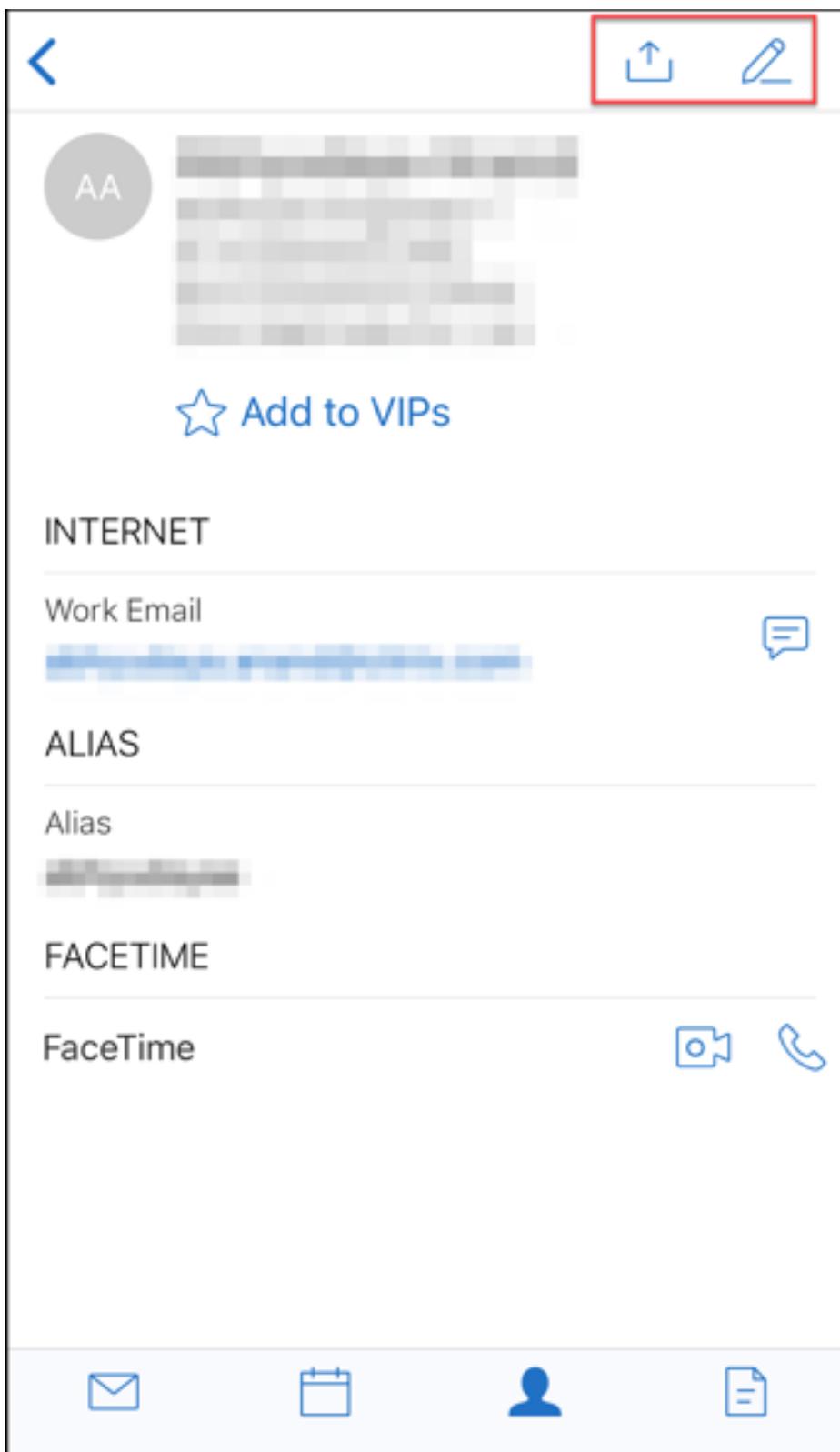
- **Editar:** toque para editar o contato.
- **Mais opções:** toque no ícone de edição para ver outras ações disponíveis, como Anexar ao email, Compartilhar e Excluir.



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 toque em **Excluir** na parte inferior da tela, conforme mostra a figura a seguir.

Cancel	Save		
ADDRESS			
Add Address			
COMPANY INFO			
Add Company			
PERSONAL			
Add Personal			
DATES			
Add Date			
NOTES			
Add Note			
Delete Contact			
			

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, consulte [Credenciais Derivadas para iOS](#).
- O Secure Mail para iOS 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 iOS oferece suporte a assinaturas em rich text. Você pode usar imagens ou links na sua assinatura de email. Para 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 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 Android Enterprise 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). Para obter detalhes, consulte [Autenticação moderna usando o Microsoft Office 365](#).

Notas:

Esta 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.

Problemas conhecidos e resolvidos

September 13, 2022

Secure Mail 22.9.0

Problemas conhecidos no Secure Mail para iOS

Não há problemas conhecidos nesta versão.

Problemas corrigidos no Secure Mail para iOS

Não há problemas corrigidos nesta versão.

- 22.9.0 (somente Secure Mail e Secure Web para iOS)

Secure Mail 22.6.2

Problemas conhecidos no Secure Mail para iOS

Não há problemas conhecidos nesta versão.

Problemas corrigidos no Secure Mail para iOS

- Quando você baixa um arquivo usando o Secure Web e tenta enviá-lo a um destinatário usando o Secure Mail, a opção **Nova mensagem** não aparece. [CXM-106056]

Secure Mail 22.6.0

Problemas conhecidos no Secure Mail para iOS

Não há problemas conhecidos nesta versão.

Problemas corrigidos no Secure Mail para iOS

- Ao redigir um e-mail no Secure Mail para iOS, aparecem detalhes de contato errados quando você tenta adicionar um contato. [CXM-104388]
- O Secure Mail e o Secure Web para iOS não respondem quando você abre o aplicativo. [CXM-105483]

Secure Mail 22.3.0

Problemas conhecidos no Secure Mail 22.3.0

- Quando você edita um evento de calendário e atualiza a hora do lembrete da reunião, o lembrete não aparece para o organizador da reunião. Esse problema ocorre se a sua organização estiver executando o servidor HCL Domino 11 (anteriormente Lotus Notes). [CXM-88099]
- Quando você atualiza um evento recorrente para um evento diário e tenta editar uma das ocorrências, a opção de edição não aparece. Esse problema ocorre se a sua organização estiver executando o servidor HCL Domino 11. [CXM-104132]
- Quando você altera a data ou a hora de uma única instância de um evento recorrente, a reunião é remarcada para uma data aleatória. Esse problema ocorre se a sua organização estiver executando o servidor HCL Domino 11. [CXM-104279]

Problemas resolvidos no Secure Mail 22.3.0

Não há problemas corrigidos nesta versão.

Problemas conhecidos e resolvidos em versões mais antigas

Para ver os problemas conhecidos e resolvidos em versões mais antigas do Secure Mail, consulte [Histórico de problemas conhecidos e resolvidos do Secure Mail](#).

Implantação do Secure Mail

December 9, 2021

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 IBM Notes Traveler Server para manter o Secure Mail em sincronia com o Microsoft Exchange ou IBM Notes. Se você usar IBM Notes, configure o servidor IBM Notes Traveler. 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 do 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 as 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 política 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

August 5, 2022

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, [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
- Com túnel — SSO de Web + Servidor interno Não KCD SSO do Exchange

Autenticação moderna com o Microsoft Office 365

August 18, 2022

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 do Office 365 e intervalo de endereços IP](#).

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.
- **Política SSO da Web para encapsulamento:** Use esta política para encapsular o tráfego OAuth para passar por Com túnel – SSO de Web. Para isso:
 - Defina a política **Usar o SSO da Web para encapsulamento** como **Ativado**.

- Na política de acesso à rede, selecione a opção **Com túnel - SSO de Web**.
- Exclua os nomes de host relacionados ao OAuth da política de **Serviços em segundo plano**.

Políticas comuns para dispositivos iOS e Android:

- **Agente de usuário personalizado para autenticação moderna:** Use esta política para alterar a sequência do agente do usuário padrão para autenticação moderna.
- **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. Você pode usar essa política para definir o endereço do servidor local ou o endereço do servidor Cloud, conforme a sua necessidade.

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 avançadas, 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.

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

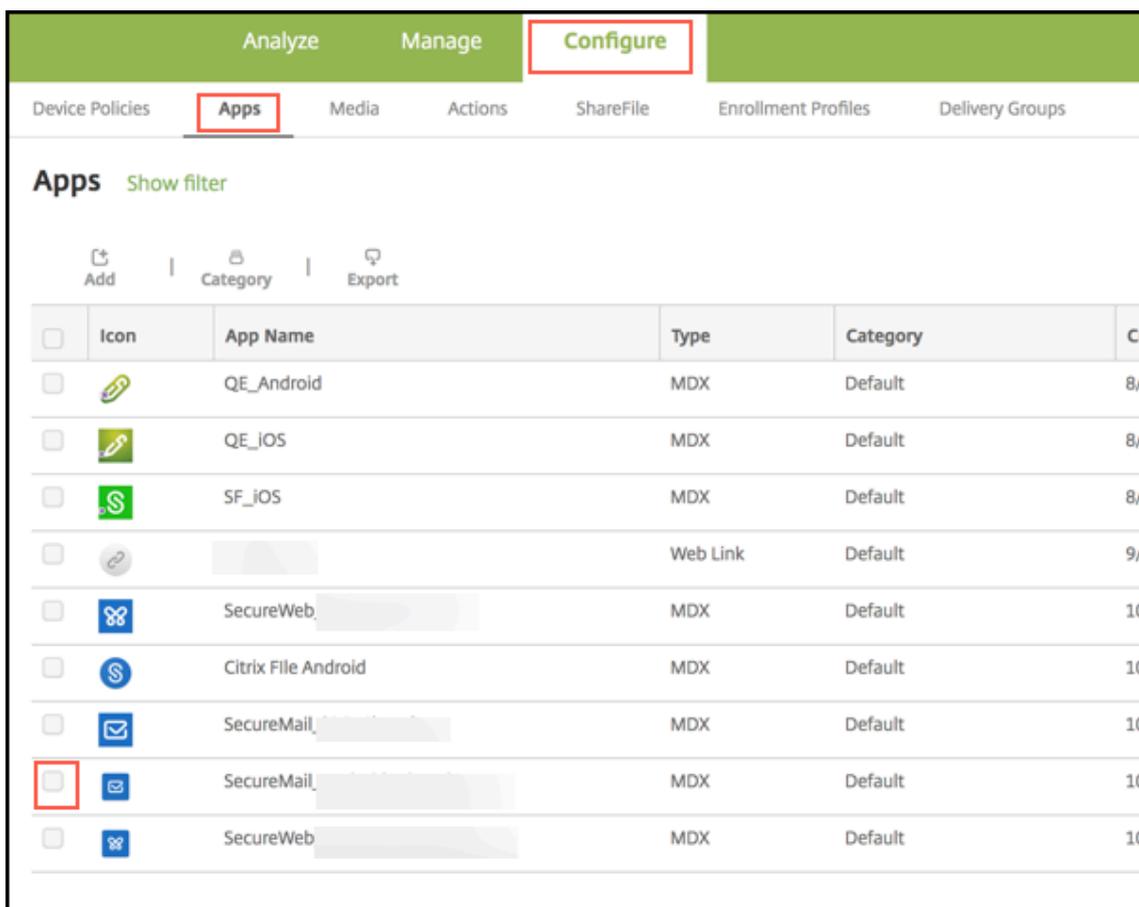
Serviços em segundo plano para o Secure Mail

August 25, 2020

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.

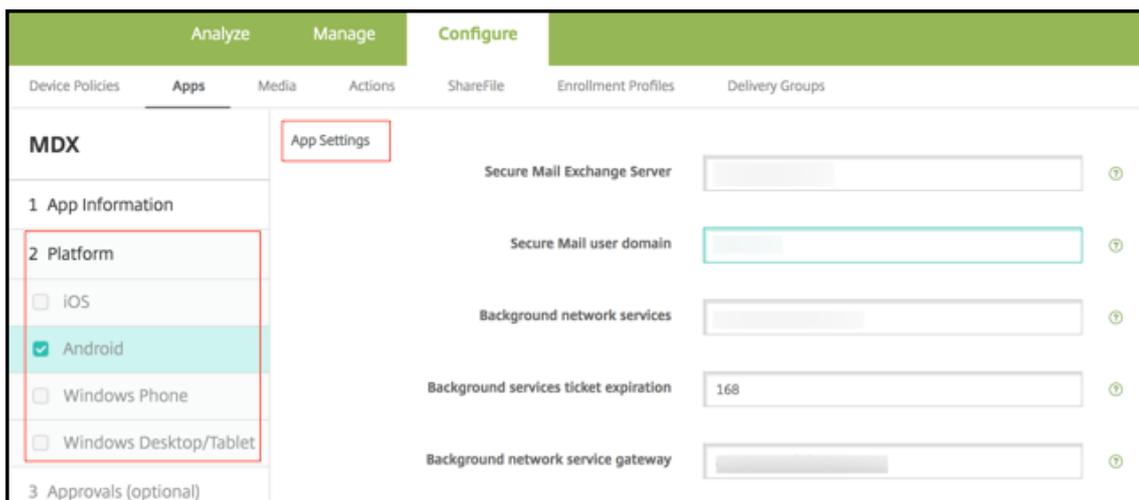
Para configurar serviços em segundo plano para o Secure Mail

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.

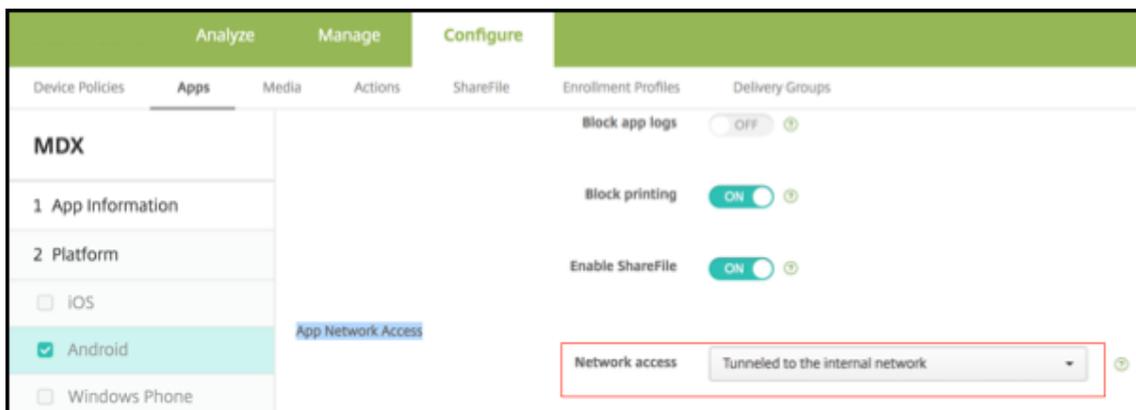


Políticas de aplicativo MDX para a configuração de serviços em segundo plano

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`.

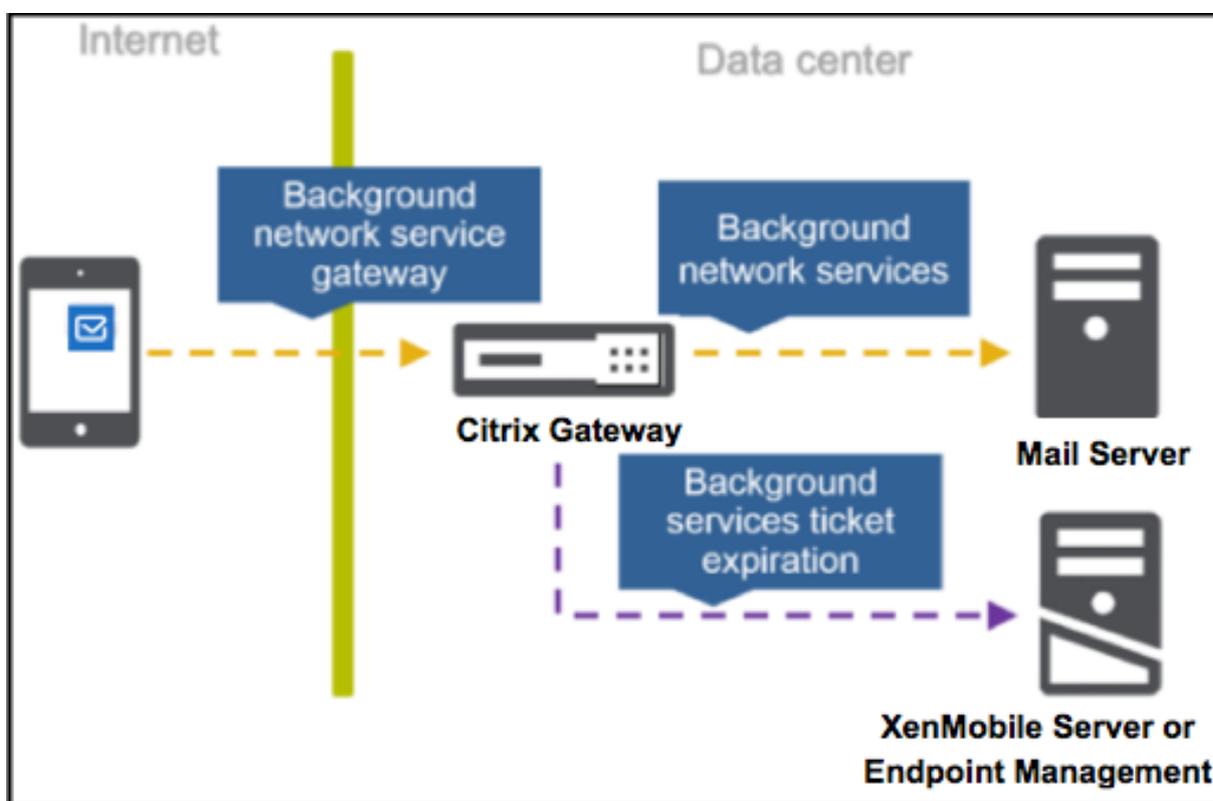
Expiração de tíquete de serviços em segundo plano: esta política especifica a validade do tíquete de serviço de rede em segundo plano. Quando o Secure Mail se conecta por meio do Citrix Gateway

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:



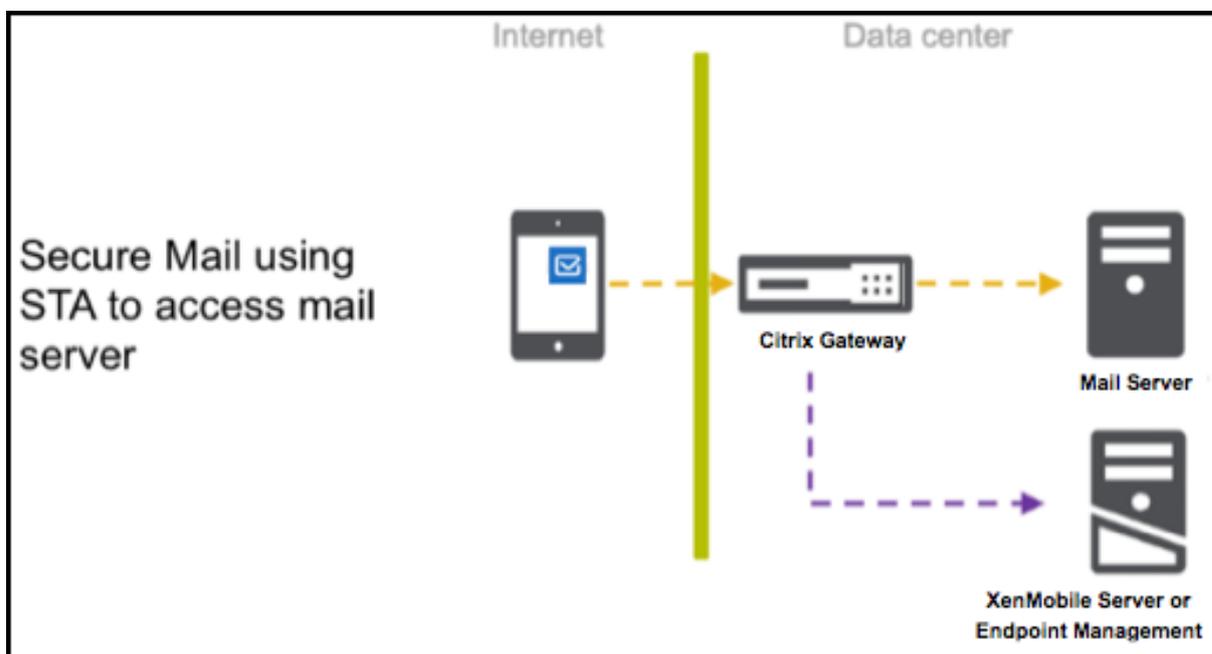
Políticas sobre uma conexão direta a um servidor de email:

- 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

December 9, 2021

Para manter o Secure Mail em sincronia com os seus servidores de email, integre o Secure Mail com um Exchange Server ou IBM Notes Traveler Server 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 do 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

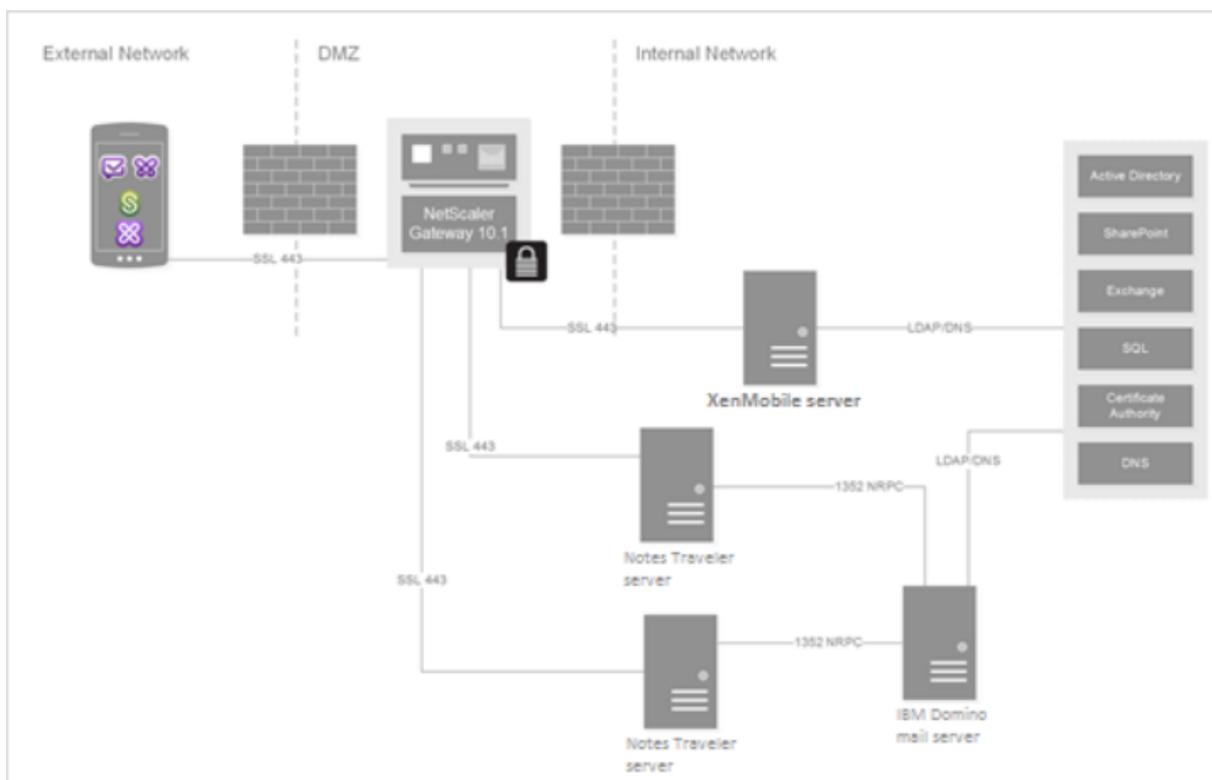
Em ambientes de IBM Notes, você deve configurar o servidor IBM Notes Traveler antes de implantar o Secure Mail. Esta seção mostra uma ilustração de implantação dessa configuração, bem como os requisitos do sistema.

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 Configurando o 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 Secure Mail.

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 este 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

December 10, 2021

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.

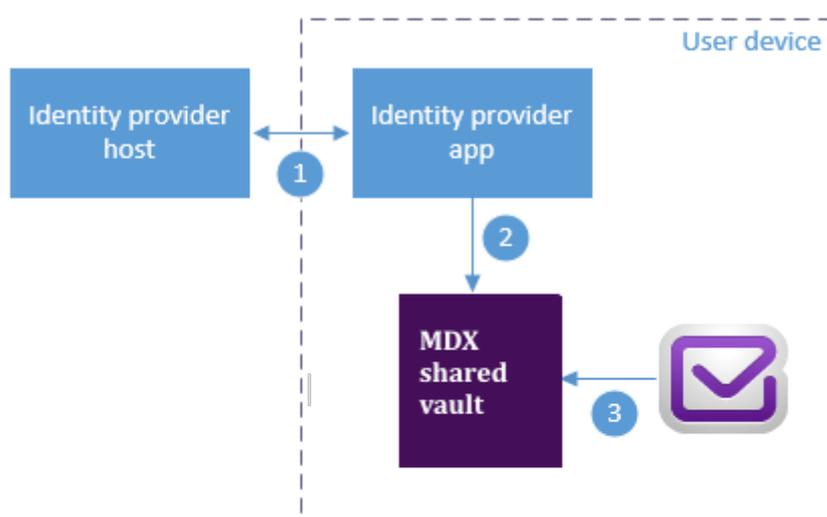
Na tabela a seguir, X indica que o Secure Mail dá suporte a um recurso S/MIME no sistema operacional do dispositivo.

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	
Suporte a credenciais derivadas		O Secure Mail dá suporte ao uso de credenciais derivadas como uma fonte de certificado. Para obter mais informações, consulte Credenciais Derivadas para iOS .

Recurso S/MIME	iOS	Android
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
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 quando você integra o Secure Mail com suporte a um provedor de identidade digital de terceiro.



- 1 The identity provider host verifies user identity and sends certificates to the identity provider app on the client device
- 2 Using the Worx API, the identity provider app sends certificates to the shared vault.
- 3 Secure Mail gets certificate from the shared vault

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 [Ativar 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, 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 15 do Exchange Server 2013
 - 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 credenciais de dispositivo](#).
- 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

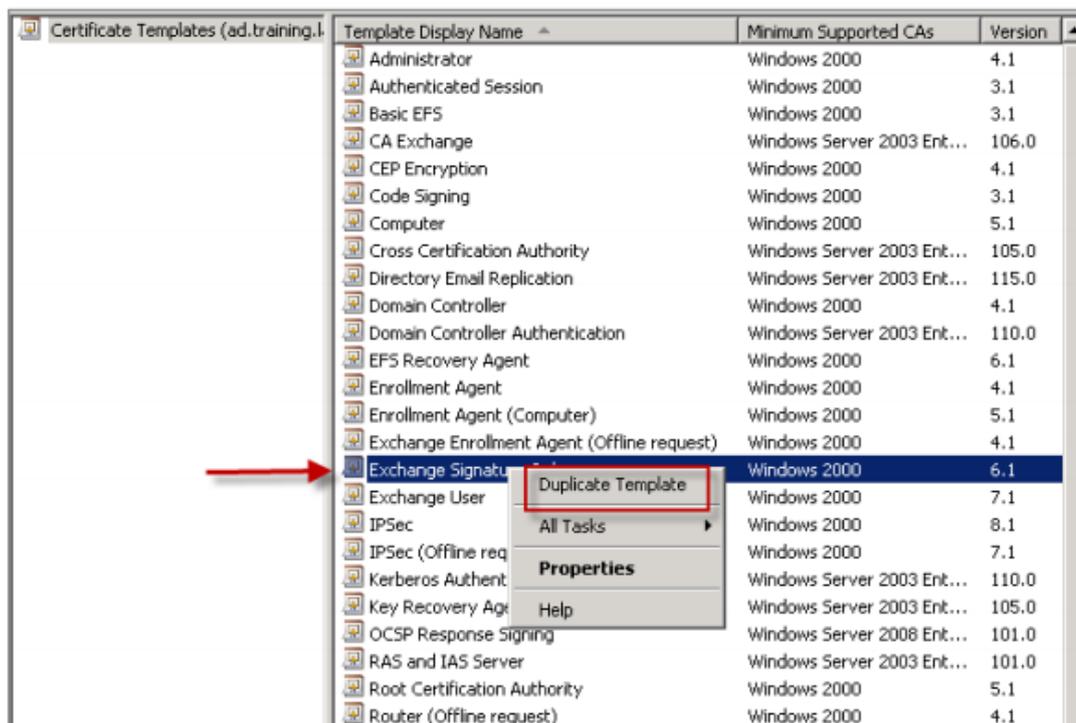
- Verifique se o site de inscrição na Web usado para solicitar certificados de usuário (por exemplo, <https://ad.domain.com/certsrv/>) está protegido com um certificado de servidor de HTTPS (particular ou público).
 - O site de inscrição na web deve ser acessado por HTTPS.
1. Vá até **Ferramentas administrativas**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

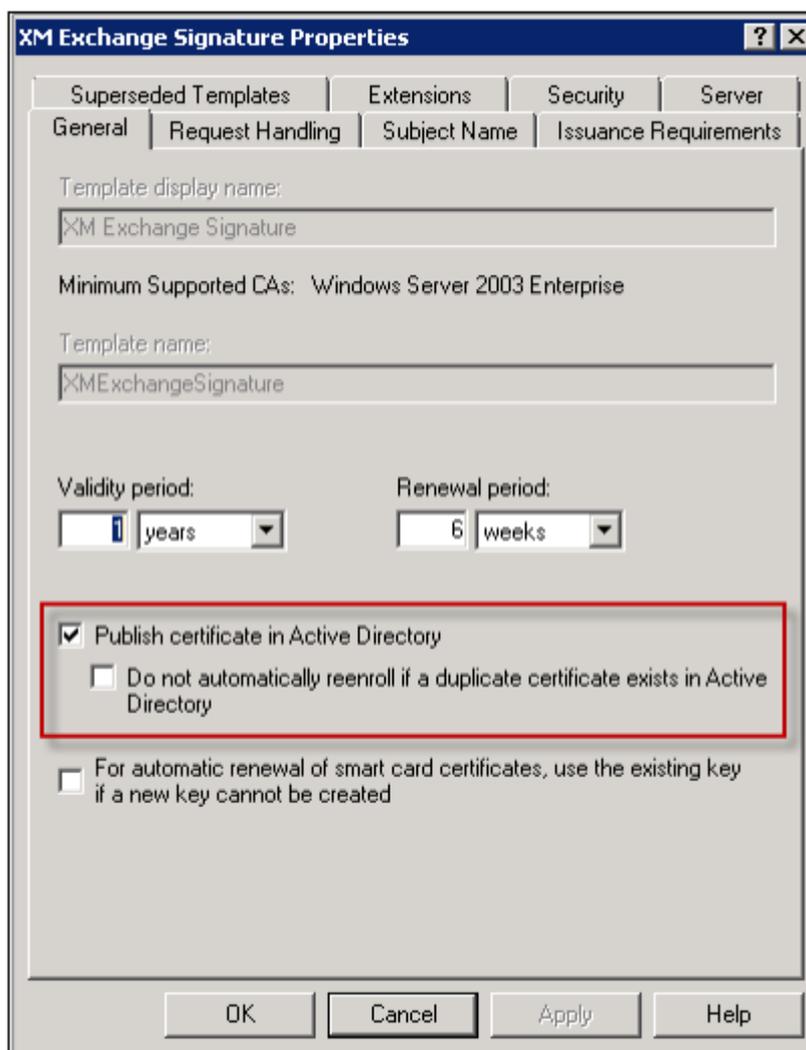
- Somente assinatura do Exchange (para assinatura)
 - Usuário do Exchange (para criptografia)
1. Abrir o snap-in da Autoridade de Certificação.
 2. Expanda a autoridade de certificação e vá para **Modelos de Certificado**.
 3. Clique com o botão direito do mouse e, em seguida, clique em **Gerenciar**.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

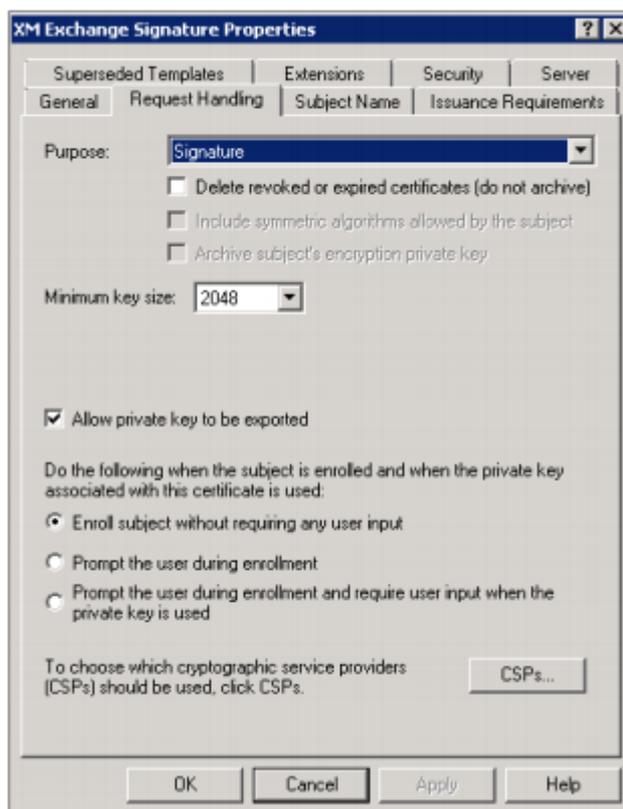
Nota:

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)**.

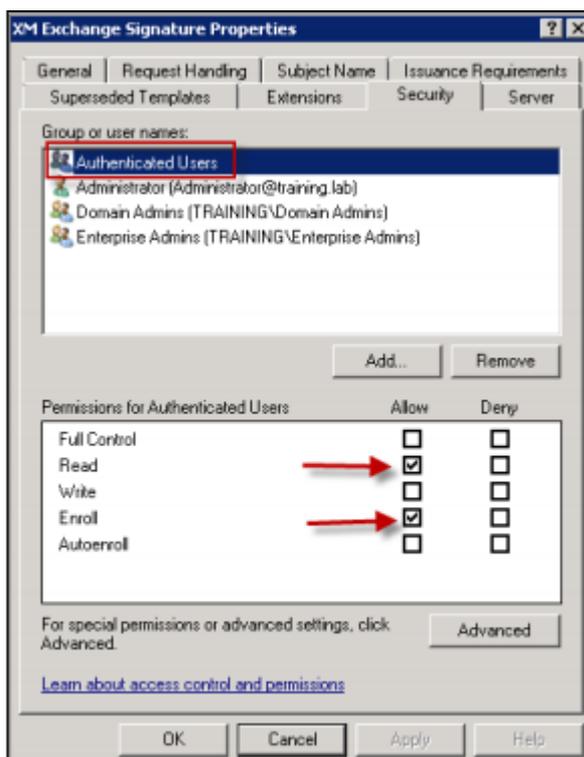


7. Clique na guia **Tratamento de solicitação** e defina os seguintes parâmetros:

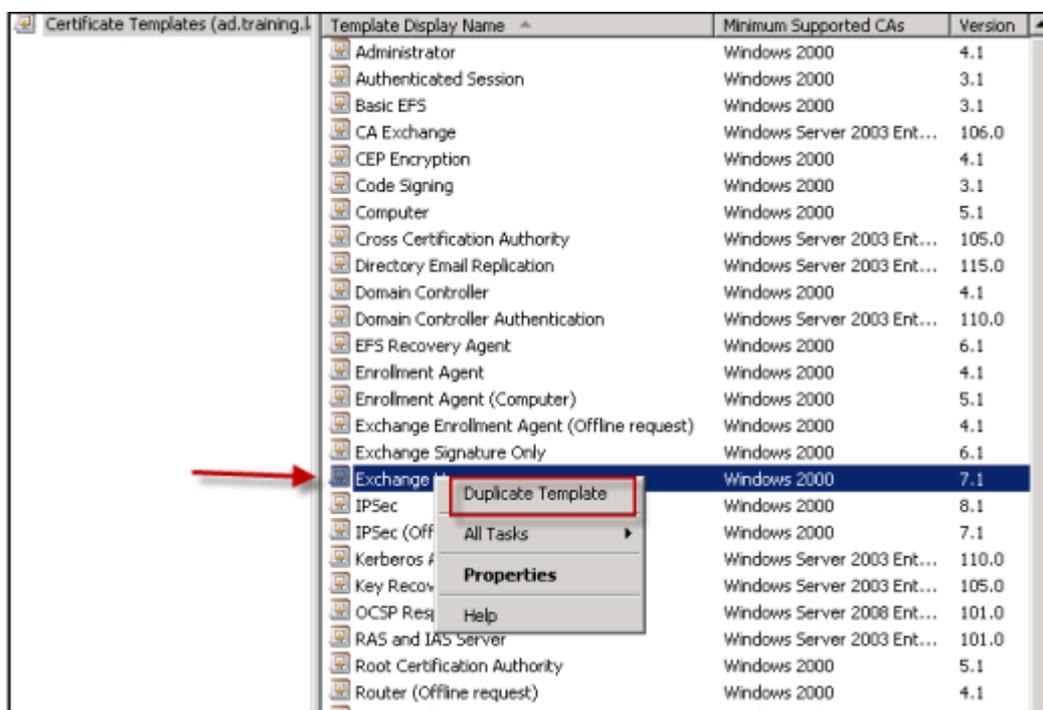
- **Finalidade:** assinatura
- **Tamanho mínimo da chave:** 2048
- **Caixa de seleção Permitir que a chave privada seja exportada:** selecionada
- **Caixa de seleção Registrar requerente sem solicitar entrada do usuário:** selecionada



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.

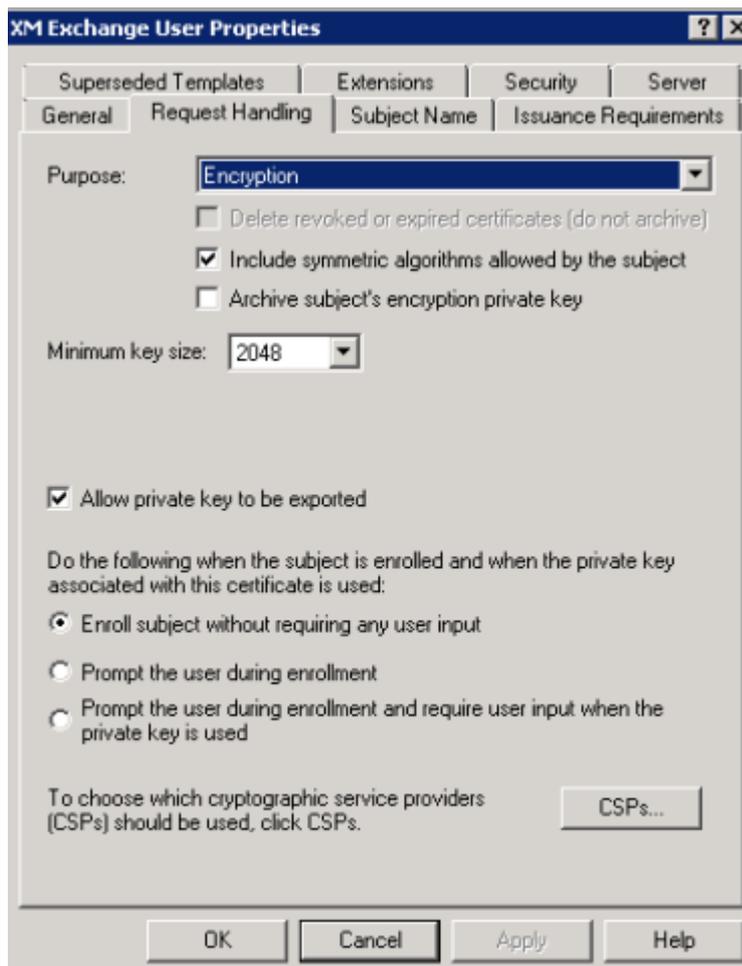


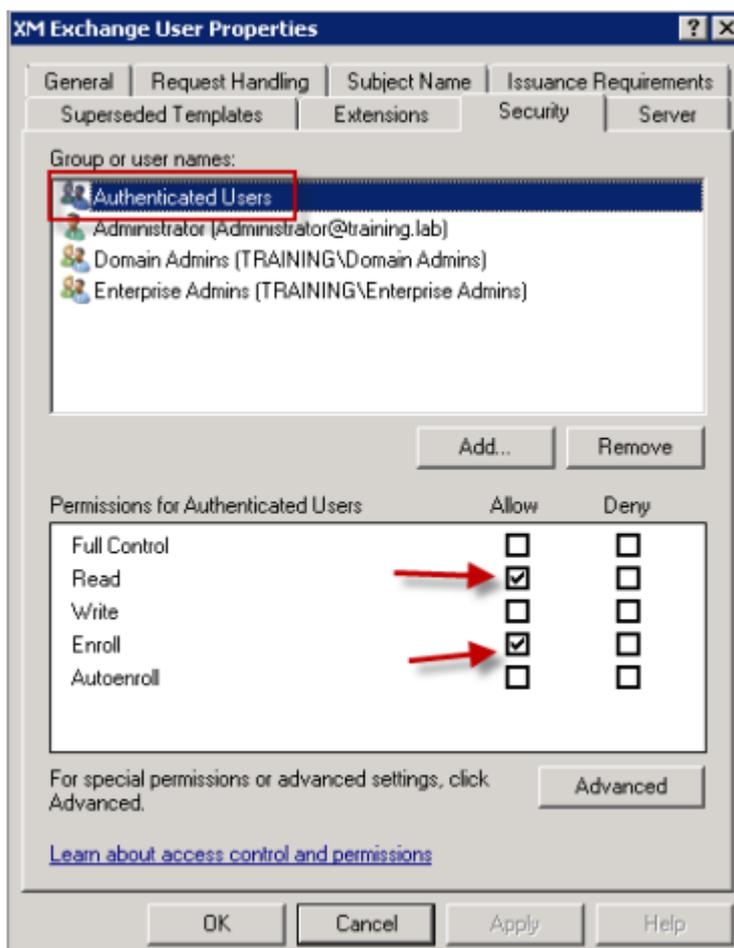
Para o novo modelo de Usuário do Exchange, use as mesmas configurações padrão para o mod-

elo original.

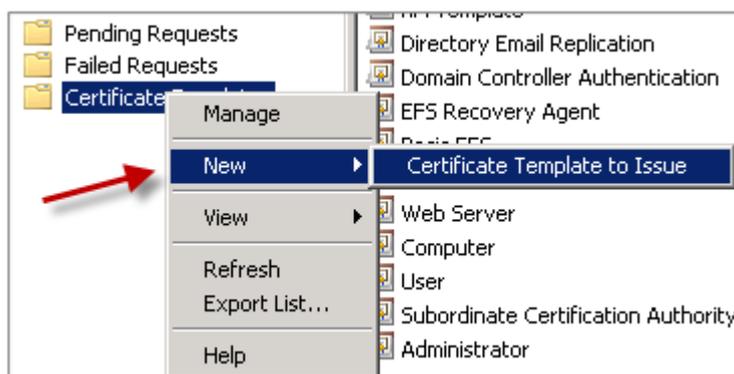
11. Clique na guia **Tratamento de solicitação** e defina os seguintes parâmetros:

- **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 assinatura e criptografia. Uma alternativa é configurar inscrição automática através de uma Política de Grupo para o grupo de usuários que usariam este recurso.

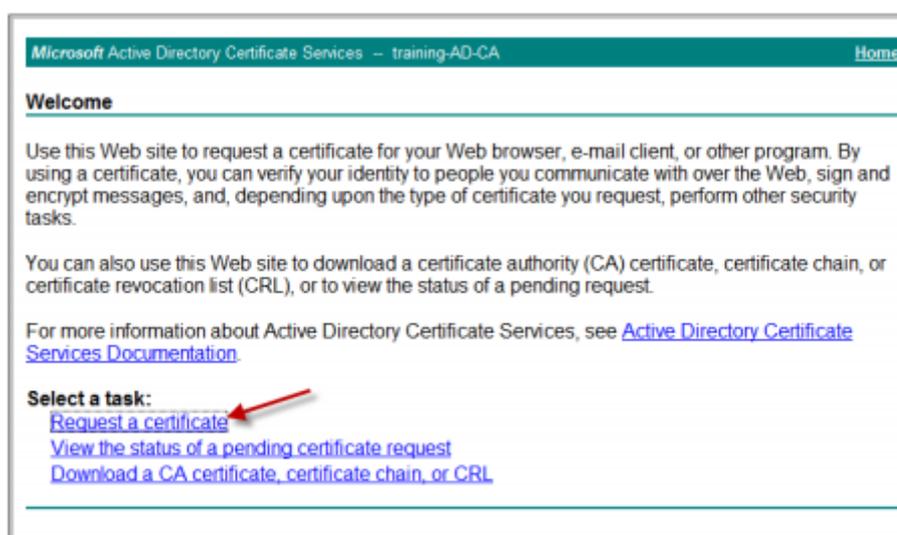
1. Em um computador com o Windows, abra o Internet Explorer e vá para o site de inscrição para solicitar um novo certificado de usuário.

Nota:

Faça login 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.

Microsoft Active Directory Certificate Services -- training-AD-CA [Home](#)

Advanced Certificate Request

Certificate Template:

XM Exchange Signature

Identifying Information For Offline Template:

Name: user1
E-Mail: user1@training.lab
Company: Citrix
Department: Support Readiness
City: FTL
State: FL
Country/Region: US

Key Options:

Create new key set Use existing key set
CSP: Microsoft Enhanced Cryptographic Provider v1.0
Key Usage: Signature
Key Size: 2048 (Min: 2048, Max: 10384, common key sizes: 2048 4096 8192 10384)
 Automatic key container name User specified key container name
 Mark keys as exportable
 Enable strong private key protection

Additional Options:

Request Format: CMC PKCS10
Hash Algorithm: sha1
Only used to sign request.
 Save request

6. Clique em **Instalar este certificado**.
7. Confirme se o certificado foi instalado com êxito.

Microsoft Active Directory Certificate Services -- training-AD-CA

Certificate Installed

Your new certificate has been successfully installed.

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.

Microsoft Active Directory Certificate Services -- training-AD-CA [Home](#)

Advanced Certificate Request

Certificate Template:

XM Exchange User

Identifying Information For Offline Template:

Name: user1
E-Mail: user1@training.lab
Company: Citrix
Department: Support Readiness
City: FTL
State: FL
Country/Region: US

Key Options:

Create new key set Use existing key set
CSP: Microsoft Enhanced Cryptographic Provider v1.0
Key Usage: Exchange
Key Size: 2048 (Min: 2048, Max: 16384, common key sizes: 2048 4096 8192 16384)
 Automatic key container name User specified key container name
 Mark keys as exportable
 Enable strong private key protection

Additional Options:

Request Format: CMC PKCS10
Hash Algorithm: sha1
Only used to sign request.
 Save request

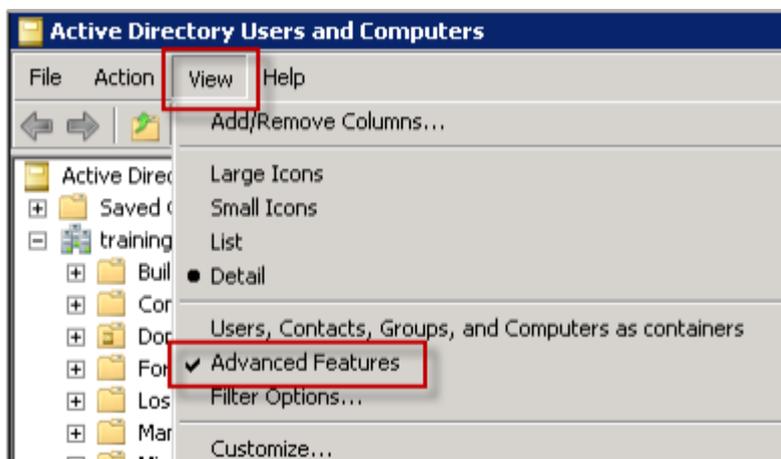
10. Verifique se você instalou o certificado com êxito e repita o mesmo procedimento para gerar um par de certificados de usuário para outro usuário de domínio. Este exemplo segue o mesmo procedimento e gera um par de certificados para “User2”.

Nota:

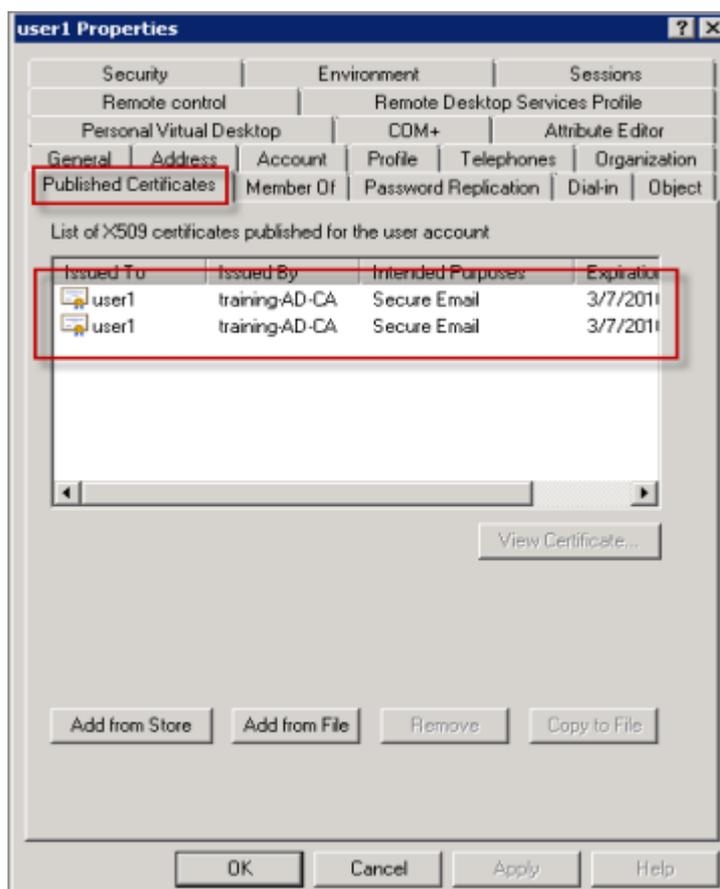
Esse procedimento usa o mesmo computador com Windows para solicitar o segundo par de certificados para “User2”.

Validação de certificados publicados

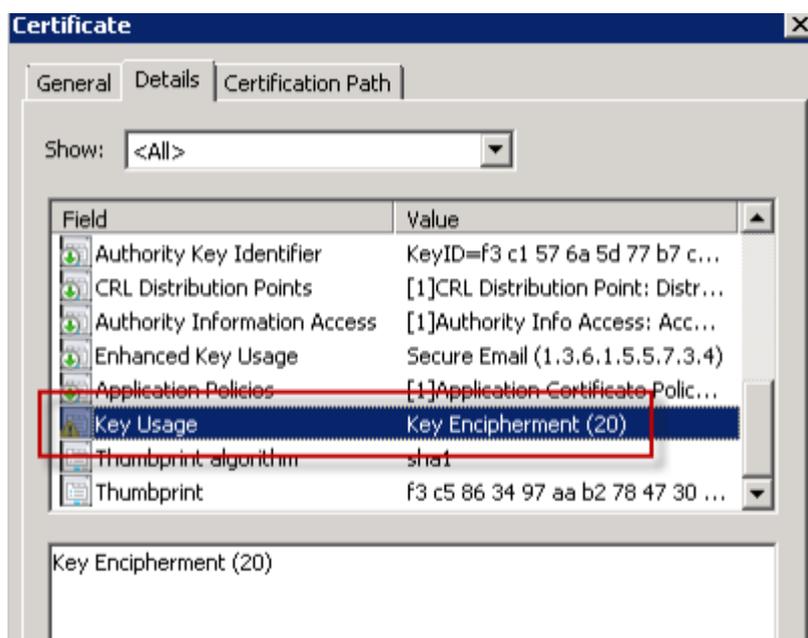
1. Para garantir que os certificados estão instalados corretamente no domínio perfil de usuário, vá para **Usuários e computadores do Active Directory > Exibir > Recursos avançados**.



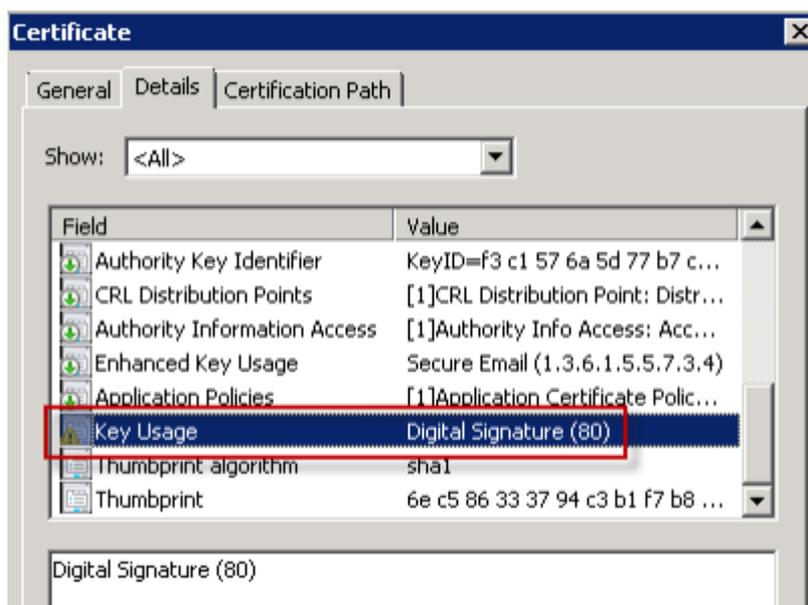
2. Ir para as propriedades do usuário (User1 neste exemplo) e, em seguida, clique na guia **Certificados publicados**. Verifique se ambos os certificados estão disponíveis. Você também pode verificar se cada certificado tem um uso específico.



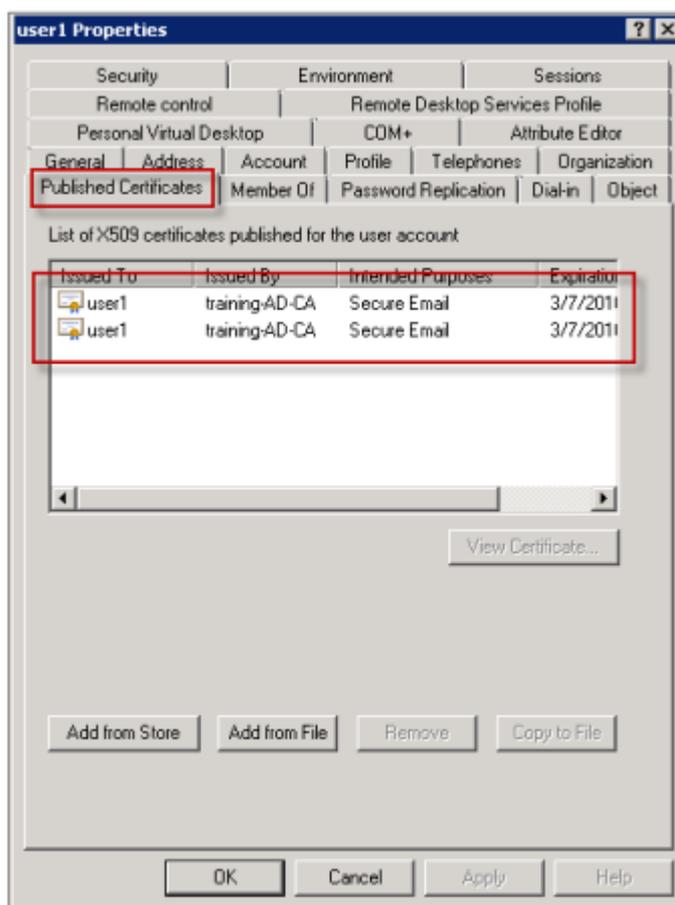
A figura apresenta um certificado para criptografar mensagens de email.



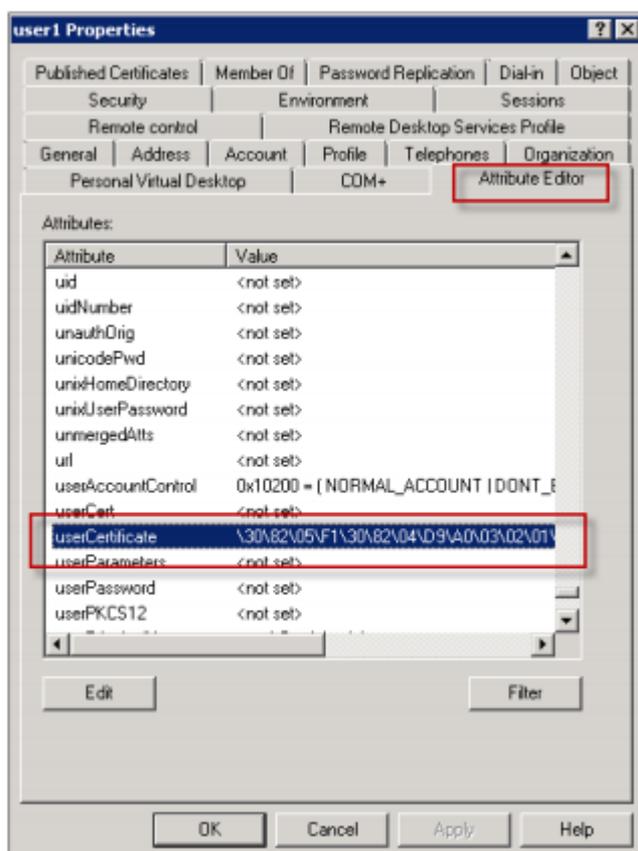
A figura apresenta um certificado para assinar mensagens de email.



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**.



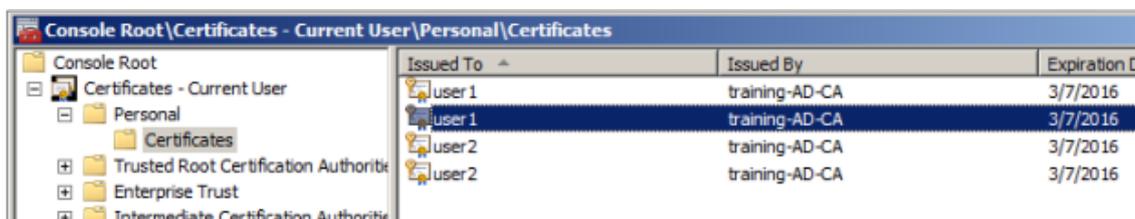
O modo de funcionamento do Secure Mail é verificando o atributo de objeto de usuário userCertificate por meio de consultas LDAP. Você pode ler o valor na guia **Editor de atributos**. Se este campo está vazio ou tem o certificado de usuário incorreto para criptografia, o Secure Mail não pode criptografar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



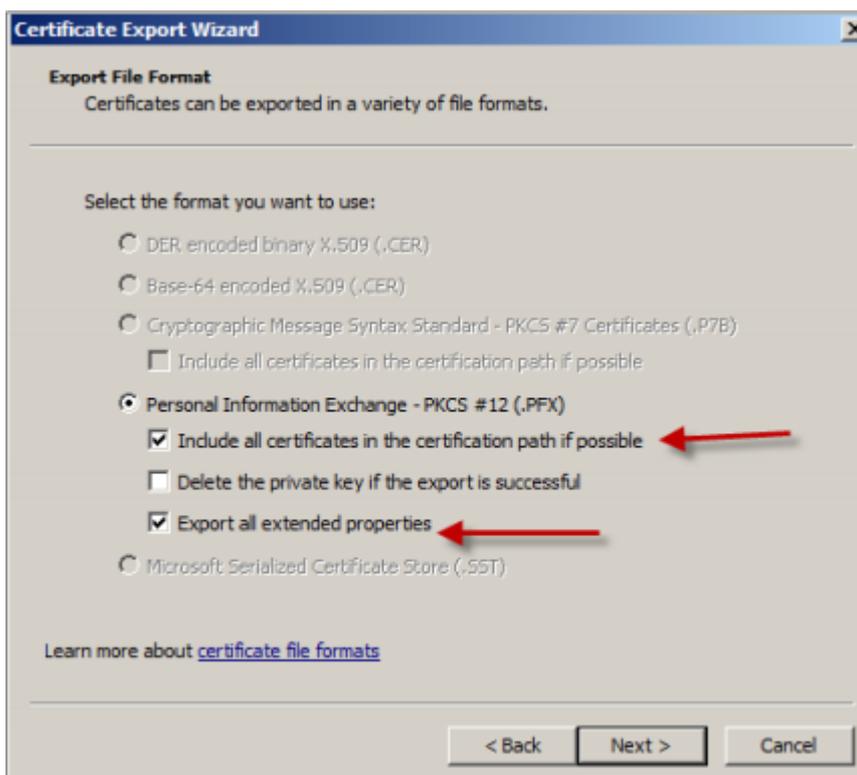
Exportação de certificados de usuário

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”.



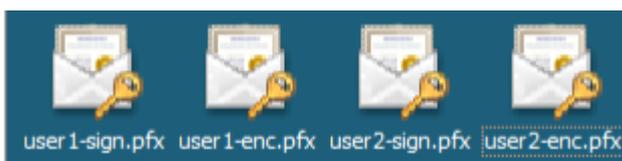
2. Clique com o botão direito do mouse no certificado e, em seguida, clique em **Todas as Tarefas > Exportar**.
3. Exportar a chave privada selecionando **Sim, exportar a chave privada**.
4. Assinale as caixas de seleção **Incluir todos os certificados no caminho de certificação, se possível** e **Exportar todas as propriedades estendidas**.



5. Quando você exportar o certificado, repita o mesmo procedimento para o restante certificados para usuários.

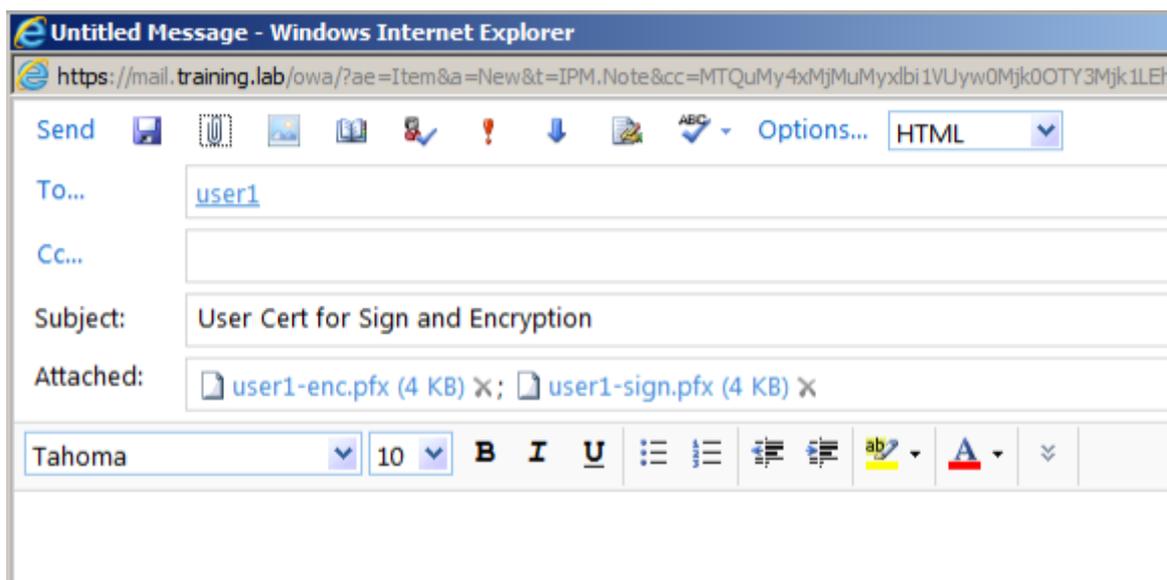
Nota:

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.



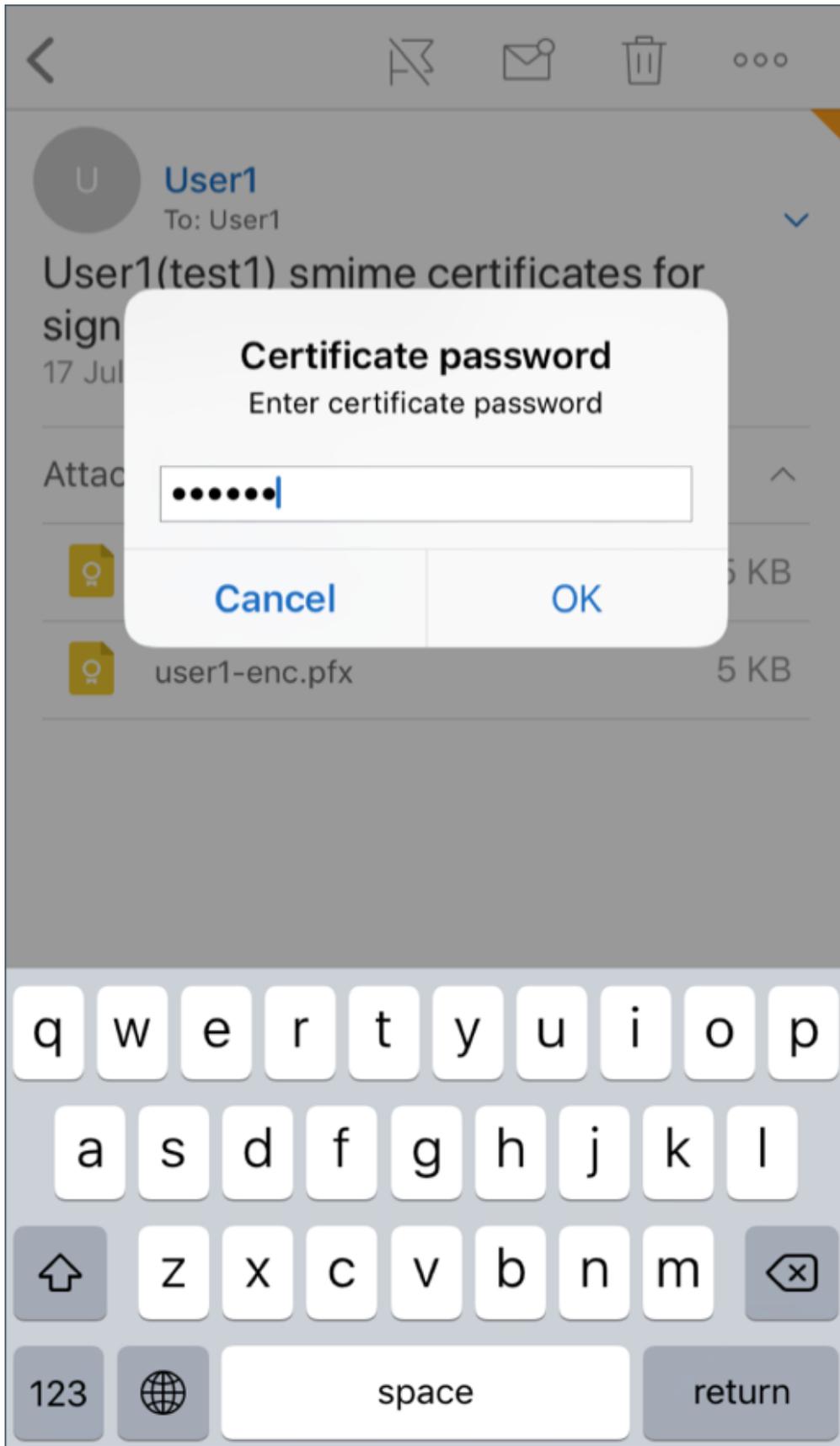
Repetir o mesmo procedimento para User2 ou outros usuários no domínio.

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.

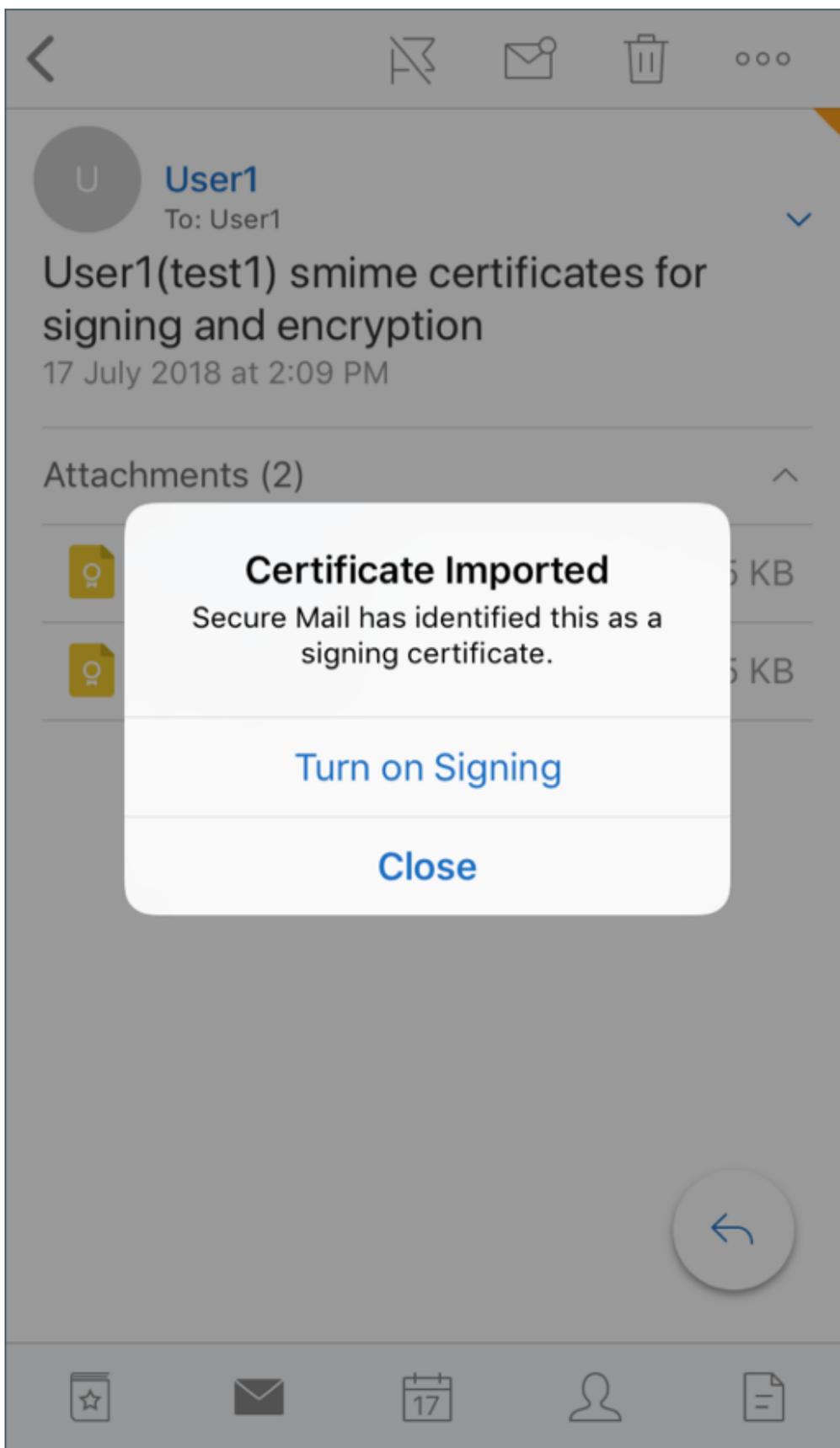
Para habilitar o S/MIME com certificados individuais de assinatura e criptografia

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.

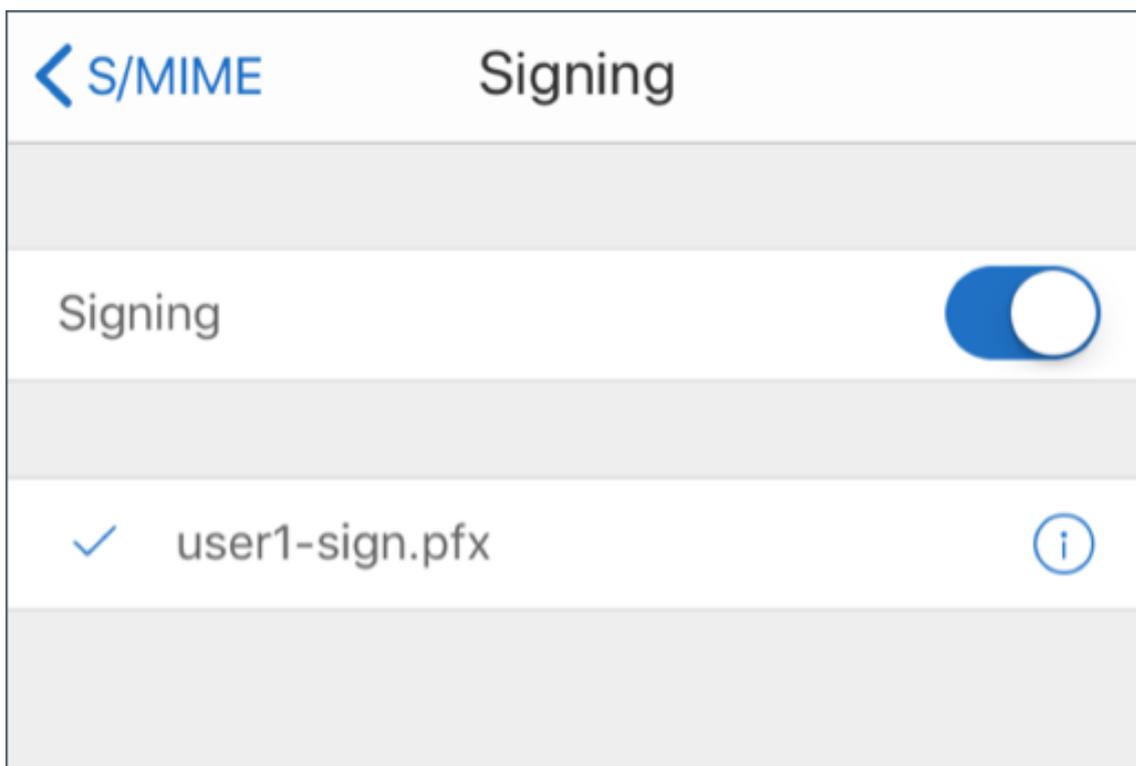
4. Toque em **Ativar a assinatura**



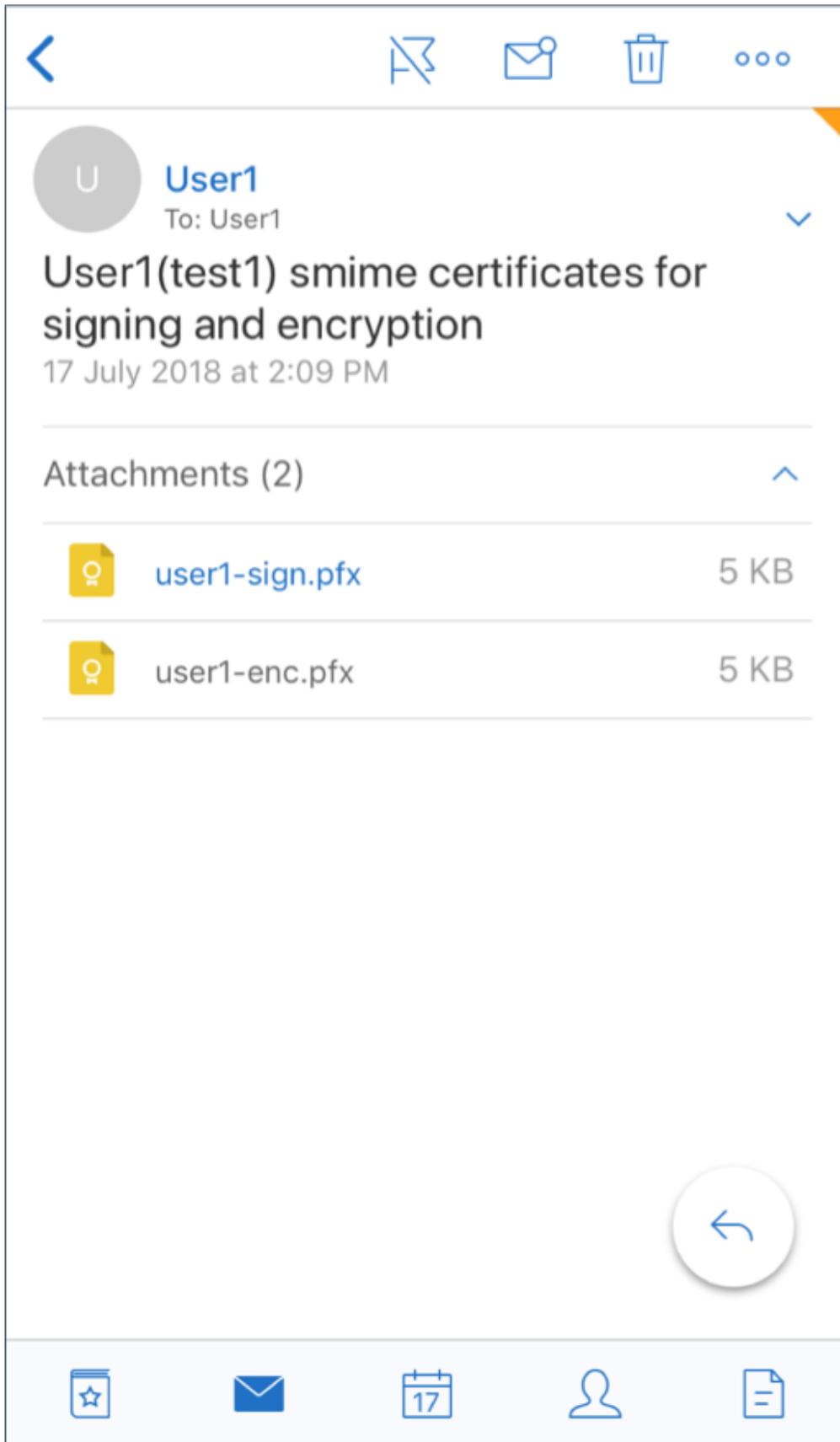
5. Alternativamente, você pode navegar para **Configurações** > e **S/MIME** e tocar em S/MIME para ativar o certificado de assinatura.

Settings	Done
Out of Office	Off
MAIL	
Ask Before Deleting	
Organize by Conversation	
Load Attachments on WiFi	
Show Pictures	
Sync Mail Period	3 days
Check Spelling	
S/MIME	
Offline Files	0 MB
Signature	
Swipe Options	
Preview Lines	1 Line
CALENDAR	

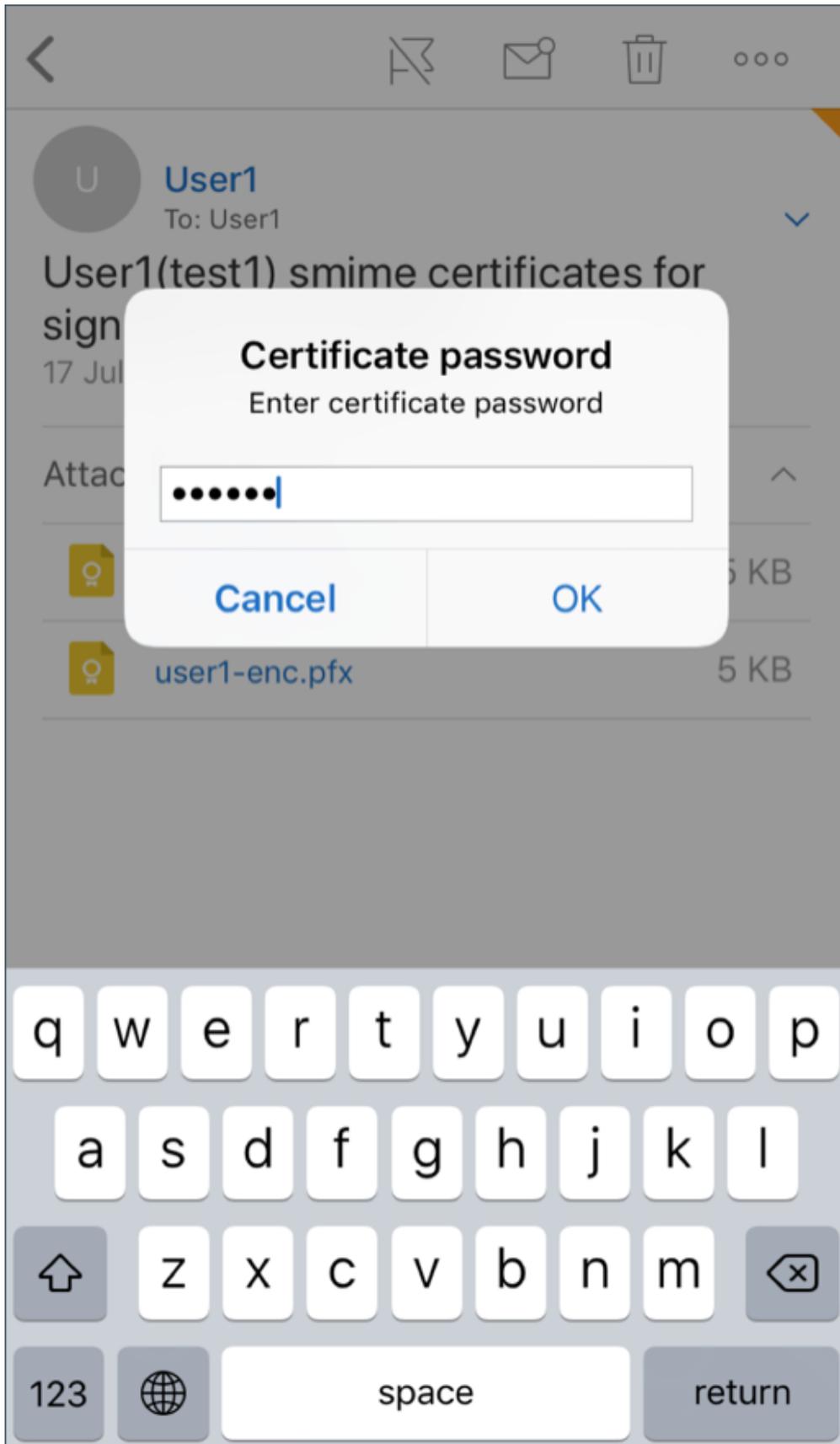
6. Na tela **Assinatura**, verifique se o certificado de assinatura correto foi importado.



7. Volte para o email e toque no certificado de criptografia para baixar e importar.

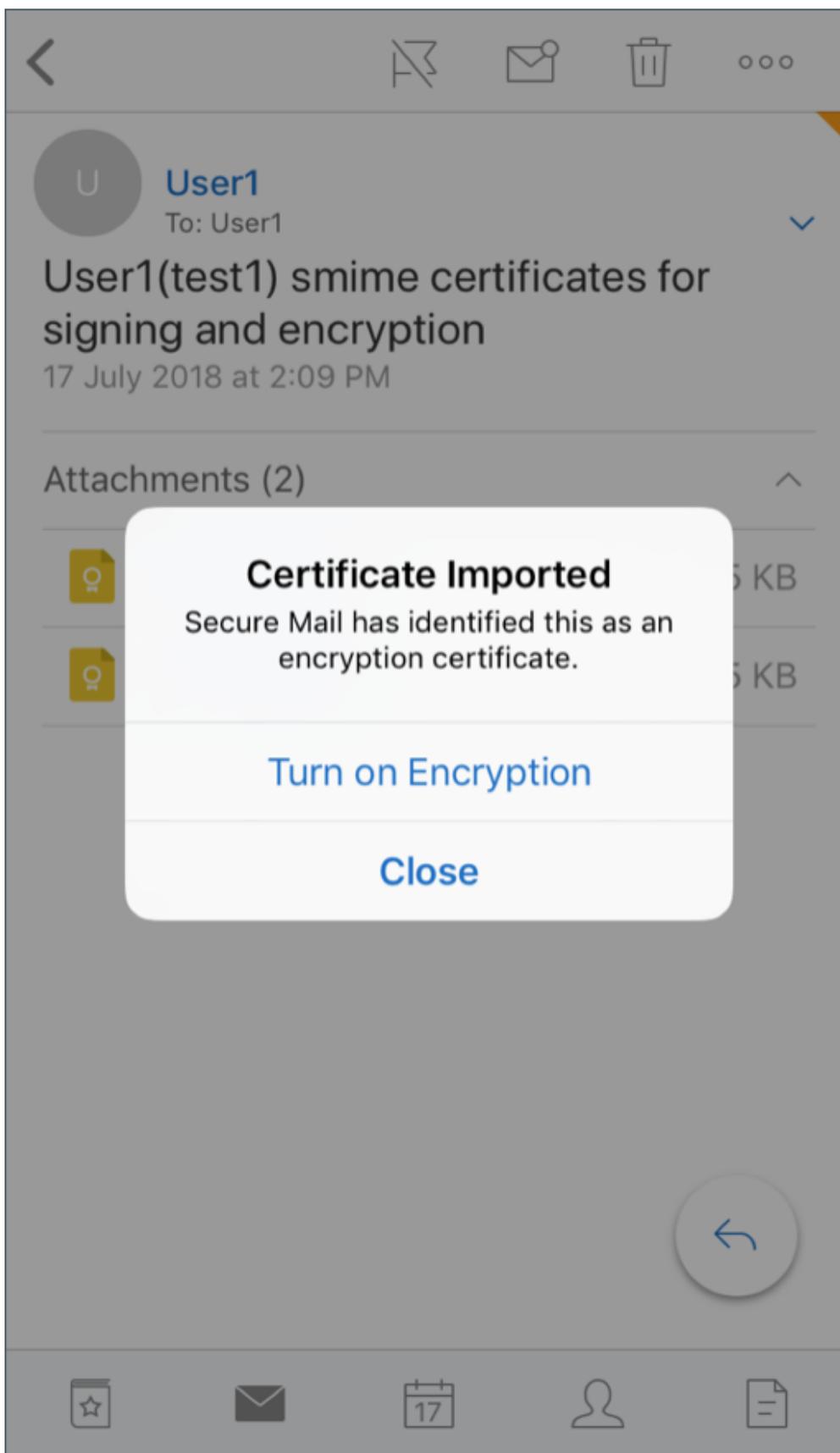


8. Digite a senha atribuída à chave privada quando o certificado de criptografia foi exportado do servidor.

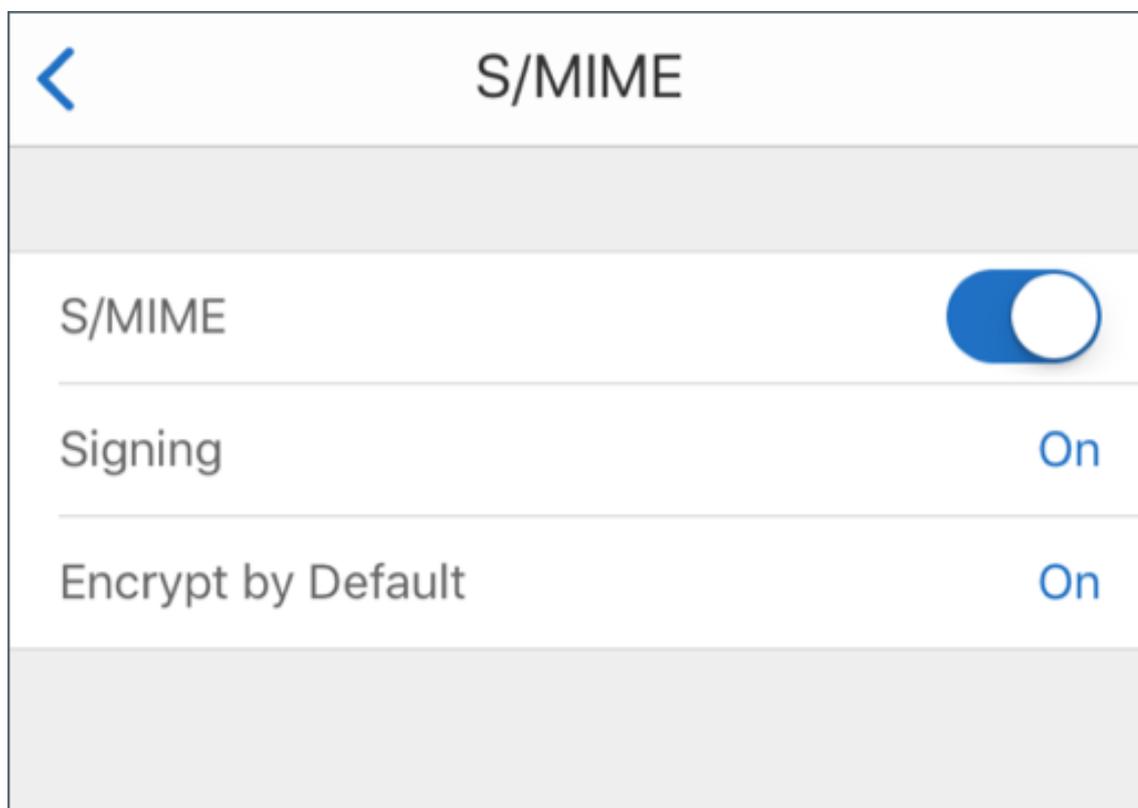


Seu certificado foi importado.

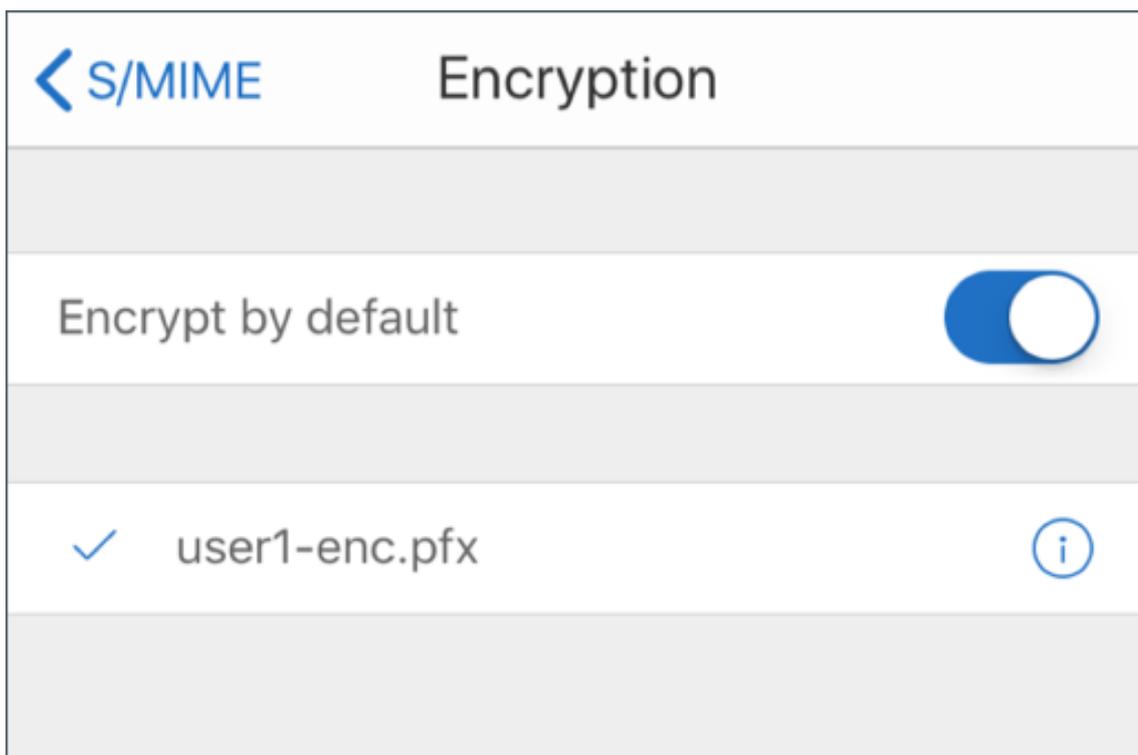
9. Toque em **Ativar a criptografia**



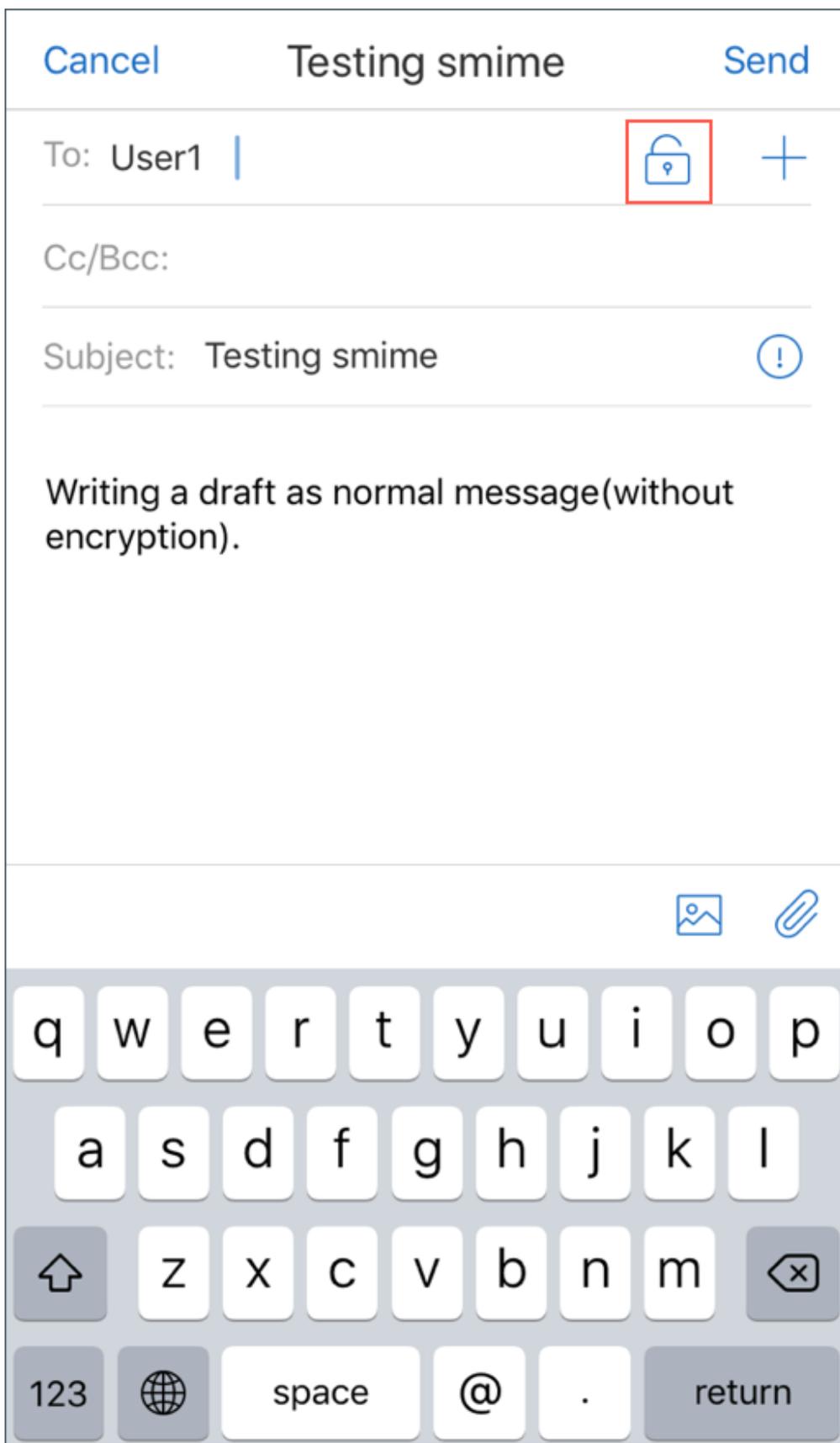
10. Alternativamente, você pode navegar para **Configurações** > e **S/MIME** e tocar em S/MIME para ativar **Criptografar como padrão**.



11. Na tela **Criptografia**, verifique se o certificado de criptografia correto foi importado.

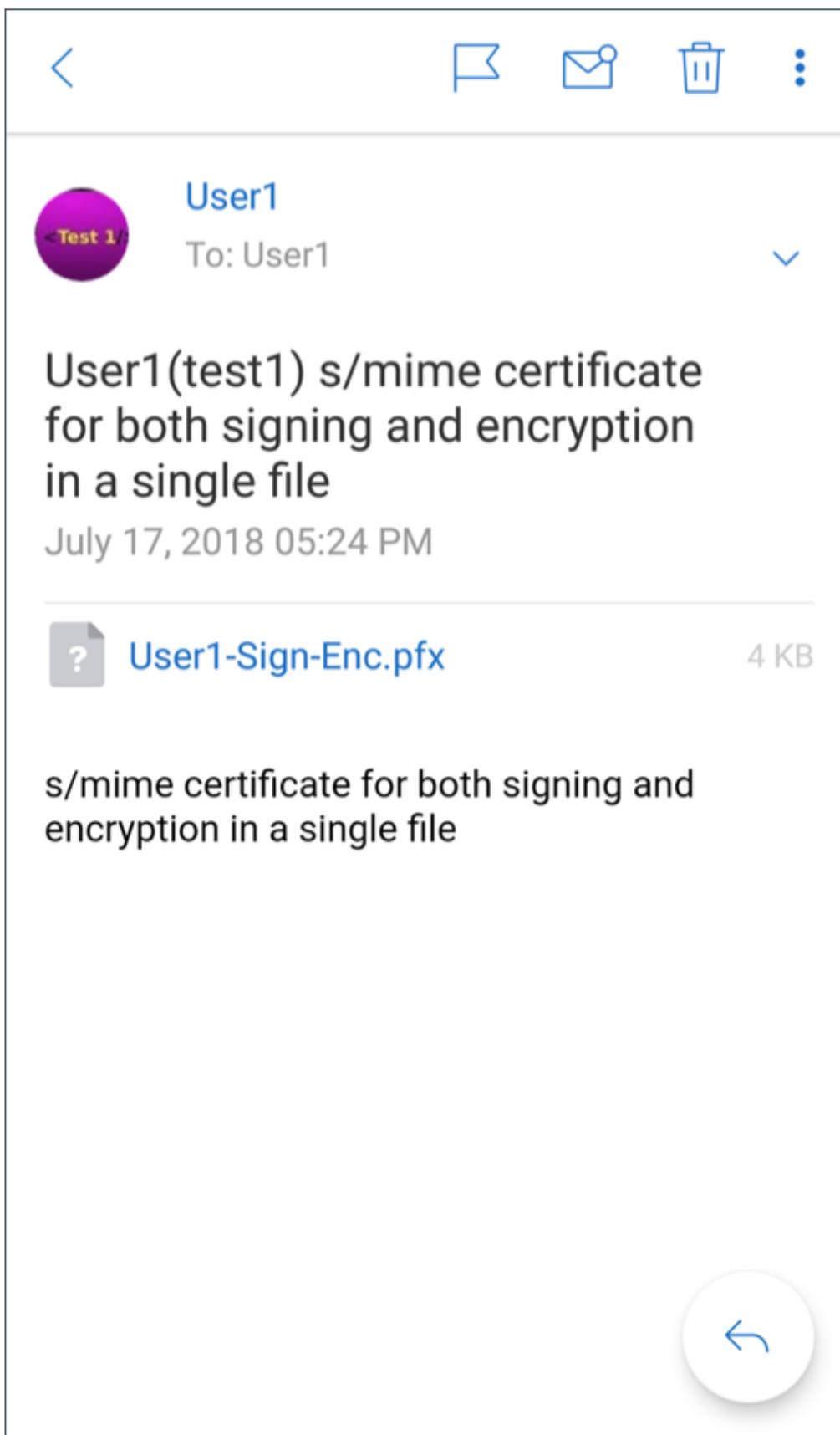
**Nota:**

- 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.

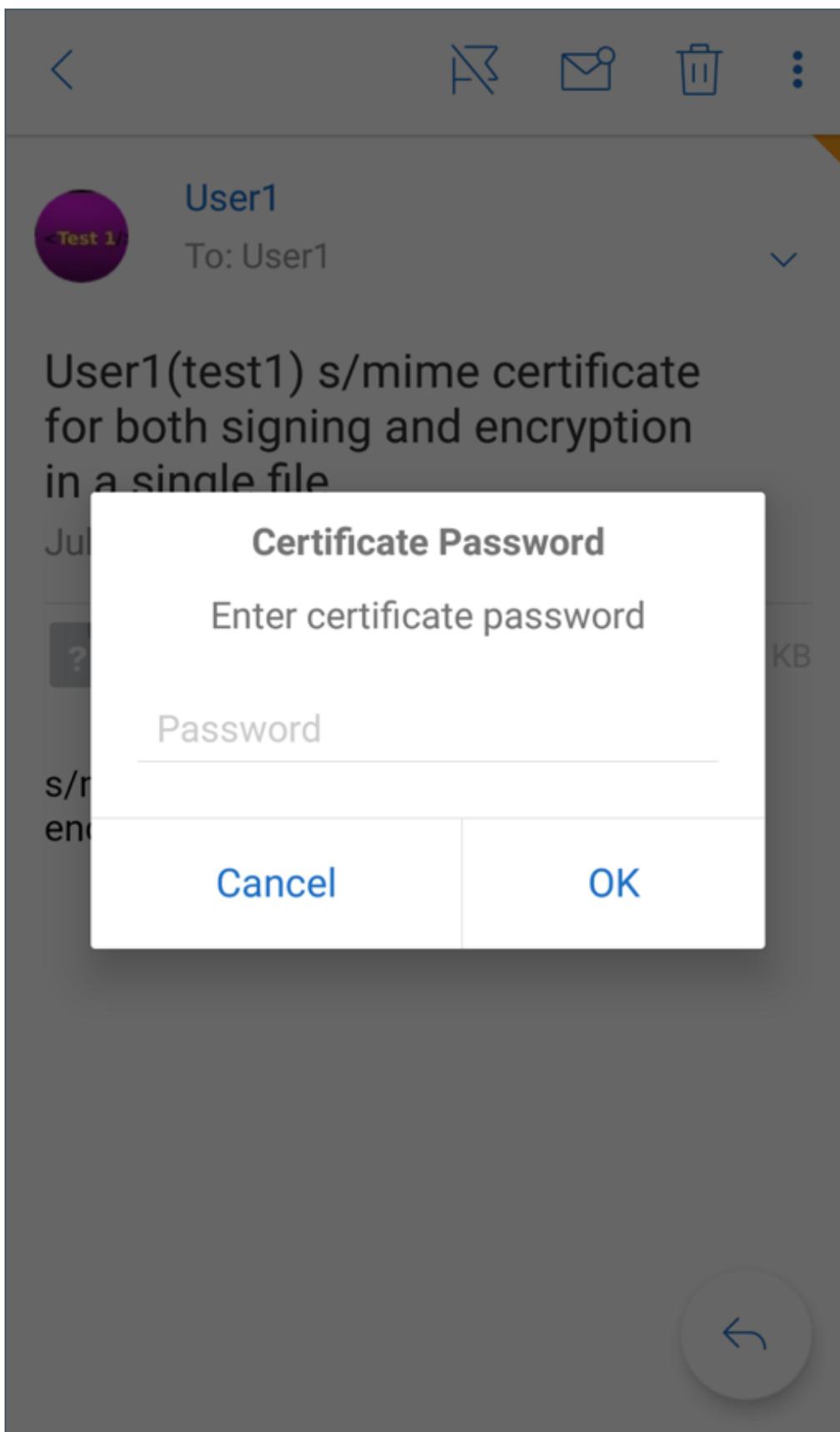


Para habilitar o S/MIME com um único certificado de assinatura e criptografia

1. Abra o Secure Mail e navegue até o e-mail que contém o certificado S/MIME.

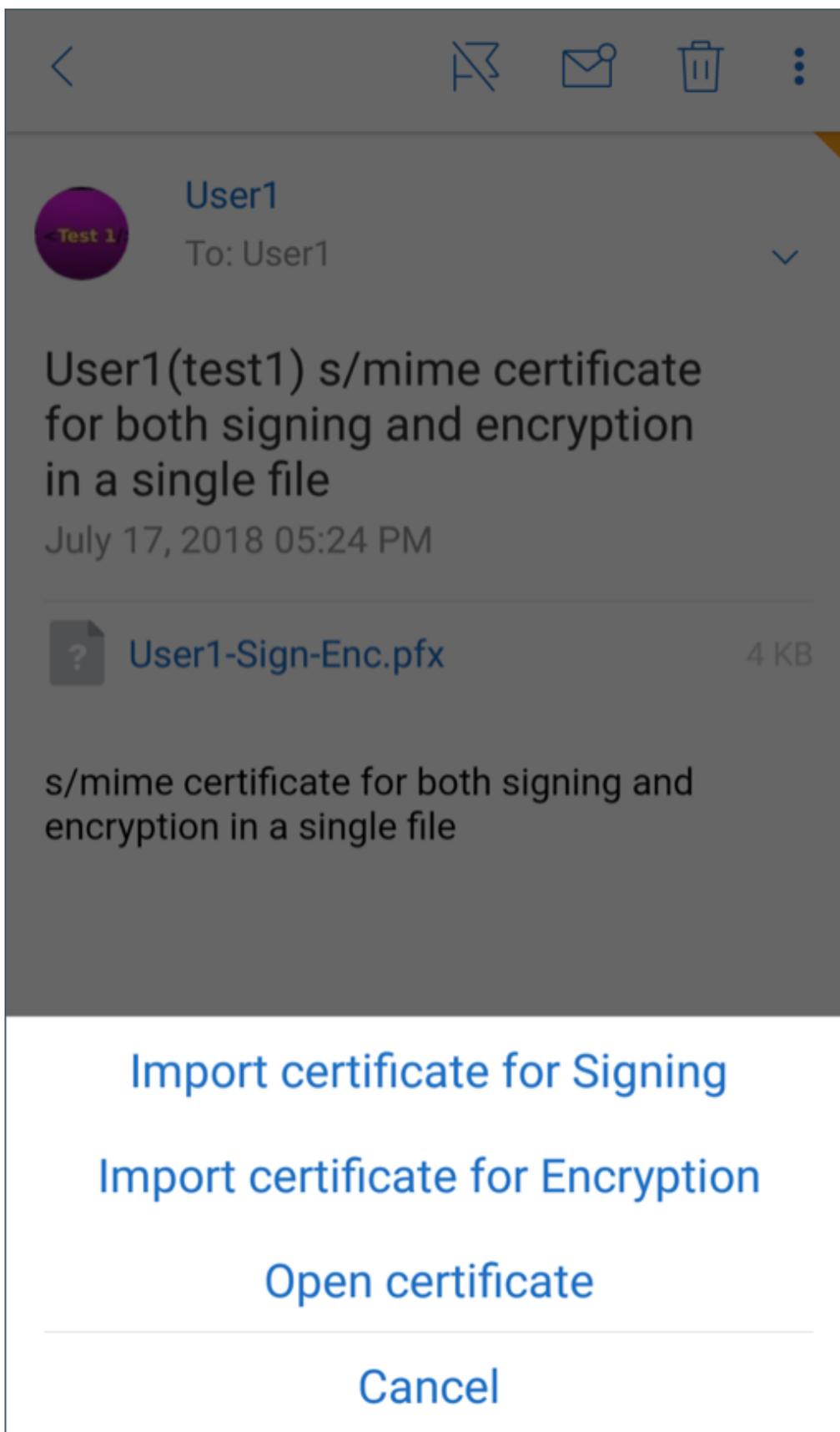


2. Toque no certificado S/MIME para baixar e importar.
3. Digite a senha atribuída à chave privada quando o certificado foi exportado do servidor.



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.



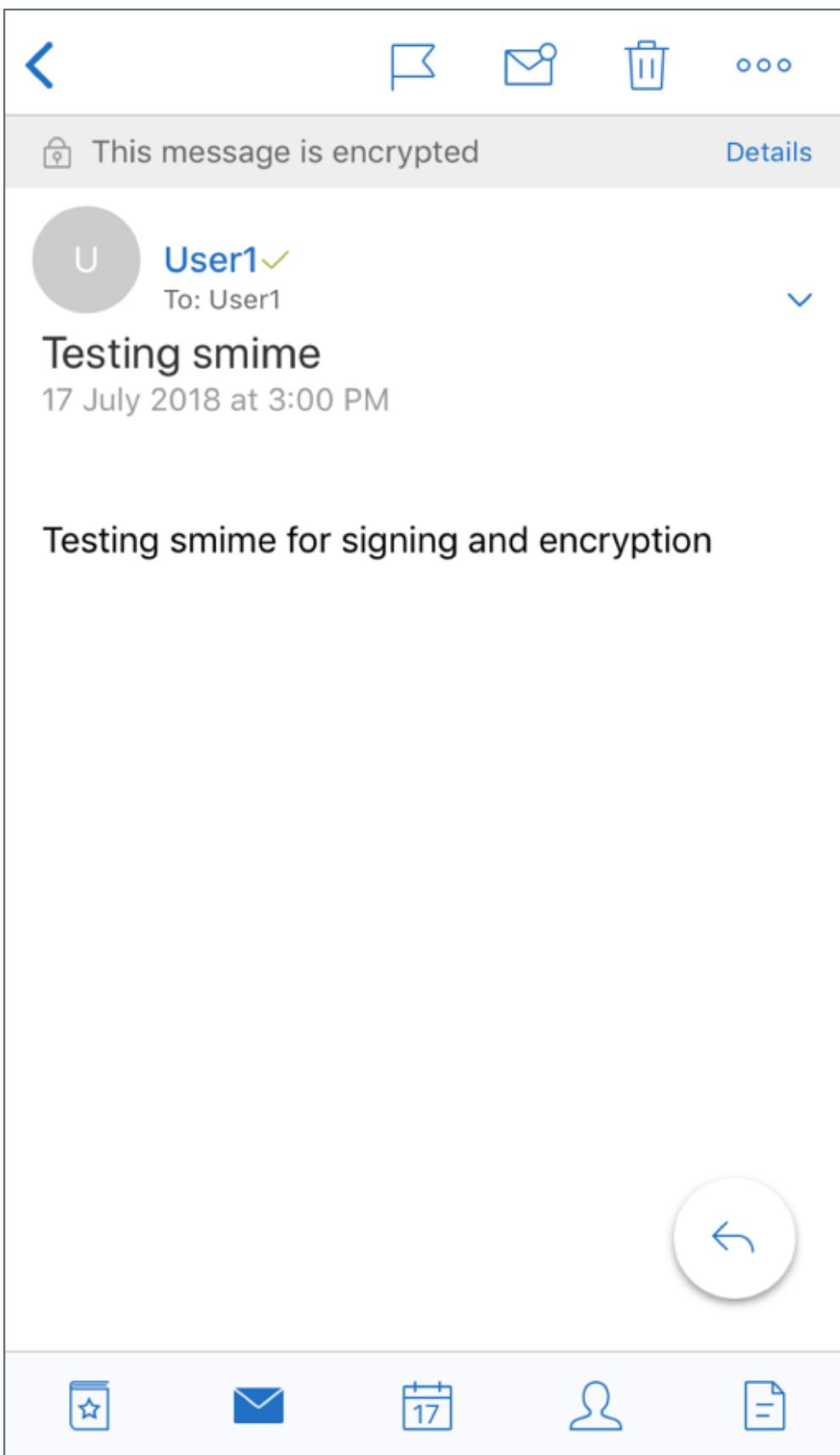
Seu certificado foi importado.

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.

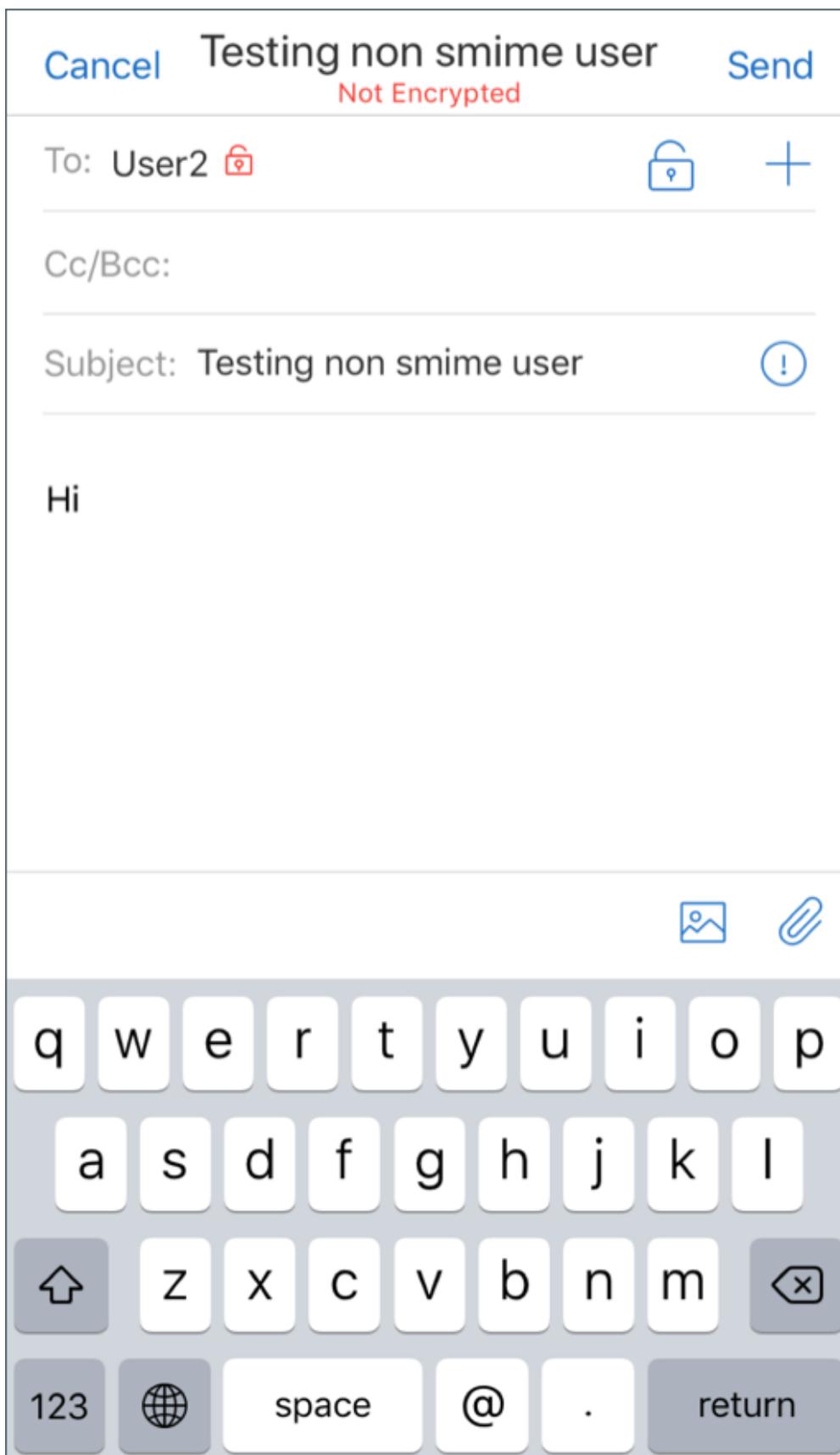
A imagem a seguir mostra um exemplo de uma mensagem criptografada conforme lida pelo destinatário.



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

The screenshot shows a contact card for 'User1'. At the top left is a back arrow. Below it is a circular profile picture with the letter 'T' and the name 'User1'. A link with a downward arrow icon says 'Save to Contacts'. The card is divided into sections by horizontal lines: 'SIGNING' with a green checkmark, 'The sender has a trusted certificate' with a 'View Certificate' link, 'INTERNET' with the email address 'test1@workxen.net', 'ALIAS' with the alias 'test1', and 'FACETIME' with a 'FaceTime' label and icons for video call and voice call. At the bottom is a navigation bar with icons for favorites, mail, calendar, contacts, and documents.

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

December 9, 2021

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 estas 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 Serviço de Descoberta Automática da Microsoft, consulte [Autodiscovery service in Exchange Server](#).

Considerações de segurança

December 9, 2021

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.

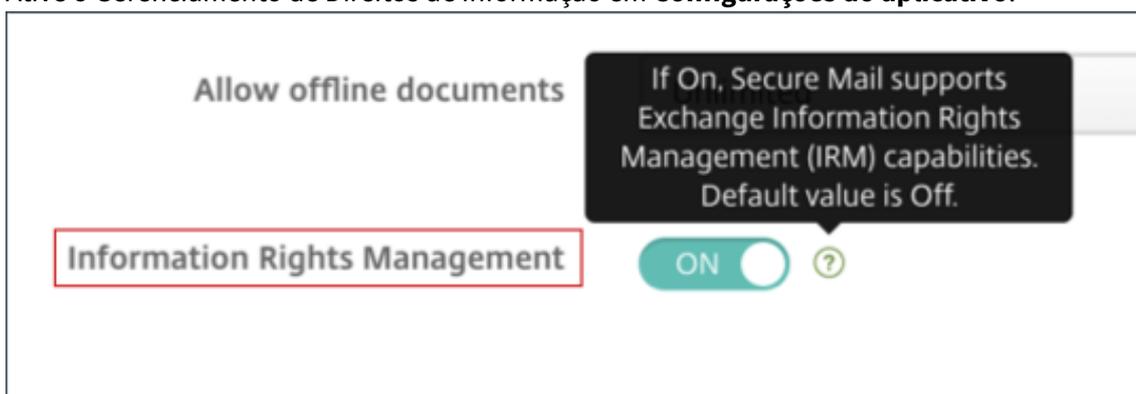
Suporte à proteção de direitos de e-mail Microsoft IRM e AIP

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 login 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**.

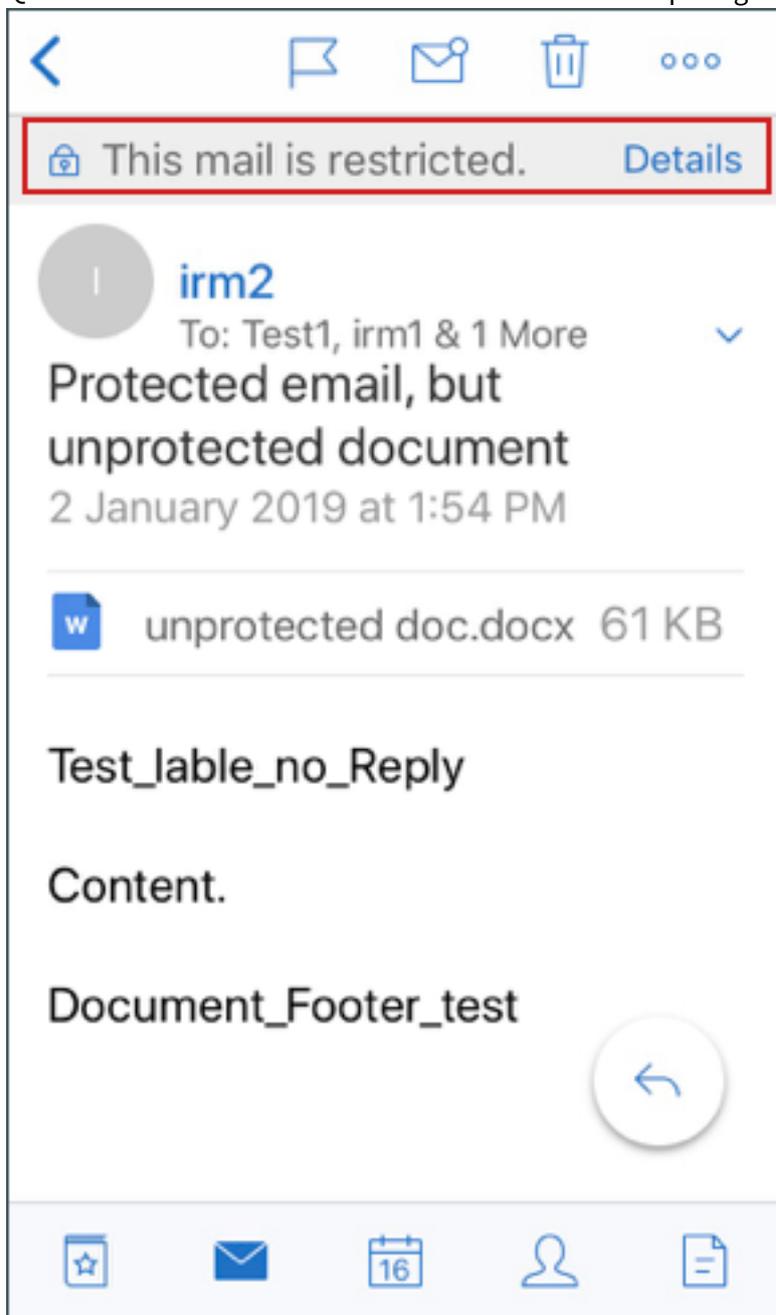


Nota:

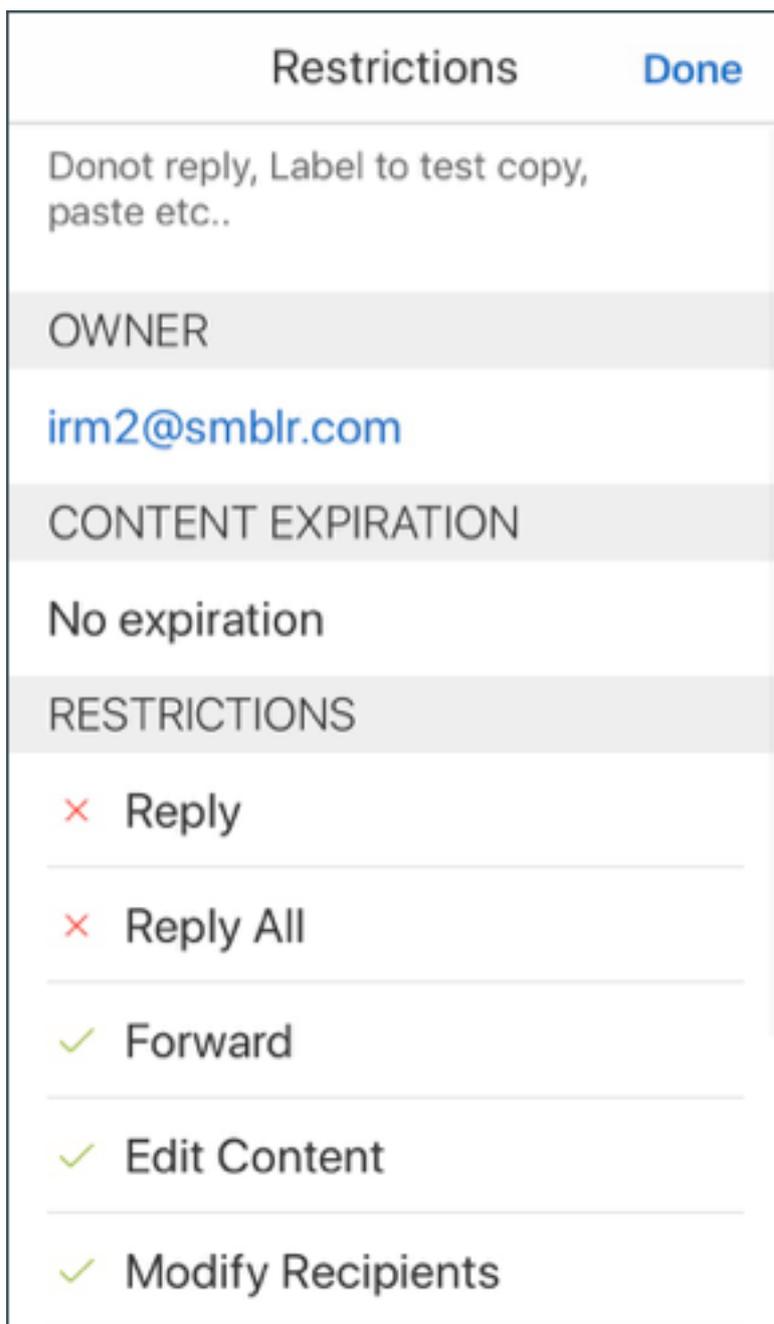
Ative o Gerenciamento de Direitos de Informação para iOS e Android.

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**.

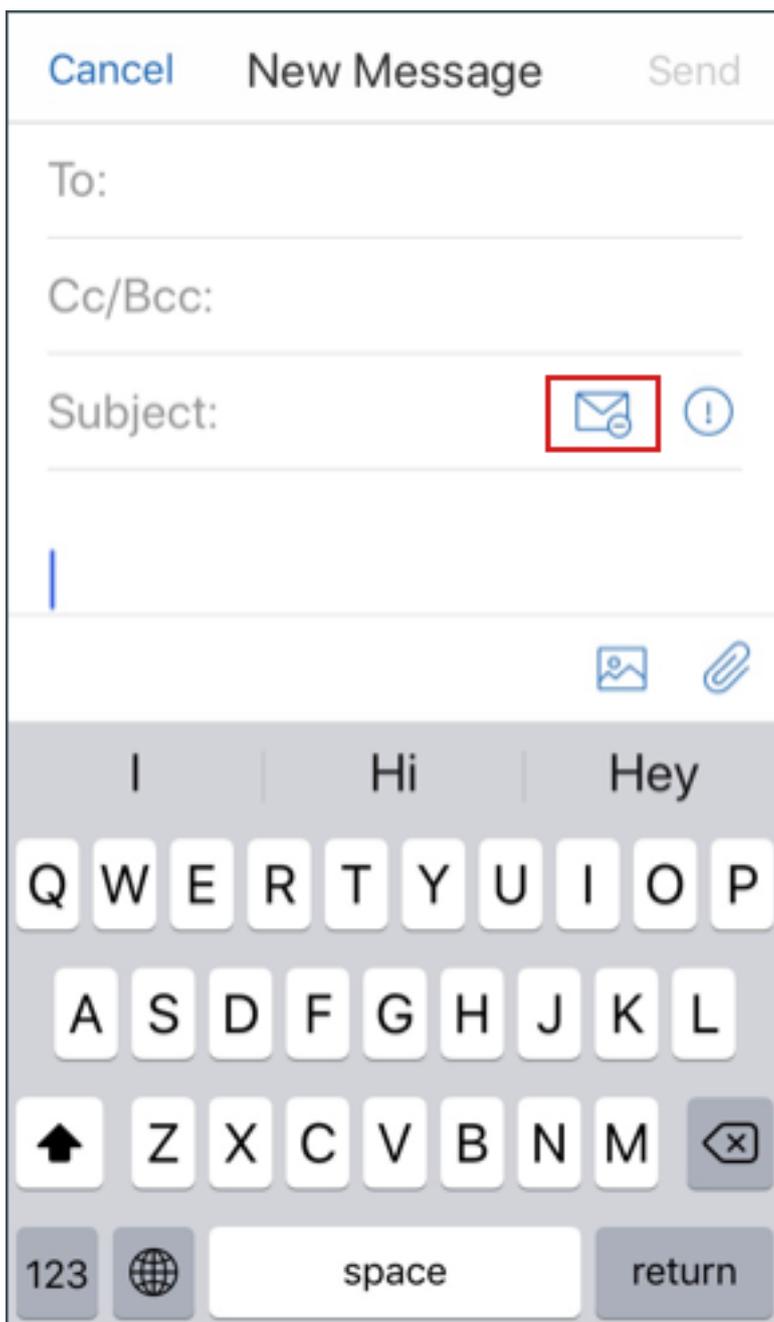


Quando você redige um email protegido por direitos

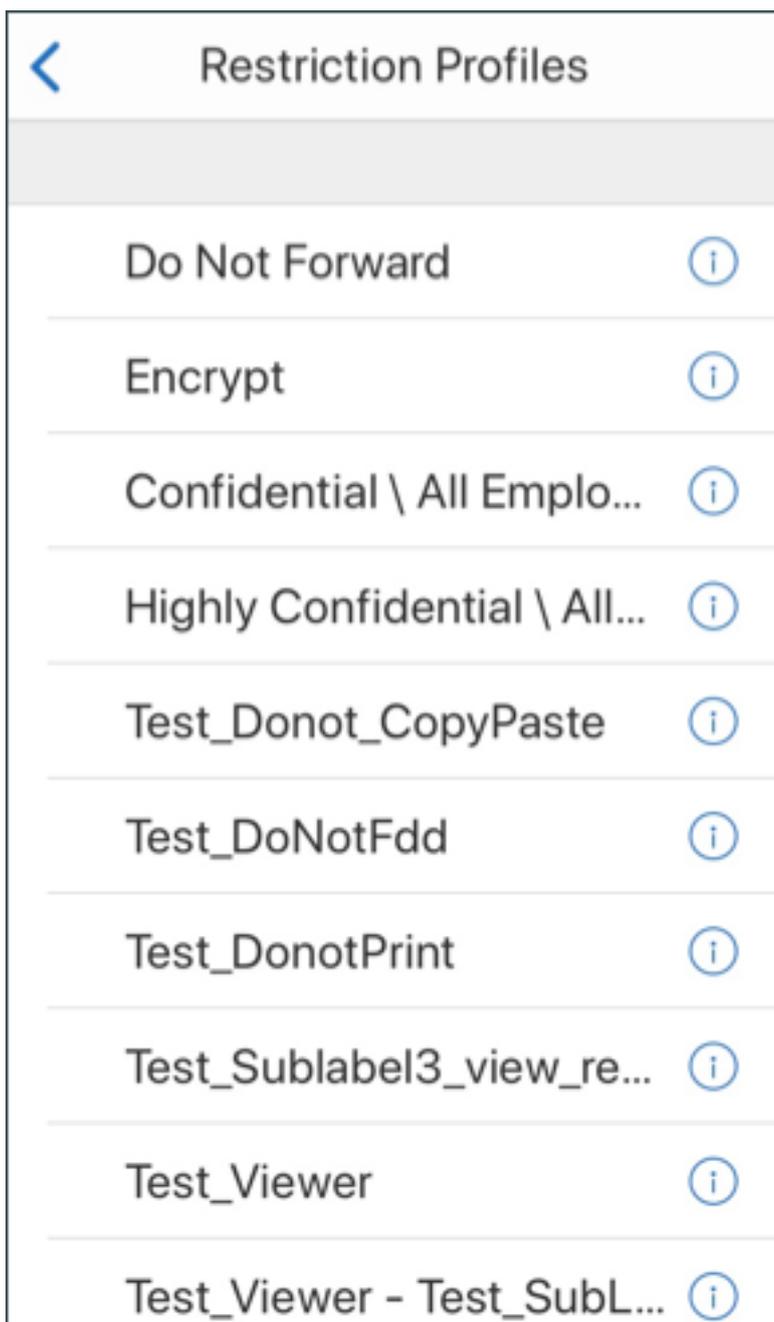
Quando os usuários redigem um email, eles podem definir perfis de restrição para habilitar a proteção de email.

Para definir restrições ao seu email:

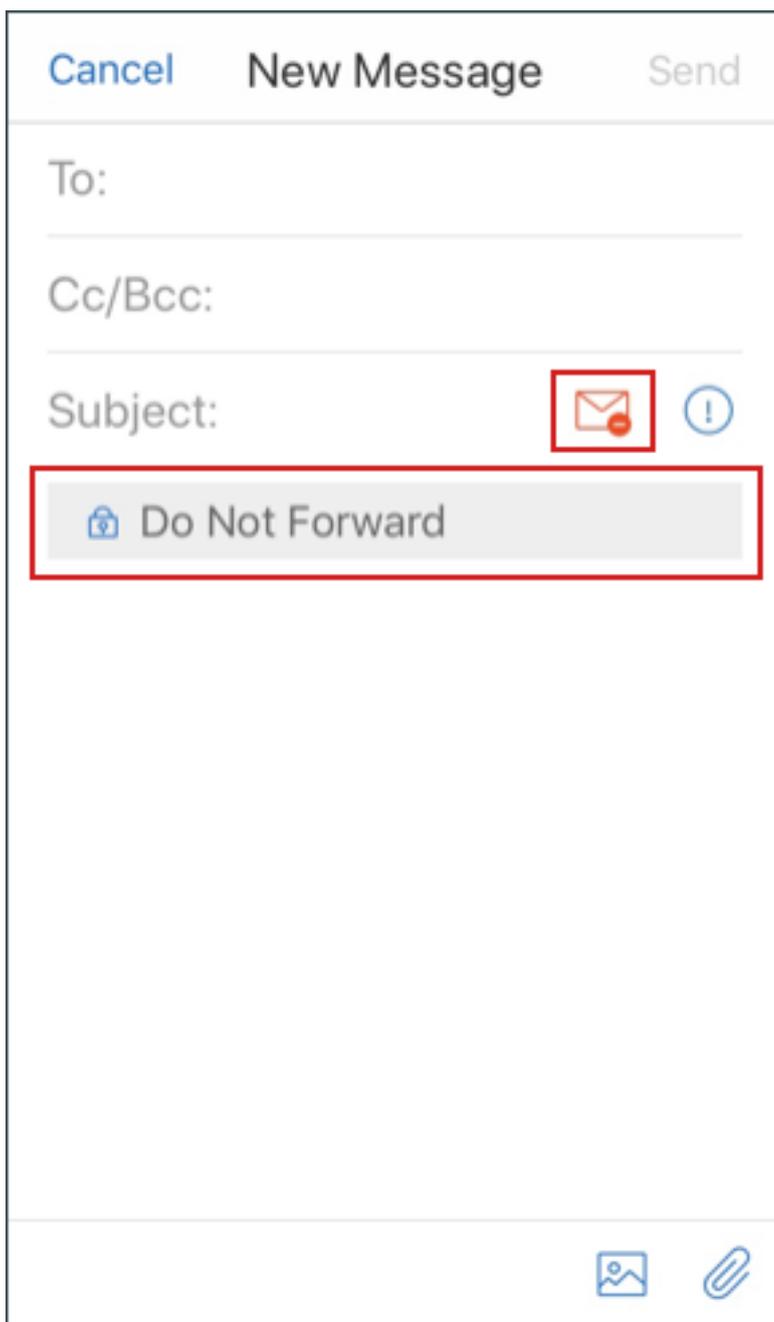
1. Faça login no Secure Mail e toque no ícone **Redigir**.
2. Na tela de redação, toque no ícone **Restrição de email**.



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:

- Revise 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

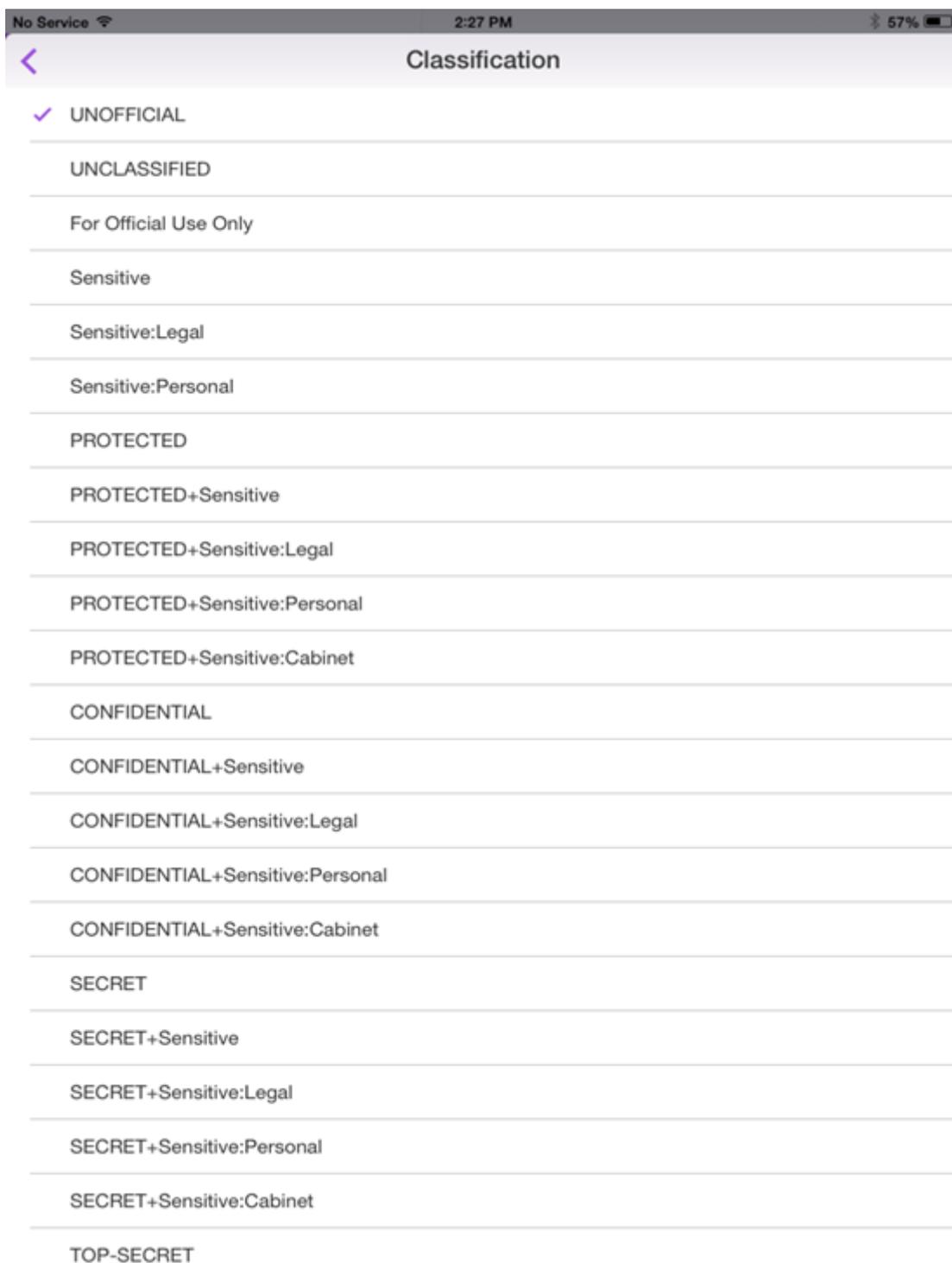
Secure Mail.

- 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: Planejamento [SEC = PROTECTED, DLM = Sensitive]
- Assunto: Planejamento [DLM = Sensitive]
- Assunto: Planejamento [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 Secure Mail,

consulte a proteção de dados da [Australian Signals Directorate Data Protection](#). 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 > Aplicativos > Adicionar** e clique em **MDX**. Para obter uma 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 iOS

February 7, 2022

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

Criar reuniões do Microsoft Teams em eventos do Calendário do Secure Mail

No Secure Mail para iOS, você pode criar convites para reuniões do Microsoft Teams enquanto cria eventos de calendário. Para criar uma reunião do Microsoft Teams, ative o botão de alternância **Reunião do Microsoft Teams**. O link do convite da reunião e os detalhes são enviados automaticamente com os detalhes do evento. Para obter mais informações, consulte [Criar reuniões do Microsoft Teams em eventos do Calendário do Secure Mail](#)

Pré-requisitos:

Certifique-se de que o administrador global do Azure Active Directory execute o seguinte:

- Habilite a autenticação moderna (OAuth) e certifique-se de que você é um usuário da caixa de correio do Exchange Online com uma licença válida do Microsoft Teams.
- Fornece o consentimento de administrador de todos os locatários para o aplicativo Secure Mail.
- Configure sua conta do Exchange no aplicativo Secure Mail e dê permissão de aplicativo para que todos os usuários entrem. Veja a tela a seguir:

- Ative a política de integração do Microsoft Teams.

Microsoft Teams integration ON ?

Limitações:

Para reuniões criadas no Secure Mail, atualmente o recurso tem as seguintes limitações no Calendário do Microsoft Outlook:

- A opção **Ingressar online** não está disponível
- A notificação **A reunião foi iniciada** não está disponível

Minimizar rascunhos

No Secure Mail para iOS, você pode minimizar um rascunho enquanto estiver redigindo um e-mail e navegar dentro do aplicativo. Esse recurso está disponível em dispositivos que executam o iOS 13 e posterior. Para obter a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Minimizar um rascunho de e-mail](#).

Denunciar e-mails de phishing com cabeçalhos MIME

No Secure Mail para iOS, 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 MIME 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 um e-mail de phishing como um anexo](#).

Suporte para WkWebView

O Secure Mail para iOS suporta WKWebView. Esse recurso melhora a maneira como os e-mail e eventos de calendário do Secure Mail são renderizados no seu dispositivo.

Suporte para Slack EMM

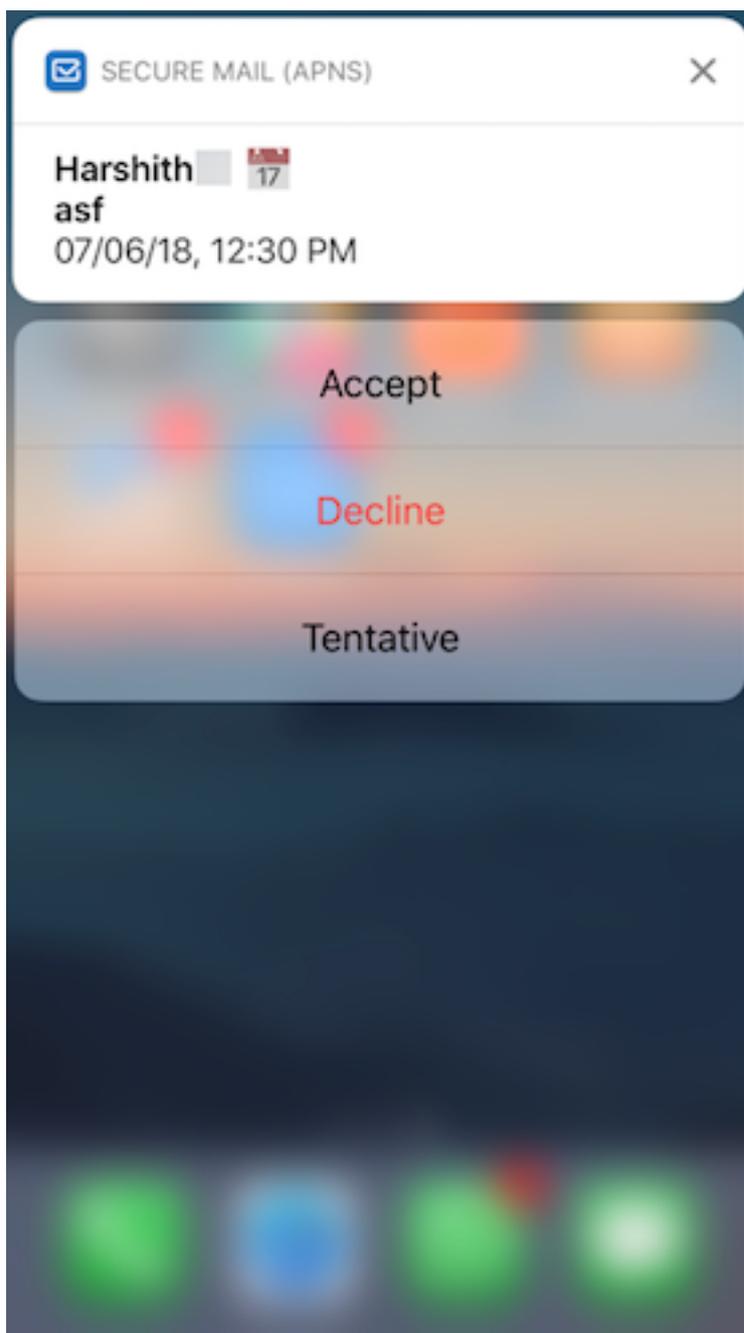
O Slack EMM é para clientes Slack com o Enterprise Mobility Management (EMM) habilitado. O Secure Mail para iOS suporta o aplicativo **Slack EMM**, que permite que os administradores escolham a integração do Secure Mail com o aplicativo **Slack** ou com o aplicativo **Slack EMM**.

Notificações em grupo

Com o recurso de notificação de grupo, as conversas em um thread de email são agrupadas. 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. O recurso requer o iOS 12.

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 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 [Notificações do Secure Mail](#).

Suporte para notificações por push avançadas em configurações da Microsoft

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**.

Suporte para S/MIME para credenciais derivadas

O Secure Mail para iOS 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 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 estas [Propriedades do cliente](#), e para o Endpoint Management consulte estas [Propriedades do cliente](#).

Para obter informações sobre como os dispositivos se registram usando credenciais derivadas, consulte [Registrar 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**.

Push notifications region Americas ⓘ

S/MIME certificate source Derived Credential ⓘ

Enable S/MIME during first Secure Mail startup OFF ⓘ

Calendar Web and Audio Options GoToMeeting and User Entered ⓘ

S/MIME public certificate source Exchange ⓘ

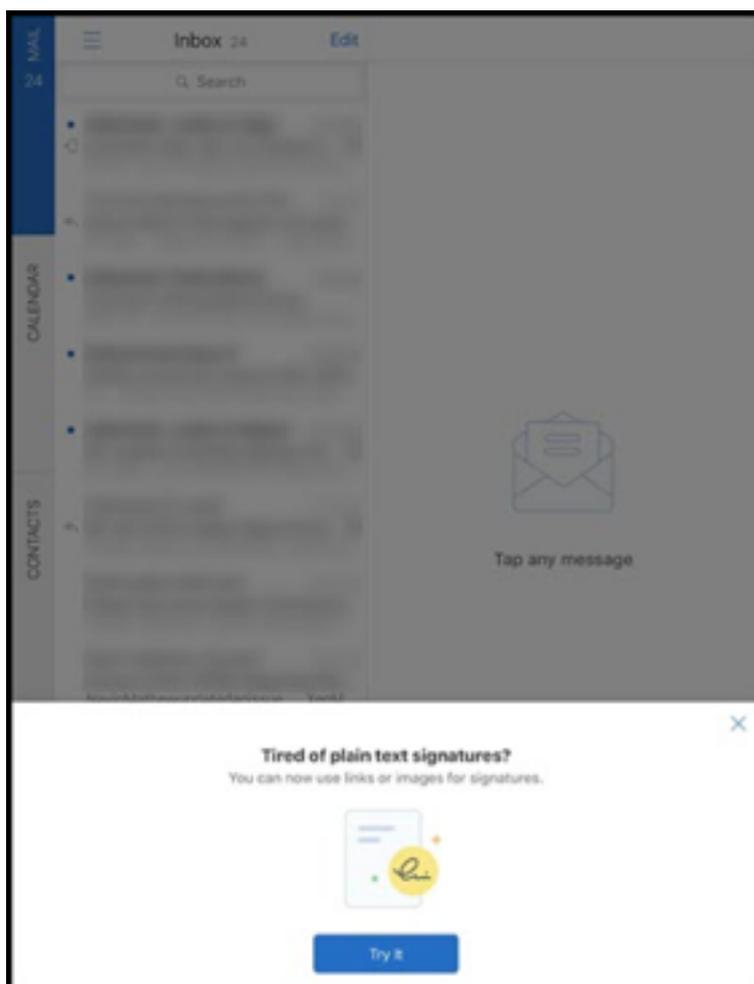
Ldap server address ⓘ

Ldap Base DN ⓘ

Back Next >

Assinaturas em Rich Text

Você pode usar imagens ou links na sua assinatura de email. Para atualizar sua assinatura, basta copiar e colar imagens ou links no campo de assinatura.



Para adicionar uma assinatura de rich text

1. Copie a imagem ou URL que você deseja usar.
2. Navegue até **Secure Mail > Configurações > Assinatura**.
3. Cole a imagem ou URL.

Como alternativa, você pode pressionar prolongadamente o campo de assinatura e tocar em **Inserir imagem** para selecionar uma imagem da sua galeria.

ID de chamador do Secure Mail

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 seu dispositivo. Você deve ativar o seguinte pré-requisito administrativo: No Citrix Endpoint Management, verifique se a política CallerIdSupportEnabled MDX está ativada.

Para obter a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Configurar ID do chamador](#).

Atribuir cores em Calendários

Para obter a documentação de ajuda do usuário sobre esse recurso de Calendário, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Atribuir cores para calendários sincronizados do Secure Mail](#).

Anexar arquivos do app Arquivos

No Secure Mail para iOS, você pode anexar arquivos do aplicativo nativo do iOS **Arquivos**. Para obter mais informações sobre o app Arquivos do iOS, consulte o artigo da Apple, [App Arquivos](#). Para obter a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Exibir e anexar arquivos](#).

Recurso de verificação ortográfica

A verificação ortográfica do Secure Mail interage com as configurações de Maiúsculas Automáticas e Verificar Ortografia do dispositivo em **Geral > Teclado** das seguintes maneiras:

Autocorreção no Dispositivo	Verificar ortografia no dispositivo	Verificar ortografia no Secure Mail	Comportamento
I	I	I	É exibido sublinhado vermelho. Quando tocada, a palavra é realçada em rosa e é exibida uma sugestão.
O	O	I	É exibida uma linha vermelha. Quando tocada, nenhuma sugestão é exibida.
I	I	O	Não é exibido sublinhado vermelho. Quando tocada, a palavra é realçada em rosa e é exibida uma sugestão

Autocorreção no Dispositivo	Verificar ortografia no dispositivo	Verificar ortografia no Secure Mail	Comportamento
0	0	0	Não aparece sublinhado vermelho, realce nem sugestões.
1	0	1	É exibido sublinhado vermelho. Quando tocada, a palavra é realçada em rosa e é exibida uma sugestão.
0	1	1	É exibido sublinhado vermelho. Quando tocada, a palavra é realçada em rosa e é exibida uma sugestão.
1	0	0	Não é exibido sublinhado vermelho. Quando tocada, a palavra é realçada em rosa e é exibida uma sugestão.
0	1	0	Não é exibido sublinhado vermelho. Quando tocada, a palavra é realçada em rosa e é exibida uma sugestão.

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.

A caixa de correio **Todas as contas** é o modo de exibição global por padrão. Este modo de exibição contém emails de todas as contas do Exchange que você tiver configurado no seu dispositivo.

A caixa de correio **Todas as contas** tem os seguintes itens de menu:

- Todos os anexos
- Entrada
 - Não lida(s)
 - Sinalizada
- Rascunhos
- Itens enviados
- Caixa de saída
- Itens excluídos

Embora o modo de exibição **Todas as contas** exiba os seus emails de várias contas coletivamente, 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

Todas as contas que você configurou aparecem como uma lista abaixo de **Todas as contas**. 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. Você pode exibir as pastas de subpastas tocando no ícone **V** ao lado da pasta.

As seguintes ações são limitadas a contas individuais apenas:

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

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.

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 **Calendário** 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.

Nota:

Quando você sai e inicia o Secure Mail, o aplicativo restaura as últimas configurações de calendário configurado no seu dispositivo.

Pesquisa

Você pode realizar uma pesquisa global no modo de exibição **Caixas de correio** ou **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.

Imprimir emails, eventos de calendário ou imagens incorporadas no iOS

Agora você pode imprimir emails, eventos de calendário ou imagens incorporadas do dispositivo iOS.

Pré-requisitos

Antes de começar, verifique se os seguintes requisitos foram atendidos:

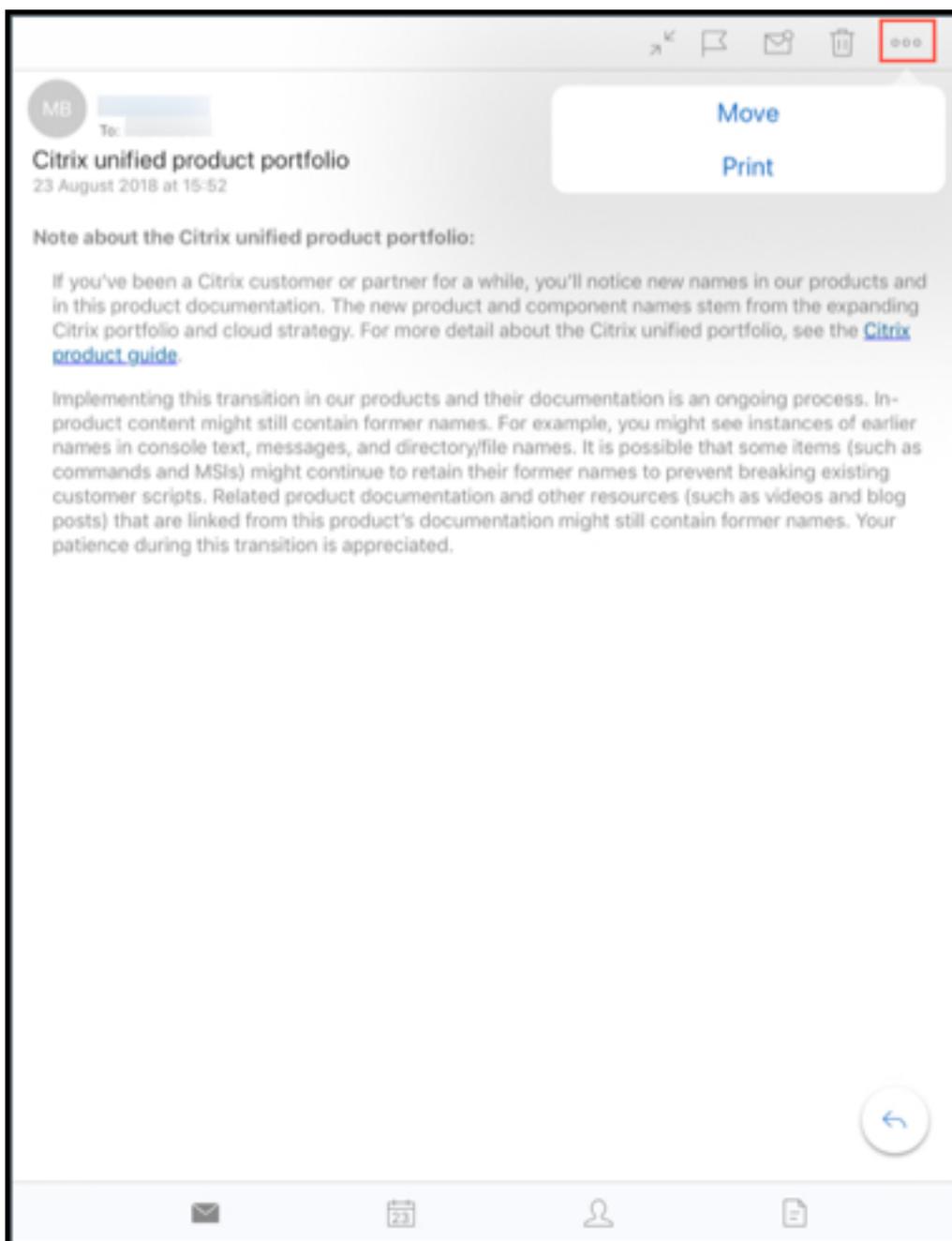
- A opção **Bloquear AirPrint** está definida como **Desativada**.

- A opção **Permitir que os visualizadores imprimam** está desativada no IRM.

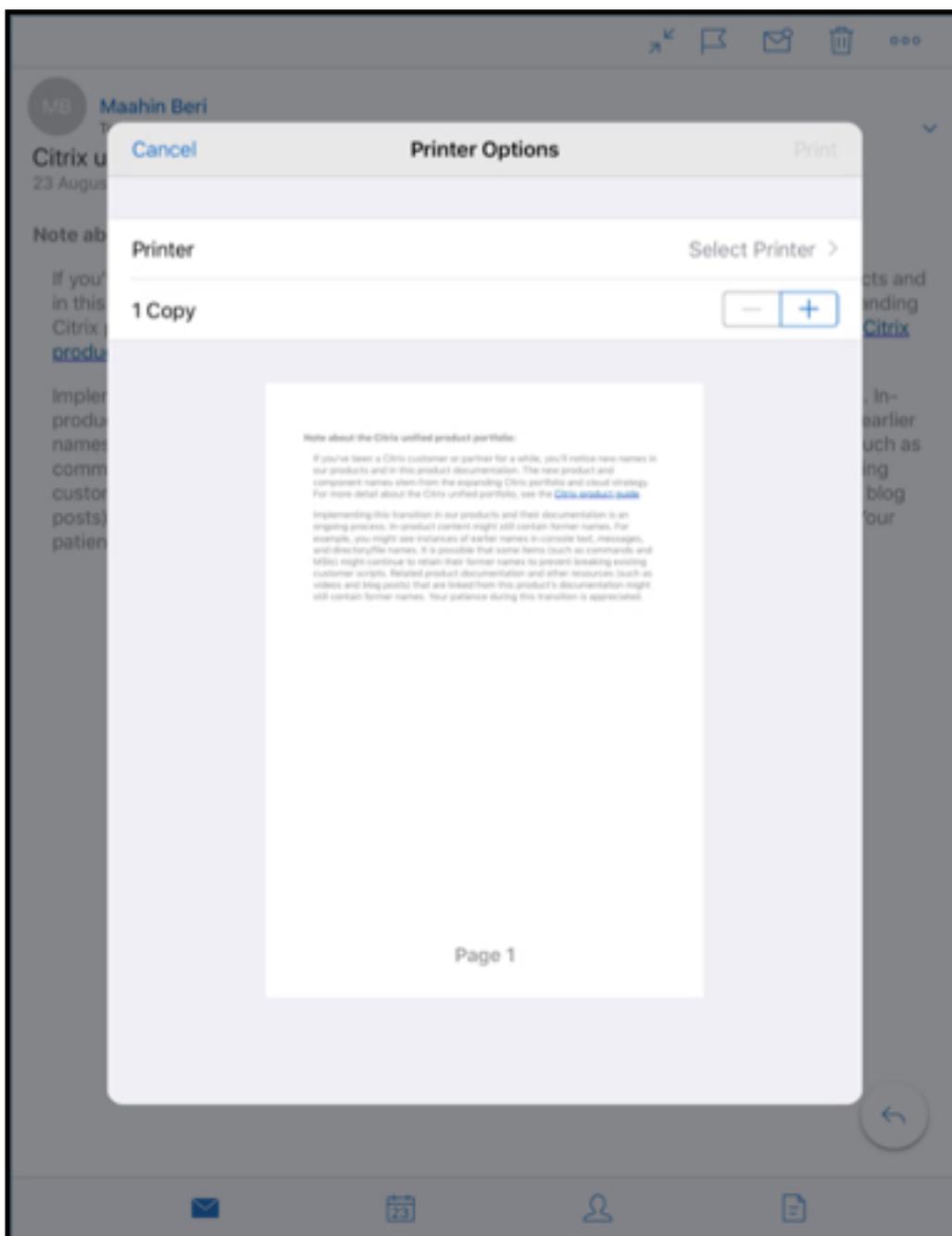
Como padrão, o recurso de impressão está ativado no Secure Mail para iOS. O recurso de impressão pode ser controlado pelo administrador com políticas administrativas por meio de Apple AirPrint ou de Gerenciamento de Direitos de Informação (IRM) da Microsoft. Nesses cenários, impressão um email, um evento de calendário ou uma imagem em linha não funcionam e poderá ser exibida uma mensagem de erro.

Para imprimir emails

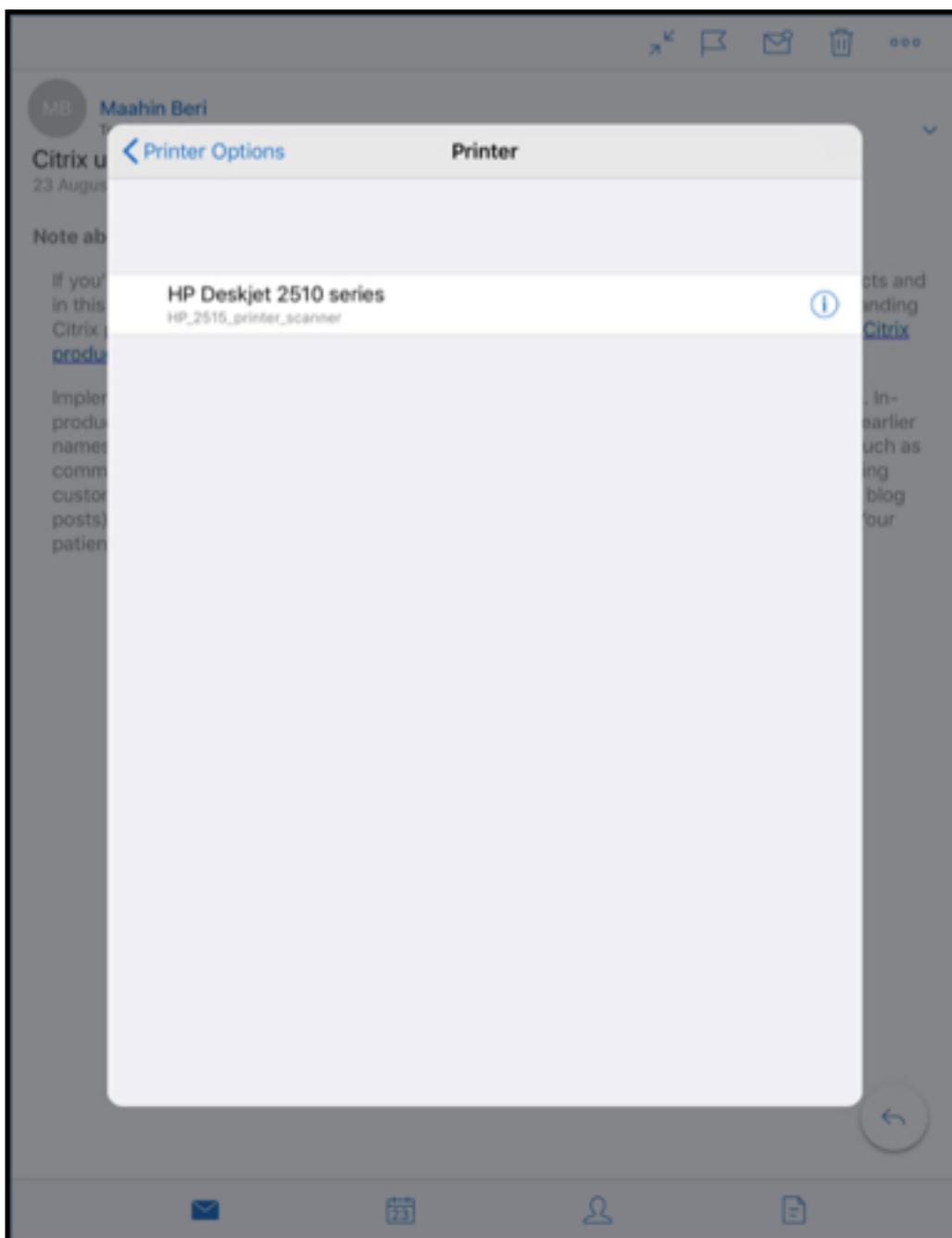
1. Abra o item de email que você deseja imprimir.
2. Toque no ícone Mais no canto superior esquerdo da tela. São exibidas as seguintes opções:
 - Mover
 - Impressão



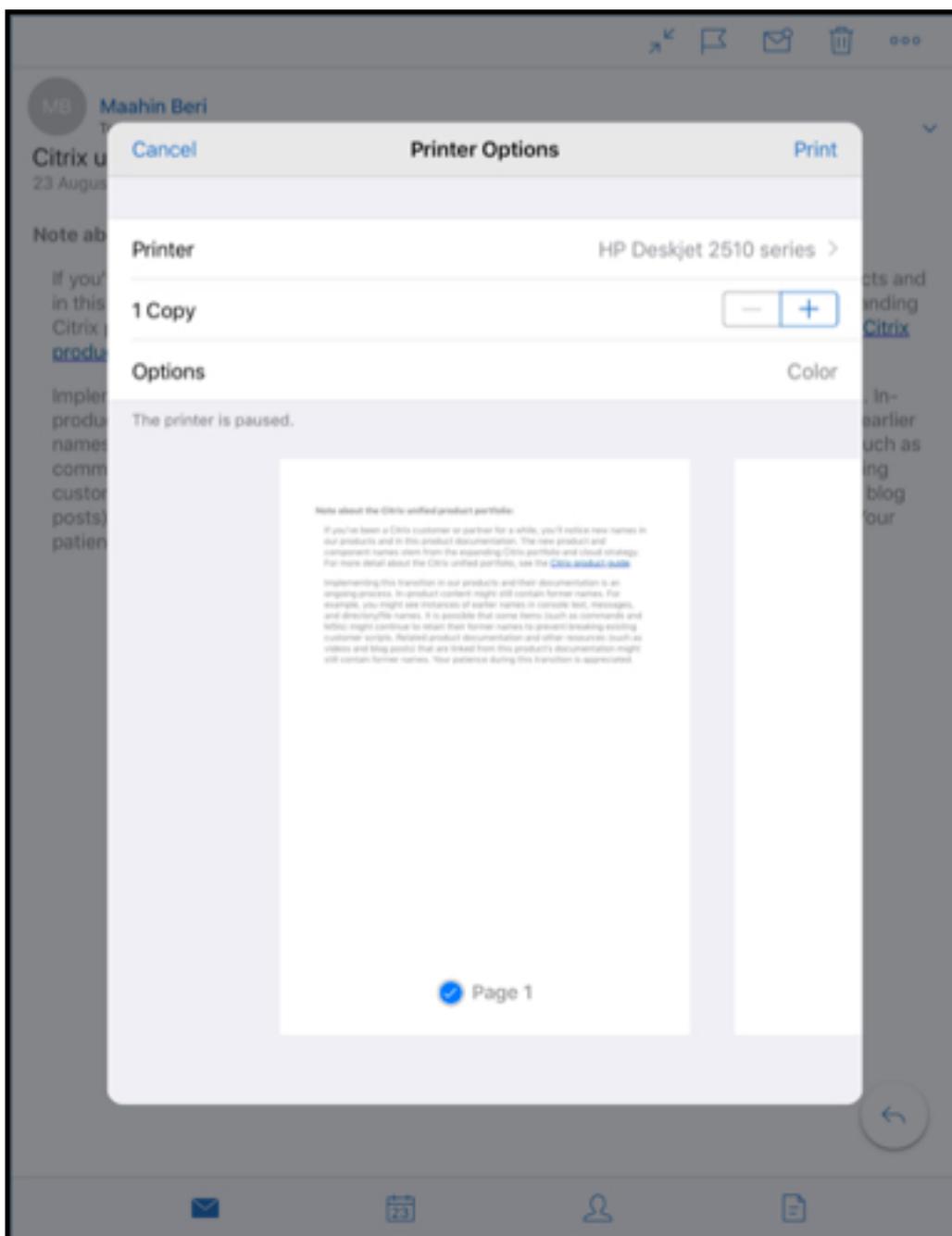
3. Toque em **Imprimir**.
É exibida a tela **Opções de impressora**.



4. Para selecionar uma impressora, toque em **Selecionar impressora**. É exibida a tela **Impressora**.



5. Selecione a impressora em que você deseja imprimir.



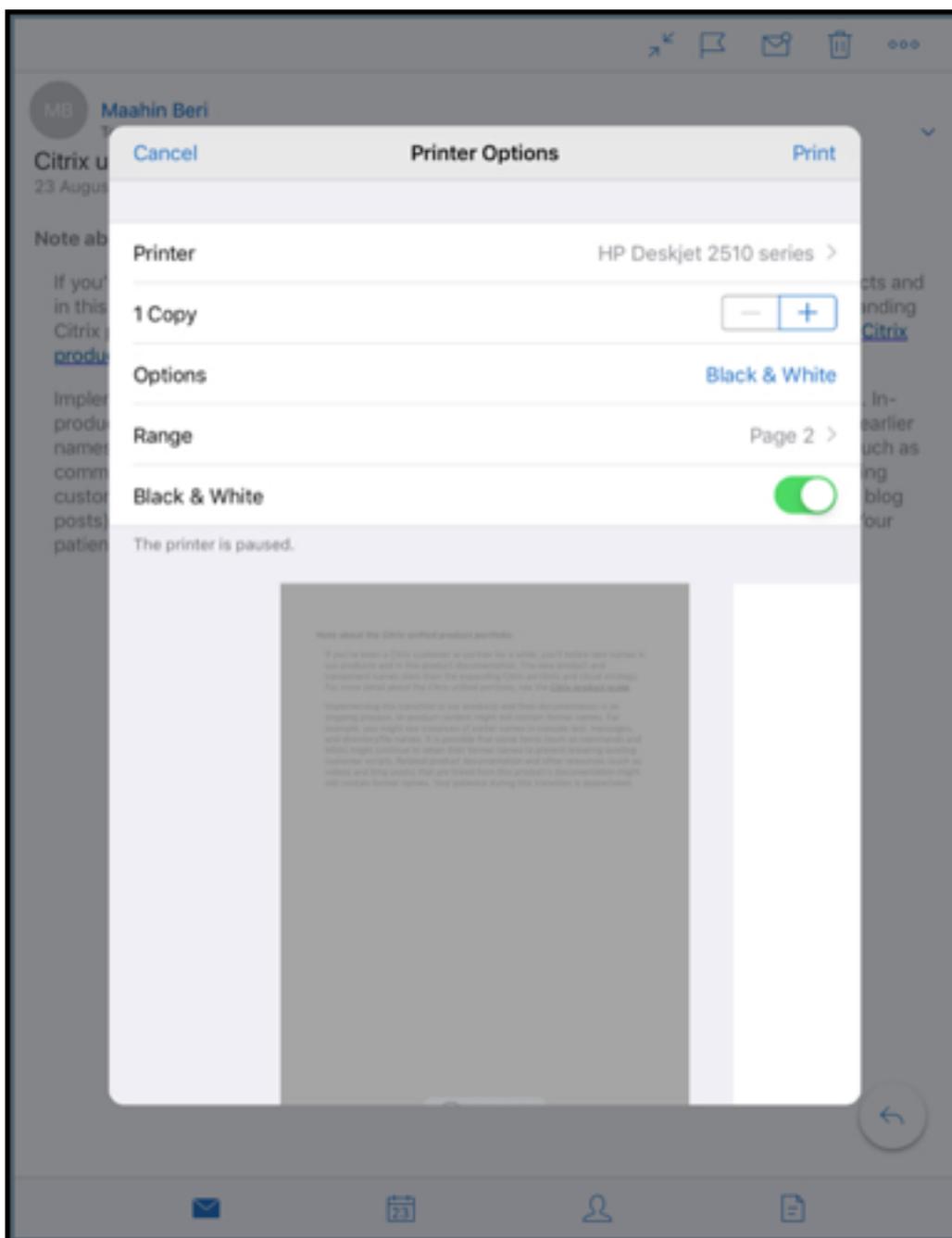
6. Toque em - ou + para diminuir ou aumentar o número de cópias para imprimir.
7. Para imprimir uma página específica ou um intervalo de páginas, toque em **Intervalo**. É exibida a tela **Intervalo de páginas**. Por padrão, está assinalada a opção **Todas as páginas**.



8. Para alterar a seleção de página, altere os números para cima ou para baixo deslizando o dedo.



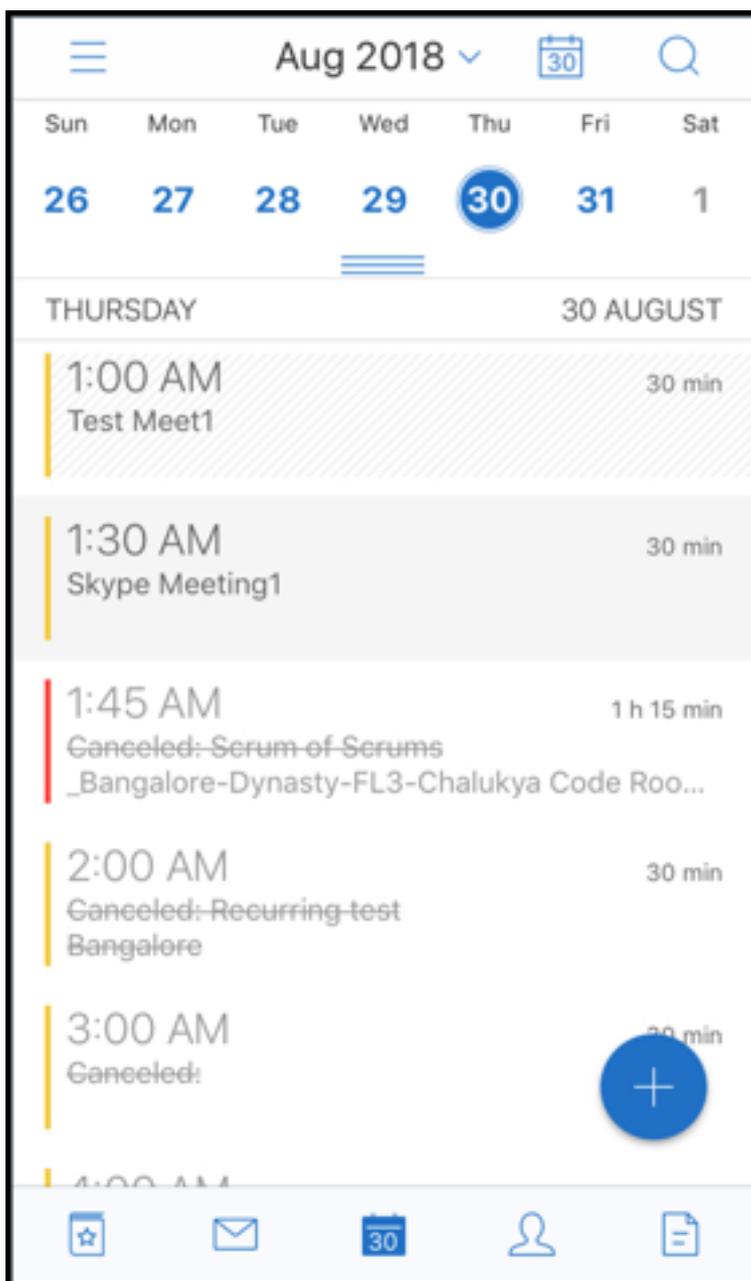
9. Toque em **Opções da impressora** para voltar à tela **Opções da impressora**.



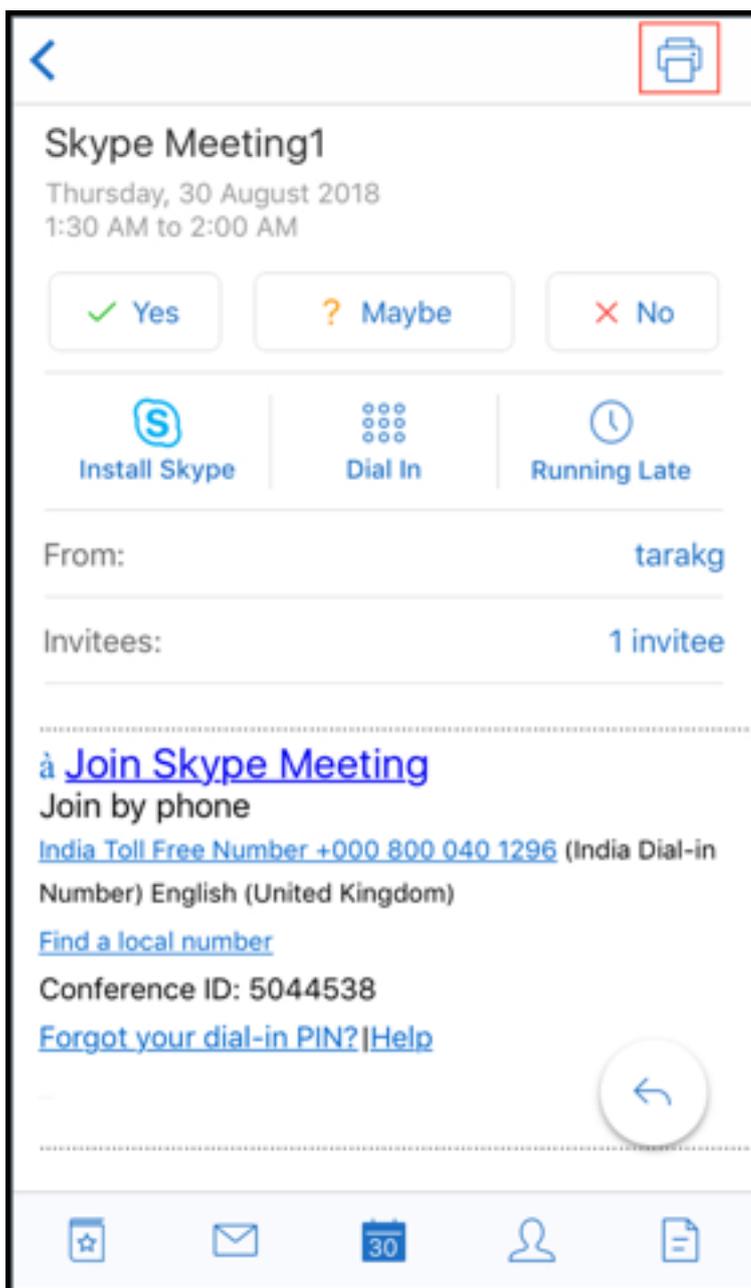
10. Para imprimir em e preto, toque no botão **Preto e branco**. Como padrão, o Secure Mail imprime em cores.
11. Toque em **Imprimir** no canto superior direito para imprimir o email.
12. Para cancelar o trabalho de impressão, toque em **Cancelar**, na parte superior esquerda.

Imprimir um evento de calendário

1. Navegue até o calendário e selecione um evento.

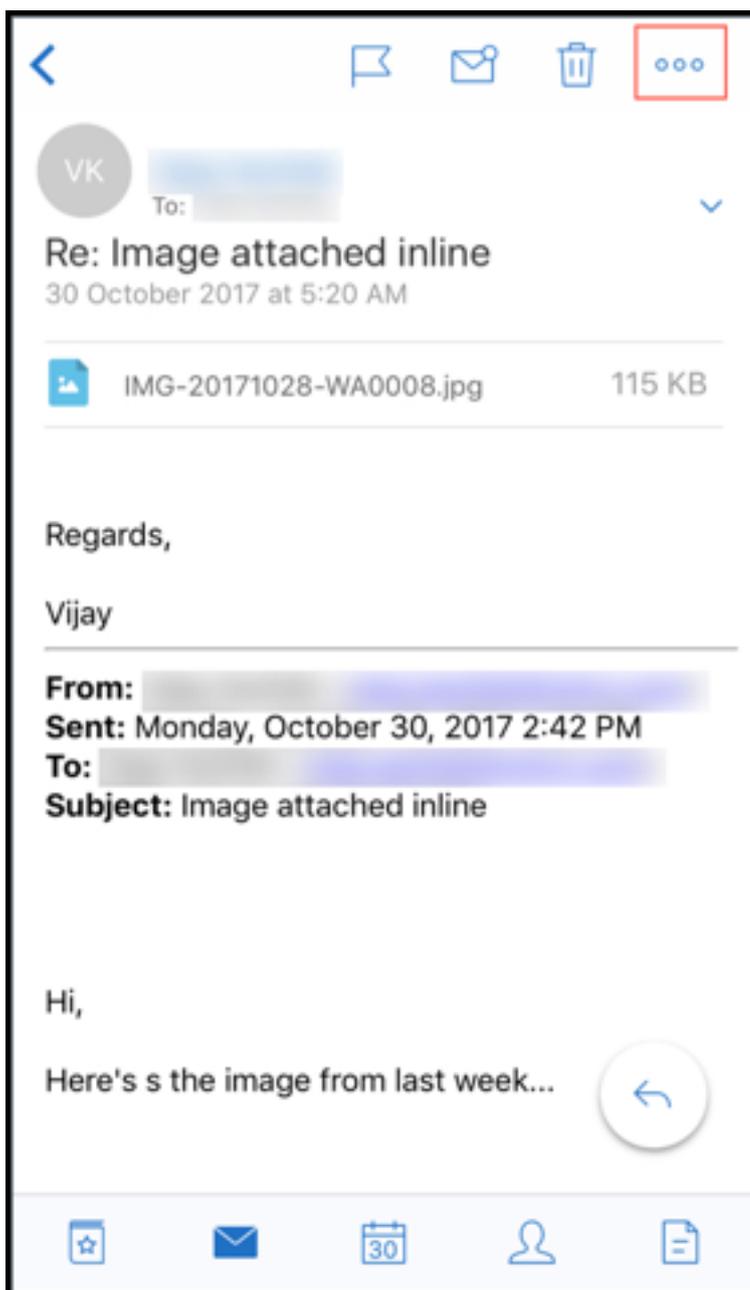


2. Toque no ícone Imprimir e siga as mesmas instruções como mencionado na seção anterior **Para imprimir emails.**



Para imprimir imagens incorporadas:

1. Abra o item de email com a imagem incorporada.
2. Toque no ícone Mais. São exibidas as seguintes opções:
 - Mover
 - Impressão
 - Cancelar



3. Toque em **Imprimir** e siga as instruções como mencionado na seção **Para imprimir emails**.

Vários códigos de conferência (discagem para uma reunião)

O Secure Mail para iOS oferece suporte a várias códigos de conferência. Agora você pode selecionar um código de conferência de uma lista de códigos de conferência disponíveis para ingressar em uma reunião.

Discar para entrar em uma reunião

1. Abra o convite de reunião e toque em **Discar**.
2. Na lista de números de telefone que for exibida, selecione um para discar.
3. Na lista de códigos de conferência que é exibida, selecione um para participar da reunião.
4. Toque em **Chamar** para participar da reunião.

Suporte para imprimir anexos de email

O Secure Mail para iOS oferece suporte a impressão anexos de email.

Recursos do Android

August 18, 2022

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

Criar reuniões do Microsoft Teams em eventos do Calendário do Secure Mail

No Secure Mail para Android, você pode criar convites para reuniões do Microsoft Teams enquanto cria eventos de calendário. Para criar uma reunião do Microsoft Teams, ative o botão de alternância **Reunião do Microsoft Teams**. O link do convite da reunião e os detalhes são enviados automaticamente com os detalhes do evento.

Cancel New Event Save

Weekly sync up meeting

Microsoft Teams

Microsoft Teams meeting

Other meeting type None

Invitees None

All Day

Time Zone (GMT+5:30) India Standard Time

Starts Fri, Mar 5, 2021 12:00 PM

Ends Fri, Mar 5, 2021 1:00 PM

More Options

Attach from Citrix Files

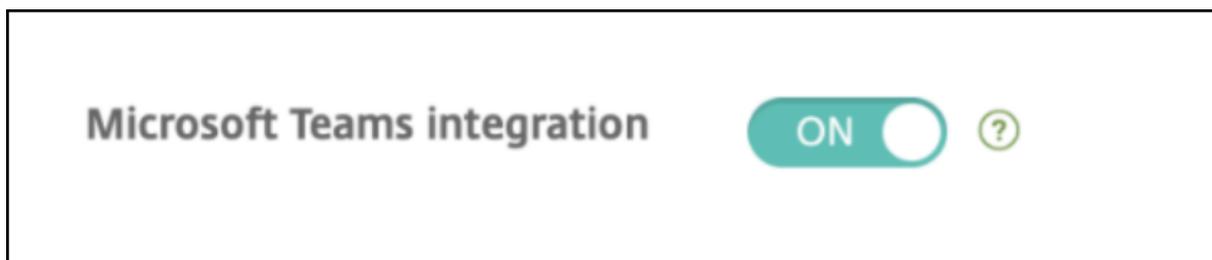
Notes

Pré-requisitos:

Certifique-se de que o administrador global do Azure Active Directory execute o seguinte:

- Habilite a autenticação moderna (OAuth) e certifique-se de que você é um usuário da caixa de correio do Exchange Online com uma licença válida do Microsoft Teams.
- Fornece o consentimento de administrador de todos os locatários para o aplicativo Secure Mail.
- Configure sua conta do Exchange no aplicativo Secure Mail e dê permissão de aplicativo para que todos os usuários entrem. Veja a tela a seguir:

- Ative a política de integração do Microsoft Teams.



Limitações:

Para reuniões criadas no Secure Mail, atualmente o recurso tem as seguintes limitações no Calendário do Microsoft Outlook:

- A opção **Ingressar online** não está disponível
- A notificação **A reunião foi iniciada** não está disponível

Sincronização de contato bidirecional

No Secure Mail para Android, você pode criar, editar e excluir contatos do Secure Mail da sua lista de contatos local.

Desfazer envio de emails

No Secure Mail para Android, você pode desfazer o envio de um email. Depois de tocar no botão **Enviar**, você recebe uma mensagem de notificação do sistema que permite desfazer a ação de envio.

Toque em **Desfazer** para reverter a ação de envio e editar a mensagem, os destinatários do email, anexar ou remover anexos ou descartar o email.

Sincronização de anexos na pasta Rascunhos

No Secure Mail para Android, quando a pasta **Rascunhos** é sincronizada, os anexos também são sincronizados e ficam disponíveis em todos os seus dispositivos. Esse recurso está disponível em dispositivos que executam o Exchange ActiveSync versão 16 ou posterior.

Visualização dentro do aplicativo de arquivos PDF

No Secure Mail para Android, você pode visualizar arquivos PDF dentro do aplicativo, juntamente com indicadores e anotações. Também está disponível a visualização aprimorada de outros anexos do Microsoft Office.

Use a política para encapsulamento com o SSO da Web para configurações executando a autenticação moderna com o Microsoft Office 365

No Secure Mail para Android, uma nova política chamada **Usar o SSO da Web para encapsulamento** é adicionada. Com essa política, você pode encapsular o tráfego OAuth para passar por Com túnel – SSO de Web. Para isso:

- Defina a política **Usar o SSO da Web para encapsulamento** como **Ativado**.
- Na política de acesso à rede, selecione a opção **Com túnel - SSO de Web**.
- Exclua os nomes de host relacionados ao OAuth da política de **Serviços em segundo plano**.

Arrastar e soltar eventos de calendário

No Secure Mail para Android, você pode alterar a hora de um evento de calendário existente arrastando e soltando o evento. Para obter a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Alterar o horário de um evento de calendário](#).

Suporte para aplicativos de 64 bits para o Google Play

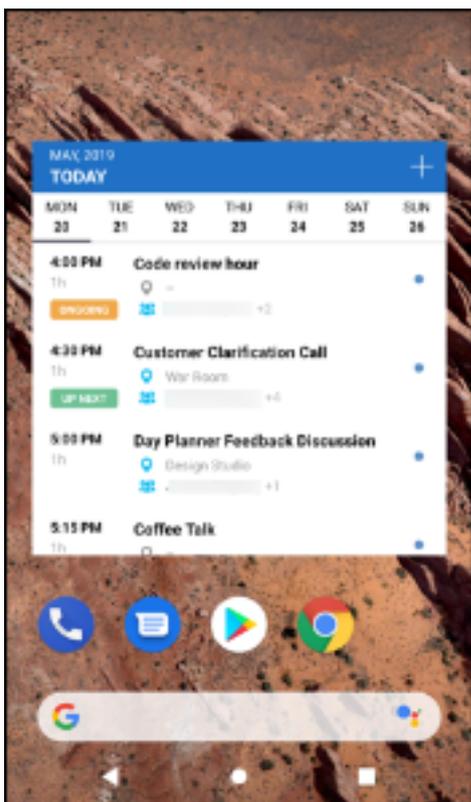
O Secure Mail para Android suporta arquiteturas de 64 bits.

Melhorias na IU Puxe para Atualizar no Secure Mail para Android

Para mantermos a conformidade com as diretrizes de Material Design, fizemos pequenas melhorias no recurso **Puxe para atualizar**. O carimbo de data/hora de sincronização está disponível na parte inferior da tela quando você toca no ícone do hambúrguer.

Widget para agenda do Calendário

No Secure Mail para Android, a agenda do **Calendário** está disponível como um widget. Neste widget, você pode visualizar os próximos eventos no **Calendário** para uma semana. Esse recurso permite que você crie um evento de **Calendário**, visualize um evento existente e edite os detalhes. A política **Bloquear captura de tela** não se aplica ao widget encontrado na tela inicial. No entanto, você pode desativar o widget usando a política **Permitir widget de agenda do calendário**.



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 usando Com túnel - SSO de Web e Secure Ticket Authority (STA) em paralelo. Você também pode permitir conexões Com túnel - SSO de Web 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 sobre como [Adicionar um aplicativo 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](#)

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.

Visualizar anexos

No Secure Mail para Android, visualizar anexos de e-mail e calendário é fácil. Para obter a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Exibir e anexar arquivos](#).

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:

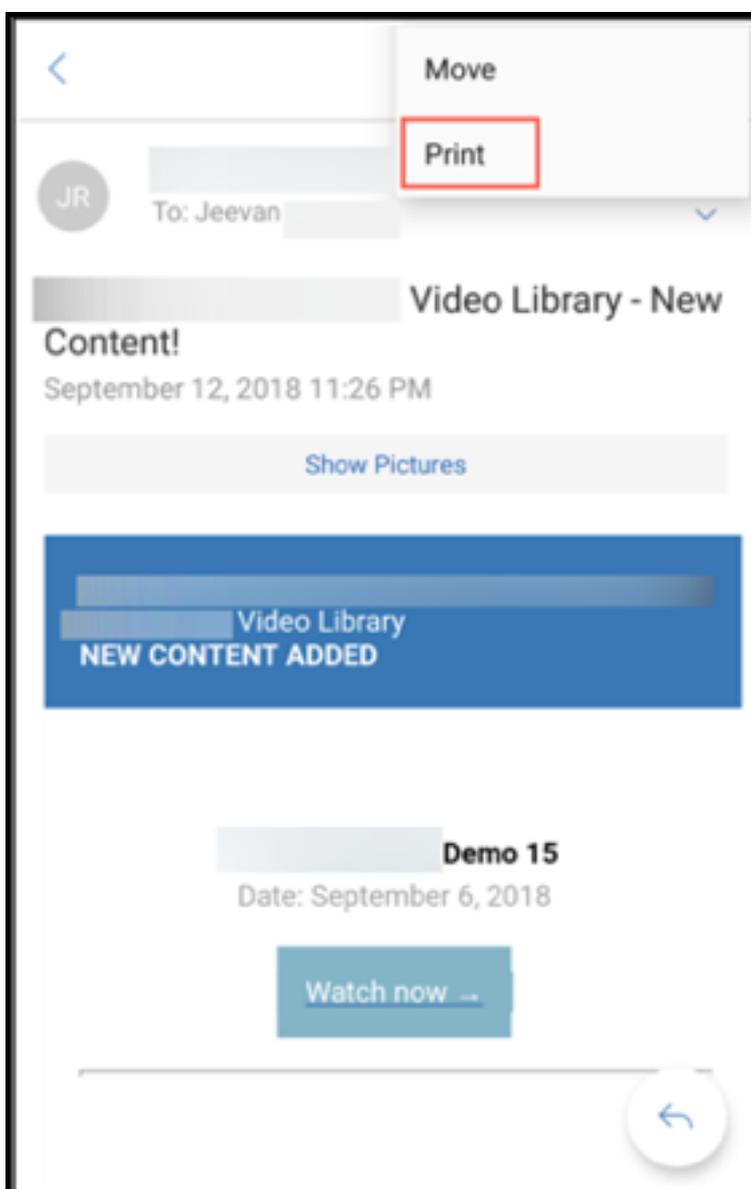
Esse recurso de impressão possui as seguintes limitações conhecidas:

- 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.

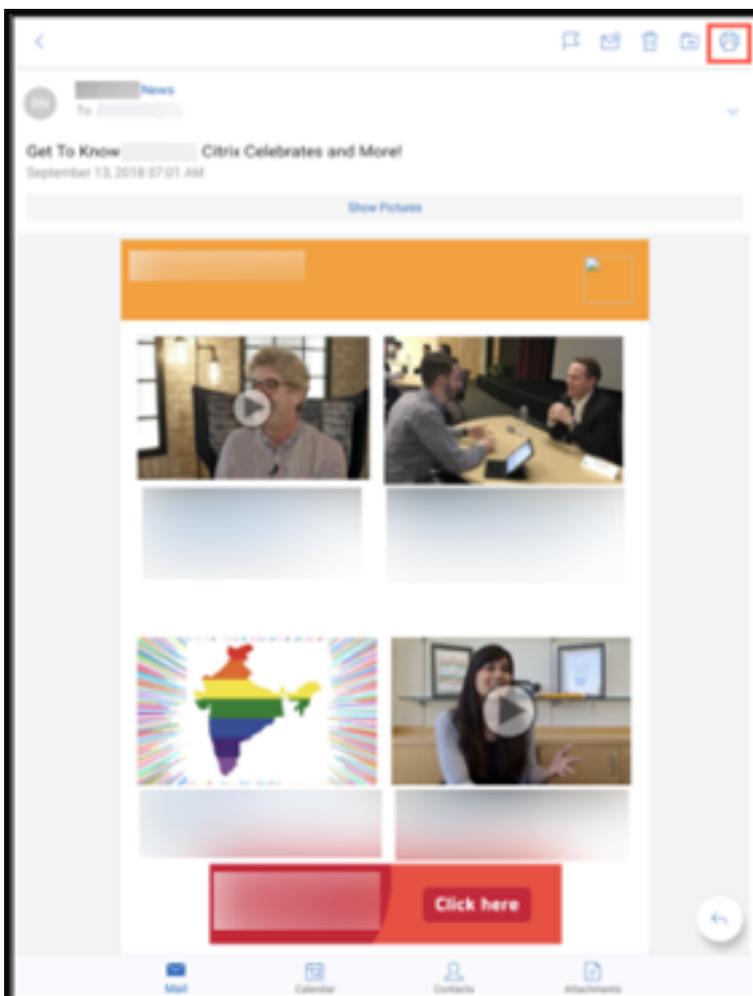
Para imprimir um email

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
 - Impressão

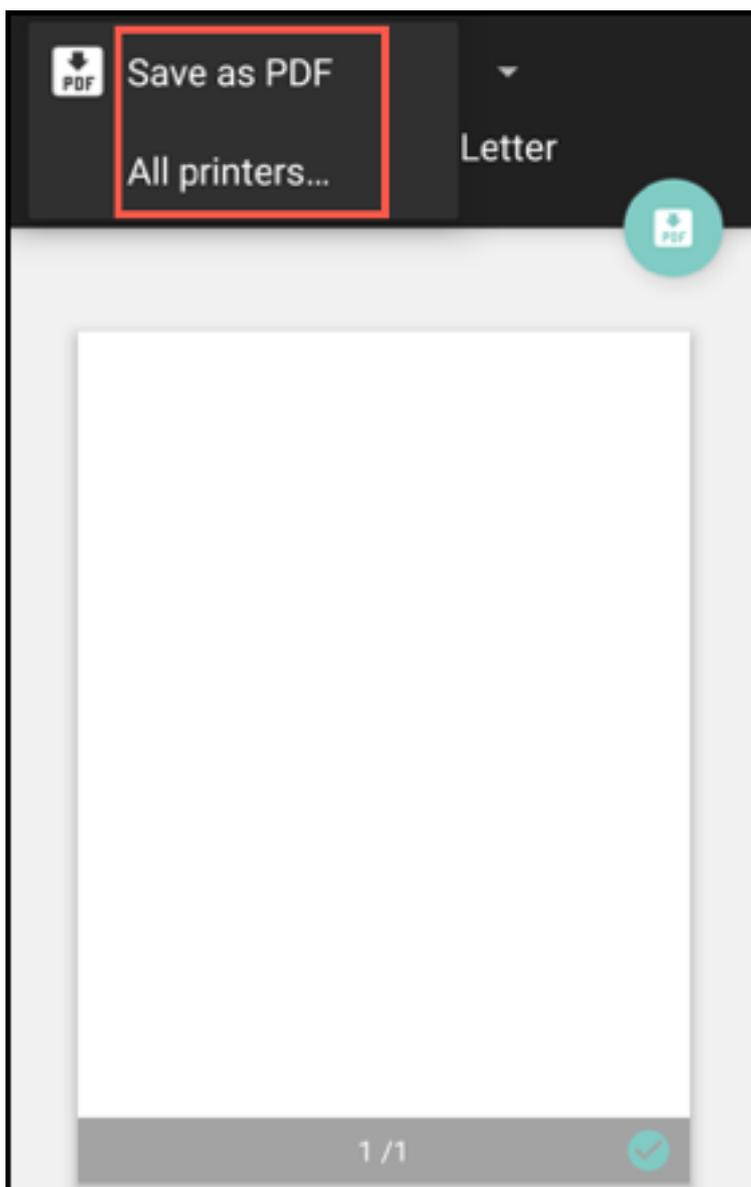


Nota:

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



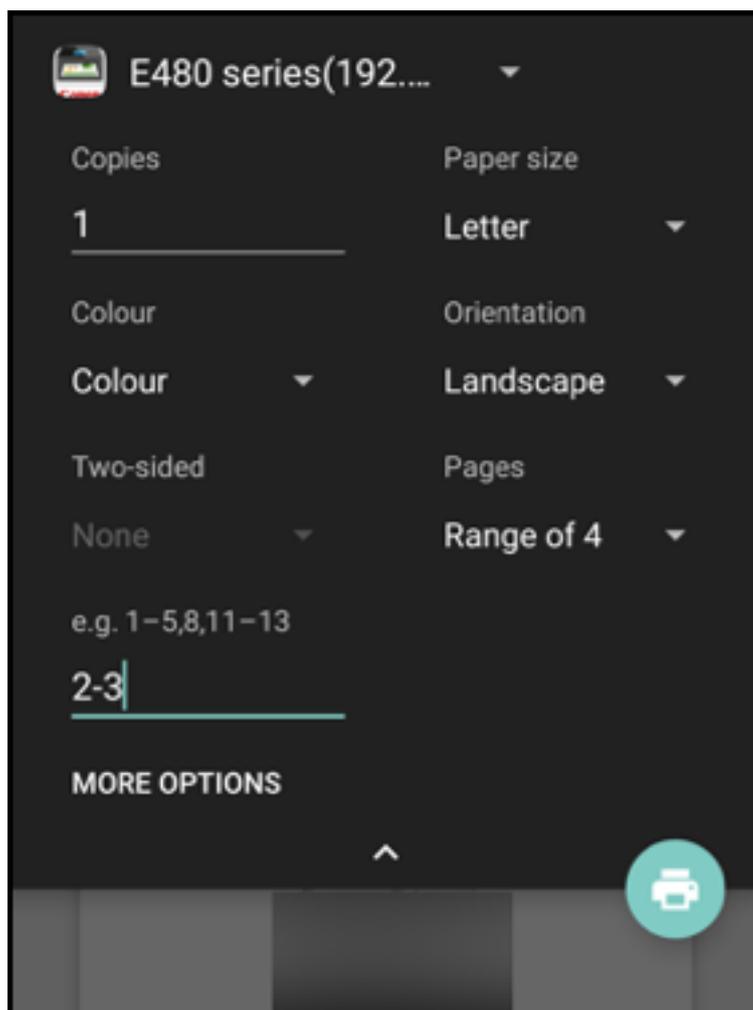
1. Toque em **Imprimir**. Uma visualização do seu e-mail é exibida.
2. Toque na lista e as seguintes opções serão exibidas:
 - Salvar como PDF
 - Todas as impressoras



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.



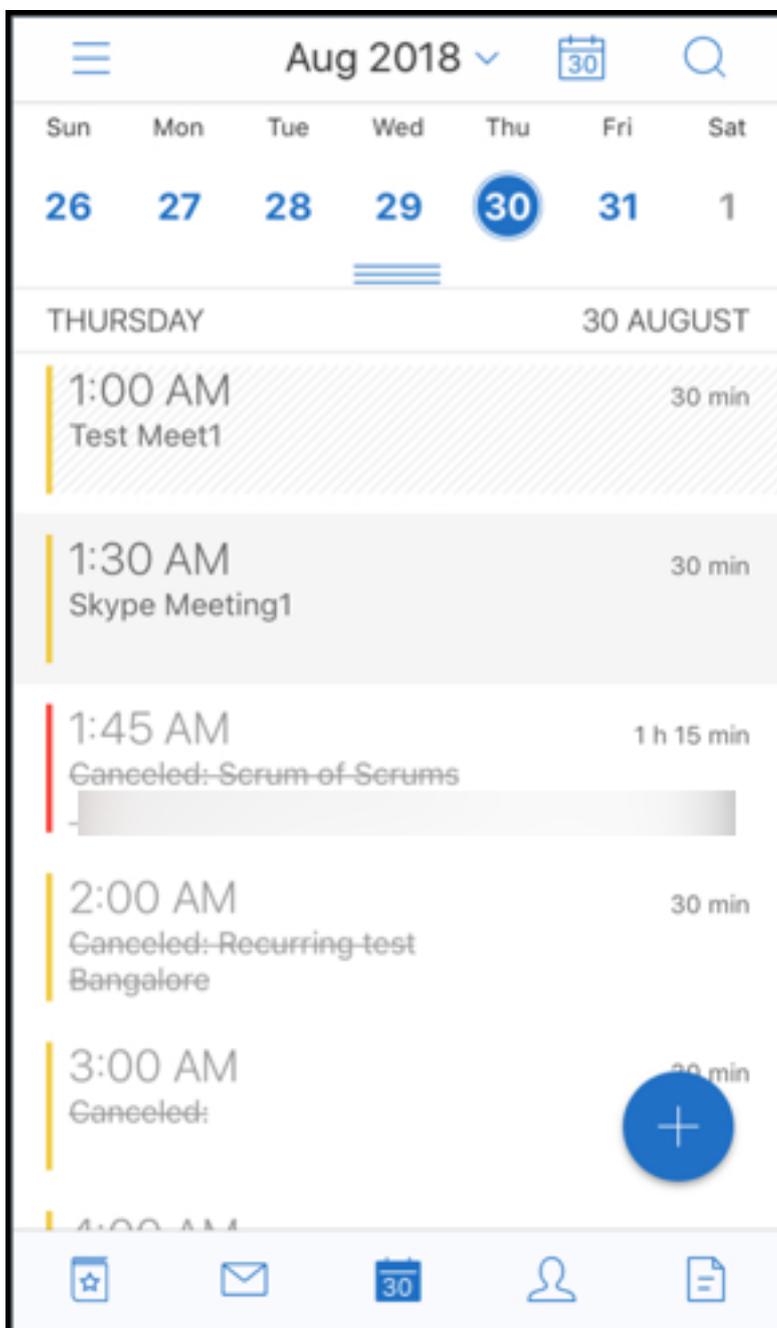
6. Selecione a impressora em que você deseja imprimir. Use as seguintes opções de impressão:
 - Insira manualmente o número de cópias que você deseja imprimir.
 - Selecione o tamanho do papel na lista.
 - Selecione a cor na lista.
 - Escolha a orientação da página conforme necessário.
 - Selecione uma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

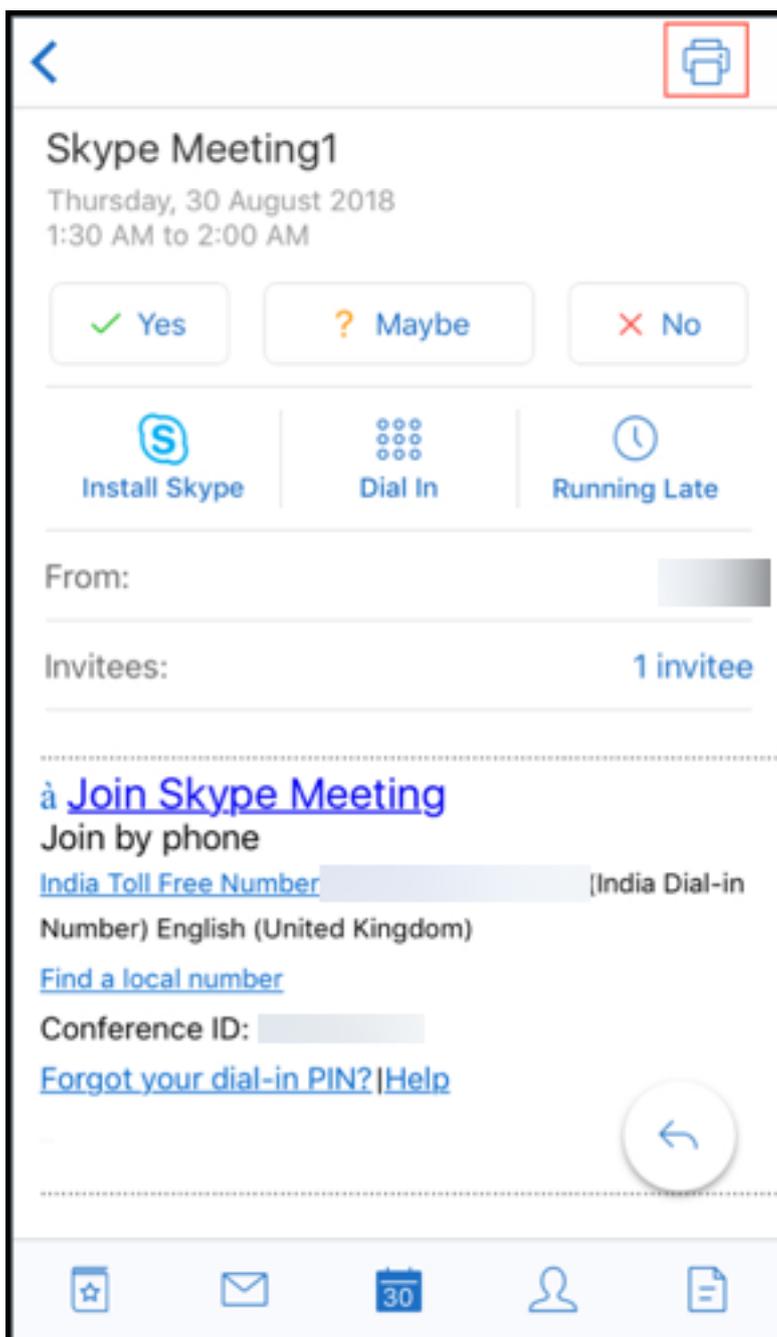
- Toque em **Mostrar imagens** no email e siga as instruções mencionadas na seção anterior [Para imprimir um email](#).

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 sobre como configurar políticas MDX para o Secure Mail, consulte [Políticas de MDX para aplicativos móveis de produtividade](#).

Notificações de subpastas

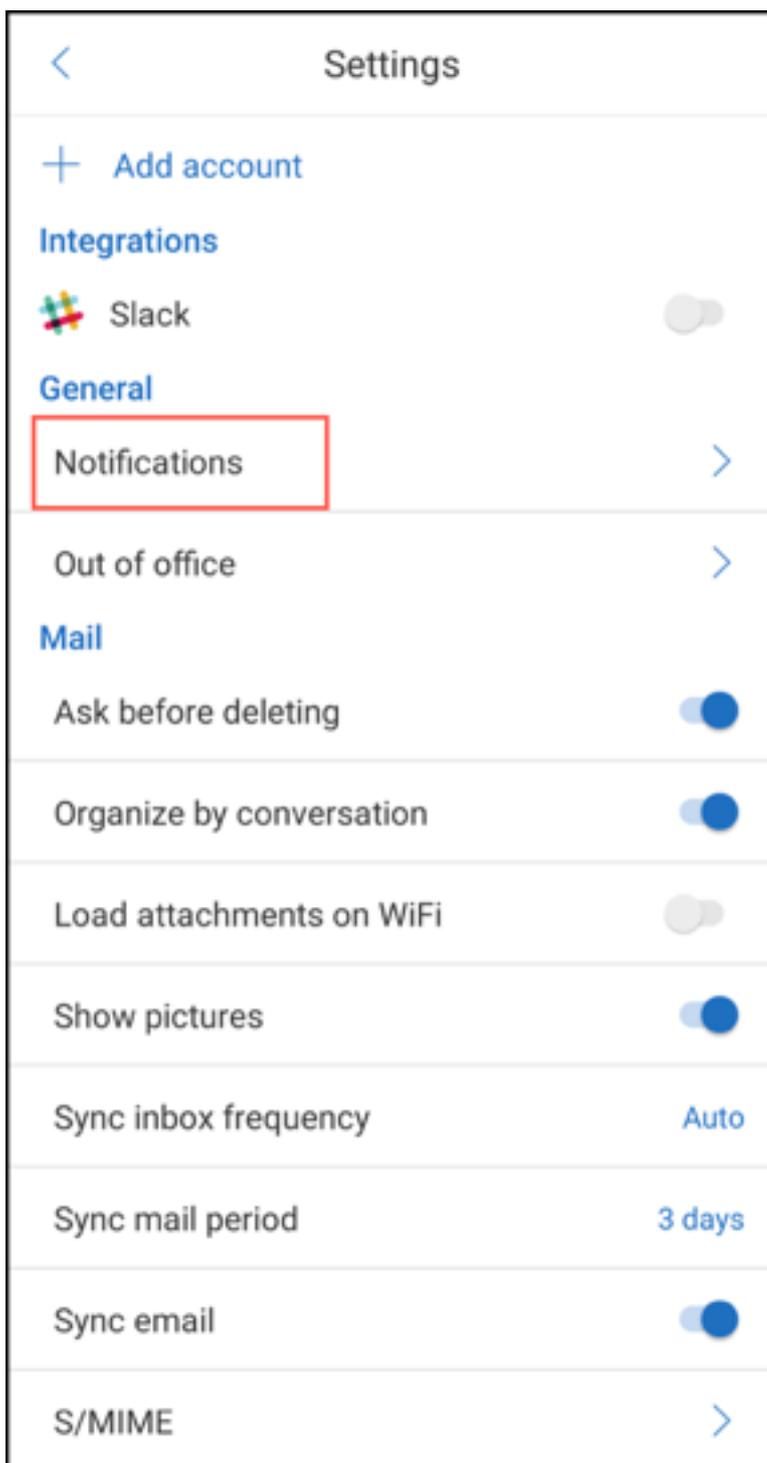
No Secure Mail para Android, você pode receber notificações por email de subpastas de sua conta de email.

Nota:

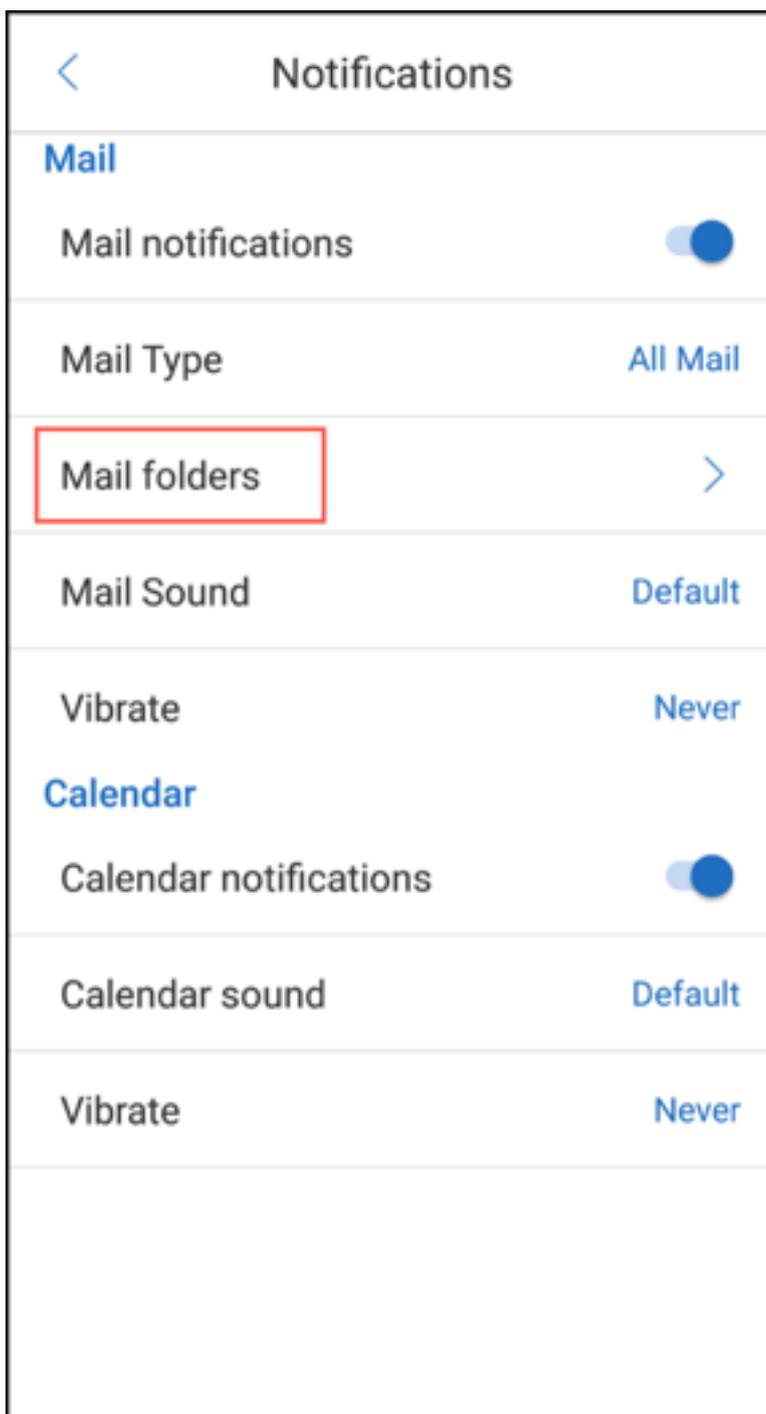
- Certifique-se de que a notificação por push baseada no FCM esteja ativada no console do Endpoint Management para receber notificações de subpastas. Para ver as etapas de configuração de notificações por push baseadas em FCM, consulte [Notificações por push para o Secure Mail](#).
- O recurso de notificação 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**.



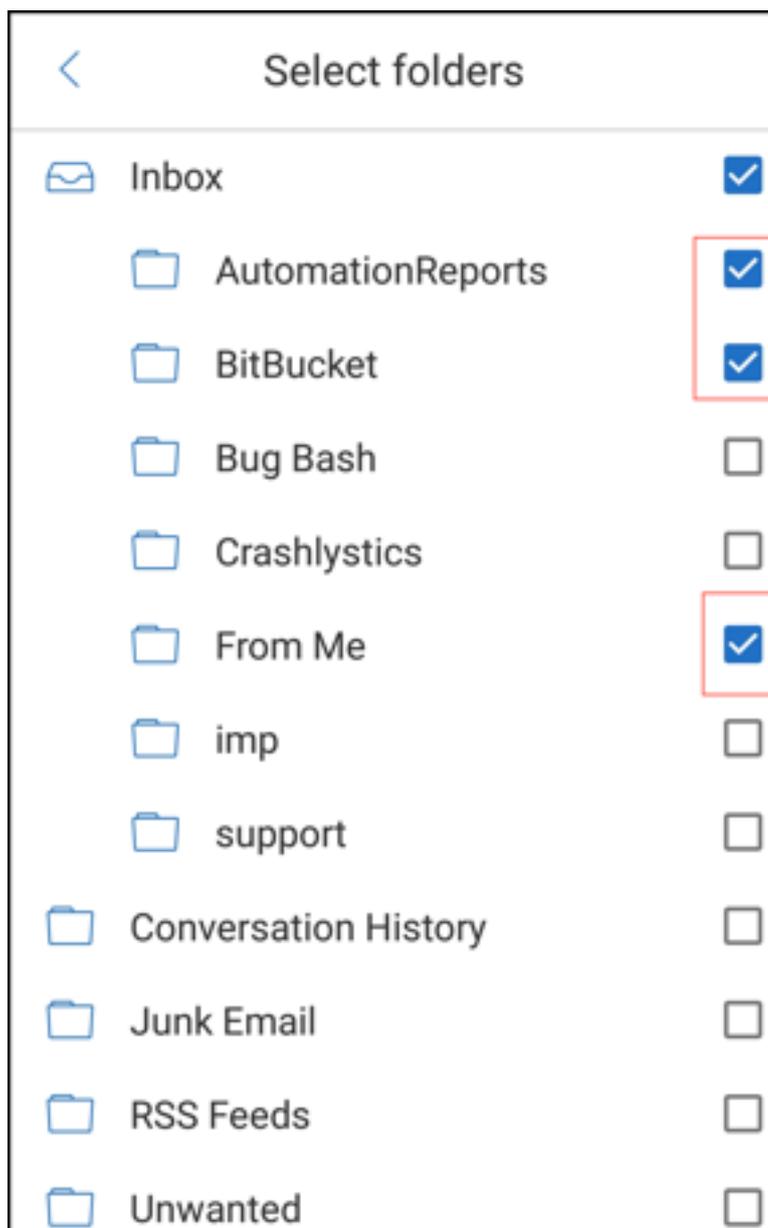
2. Na tela **Notificações**, toque em **Pastas de correio**. Uma lista de subpastas na caixa de entrada é exibida.



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.

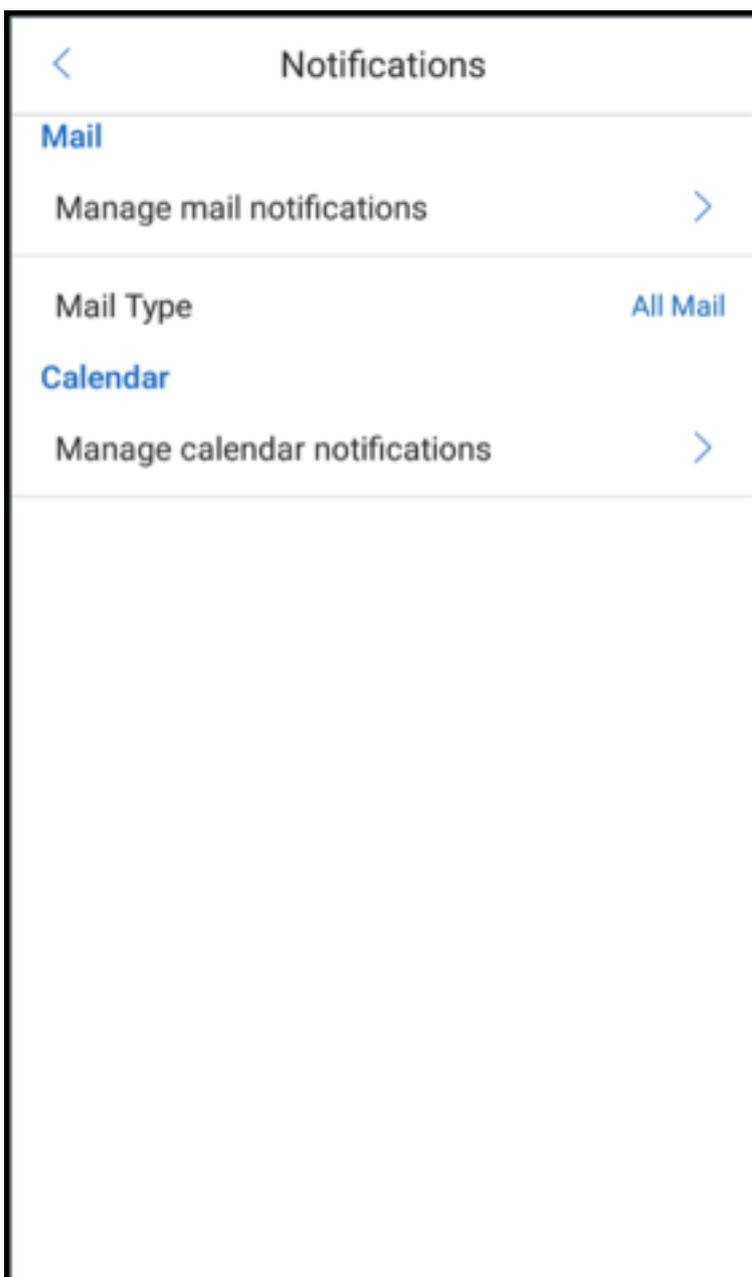


Para desabilitar as notificações da subpasta, desmarque a caixa de seleção das subpastas das quais você não deseja receber notificações.

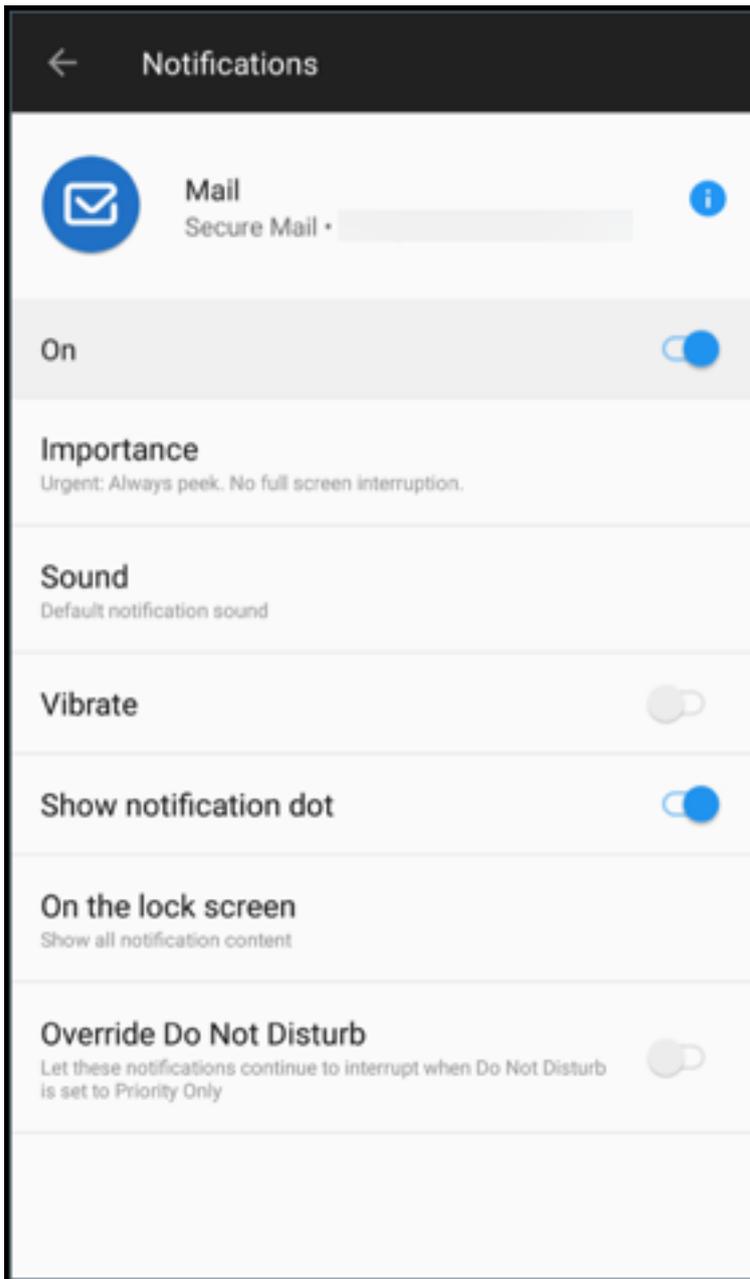
Canais de notificação

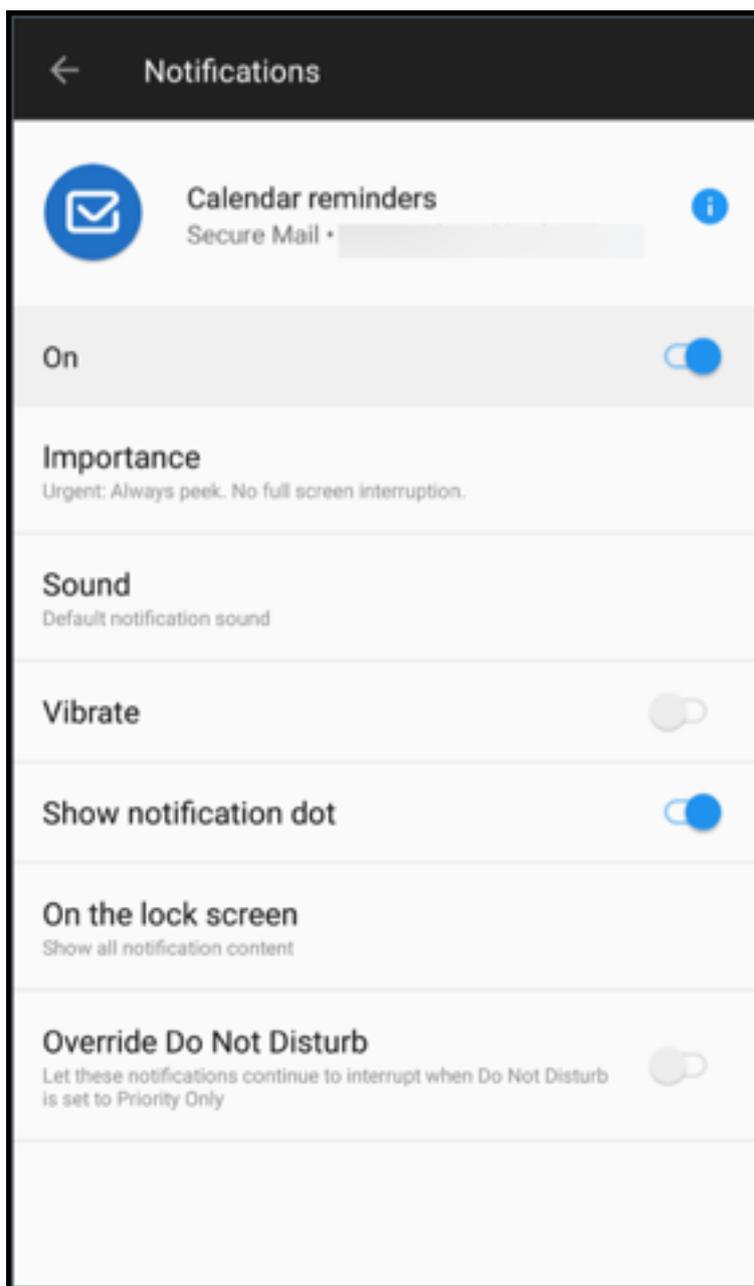
Nos dispositivos que executam o Android O ou posterior, você pode usar as configurações do canal de notificações para gerenciar como suas notificações de email e calendário são tratadas. Esse recurso permite personalizar e gerenciar suas notificações.

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.

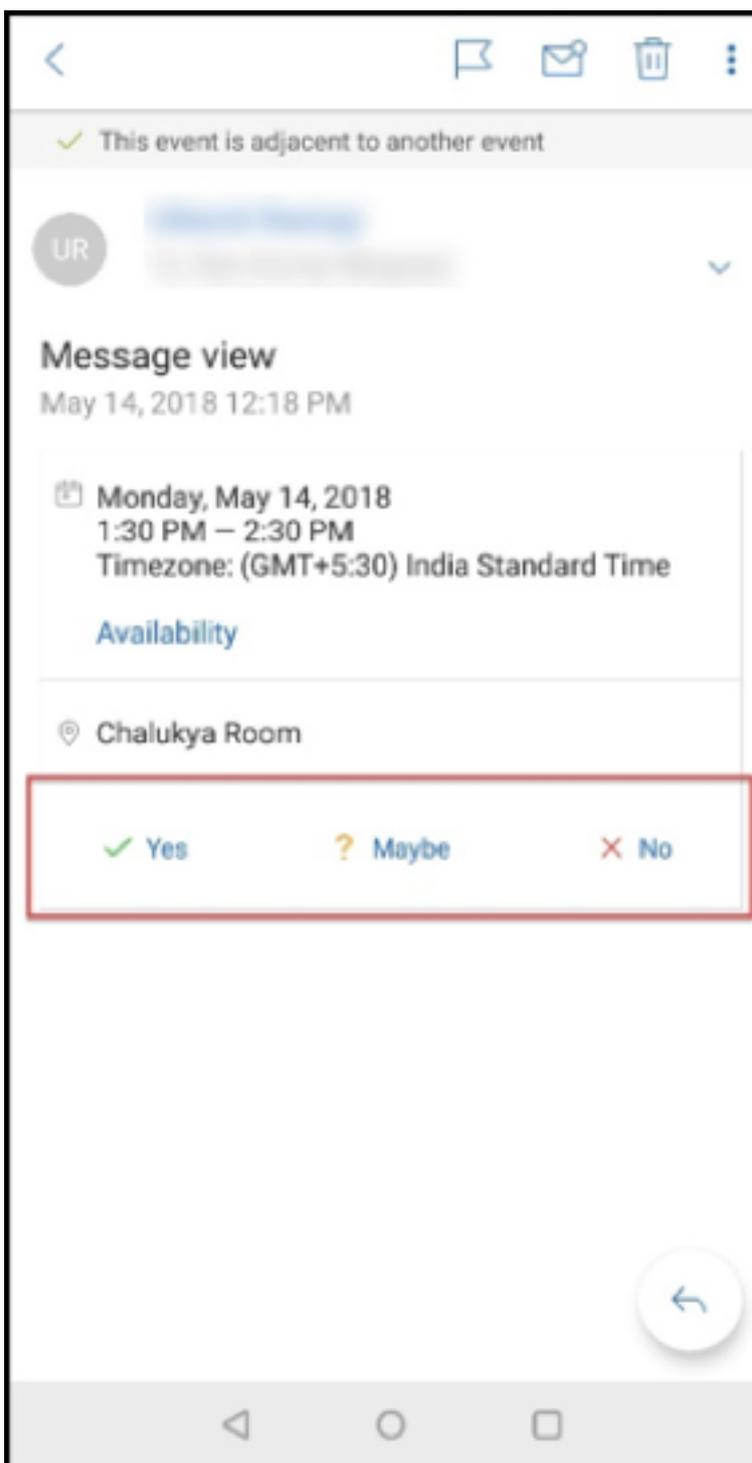
Nota:

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

Botões de resposta à reunião dentro do e-mail

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



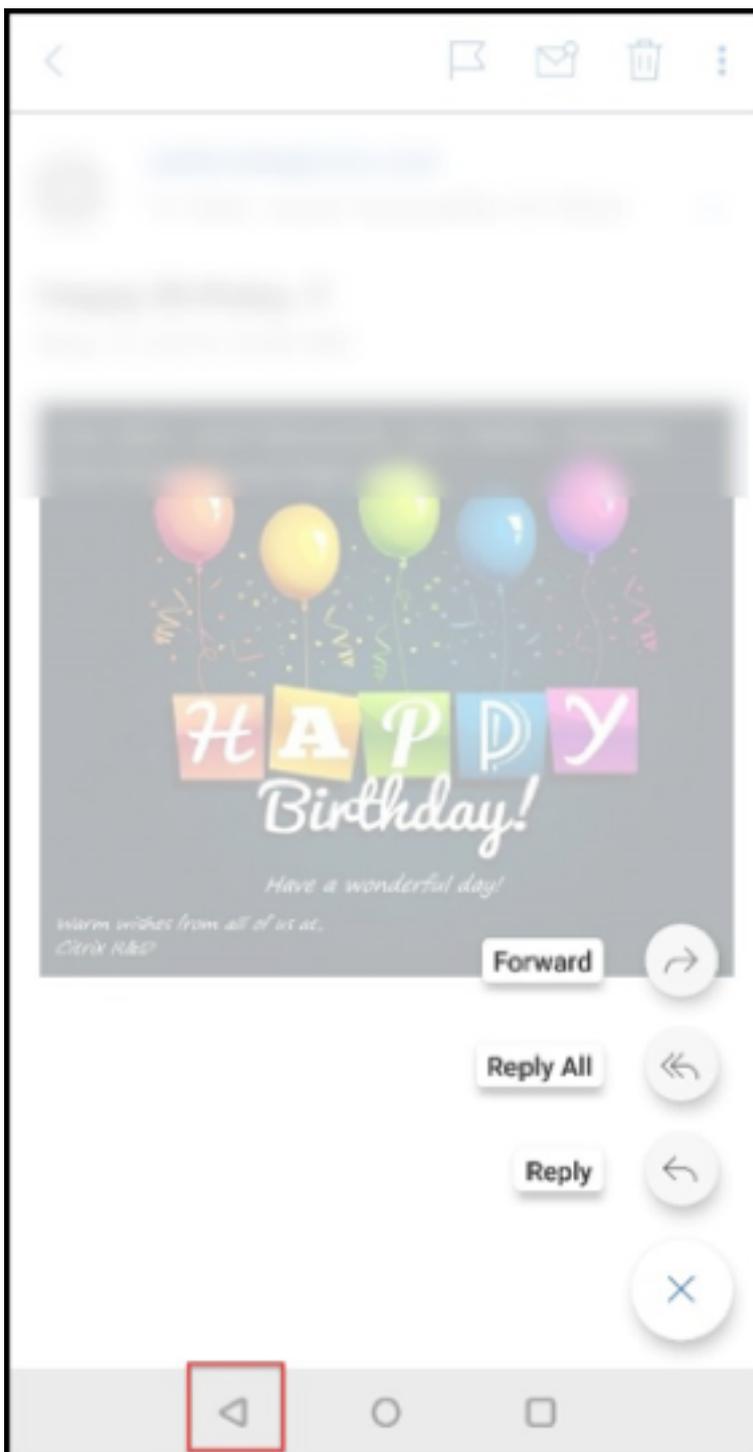
Aprimoramento a anexos

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 a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Exibir e anexar arquivos](#).

Aprimoramentos ao botão Voltar

No Secure Mail para Android, você pode tocar no botão de voltar em seu dispositivo para recolher as opções expandidas do botão **Ação flutuante**. Essa ação leva você de volta à exibição de detalhes da mensagem ou do evento.



Etapas de administração para ativar anexos de arquivos da Galeria no 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 adi-

cionem 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 atore 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.

The screenshot shows a configuration window for Secure Mail. It contains four main sections:

- Restricted Open-In exception list:** A text input field containing the value `{action=android.speech.tts.engine.CHECK_TTS_DATA}{a`.
- Inbound document exchange (Open In):** A dropdown menu currently set to `Unrestricted`.
- Inbound document exchange whitelist:** An empty text input field, which is highlighted with a purple rectangular box.
- Connection security level:** A dropdown menu currently set to `TLS`.

As IDs de pacote devem ser separados por vírgula:

`com.sec.android.gallery3d, com.sec.android.gallery3d.panorama360view, com.google.android.apps.photos`

5. Salve e implante de Secure Mail.

Os usuários do Android agora podem anexar uma imagem do aplicativo Galeria. Para obter a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Exibir e anexar arquivos](#).

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

Formato	iOS	Android
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
DOTX		X
PDF	X	X
PPT	X	X
PPTX	X	X
PPS		X
PPSX		X
DOC	X	X
DOCX	X	X
XLS	X	X
XLSM	X	X
XLSX	X	X
TXT	X	X
POT	X	X
POTX		X

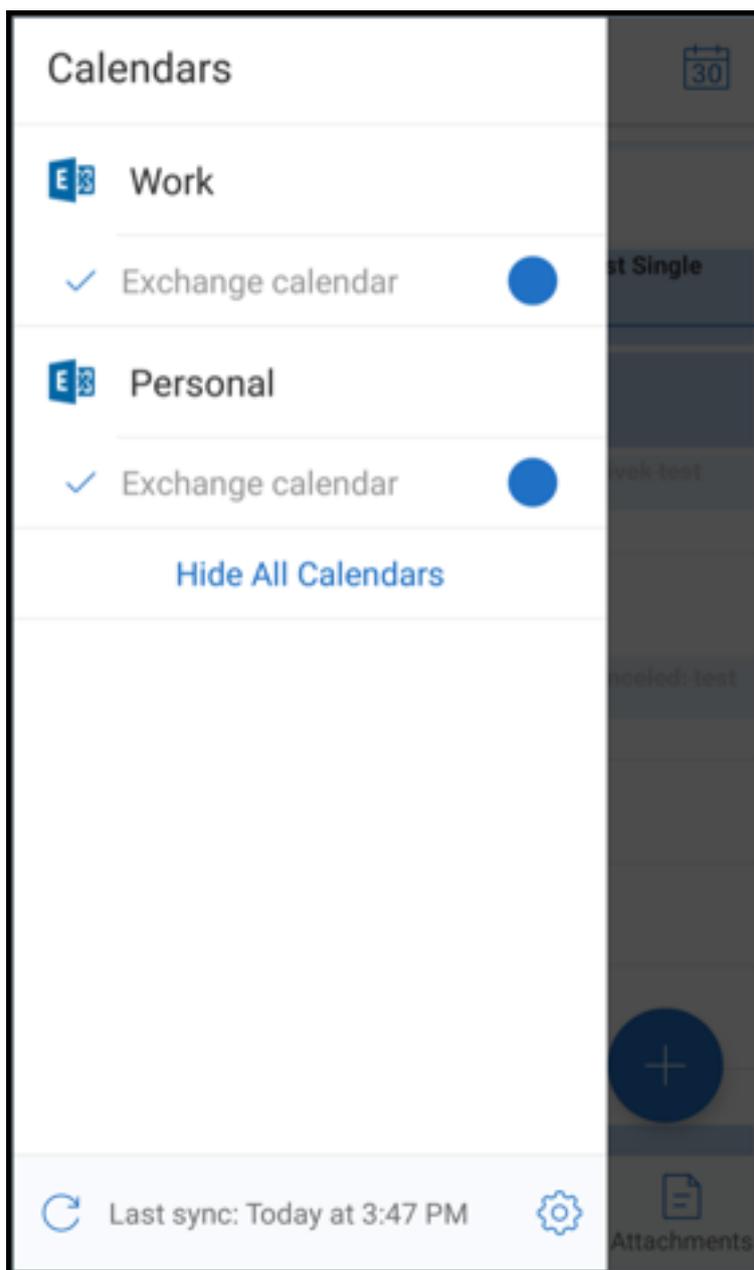
Formato	iOS	Android
HTM	X	X
HTML	X	X
ZIP	X	X
EML	X	X

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.

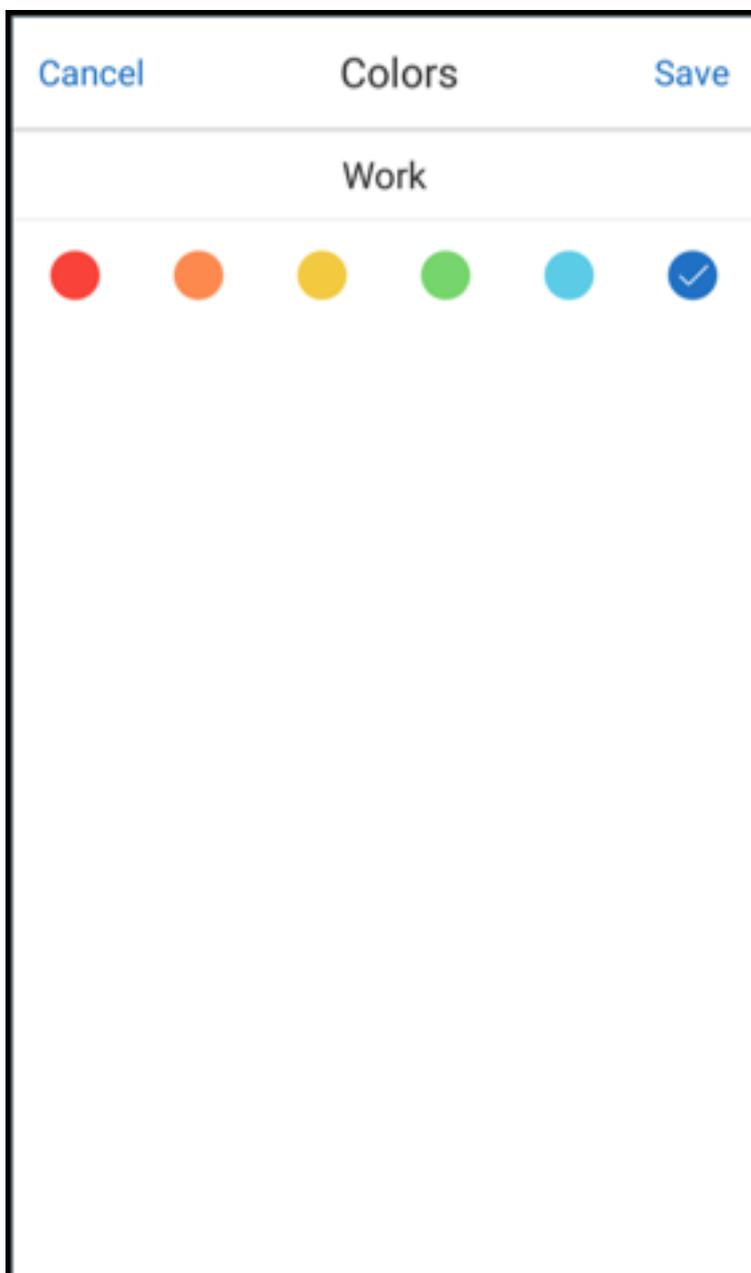


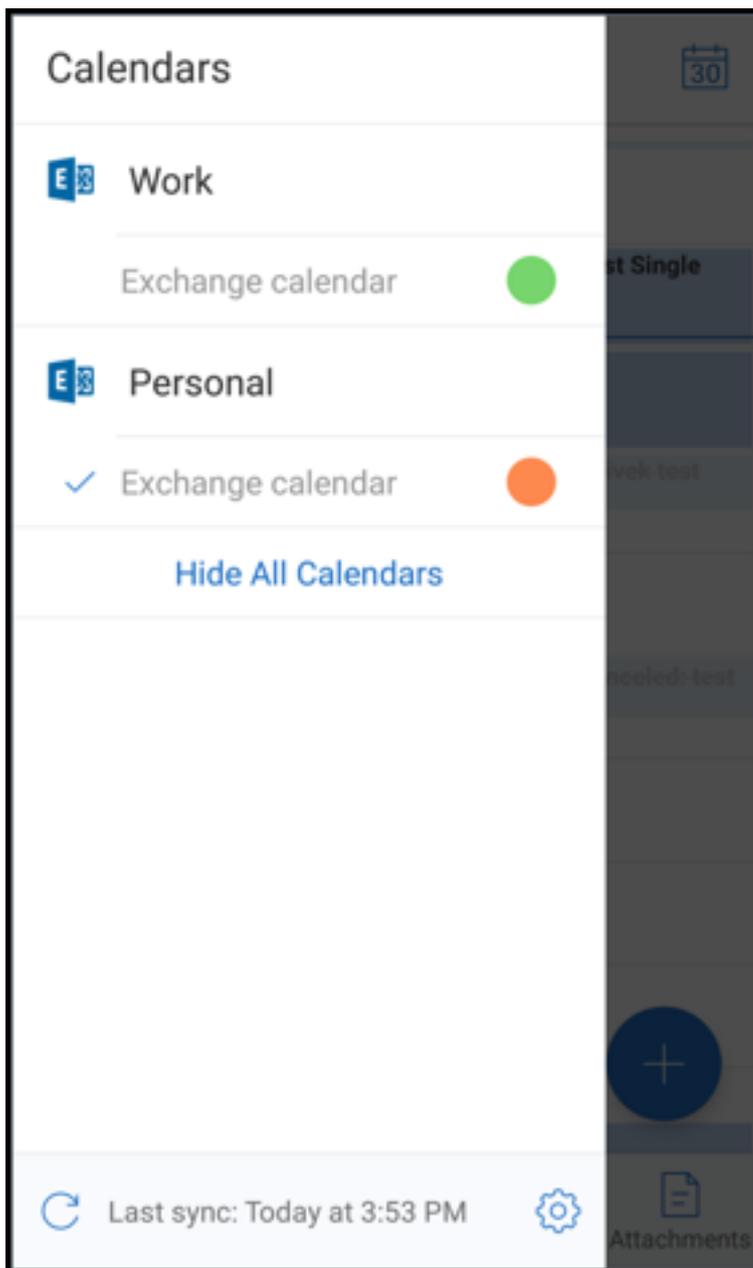
Para atribuir cores a eventos de calendário

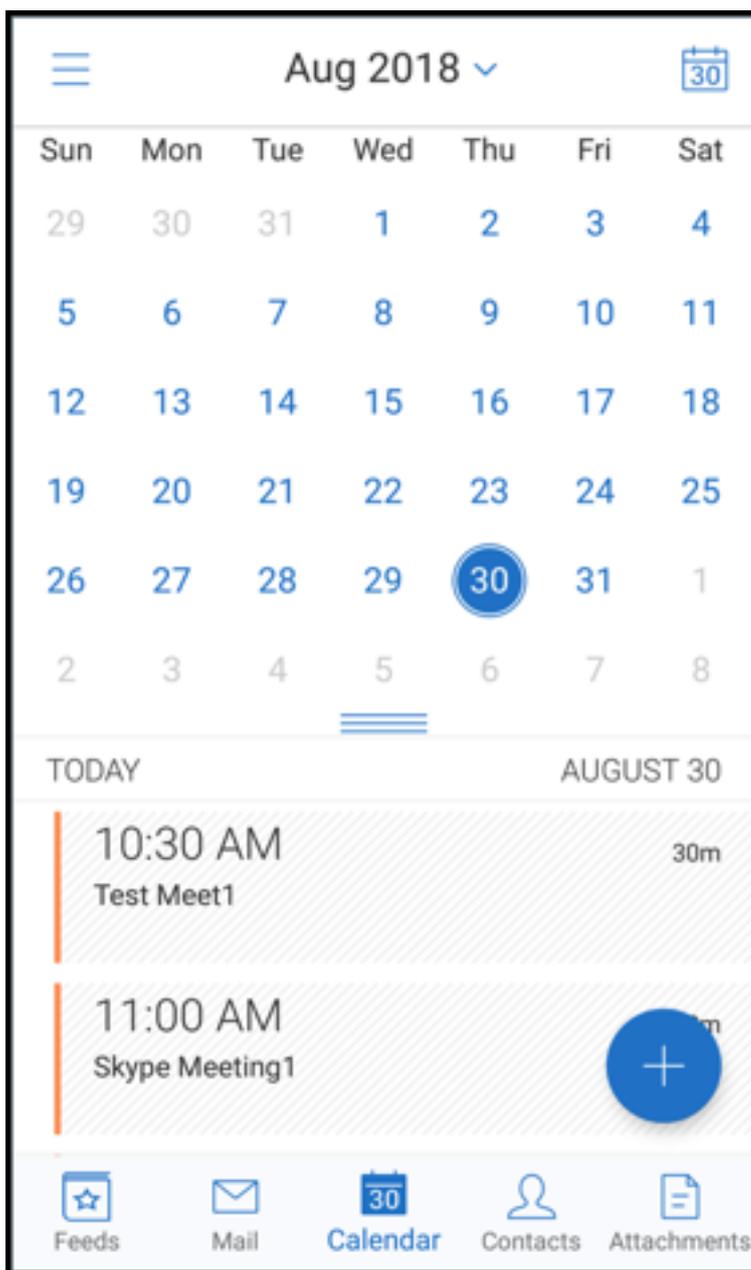
1. Toque no ícone **Calendário** na barra de rodapé e toque no ícone de hambúrguer no canto superior esquerdo.
A tela **Calendários** exibe todas as contas que você tiver configurado.
2. Toque na cor padrão exibida à direita de uma conta do Exchange.
A tela cores o exibe as cores disponíveis para aquela 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.

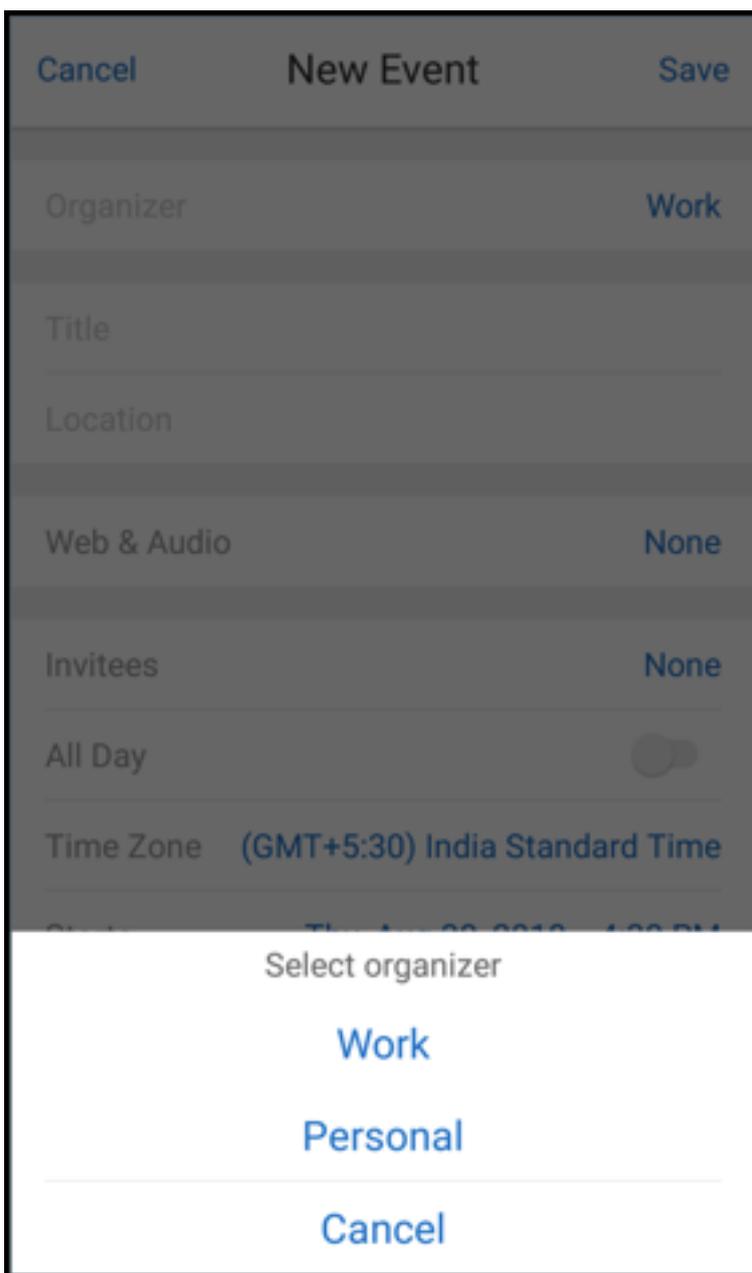






Quando você cria um convite ou evento de calendário, o campo **Organizador** é preenchido automaticamente com o endereço de email da conta padrão. Para alterar a conta de email, toque neste endereço de email e selecione outra conta.

Cancel	New Event	Save
Organizer		Work
Title		
Location		
Web & Audio		None
Invitees		None
All Day		<input type="checkbox"/>
Time Zone (GMT+5:30) India Standard Time		
Starts	Thu, Aug 30, 2018	4:30 PM
Ends	Thu, Aug 30, 2018	5:30 PM
More Options		v
Attach from ShareFile		



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.

Atualizações para serviços em segundo plano

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 push baseadas em FCM, consulte [Notificações por push para 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 Knowledge Center de suporte](#).

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.

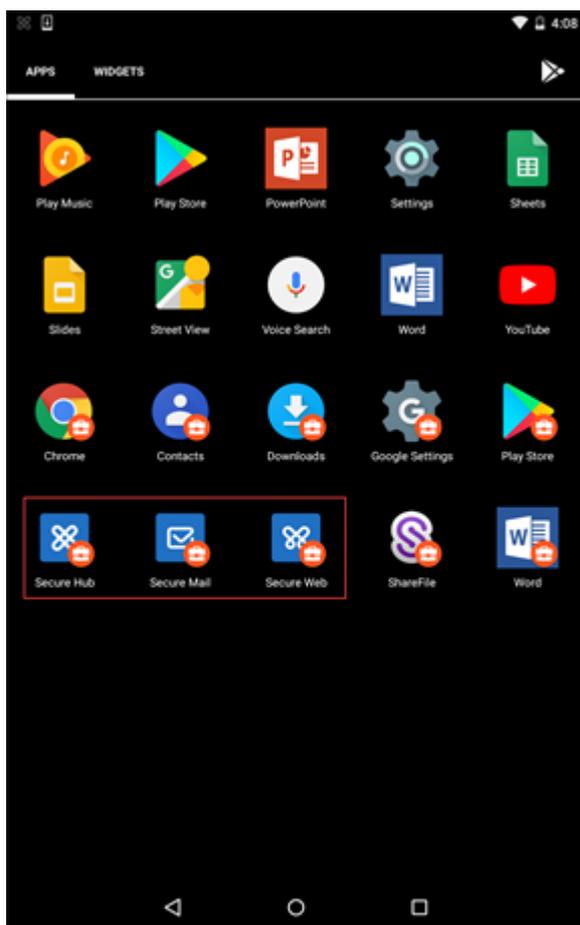
Android Enterprise no Secure Mail

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

Secure Mail

Recurso	Suporte
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)	
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 Com túnel - SSO de Web	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](#).

Recursos do iOS e Android para Secure Mail

June 14, 2022

Este artigo descreve os recursos do iOS e Android compatíveis com o Secure Mail.

Suporte para computação em nuvem do Azure Governamental

O Secure Mail oferece suporte à Computação em Nuvem Governamental (GCC) Alta para autenticação moderna (OAuth) no locatário do Azure Active Directory. O Secure Mail é registrado como um ponto de extremidade no GCC High, para atender aos requisitos obrigatórios da Microsoft para todo o serviço GCC High. Para obter detalhes, consulte [O que há de novo no Azure Active Directory no Microsoft 365 Governamental](#).

Com essa alteração, você é roteado para o GCC High no locatário do Azure Active Directory para autenticação. E é necessário que o administrador dê permissões para o Secure Mail no locatário do Azure Active Directory.

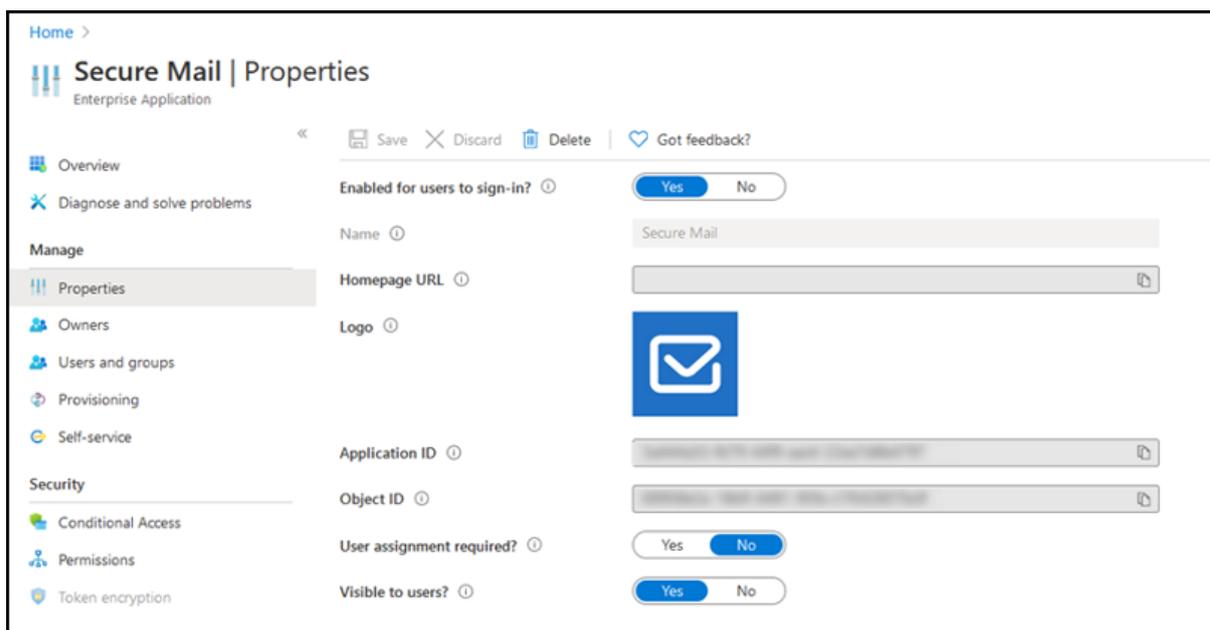
Pré-requisitos

Certifique-se de que o administrador global do Azure Active Directory execute o seguinte:

- Baixe a versão mais recente do Secure Mail em seu dispositivo.
- Configure sua conta do Exchange no aplicativo Secure Mail e dê permissão de aplicativo no Azure Active Directory para que todos os usuários entrem. Consulte a tela a seguir.

Nota:

Estas etapas são específicas apenas para os administradores globais como um requisito único. Uma vez que o aplicativo tenha acesso, você pode simplesmente atualizar a partir da App Store.



Depois de atualizar

Após uma atualização, você será solicitado a fazer a reautenticação após a expiração do token de atualização, que o redireciona para o GCC High no Azure AD. Valide o fluxo de trabalho precedente para garantir que a solicitação de autorização seja enviada para o GCC High no Azure AD.

Você pode validar o fluxo de trabalho de uma das seguintes maneiras:

- O Secure Mail com o nome de aplicativo **Secure Mail-GCC High** aparece na página de login no seu locatário do Azure Active Directory.
- Verifique os logs do Secure Mail para confirmar se os redirecionamentos ocorrem via <https://login.microsoftonline.us> após a reautenticação.

Suporte para arquivos ICS

No Secure Mail, você pode visualizar os arquivos ICS que você recebe como anexos e importá-los para o seu calendário como Eventos.

Imagem do contato no Secure Mail

No Secure Mail, visualize a imagem de um contato quando você adicionar destinatários a e-mails ou convites de reunião. Para obter a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Mostrar fotos de seus contatos](#).

Gerenciar seus feeds

No Secure Mail, agora você pode organizar o seu cartão **Feed** de acordo com os seus requisitos. Para obter a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Organize seu e-mail](#).

Use a política do Office 365 Exchange Server para definir o endereço do servidor do Office 365

No Secure Mail, uma nova política chamada **Office 365 Exchange Server** foi adicionada à seção Suporte de OAuth para Office 365. Com essa política, você pode definir o nome do host para a caixa de correio do Office 365 presente na nuvem. Essa política também habilita o suporte do Office 365 para agências governamentais. O nome do host é um valor único, como *outlook.office365.com*. O valor padrão é *outlook.office365.com*.

Suporte para gerenciamento de criptografia

O gerenciamento de criptografia permite que você use a segurança moderna da plataforma de dispositivos, ao mesmo tempo que garante que o dispositivo permaneça em um estado adequado para usar a segurança da plataforma de forma eficaz. Usando o gerenciamento de criptografia, você elimina a redundância de criptografia de dados local, uma vez que a criptografia do sistema de arquivos é fornecida pela plataforma iOS ou Android. Para habilitar esse recurso, um administrador deve configurar a política MDX de **Tipo de criptografia** como **Criptografia de plataforma com imposição de conformidade** no console Citrix Endpoint Management.

Para usar o recurso de gerenciamento de criptografia, no console Citrix Endpoint Management, defina a política de **Tipo de criptografia** como **Criptografia de plataforma com imposição de conformidade**. Isso habilita o gerenciamento de criptografia e todos os dados de aplicativos criptografados existentes nos dispositivos dos usuários a fazer a transição perfeita para um estado que é criptografado pelo dispositivo e não pelo MDX. Durante essa transição, o aplicativo é pausado para uma migração de dados única. Após a migração bem-sucedida, a responsabilidade pela criptografia de dados armazenados localmente é transferida do MDX para a plataforma do dispositivo. O MDX continua a verificar a conformidade do dispositivo após cada inicialização do aplicativo. Esse recurso funciona em ambientes MDM + MAM e apenas MAM.

Quando você define a política de **Tipo de criptografia** como **Criptografia de plataforma com imposição de conformidade**, a nova política substitui a sua criptografia MDX existente.

Para obter detalhes sobre as políticas MDX de gerenciamento de criptografia para Secure Mail, consulte a seção **Criptografia** em:

- [Políticas de MDX para aplicativos móveis de produtividade para Android](#)
- [Políticas de MDX para aplicativos móveis de produtividade para iOS](#)

Quando um dispositivo fica abaixo dos requisitos mínimos de conformidade, a política de **Comportamento do dispositivo não compatível** permite que você selecione qual ação será executada:

- **Permitir aplicativo** — Permite que o aplicativo seja executado normalmente.
- **Permitir aplicativo após aviso** — Avisa ao usuário que um aplicativo não atende aos requisitos mínimos de conformidade e permite que o aplicativo seja executado. Este é o valor padrão.
- **Bloquear aplicativo** — Bloqueia a execução do aplicativo.

Dispositivos que executam o iOS

Os critérios a seguir determinam se um dispositivo atende aos requisitos mínimos de conformidade para dispositivos com iOS:

- iOS 10 - Um aplicativo está executando uma versão do sistema operacional que é maior ou igual à versão especificada.
- Acesso ao depurador - Um aplicativo não tem a depuração habilitada.
- Dispositivo com jailbroken - Um aplicativo não está sendo executado em um dispositivo com jailbroken.
- Código secreto do dispositivo - O código secreto do dispositivo está **ON**.
- Compartilhamento de dados - O compartilhamento de dados não está habilitado para o aplicativo.

Dispositivos que executam o Android

Os critérios a seguir determinam se um dispositivo atende aos requisitos mínimos de conformidade para dispositivos com Android:

- Android SDK 24 (Android 7 Nougat) - Um aplicativo está executando uma versão do sistema operacional que é maior ou igual à versão especificada.
- Acesso ao depurador - Um aplicativo não tem a depuração habilitada.
- Dispositivos com root - Um aplicativo não está sendo executado em um dispositivo com root.
- Bloqueio do dispositivo - O código secreto do dispositivo está **ON**.
- Dispositivo criptografado - Um aplicativo está sendo executado em um dispositivo criptografado.

Suporte para emails responsivos

O Secure Mail foi otimizado para entregar e-mails responsivos. Anteriormente, o conteúdo de e-mail com grandes tabelas ou imagens era renderizado incorretamente. Este recurso fornece conteúdo de e-mail mais legível em todos os dispositivos suportados, independentemente do formato e tamanho do e-mail.

Arrastar e soltar eventos de calendário

No Secure Mail, você pode alterar a hora de um evento de calendário existente arrastando e soltando o evento. Para obter a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Alterar o horário de um evento de calendário](#).

Gerenciar seus feeds

No Secure Mail, agora você pode organizar o seu cartão **Feed** de acordo com os seus requisitos. Para obter a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Organize seu e-mail](#).

Avanço automático

No Secure Mail, quando você exclui uma mensagem em **Conversas**, você pode escolher para qual mensagem retornar. Para usar esse recurso, navegue até **Configurações > Avanço automático**. Em seguida, selecione sua preferência nas opções disponíveis. Para obter a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Excluir e avançar automaticamente para um e-mail em Conversas](#).

Sincronização automática da pasta Rascunhos

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.

Para obter a documentação de ajuda do usuário sobre esse recurso, incluindo um vídeo, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Sincronização automática da pasta Rascunhos](#).

Suporte para login único usando o Microsoft Intune no modo MDM + MAM

Para dispositivos que executam o iOS:

Para poder usar esse recurso, verifique se o aplicativo Microsoft Authenticator está instalado no seu dispositivo. Para obter mais informações sobre como instalar o aplicativo Microsoft Authenticator, consulte **Download and install the Microsoft Authenticator** em Docs.microsoft.com.

Para dispositivos que executam o Android:

Para poder usar esse recurso, verifique se o aplicativo Portal da Empresa do Intune está instalado em seu dispositivo. Depois de fazer login no aplicativo Portal da Empresa do Intune, você poderá usar o SSO no modo MDM + MAM sem precisar autenticar novamente no Secure Mail usando suas credenciais.

Melhorias em Contatos

No Secure Mail, 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, 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.

Várias contas do Exchange

Em Configurações, no Secure Mail, você 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. Os pré-requisitos do administrador são os seguintes:

- 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. 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 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 ADC.
- O Secure Mail para iOS oferece suporte somente a servidores de correio Exchange e Office 365.

Para obter a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Adicionar contas do Exchange](#).

Contatos

Para obter a documentação de ajuda do usuário sobre Contatos, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Exibir e sincronizar os seus contatos](#).

Atribuir cores em Calendários

Para obter a documentação de ajuda do usuário sobre esse recurso de Calendário, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Atribuir cores para calendários sincronizados do Secure Mail](#).

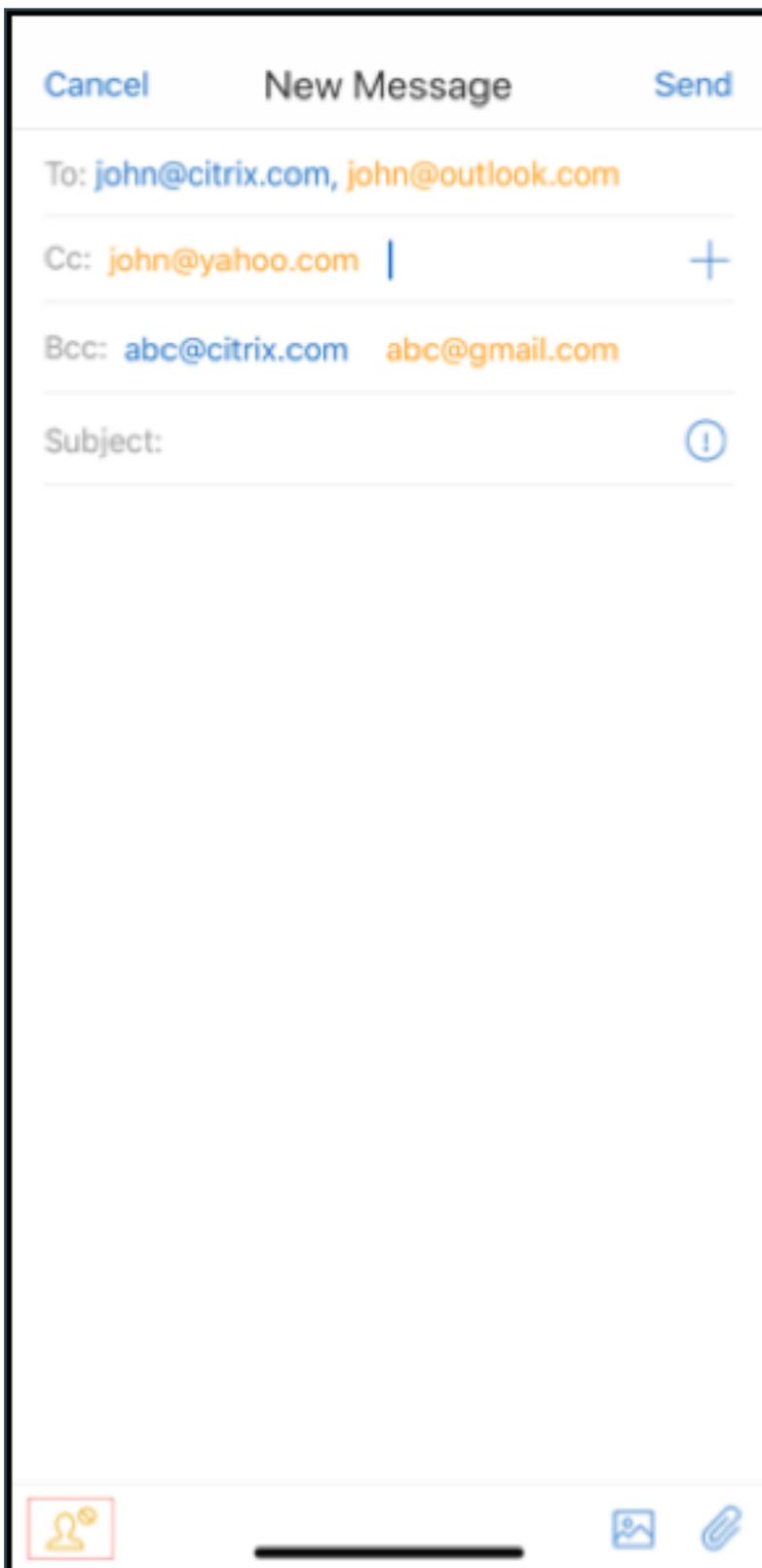
Domínios internos

Você pode identificar e editar destinatários de email que pertencem a organizações externas.

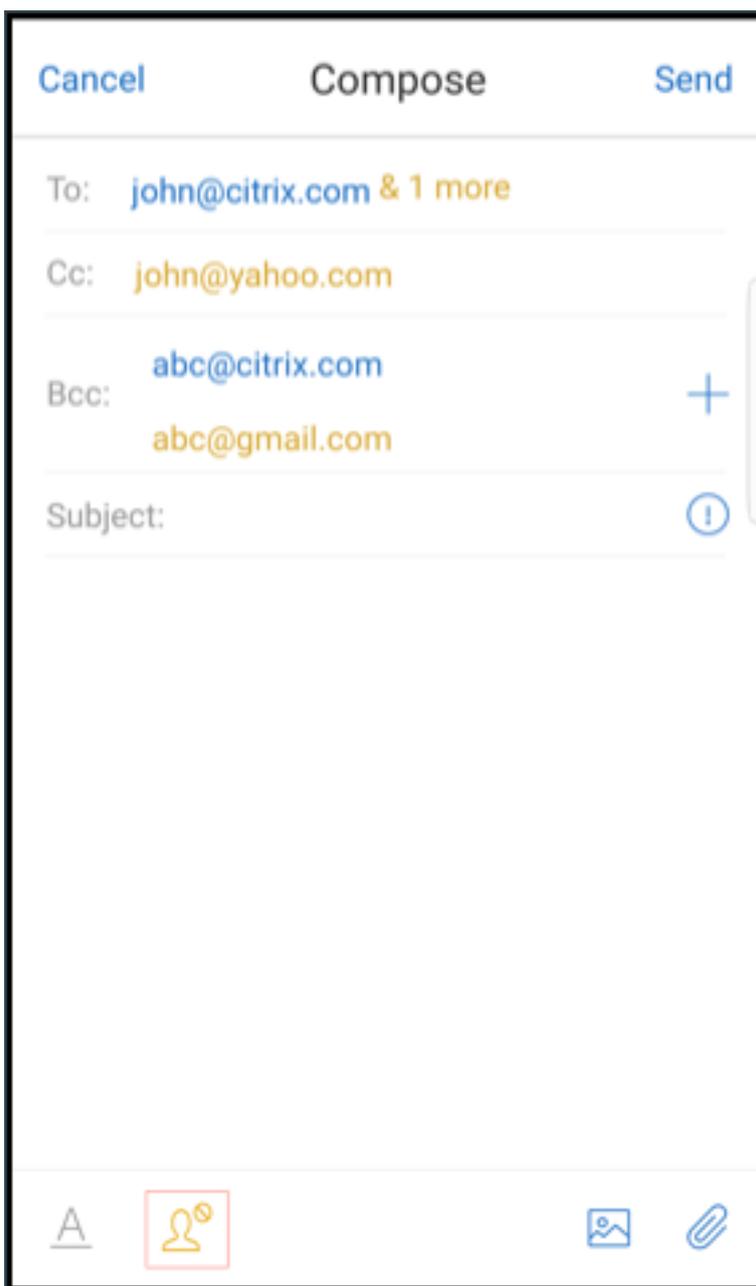
Pré-requisito: Certifique-se de ter ativado a política de **Domínios Internos** no Citrix Endpoint Management e reiniciado o aplicativo.

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.

Em dispositivos que executam o iOS:

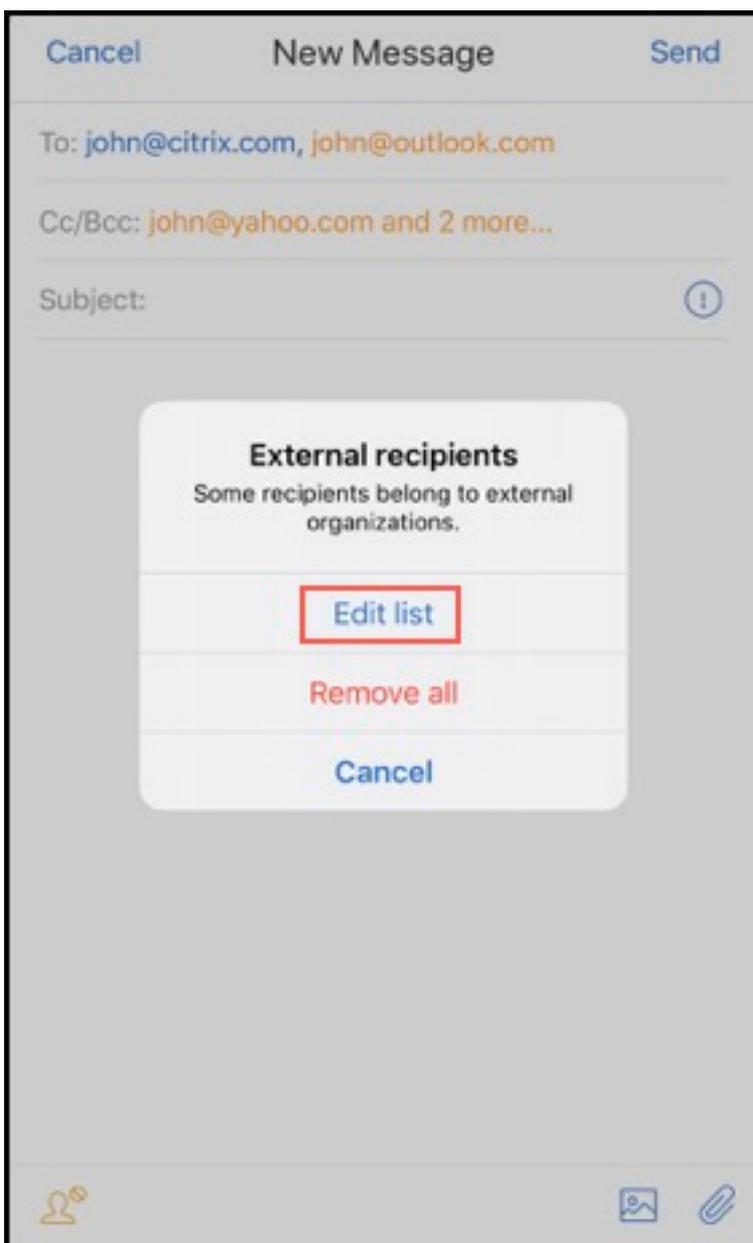


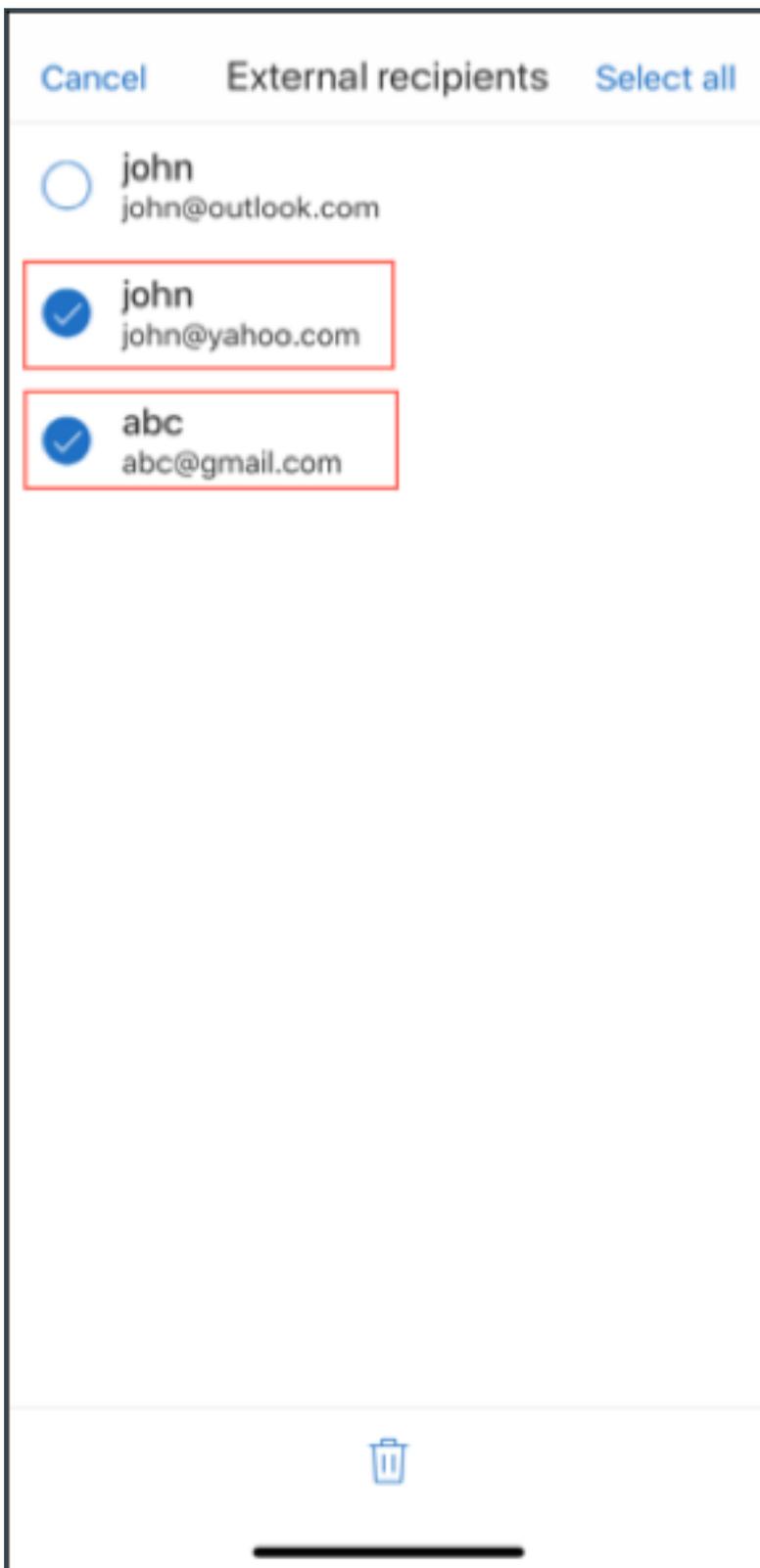
Em dispositivos que executam o Android:



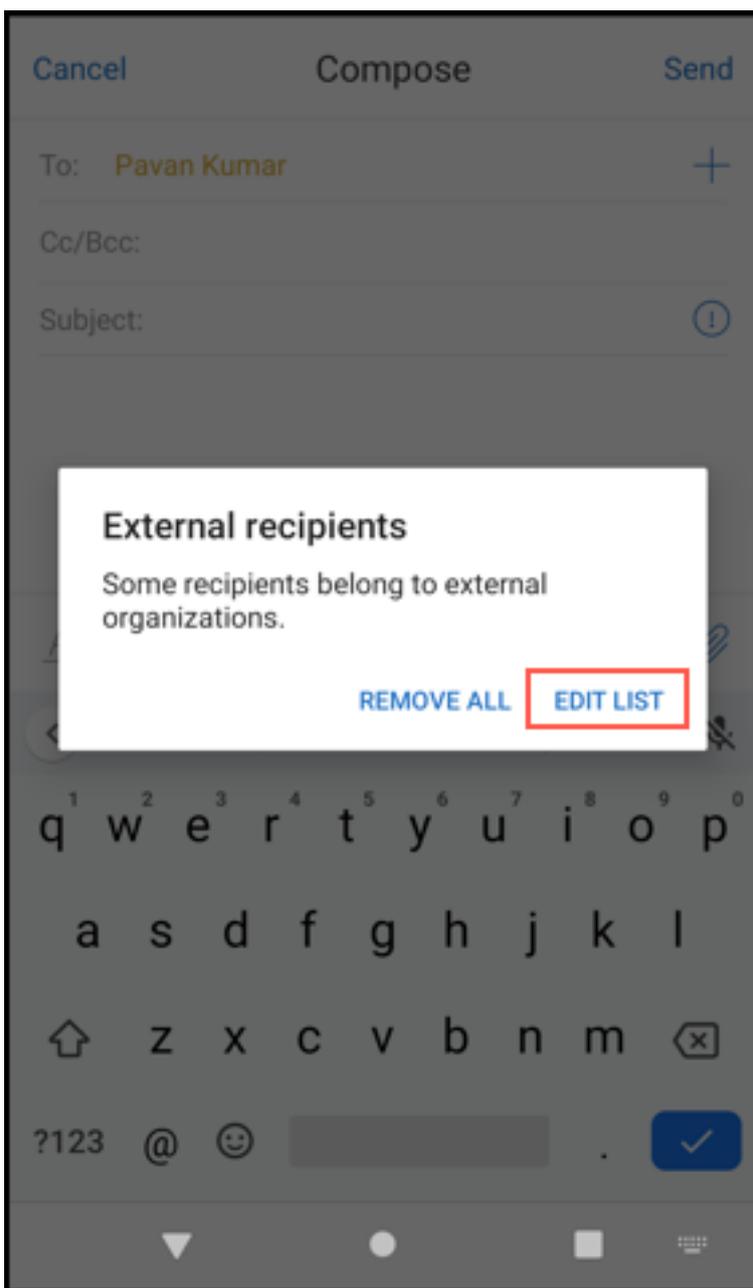
Quando você toca no ícone **Contatos**, uma janela pop-up aparece com opções para editar a lista ou remover tudo. Toque em **Editar lista** para escolher os destinatários que deseja remover. Depois de selecionar os destinatários, toque no ícone de **Lixeira**.

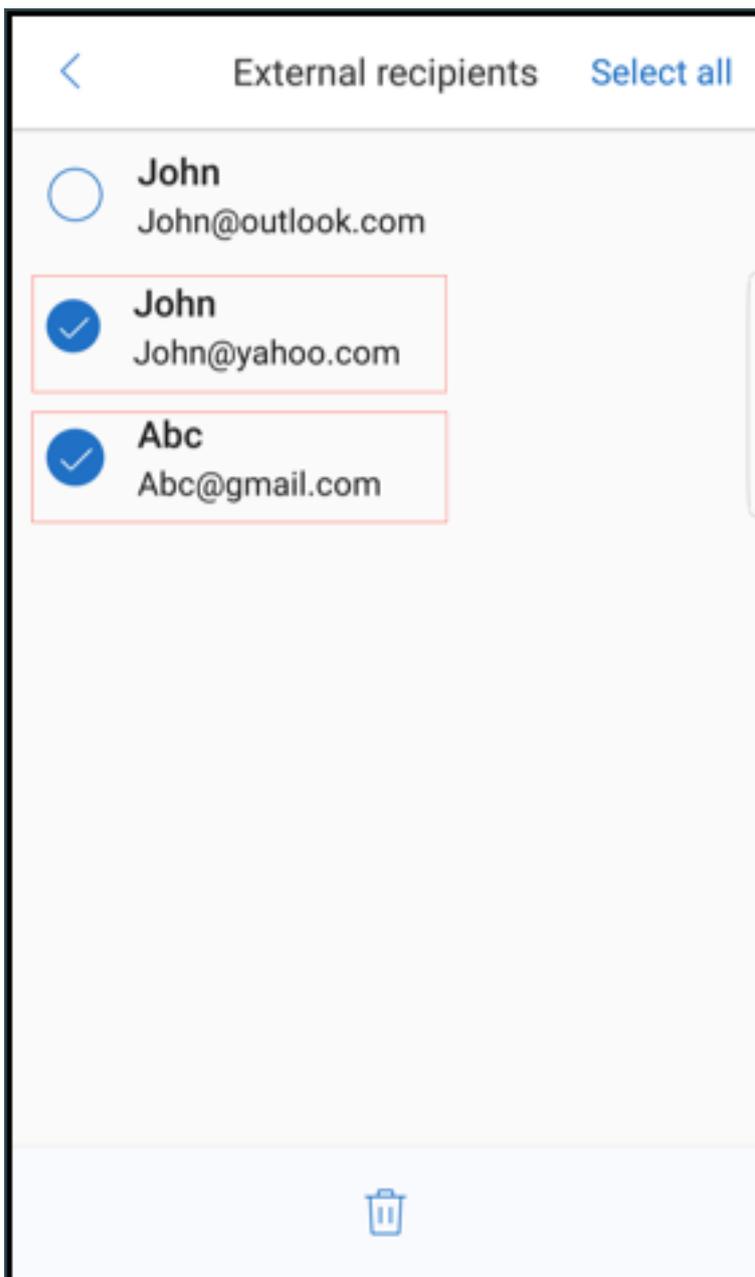
Em dispositivos que executam o iOS:





Em dispositivos que executam o Android:





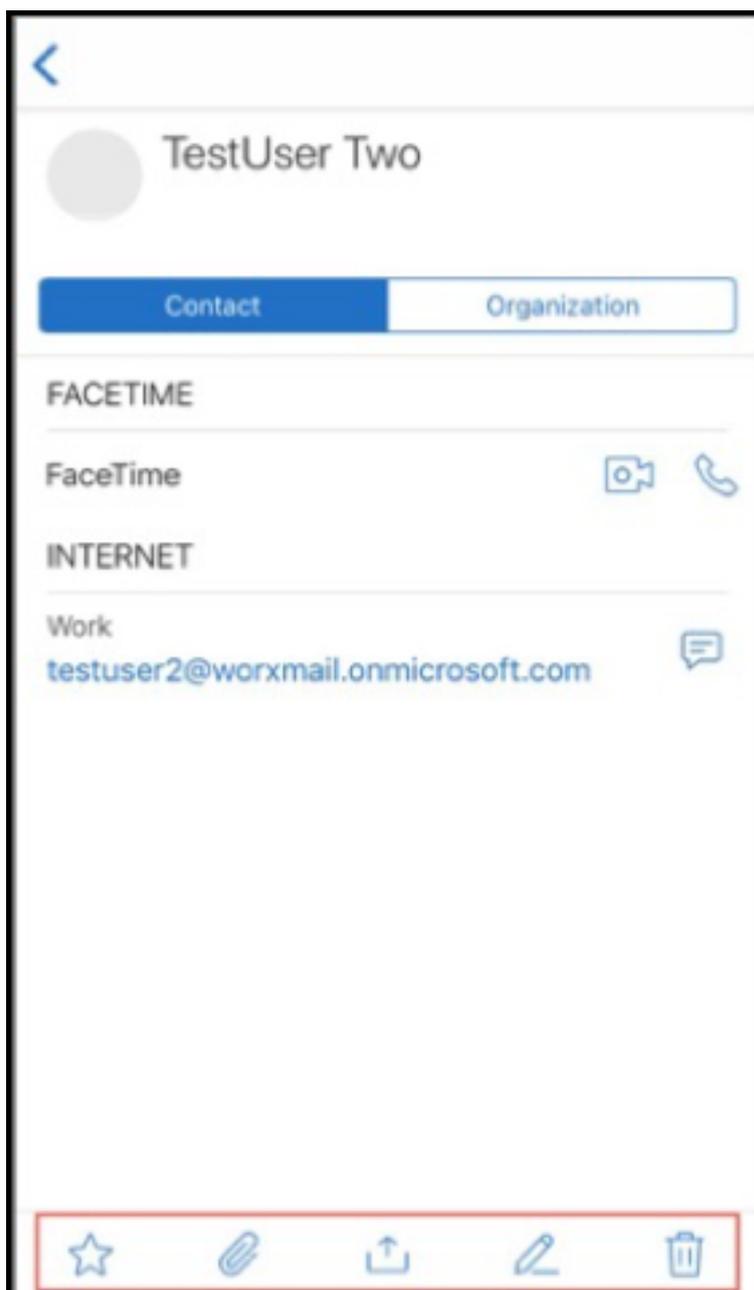
Melhorias ergonômicas

Com esse aprimoramento, os botões de ação são 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**.

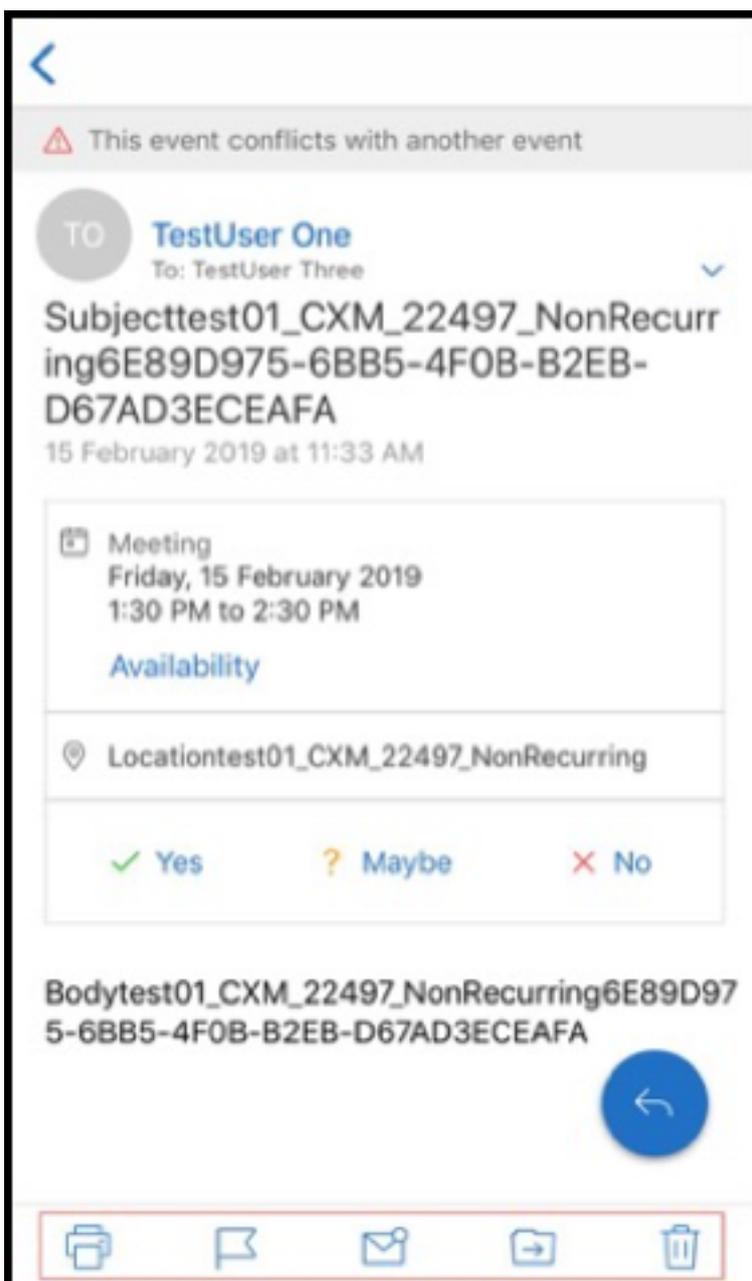
Nota:

No Android, as alterações são feitas nas telas **Caixa de entrada** e **Calendário**.

Em dispositivos que executam o iOS



Em dispositivos que executam o Android



O botão de ação flutuante **Responder** foi aprimorado para se alinhar à identidade visual da Citrix e ao guia de estilo.

Além disso, com este aprimoramento, a opção para acessar os botões na tela principal da Caixa de Entrada a partir de um e-mail aberto é removida. Você precisa sair do e-mail aberto para acessar itens como **Feeds, Calendário, Contatos e Anexos**.

As opções na barra de rodapé do iOS foram alteradas, o que ajuda a manter a uniformidade entre iOS e Android.

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 \(visualização\)](#).

Denunciar e-mail de phishing (como encaminhamento)

No Secure Mail, 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 a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Denunciar um e-mail de phishing](#).

Denunciar um e-mail de phishing

Você pode denunciar um e-mail de phishing com base na política que um administrador configura. Para obter a documentação de ajuda do usuário sobre esse recurso, incluindo detalhes sobre as configurações de administrador, consulte o artigo do Centro de Ajuda ao Usuário Citrix, [Denunciar um e-mail de phishing](#).

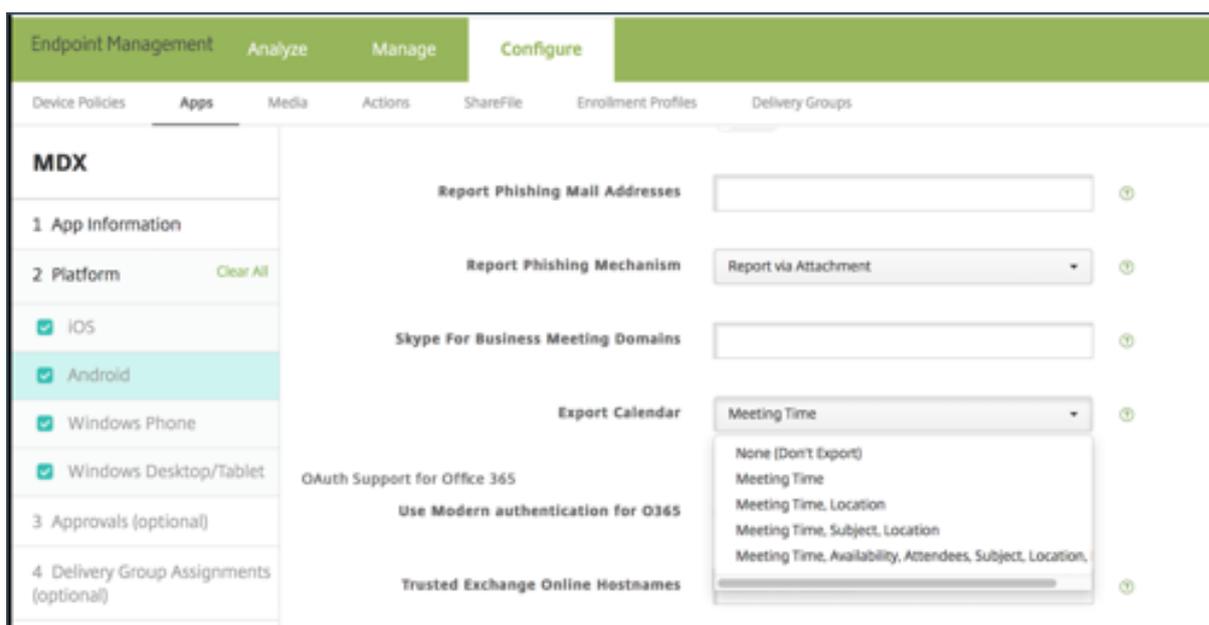
Exportar eventos de calendário do Secure Mail

Usando o Secure Mail para iOS e Android, você pode exportar eventos de calendário do Secure Mail para o aplicativo de calendário nativo do seu dispositivo. Para obter a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Exportar seus eventos de calendário do Secure Mail](#).

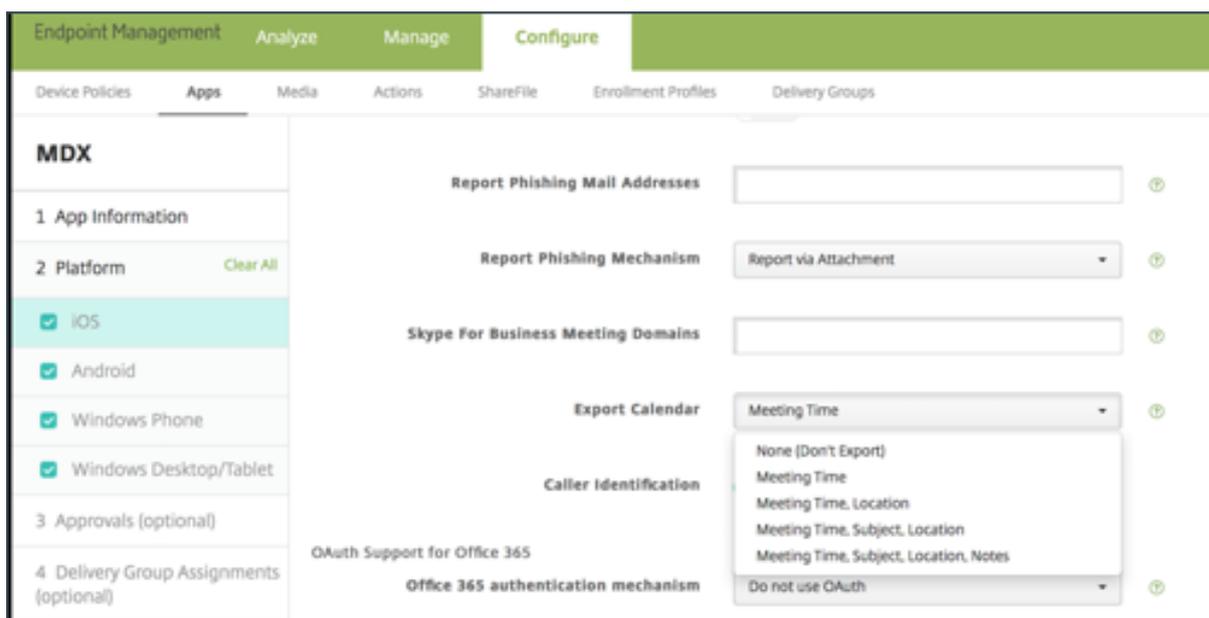
Os seguintes valores da política MDX estão disponíveis para os campos de evento do calendário que aparecem em seu calendário pessoal:

- Nenhum (não exportar)
- Hora da reunião
- Hora da reunião, local
- Hora da reunião, assunto, local
- **(Para Android)** Hora da reunião, disponibilidade, participantes, assunto, local, anotações
- **(Para iOS)** Hora da reunião, assunto, local, anotações

Opções do Android:



Opções do iOS:



Para iOS

Embora os eventos de calendário exportados do Secure Mail sejam **leitura/gravação**, as alterações feitas em eventos fora do Secure Mail não estão disponíveis.

Importante:

- Esse recurso é visível, mas desabilitado no Secure Mail, se uma das seguintes condições for verdadeira:

- A política de Exportação de Calendário está definida como **OFF**.
- Sua versão do MDX não contém a política
- Esse recurso não funciona se as contas de e-mail já estiverem configuradas no seu aplicativo de calendário pessoal e sua conta do iCloud estiver desativada. Esse recurso funciona se nenhuma outra conta estiver configurada no seu aplicativo de calendário pessoal.
- Para iniciar a URL e editar os eventos de calendário do Secure Mail a partir do seu calendário pessoal, verifique se o valor “**ctxevent:**” está incluído na política MDX de esquemas de URL do aplicativo.

Para Android

Os eventos de calendário que são exportados do Secure Mail são somente leitura. Para editar eventos do Secure Mail, toque no link **Evento do Secure Mail** no evento do seu calendário.

Importante:

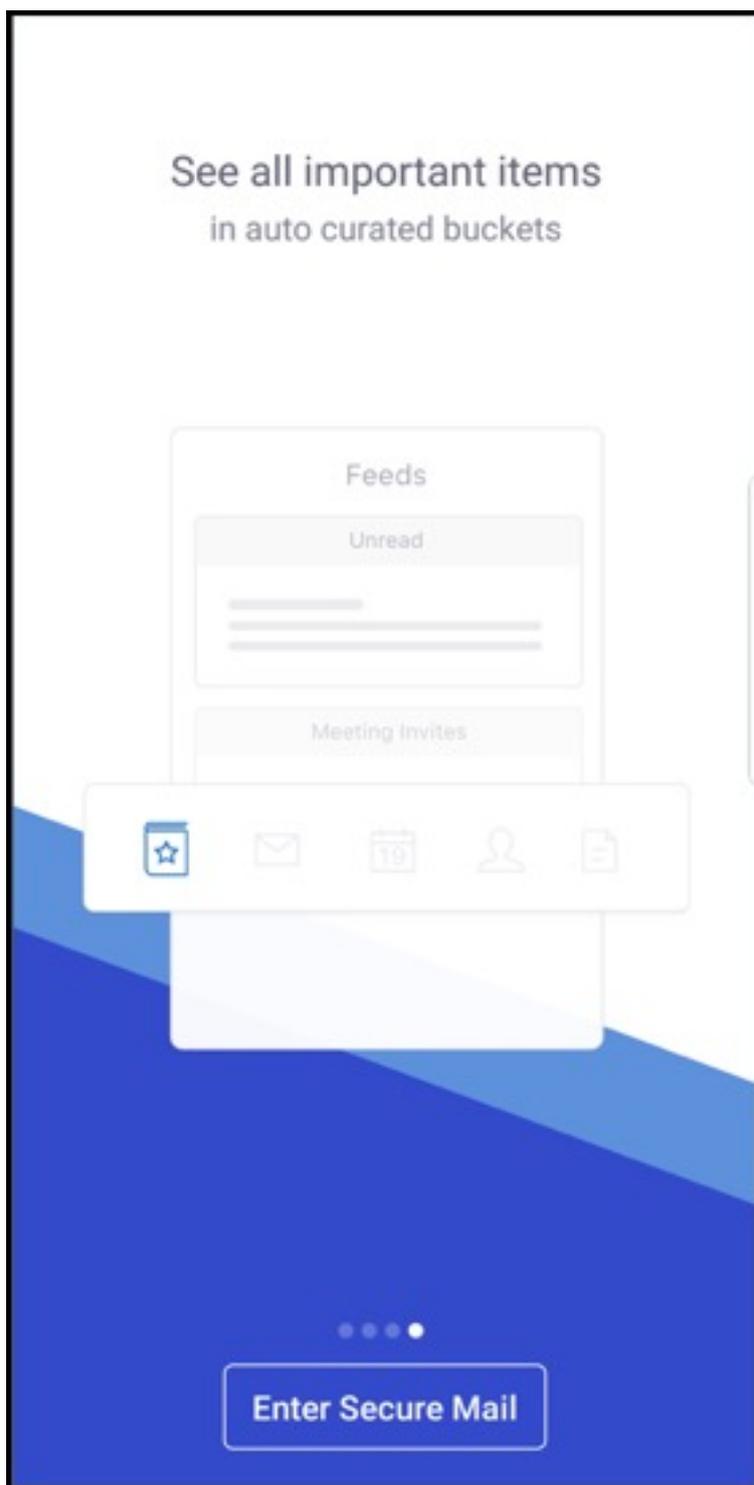
- Esse recurso é visível, mas desabilitado no Secure Mail, se uma das seguintes condições for verdadeira:
 - A política de Exportação de Calendário está definida como **OFF**.
 - Sua versão do MDX não contém a política
- Certifique-se de que a política MDX de troca de documentos recebidos esteja definida como **Irrestrito**.
- O link Evento do Secure Mail não está disponível nos dispositivos Samsung e Huawei.

Pastas de feed

O Secure Mail apresenta todos os seus emails não lidos, convites para reuniões que exigem sua atenção e suas próximas reuniões na pasta **Feeds**.

Para ver seus cartões de feed

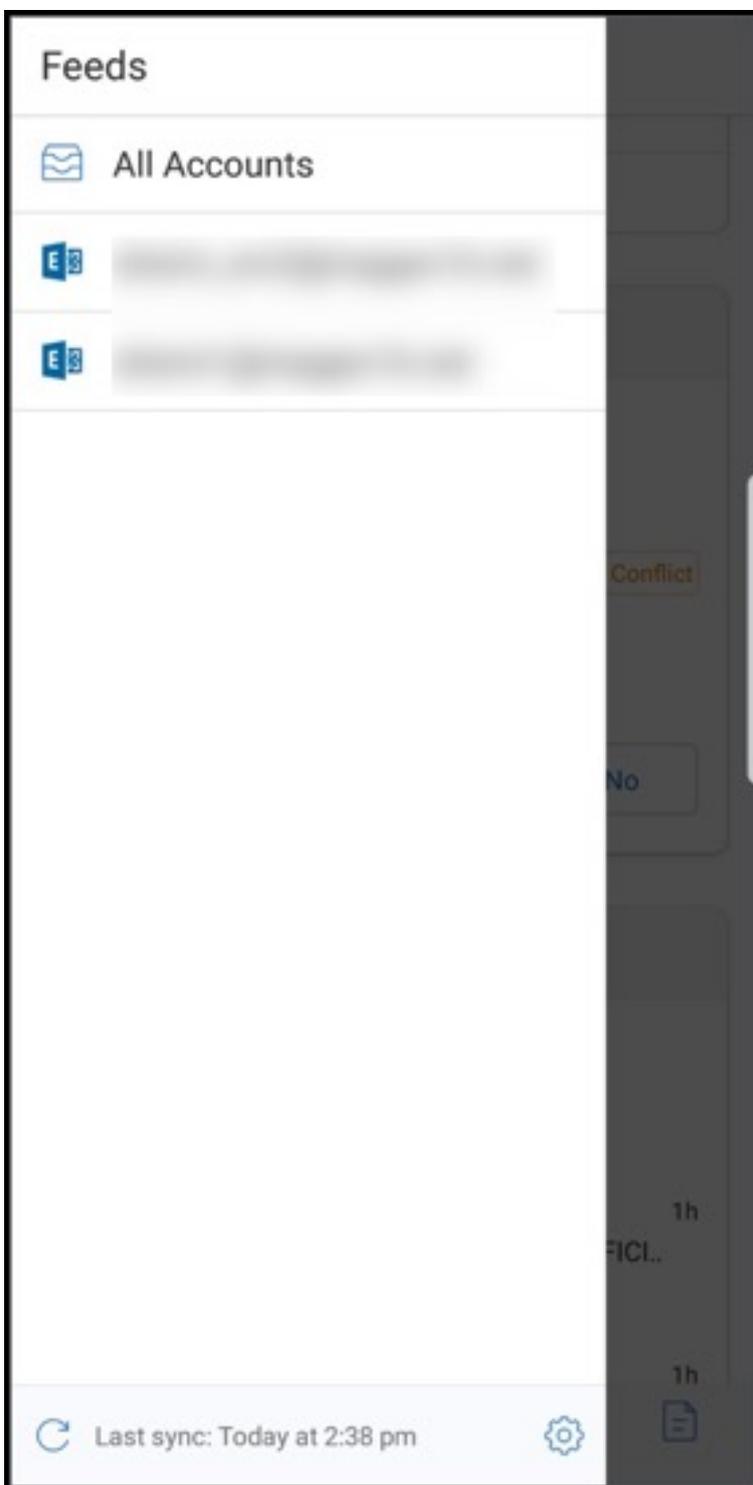
Toque no ícone **Feeds** na parte inferior direita da barra de guias do rodapé.



Os seguintes cartões de feed aparecem:

- Não lida(s)
- Convites para reuniões
- Próximas reuniões

Por padrão, o Secure Mail exibe feeds apenas da sua conta principal. Se você configurou mais de uma conta, poderá ver os feeds das outras contas. Para ver os feeds de outra conta, toque em **Feeds**, toque no ícone do hambúrguer de menus e selecione a respectiva conta.



Os feeds são classificados com base no carimbo de data/hora do item e aparecem com o seguinte

limite superior:

- Cinco emails não lidos
- Dois convites para reuniões
- Três reuniões agendadas

Para ver todos os itens em um cartão de feed, toque em **Ver todos**.

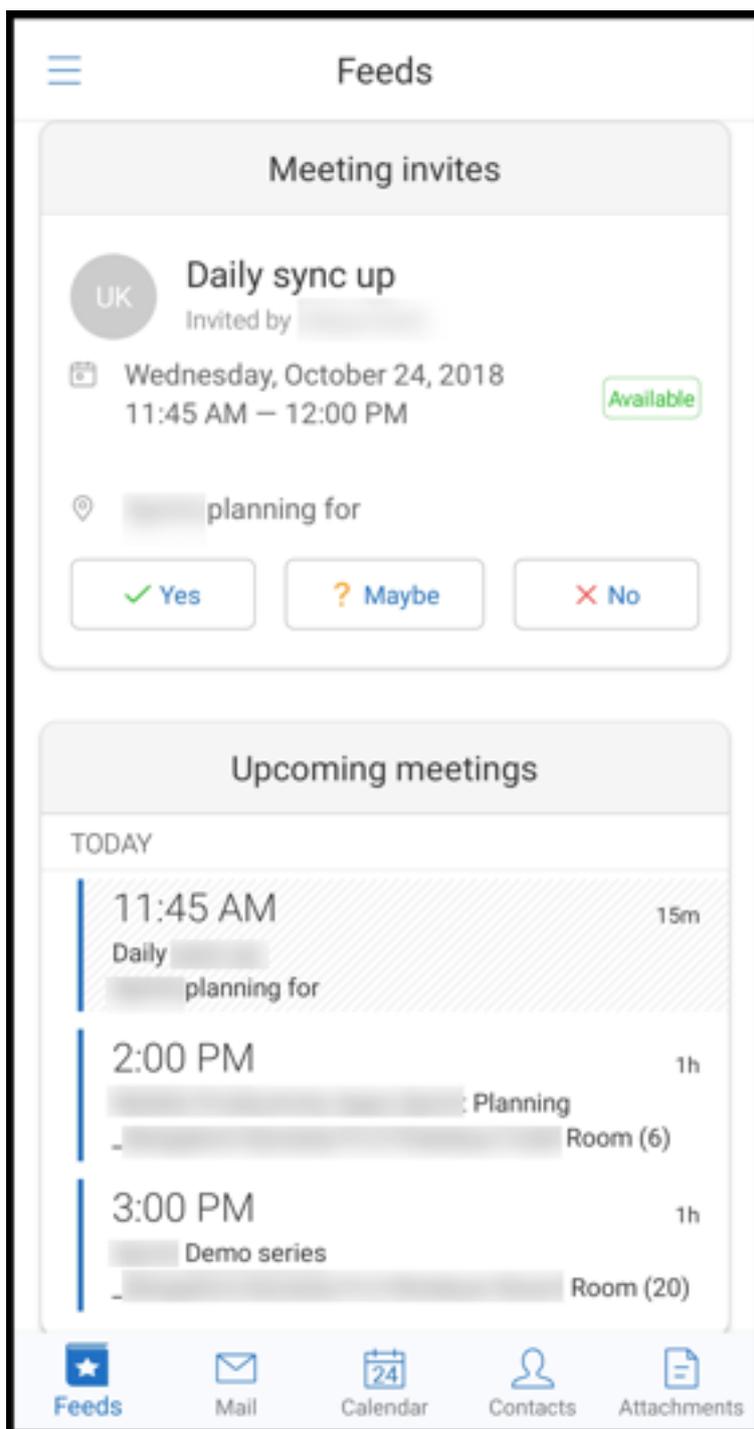
Nota:

O número de feeds exibidos em cada cartão depende do período de sincronização de emails que você definiu no seu dispositivo.

Aprimoramentos à pasta Feeds

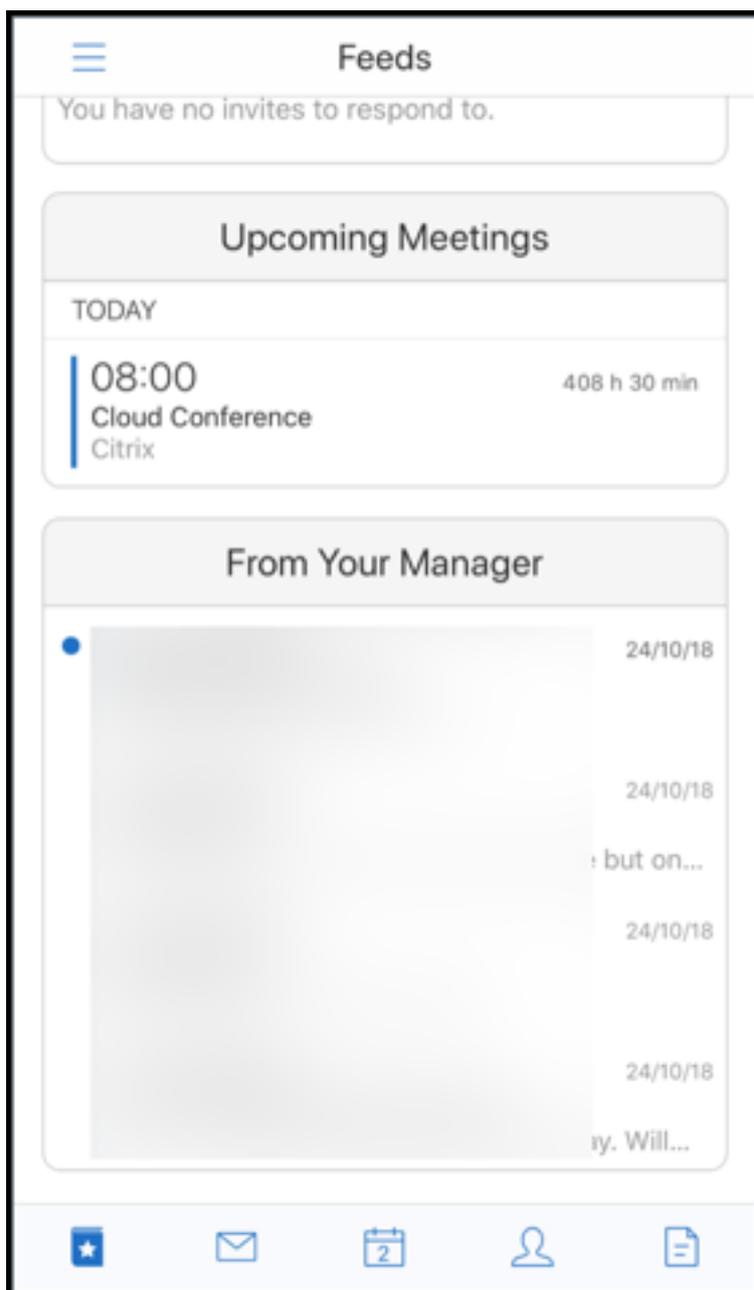
A seguir estão os aprimoramentos à pasta **Feeds**:

- 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 do próximo período de 24 horas aparecem no cartão Feeds e são categorizadas nas Seções **Hoje** e **Amanhã**.



Feeds do seu gerente

No Secure Mail, 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.

Entrar em reuniões a partir do calendário

No Secure Mail, os usuários podem participar de reuniões diretamente a partir de convites no Calendário. As seguintes tabelas listam os tipos de reunião e formatos de número de telefone que têm suporte e os requisitos de discagem para cada um.

Tipos de reunião com suporte

Tipo de reunião	Requisitos de identificação	Ação depois de tocar em Participar de uma reunião
Microsoft Teams		Se o aplicativo Microsoft Teams estiver instalado, o aplicativo é aberto e o usuário entra na reunião. Se o aplicativo não estiver instalado, o usuário verá uma opção para instalar o Microsoft Teams a partir da loja de aplicativos.
GoToMeeting (GTM)	Um dos seguintes no conteúdo da reunião: 1) Este tipo de URL: https://www1.gotomeeting.com/join/1234567892 ; 2) Código de acesso do GTM em qualquer um destes formatos: GTM: 123456789, GTM - 123456789, G2M - 123456789, G2M: 123456789	Se o aplicativo GTM estiver instalado, aplicativo é aberto e o usuário entra na reunião. Se o aplicativo não estiver instalado, o usuário vê uma opção para ir à loja de aplicativos para instalar GTM. No caso de GTMs no formato gotomeet.me/nome-de-usuário, o aplicativo é aberto e o usuário entra na reunião.

Tipo de reunião	Requisitos de identificação	Ação depois de tocar em Participar de uma reunião
WebEx		O Citrix Secure Web abre e abre o aplicativo WebEx não preparado, se estiver instalado no dispositivo. O WebEx deve ser adicionado como uma exceção na política Lista restrita de exceção de Abrir em do Secure Web na política URLs permitidos no iOS.
Skype for Business		Os usuários podem clicar em um link que se abre no Secure Web e que então abre o aplicativo Skype for Business não preparado, se estiver instalado no dispositivo. Adicione o aplicativo Skype for Business como uma exceção na política Lista restrita de exceção de Abrir em do Secure Web no Android. Adicione a exceção na política de URLs permitidos no iOS.

Configurar a lista de políticas a seguir permite que os usuários toquem em um link de reunião para abrir o aplicativo relevante.

Aplicativo Microsoft Teams

- ****iOS - Política “Permitir URLs”:** ^msteams:
- ****Android - Política “Exclusões Abrir em”:** {action=android.intent.action.VIEW scheme=msteams package=com.microsoft.teams}

Aplicativo Zoom

- **iOS - Política “Permitir URLs”:** +^zoomus:

- **Android - Política “Exclusões Abrir em”:**{action=android.intent.action.VIEW scheme=zoomus package=us.zoom.videomeetings}

Webex (aplicativo não preparado)

- **iOS - “Política ‘Permitir URLs’:** +^wbx: Uma sequência de políticas de exemplo é ^http;^https;^mailto:=ctxmail;+^citrixreceiver;+^telprompt;+^tel;+^col-g2m-2;+^col-g2w-2;+^wbx;+^maps:ios_addr:
- **Android - Política “Exclusões Abrir em”:** {action=android.intent.action.VIEW scheme=wbx package=com.cisco.webex.meetings}

Skype for Business

- **iOS - Política “Permitir URLs”:** +^lync:
- **Android - Política “Exclusões Abrir em”:**{action=android.intent.action.VIEW scheme=lync package=com.microsoft.office.lync15}

Skype

- **iOS - Política “Exclusões Abrir em”:** +^skype:
- **Android - Política “Exclusões Abrir em”:** {action=android.intent.action.VIEW scheme=skype package=com.skype.raider}

Especificações de discagem

A lista a seguir indica o tipo de reunião e o respectivo formato de número de telefone suportado e formato de código de conferência para cada um.

GoToMeeting (GTM):

Formatos de número de telefone com suporte:

- Qualquer número de telefone em formatos GTM. Exemplos:
 - Índia (chamada gratuita) 000 800 100 7855
 - Estados Unidos (chamada gratuita): 1 877 309 2073
- Qualquer número de telefone que satisfaça aos formatos padrão de RFC 3966. Para detalhes, consulte o [documento de protocolo de rastreamento de padrões da Internet](#).

Formatos de código de conferência com suporte:

O código de conferência é obtido a partir de qualquer um dos seguintes formatos no corpo da reunião:

- URL (*.gotomeeting.com/join/123456789)
- URL (formato [gotomeet.me/username](#))

- Formatos “GTM”, como “GTM:123456789”
- Formatos “G2M” como “G2M:123456789”
- Formatos como “Código de Acesso: 123456789”

WebEx:

Formatos de número de telefone com suporte:

- Qualquer número de telefone em formatos de chamada do WebEx. Exemplos (Verizon e EUA):
 - 1-866-652-5088
 - 1-517-466-3109
- Qualquer número de telefone em formato de conexão de áudio WebEx. Exemplo:
 - 1-650-479-3207 (EUA chamada tarifada)
- Qualquer número de telefone que satisfaça aos formatos padrão de RFC 3966.

Formatos de código de conferência com suporte:

O conteúdo da reunião deve conter um destes formatos:

- Número da reunião: 123 456 789
- Código de acesso: 123 456 789

Nota:

No caso de códigos de conferência que têm até nove dígitos, a tecla # é adicionada automaticamente para discar para a reunião.

Skype for Business

Formatos de número de telefone com suporte:

- Qualquer número de telefone em formatos RFC 3966. Para detalhes, consulte o [documento de protocolo de rastreamento de padrões da Internet](#).

Formatos de código de conferência com suporte:

O corpo da reunião contém este texto: “ID da conferência: 123456789”

Nota:

O símbolo # é adicionado automaticamente no caso de reuniões do Skype for Business.

Informações genéricas de conferência de áudio

Formatos de número de telefone com suporte:

- Qualquer número de telefone nos formatos RFC 3966 Para obter detalhes, consulte o [documento de protocolo de rastreamento de normas da Internet](#). Exemplos:

- 5555555555
- (555) 555-5555
- 555-555-5555
- 555-555-555-5555 (no caso de código de país)
- 1-555-555-5555
- +1-555-555-5555

Nota:

Use um único separador entre dígitos no número de telefone. Por exemplo, “) –” pode fazer com que o número não seja reconhecido.

Formatos de código de conferência com suporte:

Formato recomendado: “(número de telefone);”(código)”

Você pode especificar até quatro vírgulas e fornecer a tecla # se necessário. Consulte a tabela situada posteriormente neste documento para obter uma lista de formatos para os quais há suporte.

Para uma conferência de áudio, os seguintes formatos permitem que os usuários toquem em **Dis-car**. Eles podem tocar o número de telefone do corpo da reunião calendário, no entanto, podem discar para a reunião. Eles devem então digitar códigos de conferência manualmente. Os seguintes formatos de número de telefone e de conferência têm suporte.

Formatos de número de telefone com suporte	Separador de código de conferência	Exemplo
Qualquer número de telefone em formatos RFC 3966. Exemplos: 5555555555; (555) 555-5555; 555-555-5555; 555-555-555-5555 (no caso de código do país); 1-555-555-5555;+1-555-555-5555	Código do participante	1-888-999-9999 Código de participantes: 9999999
	PIN do Participante	1-888-999-9999 PIN de participante: 99999999
	Código de convidado	1-888-999-9999 Código de convidado: 99999999
	PIN de convidado	1-888-999-9999 PIN de convidado:99999999
	Código de participante/convidado	1-888-999-9999 Código de participante/convidado:99999999

Formatos de número de telefone com suporte	Separador de código de conferência	Exemplo
	Código de cargo	1-888-999-9999 Código do cargo:99999999
	PIN de cargo	1-888-999-9999 PIN do cargo:99999999
	Código de membro de diretoria	1-888-999-9999 Código do membro da diretoria:99999999
	PIN de membro de diretoria	1-888-999-9999 PIN do membro da diretoria:99999999
	PIN de host	1-888-999-9999 PIN de host:99999999
	PIN	1-888-999-9999 PIN:99999999
	Código de acesso	1-888-999-9999 Código de acesso:99999999
	Código	1-888-999-9999 Código:99999999
	Código de conferência	1-888-999-9999 Código de conferência:99999999
	ID da conferência	1-888-999-9999 ID de conferência:99999999
	,	+1 (631) 992-3240,958209234#
	”	+1 (631) 992-3240,,958209234#
	””	+1 (631) 992-3240,,,958209234#
	”””	+1 (631) 992-3240,,,,958209234#
	código secreto	+1 (631) 992-3240 código secreto 958209234#
	ext:	+1 (631) 992-3240 ext:958209234#

Formatos de número de telefone com suporte	Separador de código de conferência	Exemplo
	ext.	+1 (631) 992-3240 ext. 958209234#
	;ext=	+1 (631) 992-3240;ext. 958209234#
	extn	+1 (631) 992-3240 extn 958209234#
	HC	+1 (631) 992-3240 HC 958209234#
	xtn	1 (631) 992-3240 xtn 958209234#
	xt	+1 (631) 992-3240 xt 958209234#
	x	+1 (631) 992-3240 x 958209234#
	PC	+1 (631) 992-3240 PC 958209234#
	pc	+1 (631) 992-3240 pc 958209234#

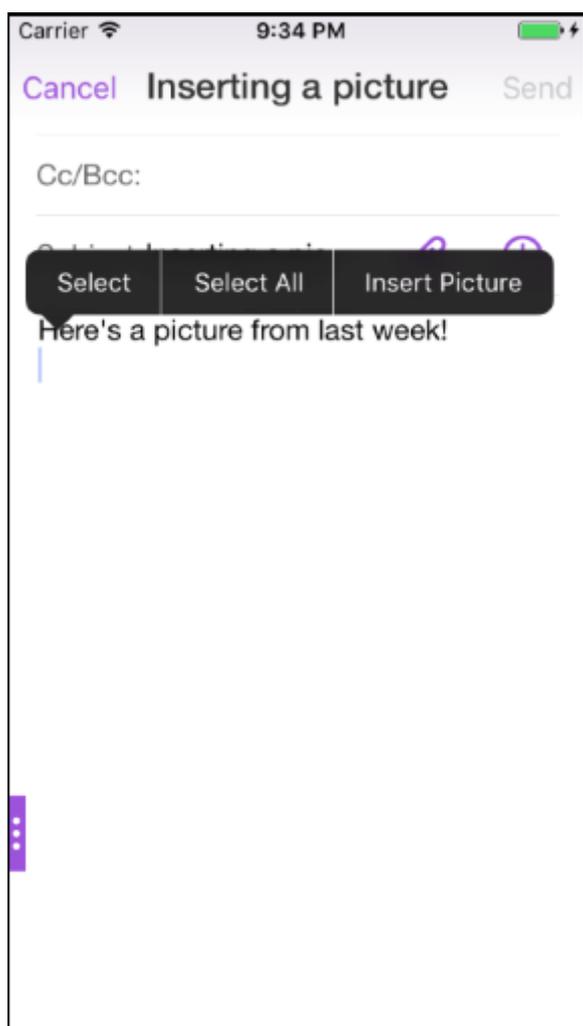
Sobreposição de calendário pessoal

Em dispositivos iOS e Android, é possível importar seu calendário pessoal do aplicativo nativo de calendário e veja seus eventos pessoais no Secure Mail. Para obter a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Ver eventos em seu calendário pessoal](#).

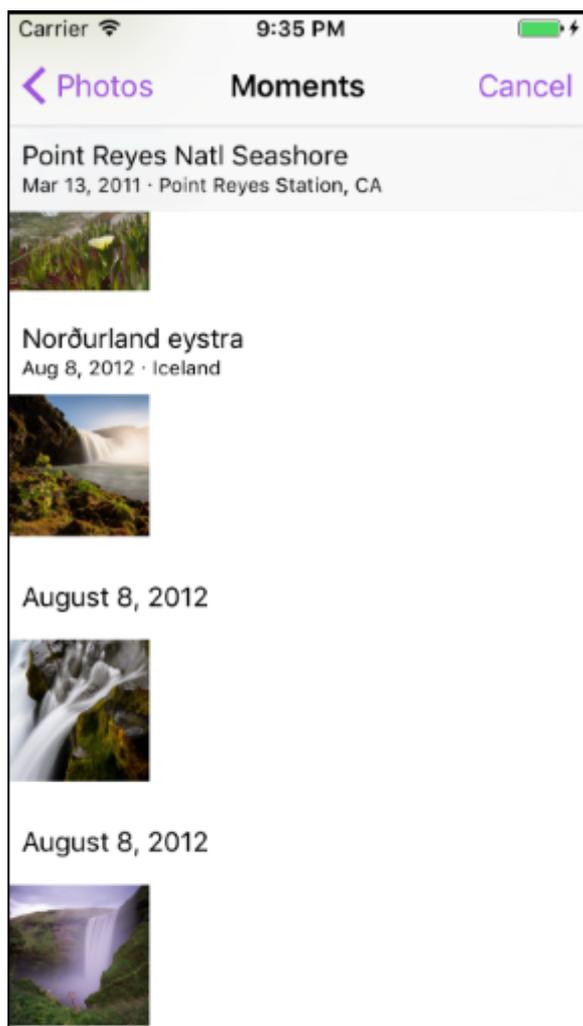
Inserir uma imagem em linha

O procedimento a seguir descreve como inserir uma imagem em linha.

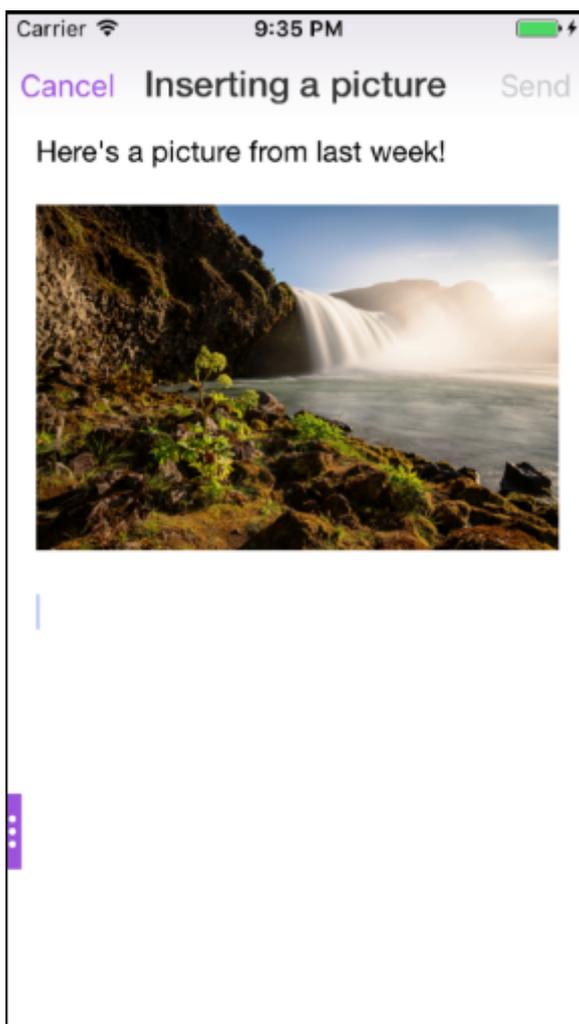
1. Para anexar uma imagem em linha ao seu email, pressione longamente o corpo do email. Nas opções que aparecem, toque em **Inserir figura**.



2. O Secure Mail poderá solicitar a você o acesso às suas fotos. É exibida a Galeria de fotos Navegue até a galeria e toque na imagem que deseja inserir.



3. O email agora contém a imagem que você selecionou.



Ações de deslizamento

Em dispositivos iOS e Android, execute as ações deslizando um email para a esquerda ou para a direita. Para obter a documentação de ajuda do usuário sobre esse recurso, consulte o artigo no Centro de Ajuda ao Usuário Citrix, [Usar ações de deslizar](#).

Ingresse em reuniões do Skype for Business para iOS e Android

Você pode ingressar em reuniões do Skype for Business diretamente por meio do Secure Mail. Este recurso requer que o aplicativo Skype para Business esteja instalado no seu dispositivo.

Para ingressar em uma reunião do Skype for Business

1. Toque no lembrete de reunião de negócios ou evento de calendário do Skype for Business.

2. Na tela **Detalhes do evento**, toque em **Ingressar em uma reunião** do Skype. A reunião Skype for Business é iniciado em uma nova janela.

Se você não tiver instalado o Skype for Business no seu dispositivo, toque em **Instalar Skype** para instalar o aplicativo.

Visualização dentro do aplicativo de anexos e outros aprimoramentos anexos

Agora você pode visualizar anexos (MS Office e imagens) dentro do aplicativo Secure Mail, em vez de abri-los usando aplicativos de terceiros, como o QuickEdit.

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.
- Selecione uma nova mensagem à qual arquivo deverá ser anexado.
- Salvar o anexo para acesso offline.
- Excluir anexos de arquivos offline.
- Abrir o anexo usando outro aplicativo.
- Exibir o origem email ou evento de calendário do anexo.

Nota:

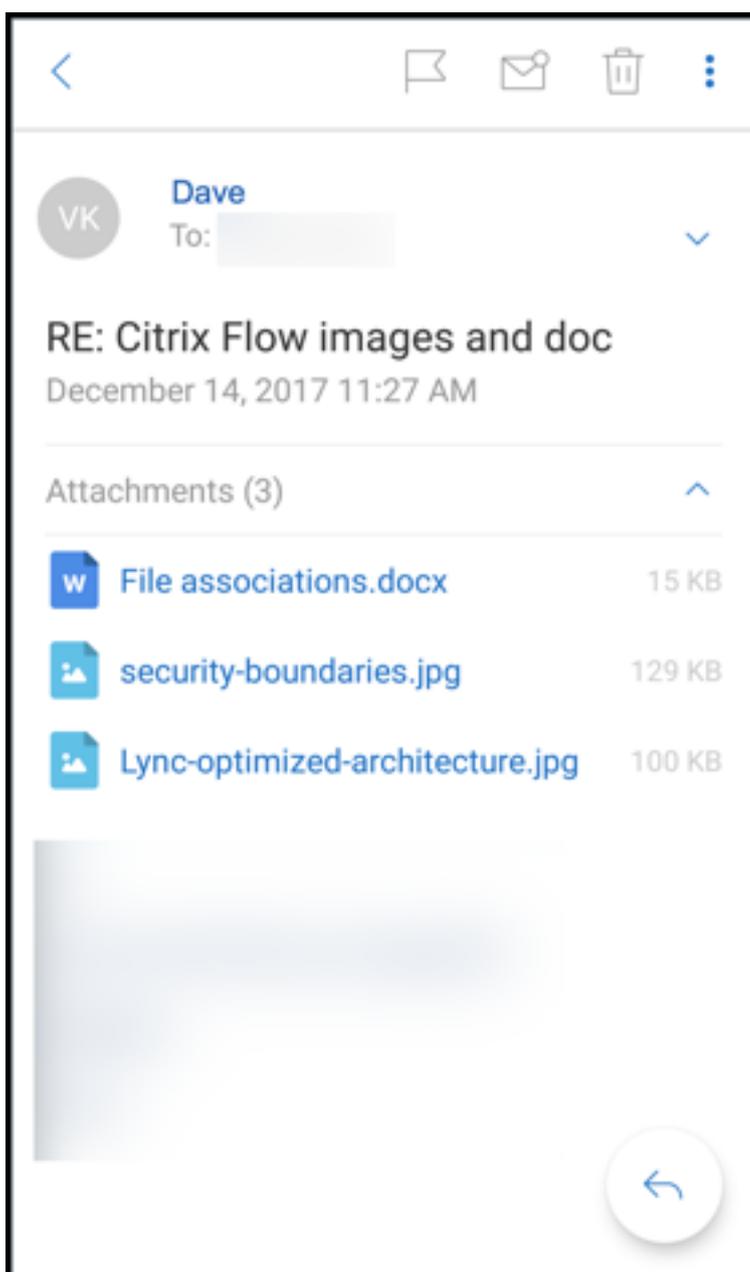
Você pode exibir o email ou evento de calendário de origem apenas ao exibir anexos do repositório de **Anexos**.

Você também pode visualizar anexos nos seguintes casos:

- Ao exibir mensagem.
- A compor uma nova mensagem.
- Pasta de anexos.
- Eventos de calendário

Para selecionar uma nova mensagem à qual anexar o arquivo

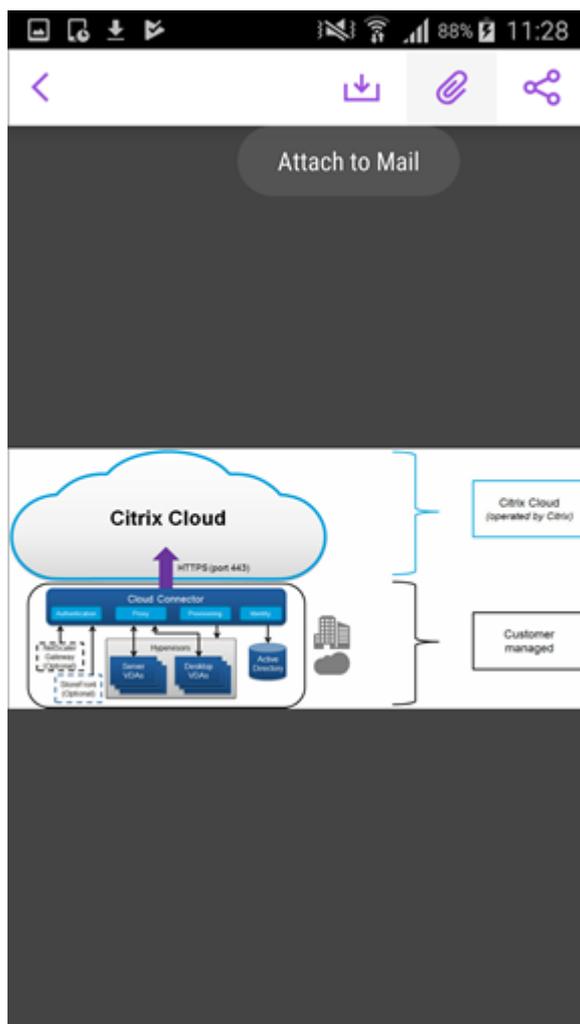
1. Abra o email com o anexo.



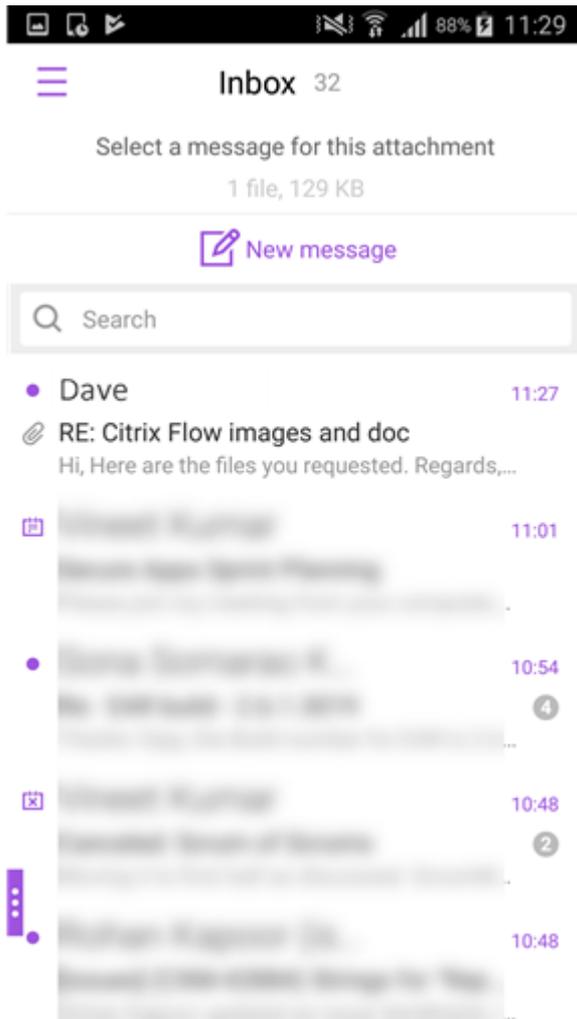
2. Toque no anexo.

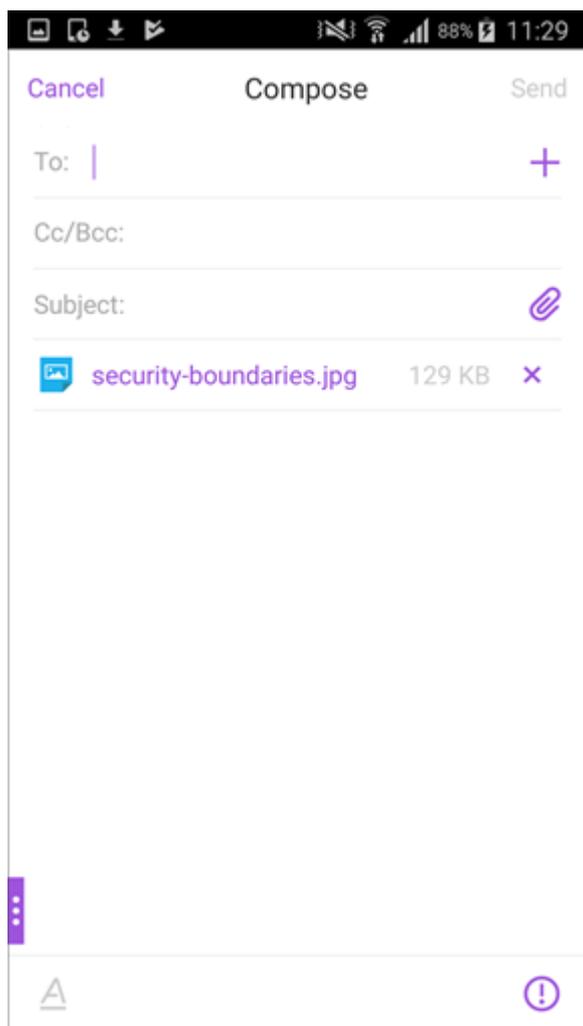
3. Toque no ícone **Anexar**.

É exibida a caixa de entrada.



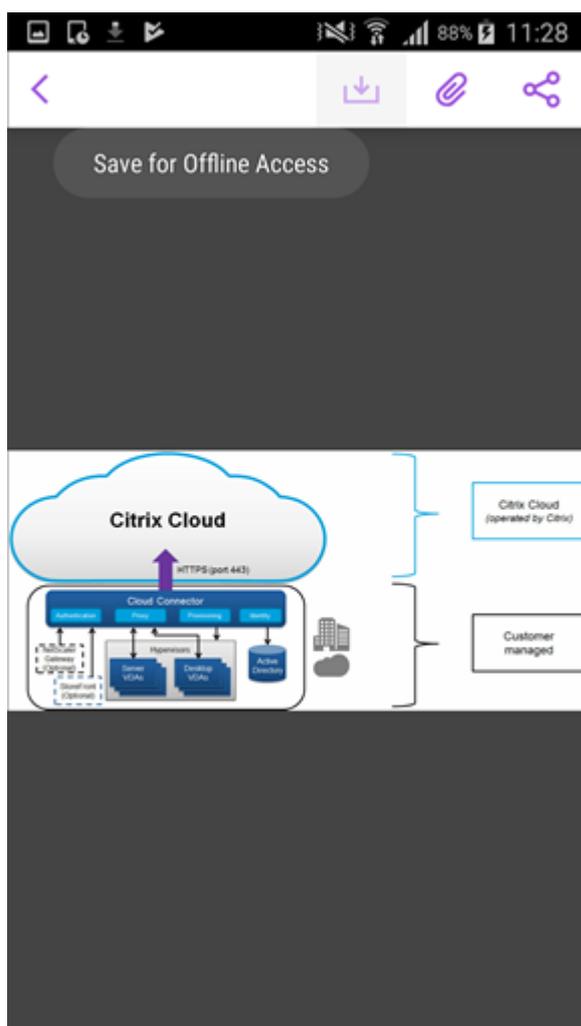
4. Selecione uma mensagem existente à qual anexar esse arquivo ou toque em **Nova mensagem** para anexar esse arquivo a uma nova mensagem.





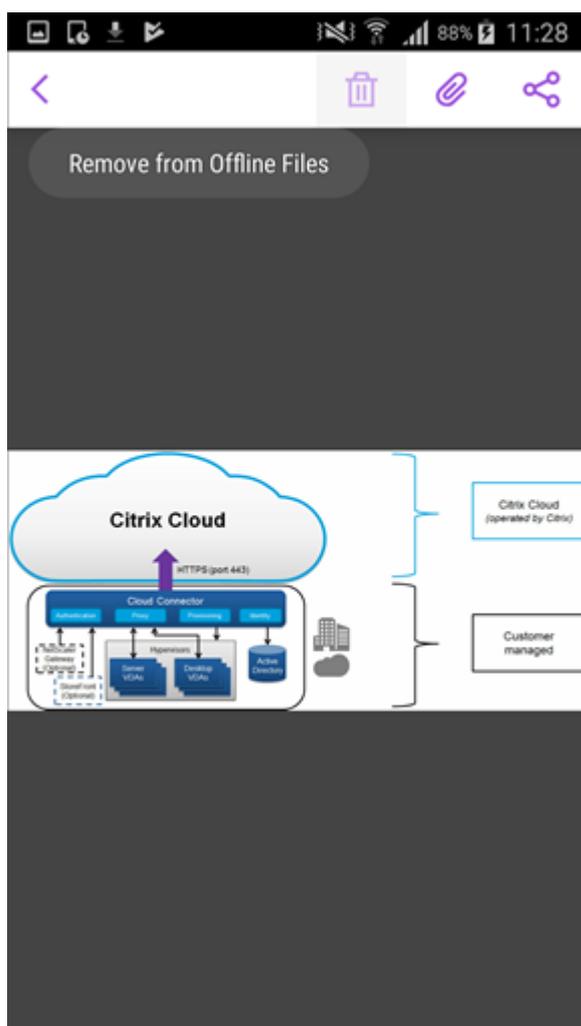
Para salvar o anexo para acesso offline

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



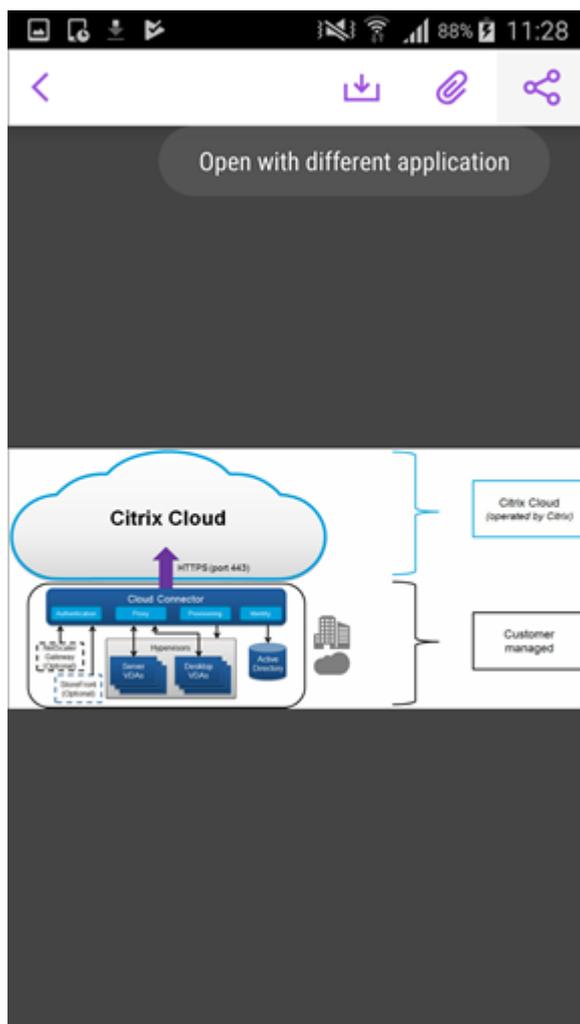
Para excluir o anexo dos arquivos offline

1. Abra o anexo.
2. Toque no ícone **Mais** no canto superior direito da página e toque em **Remover dos arquivos offline** para excluir o anexo dos arquivos offline.

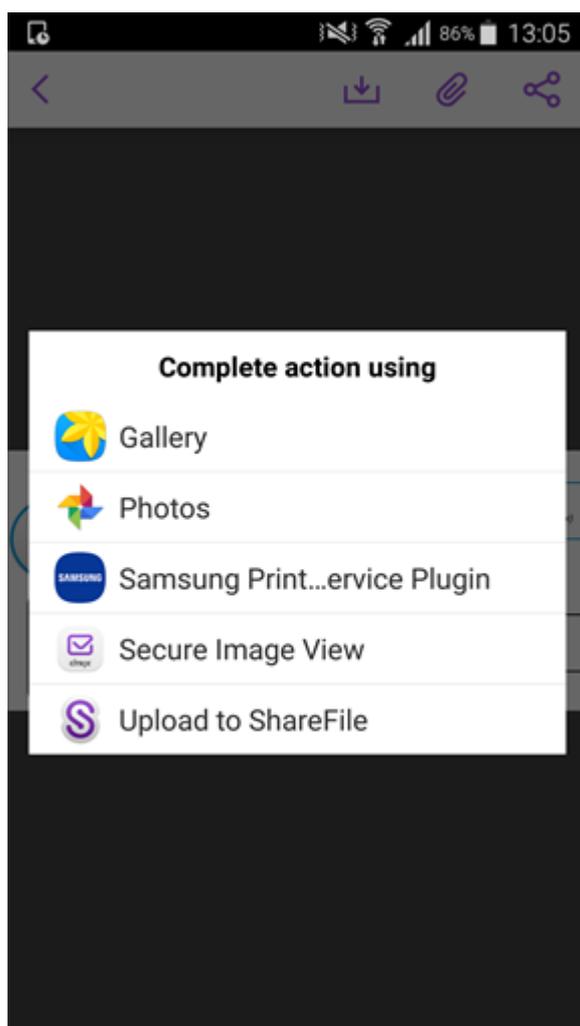


Para abrir o anexo usando outro aplicativo

1. Abra o anexo.
2. Toque no ícone **Mais** no canto superior direito da página e toque em **Abrir com.** para abrir o anexo usando outro aplicativo.

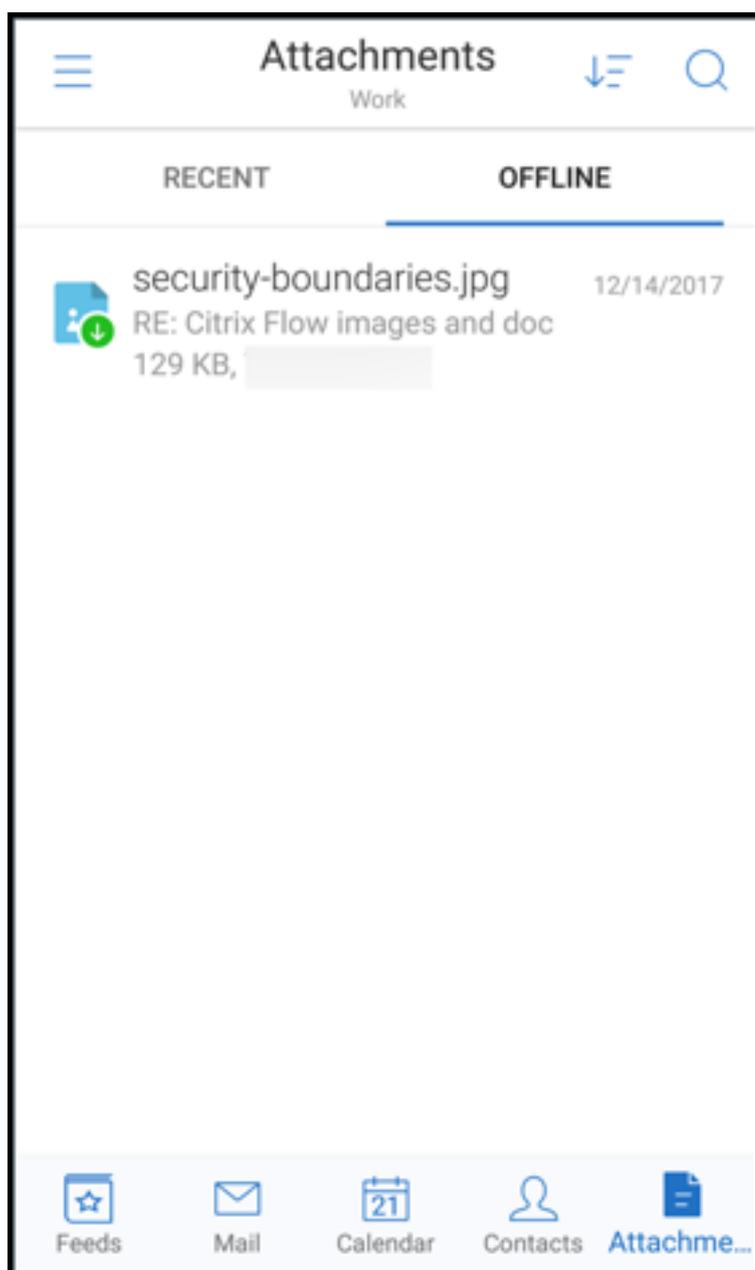


3. Nas opções que aparecem, toque naquele com o qual deseja abrir o anexo.

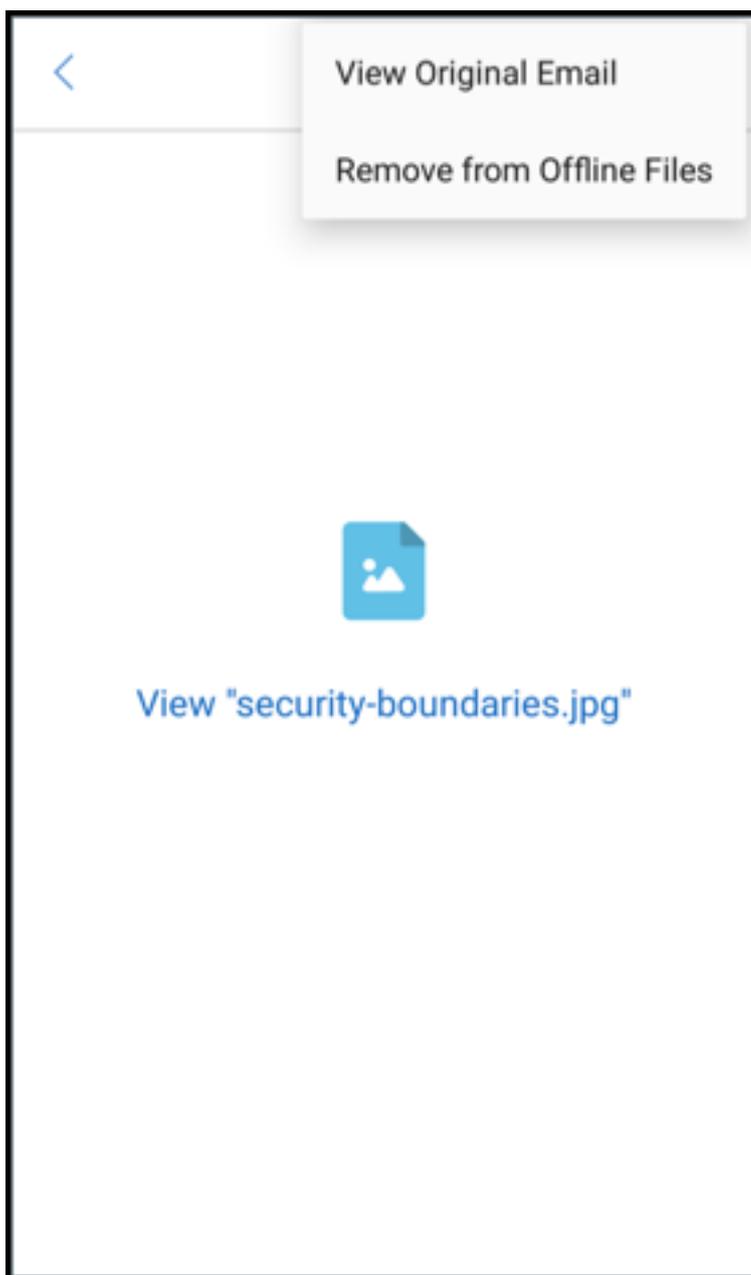


Para exibir o email ou evento de calendário de origem do anexo

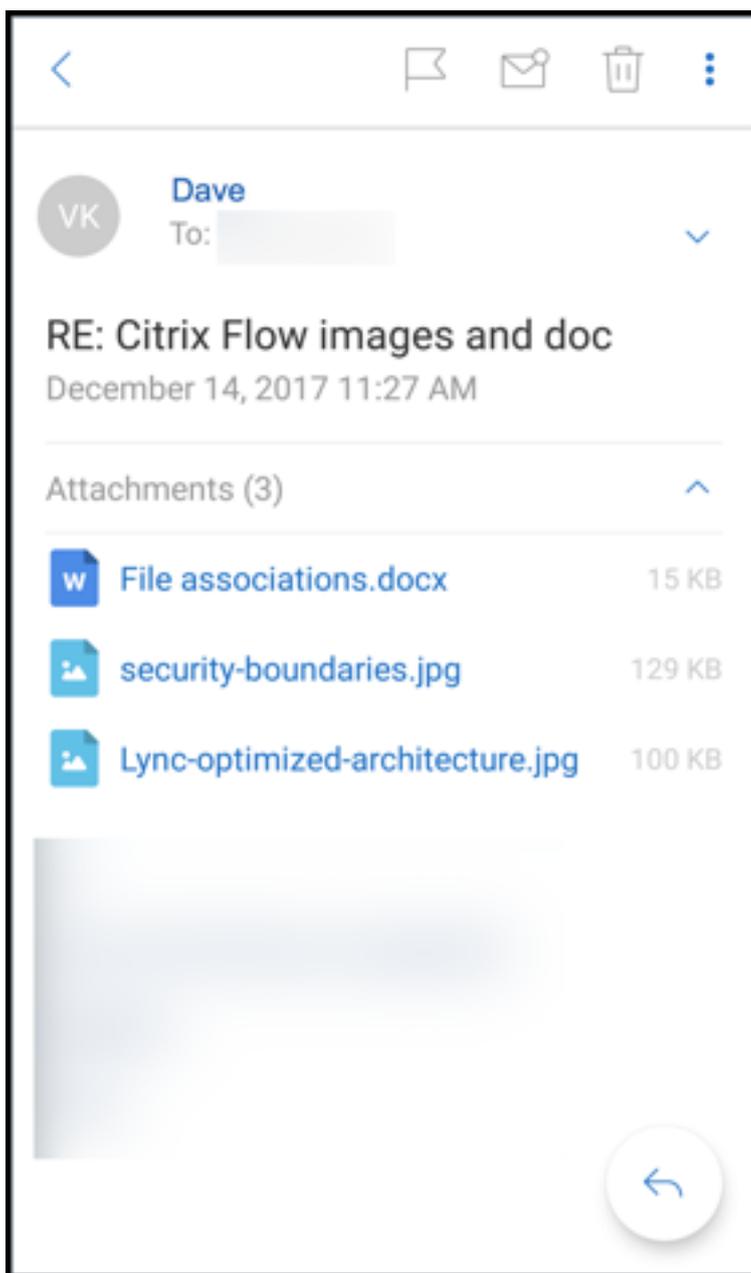
1. Toque no ícone **Anexos** no canto inferior direito da tela.
2. Toque em **OFFLINE**.



3. Toque no anexo e, em seguida, toque no ícone **Mais** no canto superior direito da tela.



4. O email de origem é exibido.



Migração de nomes de usuário (UPN) para endereços de email

No Secure Mail para iOS e Android, você pode migrar de uma autenticação baseada em nome de usuário e senha do Exchange para uma autenticação com base em UPN e senha.

Com esse recurso ativado, você não precisa fazer nenhuma das seguintes coisas:

- Reinstalar o Secure Mail.
- Excluir e adicione a conta no Secure Mail.
- Alterar o nome do usuário no Secure Mail.

Pré-requisitos

Antes de iniciar a migração, verifique se os usuários estão executando o Secure Mail versão 10.7.25 ou posterior.

Para usar esse recurso, você deve ativar a política Falha de On Auth na tentativa de migração de nome de usuário.

Para migrar para autenticação com base em UPN

1. Ative a política Falha de On Auth na tentativa de migração de nome de usuário no Endpoint Management.
2. Migre sua conta de usuário do Exchange para um novo nome UPN que corresponda ao endereço de email SMTP principal do usuário.
Isso causa uma falha na autenticação. O Secure Mail tenta fazer a autenticação usando o endereço de email SMTP principal.

Se a autenticação for bem-sucedida, a conta de usuário será migrada para o UPN atualizado.

Para confirmar a migração

Em dispositivos iOS: vá para **Configurações** e toque na conta para exibir os detalhes. Se a migração for bem-sucedida, o endereço de email SMTP principal será exibido no campo **Nome de usuário** na tela **CONTA**.

Em dispositivos Android: vá para **Configurações** e toque na conta para exibir os detalhes. Se a migração for bem-sucedida, o endereço de email SMTP principal será exibido no campo **Nome de usuário** na tela **Detalhes da conta**.

Listas de distribuição pessoais

Pré-requisitos

- O Exchange Web Services (EWS) está habilitado no seu Exchange Server.
- Microsoft Exchange Server versão 10 SP1 ou posterior.

O Secure Mail para iOS e Android suporta grupos de contato pessoais. Você pode visualizar os grupos de contatos que criou em seu cliente de desktop do Outlook com o Secure Mail. Os grupos de contatos que você criou aparecem nos Contatos no Secure Mail.

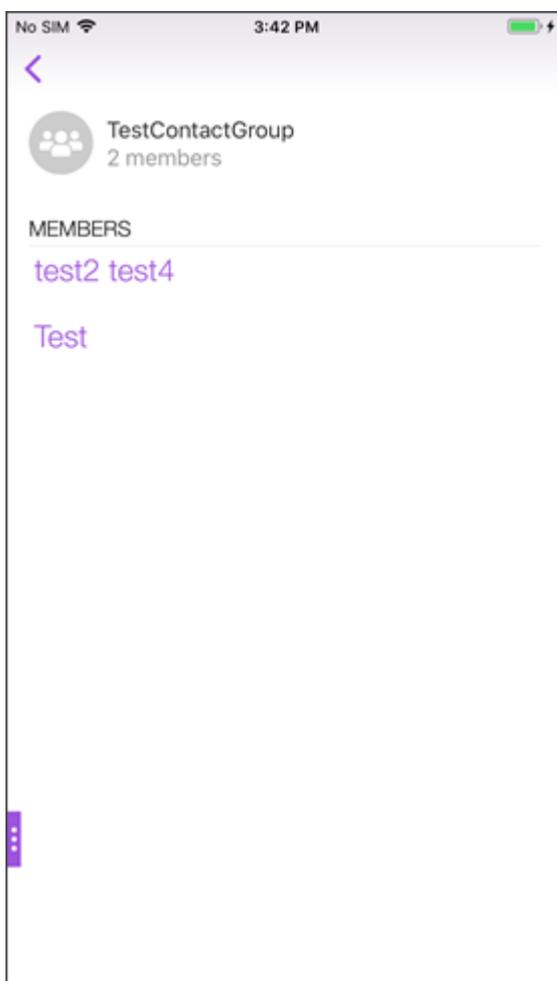
Nota:

Você não pode visualizar membros de um grupo de contatos aninhado no Secure Mail.

Você pode usar listas de distribuição pessoais ao redigir um email ou criar um evento de calendário. Se você tiver criado um grupo contato pessoal (lista de distribuição) usando o Exchange, você pode exibir os grupos no Secure Mail.

Para ver uma lista de distribuição pessoal

1. No Secure Mail, abra **Contatos**.
2. Digite o nome do grupo de contatos.
O grupo aparece no resultado da pesquisa.
3. Toque no grupo de contatos para ver os membros.

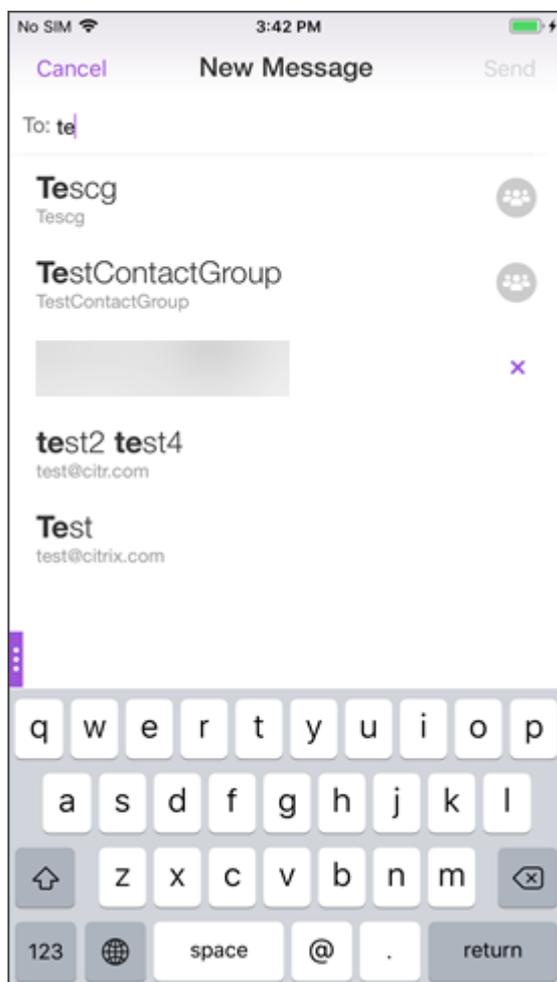


Nota:

Você não pode editar um grupo de contatos no Secure Mail.

Para redigir um e-mail para um grupo de contato

1. Abra o Secure Mail e toque no botão de ação flutuante **Editar** para redigir um e-mail.
2. Na tela **Nova mensagem**, digite o nome do grupo de contatos no campo **Para:**.
3. Na lista de contatos que aparece, selecione o grupo de contatos.

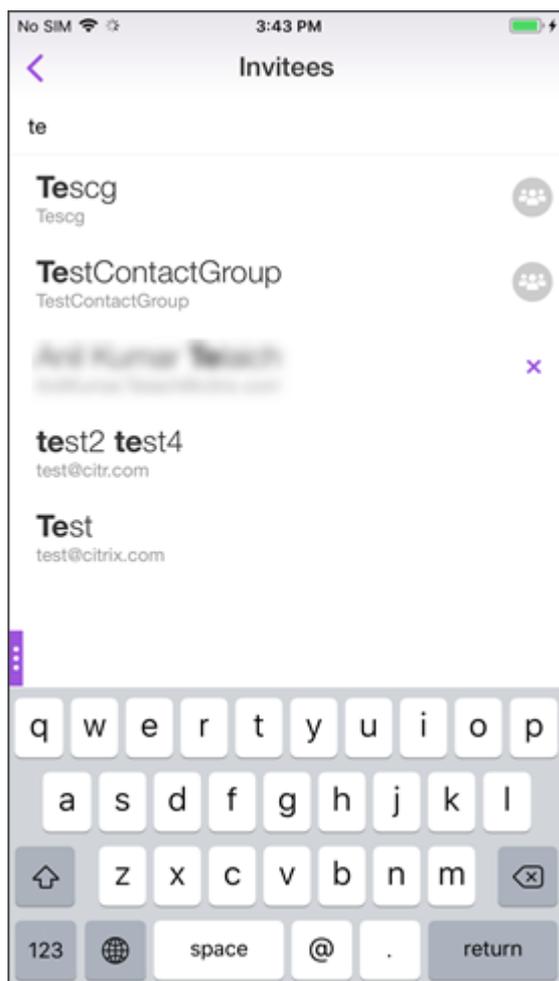


Os grupos de contato são indicados pelo seguinte ícone:



Para enviar um convite de calendário para um grupo de contatos

1. Abra o Secure Mail e navegue até **Calendário**.
2. Toque no ícone **+** para criar um evento de calendário.
3. Na tela **Novo evento**, toque em **Convidados** para adicionar membros.
4. Digite o nome do grupo de contato para enviar o convite para o grupo.



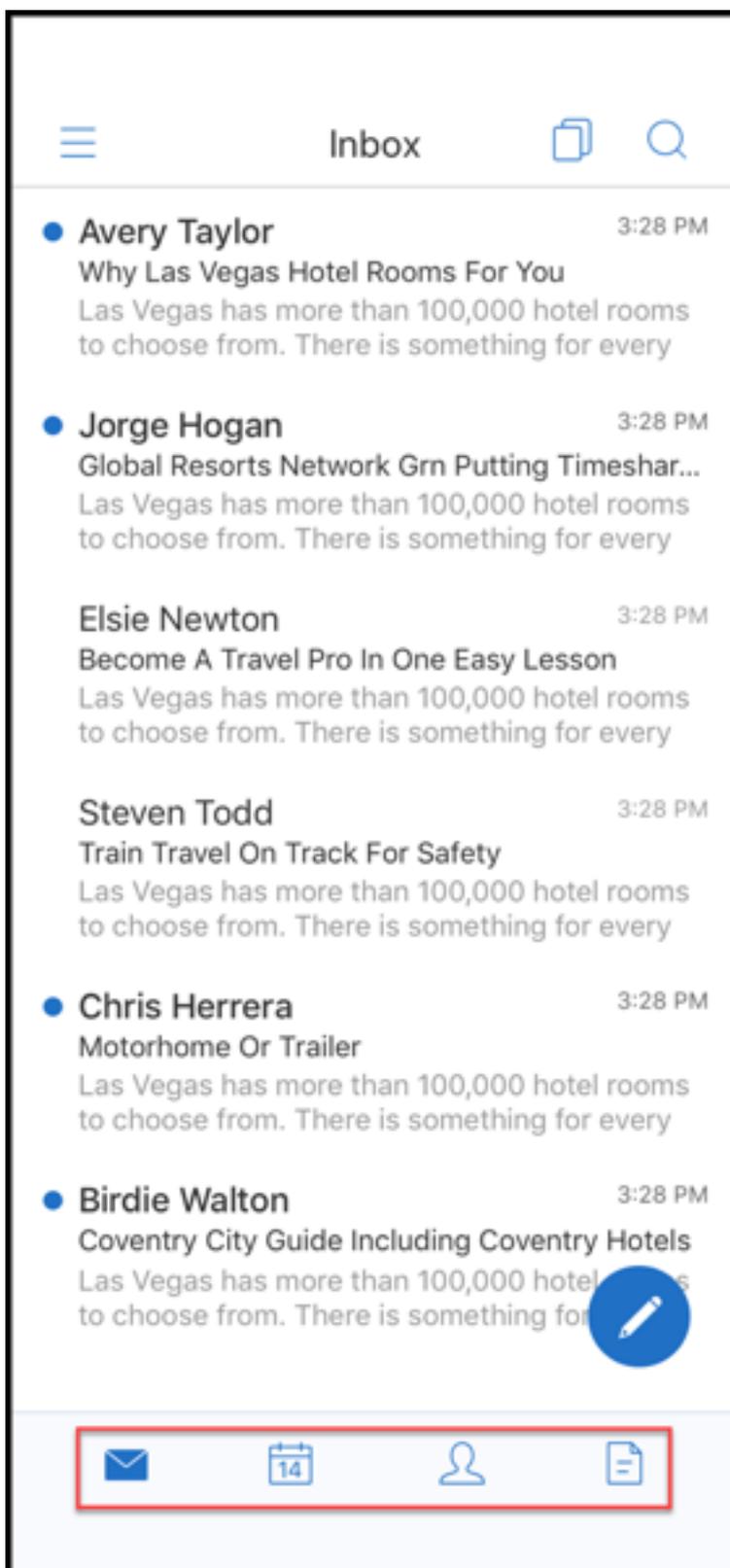
5. Na lista de contatos que aparece, selecione o grupo de contatos.

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**.

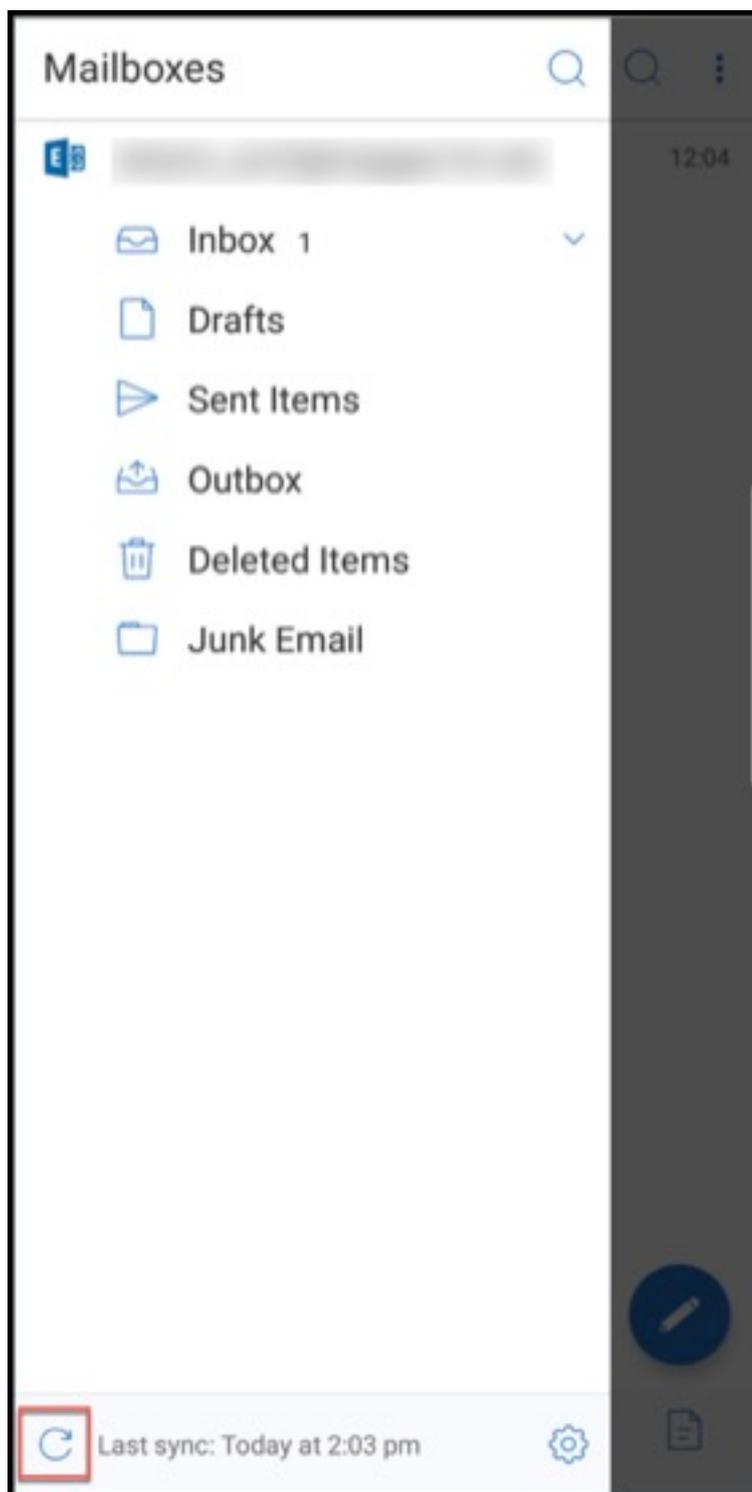
Para sincronizar suas pastas

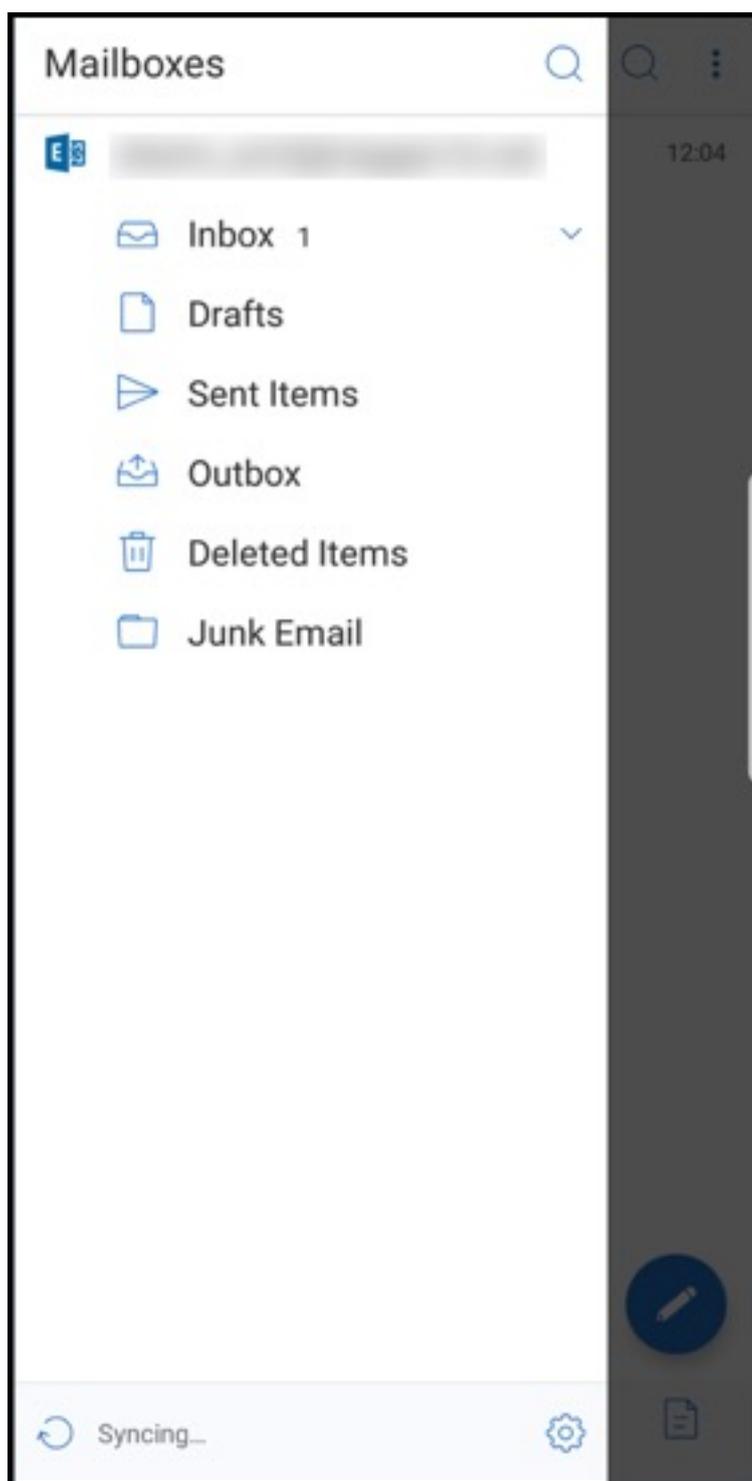
1. Abra o Secure Mail.
2. Nas pastas disponíveis na barra de guias do rodapé, toque na pasta que você deseja sincronizar.



3. Toque no ícone de hambúrguer no canto superior esquerdo da tela.

4. Toque no ícone **Sincronizar** na parte inferior esquerda da tela.





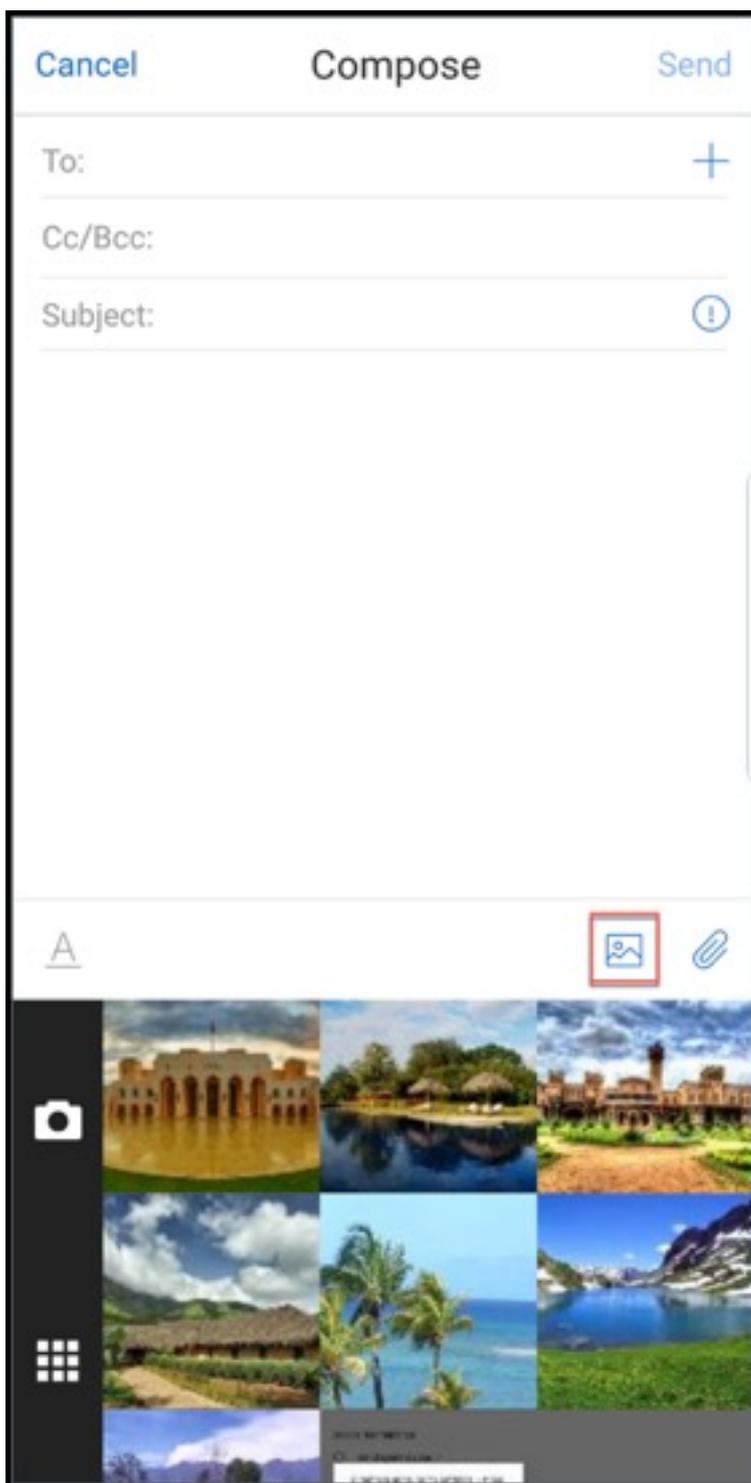
5. A pasta é sincronizada e seu conteúdo é atualizado. O carimbo de data/hora aparece ao lado do ícone **Sincronizar**.

Melhorias no anexo de fotos

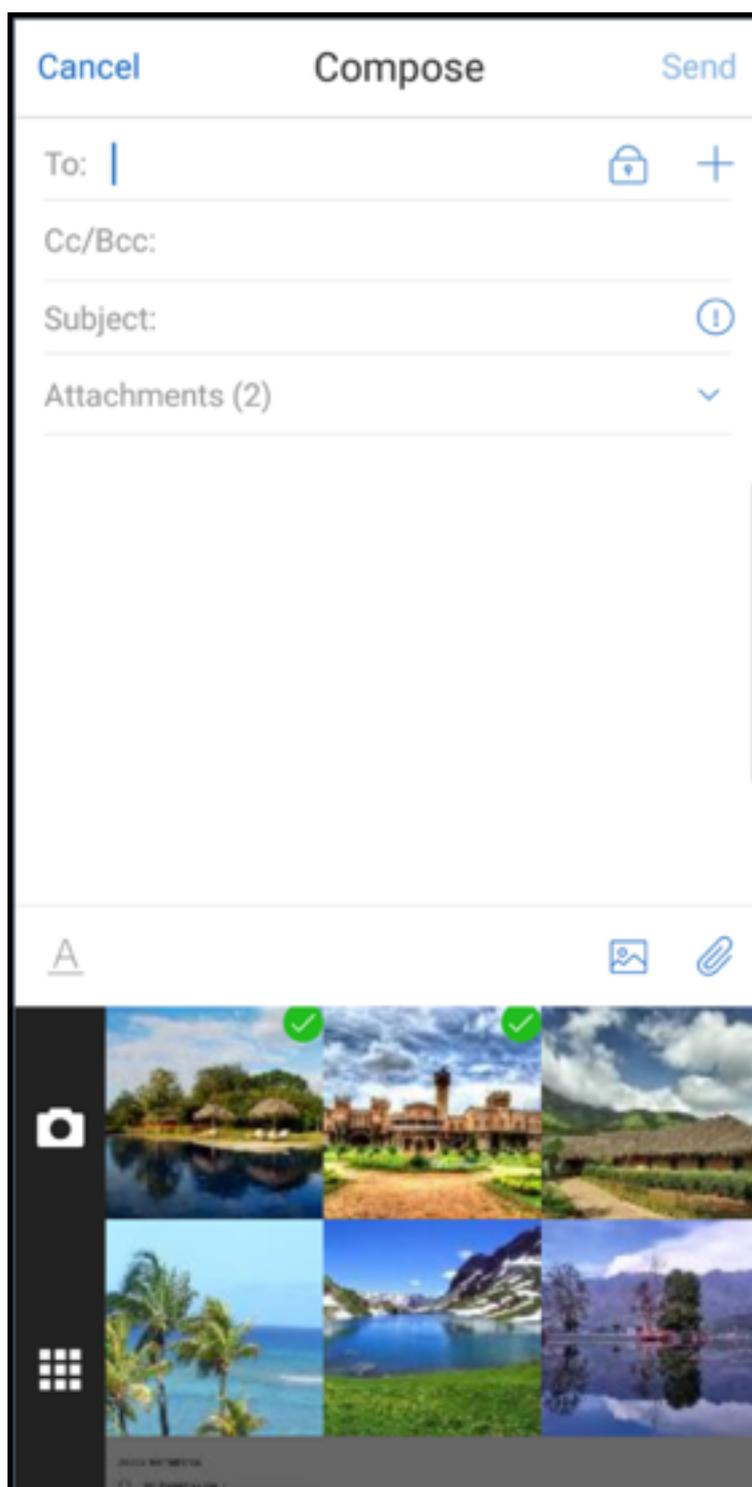
No Secure Mail para iOS e Android, você pode anexar fotos facilmente tocando no novo ícone da **Galeria**.

Para anexar fotos ao seu email

1. Abra o Secure Mail.
2. Toque em **Redigir** para criar um novo e-mail ou toque no botão flutuante de ação **Responder** para responder a um e-mail.
3. Toque no ícone **Galeria** ao lado do ícone **Anexos** no canto inferior direito da tela.



4. Sua galeria aparece na parte inferior da tela, juntamente com os ícones **Câmera** e **Recente**.
5. Navegue e selecione as imagens na sua galeria que você deseja anexar ou toque no ícone **Câmera** para tirar uma foto.

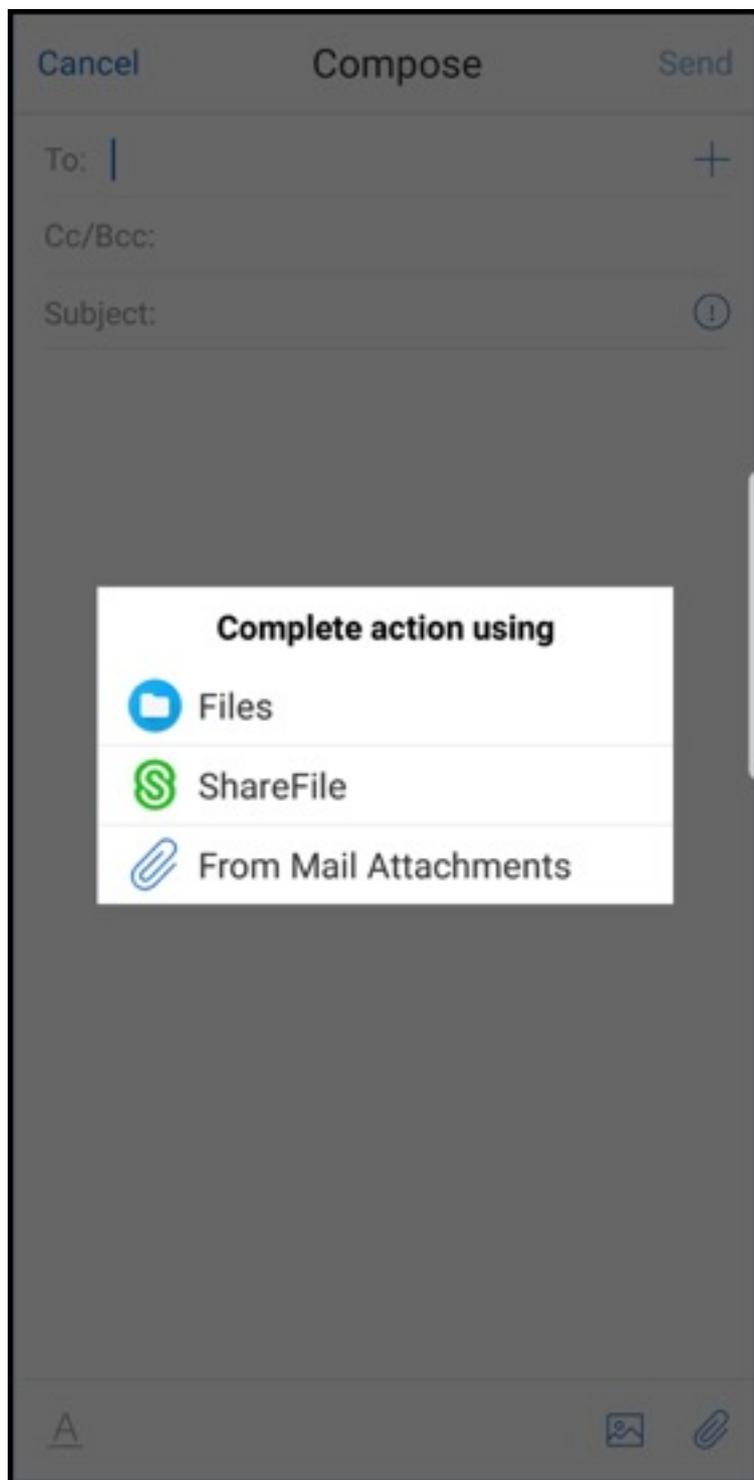


Nota:

Quando você toca no ícone **Anexos**, as seguintes opções aparecem:

- Arquivos

- ShareFile (agora, Citrix Files)
- Anexos de email



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.

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).

Política de MDX Permitir domínios do Secure Web para Secure Mail

No Secure Mail, algumas URLs externas devem ser abertas em um navegador nativo e não no Secure Web. Como resultado, por padrão, todas as URLs são abertas em um navegador nativo. No entanto, você pode criar uma lista das URLs que deseja abrir especificamente no Secure Web. Para isso, você configura uma política de MDX no console do Citrix Endpoint Management chamada Domínios do Secure Web permitidos.

Após implementar a política, os domínios de host de URL, apresentados em lista e separados por vírgulas, são comparados com a parte de nome de host de qualquer URL que o aplicativo normalmente envia a um manipulador externo. Normalmente, você configura essa política como uma lista de domínios internos para que o Secure Web manipule.

Se você deixar a política em branco, que é a configuração padrão, todo o tráfego da web será enviado para o Secure Web até que você exclua explicitamente as URLs da filtragem ou redirecione as URLs. Para redirecionar as URLs, configure o filtro Excluir URL para a política de MDX de domínios. Esta política indica as URLs que devem ser abertas no navegador nativo. Essa política tem prioridade sobre a política de domínios do Secure Web.

Você pode configurar essas políticas de MDX para Android e iOS.

Exemplo de configuração da política de domínios do Secure Web

Os procedimentos a seguir mostram como solicitar aos usuários com Secure Mail para Android que abram URLs no navegador nativo Chrome ou no Secure Web. No iOS, as etapas mostram que URLs que normalmente abririam em um navegador Safari abrem automaticamente no Secure Web.

Para Secure Mail para Android

1. Na lista de políticas de Interação de aplicativos, em Lista restrita de exceção de Abrir em, digite `{package=com.android.chrome}`.

2. Na lista de políticas de Interação de aplicativos (URL de saída), em **Permitir domínios do Secure Web**, adicione o sufixo DNS do site interno.

Para outros navegadores de terceiros, use o seguinte formato, conforme necessário:

```
{ package=<packageID of the browser> }
```

Para Secure Mail para iOS

1. Na lista de políticas de Interação de aplicativos (URL de saída), em **URLs permitidas**, adicione *+^safari:*
2. Em **Esquemas de URL de aplicativo**, adicione *safari:*
3. Em **Permitir domínios do Secure Web**, adicione o sufixo DNS do site interno.

Integração do Secure Mail com Slack

November 17, 2021

Citrix Secure Mail and its integration with Slack is not created by, affiliated with, or supported by Slack Technologies, Inc.

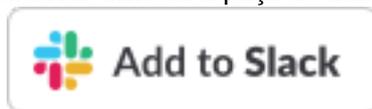
Agora você pode levar sua conversa por e-mail para o aplicativo Slack em dispositivos com iOS ou Android.

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.

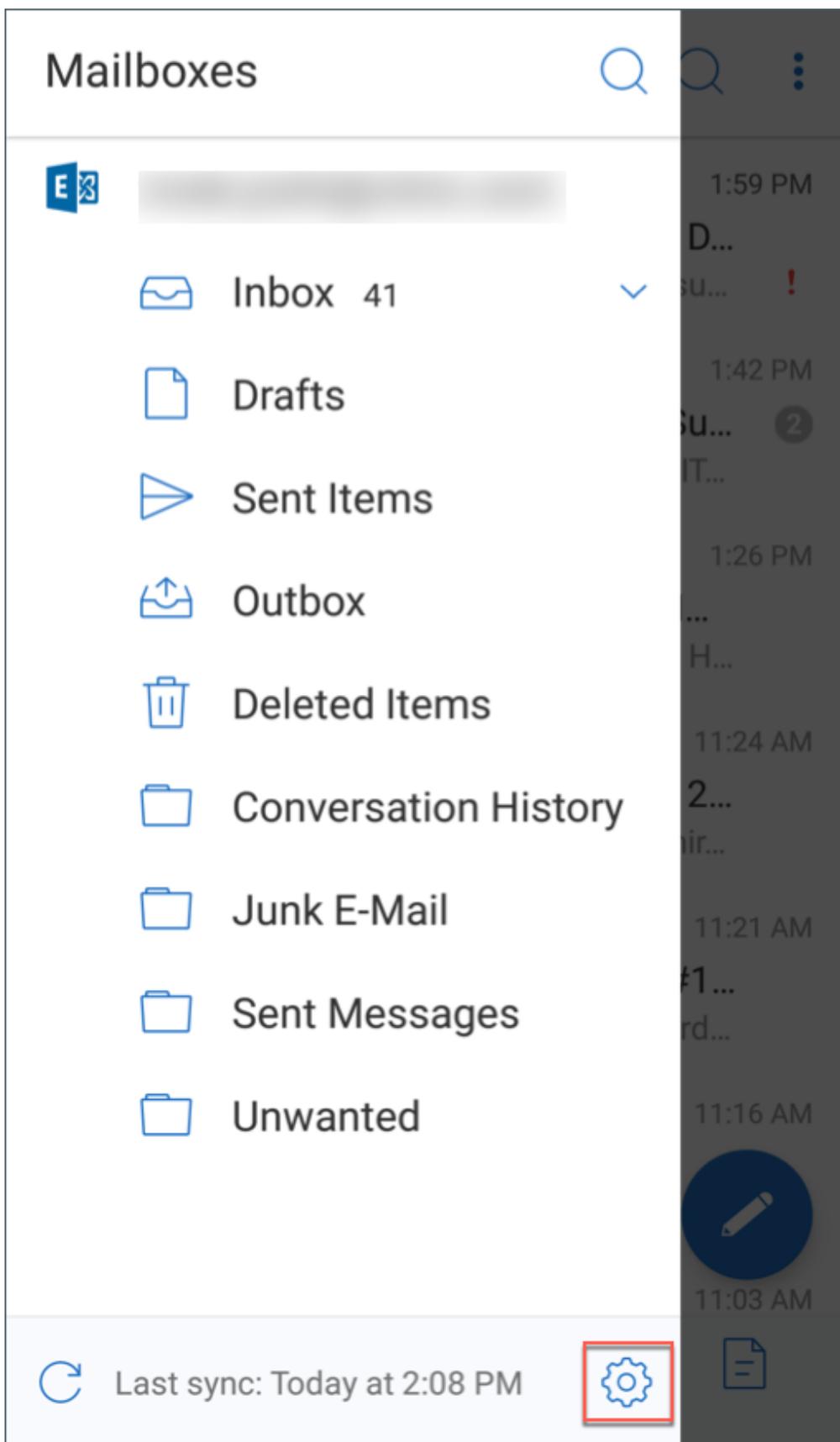
Pré-requisitos

- 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.

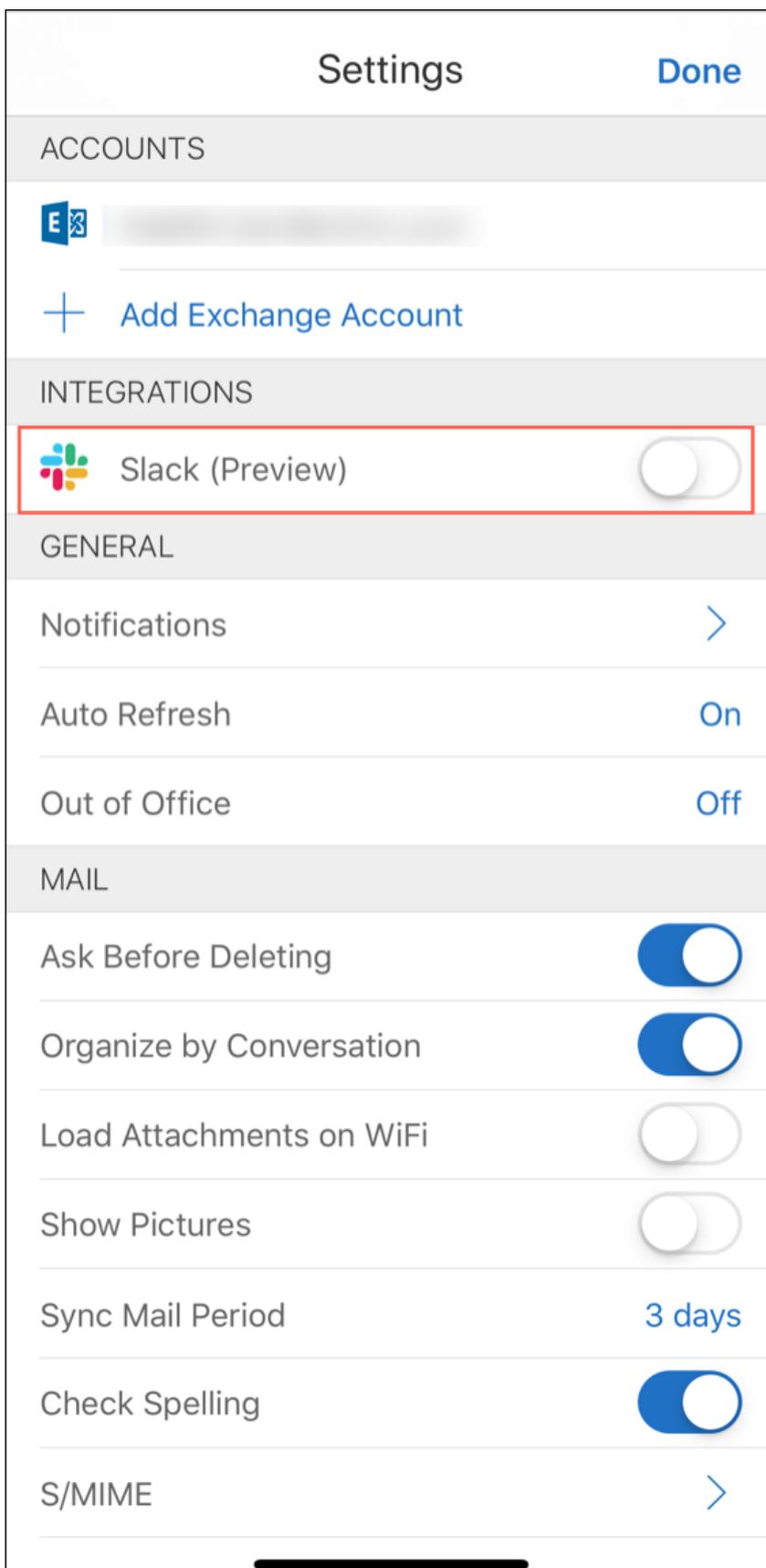


Para ativar esse recurso no seu dispositivo

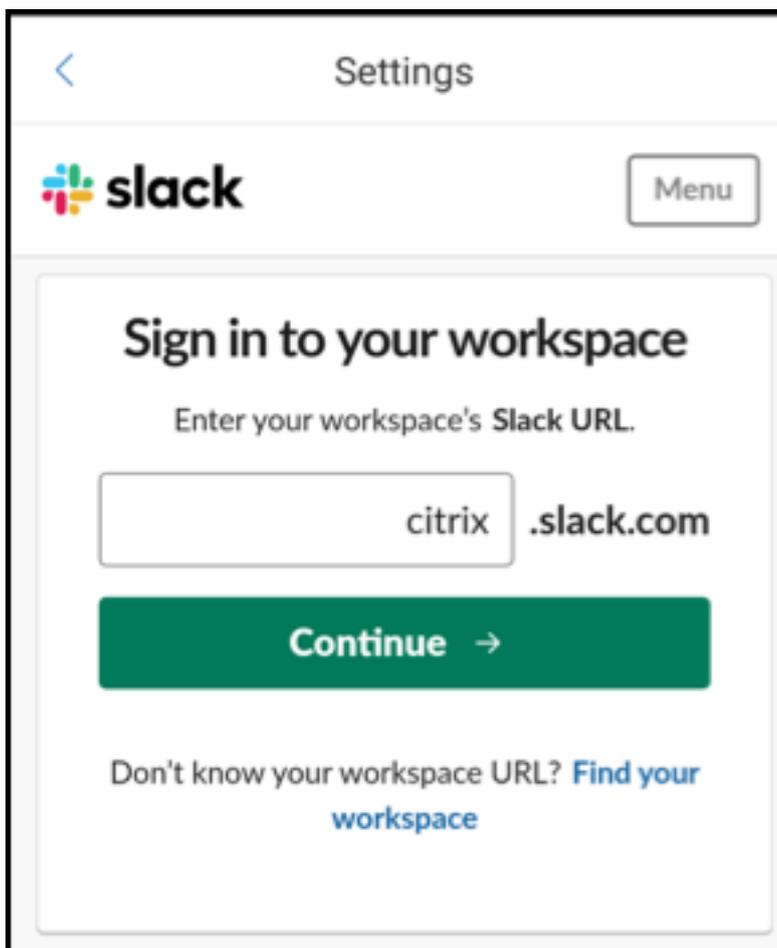
1. Abra o Secure Mail e toque no ícone de hambúrguer.
2. Na tela **Caixas de correio**, toque no ícone de configurações na parte inferior direita da tela.



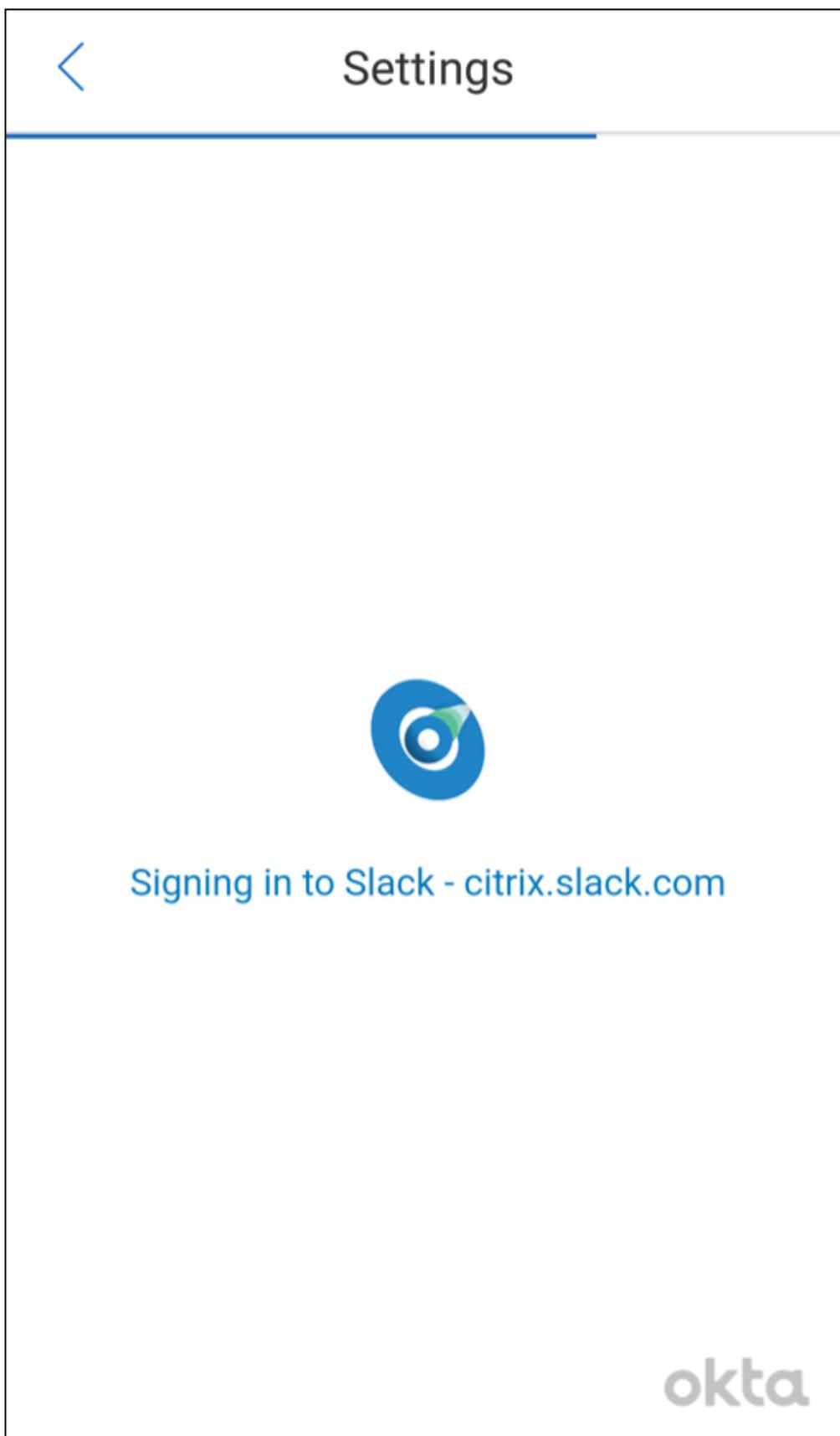
3. Na tela **Configurações**, toque em **Slack**, em **Integrações**.



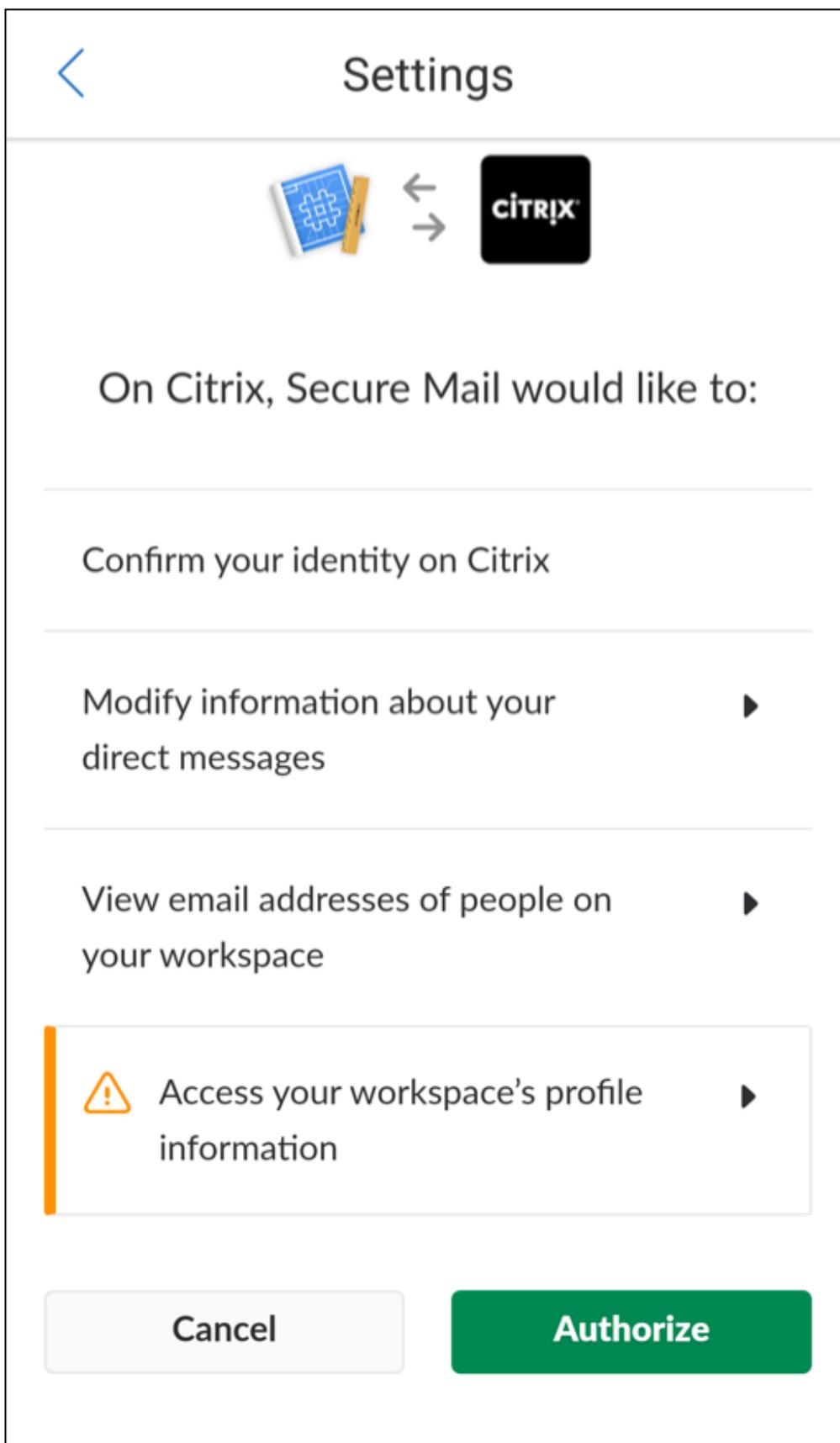
4. Forneça sua URL do espaço de trabalho do Slack e toque em **Continuar**.



5. Forneça suas credenciais e toque em **Fazer logon**.



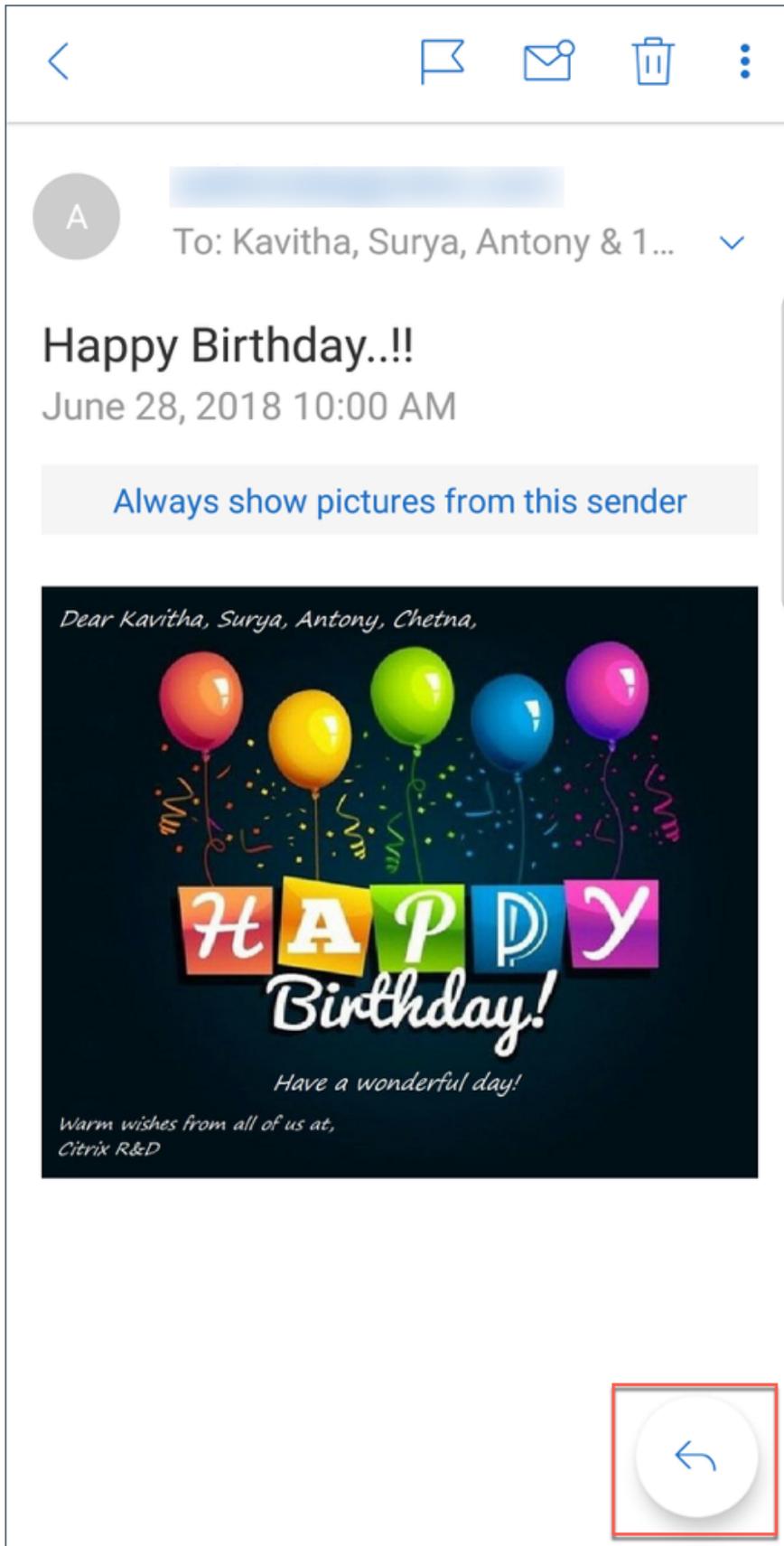
6. Quando solicitado a autorizar o acesso do Secure Mail às informações, toque em **Autorizar**.



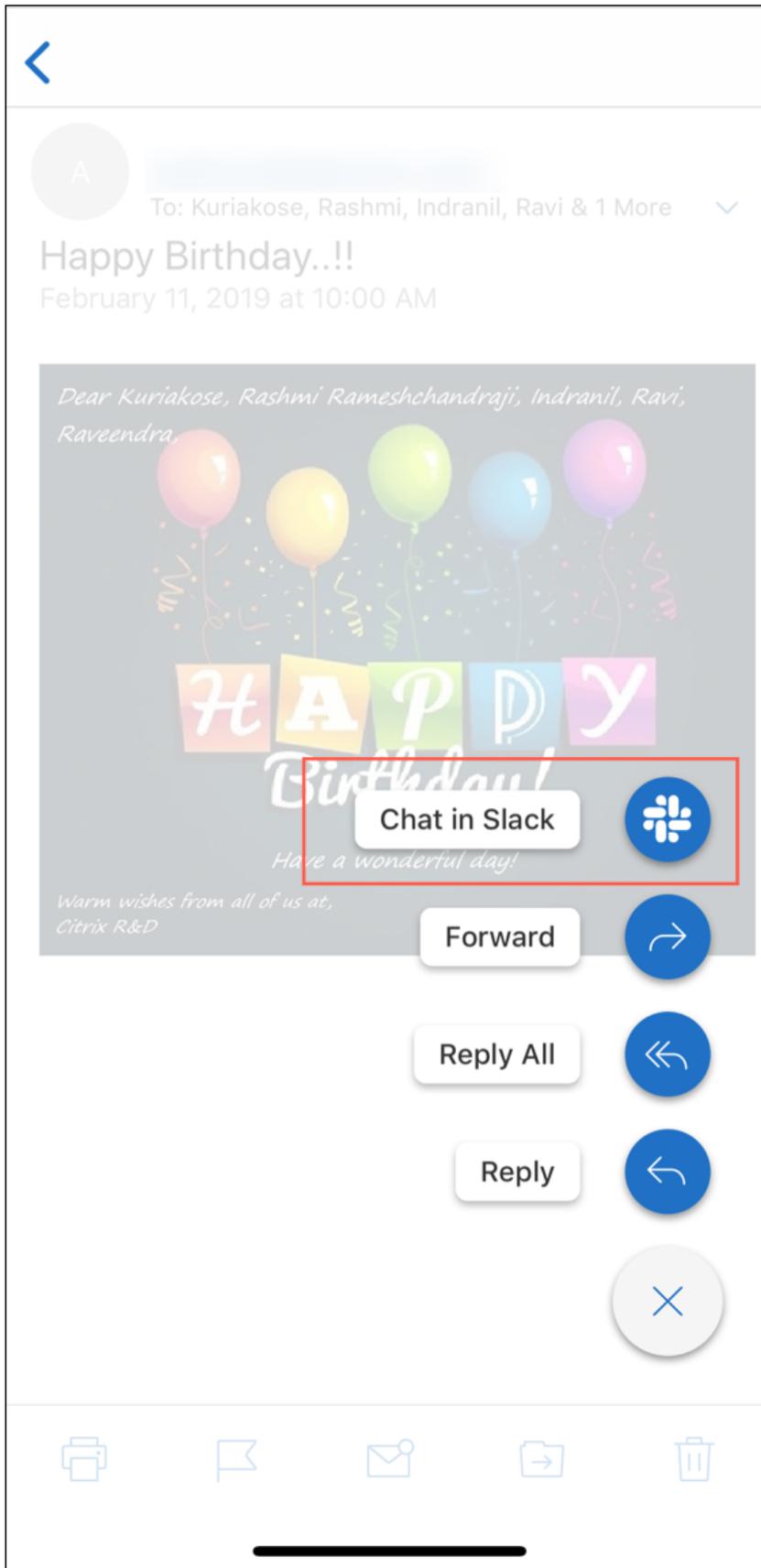
Agora você está conectado ao Slack.

Para usar este recurso

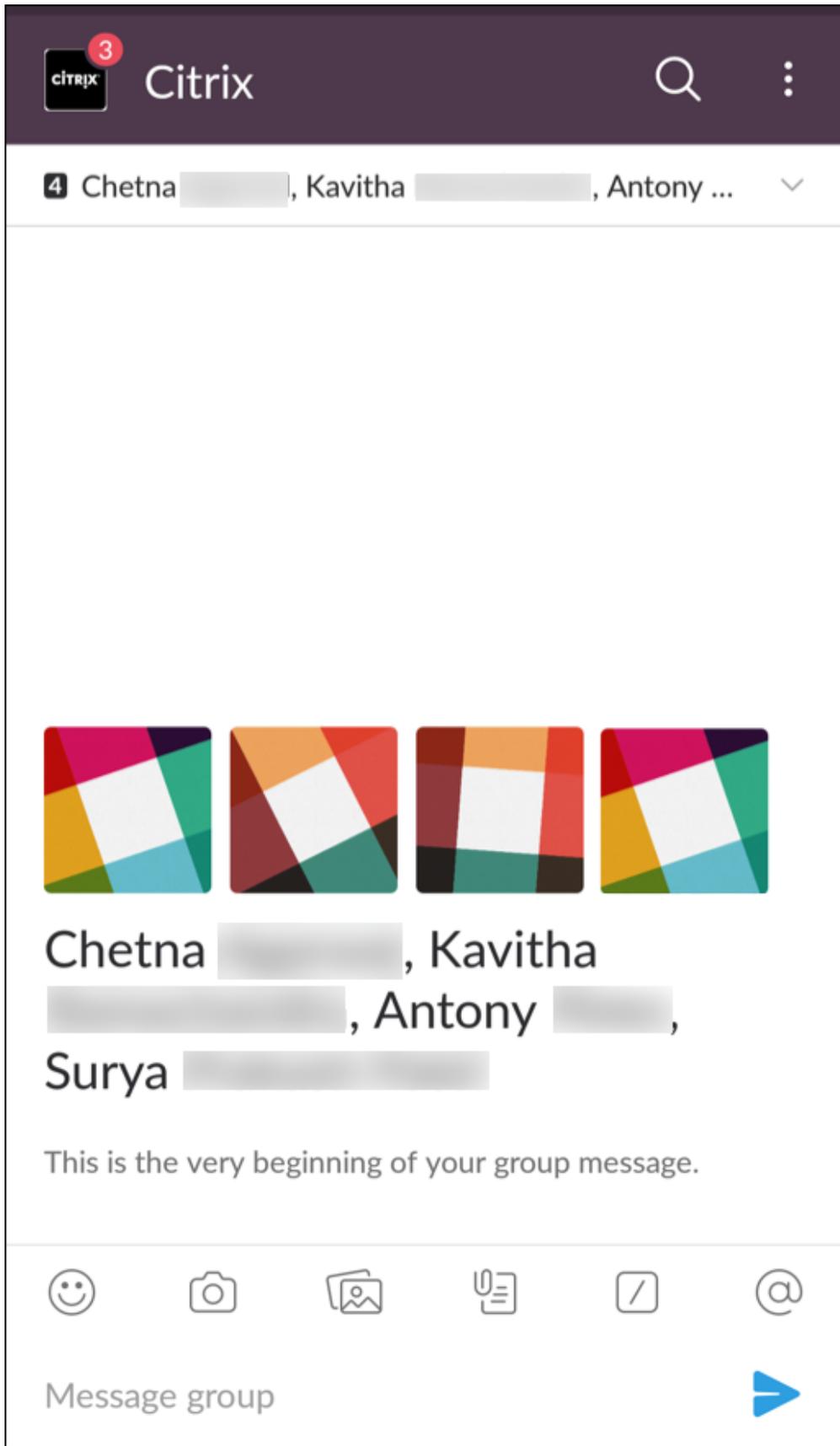
1. Abra qualquer conversa de email no Secure Mail e, em seguida, toque no botão de ação flutuante.



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

December 9, 2021

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 Management como **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 definida como **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** esteja definido como **I**, as atualizações a contatos no Exchange ou Secure Mail disparam 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. Os contatos podem ser exportados e sincronizados mesmo que os usuários tenham o Hotmail ou o Exchange configurado 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 substitui a verificação de contatos de uma conta do Exchange/Hotmail configurada

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**.

Limitação:

Quando você habilita **Sync with local contacts**, somente a pasta de contatos padrão é sincronizada. As subpastas que você possa ter não são incluídas nos contatos sincronizados.

Notificações do Secure Mail

A tabela a seguir lista 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 obter detalhes de configuração, consulte [Notificações por Push para o Secure Mail para iOS](#).

Notificações por Push para o Secure Mail

December 9, 2021

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 Notificações por push remotas 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

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)

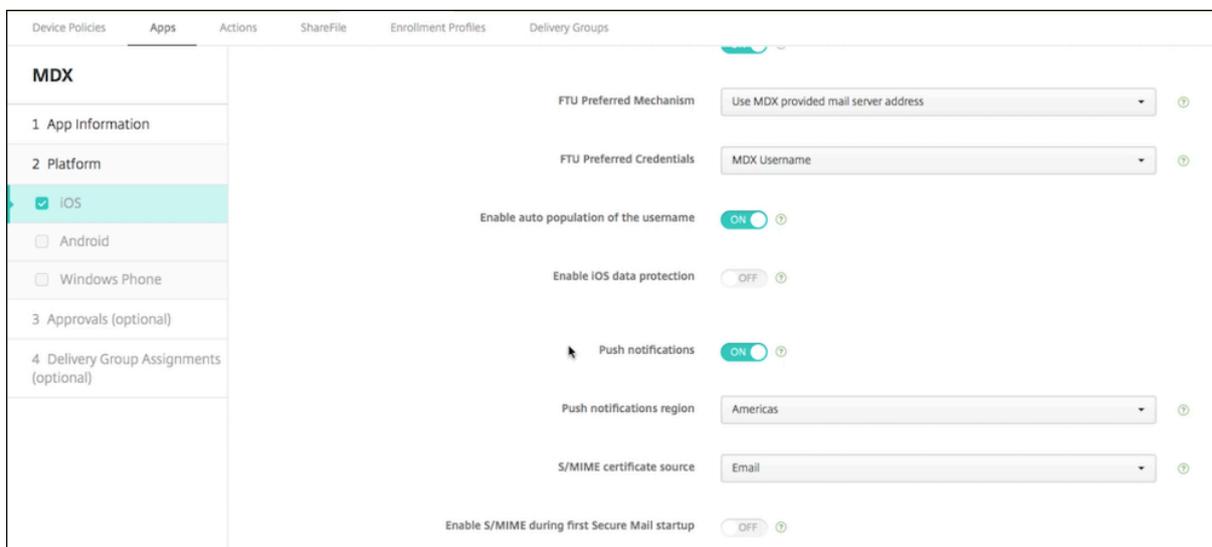
Requisitos do sistema para notificações por push

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:

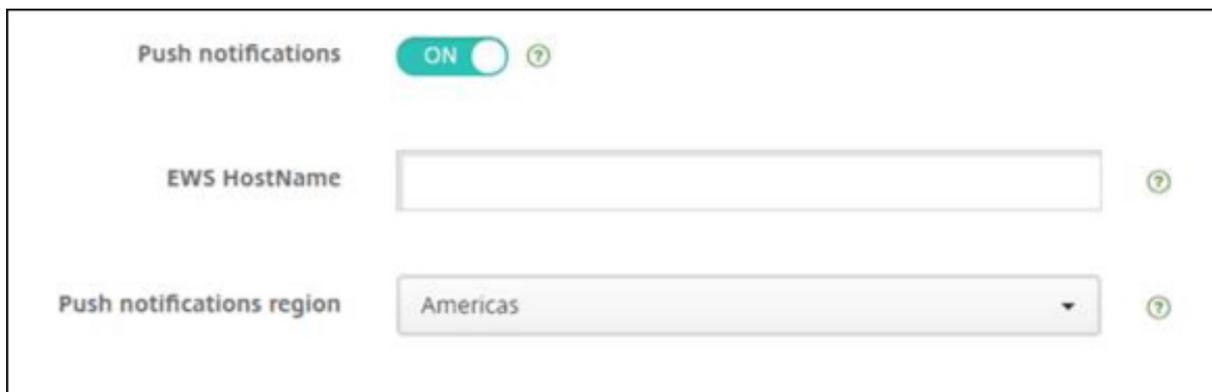
Região	URL	Endereço IP
Américas	https://us-east-1.pushreg.xm.citrix.com	52.7.65.6; 52.7.147.0
EMEA	https://eu-west-1.pushreg.xm.citrix.com	54.154.200.233; 54.154.204.192
ÁSIA-PACÍFICO	https://ap-southeast-1.pushreg.xm.citrix.com	52.74.236.173; 52.74.25.245

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.xml.citrix.com	52.6.252.176; 52.4.180.132
EMEA	https://eu-west-1.mailboxlistener.xml.citrix.com	54.77.174.172; 52.17.147.220
ÁSIA-PACÍFICO	https://ap-southeast-1.mailboxlistener.xml.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.

```
1 <configuration>
2 <system.net>
3 <defaultProxy>
4 <proxy usesystemdefault="true" bypassonlocal="true" />
5 </defaultProxy>
6 </system.net>
7 </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 o 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. Para obter mais informações sobre a integração do Citrix Endpoint Management com o Citrix Gateway, consulte a seção [Integração com Citrix Gateway e Citrix ADC](#).

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, use o [Endpoint Management Analyzer](#).

Perguntas frequentes de notificação por push do Secure Mail

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.

Nota:

Essa situação ocorre somente se as notificações por push em rich text estiverem desativadas. Para obter mais informações sobre notificações por push em Rich Text, consulte [Notificações por Push em rich text para o Secure Mail para iOS](#).

- 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 de tela de bloqueio não aparecem.

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 roteia 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. Como tal, pode decorrer algum tempo entre estas duas situações:

- Quando um email chega à caixa de entrada de um usuário no Exchange.

- Quando o Secure Mail sincroniza a mensagem 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 importante, que pode causar confusão, é que o Secure Mail nem sempre mostra novos e-mails em tempo real na tela de bloqueio. Esse comportamento difere do Gmail, Microsoft Outlook e de outros aplicativos. O principal motivo dessa diferença é a segurança. Para se alinhar com o comportamento dos outros aplicativos, o serviço de ouvinte da Citrix requer que as credenciais do usuário sejam autenticadas com o Exchange. As credenciais são necessárias para obter o conteúdo do e-mail. As credenciais também são necessárias para transmitir esse conteúdo de e-mail através do serviço de ouvinte da Citrix e para o serviço 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. Esse comportamento 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 em dados fornecidos pela Microsoft na notificação de APNs. A razão é que o Outlook para iOS faz uso de um modelo no qual a Microsoft armazena as credenciais de 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 novos dados de email. Esse modelo opera de forma semelhante ao modelo do Gmail. No modelo do Gmail, o iOS simplesmente usa os dados para gerar uma notificação de tela de bloqueio com base nesses 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 precisam confiar à Microsoft as senhas de seus usuários. Essa confiança permite que a Microsoft acesse a caixa de correio do usuário, o que representa um risco de segurança.

Para mais perguntas frequentes específicas aos administradores sobre notificações por push, consulte este [artigo de suporte do Knowledge Center](#). Para mais perguntas frequentes específicas ao usuário, consulte este [artigo de suporte do Knowledge Center](#).

Notificações por Push em rich text para o Secure Mail para iOS

December 9, 2021

O Secure Mail para iOS dá suporte a notificações por push em rich text. As notificações em rich text garantem que você receba notificações da tela de bloqueio na 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
- Aplicativos gerenciados pela integração do Endpoint Management com o Microsoft InTune/EMS
- Dispositivos registrados por meio de credenciais derivadas

Como as notificações por push funcionam no Secure Mail iOS

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

- **Novos emails, solicitações de reuniões, cancelamentos de reuniões, atualizações de reuniões:** quando os APNs enviam notificações remotas para o iOS Secure Mail e o Secure Mail atualiza todas as pastas marcadas para atualização automática.

Nota:

Por padrão, as pastas Caixa de entrada, Calendário e Contato são marcadas para atualização automática. Os usuários podem selecionar qualquer outra pasta de email para atualização automática em **Secure Mail > Configurações > Atualização automática**.

- 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.
- 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.

Comportamento de notificações por push sem suporte a notificações por push em rich text

Para configurações que não são suportadas pelo recurso de notificações por push em rich text para iOS, o Secure Mail ainda fornece a contagem de e-mails não lidos da Caixa de entrada para o 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.

Perguntas frequentes de notificações por push do Secure Mail iOS

Quando o iOS fornece notificações para Secure Mail

Quando o recurso de notificação por push em rich text está habilitado, o iOS entrega notificações remotas ao Secure Mail. Essas notificações acontecem mesmo que o aplicativo não esteja sendo executado em segundo plano ou esteja no modo de baixo consumo de energia.

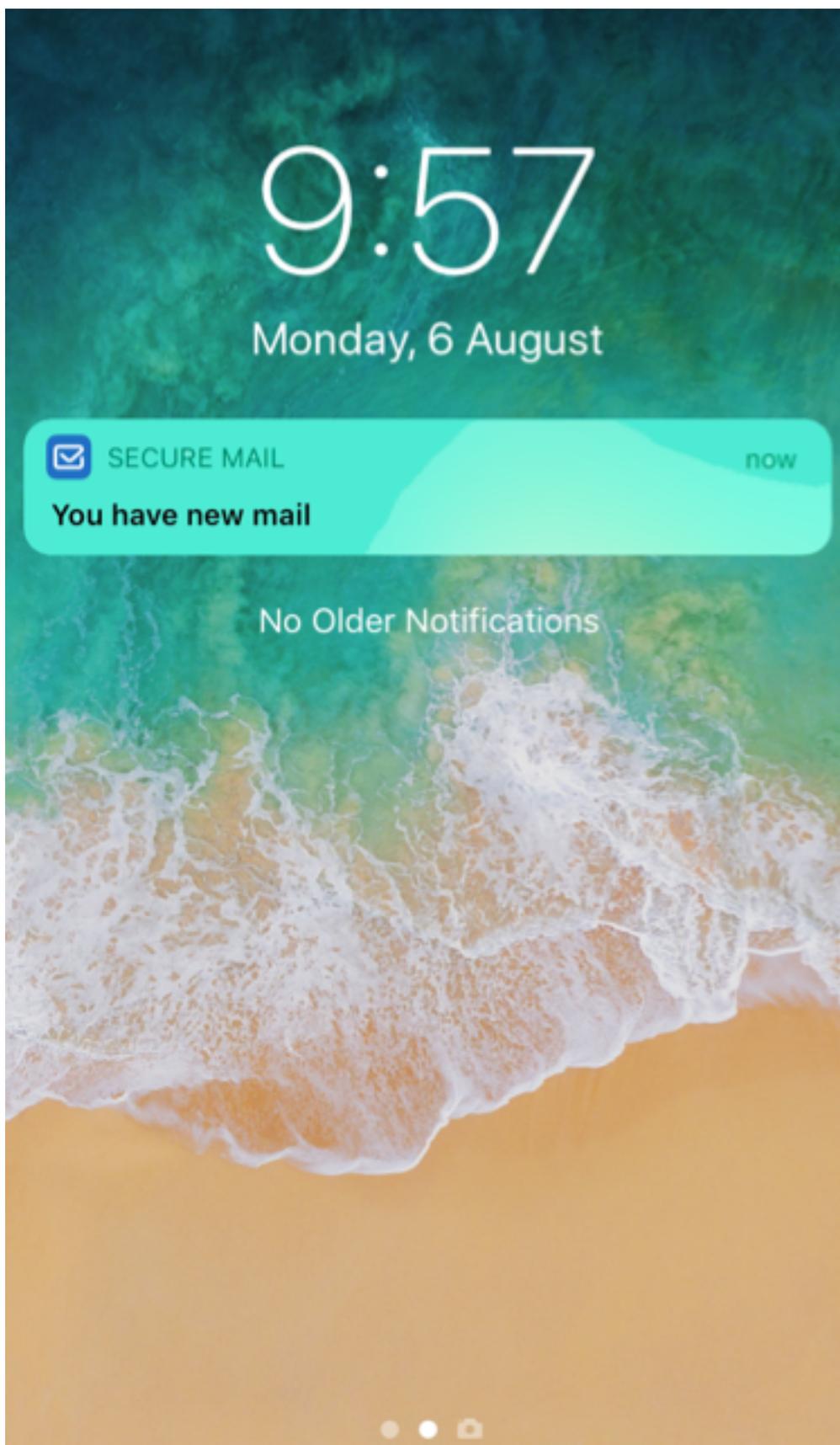
Nota:

Quando as notificações por push em rich text não estão habilitadas, as notificações podem não ser entregues ao Secure Mail quando o Secure Mail não está ativo. Essa situação ocorre por vários motivos, como os seguintes motivos:

- Se o dispositivo estiver no modo de baixo consumo de energia e o Secure Mail estiver em segundo plano: este é o caso mais comum em que as notificações não são 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 essa configuração.
- Se o dispositivo tiver conectividade de rede insatisfatória: esta situação depende do dispositivo iOS.

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

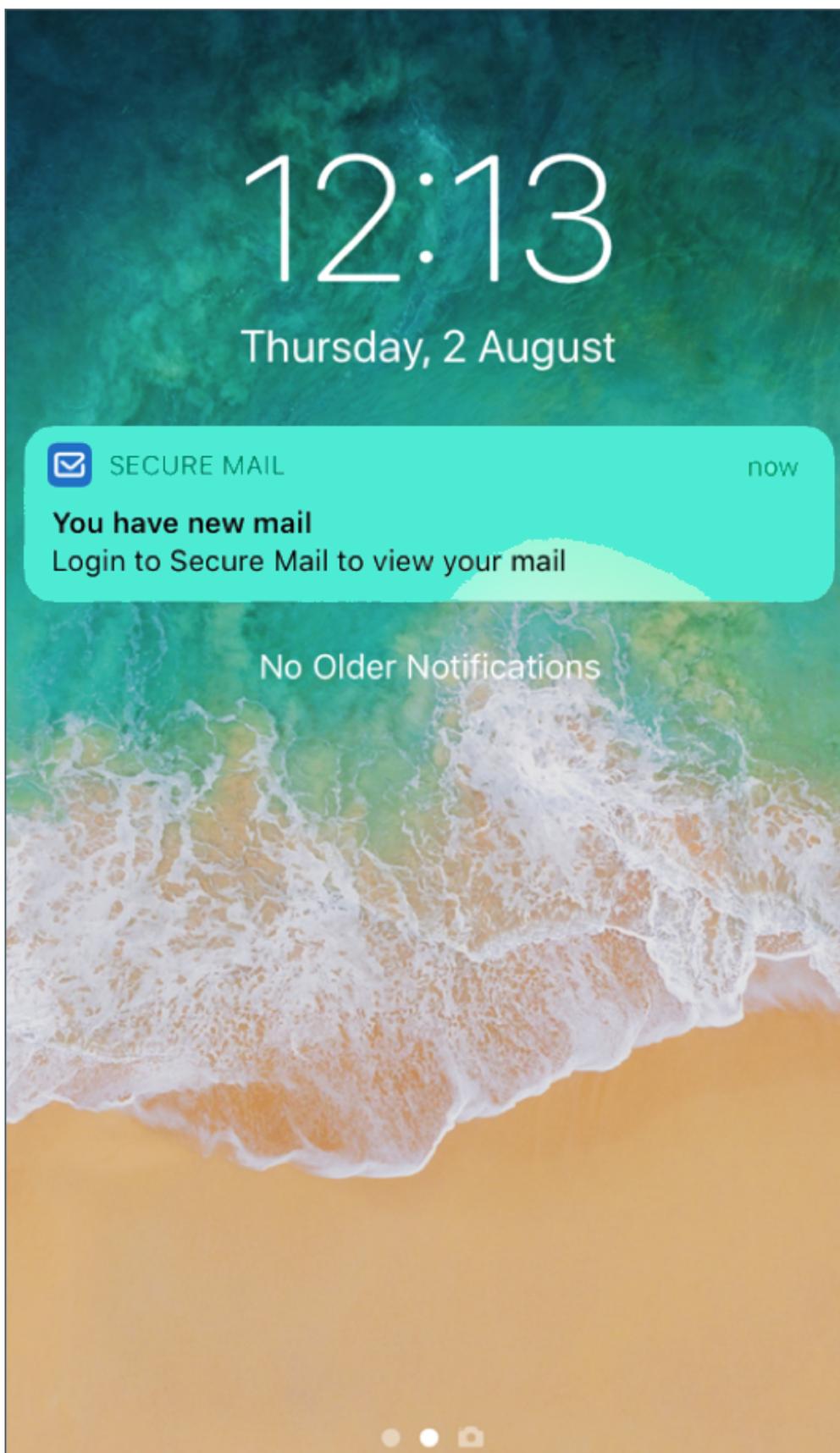
A notificação “Você tem novo e-mail” aparece em dispositivos iOS quando o Secure Mail não recebe uma resposta do EWS (Serviços Web do Exchange) no tempo especificado. O tempo necessário para obter os detalhes da mensagem é de 30 segundos.



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

Além da resposta atrasada do EWS, o Secure Mail 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 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 Exchange Server 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 seu dispositivo tiver sido reiniciado, mas 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.

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

December 9, 2021

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 de recursos do Secure Mail para cada plataforma, consulte [Recursos por plataforma](#).

Teste e resolução de problemas no Secure Mail

December 9, 2021

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 [Endpoint Management Analyzer Tool](#).

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 User-AuditLogFile.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.

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

© 2022 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).