citrix

# Secure Mail

## Contents

**Introducción a Secure Mail** 3

**Novedades en Secure Mail** 4

**Problemas conocidos y problemas resueltos** 32

**Implementar Secure Mail** 33

**Configurar Secure Mail** 34

**Integrar Secure Mail en Microsoft Intune/EMS** 35

**Autenticación moderna en Microsoft Office 365** 36

**Servicios en segundo plano para Secure Mail** 39

**Integrar Exchange Server o IBM Notes Traveler Server** 42

**S/MIME para Secure Mail** 45

**Single Sign-On para Secure Mail** 56

**Consideraciones sobre seguridad** 59

**Funciones de iOS** 64

**Funciones de Android** 72

**Funciones de iOS y Android para Secure Mail** 85

**Integrar Secure Mail con Slack (Tech Preview)** 109

**Notificaciones y sincronización** 111

**Notificaciones push para Secure Mail** 113

**Notificaciones push enriquecidas en Secure Mail para iOS** 120

**Interactividad de Secure Mail con otras aplicaciones móviles de productividad y Citrix Files** 124

**Probar Secure Mail y solucionar problemas de Secure Mail** 124

# Introducción a Secure Mail

October 19, 2020

Citrix Secure Mail permite a los usuarios administrar su correo electrónico, su calendario y sus contactos en sus teléfonos móviles y tabletas. Para mantener la continuidad con las cuentas de Microsoft Outlook o IBM Notes, Secure Mail se sincroniza con Microsoft Exchange Server e IBM Notes Traveler Server.

Como parte de la familia de aplicaciones de Citrix, Secure Mail es compatible con Single Sign-On en Citrix Secure Hub. Una vez que los usuarios inician sesión en Secure Hub, pueden pasar directamente a Secure Mail sin tener que volver a introducir su nombre de usuario y contraseña. Puede configurar Secure Mail para que se instale automáticamente en los dispositivos de los usuarios cuando se inscriban en Secure Hub, o bien, puede dejar que sean los usuarios quienes agreguen la aplicación desde el Store.

Secure Mail es compatible con:

- Exchange Server 2019 Cumulative Update 5
- Exchange Server 2019 Cumulative Update 6
- Exchange Server 2019 Cumulative Update 5
- Exchange Server 2016 Cumulative Update 8
- Exchange Server 2016 Cumulative Update 17
- Exchange Server 2016 Cumulative Update 16
- Exchange Server 2016 Cumulative Update 13
- Exchange Server 2013 Cumulative Update 23
- Exchange Server 2013 Cumulative Update 22
- Exchange Server 2013 Cumulative Update 21
- Exchange Server 2010 SP3 Update Rollup 26
- Exchange Server 2010 SP3 Update Rollup 24
- IBM Domino Mail Server, versión 10.0.1
- IBM Domino Mail Server versión 9.0.1 FP10 HF197
- IBM Lotus Notes Traveler, versión 10.0.1.0, compilación 201811191126_20
- IBM Lotus Notes Traveler 9.0.1.21
- Microsoft Office 365 (Exchange Online)

Para comenzar, descargue Secure Mail y otros componentes de Endpoint Management desde la página de descargas de Citrix Endpoint Management.

Para conocer los requisitos del sistema de Secure Mail y otras aplicaciones móviles de productividad, consulte Requisitos del sistema.

Para obtener más información acerca de las notificaciones en Secure Mail para iOS y Android cuando

la aplicación está cerrada o se ejecuta en segundo plano, consulte Notificaciones push para Secure Mail.

Para conocer las funciones de iOS admitidas en Secure Mail, consulte Funciones de iOS para Secure Mail.

Para conocer las funciones de Android admitidas en Secure Mail, consulte Funciones de iOS y Android para Secure Mail.

Para conocer las funciones de iOS y Android admitidas en Secure Mail, consulte Funciones de iOS y Android para Secure Mail.

Para ver documentación de ayuda para usuarios, consulte la página Citrix Secure Mail del Centro de ayuda para usuarios de Citrix.

## Novedades en Secure Mail

October 19, 2020

En las siguientes secciones se indican las nuevas funciones de la versión actual y las versiones anteriores de Secure Mail.

Para ver documentación de ayuda para usuarios, consulte la página Citrix Secure Mail del Centro de ayuda para usuarios de Citrix.

> **Nota:**
>
> A partir de junio de 2020, no se admiten las versiones de Android 6.x y iOS 11.x de Secure Hub, Secure Mail, Secure Web y la aplicación Citrix Workspace.

### Novedades en la versión actual

#### Secure Mail 20.10.0

A partir de esta versión, Secure Mail es compatible con Exchange Server 2019 Cumulative Update 7 y Exchange Server 2016 Cumulative Update 18.

#### Secure Mail para iOS

**Unirse a las reuniones de Microsoft Teams desde Secure Mail.** En Secure Mail para iOS, puede unirse a las reuniones de Microsoft Teams (MS Teams) directamente desde las invitaciones del Calendario. Si la aplicación MS Teams está instalada, la aplicación se abre y se une a la reunión. Cuando

la aplicación no está instalada, aparece una opción para ir a App Store e instalar MS Teams. Para las reuniones en formato https://teams.microsoft.com/l/meetup-join/meetinglink, se abre la aplicación y se une a la reunión directamente.

> **Nota:**
>
> Asegúrese de que su administrador incluya `+^msteams:` en la directiva URL permitidas. Para obtener información detallada, consulte Interacción entre aplicaciones (URL de salida).

#### Secure Mail para Android

- **Unirse a las reuniones de Microsoft Teams desde Secure Mail.** En Secure Mail para Android, puede unirse a las reuniones de Microsoft Teams (MS Teams) directamente desde las invitaciones del Calendario. Si la aplicación MS Teams está instalada, la aplicación se abre y se une a la reunión. Cuando la aplicación no está instalada, aparece una opción para ir a Google Play e instalar MS Teams. Para las reuniones en formato https://teams.microsoft.com/l/meetup-join/meetinglink, se abre la aplicación y se une a la reunión directamente.

  > **Nota:**
  >
  > Asegúrese de que su administrador incluya `{ action=android.intent.action.VIEW scheme=msteams package=com.microsoft.teams }` en la directiva Lista de excepciones de la apertura restringida. Para obtener información detallada, consulte Interacción entre aplicaciones.

- Secure Mail admite los requisitos actuales de la API de destino de Google Play para Android 10.

### Novedades en versiones anteriores

#### Secure Mail 20.9.5

#### Secure Mail para Android

Esta versión incluye correcciones de errores.

#### Secure Mail 20.9.0

**Compatibilidad con Azure Government Cloud Computing.** Secure Mail para iOS y Android es compatible con autenticación moderna (OAuth) de Government Cloud Computing (GCC) High en arrendatarios de Azure Active Directory. Secure Mail está registrado como punto final en GCC High, a efectos de cumplir con los requisitos obligatorios de Microsoft para todos los servicios de GCC High. Para obtener información detallada, consulte Novedades de Azure Active Directory en Microsoft 365 Government.

Con este cambio, el usuario se enruta a GCC High en el arrendatario de Azure Active Directory para la autenticación. Además, el administrador debe conceder permisos para Secure Mail en el arrendatario de Azure Active Directory.

#### Requisitos previos

Asegúrese de que el administrador global de Azure Active Directory haga lo siguiente:

- Descargue la última versión de Secure Mail en su dispositivo.
- Configure su cuenta de Exchange en la aplicación Secure Mail y otorgue permiso de aplicación en Azure Active Directory para que todos los usuarios inicien sesión. Consulte la siguiente pantalla.

> **Nota:**
>
> Los administradores globales deben hacer esto una sola vez. Una vez que se concede acceso a la aplicación, basta con actualizar la versión desde App Store.

#### Después de la actualización de versión

Después de una actualización de versión, se le solicitará que renueve la autorización una vez que caduque el token de actualización, que redirige a GCC High en Azure Active Directory. Valide el flujo de trabajo anterior para asegurarse de que la solicitud de autorización se envía a GCC High en Azure Active Directory.

Puede validar el flujo de trabajo de una de las siguientes maneras:

- Secure Mail con el nombre de aplicación **Secure Mail-GCC High** aparece en la página de inicio de sesión del arrendatario de Azure Active Directory.
- Compruebe los registros de Secure Mail para confirmar que los redireccionamientos se producen a través de https://login.microsoftonline.us después de la reautenticación.

### Secure Mail 20.8.5

#### Secure Mail para Android

Secure Mail para Android es compatible con Android 11.

### Secure Mail 20.8.0

A partir de esta versión, Secure Mail es compatible con Exchange Server 2019 Cumulative Update 6 y Exchange Server 2016 Cumulative Update 17.

### Secure Mail para Android

**Modo dual (vista previa) para la versión para Android de Secure Mail.** Dispone de un SDK de administración de aplicaciones móviles (MAM) para reemplazar áreas de funcionalidad MDX que no cubren las plataformas iOS y Android. La tecnología de empaquetado MDX está programada para alcanzar el final de su vida útil (EOL) en septiembre de 2021. Para seguir administrando sus aplicaciones empresariales, debe incorporar el SDK de MAM.

A partir de la versión 20.8.0, las aplicaciones de Android se publican con MDX y el SDK de MAM en preparación para la estrategia de fin de vida de MDX mencionada anteriormente. El modo dual MDX está diseñado para ofrecer una forma de transición desde el antiguo MDX Toolkit a nuevos SDK de MAM. El uso del modo dual le permite continuar administrando aplicaciones con MDX Toolkit (ahora MDX antiguo) o cambiar al nuevo SDK de MAM.

Una vez que cambie al SDK de MAM para administrar las aplicaciones, Citrix implementará nuevos cambios y no se requiere intervención alguna por parte de los administradores.

Para obtener más información sobre el SDK de MAM (Vista previa), consulte los siguientes artículos:

- Introducción al SDK de MAM
- Sección de Citrix Developer sobre Administración de dispositivos
- entrada del blog de Citrix
- Descargue el SDK cuando inicie sesión en la página de descargas de Citrix

#### Requisitos previos

Para implementar correctamente la funcionalidad de modo dual, compruebe lo siguiente:

- Actualice Citrix Endpoint Management a las versiones 10.12 RP2 o posterior, o 10.11 RP5 o posterior.
- Actualice sus aplicaciones móviles a la versión 20.8.0 o posterior.
- Actualice el archivo de directivas a la versión 20.8.0 o posterior.
- Si su organización utiliza aplicaciones de terceros, asegúrese de incorporar el SDK de MAM en dichas aplicaciones antes de cambiar a la opción SDK de MAM para las aplicaciones móviles de productividad de Citrix. Todas las aplicaciones administradas deben transferirse al SDK de MAM al mismo tiempo.

> **Nota:**
>
> El SDK de MAM es compatible con todos los clientes basados en la nube.

#### Limitaciones

- El SDK de MAM solamente admite aplicaciones publicadas bajo la plataforma Android Enterprise en la implementación de Citrix Endpoint Management. Para las aplicaciones recién publicadas, el cifrado predeterminado es el basado en plataforma.

- El SDK de MAM solamente admite el cifrado basado en plataforma, y no el cifrado MDX.
- Si no actualiza Citrix Endpoint Management y los archivos de directiva se ejecutan en la versión 20.8.0 o posterior para las aplicaciones móviles, se crearán entradas duplicadas de la directiva de conexión en red para Secure Mail.

Al configurar Secure Mail en Citrix Endpoint Management, la funcionalidad de modo dual le permite continuar administrando aplicaciones con MDX Toolkit (ahora **MDX antiguo**) o cambiar al nuevo **SDK de MAM**. Citrix recomienda cambiar al **SDK de MAM**, ya que los SDK de MAM son más modulares y están pensados para permitirle usar solamente el subconjunto de la funcionalidad MDX que su organización utiliza.

En el **contenedor de directivas MDX o del SDK de MAM**, obtiene las siguientes opciones para la configuración de directivas:

- **SDK de MAM**
- **MDX antiguo**

En la directiva **Contenedor de directivas MDX o de SDK de MAM**, solo puede cambiar de la opción **MDX antiguo** a **SDK de MAM**. La posibilidad de cambiar de **SDK de MAM** a **MDX antiguo** no está permitida, y debe volver a publicar la aplicación. El valor predeterminado es **MDX antiguo**. Asegúrese de establecer el mismo modo de directiva para las aplicaciones Secure Mail y Secure Web que se ejecutan en el mismo dispositivo. No puede tener dos modos diferentes ejecutándose en un mismo dispositivo.

#### Secure Mail para iOS

**Optimización de la sincronización de buzones.** En Secure Mail para iOS, se ha mejorado la sincronización de **buzones** a fin de proporcionar una mejor experiencia de usuario. El **calendario** y los **contactos** se sincronizan más rápidamente. Los correos electrónicos que tienen más de 3 semanas se truncan para reducir el tiempo de sincronización. Puede ver todo el correo electrónico al abrirlo.

### Secure Mail 20.7.5

> **Nota:**
>
> Android 6.x dejó de admitirse el 30 de junio de 2020.

Para obtener la información más reciente sobre las aplicaciones móviles de productividad, consulte el artículo Anuncios recientes.

### Secure Mail 20.7.0

Esta versión incluye correcciones de errores.

**Secure Mail 20.6.5**

Esta versión incluye correcciones de errores.

**Secure Mail 20.6.0**

Esta versión incluye correcciones de errores.

**Secure Mail 20.5.0**

Esta versión incluye correcciones de errores.

**Secure Mail 20.4.5**

**Secure Mail para Android**

A partir de esta versión, Secure Mail es compatible con Exchange Server 2019 Cumulative Update 5 y Exchange Server 2016 Cumulative Update 16.

**Secure Mail 20.4.0**

A partir de esta versión, Secure Mail es compatible con Exchange Server 2016 Cumulative Update 15 y Exchange Server 2013 Cumulative Update 23.

**Secure Mail 20.3.0**

**Secure Mail para Android**

**Cree carpetas en Contactos.** En Secure Mail para Android, puede agregar, modificar y eliminar carpetas en la sección **Contactos** de su cuenta de correo electrónico.

**Secure Mail para iOS**

Esta versión incluye correcciones de errores.

**Secure Mail 20.2.0**

**Secure Mail para Android**

#### Minimizar borradores

En Secure Mail para Android, puede minimizar un borrador mientras escribe un correo electrónico y navegar dentro de la aplicación. Para obtener documentación de ayuda sobre esta función, consulte el artículo Minimizar el borrador de un correo electrónico del Centro de ayuda para usuarios de Citrix.

### Secure Mail 20.1.5

#### Secure Mail para iOS

A partir de esta versión, Secure Mail es compatible con Exchange Server 2019 Cumulative Update 4

#### Secure Mail para Android

- **Sincronización bidireccional de contactos** En Secure Mail para Android, puede crear, modificar y eliminar contactos de Secure Mail desde su lista de contactos local.
- **Compatibilidad con archivos ICS.** En Secure Mail para Android, puede obtener una vista previa de los archivos ICS que recibe como datos adjuntos e importarlos a su calendario como eventos.
- A partir de esta versión, Secure Mail es compatible con Exchange Server 2019 Cumulative Update 4

### Secure Mail 20.1.0

A partir de esta versión, Secure Mail es compatible con Exchange Server 2016 Cumulative Update 14

### Secure Mail 19.12.5

#### Secure Mail para iOS

Esta versión incluye correcciones de errores.

#### Secure Mail para Android

**Deshacer correos enviados.** En Secure Mail para Android puede deshacer correos enviados. Una vez que haya tocado el botón **Enviar**, recibirá una notificación que le permite deshacer la acción del envío. Toque **Deshacer** para revertir el envío y modificar el correo o los destinatarios del correo, adjuntar o quitar archivos adjuntos, o bien descartar el correo.

**Sincronización de archivos adjuntos en la carpeta Borradores.** En Secure Mail para Android, cuando la carpeta **Borradores** se sincroniza, los archivos adjuntos también se sincronizan y están disponibles en todos los dispositivos. Esta función está disponible en dispositivos con la versión 16 de Exchange ActiveSync o una posterior.

### Secure Mail 19.11.5

#### Secure Mail para iOS

**Imagen de contacto en Secure Mail.** En Secure Mail para iOS, puede ver la imagen de un contacto al agregar destinatarios en correos electrónicos o invitaciones a reuniones. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Mostrar imágenes de los contactos.

#### Secure Mail para Android

**Consulta de archivos PDF en la aplicación.** En Secure Mail para Android, puede ver archivos PDF dentro de la aplicación, junto con marcadores y anotaciones. También está disponible la vista mejorada de otros archivos adjuntos de Microsoft Office.

### Secure Mail para iOS 19.10.6

Esta versión incluye correcciones de errores.

### Secure Mail 19.10.5

#### Secure Mail para iOS

**Minimizar los borradores.** En Secure Mail para iOS, puede minimizar un borrador mientras está redactando un correo electrónico y navegar por la aplicación. Esta función está disponible en dispositivos con iOS 13 y versiones posteriores. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Minimizar el borrador de un correo electrónico.

#### Secure Mail para Android

Esta versión incluye correcciones de errores.

### Secure Mail 19.10.0

**Utilice la directiva de Office 365 Exchange Server para definir la dirección del servidor de Office 365.** En Secure Mail iOS y Android, se agrega una nueva directiva llamada **Office 365 Exchange Server** en la sección Funcionalidad OAuth para Office 365. Con esta directiva, puede definir el nombre de host para el buzón de Office 365 presente en la nube. Esta directiva también habilita la compatibilidad con Office 365 para agencias gubernamentales. El nombre de host es un valor único, como *outlook.office365.com*. El valor predeterminado es *outlook.office365.com*.

**Secure Mail iOS y Android admiten la administración de cifrado.** La administración de cifrado le permite utilizar la seguridad moderna de la plataforma del dispositivo para, al mismo tiempo, garantizar que dicho dispositivo permanezca en un estado suficiente para utilizar la seguridad de la plataforma de manera eficaz. Con la administración de cifrado, elimina la redundancia en el cifrado de datos locales, ya que son las plataformas Android y iOS las que proporcionan el cifrado del sistema de archivos. Para habilitar esta función, un administrador debe configurar la directiva MDX **Tipo de cifrado** en **Cifrado de plataforma con cumplimiento de requisitos** en la consola de Citrix Endpoint Management.

Para utilizar la función de administración de cifrado, en la consola de Citrix Endpoint Management, establezca la directiva **Tipo de cifrado** en **Cifrado de plataforma con cumplimiento de requisitos**. Esto habilita la administración de cifrado, y todos los datos de las aplicaciones cifradas existentes en los dispositivos de los usuarios pasan directamente a un estado cifrado por el dispositivo y no por MDX. Durante esta transición, la aplicación se pausa para una única migración de datos. Una vez realizada correctamente la migración, la responsabilidad del cifrado de los datos almacenados localmente se transfiere de MDX a la plataforma del dispositivo. MDX continúa comprobando el cumplimiento de requisitos en el dispositivo durante cada inicio de la aplicación. Esta función opera tanto en entornos MDM + MAM como en solo MAM.

Cuando establece la directiva **Tipo de cifrado** en **Cifrado de plataforma con cumplimiento de requisitos**, la nueva directiva reemplaza el cifrado MDX existente.

Para obtener información detallada acerca de las directivas MDX de administración de cifrado para Secure Mail, consulte la sección **Cifrado** en:

- Directivas MDX para aplicaciones móviles de productividad para Android
- Directivas MDX para aplicaciones móviles de productividad para iOS

Cuando un dispositivo no cumple todos los requisitos mínimos de conformidad, la directiva **Comportamiento de dispositivos no conformes** le permite seleccionar qué hacer al respecto:

- **Permitir aplicación**: Permite que la aplicación se ejecute normalmente.
- **Permitir aplicación después de la advertencia**: Advierte al usuario que una aplicación no cumple los requisitos mínimos de conformidad y permite que la aplicación se ejecute. Este es el valor predeterminado.
- **Bloquear aplicación**: Impide que la aplicación se ejecute.

#### Dispositivos con iOS

Los siguientes criterios determinan si un dispositivo cumple los requisitos mínimos de conformidad para dispositivos con iOS.

- iOS 10: Una aplicación tiene una versión de sistema operativo que es mayor o igual que la versión especificada.

- Acceso de depurador de errores: Una aplicación no tiene habilitada la depuración de errores.
- Dispositivo liberado por jailbreak: Una aplicación no se está ejecutando en un dispositivo liberado por jailbreak.
- Código de acceso del dispositivo: El código de acceso del dispositivo está **activado**.
- Uso compartido de datos: El uso compartido de datos no está habilitado para la aplicación.

#### Dispositivos con Android

Los siguientes criterios determinan si un dispositivo cumple los requisitos mínimos de conformidad para dispositivos con Android.

- Android SDK 24 (Android 7 Nougat): Una aplicación tiene una versión de sistema operativo que es mayor o igual que la versión especificada.
- Acceso de depurador de errores: Una aplicación no tiene habilitada la depuración de errores.
- Dispositivos liberados por root: Una aplicación no se está ejecutando en un dispositivo liberado por root.
- Bloqueo de dispositivo: El código de acceso del dispositivo está **activado**.
- Dispositivo cifrado: Una aplicación se está ejecutando en un dispositivo cifrado.

### Secure Mail 19.9.5

#### Secure Mail para iOS

**Compatibilidad con archivos ICS.** En Secure Mail para iOS, puede importar archivos ICS que reciba como datos adjuntos al calendario como un evento.

#### Secure Mail para Android

Esta versión incluye correcciones de errores.

### Secure Mail 19.9.0

A partir de esta versión, Secure Mail admite los siguientes servidores:

- Exchange Server 2016 Cumulative Update 13
- IBM Lotus Notes Traveler, versión 10.0.1.0, compilación 201811191126_20
- IBM Domino Mail Server, versión 10.0.1

#### Secure Mail para iOS

- Secure Mail para iOS es compatible con iOS 13.

- **Notificar mensajes de phishing con encabezados MIME.** En Secure Mail para iOS, cuando un usuario notifica un mensaje de phishing, se genera un archivo EML como adjunto correspondiente a ese correo. Los administradores reciben este correo y pueden ver los encabezados MIME asociados al correo notificado. Para habilitar esta función, un administrador debe configurar la directiva "Direcciones para notificar mensaje de phishing" y definir el "Mecanismo para notificar phishing" en Notificar mediante archivo adjunto, en la consola de Citrix Endpoint Management. Para obtener información detallada, consulte Notificar mensajes de phishing en calidad de archivo adjunto.
- **Compatibilidad con mensajes de correo electrónico adaptativos.** Secure Mail para iOS se ha optimizado para ofrecer correos electrónicos adaptativos. Anteriormente, el contenido de los correos electrónicos con tablas o imágenes grandes no se mostraba correctamente. Esta función ofrece contenido de correo electrónico que se lee mejor en todos los dispositivos compatibles, independientemente del formato y tamaño del correo electrónico.
- **Arrastrar y colocar eventos del Calendario.** En Secure Mail para iOS, puede arrastrar y colocar un evento existente de calendario para cambiarle la hora. Arrastre el evento y colóquelo en el intervalo de tiempo que quiera del mismo día o en los días que quiere actualizar.
- **Avance automático.** En Secure Mail para iOS, cuando elimina un mensaje en **Conversaciones**, puede elegir a qué mensaje volver. Para utilizar esta función, vaya a **Parámetros > Avance automático**. A continuación, seleccione su preferencia entre las opciones disponibles. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Eliminar y avanzar automáticamente a un correo electrónico en Conversaciones.
- **Funcionalidad de WkWebView.** Secure Mail para iOS admite WkWebView. Esta función mejora la forma en que se representan en su dispositivo los eventos de correo electrónico y Calendario de Secure Mail.

#### Secure Mail para Android

A partir de esta versión, Secure Mail para Android solo se admite en dispositivos con Android 6 o una versión posterior.

#### Secure Mail para Android 19.8.5

Esta versión incluye correcciones de errores.

#### Secure Mail 19.8.0

#### Secure Mail para iOS

En esta versión se incluyen mejoras de rendimiento y correcciones de errores.

### Secure Mail para Android

- Compatibilidad con Android Q.
- **Compatibilidad con aplicaciones de 64 bits para Google Play.** Secure Mail para Android admite arquitecturas de 64 bits.
- **Mejoras al deslizar la pantalla hacia abajo para actualizar la interfaz de usuario en Secure Mail para Android.** De acuerdo con las directrices de diseño de materiales, hemos realizado pequeñas mejoras en la función **Deslizar hacia abajo para actualizar**. La marca de hora de la sincronización está disponible en la parte inferior de la pantalla al tocar el icono de hamburguesa.

## Secure Mail 19.7.5

### Secure Mail para iOS

- **Sincronización automática de la carpeta Borradores.** En Secure Mail para iOS, la carpeta Borradores se sincroniza automáticamente y los borradores están disponibles en todos los dispositivos. Esta función está disponible en configuraciones con Exchange ActiveSync v16 o versiones posteriores. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Sincronización automática de la carpeta Borradores.
- **Secure Mail para iOS admite Single Sign-On cuando utiliza Microsoft Intune en el modo MDM + MAM.** Para poder usar esta función, la aplicación Microsoft Authenticator debe estar instalada en el dispositivo. Para obtener más información acerca de la instalación de la aplicación Microsoft Authenticator, consulte **Descarga e instalación de la aplicación Microsoft Authenticator** en *docs.microsoft.com*.

### Secure Mail para Android

> Nota:
>
> Citrix recomienda actualizar la versión de Secure Mail a 19.7.5 antes de actualizar su sistema operativo a Android Q.

- **Utilice SSO web para la directiva de tunelización en configuraciones que emplean autenticación moderna con Microsoft Office 365.** En Secure Mail para Android, se agrega una nueva directiva denominada **Utilizar SSO web para la tunelización**. Con esta directiva, puede tunelizar el tráfico de OAuth para que pase a través de Secure Browse. Para ello:
  - Establezca la directiva **Utilizar SSO web para la tunelización** en **Sí**.
  - En la directiva Acceso de red, seleccione la opción **SSO web en túnel**.
  - Excluya los nombres de host relacionados con OAuth de la directiva **Servicios en segundo plano**.

- **Secure Mail para Android admite Single Sign-On cuando utiliza Microsoft Intune en el modo MDM + MAM.** Para poder usar esta función, la aplicación Portal de empresa de Intune debe estar instalada en el dispositivo. Una vez que haya iniciado sesión en la aplicación Portal de empresa de Intune, podrá utilizar SSO en el modo MDM + MAM sin tener que volver a autenticarse en Secure Mail con sus credenciales.

### Secure Mail 19.6.5

#### Secure Mail para iOS

La versión 19.6.5 de Secure Mail para iOS incluye mejoras de rendimiento y correcciones de errores. Para ver una lista de problemas conocidos y resueltos, consulte Problemas conocidos y problemas resueltos.

#### Secure Mail para Android

- **Arrastrar y colocar eventos del Calendario.** En Secure Mail para Android, puede arrastrar y colocar un evento existente de calendario para cambiarle la hora. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Cambiar el momento de un evento de calendario.
- **Compatibilidad con mensajes de correo electrónico adaptativos.** Secure Mail para Android se ha optimizado para ofrecer correos electrónicos adaptativos. Anteriormente, el contenido de los correos electrónicos con tablas o imágenes grandes no se mostraba correctamente. Esta función ofrece contenido de correo electrónico y se lee mejor en todos los dispositivos compatibles, independientemente del formato y tamaño del correo electrónico.
- **Imagen de contacto en Secure Mail.** En Secure Mail para Android, puede ver la imagen del contacto al agregar destinatarios en correos electrónicos o invitaciones a reuniones. La imagen del contacto se muestra junto al nombre. Si hay varias personas con el mismo nombre, la imagen ayuda a identificar al destinatario correcto cuando agrega destinatarios en correos electrónicos o invitaciones a reuniones. Para buscar contactos que no se hayan guardado localmente, introduzca al menos cuatro caracteres del nombre del destinatario para mostrar la imagen.
- **Widget para la agenda del Calendario.** En Secure Mail para Android, la agenda del **Calendario** está disponible como un widget. Desde este widget, puede ver los próximos eventos en el **Calendario** de una semana. Esta función le permite crear eventos del **Calendario**, ver eventos existentes y modificar los detalles. La directiva **Bloquear captura de pantalla** no se aplica al widget colocado en la pantalla de inicio. Sin embargo, puede inhabilitar el widget mediante la directiva **Permitir widget de agenda del calendario**.

### Secure Mail 19.5.5

#### Secure Mail para Android

La versión 19.5.5 de Secure Mail para Android incluye mejoras de rendimiento y correcciones de errores. Para ver una lista de problemas conocidos y resueltos, consulte Problemas conocidos y problemas resueltos.

#### Secure Mail para iOS

- Secure Mail para iOS admite Single Sign-On cuando utiliza Microsoft Intune en el modo MDM + MAM. Para poder usar esta función, la aplicación Microsoft Authenticator debe estar instalada en el dispositivo. La aplicación Microsoft Authenticator está disponible en las tiendas de aplicaciones.
- **Compatibilidad con Slack EMM:** Slack EMM está destinado a clientes de Slack con Enterprise Mobility Management (EMM) habilitado. Secure Mail para iOS admite la aplicación **Slack EMM**, que permite a los administradores elegir la integración de Secure Mail con la aplicación **Slack** o la aplicación **Slack EMM**.

### en Secure Mail 19.5.0

#### Secure Mail para Android

**Administre sus feeds.** En Secure Mail para Android, puede organizar su tarjeta de **Feeds** en función de sus requisitos.

Para obtener más información sobre cómo administrar sus feeds, consulte Administrar sus feeds.

**Sincronización automática de la carpeta Borradores.** En Secure Mail para Android, la carpeta Borradores se sincroniza automáticamente y los borradores están disponibles en todos los dispositivos. Para ver documentación de ayuda para usuarios y un vídeo sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Sincronización automática de la carpeta Borradores.

### Secure Mail para Android 19.4.6, 19.4.5 y 19.3.5

En estas versiones se incluyen mejoras de rendimiento y correcciones de errores.

Para ver una lista de problemas conocidos y resueltos, consulte Problemas conocidos y problemas resueltos.

### Secure Mail 19.3.0

A partir de esta versión, Secure Mail admite los siguientes servidores:

- Exchange Server 2019 Cumulative Update 1
- Exchange Server 2016 Cumulative Update 12
- Exchange Server 2013 Cumulative Update 22
- Exchange Server 2010 SP3 Update Rollup 26

Para obtener más información acerca de la lista completa de compatibilidad con servidores Secure Mail, consulte Introducción a Secure Mail.

#### Secure Mail para iOS

**Administre sus feeds.** En Secure Mail para iOS, puede organizar su tarjeta de **Feeds** en función de sus requisitos.

> **Nota:**
>
> Esta función no está disponible para iPads.

Para obtener más información sobre cómo administrar sus feeds, consulte Administrar sus feeds.

#### Secure Mail para iOS y Android

**Dominios internos.** Puede identificar y modificar destinatarios de correo que pertenezcan a organizaciones externas. Para utilizar esta función, asegúrese de haber habilitado la directiva **Dominios internos** en Citrix Endpoint Management.

Al crear, responder o reenviar un correo electrónico, los destinatarios externos se resaltan en la lista de correo. El icono **Contactos** aparece como una advertencia en la parte inferior izquierda de la pantalla. Toque el icono **Contactos** para modificar la lista de correo.

Para obtener más información acerca de los dominios internos, consulte Dominios internos.

**Mejoras ergonómicas.** Los botones de acción se han movido de la parte superior de la pantalla a la parte inferior para facilitar el acceso. Estos cambios se han implementado en las pantallas **Bandeja de entrada**, **Calendario** y **Contactos**.

> **Nota:**
>
> En los dispositivos con Android, los cambios se han implementado en las pantallas **Bandeja de entrada** y **Calendario**.

Para obtener más información sobre las mejoras ergonómicas, consulte Mejoras ergonómicas.

### Secure Mail 19.2.0

#### Secure Mail para iOS

En esta versión se incluyen mejoras de rendimiento y correcciones de errores.

Para ver una lista de problemas conocidos y resueltos, consulte Problemas conocidos y problemas resueltos.

**Secure Mail para Android**

- **Mejoras en Contactos.** En Secure Mail para Android, cuando toca **Contactos** y selecciona un contacto, los detalles de ese contacto aparecen en la ficha **Contacto**. Al tocar la ficha **Organización**, aparecen los detalles de la jerarquía de la organización, como **ADMINISTRADOR**, **COLABORADORES DIRECTOS** y **COMPAÑEROS**. Al tocar el icono Más en la parte superior derecha de la pantalla, aparecen las siguientes opciones:
  - **Adjuntar a correo**
  - **Compartir**
  - **Eliminar**

  En la ficha **Organización**, puede tocar el icono "Más", situado a la derecha de **ADMINISTRADOR**, **COLABORADORES DIRECTOS** o **COMPAÑEROS**. A continuación, cree un correo electrónico o una invitación de calendario. El campo **Para:** del correo electrónico o evento de calendario se rellena automáticamente con los detalles de **ADMINISTRADOR**, **COLABORADORES DIRECTOS** o **COMPAÑEROS**.

  **Requisitos previos:**

  Compruebe que los servicios web de Exchange (EWS) están habilitados en su servidor de Exchange.

  Los detalles de contacto que aparecen dependen de los detalles de la organización, obtenidos de Active Directory. Para que aparezcan los detalles correctos para sus contactos, compruebe que el administrador haya definido la jerarquía de la organización en Active Directory.

  > **Nota:**
  >
  > Esta función no está disponible en el servidor IBM Lotus Notes.

- **Directiva de acceso de red**. En Secure Mail para Android, se agrega una nueva opción llamada **SSO web en túnel** a la directiva MDX de acceso de red. Configurar esta directiva le dará la flexibilidad de usar el túnel para transferir el tráfico interno a través de Secure Browse y Secure Ticket Authority (STA) en paralelo. También puede permitir conexiones Secure Browse para servicios de autenticación, como NTLM, Okta y Kerberos. Al configurar STA inicialmente, debe agregar nombres de dominio completos individuales y puertos de direcciones de servicios a la directiva Servicios de red en segundo plano. Sin embargo, si configura la opción **SSO web en túnel**, no es necesario realizar estas configuraciones.

Cómo habilitar esta directiva para Secure Mail para Android en la consola de Citrix Endpoint Management:

1. Descargue y use el archivo MDX para Android. Para obtener más información, consulte los pasos de Funcionamiento de las aplicaciones MDX y las aplicaciones móviles.
2. En la directiva Acceso de red, haga clic en la opción **SSO web en túnel**. Para obtener más información, consulte Acceso a red de las aplicaciones

#### Secure Mail para iOS 19.1.6

En esta versión se incluyen mejoras de rendimiento y correcciones de errores.

#### Secure Mail 19.1.5

A partir de esta versión, Secure Mail admite los siguientes servidores:

- Exchange Server 2016 Cumulative Update 11
- Exchange Server 2010 SP3 Update Rollup 24

Para obtener más información acerca de la lista completa de compatibilidad con servidores Secure Mail, consulte Introducción a Secure Mail.

#### Secure Mail 19.1.0

#### Secure Mail para iOS

- **Mejoras en Contactos.** En Secure Mail para iOS, cuando toca **Contactos** y selecciona un contacto, los detalles de ese contacto aparecen en la ficha **Contacto**. Al pulsar la ficha **Organización**, aparecen los detalles de la jerarquía de la organización, como **Administrador**, **Colaboradores directos** y **Compañeros**. Al tocar el icono Más en la parte superior derecha de la pantalla, aparecen las siguientes opciones:
  - Edit (Modificar)
  - Agregar a VIP
  - Cancelar

  En la ficha **Organización**, puede tocar en el icono "Más", situado a la derecha de **Administrador**, **Colaboradores directos** o **Compañeros**. Esta acción permite crear un correo electrónico o un evento de calendario. El campo **Para:** del correo electrónico o
  evento de calendario se rellena automáticamente con los detalles de **Administrador**, **Colaboradores directos** o **Compañeros**. Puede redactar y enviar el correo electrónico.

  **Requisitos previos:**

  Compruebe que los servicios web de Exchange (EWS) están habilitados en su servidor de Exchange.

Los detalles de contacto que aparecen dependen de los detalles de la organización (contacto de Outlook), obtenidos de Active Directory. Para que aparezcan los detalles correctos para sus contactos, compruebe que el administrador haya definido la jerarquía de la organización en Active Directory.

> **Nota:**
>
> Esta función no está disponible en el servidor IBM Lotus Notes.

- **Exporte la hora y la ubicación de la reunión a su calendario nativo.** En Secure Mail para iOS, se agrega un nuevo valor **Hora de reunión, Ubicación** a la directiva MDX **Exportar calendario**. Esta mejora permite exportar la hora y la ubicación de las reuniones de los eventos del calendario de Secure Mail a su calendario nativo.
- Secure Mail para iOS admite notificaciones push enriquecidas en configuraciones que ejecutan Microsoft Enterprise Mobility + Security (EMS) /Intune con autenticación moderna (O365).

  Para habilitar la función de notificaciones push enriquecidas, debe cumplir los siguientes requisitos previos:

  - En la consola de Endpoint Management, active las **notificaciones push**.
  - Establezca la directiva **Acceso de red** en **Sin restricciones**.
  - Establezca la directiva **Control de notificaciones en pantalla bloqueada** en **Permitir** o **Remitente del correo o título del evento**.
  - Vaya a **Secure Mail** > **Parámetros** > **Notificaciones** y habilite **Notificaciones de correo**.
- Los usuarios de Secure Mail pueden utilizar la aplicación Zoom para unirse a reuniones. Para obtener información sobre cómo configurar las directivas necesarias para utilizar la aplicación Zoom, consulte Unirse a reuniones desde el calendario.
- Esta versión admite iPad Pro de 11 pulgadas y iPad Pro de 12,9 pulgadas.

**Secure Mail para Android**

- **Mejoras en los datos adjuntos** En Secure Mail para Android, se ha simplificado la visualización de datos adjuntos. Para proporcionar una mejor experiencia, se han eliminado los pasos no esenciales, pero se conservan las opciones de datos adjuntos que existían en las versiones anteriores.

  Puede ver los datos adjuntos en la aplicación Secure Mail. El archivo adjunto se abre directamente si se puede ver mediante Secure Mail. Si los datos adjuntos no se pueden ver mediante Secure Mail, aparecerá una lista de aplicaciones. Puede seleccionar la aplicación necesaria para ver los datos adjuntos. Para obtener información detallada, consulte Visualizar datos adjuntos.
- Los usuarios de Secure Mail pueden utilizar la aplicación Zoom para unirse a reuniones. Para obtener información sobre cómo configurar las directivas necesarias para utilizar la aplicación Zoom, consulte Unirse a reuniones desde el calendario.

- **Exporte la hora y la ubicación de la reunión a su calendario nativo.** En Secure Mail para Android, se agrega un valor **Hora de reunión, Ubicación** a la directiva MDX **Exportar calendario**. Esto le permite exportar la hora y la ubicación de las reuniones de los eventos del calendario de Secure Mail a su calendario nativo.

> **Nota:**
>
> Android 5.x dejó de admitirse el 31 de diciembre de 2018.

#### Secure Mail 18.12.0

En esta versión se incluyen mejoras de rendimiento y correcciones de errores.

Para ver una lista de problemas conocidos y resueltos, consulte Problemas conocidos y problemas resueltos.

#### Secure Mail 18.11.5

#### Secure Mail para Android

- **Notificar mensajes de phishing con encabezados ActiveSync.** En Secure Mail para Android, cuando un usuario notifica un mensaje de phishing, se genera un archivo EML como adjunto correspondiente a ese correo. Los administradores reciben este correo y pueden ver los encabezados ActiveSync asociados al mensaje notificado.

  Para habilitar esta función, un administrador debe configurar la directiva **Direcciones para notificar mensaje de phishing** y definir el **Mecanismo para notificar phishing** en **Notificar mediante archivo adjunto**. El administrador configura estos parámetros en la consola de Citrix Endpoint Management. Para obtener información detallada sobre la configuración de directivas MDX para Secure Mail, consulte Directivas MDX para aplicaciones móviles de productividad.

- **Imprimir correos electrónicos y eventos de calendario** En Secure Mail para Android, puede imprimir correos electrónicos y eventos de calendario desde el dispositivo Android. Para esta funcionalidad de impresión, se utiliza el framework de Android Print. Para obtener información detallada, consulte Imprimir correos electrónicos y eventos de calendario.

- **Feeds del administrador.** En Secure Mail para Android, puede ver los correos electrónicos del administrador en la pantalla **Feeds**. Puede aparecer un máximo de cinco mensajes de correo electrónico en los feeds **De su administrador**, en función de los parámetros del **Periodo de sincronización de correo**. Para ver más correos electrónicos de parte del administrador, toque **Ver todo**.

  **Requisitos previos:**

  Compruebe que los servicios web de Exchange (EWS) están habilitados en su servidor de Exchange.

Los datos que aparecen en la tarjeta de administrador dependen de los detalles de la organización (contacto de Outlook), obtenidos de Active Directory. Para que aparezcan los detalles correctos en el feed del administrador, compruebe que el administrador haya definido la jerarquía de la organización en Active Directory.

> **Nota:**
>
> Esta función no está disponible en el servidor IBM Lotus Notes.

### Secure Mail 18.11.1

> Importante:
>
> Se ha resuelto el siguiente problema en Secure Mail para Android 18.11.1.
>
> En Secure Mail para Android con conexiones a IBM Notes Traveler 9.0.1 SP 10, los correos electrónicos con archivos adjuntos permanecen en la bandeja de salida. [CXM-58962]

### Secure Mail 18.11.0

#### Secure Mail para Android

- **Notificaciones de subcarpeta.** En Secure Mail para Android, puede recibir notificaciones de correo desde subcarpetas de la cuenta de correo. Para obtener información detallada, consulte Notificaciones de subcarpeta.
- **Actualizaciones a los servicios en segundo plano en Secure Mail para Android.** Para cumplir con el requisito de límites de ejecución en segundo plano de Google Play en dispositivos con Android 8.0 (API de nivel 26) o posterior, hemos actualizado los servicios en segundo plano de Secure Mail. Para una sincronización de correo ininterrumpida y unas notificaciones continuas en el dispositivo, habilite el servicio de notificaciones push de Firebase Cloud Messaging (FCM). Para obtener más información sobre cómo habilitar las notificaciones push basadas en FCM, consulte Notificaciones push para Secure Mail.

Debe activar las **notificaciones de correo** en los parámetros de Secure Mail del dispositivo. Para obtener información más detallada sobre esta actualización, consulte este artículo de Citrix Support Knowledge Center.

**Limitaciones:**

- Si no ha habilitado las notificaciones push basadas en FCM, la sincronización en segundo plano se produce una vez cada 15 minutos. Este intervalo puede variar según si la aplicación se está ejecutando en segundo plano o en primer plano.
- Cuando los usuarios actualizan manualmente la hora desde los parámetros del dispositivo, la fecha en el widget del calendario no se actualiza automáticamente.

### Secure Mail para iOS

- **Disponible en iOS 12.1.** Secure Mail para iOS está disponible en iOS 12.1.
- **Mejoras en los mensajes de error de notificaciones push enriquecidas.** En Secure Mail para iOS, los mensajes de error referentes a notificaciones push aparecen en el centro de notificaciones correspondiente del dispositivo y se agrupan por tipo de error de la notificación. Para obtener más información acerca de los mensajes de error de notificación push en Secure Mail para iOS, consulte Mensajes de error de notificación push en Secure Mail para iOS.
- **Feeds del administrador.** En Secure Mail para iOS, puede ver los correos electrónicos del administrador en la pantalla **Feeds**. Puede aparecer un máximo de cinco mensajes de correo electrónico en los feeds **De su administrador**, en función de los parámetros del **Periodo de sincronización de correo**. Para ver más correos electrónicos de parte del administrador, toque **Ver todo**.

  **Requisitos previos:**

  Compruebe que los servicios web de Exchange (EWS) están habilitados en su servidor de Exchange.

  Los datos que aparecen en la tarjeta de administrador dependen de los detalles de la organización (contacto de Outlook), obtenidos de Active Directory. Para que aparezcan los detalles correctos en el feed del administrador, compruebe que el administrador haya definido la jerarquía de la organización en Active Directory.

  > **Nota:**
  >
  > Esta función no está disponible en el servidor IBM Lotus Notes.

### Secure Mail 18.10.5

- **Integración de Secure Mail con Slack (Tech Preview):** Ahora puede llevar su conversación por correo electrónico a la aplicación Slack en dispositivos iOS o Android. Para obtener información detallada, consulte Integrar Secure Mail con Slack (Tech Preview).
- **Mejoras en la carpeta Feeds:** En Secure Mail para iOS, se han incorporado las siguientes mejoras a la carpeta Feeds existente:
  - Puede ver hasta cinco de las próximas reuniones en su tarjeta Feeds.
  - Las reuniones para el periodo de las próximas 24 horas aparecen en la tarjeta Feeds y se clasifican en las secciones **Hoy** y **Mañana**.

### Secure Mail 18.10.0

- **Canales de notificación de Secure Mail para notificaciones de correo y calendario:** En los dispositivos que ejecutan Android O o posterior, puede usar la configuración del canal de notifi-

caciones para administrar la forma en que se manejan sus notificaciones de correo electrónico y calendario. Esta función permite personalizar y administrar sus notificaciones. Para obtener información detallada, consulte Canales de notificaciones.

- **Notificar mensajes de phishing (en calidad de reenvíos):**En Secure Mail para iOS, puede usar la función "Notificar phishing" para informar sobre un correo electrónico sospechoso de phishing como un reenvío. Puede reenviar los mensajes sospechosos a las direcciones de correo electrónico que los administradores configuren en la directiva. Para habilitar esta función, un administrador debe configurar la directiva "Direcciones para notificar mensaje de phishing" y definir el **Mecanismo para notificar phishing** en **Notificar mediante reenvío**. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Notificar mensajes de phishing.

**Secure Mail 18.9.0**

- Nuevo esquema de numeración de versiones, en el formato "aa.mm.versión". Por ejemplo, versión **18.9.0**.
- **Notificar mensajes de phishing (en calidad de reenvíos):** En Secure Mail para Android, puede usar la función "Notificar phishing" para informar sobre un correo electrónico sospechoso de phishing como un reenvío. Puede reenviar los mensajes sospechosos a las direcciones de correo electrónico que los administradores configuren. Para habilitar esta función, un administrador debe configurar la directiva "Direcciones para notificar mensaje de phishing" y definir el "Mecanismo para notificar phishing" en **Notificar mediante reenvío**. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Notificar mensajes de phishing.
- **Mejoras en las tarjetas Feeds:** En Secure Mail para Android, se han realizado las siguientes mejoras en la carpeta **Feeds** existente:
  - Las invitaciones a las reuniones de todas las carpetas sincronizadas automáticamente aparecen en la tarjeta Feeds.
  - Puede ver hasta cinco de las próximas reuniones en su tarjeta Feeds.
  - Ahora las próximas reuniones aparecen en función de un período de 24 horas a partir de su hora actual. Estas invitaciones a reuniones se clasifican en **Hoy** y **Mañana**.
    En versiones anteriores, las próximas reuniones hasta el final del día aparecen es sus feeds.
- **Exportar eventos del calendario de Secure Mail:** Con Secure Mail para iOS y Android, puede exportar los eventos del calendario de Secure Mail a la aplicación de calendario nativa de su dispositivo. Para habilitar esta función, toque **Parámetros** y arrastre a la derecha el control deslizante de "Exportar eventos del calendario". Para obtener información detallada, consulte Exportar eventos del calendario de Secure Mail.

**Secure Mail 10.8.65**

- **Disponible con iOS 12:** En Secure Mail para iOS, admitimos la función "Notificaciones de grupo". Con esta función, las conversaciones se agrupan a partir de un hilo de correo. Puede ver rápidamente las notificaciones agrupadas en la pantalla de bloqueo del dispositivo. Los parámetros de las notificaciones de grupo están habilitados de forma predeterminada en el dispositivo.
- En Secure Mail para iOS, los botones **Guardar borrador** y **Eliminar borrador** son más grandes. Esta mejora permite a los clientes distinguir mejor una opción de la otra.
- En Secure Mail para iOS, puede identificar las llamadas entrantes de sus contactos de Secure Mail. Para ello, habilite la identificación de llamadas de Secure Mail en los **Ajustes** del dispositivo. Al habilitar esta configuración, cuando recibe una llamada entrante, el dispositivo muestra el nombre de la aplicación con el ID de la llamada, como "ID de llamada de Secure Mail: Julio Gómez". Para obtener información detallada, consulte Identificar llamada en Secure Mail.

**Secure Mail 10.8.60**

- Secure Mail es compatible con Android P.
- Ahora Secure Mail está disponible en polaco.
- En Secure Mail para iOS, puede adjuntar archivos a su correo electrónico desde la aplicación Archivos nativa de iOS. Para obtener más información, consulte Funciones de iOS.

**Secure Mail 10.8.55**

No hay funciones nuevas en Secure Mail 10.8.55. Para ver los problemas resueltos, consulte Problemas conocidos y problemas resueltos.

**Secure Mail 10.8.50**

**Mejoras para adjuntar fotos**. En Secure Mail para iOS, puede adjuntar fotos fácilmente al tocar en el nuevo icono **Galería**. Toque el icono **Galería** y seleccione las fotos que quiera adjuntar a su correo electrónico.

**Pantalla "Feeds" en Secure Mail**. Secure Mail para iOS y Android destaca todos los correos electrónicos no leídos, las invitaciones a reuniones que requieren su atención y las próximas reuniones en la pantalla **Feeds**.

**Secure Mail 10.8.45**

**Sincronización de carpetas**. En Secure Mail para iOS y Android, puede tocar el icono **Sincronizar** para actualizar todo el contenido de Secure Mail. Encontrará el icono **Sincronizar** en los paneles

deslizables de Secure Mail como Buzones, Calendarios, Contactos y Archivos adjuntos. Cuando toca el icono **Sincronizar**, se actualizan las carpetas que haya configurado para la actualización automática, como Buzones, Calendarios y Contactos. La marca de hora de la última sincronización aparece junto al icono **Sincronizar**.

**Mejoras para adjuntar fotos**. En Secure Mail para Android, puede adjuntar fotos fácilmente al tocar el nuevo icono **Galería**. Toque el icono **Galería** y seleccione las fotos que quiera adjuntar a su correo electrónico.

#### Secure Mail 10.8.40

**Búsquedas en el calendario.** En Secure Mail para iOS, puede buscar eventos, asistentes o cualquier otro texto en el calendario.

#### Secure Mail 10.8.35

La versión de Secure Mail para iOS es 10.8.36.

- **Opciones de respuesta a notificaciones.** En Secure Mail para iOS, los usuarios pueden responder a notificaciones de reunión (Aceptar, Rechazar y Provisional). Pueden responder a notificaciones de mensajes (Responder y Eliminar).
- **Mejoras en el botón Atrás de Secure Mail para Android.** En Secure Mail para Android, puede tocar en el botón Atrás de su dispositivo para descartar las opciones expandidas del botón de acción flotante. Si el botón de acción flotante está en estado expandido, la acción de tocar en el botón Atrás de su dispositivo colapsa las opciones de respuesta. Esta acción lo lleva de vuelta a la vista de detalles del mensaje o evento.
- **En Secure Mail para Android, los botones de respuesta a las reuniones aparecen dentro del correo electrónico.** Cuando reciba una notificación por correo electrónico sobre invitaciones a reuniones, puede responder a la invitación tocando en una de las siguientes opciones:
  - Sí
  - Quizá
  - No

#### Secure Mail 10.8.25

**Ahora Secure Mail para iOS admite S/MIME para las credenciales derivadas:** Para que esta función funcione, debe hacer lo siguiente:

- Seleccione “Credencial derivada” como origen del certificado S/MIME. Para obtener información detallada, consulte Credenciales derivadas para iOS.

- Agregue la propiedad del cliente Atributos LDAP en Citrix Endpoint Management. Use la siguiente información:
  - **Clave:** SEND_LDAP_ATTRIBUTES
  - **Valor:** `userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme=${ user.samaccountname } ,displayName=${ user.displayName } ,mail=${ user.mail }`

Si quiere conocer los pasos para agregar una propiedad del cliente a XenMobile Server, consulte Propiedades de cliente; para agregar una propiedad del cliente a Endpoint Management, consulte Propiedades de cliente.

Para obtener información sobre cómo se inscriben los usuarios con credenciales derivadas, consulte Inscribir dispositivos mediante credenciales derivadas.

1. En la consola de Endpoint Management, vaya a **Configurar > Aplicaciones**.
2. Seleccione **Secure Mail** y haga clic en **Modificar**.
3. En el apartado de la plataforma iOS, en "Origen de certificado S/MIME", seleccione **Credencial derivada**.

**Secure Mail para iOS y Android presenta un nuevo diseño:** Hemos simplificado y hecho más eficiente la navegación del usuario. Hemos alineado el menú y los botones de acción de Secure Mail en forma de una barra de navegación. Para ver un vídeo que demuestre los cambios de navegación del usuario, consulte:

En la siguiente imagen se muestra la nueva barra de navegación en dispositivos iOS.

En la siguiente imagen se muestra la nueva barra de navegación en dispositivos Android.

**Lo que ha cambiado:**

- Se ha eliminado el icono de selección. Las funciones de Secure Mail (Correo, Calendario, Contactos y Adjuntos) están ahora disponibles como botones en la barra de pie de página. En la siguiente imagen se muestra este cambio.

  > **Nota:**
  >
  > En dispositivos Android, la barra de pie de página no está disponible después de abrir un elemento de correo. Por ejemplo, como se muestra en la siguiente imagen, si abre un correo electrónico o un evento de calendario, la barra de pie de página no estará disponible.

- El menú **Parámetros** está disponible en todos los menús (Correo, Calendario, Contactos y Adjuntos). Para ir a **Parámetros**, toque el icono de tres líneas y, a continuación, toque el botón Parámetros, disponible en la parte inferior derecha, como se muestra en la siguiente imagen.
- El icono **Buscar** reemplaza la barra de búsqueda. Ese icono está disponible en las vistas Bandeja de entrada, Contactos y Adjuntos.

- En los dispositivos iOS, puede tocar y mantener presionado un elemento de correo para seleccionarlo.
- Puede tocar en el botón de acción flotante **Redactar** para redactar un nuevo correo electrónico, como se muestra en la siguiente imagen.
- Ahora están disponibles estas opciones de menú en la parte superior derecha de la pantalla:
  - **Opciones de sincronización:** Toque el icono de desbordamiento en la parte superior derecha y vaya a **Más opciones > Opciones de sincronización** para cambiar las preferencias de sincronización.

    > **Nota:**
    >
    > Esta opción solo está disponible en dispositivos Android.

  - **Icono Buscar:** Toque el icono para buscar un correo electrónico concreto.
- **Icono de vista de clasificación:** Toque el icono para clasificar la conversación.
- **Botón de acción flotante para responder:** Cuando consulte un correo electrónico, puede tocar en el icono para Reenviar, Responder a todos o Responder, como se muestra en la siguiente imagen.
- Cuando consulta un correo electrónico, dispone de las siguientes opciones de menú en la parte superior derecha de la pantalla:
  - **Destacar:** Toque el icono para destacar un correo electrónico.
  - **Marcar como no leído:** Toque el icono para marcar el correo electrónico como no leído.
  - **Eliminar:** Toque el icono para eliminar el correo electrónico.
  - **Más opciones:** Toque el icono de desbordamiento para ver otras acciones disponibles, como Mover.

**Cambios en el calendario**

- Desde el calendario, puede tocar en un botón de acción flotante de evento para crear un evento, como se muestra en la siguiente imagen.
- Ahora están disponibles estas opciones de menú en la parte superior derecha de la pantalla:
  - **Hoy:** Toque el icono para ver los eventos de hoy.
  - **Buscar:** Toque el icono para buscar un correo electrónico concreto.
  - **Botón de acción flotante para responder:** Cuando consulte un evento, puede tocar en el icono para Reenviar, Responder a todos o Responder.

Cuando consulta un evento, las acciones de respuesta al evento (Sí, Tal vez y No) se alinean y están disponibles debajo de los detalles del evento.

**Cambios en los contactos**

- Puede tocar en el botón de acción flotante **Crear contacto nuevo**, como se muestra en la siguiente imagen.
- La opción de menú **Buscar** ahora está disponible en la parte superior derecha de la pantalla. Puede tocar en esa opción para buscar un contacto.
- Cuando consulta los datos de un contacto, dispone de las siguientes opciones de menú en la parte superior derecha de la pantalla:

  **En dispositivos Android:**

  - **Modificar:** Toque el icono para modificar los datos del contacto.
  - **Más opciones:** Toque el icono de modificación para ver otras acciones disponibles, como Adjuntar a correo, Compartir o Eliminar.

  **En dispositivos iOS:**

  - **Modificar:** Toque el icono para modificar los datos del contacto.
  - **Compartir:** Toque este icono para ver otras acciones disponibles, como Compartir contacto o Adjuntar a correo.

  > **Nota:**
  >
  > Para eliminar un contacto en dispositivos iOS, seleccione el contacto, toque **Modificar** y luego toque **Eliminar** en la parte inferior de la pantalla, como se muestra en la siguiente imagen.

**Cambios en los adjuntos**

Ahora están disponibles estas opciones de menú para los datos adjuntos, situadas en la parte superior derecha de la pantalla:

- **Ordenar:** Toque el icono **Ordenar** y elija los filtros apropiados para ordenar los adjuntos.
- **Buscar:** Toque el icono para buscar un adjunto concreto.

**Secure Mail 10.8.20**

- Secure Mail para iOS ahora admite el uso de credenciales derivadas para la inscripción y la autenticación. Para obtener más información sobre las credenciales derivadas, consulte Credenciales derivadas para iOS.
- Secure Mail para iOS admite las notificaciones push enriquecidas. Con las notificaciones enriquecidas, se reciben notificaciones en la bandeja de entrada de un dispositivo bloqueado incluso aunque Secure Mail no se esté ejecutando en segundo plano. Esta función se admite con

autenticaciones por contraseña y autenticaciones basadas en el cliente. Para obtener información detallada, consulte Notificaciones push enriquecidas.

> **Nota:**
>
> Debido al cambio en la arquitectura para admitir la función de notificaciones push enriquecidas, las notificaciones de correo **Solo VIP** ya no están disponibles.

- Secure Mail para Android y iOS ahora admite firmas de texto enriquecido. Puede usar imágenes o enlaces en su firma de correo electrónico. Para obtener información detallada, consulte Firmas de texto enriquecido.

#### Secure Mail 10.8.15

- **Secure Mail para iOS ahora admite firmas de texto enriquecido.** Puede usar imágenes o enlaces en su firma de correo electrónico. Para obtener información detallada, consulte Firmas de texto enriquecido.
- **Secure Mail admite Android Enterprise, anteriormente conocido como Android for Work**. Puede crear un perfil de trabajo independiente mediante aplicaciones Android Enterprise en Secure Mail. Para obtener información detallada, consulte Android Enterprise en Secure Mail.
- **Secure Mail genera los recursos incrustados cuando se consulta un correo electrónico.** Si los recursos están presentes en su red interna (como correos electrónicos con URL de imágenes que son enlaces internos), Secure Mail se conecta a la red interna para obtener el contenido y generarlo.
- **Secure Mail admite la autenticación moderna**. La autenticación moderna es una autenticación OAuth basada en token con nombre de usuario y contraseña. Esto admite Office 365 para servicios de federación de Active Directory (AD FS) externos e internos, así como proveedor de identidades (IdP).
- **Mejoras en el rendimiento del repositorio de archivos adjuntos**. Puede desplazarse por el repositorio de archivos adjuntos mucho más rápido.

#### Secure Mail 10.8.10

- **Compatibilidad para imprimir archivos adjuntos de correo electrónico**. Secure Mail para iOS admite la impresión de archivos adjuntos de correo electrónico.
- **Autenticación moderna con Microsoft Office 365**. Secure Mail para iOS admite la autenticación moderna. La autenticación moderna es una autenticación OAuth basada en token con nombre de usuario y contraseña. Se incluye la compatibilidad con Office 365 para servicios de federación de Active Directory (AD FS) externos e internos y con el proveedor de identidades (IdP). Para obtener información detallada, consulte Autenticación moderna con Microsoft Office 365.

> **Notas:**
>
> Esta versión no admite la autenticación moderna junto con la integración de Endpoint Management con Microsoft Intune/EMS.
>
> Esta versión incluye la autenticación moderna en una situación donde ADFS es accesible externamente.

## Problemas conocidos y problemas resueltos

October 19, 2020

Citrix admite actualizaciones desde las dos últimas versiones de las aplicaciones móviles de productividad.

### Secure Mail 20.10.0

#### Problemas conocidos en Secure Mail 20.10.0

En Secure Mail para iOS, falta la opción Subcarpeta (**Carpetas de correo**) en los parámetros de notificaciones. [CXM-85182]

#### Problemas resueltos en Secure Mail 20.10.0

No hay problemas resueltos en esta versión.

### Secure Mail 20.9.5

#### Secure Mail para Android

No hay problemas conocidos ni resueltos en esta versión.

### Secure Mail 20.9.0

#### Problemas conocidos en Secure Mail 20.9.0

En Secure Mail para iOS, falta la opción Subcarpeta (**Carpetas de correo**) en los parámetros de notificaciones. [CXM-85182]

#### Problemas resueltos en Secure Mail 20.9.0

En Secure Mail para iOS, aparece una hora incorrecta (una diferencia de 1 hora) en las invitaciones a reuniones cuando la zona horaria es Arizona. [CXM-86867]

### Problemas conocidos y problemas resueltos en versiones anteriores

Para consultar los problemas conocidos y solucionados en versiones anteriores de Secure Mail, consulte Historial de problemas conocidos y resueltos de Secure Mail.

## Implementar Secure Mail

July 17, 2020

Para implementar Secure Mail con Citrix Endpoint Management (antes XenMobile), siga estos pasos generales:

1. Secure Mail puede integrarse con un servidor Exchange Server o IBM Notes Traveler Server para mantener Secure Mail sincronizado con Microsoft Exchange Server o IBM Notes. Si usa IBM Notes, configure el servidor IBM Notes Traveler Server. La configuración usa las credenciales de Active Directory para la autenticación en Exchange o IBM Notes Traveler. Para obtener información detallada, consulte Integrar Exchange Server o IBM Notes Traveler Server.

   > **Importante:**
   >
   > No puede sincronizar el correo de Secure Mail con IBM Notes Traveler (anteriormente IBM Lotus Notes Traveler). Esta capacidad de terceros de Lotus Notes no se admite actualmente. Por eso, cuando elimina de Secure Mail el correo de una reunión a la que ha respondido, ese correo no se elimina del servidor IBM Notes Traveler. Si los usuarios aceptan un evento de calendario y luego lo rechazan con un comentario o realizan alguna acción con un comentario, el comentario no se incluye. [CXM-47936] Para obtener información acerca de las limitaciones conocidas con IBM/Lotus Notes, consulte esta entrada del blog de Citrix.

2. Si lo prefiere, puede habilitar el inicio SSO desde Secure Hub. Para hacerlo, configure la información de la cuenta de Citrix Files en la consola de Endpoint Management para habilitar Endpoint Management como proveedor de identidades SAML para Citrix Files. En la configuración se usan las credenciales de Active Directory para autenticarse en Citrix Files.

   Configurar la información referente a la cuenta de Citrix Files en Endpoint Management es una operación que solo hay que realizar una vez para todos los clientes Citrix, clientes Citrix Files

y clientes Citrix Files que no son MDX. Para obtener información detallada, consulte Para configurar la información de la cuenta de Citrix Files en la consola de Endpoint Management para SSO.

3. Descargue el archivo MDX de Secure Mail desde el sitio de descargas de Citrix.
4. Agregue Secure Mail a Endpoint Management y configure las directivas MDX. Para obtener información detallada, consulte Agregar aplicaciones.

> Nota:
>
> A partir de Secure Mail 10.6.5, puede configurar una nueva directiva MDX de análisis orientada a Secure Mail para iOS y Android. Citrix recopila datos de análisis para mejorar la calidad del producto. La directiva Google Analytics con nivel de detalle permite especificar si los datos recopilados son anónimos o se pueden asociar a su dominio de empresa. Seleccionar la **recopilación anónima** permite que no se incluya el dominio de empresa de los usuarios en los datos que se recopilan. Esta directiva nueva sustituye a una directiva anterior de Google Analytics.

Cuando la directiva se establece en la recopilación anónima, recopilamos los siguientes tipos de datos. No tenemos manera de vincular estos datos a un usuario o empresa individual porque no solicitamos información que identifique al usuario. No se envía información personal de identidad a Google.

- Estadísticas del dispositivo (como la versión del sistema operativo, la versión de la aplicación y el modelo del dispositivo)
- Información de la plataforma (como la versión de ActiveSync y la versión del servidor Secure Mail)
- Puntos de error para la calidad del producto, como los registros de APNs, la sincronización y el envío de correo, la descarga de datos adjuntos y la sincronización de calendario.

Tenga en cuenta que, cuando la directiva está establecida en la opción de **recopilación completa**, no se recopila ninguna otra información identificable aparte del dominio de empresa. La opción predeterminada es **Completa**.

## Configurar Secure Mail

June 18, 2019

Se pueden configurar e integrar en Secure Mail las siguientes funciones:

- Integrar Secure Mail en Microsoft Intune/EMS
- Autenticación moderna en Office 365
- Servicios en segundo plano para Secure Mail
- Integrar Exchange Server o IBM Notes Traveler Server

- S/MIME para Secure Mail
- Single Sign-On para Secure Mail

## Integrar Secure Mail en Microsoft Intune/EMS

August 21, 2020

Con esta integración, puede administrar y entregar Citrix Secure Mail con más seguridad, al mismo tiempo que dispone de los medios necesarios para mejorar la productividad.

Secure Mail admite varias configuraciones de Microsoft Intune. Puede conectar Secure Mail a buzones locales de Exchange o buzones de Office 365. Para configurar la integración de Endpoint Management con EMS/Intune, consulte Integrar Citrix Endpoint Management en Microsoft Intune/EMS.

Secure Mail admite los siguientes modos de implementación:

- MAM de Intune
- MAM y MDM de Intune
- MAM de Intune con solo MDM de Endpoint Management
- MAM de Intune con MDM y MAM de Endpoint Management

### Servidores de correo compatibles

- Exchange Online
- Exchange Server 2016
- Exchange Server 2013

### Limitaciones

Secure Mail no admite la autenticación basada en certificados.

> **Importante:**
>
> Para usar Secure Mail en modo MDM junto con Citrix Endpoint Management (MDM y MAM), debe configurar Secure Hub en el entorno.

#### Para configurar Secure Mail para Intune

Si el entorno está configurado en el modo MDM de Citrix Endpoint Management, Secure Mail rellena automáticamente los nombres de usuario en una experiencia de primer uso.

Para habilitar esta función, debe configurar directivas personalizadas en la consola de Endpoint Management. Para obtener información detallada, consulte Configurar Secure Mail en la documentación de Endpoint Management.

### Funciones incompatibles con Intune

Las siguientes funciones de Secure Mail no son compatibles con la integración de Endpoint Management en EMS/Intune:

- Secure Ticket Authority (STA)
- Inscripción por correo electrónico con Single Sign-On (SSO)
- Notificaciones push enriquecidas
- Citrix Files (antes ShareFile)
- Cifrado y firma S/MIME
- Microsoft Information Rights Management
- Secure Browse y servidor Exchange interno sin SSO de KCD

## Autenticación moderna en Microsoft Office 365

August 21, 2020

Secure Mail admite la autenticación moderna en Microsoft Office 365 para Servicios de federación de Active Directory (AD FS) o el proveedor de identidades (IdP). La autenticación moderna es una autenticación OAuth basada en token con nombre de usuario y contraseña. Los usuarios de Secure Mail con dispositivos iOS pueden aprovechar las ventajas de la autenticación basada en certificados al conectarse a Office 365. Cuando inician sesión en Secure Mail, los usuarios se autentican con un certificado de cliente, en lugar de escribir sus credenciales.

Antes de continuar, haga lo siguiente:

1. Habilitar la autenticación moderna (OAuth) para Microsoft Office 365.
2. Habilite los dispositivos de punto final, las URL y los intervalos de direcciones IP de Office 365 en su firewall para garantizar una conectividad de red óptima. Para obtener información detallada, consulte la documentación de Microsoft en Direcciones URL e intervalo de direcciones IP de Office 365.

### Requisitos previos de la directiva de Citrix Endpoint Management

Habilite las siguientes directivas en la consola de Citrix Endpoint Management:

**Para dispositivos que ejecutan iOS:**

- **Mecanismo de autenticación de Office 365:** Utilice esta directiva para indicar el mecanismo de OAuth utilizado para la autenticación cuando se configura una cuenta en Office 365. Esta directiva tiene los siguientes valores que debe configurar:
  - **No usar OAuth:** Utilice esta directiva para la autenticación básica durante la configuración de la cuenta.
  - **Usar OAuth con nombre de usuario y contraseña:** Utilice esta directiva para el protocolo OAuth durante la autenticación. Los usuarios deben proporcionar su nombre de usuario y contraseña y, opcionalmente, un código de autenticación de varios factores para el flujo de OAuth.
  - **Usar OAuth con certificado de cliente:** Use esta directiva si Office 365 está configurado para realizar la autenticación basada en certificados. La configuración predeterminada es **No Usar OAuth**.

**Para dispositivos que ejecutan Android:**

- **Usar autenticación moderna para O365:** Utilice esta directiva para el protocolo OAuth durante la autenticación.
- **Agente de usuario personalizado para autenticación moderna:**Utilice esta directiva para cambiar la cadena de agente de usuario predeterminada para la autenticación moderna.
- **Directiva SSO web para tunelización:** Utilice esta directiva para tunelizar el tráfico de OAuth a través de Secure Browse. Para ello:
  - Establezca la directiva **Utilizar SSO web para la tunelización** en **Sí**.
  - En la directiva Acceso de red, seleccione la opción **SSO web en túnel**.
  - Excluya los nombres de host relacionados con OAuth de la directiva **Servicios en segundo plano**.

**Directivas comunes para dispositivos iOS y Android:**

- **Nombres de host Exchange Online de confianza:** Utilice esta directiva para definir una lista de nombres de host Exchange Online de confianza que utilizan el mecanismo OAuth para la autenticación cuando se configura una cuenta. Los elementos de esta lista están separados por comas, como servidor.empresa.com, servidor.empresa.co.uk. Esta lista puede contener un valor predeterminado o una URL mnemónica, pero no puede estar vacía. El valor predeterminado es **outlook.office365.com**.
- **Nombres de host AD FS de confianza**: utilice esta directiva para definir una lista de nombres de host AD FS de confianza para las páginas web donde la contraseña se rellena automáticamente durante la autenticación OAuth de Office 365. Este es un formato separado por comas, como `sts.companyname.com`, `sts.company.co.uk`. Si la lista está vacía, Secure Mail no rellena automáticamente las contraseñas. Secure Mail coteja los nombres de host de la lista con el nombre de host de la página web encontrada durante la autenticación de Office 365 y comprueba si la página usa el protocolo HTTPS. Por ejemplo, cuando `sts.company.com` es un nombre de host de la lista, y el usuario va a `https://sts.company.com`, Secure Mail rellena

la contraseña siempre que la página tenga un campo de contraseña. El valor predeterminado es `login.microsoftonline.com`.

- **Secure Mail Exchange Server:** Utilice esta directiva para definir la dirección de su Exchange Server. Puede utilizar esta directiva para definir la dirección del servidor local o la dirección del servidor en la nube, conforme a sus requisitos.

Secure Mail para iOS ahora tiene habilitada la autenticación moderna cuando las directivas se actualizan en el dispositivo.

## Limitaciones

- Si está utilizando la autenticación moderna en su entorno, la función Notificaciones push enriquecidas para iOS no está disponible. Para obtener información detallada sobre las notificaciones push enriquecidas, consulte Notificaciones push para Secure Mail.
- No se admiten varias cuentas en configuraciones que ejecuten una autenticación basada en certificados.

### Directivas de Secure Mail

En las siguientes tablas se indican las directivas de Secure Mail que se requieren en función de la infraestructura de Exchange:

| Infraestructura de Exchange | Mecanismo de autenticación de Office 365 / Usar autenticación moderna para O365 | Nombres de host AD FS Online de confianza. | Nombres de host Exchange Online de confianza |
|---|---|---|---|
| Local | NO | N/A | N/A |
| Híbrido* | SÍ | AD FS/IDP | `Outlook.office365.com` o dirección URL mnemónica |
| Exchange Online | SÍ | AD FS/IDP | `Outlook.office365.com` o dirección URL mnemónica |

| Infraestructura de Exchange | Servidor Exchange de Secure Mail | Servicios de red en segundo plano (iOS) | Servicios de red en segundo plano (Android) |
|---|---|---|---|
| Local | Nombre de host local de Exchange | Local | Local |
| Híbrido* | local, nombres de host de Exchange Online | Local, nombre de host local de Exchange | Local, nombre de host local de Exchange, AD FS o IdP (solo interno) |
| Exchange Online | `Outlook.office365.com` | Nombres de host Exchange Online | Nombre de host local de Exchange, AD FS, IdP |

* Secure Mail admite una infraestructura híbrida de Exchange con buzones migrados.

Si el buzón de los usuarios locales se migra a Exchange Online, Secure Mail detecta automáticamente este cambio y solicita a los usuarios la autenticación moderna sin la necesidad de reconfigurar su cuenta.

**Tabla de compatibilidad de Secure Mail con OAuth**

La siguiente tabla enumera la compatibilidad de Secure Mail OAuth en dispositivos iOS y Android:

| Tipo de autenticación | IdP o AD FS externos | IdP o AD FS internos | Azure AD | Microsoft Intune |
|---|---|---|---|---|
| Nombre de usuario y contraseña | Sí | Sí | Sí | Sí |
| Certificado de cliente | Sí | Solo Android | No | No |

## Servicios en segundo plano para Secure Mail

August 21, 2020

Para acceder a su servidor de correo a través de Citrix Gateway, debe configurar los servicios en segundo plano para Secure Mail. Cuando agrega Secure Mail a Citrix Endpoint Management (anterior-

mente conocido como XenMobile), configure los servicios en segundo plano en los parámetros de directivas de la aplicación MDX.

### Para configurar los servicios en segundo plano para Secure Mail

1. Inicie sesión en la consola de Endpoint Management mediante las credenciales de administrador.
2. En la consola, haga clic en la ficha **Configurar**, luego en **Aplicaciones**, y, a continuación, seleccione la aplicación Secure Mail y haga clic en **Modificar**.
3. En la página **Configuraciones de directivas de MDX**, en la sección **Plataforma** seleccione la plataforma iOS o Android, según sea necesario.
4. En la sección **Configuraciones de aplicaciones**, configure las directivas.

### Directivas de aplicaciones MD para la configuración de los servicios en segundo plano

Las siguientes directivas de la aplicación MDX afectan a la comunicación de Secure Mail con Citrix Gateway, el servidor Citrix Endpoint Management, los servidores Secure Ticket Authority (STA) y el servidor de correo electrónico.

**Acceso de red:** La directiva de acceso de red especifica si Secure Mail puede usar una red privada virtual (VPN) para acceder a los servicios de la red en segundo plano o si todo el tráfico pasa sin restricciones a través de Internet.

- Si la directiva de acceso de red se establece en **Túnel a la red interna** , solo las URL que figuren en los servicios de red en segundo plano pasan a través de Citrix Gateway. El resto del tráfico pasa sin restricciones a través de Internet. De forma predeterminada, el acceso a Secure Mail se hace por **túnel a la red interna**.
- Si la directiva de acceso de red se establece en **Sin restricciones**, todo el tráfico que se origina en Secure Mail se envía sin restricciones a través de Internet. La red privada virtual (VPN) no se utiliza para acceder a servicios en segundo plano.

**Para el servidor Secure Mail Exchange:** Establezca la directiva **Servidor Exchange de Secure Mail** en el nombre de dominio completo (FQDN) del servidor de correo electrónico.

**Servicio de red en segundo plano:** La directiva de servicio de red en segundo plano especifica la lista de servidores de correo que pueden acceder a través de Citrix Gateway. Enumere los nombres de host y el número de puerto como un valor separado por comas. Asegúrese de que no haya espacios iniciales y finales entre los valores. Para las direcciones del servidor de correo, incluya: `hostnameFQDN:portnumber`. Por ejemplo: `mail1.example.com:443,mail2.example.com:443` (sin espacios entre las comas).

**Puerta de enlace de servicio de red en segundo plano:** Use la directiva "Puerta de enlace de servicio de red en segundo plano" para especificar el Citrix Gateway que usará Secure Mail para conectarse al servidor de correo. Para las direcciones de Citrix Gateway, incluya: `citrixgatewayFQDN :portnumber`. Por ejemplo: `gateway3.example.com:443`.

**Caducidad del tíquet de servicios en segundo plano:** Esta directiva especifica el periodo de validez del tíquet del servicio de red en segundo plano. Cuando Secure Mail se conecta a través de Citrix Gateway a un servidor de correo, Citrix Endpoint Management emite un token que se usa para conectarse al servidor de correo interno. Esta directiva determina el tiempo durante el que Secure Mail podrá utilizar este token. No se requiere un token para autenticarse y conectarse al servidor de correo si el token está activo. Cuando se alcanza el límite de tiempo, los usuarios deben volver a iniciar sesión para generar un nuevo token. El valor predeterminado de este token es 168 horas (7 días).

Para obtener más información sobre las directivas de aplicaciones MDX para los servicios en segundo plano, consulte:

- Directivas de configuración de la aplicación de Secure Mail para Android
- Directivas de configuración de la aplicación Secure Mail para iOS

La siguiente imagen muestra el flujo de comunicación y dónde se pueden aplicar estas directivas.

En las siguientes ilustraciones, se muestran los tipos de conexiones de Secure Mail a un servidor de correo. Después de cada ilustración hay una lista de las configuraciones de directiva relacionadas.

**Conexión directa con un servidor de correo:**

Directivas para una conexión directa con un servidor de correo:

- Acceso de red: **Sin restricciones**

Si el acceso de red no tiene restricciones, las siguientes directivas no son aplicables:

- Servicios de red en segundo plano: N/A
- Caducidad del tíquet de servicios en segundo plano: N/A
- Puerta de enlace de servicio de red en segundo plano: N/A

**Conexión a un servidor de correo a través de STA:**

Directivas para conectarse a un servidor de correo a través de STA:

- Acceso de red: **Túnel a la red interna**
- Servicios de red en segundo plano: `mail.example.com:443,mail1.example1.com:443`
- Caducidad del tíquet de servicios en segundo plano: **168**
- Puerta de enlace de servicio de red en segundo plano: `gateway3.example.com:443`

> Nota:
>
> Citrix recomienda el uso de una conexión STA para Secure Mails porque admite conexiones a sesiones duraderas.

Para obtener más información sobre STA, consulte este artículo de Citrix Knowledge Center.

## Integrar Exchange Server o IBM Notes Traveler Server

June 18, 2019

Para mantener Secure Mail sincronizado con los servidores de correo, Secure Mail se puede integrar en un servidor Exchange o IBM Notes Traveler que resida en la red interna o esté detrás de Citrix Gateway.

- Para configurar los servicios en segundo plano para Secure Mail, consulte Servicios en segundo plano para Secure Mail.
- Para configurar IBM Notes Traveler Server para Secure Mail, consulte Configurar IBM Notes Traveler Server para Secure Mail.

> **Importante:**
>
> No puede sincronizar el correo de Secure Mail con IBM Notes Traveler (anteriormente IBM Lotus Notes Traveler). Esta capacidad de terceros de Lotus Notes no se admite actualmente. Por eso, cuando elimina por ejemplo un correo de reunión de Secure Mail, ese correo no se elimina del servidor IBM Notes Traveler. [CXM-47936]
> Para obtener información acerca de las limitaciones conocidas con IBM/Lotus Notes, consulte esta entrada del blog de Citrix.

La sincronización también está disponible para Secure Notes y Secure Tasks. Cabe señalar, sin embargo, que Secure Notes y Secure Tasks han alcanzado el estado Fin de vida (EOL) el 31 de diciembre de 2018. Para obtener información detallada, consulte Fin de vida y aplicaciones retiradas.

- Si quiere sincronizar Secure Notes para iOS, intégrelo en un servidor Exchange.
- Si quiere sincronizar Secure Notes y Secure Tasks para Android, utilice la cuenta de Secure Mail para Android.

Cuando agregue Secure Mail, Secure Notes y Secure Tasks a Citrix Endpoint Management (anteriormente conocido como XenMobile), configure las directivas MDX como se indica en Directivas de aplicaciones MD para la configuración de los servicios en segundo plano.

> **Nota:**
>
> Secure Mail para Android y Secure Mail para iOS admiten la ruta completa especificada de un servidor Notes Traveler. Por ejemplo: `https://mail.example.com/traveler/Microsoft-Server-ActiveSync`.
>
> Ya no es necesario configurar el directorio de Domino con las reglas de sustitución de sitios web para Traveler Server.

## Configurar IBM Notes Traveler Server para Secure Mail

En los entornos de IBM Notes, es necesario configurar el servidor IBM Notes Traveler antes de implementar Secure Mail. En esta sección se muestra una imagen de la implementación de esta configuración, así como los requisitos del sistema.

> **Importante:**
>
> Si el servidor Notes Traveler usa SSL 3.0, tenga en cuenta que SSL 3.0 contiene una vulnerabilidad conocida como ataque POODLE (Padding Oracle On Downgraded Legacy Encryption), que es un ataque de tipo intermediario que afecta a cualquier aplicación que se conecta a un servidor mediante SSL 3.0. Para evitar la vulnerabilidad introducida por el ataque POODLE, Secure Mail inhabilita las conexiones SSL 3.0 de manera predeterminada y usa TLS 1.0 para conectarse al servidor. Por eso, Secure Mail no puede conectarse a servidores Notes Traveler que usen SSL 3.0. Para obtener información detallada sobre una solución temporal recomendada, consulte la sección Configurar el nivel de seguridad de SSL/TLS en Integrar Exchange Server o IBM Notes Traveler Server.

En los entornos de IBM Notes, es necesario configurar el servidor IBM Notes Traveler antes de implementar Secure Mail.

En la imagen siguiente se muestra la ubicación en la red de los servidores IBM Notes Traveler y un servidor de correo IBM Domino en un entorno de ejemplo.

## Requisitos del sistema

### Requisitos del servidor de infraestructura

- IBM Domino Mail Server 9.0.1
- IBM Notes Traveler 9.0.1

### Protocolos de autenticación

- Base de datos de Domino
- Protocolo de autenticación de Lotus Notes
- Protocolo de autenticación de Lightweight Directory

### Requisitos de puertos

- Exchange: el puerto SSL predeterminado es 443.
- IBM Notes: SSL se admite en el puerto 443. Sin SSL se admite, de forma predeterminada, en el puerto 80.

### Configurar el nivel de seguridad de SSL/TLS

Citrix ha realizado modificaciones en Secure Mail para solventar las vulnerabilidades introducidas por los ataques POODLE, como se describe en la nota “Importante” mencionada anteriormente. Por lo tanto, si su servidor Notes Traveler usa SSL 3.0, para habilitar las conexiones la solución recomendada es utilizar TLS 1.2 en el servidor IBM Notes Traveler 9.0.

IBM dispone de una revisión para impedir el uso de SSL 3.0 en las comunicaciones seguras de servidor a servidor de Notes Traveler. La revisión, publicada en noviembre de 2014, viene incluida como actualización intermedia en las siguientes versiones del servidor Notes Traveler: 9.0.1 IF7, 9.0.0.1 IF8 y 8.5.3 Upgrade Pack 2 IF8 (y será incluida en futuras versiones también). Para obtener información detallada sobre el parche, consulte LO82423: DISABLE SSLV3 FOR TRAVELER SERVER TO SERVER COMMUNICATION.

Como solución temporal, cuando agregue Secure Mail a Endpoint Management, cambie la directiva “Nivel de seguridad de la conexión” a **SSLv3 y TLS**. Para obtener la información más reciente sobre este problema, consulte Conexiones SSLv3 inhabilitadas de forma predeterminada en Secure Mail 10.0.3.

En la siguiente tabla, se indican los protocolos que admite Secure Mail por sistema operativo, según el valor que tenga la directiva “Nivel de seguridad de la conexión”. Su servidor de correo electrónico también debe ser capaz de negociar el protocolo.

En la siguiente tabla se muestran los protocolos admitidos en Secure Mail cuando el nivel de seguridad de conexión es SSL 3 y TLS.

| Tipo de sistema operativo | SSLv3 | TLS |
|---|---|---|
| iOS 9 y posterior | No | Sí |
| Anterior a Android M | Sí | Sí |
| Android M y Android N | Sí | Sí |
| Android O | No | Sí |

En la siguiente tabla se muestran los protocolos admite en Secure Mail cuando el nivel de seguridad de la conexión es TLS.

| Tipo de sistema operativo | SSLv3 | TLS |
|---|---|---|
| iOS 9 y posterior | No | Sí |
| Anterior a Android M | No | Sí |
| Android M y Android N | No | Sí |

| | | |
|---|---|---|
| Tipo de sistema operativo | SSLv3 | TLS |
| Android O | No | Sí |

### Configurar Notes Traveler Server

La siguiente información corresponde a las páginas de configuración en el cliente IBM Domino Administration.

- **Security:** La autenticación de Internet está establecida en “Fewer name variations with higher security”. Este parámetro se utiliza para asignar un UID a un ID de usuario de AD en los protocolos de autenticación de LDAP.
- **NOTES.INI Settings:** Agregue **NTS_AS_ENFORCE_POLICY**=**false**. Eso permite administrar las directivas de Secure Mail a través de Endpoint Management, en lugar de Traveler. Esta configuración puede entrar en conflicto con las implementaciones actuales del cliente, pero simplificará la administración del dispositivo en implementaciones de Endpoint Management.
- **Synchronization protocols:** Por el momento, Secure Mail no admite SyncML en IBM Notes ni la sincronización de dispositivos móviles. Secure Mail sincroniza elementos de correo, calendario y contactos a través del protocolo de Microsoft ActiveSync integrado en los servidores Traveler. Si se fuerza SyncML como protocolo principal, Secure Mail no se podrá conectar a través de la infraestructura de Traveler.
- **Domino Directory Configuration - Web Internet Sites:** Invalidar la autenticación de sesión para /traveler con el fin de inhabilitar la autenticación por formularios.

## S/MIME para Secure Mail

July 17, 2020

Secure Mail admite Secure/Multipurpose Internet Mail Extensions (S/MIME), que permite a los usuarios firmar y cifrar mensajes para mayor seguridad. La firma asegura al destinatario que el mensaje fue enviado por el remitente identificado, no por un impostor. El cifrado permite que solo los destinatarios que tienen un certificado compatible puedan abrir el mensaje.

Para obtener más información acerca de S/MIME, consulte Microsoft TechNet.

En la siguiente tabla, una X indica que Secure Mail admite una función S/MIME en un sistema operativo de dispositivo.

| Función de S/MIME | iOS | Android |
| --- | --- | --- |
| **Integrar con proveedores de identidades digitales:** Puede integrar Secure Mail en un proveedor de identidades digitales de terceros. El host del proveedor de identidades proporciona certificados para una aplicación de proveedor de identidades en los dispositivos de los usuarios. Esa aplicación envía certificados a una caja fuerte compartida de Endpoint Management, que es una zona de almacenamiento segura para datos de aplicaciones confidenciales. Secure Mail obtiene certificados de la caja fuerte compartida. Para obtener información detallada, consulte Integrar con un proveedor de identidades digitales. | X | |
| **Compatibilidad con credenciales derivadas** | Secure Mail admite credenciales derivadas como origen de certificado. Para obtener más información sobre las credenciales derivadas, consulte Credenciales derivadas para iOS. | |

| Función de S/MIME | iOS | Android |
| --- | --- | --- |
| **Distribuir certificados por correo electrónico:** La distribución de certificados por correo electrónico requiere crear primero plantillas de certificado y luego usarlas para solicitar certificados de usuario. Después de instalar y validar los certificados, debe exportar los certificados de usuario y, a continuación, enviarlos por correo electrónico a los usuarios. Luego, los usuarios abren el correo electrónico en Secure Mail e importan los certificados. Para obtener información detallada, consulte Distribuir certificados por correo electrónico. | X | X |
| **Importación automática de certificados para fines específicos:** Secure Mail detecta si un certificado solo es para firma o para cifrado, lo importa automáticamente y notifica al usuario. Si un certificado sirve para ambos fines, se pregunta a los usuarios si quieren importarlo. | X | |

### Integrar con un proveedor de identidades digitales

En el siguiente diagrama, se muestra la ruta que recorre un certificado desde el host del proveedor de identidades digitales hasta Secure Mail. Eso ocurre cuando Secure Mail se integra con un proveedor externo admitido de identidades digitales.

La caja fuerte compartida MDX es una zona de almacenamiento segura donde se guardan datos confidenciales de aplicaciones, tales como certificados. Solo la aplicación que Endpoint Management habilite puede acceder a la caja fuerte compartida.

### Requisitos previos

Secure Mail admite la integración con Entrust IdentityGuard.

### Configurar la integración

1. Prepare la aplicación del proveedor de identidades y entréguela a los usuarios:
    - Póngase en contacto con Entrust para obtener el archivo IPA a empaquetar.
    - Use MDX Toolkit para empaquetar la aplicación.

      Para implementar esta aplicación en dispositivos de usuario que ya tienen una versión de la aplicación fuera del entorno Endpoint Management, utilice un ID de aplicación único para ella. Utilice el mismo perfil de aprovisionamiento para esa aplicación que para Secure Mail.
    - Agregue la aplicación a Endpoint Management y publíquela en el almacén de aplicaciones de Endpoint Management.
    - Indique a los usuarios que deben instalar la aplicación del proveedor de identidades desde Secure Hub. Proporcione instrucciones, según sea necesario, sobre los pasos posteriores a la instalación.

      Según cómo se configuren las directivas de S/MIME para Secure Mail en el paso siguiente, Secure Mail podrá pedir a los usuarios que instalen los certificados o habiliten S/MIME en los parámetros de Secure Mail. Los pasos para los dos procedimientos están descritos en Habilitar S/MIME en Secure Mail para iOS.
2. Cuando agregue Secure Mail a Endpoint Management, configure estas directivas:
    - Establezca la directiva “Origen de certificado S/MIME” en **Caja fuerte compartida**. Este parámetro significa que Secure Mail usa los certificados que su proveedor de identidades digitales guarda en su caja fuerte compartida.
    - Para habilitar S/MIME durante la configuración inicial de Secure Mail, configure la directiva “Habilitar S/MIME durante el primer inicio de Secure Mail”. Esta directiva determina

si Secure Mail habilita S/MIME cuando haya certificados en la caja fuerte compartida. Si no hay certificados disponibles, Secure Mail pide al usuario que importe certificados. Si la directiva no está habilitada, los usuarios pueden habilitar S/MIME en los parámetros de Secure Mail. De forma predeterminada, Secure Mail no habilita S/MIME, lo que significa que los usuarios deben habilitarlo desde los parámetros de Secure Mail.

### Usar credenciales derivadas

En lugar de integrarse en un proveedor de identidades digitales, puede permitir el uso de credenciales derivadas.

Cuando agregue Secure Mail a Endpoint Management, establezca la directiva "Origen de certificado S/MIME" en **Credenciales derivadas**. Para obtener más información sobre las credenciales derivadas, consulte Credenciales derivadas para iOS.

### Distribuir certificados por correo electrónico

En lugar de integrarse en un proveedor de identidades digitales o usar credenciales derivadas, puede optar por distribuir los certificados a los usuarios por correo electrónico. Esta opción requiere los siguientes pasos generales, descritos en esta sección.

1. Use el Administrador del servidor para habilitar la inscripción para los Servicios de certificados de Microsoft y para verificar su configuración de autenticación en IIS.
2. Cree plantillas de certificado para firmar y cifrar mensajes de correo electrónico. Use esas plantillas para solicitar certificados de usuario.
3. Instale y valide los certificados y, a continuación, exporte los certificados de usuario y envíelos por correo electrónico a los usuarios.
4. Los usuarios abren el mensaje en Secure Mail e importan los certificados. De este modo, los certificados están disponibles solo para Secure Mail. No aparecen en el perfil iOS de S/MIME.

### Requisitos previos

Las instrucciones de esta sección se basan en los siguientes componentes:

- XenMobile Server 10 y posterior
- Una versión compatible de Citrix Gateway, anteriormente conocido como NetScaler Gateway
- Secure Mail para iOS (versión mínima 10.8.10); Secure Mail para Android (versión mínima 10.8.10)
- Microsoft Windows Server 2008 R2 o posterior con los Servicios de certificados de Microsoft actuando como entidad de certificación (CA) raíz
- Microsoft Exchange:
  - Exchange Server 2016 Cumulative Update 4

  - Exchange Server 2013 Cumulative Update 15
  - Exchange Server 2010 SP3 Update Rollup 16

Complete los siguientes requisitos previos antes de configurar S/MIME:

- Entregue los certificados raíz e intermedios a los dispositivos móviles, ya sea manualmente o a través de una directiva de credenciales en Endpoint Management. Para obtener información detallada, consulte Directiva Credenciales.
- Si utiliza certificados de servidor privados para proteger el tráfico de ActiveSync hacia Exchange Server, debe instalar todos los certificados raíz e intermedios en los dispositivos móviles.

### Habilitar la inscripción web para los Servicios de certificados de Microsoft

1. Vaya a **Herramientas administrativas** y seleccione **Administrador del servidor**.
2. En **Servicios de certificados de Active Directory**, compruebe si **Inscripción web de entidad de certificación** está instalada.
3. Seleccione **Agregar servicios de rol** para instalar la inscripción web de entidad de certificación, si es necesario.
4. Seleccione **Inscripción web de entidad de certificación** y haga clic en **Siguiente**.
5. Cuando termine la instalación, haga clic en **Cerrar** o **Finalizar**.

### Verificar los parámetros de autenticación en IIS

- Compruebe que el sitio web de inscripción usado para solicitar certificados de usuario (por ejemplo, `https://ad.domain.com/certsrv/`) está protegido con un certificado de servidor HTTPS (público o privado).
- Es necesario acceder al sitio de inscripción web a través de HTTPS.

1. Vaya a **Herramientas administrativas** y seleccione **Administrador del servidor**.
2. En **Servidor web (IIS)**, mire en **Servicios de rol**. Compruebe que Autenticación de asignaciones de certificado de cliente y Autenticación de asignaciones de certificado de cliente de IIS estén instalados. Si no lo están, instale esos servicios de rol.
3. Vaya a **Herramientas administrativas** y seleccione **Administrador de Internet Information Services (IIS)**.
4. En el panel izquierdo de la ventana del **Administrador de IIS**, seleccione el servidor que ejecuta la instancia de IIS para la inscripción web.
5. Haga clic en **Autenticación**.
6. Compruebe que **Autenticación de certificados de cliente de Active Directory** tiene el valor **Habilitado**.
7. Haga clic en **Sitios > Sitio predeterminado para Microsoft Internet Information Services > Enlaces** en el panel derecho.
8. Si no existe ningún enlace HTTPS, agregue uno.

9. Vaya a Sitio web predeterminado.
10. Haga clic en **Configuración de SSL** y, a continuación, haga clic en **Aceptar para Certificados de cliente**.

### Crear plantillas de certificado

Con el fin de firmar y cifrar mensajes de correo electrónico, Citrix recomienda crear certificados en Servicios de certificados de Active Directory de Microsoft. Si utiliza el mismo certificado para ambos propósitos y archiva el certificado de cifrado, es posible recuperar un certificado de firma y permitir la suplantación.

El siguiente procedimiento duplica las plantillas de certificado en el servidor de la entidad de certificación (CA):

- Solo la firma de Exchange (para firmar)
- Usuario de Exchange (para cifrado)

1. Abra el complemento Entidad de certificación.
2. Expanda Entidad de certificación y vaya a **Plantillas de certificado**.
3. Haga clic con el botón secundario y, a continuación, haga clic en **Administrar**.
4. Busque la plantilla “Solo la firma de Exchange”, haga clic con el botón secundario en ella y haga clic en **Duplicar plantilla**.
5. Asígnele el nombre que quiera.
6. Marque la casilla **Publicar certificado en Active Directory**.

   > **Nota:**
   >
   > Si no marca la casilla **Publicar certificado en Active Directory**, los usuarios deberán publicar manualmente los certificados de usuario (para firma y cifrado). Pueden hacerlo desde **Cliente de correo Outlook > Centro de confianza > Seguridad del correo electrónico > Publicar en GAL (lista global de direcciones)**.

7. Haga clic en la ficha **Administración de solicitudes** y configure los siguientes parámetros:
   - **Propósito:** Firma
   - **Tamaño mínimo de clave:** 2048
   - **Permitir que la clave privada se pueda exportar:** Casilla marcada
   - **Inscribir el sujeto sin exigir ninguna acción por parte del usuario:** Casilla marcada
8. Haga clic en la ficha **Seguridad** y, en **Nombres de grupos o usuarios**, compruebe que se ha agregado el grupo de seguridad de dominio **Usuarios autenticados** (o cualquier otro). Asimismo, compruebe que, en **Permisos para Usuarios autenticados**, las casillas **Leer e Inscribir** están marcadas con **Permitir**.

9. En todas las demás fichas y parámetros, deje los valores predeterminados.
10. En **Plantillas de certificado**, haga clic en **Usuario de Exchange** y luego repita los pasos del 4 al 9.

    Para la nueva plantilla de Usuario de Exchange, use los mismos parámetros predeterminados que los de la plantilla original.
11. Haga clic en la ficha **Administración de solicitudes** y configure los siguientes parámetros:
    - **Propósito:** Cifrado
    - **Tamaño mínimo de clave:** 2048
    - **Permitir que la clave privada se pueda exportar:** Casilla marcada
    - **Inscribir el sujeto sin exigir ninguna acción por parte del usuario:** Casilla marcada
12. Una vez creadas ambas plantillas de certificado, asegúrese de emitirlas. Seleccione **Nueva** y, a continuación, haga clic en **Plantilla de certificado que se va a emitir**.

### Solicitar certificados de usuario

En este procedimiento se utiliza “user1” para ir a la página de inscripción web; por ejemplo, `https://ad.domain.com/certsrv/`. El procedimiento solicita dos nuevos certificados de usuario para correo electrónico seguro: un certificado de firma y otro de cifrado. Puede repetir el mismo procedimiento para otros usuarios del dominio que requieran el uso de S/MIME con Secure Mail.

Para generar los certificados de usuario para firma y cifrado, se usa la inscripción manual a través del sitio web de inscripción (por ejemplo: `https://ad.domain.com/certsrv/`) en Microsoft Certificate Services. Una alternativa es configurar la autoinscripción a través de una directiva de grupo para el grupo de usuarios que pueden usar esta funcionalidad.

1. En un equipo Windows, abra Internet Explorer y vaya al sitio web de inscripciones para solicitar un nuevo certificado de usuario.

   > **Nota:**
   >
   > Debe iniciar sesión con la cuenta de usuario de dominio correcta para solicitar el certificado.
2. Cuando haya iniciado sesión, haga clic en **Solicitar un certificado**.
3. Haga clic en **Solicitud avanzada de certificado**.
4. Haga clic en **Crear y enviar una solicitud a esta CA**.
5. Genere el certificado de usuario para firma. Seleccione el nombre de la plantilla adecuada, escriba su configuración de usuario y, junto a **Formato de solicitud**, seleccione **PKCS10**.

   Con ello, se envía la solicitud.

6. Haga clic en **Instalar este certificado**.
7. Compruebe que el certificado se ha instalado correctamente.
8. Repita el procedimiento, pero ahora para cifrar mensajes de correo electrónico. Con el mismo nombre de usuario que ha iniciado sesión en el sitio web de inscripción, vaya al enlace Home para solicitar un nuevo certificado.
9. Seleccione la nueva plantilla de cifrado y, a continuación, escriba los mismos parámetros de usuario que introdujo en el paso 5.
10. Compruebe que el certificado se ha instalado correctamente y luego repita el mismo procedimiento para generar otro par de certificados de usuario para otro usuario de dominio. Este ejemplo sigue el mismo procedimiento y genera un par de certificados para “User2”.

> **Nota:**
>
> En este procedimiento se utiliza el mismo equipo Windows para solicitar el segundo par de certificados para “User2”.

### Validar certificados publicados

1. Para comprobar que los certificados se han instalado correctamente en el perfil del usuario de dominio, vaya a **Usuarios y equipos de Active Directory > Ver > Características avanzadas**.
2. Vaya a las propiedades del usuario (User1 en este ejemplo) y haga clic en la ficha **Certificados publicados**. Ambos certificados deben estar disponibles. También puede verificar si cada certificado tiene un uso específico.

   Esta ilustración muestra un certificado para cifrar mensajes de correo electrónico.

   Esta ilustración muestra un certificado para firmar mensajes de correo electrónico.

   Compruebe que se ha asignado el certificado de cifrado correcto al usuario. Puede verificar esta información en **Usuarios y equipos de Active Directory > propiedades del usuario**.

   Secure Mail comprueba el atributo userCertificate del objeto de usuario mediante consultas de LDAP. Este valor se encuentra en la ficha **Editor de atributos**. Si este campo está vacío o tiene un certificado de usuario para cifrado que no es correcto, Secure Mail no podrá cifrar ni descifrar mensajes.

### Exportar certificados de usuario

Este procedimiento exporta los pares de certificados de “User1” y User2” en el formato PFX (PKCS#12) junto con la clave privada. Cuando se exportan, los certificados se envían por correo electrónico al usuario a través de Outlook Web Access (OWA).

1. Abra la consola de MMC y vaya al complemento para **Certificados: usuario actual**. Verá los pares de certificados de “User1” y User2”.
2. Haga clic con el botón secundario en el certificado y seleccione **Todas las tareas > Exportar**.
3. Exporte la clave privada seleccionando **Exportar la clave privada**.
4. Marque las casillas **Si es posible, incluir todos los certificados en la ruta de acceso de certificación** y **Exportar todas las propiedades extendidas**.
5. Cuando exporte el primer certificado, repita el mismo procedimiento para el resto de los certificados de los usuarios.

   > **Nota:**
   >
   > Etiquete claramente cuál es el certificado de firma y cuál es el certificado de cifrado. En este ejemplo, los certificados se han etiquetado como “userX-sign.pfx” y “userX-enc.pfx”.

### Enviar certificados a través de correo electrónico

Una vez exportados todos los certificados en formato PFX, puede usar Outlook Web Access (OWA) para enviarlos por correo electrónico. El nombre de inicio de sesión utilizado en este ejemplo es User1. El mensaje enviado contiene ambos certificados de este usuario.

Repita el procedimiento para User2 u otros usuarios en el dominio.

### Habilitar S/MIME en Secure Mail para iOS y Android

Una vez entregado el mensaje de correo electrónico, el siguiente paso es abrirlo con Secure Mail y, a continuación, habilitar S/MIME con los certificados apropiados para la firma y el cifrado.

#### Para habilitar S/MIME con certificados individuales de firma y cifrado

1. Abra Secure Mail, vaya al correo electrónico que contiene los certificados S/MIME.
2. Toque en el certificado de firma a descargar e importar.
3. Escriba la contraseña asignada a la clave privada cuando el certificado de firma se exportó desde el servidor.

   La importación del certificado se ha completado.
4. Toque en **Activar firma**.
5. Como alternativa, puede ir a **Configuración** (o “Ajustes”) > **S/MIME** y tocar en “S/MIME” para activar el certificado de firma.
6. En la pantalla **Firma**, verifique que se ha importado el certificado de firma correcto.

7. Vuelva al correo electrónico y toque en el certificado de cifrado a descargar e importar.
8. Escriba la contraseña asignada a la clave privada cuando el certificado de cifrado se exportó desde el servidor.

   La importación del certificado se ha completado.
9. Toque en **Activar cifrado**.
10. Como alternativa, puede ir a **Ajustes** (o "Configuración") > **S/MIME** y tocar en "S/MIME" para habilitar **Cifrar de forma predeterminada**.
11. En la pantalla **Cifrado**, verifique que se ha importado el certificado de cifrado correcto.

> **Nota:**
>
> a) Si un correo electrónico está firmado digitalmente con S/MIME y tiene datos adjuntos, pero el destinatario no tiene S/MIME habilitado, los datos adjuntos no se reciben. Este comportamiento es una limitación de ActiveSync. Para recibir correctamente mensajes S/MIME, active S/MIME en los parámetros de Secure Mail.
>
> b) La opción **Cifrar de forma predeterminada** permite minimizar los pasos necesarios para cifrar el correo electrónico. Si esta función está activada, su correo electrónico estará en el estado de cifrado mientras lo redacta. En cambio, si esta función está desactivada, su correo electrónico estará en el estado sin cifrar mientras lo redacta; deberá tocar en el icono **Bloquear** para cifrarlo.

**Para habilitar S/MIME con un solo certificado de firma y cifrado**

1. Abra Secure Mail, vaya al correo electrónico que contiene el certificado S/MIME.
2. Toque en el certificado S/MIME a descargar e importar.
3. Escriba la contraseña asignada a la clave privada cuando el certificado se exportó desde el servidor.
4. De las opciones de certificado que aparecen, toque en la opción apropiada para importar el certificado de firma o cifrado.
   Toque en **Abrir certificado** para ver detalles sobre el certificado.

   La importación del certificado se ha completado.

   Los certificados importados se encuentran en **Ajustes (o "Configuración") > S/MIME**.

## Probar S/MIME en iOS y Android

Una vez que haya realizado los pasos indicados en la sección anterior, su destinatario puede leer el correo firmado y cifrado que le envíe.

En la siguiente imagen se muestra el ejemplo de un mensaje cifrado tal y como lo leerá el destinatario.

En la siguiente imagen se muestra un ejemplo de verificación del certificado firmado de confianza.

Secure Mail busca los certificados públicos de cifrado de los destinatarios en el dominio de Active Directory. Si un usuario envía un mensaje cifrado a un destinatario que no tiene una clave de cifrado pública válida, el mensaje se envía sin cifrar. Cuando se envía un mensaje de grupo, si un destinatario no tiene una clave válida, el mensaje se envía sin cifrar a todos los destinatarios.

### Configurar orígenes de certificados públicos

Para usar certificados públicos S/MIME, configure las directivas: origen del certificado público S/MIME, la dirección del servidor LDAP, el DN Base de LDAP y el acceso LDAP anónimo.

Además de las directivas de aplicaciones, haga lo siguiente.

- Si los servidores LDAP son públicos, compruebe que el tráfico se envía directamente a los servidores LDAP. Para ello, configure la directiva “Acceso de red” en **Túnel a la red interna** para Secure Mail y configure una DNS dividida para Citrix ADC.
- Si los servidores LDAP se encuentran en una red interna, lleve a cabo lo siguiente:
  - Para iOS, no debe configurar la directiva “Puerta de enlace de servicio de red en segundo plano”. Si configura la directiva, los usuarios reciben indicaciones frecuentes de autenticación.
  - Para Android, compruebe que ha agregado la **URL del servidor LDAP** a la lista de la directiva “Puerta de enlace de servicio de red en segundo plano”.

## Single Sign-On para Secure Mail

June 18, 2019

Puede configurar Endpoint Management para que inscriba a los usuarios automáticamente en Secure Mail cuando se inscriban en Secure Hub. Los usuarios no tienen que introducir información adicional ni realizar pasos adicionales para inscribirse en Secure Mail. Para los usuarios que se inscriben en Secure Hub con credenciales de correo electrónico, esta funcionalidad requiere que esté habilitada la detección automática. Si la detección automática no está habilitada, puede habilitarla para los siguientes métodos de inscripción:

- La dirección de Endpoint Management se pasa a Secure Mail desde Secure Hub.
- Los usuarios introducen la dirección de Endpoint Management al inscribirse en Secure Hub.

### Para habilitar la inscripción automática en Secure Mail

1. En las propiedades del cliente de Endpoint Management, en la página **Parámetros**, haga lo siguiente:

   a. Establezca los siguientes valores en **true**:

   - ENABLE_PASSCODE_AUTH
   - ENABLE_PASSWORD_CACHING
   - ENABLE_CREDENTIAL_STORE

   b. Agregue esta configuración:

   - **Nombre simplificado**: SEND_LDAP_ATTRIBUTES
   - **Valor**: userPrincipalName=${user.userprincipalname},sAMAccountNAme=${user.samaccountname}, displayName= ${ user.displayName} ,mail= ${ user.mail}

2. En la página **Configuración**, agregue esta configuración a la propiedad del servidor:

   MAM_MACRO_SUPPORT establecido en **verdadero**

3. Configure estas propiedades de Secure Mail:

   - Establezca “Mecanismo de autenticación inicial” en **Dirección de correo electrónico del usuario**.
   - Establezca “Credenciales iniciales de autenticación” en **userPrincipalName**.

4. Configure el servicio Detección automática basado en correo electrónico para el buzón de Exchange Server del usuario. Para obtener asistencia, póngase en contacto con su administrador de Microsoft Exchange. En este artículo se asume que ha configurado el servicio Detección automática consultando al DNS para obtener un registro de servicios.

### Para configurar la directiva de Secure Mail

Cargue la aplicación Secure Mail en Endpoint Management. Cargue el archivo MDX asociado a la versión correspondiente de la aplicación Secure Mail. A continuación, configure los siguientes parámetros de la aplicación Secure Mail:

1. En “Mecanismo de autenticación inicial”, haga clic en **Dirección de correo electrónico del usuario**.
2. En **Credenciales iniciales de autenticación**, haga clic en **userPrincipalName** o **sAMAccountName**. Su selección se basa en el tipo de autenticación configurado en el servidor de correo de Exchange del usuario.
3. Deje vacíos los campos de dominio de usuario de Secure Mail y Exchange Server de Secure Mail.
4. Configure otras directivas de Secure Mail según sea necesario y realice las asignaciones necesarias de grupos de entrega.

### Experiencia de punto a punto del usuario con SSO en Secure Mail y aprovisionamiento automático

Debe cumplir los siguientes requisitos previos.

1. Instale Secure Hub desde el App Store de Apple (iOS) o la tienda Google Play (Android).
2. Abra Secure Hub y escriba una dirección de correo electrónico y una contraseña para inscribirse en Endpoint Management.
3. Instale Secure Mail desde el App Store de Apple (iOS) o la tienda Google Play (Android).
4. Abra Secure Mail y toque en **Aceptar**. Este paso permite a Secure Hub administrar Secure Mail. Al abrir, Secure Mail se configura automáticamente.

El servidor de Exchange que corresponde a la base de datos del buzón del usuario se obtiene del servicio Detección automática que configuró. La consulta de registro de servicios DNS utiliza la dirección de correo electrónico del usuario obtenida de Secure Hub.

Todos los detalles requeridos para la configuración de la cuenta (como la dirección de correo electrónico, userPrincipalName o sAMAccountName, y la contraseña) se obtienen desde Secure Hub.

Cuando la cuenta está configurada, los usuarios ven los detalles en el dispositivo, en **Secure Mail** > **Parámetros** > **Cuenta**.

### Solucionar problemas

Si se produce algún problema con la configuración de SSO, puede intentar resolverlo con los siguientes pasos.

1. Compruebe que la versión de XenMobile Server es 10.5 o posterior.
2. Compruebe que Endpoint Management está configurado para el servicio de detección automática, y la inscripción de usuarios está configurada para usar la dirección de correo electrónico.
3. Compruebe que el dominio de Exchange Server está configurado con la detección automática. Compruebe que la consulta del registro de servicios devuelve los datos esperados del servidor de correo para los clientes de correo ActiveSync.
4. En caso de un problema con esta funcionalidad, recopile la siguiente información y comuníquese con la asistencia técnica de Citrix:
    - Descargue los registros de diagnóstico de Endpoint Management.
    - Recopile los registros de diagnóstico de Secure Mail con el nivel de registro más alto.
    - Recopile los registros de IIS desde el directorio C:\inetpub\logs\LogFiles\W3SVC1 del servidor Exchange Server que aloja el servicio Detección automática. Para obtener información

más detallada sobre el servicio Detección automática de Microsoft, consulte el Servicio de detección automática en Exchange Server.

## Consideraciones sobre seguridad

July 17, 2020

En este artículo se analizan los aspectos de seguridad que tener en cuenta para proteger Secure Mail y los parámetros concretos que se pueden habilitar para aumentar la seguridad de los datos.

### Disponibilidad de la protección de derechos de correo electrónico de Microsoft IRM y AIP

Secure Mail para Android y Secure Mail para iOS admiten mensajes protegidos con Information Rights Management (IRM) de Microsoft y la solución Azure Information Protection (AIP). Esta disponibilidad está sujeta a la directiva IRM configurada en Citrix Endpoint Management.

Esta función permite a las organizaciones que utilizan IRM aplicar una protección al contenido de sus mensajes. La función también permite a los usuarios de dispositivos móviles crear y consumir contenido cuyos derechos están protegidos. De forma predeterminada, la funcionalidad de IRM está **desactivada**. Para habilitarlo, **active** la directiva "Information Rights Management".

#### Para habilitar Information Rights Management en Secure Mail

1. Inicie sesión en Endpoint Management y vaya a **Configurar** > **Aplicaciones** y haga clic en **Agregar**.
2. En la pantalla **Agregar aplicación**, haga clic en **MDX**.
3. En la pantalla **Información de la aplicación**, introduzca los detalles de la aplicación y haga clic en **Siguiente**.
4. En función del sistema operativo de su dispositivo, seleccione y cargue el archivo MDX.
5. Active la directiva de IRM (Information Rights Management) en **Parámetros de aplicación**.

> Nota:
>
> Habilite Information Rights Management tanto para iOS como para Android.

#### Recibir un correo electrónico con protección de derechos

Cuando los usuarios reciben un correo con contenido protegido, ven la siguiente pantalla:

Para ver detalles sobre los derechos que corresponden al usuario, toque en **Detalles**.

#### Redactar un correo electrónico con protección de derechos

Cuando los usuarios redactan un correo, pueden establecer perfiles de restricción para habilitar la protección del correo electrónico.

**Para establecer restricciones en su correo electrónico:**

1. Inicie sesión en Secure Mail y toque en el icono **Redactar**.
2. En la pantalla de redacción, toque en el icono **Restricción de correo electrónico**.
3. En la pantalla **Perfiles de restricción**, toque en las restricciones que desee aplicar al correo electrónico y, a continuación, haga clic en Volver.

   Las restricciones aplicadas aparecen debajo del campo Asunto.

Es posible que algunas empresas requieran un cumplimiento estricto de su directiva IRM. Los usuarios con acceso a Secure Mail pueden intentar omitir la directiva IRM si modifican Secure Mail, el sistema operativo o incluso la plataforma de hardware.

Aunque Endpoint Management puede detectar algunos ataques, tenga en cuenta las siguientes medidas de precaución para aumentar la seguridad:

- Revise la información relativa a la seguridad suministrada por el proveedor del dispositivo.
- Configure los dispositivos según corresponda, ya sea mediante las funciones de Endpoint Management o no.
- Proporcione instrucciones a los usuarios sobre el uso apropiado de las funciones de IRM, incluido Secure Mail.
- Implemente software de seguridad adicional externo para ofrecer más resistencia a este tipo de ataques.

### Clasificaciones de seguridad del correo electrónico

Secure Mail para iOS y Android admite marcas de clasificación de correo electrónico, lo que permite a los usuarios especificar marcas de seguridad (SEC) y marcas de limitación de difusión (DLM) cuando envíen mensajes de correo electrónico. El marcado SEC incluye: Protegido (Protected), Confidencial (Confidential) y Secreto (Secret). El marcado DLM incluye: Reservado (Sensitive), Legal o Personal. Al redactar un mensaje de correo electrónico, un usuario de Secure Mail puede seleccionar una marca para indicar el nivel de clasificación del mensaje, como se muestra en las siguientes imágenes.

Los destinatarios pueden ver la marca de clasificación en el asunto del mensaje. Por ejemplo:

- Asunto: Planificar [SEC = PROTEGIDO, DLM = Reservado]

- Asunto: Planificar [DLM = Reservado]
- Asunto: Planificar [SEC = SIN CLASIFICAR]

Los encabezados de correo electrónico incluyen el marcado de clasificación una extensión de encabezado de mensaje de Internet, que se muestra en negrita en este ejemplo:

Fecha: vie, 01 de mayo de 2015 12:34:50 +530

Asunto: Planificar [SEC = PROTEGIDO, DLM = Reservado]

Prioridad: normal

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

De: **operations@example.com**

Para: Equipo **<mylist@example.com>**

Versión MIME: 1.0 Tipo de contenido: **multipart/alternative;boundary="_com.example.email_6428E5E4-9DB3-4133-9F48-155913E39A980"**

Secure Mail solo muestra las marcas de clasificación. La aplicación no realiza ninguna acción basada en ellas.

Cuando un usuario responde o redirige un mensaje de correo electrónico que tiene marcas de clasificación, el marcado SEC y DLM conserva los valores marcados en el mensaje original de manera predeterminada. El usuario puede cambiarlo por otro marcado distinto. Secure Mail no valida dichos cambios en función del mensaje original.

Las marcas de clasificación de correo electrónico se configuran través de las siguientes directivas MDX.

- **Clasificación de correo electrónico:** Si el valor es **Sí**, Secure Mail admite marcas de clasificación para SEC (seguridad) y para DLM (limitación de la difusión). Las marcas de clasificación aparecen en los encabezados de los correos como valores "X-Protective-Marking". Asegúrese de configurar las directivas de clasificación de correo electrónico relacionadas. Esta opción está **desactivada** de forma predeterminada.
- **Espacio de nombres de clasificación de correo:** Especifica el espacio de nombres de clasificación requerido en el encabezado del correo electrónico según el estándar de clasificación utilizado. Por ejemplo, el espacio de nombres "gov.au" aparece en el encabezado como "NS=gov.au". Está vacío de forma predeterminada.
- **Versión de clasificación del correo electrónico:** Especifica la versión de la clasificación requerida en el encabezado del correo electrónico según el estándar de clasificación utilizado. Por ejemplo, la versión "2012.3" aparece en el encabezado como "VER=2012.3". Está vacío de forma predeterminada.
- **Clasificación predeterminada del correo:** Especifica la marca protectora que Secure Mail aplica a un mensaje de correo electrónico si un usuario no elige ninguna marca. Este valor

debe estar incluido en la lista de la directiva Marcas de clasificación de correo. El valor predeterminado es **No oficial**.

- **Marcas de clasificación de correo:** Especifica las marcas de clasificación que pueden utilizar los usuarios finales. Si la lista está vacía, Secure Mail no incluye ninguna lista de marcas de protección. La lista de marcas contiene parejas de valores separados por punto y coma. Cada par incluye el valor de lista que aparece en Secure Mail y el valor de marcado (el texto agregado al asunto del mensaje y al encabezado en Secure Mail). Por ejemplo, en la pareja de marcado "UNOFFICIAL,SEC=UNOFFICIAL;", el valor de la lista es "UNOFFICIAL" y el valor de marcado es "SEC=UNOFFICIAL".

El valor predeterminado es una lista de marcado de clasificación que usted puede modificar. Se facilitan las siguientes marcas con Secure Mail.

- UNOFFICIAL,SEC=UNOFFICIAL
- UNCLASSIFIED,SEC=UNCLASSIFIED
- Solo para uso oficial, 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

## Proteger datos en iOS

Las empresas que deban cumplir las normas de protección de datos del ASD (Australian Signals Directorate) pueden usar las directivas **Habilitar protección de datos de iOS** para Secure Mail y Secure Web. De forma predeterminada, esas directivas están **desactivadas**.

Si la directiva **Habilitar protección de datos de iOS** tiene el valor **Sí** para Secure Web, este aplica el nivel de protección de Clase A a todos los archivos del sandbox. Para obtener información detallada sobre la protección de datos de Secure Mail, consulte Protección de datos del Australian Signals Directorate. Si habilita esta directiva, se aplicará la clase más alta de protección de datos, de modo que no hay necesidad de especificar también la directiva **Minimum data protection class**.

### Para cambiar la directiva Habilitar protección de datos de iOS

1. Use la consola de Endpoint Management para cargar los archivos MDX de Secure Web y Secure Mail en Endpoint Management. Para una nueva aplicación, vaya a **Configurar > Aplicaciones > Agregar** y haga clic en **MDX**. Para realizar una actualización, consulte Actualizar aplicaciones MDX o de empresa.
2. Para Secure Mail, vaya a **Parámetros de aplicación**, busque la directiva **Habilitar protección de datos de iOS** y **actívela**. Los dispositivos que ejecutan versiones anteriores del sistema operativo no se verán afectados cuando se habilite esta directiva.
3. Para Secure Web, vaya a Parámetros de **aplicación**, busque la **directiva Habilitar protección de datos de iOS** y **actívela**. Los dispositivos que ejecutan versiones anteriores del sistema operativo no se verán afectados cuando se habilite esta directiva.
4. Configure las directivas de aplicación de la manera habitual y guarde los parámetros para implementar la aplicación en el almacén de aplicaciones de Endpoint Management.

## Protección de datos del Australian Signals Directorate

Secure Mail admite la protección de datos del Australian Signals Directorate (ASD) para aquellas organizaciones que deban cumplir los requisitos de seguridad informática del ASD. De forma predeterminada, la directiva “Habilitar protección de datos de iOS” está **desactivada** y Secure Mail aplica una protección de datos de Clase C o la protección de los datos definida en el perfil de aprovisionamiento.

Si la directiva está **activada**, Secure Mail especifica el nivel de protección al crear y abrir archivos en el sandbox de las aplicaciones. Secure Mail aplica la protección de datos de Clase A en:

- Elementos de la bandeja de salida
- Fotos de la cámara o del carrete
- Imágenes pegadas desde otras aplicaciones
- Archivos adjuntos descargados

Secure Mail aplica la protección de datos de Clase B en:

- Correo almacenado
- Elementos del calendario
- Contactos
- Archivos de directivas de ActiveSync

La protección de datos de Clase B permite la sincronización en un dispositivo bloqueado y permite que las descargas se completen aunque el dispositivo se bloquee una vez iniciada la descarga.

Con la protección de datos habilitada, los elementos de la bandeja de salida que se encuentran en la cola no se envían cuando el dispositivo está bloqueado porque los archivos no se pueden abrir. Si el dispositivo cierra y luego reinicia Secure Mail cuando el dispositivo está bloqueado, Secure Mail no se puede sincronizar hasta que el dispositivo se desbloquee y Secure Mail se inicie.

Citrix recomienda que, si se habilita esta directiva, se habilite la captura de registro de Secure Mail solo cuando sea necesario, para evitar la creación de archivos de registros con protección de datos de Clase C.

## Funciones de iOS

July 17, 2020

En este artículo se analizan las funciones de iOS que se admiten en Secure Mail.

### Minimizar borradores

En Secure Mail para iOS, puede minimizar un borrador mientras está redactando un correo electrónico y navegar por la aplicación. Esta función está disponible en dispositivos con iOS 13 y versiones posteriores. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Minimizar el borrador de un correo electrónico.

### Notificar mensajes de phishing con encabezados MIME

En Secure Mail para iOS, cuando un usuario notifica un mensaje de phishing, se genera un archivo EML como adjunto correspondiente a ese correo. Los administradores reciben este correo y pueden ver los encabezados MIME asociados al correo notificado. Para habilitar esta función, un administrador debe configurar la directiva “Direcciones para notificar mensaje de phishing” y definir el “Mecanismo para notificar phishing” en Notificar mediante archivo adjunto, en la consola de Citrix Endpoint Management. Para obtener información detallada, consulte Notificar mensajes de phishing en calidad de archivo adjunto.

### Compatibilidad con WKWebView

Secure Mail para iOS admite WkWebView. Esta función mejora la forma en que se representan en su dispositivo los eventos de correo electrónico y Calendario de Secure Mail.

### Compatibilidad con Slack EMM

Slack EMM está destinado a clientes de Slack con Enterprise Mobility Management (EMM) habilitado. Secure Mail para iOS admite la aplicación **Slack EMM**, que permite a los administradores elegir la integración de Secure Mail con la aplicación **Slack** o la aplicación **Slack EMM**.

### Notificaciones de grupo

Con la función de notificaciones de grupo, las conversaciones se agrupan a partir de un hilo de correo. Puede ver rápidamente las notificaciones agrupadas en la pantalla de bloqueo del dispositivo. Los parámetros de las notificaciones de grupo están habilitados de forma predeterminada en el dispositivo. La función requiere iOS 12.

### Opción de respuesta a notificaciones

En Secure Mail para iOS, los usuarios pueden responder a notificaciones de reunión (Aceptar, Rechazar y Provisional). Pueden responder a notificaciones de mensajes (Responder y Eliminar).

### Mejoras en los mensajes de error de notificaciones push enriquecidas

En Secure Mail para iOS, los mensajes de error referentes a notificaciones push aparecen en el centro de notificaciones correspondiente del dispositivo y se agrupan por tipo de error de la notificación. Para obtener información detallada, consulte Notificaciones de Secure Mail.

### Notificaciones push enriquecidas disponibles en las configuraciones de Microsoft

Secure Mail para iOS admite notificaciones push enriquecidas en configuraciones que ejecutan Microsoft Enterprise Mobility + Security (EMS) /Intune con autenticación moderna (O365). Para habilitar la función de notificaciones push enriquecidas, debe cumplir los siguientes requisitos previos:

- En la consola de Endpoint Management, active las **notificaciones push**.
- Establezca la directiva **Acceso de red** en **Sin restricciones**.
- Establezca la directiva **Control de notificaciones en pantalla bloqueada** en **Permitir** o **Remitente del correo o título del evento**.
- Vaya a **Secure Mail** > **Parámetros** > **Notificaciones** y habilite **Notificaciones de correo**.

### Compatibilidad con S/MIME para credenciales derivadas

Secure Mail para iOS admite S/MIME para credenciales derivadas. Para que esta característica funcione, debe hacer lo siguiente:

- Seleccione "Credencial derivada" como origen del certificado S/MIME. Para obtener información detallada, consulte Credenciales derivadas para iOS.
- Agregue la propiedad del cliente Atributos LDAP en Citrix Endpoint Management. Use la siguiente información:
  - **Clave:** SEND_LDAP_ATTRIBUTES
  - **Valor:** `userPrincipalName=${ user.userprincipalname } ,sAMAccountNAme=${ user.samaccountname } ,displayName=${ user.displayName } ,mail=${ user.mail }`

Si quiere conocer los pasos para agregar una propiedad del cliente a XenMobile Server, consulte Propiedades de cliente; para agregar una propiedad del cliente a Endpoint Management, consulte Propiedades de cliente.

Para obtener información sobre cómo se inscriben los usuarios con credenciales derivadas, consulte Inscribir dispositivos mediante credenciales derivadas.

1. En la consola de Endpoint Management, vaya a **Configurar > Aplicaciones**.
2. Seleccione **Secure Mail** y haga clic en **Modificar**.
3. En el apartado de la plataforma iOS, en "Origen de certificado S/MIME", seleccione **Credencial derivada**.

### Identificar llamada en Secure Mail

En Secure Mail para iOS, puede identificar las llamadas entrantes de sus contactos de Secure Mail. Para ello, habilite la identificación de llamadas de Secure Mail en los ajustes de su dispositivo. Debe habilitar el siguiente requisito previo administrativo: En Citrix Endpoint Management, la directiva MDX CallerIDSupportEnabled MDX debe estar habilitada.

Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Configurar ID de llamada.

### Establecer colores en Calendarios

Para ver documentación de ayuda para usuarios sobre esta función del calendario, consulte el artículo del Centro de ayuda para usuarios de Citrix Establecer colores para calendarios de Secure Mail sincronizados.

### Adjuntar archivos desde la aplicación Archivos

En Secure Mail para iOS, puede adjuntar archivos desde la aplicación nativa **Archivos** de iOS. Para obtener más información sobre la aplicación Archivos de iOS, consulte el artículo Aplicación Archivos de Apple. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Ver y adjuntar archivos.

### Función de corrección ortográfica

La revisión ortográfica de Secure Mail interactúa con los parámetros Mayúsculas automáticas y Comprobar ortografía de los ajustes del dispositivo (en la sección **General > Teclado**) de este modo:

| Corrección automática en el dispositivo | Revisión ortográfica en el dispositivo | Revisión ortográfica en Secure Mail | Comportamiento |
|---|---|---|---|
| SÍ | SÍ | SÍ | Subrayado en rojo. Cuando se toca sobre la palabra, esta se resalta en color rosa y aparece una sugerencia de escritura. |
| NO | NO | SÍ | Subrayado en rojo. Cuando se toca sobre la palabra, no aparece ninguna sugerencia. |
| SÍ | SÍ | NO | No se ve ningún subrayado en rojo. Cuando se toca sobre la palabra, esta se resalta en color rosa y aparece una sugerencia de escritura. |
| NO | NO | NO | No hay ningún subrayado, ni se resaltan las palabras ni aparecen sugerencias. |

| Corrección automática en el dispositivo | Revisión ortográfica en el dispositivo | Revisión ortográfica en Secure Mail | Comportamiento |
|---|---|---|---|
| SÍ | NO | SÍ | Subrayado en rojo. Cuando se toca sobre la palabra, esta se resalta en color rosa y aparece una sugerencia de escritura. |
| NO | SÍ | SÍ | Subrayado en rojo. Cuando se toca sobre la palabra, esta se resalta en color rosa y aparece una sugerencia de escritura. |
| SÍ | NO | NO | No se ve ningún subrayado en rojo. Cuando se toca sobre la palabra, esta se resalta en color rosa y aparece una sugerencia de escritura. |
| NO | SÍ | NO | No se ve ningún subrayado en rojo. Cuando se toca sobre la palabra, esta se resalta en color rosa y aparece una sugerencia de escritura. |

**Pantalla Buzones**

La pantalla **Buzones** muestra todas las cuentas que haya configurado y presenta las siguientes vistas:

- **Todas las cuentas:** Contiene los correos de todas las cuentas de Exchange que se hayan configurado.
- **Cuentas individuales:** Contiene los mensajes de correo electrónico y las carpetas de una sola cuenta. Estas cuentas se muestran como una lista que puede expandir para ver las subcarpetas.

El buzón **Todas las cuentas** es la vista global predeterminada. Esta vista contiene los correos y los archivos adjuntos de todas las cuentas de Exchange que se hayan configurado en el dispositivo.

El buzón **Todas las cuentas** presenta los siguientes elementos de menú:

- Todos los datos adjuntos
- Entrada
  - No leído
  - Destacado
- Borradores
- Elementos enviados
- Bandeja de salida
- Elementos eliminados

Aunque la vista **Todas las cuentas** muestra los mensajes de correo electrónico de varias cuentas de forma colectiva, las siguientes acciones usan la dirección de correo electrónico de la cuenta principal o predeterminada:

- Mensaje nuevo
- Nuevo evento

Para cambiar la dirección de correo electrónico del remitente cuando se redacta un correo nuevo desde la vista **Todas las cuentas**, toque en la dirección predeterminada en el campo **De:** y seleccione otra cuenta de las que aparecen.

> **Nota:**
>
> Al redactar un correo electrónico desde la vista de conversación, se rellena automáticamente el campo **De:** con la dirección de correo electrónico a la que está dirigida la conversación.

#### Cuentas individuales

Todas las cuentas que haya configurado aparecen en forma de lista en **Todas las cuentas**. La cuenta principal o predeterminada siempre aparece en primera posición, seguida de las demás cuentas por orden alfabético.

Las cuentas individuales muestran las subcarpetas que haya creado. Para ver las carpetas que contienen esas subcarpetas, toque en el icono **V** situado junto a cada subcarpeta.

Las siguientes acciones están limitadas a las cuentas individuales:

- Mover elementos.

- Redactar mensajes de correo electrónico desde la vista de conversación.
- Importar vCard.
- Guardar contactos.

## Calendario

El calendario muestra todos los eventos de las distintas cuentas definidas en el dispositivo. Puede establecer colores para cuentas individuales, para diferenciar los eventos de calendario pertenecientes a ellas.

### Para establecer colores para eventos de calendario

1. Toque el icono **Calendario** en la barra al pie de página y luego toque el icono de tres líneas en la parte superior izquierda.
   La pantalla **Calendario** muestra todas las cuentas configuradas.
2. Toque el color predeterminado que aparece a la derecha de una cuenta de Exchange.
   La pantalla Colores muestra los colores disponibles para esa cuenta.
3. Seleccione el color que quiera y, a continuación, toque **Guardar**.
4. Para volver a la pantalla anterior, toque **Cancelar**.
   El color seleccionado se establece para todos los eventos del calendario pertenecientes a esa cuenta de Exchange.

Cuando crea un evento o una invitación de calendario, el campo **Organizador** se rellena automáticamente con el ID de correo de la cuenta predeterminada. Para cambiar la cuenta de correo, toque esta dirección de correo electrónico y seleccione otra cuenta.

> **Nota:**
>
> Cuando salga de Secure Mail y lo inicie de nuevo, la aplicación restaura los últimos parámetros de calendario configurados en el dispositivo.

### Buscar

Puede realizar una búsqueda global desde las vistas **Buzones** o **Contactos**. Esta acción muestra los resultados correspondientes después de buscar en todas las cuentas existentes en la aplicación. Todas las búsquedas desde dentro de una cuenta individual muestran resultados pertenecientes a esa cuenta solamente.

## Imprimir correos electrónicos, eventos de calendario o imágenes en línea en iOS

Ahora puede imprimir correos electrónicos, eventos de calendario o imágenes en línea desde su dispositivo iOS.

**Requisitos previos**

Antes de comenzar, asegúrese de que se cumplan los siguientes requisitos:

- La opción **Bloquear AirPrint** está **desactivada**.
- La opción **Permitir que los usuarios impriman** está inhabilitada en IRM.

De forma predeterminada, la función de impresión está habilitada en Secure Mail para iOS. La función de impresión puede estar controlada por el administrador a través de directivas administrativas desde Apple AirPrint o con Information Rights Management (IRM) de Microsoft. En estos casos, la impresión de un correo electrónico, un evento del calendario o una imagen en línea no funcionará y podría aparecer un mensaje de error.

**Para imprimir correos electrónicos**

1. Abra el elemento de correo electrónico que desea imprimir.
2. Toque el icono “Más” situado en la parte superior izquierda de la pantalla. Aparecen las siguientes opciones:
    - Mover
    - Imprimir
3. Toque **Imprimir**.
   Aparece la pantalla **Opciones de impresora**.
4. Para seleccionar una impresora, toque en **Seleccionar impresora**.
   Aparecerá la pantalla **Impresora**.
5. Seleccione la impresora donde quiera imprimir.
6. Toque en **–** o **+** para disminuir o aumentar la cantidad de copias que quiere imprimir.
7. Para imprimir una página específica o un rango de páginas, toque en **Intervalo**.
   Aparece la pantalla **Intervalo de páginas**. De forma predeterminada, está seleccionada la opción **Todas las páginas**.
8. Para cambiar la selección de páginas, deslice los números de página hacia abajo o hacia arriba.
9. Toque en **Opciones de impresora** para volver a la pantalla **Opciones de impresora**.
10. Para imprimir en blanco y negro, toque en el botón **Blanco y negro**. De forma predeterminada, Secure Mail imprime en color.
11. Toque en **Imprimir**, en la parte superior derecha, para imprimir el mensaje de correo electrónico.
12. Para cancelar el trabajo de impresión, toque en **Cancelar** en la parte superior izquierda.

**Para imprimir un evento de calendario**

1. Vaya al calendario y seleccione un evento.
2. Toque en “Imprimir” y siga las mismas instrucciones que se mencionan en la sección **Para imprimir correos electrónicos**.

**Para imprimir imágenes alineadas**:

1. Abra el elemento de correo electrónico con la imagen en línea.
2. Toque en el icono “Más”. Aparecen las siguientes opciones:
    - Mover
    - Imprimir
    - Cancelar
3. Toque en **Imprimir** y siga las mismas instrucciones que se mencionan en la sección **Para imprimir correos electrónicos** anterior.

### Varios códigos de conferencia (acceso telefónico a una reunión)

Secure Mail para iOS admite varios códigos de conferencia. Ahora puede seleccionar un código de conferencia en una lista de los códigos de conferencia disponibles para unirse a una reunión.

**Para unirse a una reunión por teléfono**

1. Abra la invitación de la reunión y toque en **Marcar**.
2. De la lista de números de teléfono que aparecen, seleccione uno para el acceso telefónico.
3. De la lista de códigos de conferencia que aparecen, seleccione uno para unirse a la reunión.
4. Toque en **Llamar** para unirse a la reunión.

### Compatibilidad para imprimir archivos adjuntos de correo electrónico

Secure Mail para iOS admite la impresión de archivos adjuntos de correo electrónico.

## Funciones de Android

July 17, 2020

En este artículo se analizan las funciones de Android que se admiten en Secure Mail.

### Sincronización bidireccional de contactos

En Secure Mail para Android, puede crear, modificar y eliminar contactos de Secure Mail desde su lista de contactos local.

### Deshacer correos enviados

En Secure Mail para Android puede deshacer correos enviados. Una vez que haya tocado el botón **Enviar**, recibirá una notificación que le permite deshacer la acción del envío. Toque **Deshacer** para revertir el envío y modificar el correo o los destinatarios del correo, adjuntar o quitar archivos adjuntos, o bien descartar el correo.

### Sincronización de archivos adjuntos en la carpeta Borradores

En Secure Mail para Android, cuando la carpeta **Borradores** se sincroniza, los archivos adjuntos también se sincronizan y están disponibles en todos los dispositivos. Esta función está disponible en dispositivos con la versión 16 de Exchange ActiveSync o una posterior.

### Consulta de archivos PDF en la aplicación

En Secure Mail para Android, puede ver archivos PDF dentro de la aplicación, junto con marcadores y anotaciones. También está disponible la vista mejorada de otros archivos adjuntos de Microsoft Office.

### Utilice SSO web para la directiva de tunelización en configuraciones que emplean autenticación moderna con Microsoft Office 365

En Secure Mail para Android, se agrega una nueva directiva denominada **Utilizar SSO web para la tunelización**. Con esta directiva, puede tunelizar el tráfico de OAuth para que pase a través de Secure Browse. Para ello:

- Establezca la directiva **Utilizar SSO web para la tunelización** en **Sí**.
- En la directiva Acceso de red, seleccione la opción **SSO web en túnel**.
- Excluya los nombres de host relacionados con OAuth de la directiva **Servicios en segundo plano**.

### Arrastrar y colocar eventos del Calendario

En Secure Mail para Android, puede arrastrar y colocar un evento existente de calendario para cambiarle la hora. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Cambiar el momento de un evento de calendario.

### Compatibilidad con aplicaciones de 64 bits para Google Play

Secure Mail para Android admite arquitecturas de 64 bits.

### Mejoras al deslizar la pantalla hacia abajo para actualizar la interfaz de usuario en Secure Mail para Android

De acuerdo con las directrices de diseño de materiales, hemos realizado pequeñas mejoras en la función **Deslizar hacia abajo para actualizar**. La marca de hora de la sincronización está disponible en la parte inferior de la pantalla al tocar el icono de hamburguesa.

### Widget para la agenda del Calendario

En Secure Mail para Android, la agenda del **Calendario** está disponible como un widget. Desde este widget, puede ver los próximos eventos en el **Calendario** de una semana. Esta función le permite crear eventos del **Calendario**, ver eventos existentes y modificar los detalles. La directiva **Bloquear captura de pantalla** no se aplica al widget colocado en la pantalla de inicio. Sin embargo, puede inhabilitar el widget mediante la directiva **Permitir widget de agenda del calendario**.

### Directiva de acceso de red

En Secure Mail para Android, se agrega una nueva opción llamada **SSO web en túnel** a la directiva MDX de acceso de red. Configurar esta directiva le dará la flexibilidad de usar el túnel para transferir el tráfico interno a través de Secure Browse y Secure Ticket Authority (STA) en paralelo. También puede permitir conexiones Secure Browse para servicios de autenticación, como NTLM, Okta y Kerberos. Al configurar STA inicialmente, debe agregar nombres de dominio completos individuales y puertos de direcciones de servicios a la directiva Servicios de red en segundo plano. Sin embargo, si configura la opción **SSO web en túnel**, no es necesario realizar estas configuraciones.

Cómo habilitar esta directiva para Secure Mail para Android en la consola de Citrix Endpoint Management:

1. Descargue y use el archivo MDX para Android. Para obtener más información, consulte los pasos de Funcionamiento de las aplicaciones MDX y las aplicaciones móviles.
2. En la directiva Acceso de red, haga clic en la opción **SSO web en túnel**. Para obtener más información, consulte Acceso a red de las aplicaciones

### Mejoras en las tarjetas Feeds

En Secure Mail para Android, se han realizado las siguientes mejoras en la carpeta **Feeds** existente:

- Las invitaciones a las reuniones de todas las carpetas sincronizadas automáticamente aparecen en la tarjeta Feeds.

- Puede ver hasta cinco de las próximas reuniones en su tarjeta Feeds.
- Ahora las próximas reuniones aparecen en función de un período de 24 horas a partir de su hora actual. Estas invitaciones a reuniones se clasifican en **Hoy** y **Mañana**. En versiones anteriores, las próximas reuniones hasta el final del día aparecen es sus feeds.

## Visualizar datos adjuntos

En Secure Mail para Android, es fácil visualizar archivos adjuntos de correo y calendario. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Ver y adjuntar archivos.

## Imprimir correos electrónicos y eventos de calendario

En Secure Mail para Android, puede imprimir correos electrónicos y eventos de calendario desde el dispositivo Android. Para esta funcionalidad de impresión, se utiliza el framework de Android Print.

### Requisitos previos

- Compruebe que un administrador haya **desactivado** la directiva **Bloquear impresión** en la consola de Citrix Endpoint Management. Para obtener información sobre esta directiva para Android, consulte Directiva de bloquear impresión.
- Si un correo electrónico está protegido por IRM, debe habilitar la opción **Allow viewers to print** en el correo electrónico.

No puede imprimir un mensaje de correo electrónico o un evento de calendario si estas directivas están configuradas de forma incorrecta.

> **Nota:**
>
> Esta función de impresión presenta las siguientes limitaciones conocidas:
>
> - Las imágenes alineadas solo se imprimen si las ha descargado tocando en **Mostrar imágenes**. Si no toca **Mostrar imágenes**, solo se imprimen los marcadores de posición que contengan esas imágenes.
> - En Secure Mail, los correos electrónicos de gran tamaño se truncan. Antes de imprimir, toque **Descargar mensaje completo** para imprimir el correo electrónico completo. Si el mensaje completo no se descarga, se imprime un correo electrónico truncado.
> - No se agregan metadatos de un correo electrónico o evento al imprimir estos elementos.

### Para imprimir un correo electrónico

1. Abra el correo electrónico que quiere imprimir.

2. Toque el icono “Más” situado en la parte superior izquierda de la pantalla. Aparecen las siguientes opciones:
    - Mover
    - Imprimir

> **Nota:**
>
> En tabletas, puede usar directamente el icono de impresión situado en la parte superior izquierda de la pantalla para imprimir un correo electrónico.

1. Toque **Imprimir**. Aparecerá una vista previa del correo electrónico.
2. Toque la lista y aparecerán las siguientes opciones:
    - Guardar en PDF
    - Todas las impresoras
3. Toque **Guardar en PDF** para guardar el correo electrónico en formato PDF.
4. Toque **Todas las impresoras**. Instale la impresora que más se ajuste a sus necesidades.
5. Una vez instalada la impresora, toque **Seleccionar impresora** para seleccionar una impresora. Aparecerá la pantalla **Impresora**.

    > **Nota:**
    >
    > Las opciones de impresión varían en función de la impresora seleccionada. La siguiente imagen es de una impresora Canon E480 y se utiliza solo para fines de representación.

6. Seleccione la impresora donde quiera imprimir. Utilice las siguientes opciones de impresión:
    - Introduzca manualmente la cantidad de copias a imprimir.
    - Seleccione el tamaño del papel en la lista.
    - Seleccione el color en la lista.
    - Elija la orientación necesaria de la página.
    - Seleccione una página, un rango de páginas o escríbalo manualmente.
7. Después de configurar las opciones de impresión, toque el icono “Imprimir” de la pantalla.

#### Para imprimir una imagen alineada

- Toque **Mostrar imágenes** en el correo electrónico y siga las mismas instrucciones que se mencionan en la sección anterior Para imprimir un correo electrónico.

#### Para imprimir un evento de calendario

1. Vaya al calendario y toque un evento.

2. Toque “Imprimir” y siga las mismas instrucciones que se mencionan en la sección anterior Para imprimir un correo electrónico.

### Notificar mensajes de phishing con encabezados ActiveSync

En Secure Mail para Android, cuando un usuario notifica un mensaje de phishing, se genera un archivo EML como adjunto correspondiente a ese correo. Los administradores reciben este correo y pueden ver los encabezados ActiveSync asociados al mensaje notificado.

Para habilitar esta función, un administrador debe configurar la directiva “Direcciones para notificar mensaje de phishing” y definir el “Mecanismo para notificar phishing” en **Notificar mediante archivo adjunto**, en la consola de Citrix Endpoint Management. Para obtener información detallada sobre la configuración de directivas MDX para Secure Mail, consulte Directivas MDX para aplicaciones móviles de productividad.

### Notificaciones de subcarpeta

En Secure Mail para Android, puede recibir notificaciones de correo desde subcarpetas de la cuenta de correo.

> **Nota:**
>
> - Compruebe que la notificación push basada en FCM está habilitada en la consola de Endpoint Management para obtener las notificaciones de las subcarpetas. Para conocer los pasos de la configuración de las notificaciones push basadas en FCM, consulte Notificaciones push para Secure Mail.
> - La función de notificaciones de subcarpeta no está disponible para Lotus Notes Server.

#### Para habilitar las notificaciones de subcarpetas

1. Vaya a **Parámetros** y, a continuación, en **General**, toque **Notificaciones**.
2. En la pantalla **Notificaciones**, toque **Carpetas de correo**. Aparecerá una lista de las subcarpetas que contiene la bandeja de entrada.
3. Toque para seleccionar las subcarpetas de las que quiere recibir notificaciones. La bandeja de entrada está seleccionada de forma predeterminada.

   > **Nota:**
   >
   > Si activa las notificaciones para subcarpetas, también se activa la sincronización automática.

Para inhabilitar las notificaciones de subcarpeta, desmarque las casillas de las subcarpetas cuyas notificaciones no quiera recibir.

### Canales de notificaciones

En los dispositivos que ejecutan Android O o posterior, puede usar los parámetros del canal de notificaciones para administrar la forma en que se gestionan sus notificaciones de correo electrónico y calendario. Esta función permite personalizar y administrar sus notificaciones.

Para configurar las notificaciones de recordatorios de correo o calendario, abra Secure Mail y vaya a **Parámetros > Notificaciones** y seleccione la opción de notificación deseada.

A continuación, puede ir a **Administrar notificaciones de correo** o **Administrar notificaciones de calendario** para gestionar las notificaciones de correo electrónico o calendario respectivamente.

Como alternativa, puede presionar prolongadamente en el icono de la aplicación Secure Mail en el dispositivo, seleccionar **Información de la aplicación** y luego tocar en **Notificaciones**.

Si el parámetro de vibración estaba establecido en **Solo en modo silencioso**, cambiará a la configuración predeterminada de vibración (**apagada**) con esta función.

> Nota:
>
> Las notificaciones en la pantalla de bloqueo están disponibles en función de cómo haya configurado el administrador la directiva MDX Control de notificaciones en pantalla bloqueada.

### Botones de respuesta a reuniones dentro del correo electrónico

En Secure Mail para Android, los botones de respuesta a las reuniones aparecen dentro del correo electrónico. Cuando reciba una notificación por correo electrónico sobre invitaciones a reuniones, puede responder a la invitación tocando en una de las siguientes opciones:

- Sí
- Quizá
- No

### Mejoras en los datos adjuntos

En Secure Mail para Android, se ha simplificado la visualización de datos adjuntos. Para proporcionar una mejor experiencia, se han eliminado los pasos no esenciales, pero se conservan las opciones de datos adjuntos que existían en las versiones anteriores.

Puede ver los datos adjuntos en la aplicación Secure Mail. El archivo adjunto se abre directamente si se puede ver mediante Secure Mail. Si los datos adjuntos no se pueden ver mediante Secure Mail, aparecerá una lista de aplicaciones. Puede seleccionar la aplicación necesaria para ver los datos adjuntos. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Ver y adjuntar archivos.

### Mejoras en el botón Atrás

En Secure Mail para Android, puede tocar en el botón Atrás de su dispositivo para contraer las opciones expandidas del botón de **acción flotante**. Esta acción lo lleva de vuelta a la vista de detalles del mensaje o evento.

### Pasos de administración para habilitar los archivos adjuntos de la Galería en Android

En las versiones de Secure Mail 10.3.5 y posteriores, los usuarios no pueden adjuntar imágenes directamente desde la Galería cuando la directiva "Intercambio de documentos entrantes (Abrir en)" está establecida en **Restringido**. Si quiere conservar esta directiva con el valor **Restringido**, pero quiere permitir que los usuarios adjunten fotos desde la Galería, siga estos pasos en la consola de Endpoint Management.

1. **Desactive** el parámetro **Bloquear galería**.
2. Obtenga el ID de paquete de la Galería correspondiente a los dispositivos. Algunos ejemplos:
   - **LG Nexus 5:**
     com.google.android.gallery3d, com.google.android.apps.photos
   - **Samsung Galaxy Nota 3:**
     com.sec.android.gallery3d, com.sec.android.gallery3d.panorama360view, com.google.android.apps.p
   - **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. Haga visible la directiva oculta InboundDocumentExchangeWhitelist:
   - Descargue el archivo APK de WorxMail y empaquete el archivo con el MDX Toolkit.
   - Busque el archivo MDX en su equipo y cambie el sufijo del archivo a .zip.
   - Abra el archivo .zip y busque el archivo policy_metadata.xml
   - Busque y cambie InboundDocumentExchangeWhitelist de `PolicyHidden>**true**</PolicyHidden>` a `<PolicyHidden>**false**</PolicyHidden>`.
   - Guarde el archivo policy_metadata.xml.
   - Seleccione todos los archivos de esa carpeta y comprímalos para crear el archivo .zip.

     > **Nota:**
     >
     > No comprima la carpeta exterior. Seleccione todos los archivos dentro de esta car-

> peta y comprima los archivos seleccionados.

- Haga clic en el archivo comprimido resultante.
- Elija **Get Info** y cambie el sufijo del archivo de nuevo a MDX.

4. Cargue el archivo MDX modificado en la consola de Endpoint Management, y agregue la lista de los ID de paquete de la Galería a la directiva “Lista blanca de intercambio de documentos entrantes”, ahora visible.

   Compruebe que los ID de paquetes están separados por comas:

   com.sec.android.gallery3d, com.sec.android.gallery3d.panorama360view, com.google.android.apps.photo

5. Guarde e implemente Secure Mail.

Los usuarios de Android ahora pueden adjuntar imágenes desde la aplicación Galería. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Ver y adjuntar archivos.

#### Formatos de archivo admitidos

Una X indica un formato de archivo que se puede adjuntar, ver y abrir en Secure Mail.

| Formato | iOS | Android |
|---|---|---|
| Vídeo: H.263 AMR NB codec_Mp4 | | X |
| Vídeo: H.263 AMR NB codec_3gp | | X |
| Vídeo: H.264 AAC codec_3gp | X | X |
| Vídeo: H.264 AAC codec_mp4 | X | X |
| Vídeo: H.264 Acclc codec_mp4 | X | X |
| GTM recorded_wmv | | X |
| AVI | | X |
| WAV | X | X |
| MP4 | X | X |
| 3GP | X | X |
| Flac | | X |
| AAC | X | X |

| Formato | iOS | Android |
|---|---|---|
| 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 (de página única) | 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 |
| HTM | X | X |
| HTML | X | X |

| Formato | iOS | Android |
|---|---|---|
| ZIP | X | X |
| EML | X | X |

## Calendario

El calendario muestra todos los eventos de las distintas cuentas definidas en el dispositivo. Puede establecer colores para cuentas individuales, para diferenciar los eventos de calendario pertenecientes a ellas.

> **Nota:**
>
> La función Calendario personal siempre se asocia a su cuenta principal o predeterminada, si está habilitada.

### Para establecer colores para eventos de calendario

1. Toque el icono **Calendario** en la barra al pie de página y luego toque el icono de tres líneas en la parte superior izquierda.
   La pantalla **Calendarios** muestra todas las cuentas configuradas.
2. Toque el color predeterminado que aparece a la derecha de una cuenta de Exchange.
   La pantalla Colores muestra los colores disponibles para esa cuenta.
3. Seleccione el color que quiera y, a continuación, toque **Guardar**.
4. Para volver a la pantalla anterior, toque **Cancelar**.
   El color seleccionado se establece para todos los eventos del calendario pertenecientes a esa cuenta de Exchange.

Cuando crea un evento o una invitación de calendario, el campo **Organizador** se rellena automáticamente con el ID de correo de la cuenta predeterminada. Para cambiar la cuenta de correo, toque esta dirección de correo electrónico y seleccione otra cuenta.

### Buscar

Puede realizar una búsqueda global desde las vistas **Buzones** o **Todos los contactos**. Esta acción muestra los resultados correspondientes después de buscar en todas las cuentas existentes en la aplicación.

Todas las búsquedas desde dentro de una cuenta individual muestran resultados pertenecientes a esa cuenta solamente.

### Actualizaciones de servicios en segundo plano

Para cumplir con el requisito de límites de ejecución en segundo plano de Google Play en dispositivos con Android 8.0 (API de nivel 26) o posterior, hemos actualizado los servicios en segundo plano de Secure Mail. Para una sincronización de correo ininterrumpida y unas notificaciones continuas en el dispositivo, habilite el servicio de notificaciones push de Firebase Cloud Messaging (FCM). Para obtener más información sobre cómo habilitar las notificaciones push basadas en FCM, consulte Notificaciones push para Secure Mail.

Debe activar las **notificaciones de correo** en los parámetros de Secure Mail del dispositivo. Para obtener información más detallada sobre esta actualización, consulte este artículo de Citrix Support Knowledge Center.

**Limitaciones:**

- Si no ha habilitado las notificaciones push basadas en FCM, la sincronización en segundo plano se produce una vez cada 15 minutos. Este intervalo puede variar según si la aplicación se está ejecutando en segundo plano o en primer plano.
- Cuando los usuarios actualizan manualmente la hora desde los parámetros del dispositivo, la fecha en el widget del calendario no se actualiza automáticamente.

### Android Enterprise en Secure Mail

Secure Mail y Secure Web para Android son compatibles con Android Enterprise, anteriormente conocido como Android for Work.

#### Requisitos previos

- Para poder utilizar esta función, su dispositivo debe ejecutar Android 5.0 o posterior.
- Para las implementaciones locales, la propiedad **afw.accounts** de Endpoint Management debe establecerse en **TRUE**.

Tras configurar Android Enterprise en Endpoint Management, las aplicaciones móviles de productividad pasan a estar disponibles en el dispositivo. Las aplicaciones se identifican con el icono de Android Enterprise, como se indica en la siguiente imagen.

#### Funciones compatibles con Android Enterprise

La siguiente tabla ofrece una lista de las funciones de Secure Mail que son compatibles con Android Enterprise.

| (Función) | Asistencia técnica |
|---|---|
| Detección automática de Exchange Server | X |
| Secure Ticket Authority (STA) | X |
| Exportar contactos | X |
| Microsoft Information Rights Management | X |
| Notificaciones de pantalla bloqueada | X |
| Sincronización de correo electrónico | X |
| Clasificación de correo electrónico | X |
| Cifrado y firma S/MIME | X |
| Servicio Firebase Cloud Messaging (FCM) | X |
| Autenticación moderna (OAuth) | |
| Varias cuentas de Exchange | X |
| Calendario personal | |
| Exportar parámetros de correo electrónico | X |
| Dispositivos compartidos | |
| Integrar Endpoint Management en Microsoft Intune/EMS | |
| Office 365 | X |
| LDAP Exchange Server 2010, 2013 y 2016 | X |
| Autenticación basada en certificados (CBA) | |
| GoToMeeting | X |
| Skype Empresarial | |
| Lista de distribución personal | X |
| Compatibilidad con Citrix Files | X |
| Inscripción por correo electrónico con Single Sign-On | X |

La siguiente tabla ofrece una lista de las funciones de Secure Web que son compatibles con Android Enterprise.

| (Función) | Asistencia técnica |
|---|---|
| Modo Secure Browse | X |
| Modo de VPN completa | X |
| Todas las funciones de aplicación | X |
| Compatibilidad con Secure Mail | X |

#### Limitaciones

- Si la opción **Permitir el uso de la barra de estado** está **habilitada** para Android Enterprise en el modo de perfil de trabajo, el progreso de la exportación del calendario y las notificaciones push en Secure Mail para Android no se muestran en la barra de estado. Sin embargo, estas notificaciones se ven en la pantalla bloqueada cuando se permite. Para obtener más información, consulte Parámetros de Android Enterprise.

## Funciones de iOS y Android para Secure Mail

October 19, 2020

En este artículo se describen las funciones de iOS y Android que se admiten en Secure Mail.

### Compatibilidad con Azure Government Cloud Computing

Secure Mail es compatible con autenticación moderna (OAuth) de Government Cloud Computing (GCC) High en arrendatarios de Azure Active Directory. Secure Mail está registrado como punto final en GCC High, a efectos de cumplir con los requisitos obligatorios de Microsoft para todos los servicios de GCC High. Para obtener información detallada, consulte Novedades de Azure Active Directory en Microsoft 365 Government.

Con este cambio, el usuario se enruta a GCC High en el arrendatario de Azure Active Directory para la autenticación. Además, el administrador debe conceder permisos para Secure Mail en el arrendatario de Azure Active Directory.

#### Requisitos previos

Asegúrese de que el administrador global de Azure Active Directory haga lo siguiente:

- Descargue la última versión de Secure Mail en su dispositivo.

- Configure su cuenta de Exchange en la aplicación Secure Mail y otorgue permiso de aplicación en Azure Active Directory para que todos los usuarios inicien sesión. Consulte la siguiente pantalla.

> **Nota:**
>
> Los administradores globales deben hacer esto una sola vez. Una vez que se concede acceso a la aplicación, basta con actualizar la versión desde App Store.

#### Después de la actualización de versión

Después de una actualización de versión, se le solicitará que renueve la autorización una vez que caduque el token de actualización, que redirige a GCC High en Azure AD. Valide el flujo de trabajo anterior para asegurarse de que la solicitud de autorización se envía a GCC High en Azure AD.

Puede validar el flujo de trabajo de una de las siguientes maneras:

- Secure Mail con el nombre de aplicación **Secure Mail-GCC High** aparece en la página de inicio de sesión del arrendatario de Azure Active Directory.
- Compruebe los registros de Secure Mail para confirmar que los redireccionamientos se producen a través de https://login.microsoftonline.us después de la reautenticación.

### Compatibilidad con archivos ICS

En Secure Mail, puede obtener una vista previa de los archivos ICS que recibe como datos adjuntos e importarlos a su calendario como eventos.

### Imagen de contacto en Secure Mail

En Secure Mail, puede ver la imagen de un contacto al agregar destinatarios en correos electrónicos o invitaciones a reuniones. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Mostrar imágenes de los contactos.

### Administrar sus feeds

En Secure Mail, puede organizar su tarjeta de **Feeds** en función de sus requisitos. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Organizar el correo electrónico.

### Utilice la directiva de Office 365 Exchange Server para definir la dirección del servidor de Office 365

En Secure Mail, se agrega una nueva directiva llamada **Office 365 Exchange Server** en la sección Funcionalidad OAuth para Office 365. Con esta directiva, puede definir el nombre de host para el buzón de Office 365 presente en la nube. Esta directiva también habilita la compatibilidad con Office 365 para agencias gubernamentales. El nombre de host es un valor único, como *outlook.office365.com*. El valor predeterminado es *outlook.office365.com*.

### Compatibilidad con la administración de cifrado

La administración de cifrado le permite utilizar la seguridad moderna de la plataforma del dispositivo para, al mismo tiempo, garantizar que dicho dispositivo permanezca en un estado suficiente para utilizar la seguridad de la plataforma de manera eficaz. Con la administración de cifrado, elimina la redundancia en el cifrado de datos locales, ya que son las plataformas Android y iOS las que proporcionan el cifrado del sistema de archivos. Para habilitar esta función, un administrador debe configurar la directiva MDX **Tipo de cifrado** en **Cifrado de plataforma con cumplimiento de requisitos** en la consola de Citrix Endpoint Management.

Para utilizar la función de administración de cifrado, en la consola de Citrix Endpoint Management, establezca la directiva **Tipo de cifrado** en **Cifrado de plataforma con cumplimiento de requisitos**. Esto habilita la administración de cifrado, y todos los datos de las aplicaciones cifradas existentes en los dispositivos de los usuarios pasan directamente a un estado cifrado por el dispositivo y no por MDX. Durante esta transición, la aplicación se pausa para una única migración de datos. Una vez realizada correctamente la migración, la responsabilidad del cifrado de los datos almacenados localmente se transfiere de MDX a la plataforma del dispositivo. MDX continúa comprobando el cumplimiento de requisitos en el dispositivo durante cada inicio de la aplicación. Esta función opera tanto en entornos MDM + MAM como en solo MAM.

Cuando establece la directiva **Tipo de cifrado** en **Cifrado de plataforma con cumplimiento de requisitos**, la nueva directiva reemplaza el cifrado MDX existente.

Para obtener información detallada acerca de las directivas MDX de administración de cifrado para Secure Mail, consulte la sección **Cifrado** en:

- Directivas MDX para aplicaciones móviles de productividad para Android
- Directivas MDX para aplicaciones móviles de productividad para iOS

Cuando un dispositivo no cumple todos los requisitos mínimos de conformidad, la directiva **Comportamiento de dispositivos no conformes** le permite seleccionar qué hacer al respecto:

- **Permitir aplicación**: Permite que la aplicación se ejecute normalmente.
- **Permitir aplicación después de la advertencia**: Advierte al usuario que una aplicación no cumple los requisitos mínimos de conformidad y permite que la aplicación se ejecute. Este

es el valor predeterminado.
- **Bloquear aplicación**: Impide que la aplicación se ejecute.

#### Dispositivos con iOS

Los siguientes criterios determinan si un dispositivo cumple los requisitos mínimos de conformidad para dispositivos con iOS.

- iOS 10: Una aplicación tiene una versión de sistema operativo que es mayor o igual que la versión especificada.
- Acceso de depurador de errores: Una aplicación no tiene habilitada la depuración de errores.
- Dispositivo liberado por jailbreak: Una aplicación no se está ejecutando en un dispositivo liberado por jailbreak.
- Código de acceso del dispositivo: El código de acceso del dispositivo está **activado**.
- Uso compartido de datos: El uso compartido de datos no está habilitado para la aplicación.

#### Dispositivos con Android

Los siguientes criterios determinan si un dispositivo cumple los requisitos mínimos de conformidad para dispositivos con Android.

- Android SDK 24 (Android 7 Nougat): Una aplicación tiene una versión de sistema operativo que es mayor o igual que la versión especificada.
- Acceso de depurador de errores: Una aplicación no tiene habilitada la depuración de errores.
- Dispositivos liberados por root: Una aplicación no se está ejecutando en un dispositivo liberado por root.
- Bloqueo de dispositivo: El código de acceso del dispositivo está **activado**.
- Dispositivo cifrado: Una aplicación se está ejecutando en un dispositivo cifrado.

### Compatibilidad con mensajes de correo electrónico adaptativos

Secure Mail se ha optimizado para ofrecer correos electrónicos adaptativos. Anteriormente, el contenido de los correos electrónicos con tablas o imágenes grandes no se mostraba correctamente. Esta función ofrece contenido de correo electrónico que se lee mejor en todos los dispositivos compatibles, independientemente del formato y tamaño del correo electrónico.

### Arrastrar y colocar eventos del Calendario

En Secure Mail, puede arrastrar y colocar un evento existente de calendario para cambiarle la hora. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Cambiar el momento de un evento de calendario.

### Administrar sus feeds

En Secure Mail, puede organizar su tarjeta de **Feeds** en función de sus requisitos. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Organizar el correo electrónico.

### Avance automático

En Secure Mail, cuando elimina un mensaje en **Conversaciones**, puede elegir a qué mensaje volver. Para utilizar esta función, vaya a **Parámetros > Avance automático**. A continuación, seleccione su preferencia entre las opciones disponibles. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Eliminar y avanzar automáticamente a un correo electrónico en Conversaciones.

### Sincronización automática de la carpeta Borradores

La carpeta Borradores se sincroniza automáticamente y los borradores están disponibles en todos los dispositivos. Esta función está disponible en dispositivos que ejecutan Office 365 o Exchange Server 2016 y versiones posteriores.

> **Nota:**
>
> Si el borrador de Secure Mail contiene datos adjuntos, los datos adjuntos no se sincronizan con el servidor.

Para ver documentación de ayuda para usuarios y un vídeo sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Sincronización automática de la carpeta Borradores.

### Compatibilidad con Single Sign-On cuando se utiliza Microsoft Intune en el modo MDM + MAM

Para dispositivos que ejecutan iOS:

Para poder usar esta función, la aplicación Microsoft Authenticator debe estar instalada en el dispositivo. Para obtener más información acerca de la instalación de la aplicación Microsoft Authenticator, consulte **Descarga e instalación de la aplicación Microsoft Authenticator** en docs.microsoft.com.

Para dispositivos que ejecutan Android:

Para poder usar esta función, la aplicación Portal de empresa de Intune debe estar instalada en el dispositivo. Una vez que haya iniciado sesión en la aplicación Portal de empresa de Intune, podrá utilizar SSO en el modo MDM + MAM sin tener que volver a autenticarse en Secure Mail con sus credenciales

## Mejoras en Contactos

En Secure Mail, cuando toca **Contactos** y selecciona un contacto, los detalles de ese contacto aparecen en la ficha **Contacto**. Al pulsar la ficha **Organización**, aparecen los detalles de la jerarquía de la organización, como **Administrador**, **Colaboradores directos** y **Compañeros**. Al tocar el icono Más en la parte superior derecha de la pantalla, aparecen las siguientes opciones:

- Edit (Modificar)
- Agregar a VIP
- Cancelar

En la ficha **Organización**, puede tocar en el icono "Más", situado a la derecha de **Administrador**, **Colaboradores directos** o **Compañeros**. Esta acción permite crear un correo electrónico o un evento de calendario. El campo **Para:** del correo electrónico o
evento de calendario se rellena automáticamente con los detalles de **Administrador**, **Colaboradores directos** o **Compañeros**. Puede redactar y enviar el correo electrónico.

### Requisitos previos

Compruebe que los servicios web de Exchange (EWS) están habilitados en su servidor de Exchange.

Los detalles de contacto que aparecen dependen de los detalles de la organización (contacto de Outlook), obtenidos de Active Directory. Para que aparezcan los detalles correctos para sus contactos, compruebe que el administrador haya definido la jerarquía de la organización en Active Directory.

> **Nota:**
>
> Esta función no está disponible en el servidor IBM Lotus Notes.

## Exportar la hora y la ubicación de la reunión a su calendario nativo

En Secure Mail, se agrega un nuevo valor **Hora de reunión, Ubicación** a la directiva MDX **Exportar calendario**. Esta mejora permite exportar la hora y la ubicación de las reuniones de los eventos del calendario de Secure Mail a su calendario nativo.

## Varias cuentas de Exchange

Desde Parámetros en Secure Mail, puede agregar varias cuentas de correo electrónico de Exchange y cambiar entre ellas. Esta función permite supervisar todos sus correos, contactos y calendarios desde un único sitio. Los requisitos previos de administración son los siguientes:

- Se requiere un nombre de usuario y una contraseña para configurar cuentas adicionales. Las configuraciones de almacén de credenciales o inscripción automática se aplican solo a la

primera cuenta configurada en la aplicación. Escriba el nombre de usuario y la contraseña para todas las cuentas adicionales.

- Si la primera cuenta que se crea está basada en certificados, ya no se pueden agregar más cuentas basadas en certificados. Las cuentas adicionales deben usar la autenticación por Active Directory. Secure Mail no admite la autenticación basada en certificados cuando se configuran varias cuentas.
- Para que las cuentas adicionales puedan conectarse a un dominio o al servidor Exchange Server de una red externa, debe **activar** el túnel dividido en Citrix ADC.
- Secure Mail para iOS admite solamente servidores de correo de Exchange y Office 365.

Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Agregar cuentas de Exchange.

### Contactos

Para ver documentación de ayuda para usuarios sobre Contactos, consulte el artículo del Centro de ayuda para usuarios de Citrix Ver y sincronizar los contactos.

### Establecer colores en Calendarios

Para ver documentación de ayuda para usuarios sobre esta función del calendario, consulte el artículo del Centro de ayuda para usuarios de Citrix Establecer colores para calendarios de Secure Mail sincronizados.

### Dominios internos

Puede identificar y modificar destinatarios de correo que pertenezcan a organizaciones externas.

**Requisito previo:** Compruebe que se ha habilitado la directiva **Dominios internos** en Citrix Endpoint Management y que se ha reiniciado la aplicación.

Al crear, responder o reenviar un correo electrónico, los destinatarios externos se resaltan en la lista de correo. El icono **Contactos** aparece como una advertencia en la parte inferior izquierda de la pantalla. Toque el icono **Contactos** para modificar la lista de correo.

En dispositivos con iOS:

En dispositivos con Android:

Cuando toca el icono **Contactos**, aparece una ventana emergente con opciones para modificar la lista o eliminar todo. Pulse **Modificar lista** para elegir los destinatarios que quiere eliminar. Después de seleccionar los destinatarios, pulse el icono **Papelera**.

En dispositivos con iOS:

En dispositivos con Android:

### Mejoras ergonómicas

Con esta mejora, los botones de acción se han movido de la parte superior de la pantalla a la parte inferior para facilitar el acceso. Estos cambios se han implementado en las pantallas **Bandeja de entrada**, **Calendario** y **Contactos**.

> Nota:
>
> En el caso de Android, los cambios se han implementado en las pantallas **Bandeja de entrada** y **Calendario**.

En dispositivos con iOS

En dispositivos con Android

El botón de acción flotante **Responder** se ha mejorado para alinearse con la guía de estilo y la personalización de marca de Citrix.

Además, con esta mejora se elimina la opción de acceder a los botones de la pantalla principal de la Bandeja de entrada desde un correo electrónico abierto. Tiene que salir del correo electrónico abierto para acceder a elementos como **Feeds**, **Calendario**, **Contactos**y **Anexos**.

Las opciones en la barra de pie de página de iOS se han cambiado, lo que ayuda a mantener la uniformidad entre iOS y Android.

### Integrar Secure Mail con Slack (Tech Preview)

Ahora puede llevar su conversación por correo electrónico a la aplicación Slack en dispositivos iOS o Android. Para obtener información detallada, consulte Integrar Secure Mail con Slack (Tech Preview).

### Notificar mensaje de phishing (en calidad de reenvío)

En Secure Mail, puede usar la función “Notificar phishing” para informar sobre un correo electrónico sospechoso de phishing como un reenvío. Puede reenviar los mensajes sospechosos a las direcciones de correo electrónico que los administradores configuren en la directiva. Para habilitar esta función, un administrador debe configurar la directiva “Direcciones para notificar mensaje de phishing” y definir el **Mecanismo para notificar phishing** en **Notificar mediante reenvío**. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Notificar mensajes de phishing.

### Notificar mensajes de phishing

Puede notificar intentos de phishing en función de la directiva que configure un administrador. Para ver documentación de ayuda para usuarios sobre esta función y obtener información detallada sobre

los parámetros de administración, consulte el artículo del Centro de ayuda para usuarios de Citrix Notificar mensajes de phishing.

### Exportar eventos del calendario de Secure Mail

Con Secure Mail para iOS y Android, puede exportar eventos de calendario de Secure Mail a la aplicación de calendario nativa de su dispositivo. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Exportar eventos del calendario de Secure Mail.

Dispone de los siguientes valores de directiva MDX para los campos de eventos del calendario que aparecen en el calendario personal:

- Ninguno (No exportar)
- Hora de reunión
- Hora de reunión, Lugar
- Hora, asunto, lugar
- **(Para Android)** Hora, asunto, lugar, notas
- **(Para iOS)** Hora, disponibilidad, asistentes, asunto, lugar, notas

**Opciones de Android:**

**Opciones de iOS:**

#### Para iOS

Aunque los eventos de calendario exportados desde Secure Mail son de **lectura y escritura**, los cambios realizados en eventos fuera de Secure Mail no están disponibles.

**Importante:**

- Esta función está visible (pero inhabilitada) en Secure Mail si se cumple una de las siguientes condiciones:
  - La directiva “Exportar calendario” está **desactivada**.
  - Su versión de MDX no contiene la directiva.
- Esta función no funciona si las cuentas de correo electrónico ya están configuradas en su aplicación de calendario personal y su cuenta de iCloud está inhabilitada. Esta función funcionará si no hay ninguna otra cuenta configurada en la aplicación de calendario personal.
- Para iniciar la URL y modificar los eventos del calendario de Secure Mail desde el calendario personal, el valor **“ctxevent:”** debe estar incluido en la directiva MDX “Esquemas de URL de aplicaciones”.

**Para Android**

Los eventos de calendario que se exporten desde Secure Mail son de solo lectura. Para modificar los eventos de Secure Mail, toque el enlace **Evento de Secure Mail** en el evento de calendario.

**Importante:**

- Esta función está visible (pero inhabilitada) en Secure Mail si se cumple una de las siguientes condiciones:
  - La directiva "Exportar calendario" está **desactivada**.
  - Su versión de MDX no contiene la directiva.
- La directiva MDX "Intercambio de documentos entrantes" debe estar establecida en **Sin restricciones**.
- El enlace "Evento de Secure Mail" no está disponible en dispositivos Samsung o Huawei.

## Carpetas Feeds

Secure Mail destaca todos los correos electrónicos no leídos, las invitaciones a reuniones que requieren su atención y las próximas reuniones en la carpeta **Feeds**.

**Para ver sus tarjetas de feeds**

Toque el icono **Feeds** en la parte inferior derecha de la barra de fichas al pie de página.

Aparecen las siguientes tarjetas de feeds:

- No leído
- Invitaciones de reunión
- Próximas reuniones

De forma predeterminada, Secure Mail muestra feeds provenientes solamente de su cuenta principal. Si ha configurado más de una cuenta, puede ver feeds de otras cuentas. Para ver los feeds de otras cuentas, toque **Feeds**, toque el icono de tres líneas y seleccione la cuenta correspondiente.

Los feeds se ordenan según la marca de tiempo del elemento y aparecen con el siguiente límite superior:

- Cinco correos electrónicos no leídos
- Dos invitaciones de reunión
- Tres próximas reuniones

Para ver todos los elementos en una tarjeta de feeds, toque **Ver todo**.

> **Nota:**
>
> La cantidad de feeds que se muestra en cada tarjeta depende del período de sincronización de

> correo que haya configurado en el dispositivo.

#### Mejoras en la carpeta Feeds

A continuación se presentan las mejoras a las existentes. Carpeta **Feeds**:

- Las invitaciones a las reuniones de todas las carpetas sincronizadas automáticamente aparecen en la tarjeta Feeds.
- Puede ver hasta cinco de las próximas reuniones en su tarjeta Feeds.
- Las reuniones para el periodo de las próximas 24 horas aparecen en la tarjeta Feeds y se clasifican en las secciones **Hoy** y **Mañana**.

### Feeds del administrador

En Secure Mail, puede ver los correos electrónicos del administrador en la pantalla **Feeds**. Puede aparecer un máximo de cinco mensajes de correo electrónico en los feeds **De su administrador**, en función de los parámetros del **Periodo de sincronización de correo**. Para ver más correos electrónicos de parte del administrador, toque **Ver todo**.

**Requisitos previos:**

Compruebe que los servicios web de Exchange (EWS) están habilitados en su servidor de Exchange.

Los datos que aparecen en la tarjeta de administrador dependen de los detalles de la organización (contacto de Outlook), obtenidos de Active Directory. Para que aparezcan los detalles correctos en el feed del administrador, compruebe que el administrador haya definido la jerarquía de la organización en Active Directory.

> **Nota:**
>
> Esta función no está disponible en el servidor IBM Lotus Notes.

### Unirse a reuniones desde el calendario

En Secure Mail, los usuarios pueden unirse a reuniones directamente desde las invitaciones en el Calendario. En las siguientes tablas se enumeran los tipos de reunión y formatos de número de teléfono admitidos, y sus respectivos requisitos de marcado.

#### Tipos de reunión admitidos

| Tipo de reunión | Requisitos de identificación | Acción después de tocar en Unirse a la reunión |
|---|---|---|
| GoToMeeting (GTM) | Alguno de los siguientes en el contenido de la reunión: 1) Este tipo de URL: `https://www1.gotomeeting.com/join/1234567892`; 2) Código de acceso de GTM en alguno de estos formatos: GTM: 123456789, GTM – 123456789, G2M – 123456789, G2M: 123456789 | Si la aplicación GTM está instalada, esta se inicia y el usuario se une a la reunión. Si la aplicación no está instalada, el usuario ve una opción para ir a la tienda de aplicaciones para instalar GTM. Para reuniones de GoToMeeting en el formato gotomeet.me/nombreDeUsuario, la aplicación se abre y el usuario se une a la reunión. |
| WebEx | | Citrix Secure Web se abre e inicia la aplicación de WebEx sin empaquetar, si está instalada en el dispositivo. WebEx debe agregarse como excepción en la directiva de Secure Web “Lista de excepciones de la apertura restringida” en Android y en la directiva “Direcciones URL permitidas” en iOS. |

| Tipo de reunión | Requisitos de identificación | Acción después de tocar en Unirse a la reunión |
|---|---|---|
| Skype Empresarial | | Los usuarios pueden hacer clic en un enlace que se abre en Secure Web, que a su vez abre la aplicación Skype Empresarial no empaquetada si está instalada en el dispositivo. Agregue la aplicación Skype Empresarial como excepción en la directiva “Lista de excepciones de la apertura restringida” de Secure Web en Android. Agregue la excepción en la directiva “Direcciones URL permitidas” en iOS. |

Configurar la siguiente lista de directivas permite a los usuarios tocar en un enlace de reunión para abrir la aplicación correspondiente.

**Aplicación Zoom**

- **iOS: “Directiva “Permitir direcciones URL”:** +^zoomus:
- **Android - Directiva “Exclusiones de la apertura”:**{action=android.intent.action.VIEW scheme=zoomus package=us.zoom.videomeetings}

**WebEx (aplicación no empaquetada)**

- **iOS - “Allow URLs” Policy”:** +^wbx: Example policy string is ^http:,^https:,^mailto:=ctxmail:,+^citrixreceiver g2m-2:,+^col-g2w-2:,+^wbx:,+^maps:ios_addr:
- **Android - Directiva “Exclusiones de la apertura”:** {action=android.intent.action.VIEW scheme=wbx package=com.cisco.webex.meetings}

**Skype Empresarial**

- **iOS - Directiva “Direcciones URL permitidas”:** +^lync:

- **Android - Directiva "Exclusiones de la apertura":**{action=android.intent.action.VIEW scheme=lync package=com.microsoft.office.lync15}

**Skype**

- **iOS - Directiva "Direcciones URL permitidas":** +^skype:
- **Android - Directiva "Exclusiones de la apertura":** {action=android.intent.action.VIEW scheme=skype package=com.skype.raider}

**Especificaciones de marcado**

En la siguiente lista se indica el tipo de reunión y el formato respectivo del número de teléfono admitido, así como el formato del código de conferencia para cada uno.

**GoToMeeting (GTM):**

Formatos de número de teléfono admitidos:

- Cualquier número de teléfono en formatos de GTM. Ejemplos:
  - India (gratuito): 000 800 100 7855
  - Estados Unidos (gratuito): 1 877 309 2073
- Cualquier número de teléfono que satisfaga los estándares de formato RFC 3966. Para obtener más detalles, consulte la Documento de protocolo de seguimiento de normas de Internet.

Formatos de códigos de conferencia admitidos:

El código de conferencia se selecciona desde alguno de los formatos siguientes en el cuerpo de la reunión:

- URL (*.gotomeeting.com/join/123456789)
- URL (formato `gotomeet.me/username`)
- Formatos "GTM", como "GTM:123456789"
- Formatos "G2M" como "G2M:123456789"
- Formatos como "Código de acceso: 123456789"

**WebEx:**

Formatos de número de teléfono admitidos:

- Cualquier número de teléfono en formato de llamada Call-in de WebEx. Ejemplos (Verizon y EE. UU.):
  - 1-866-652-5088
  - 1-517-466-3109
- Cualquier número de teléfono en formato de conexión de audio de WebEx. Ejemplo:
  - 1-650-479-3207 (de pago EE. UU.)
- Cualquier número de teléfono que satisfaga los estándares de formato RFC 3966.

Formatos de códigos de conferencia admitidos:

El contenido de la reunión debe contener alguno de los formatos siguientes:

- Número de reunión: 123 456 789
- Código de acceso: 123 456 789

> **Nota:**
>
> Para códigos de conferencia de 9 dígitos o menos, se agrega almohadilla (#) automáticamente para entrar en la reunión.

#### Skype Empresarial

Formatos de número de teléfono admitidos:

- Cualquier número de teléfono en formatos RFC 3966. Para obtener más detalles, consulte la Documento de protocolo de seguimiento de normas de Internet.

Formatos de códigos de conferencia admitidos:

El cuerpo de la reunión contiene este texto: “ID de conferencia: 123456789”

> **Nota:**
>
> La almohadilla (#) se agrega automáticamente para las reuniones de Skype Empresarial.

#### Información genérica de audioconferencia

Formatos de número de teléfono admitidos:

- Cualquier número de teléfono en formatos RFC 3966. Para obtener más información, consulte el Documento de protocolo de seguimiento de normas de Internet. Ejemplos:
  - 5555555555
  - (555) 555-5555
  - 555-555-5555
  - 555-555-555-5555 (en el caso de incluir código de país)
  - 1-555-555-5555
  - +1-555-555-5555

> **Nota:**
>
> Use un único separador entre los dígitos del número de teléfono. Por ejemplo, si usa “) –” puede que no sea posible reconocer el número.

**Formatos de códigos de conferencia admitidos:**

Formato recomendado: “(número de teléfono)”,”(código)”

Puede especificar hasta cuatro comas y proporcionar la tecla # si es necesario. Consulte la tabla más adelante en este documento para ver una lista de los formatos compatibles.

Para una conferencia de audio, los siguientes formatos permiten a los usuarios tocar en **Marcar**. Sin embargo, si tocan en el número de teléfono desde el cuerpo de la reunión en el calendario, pueden entrar en la reunión. A continuación, deben introducir manualmente los códigos de conferencia. Se admiten los siguientes formatos de número de teléfono y códigos de conferencia.

| Formatos de número de teléfono admitidos | Separador de código de conferencia | Ejemplo |
|---|---|---|
| Cualquier número de teléfono en formatos RFC 3966. Ejemplos: 5555555555; (555) 555-5555; 555-555-5555; 555-555-555-5555 (en caso de ser el código de un país); 1-555-555-5555;+1-555-555-5555 | Código de participante | 1-888-999-9999 Código de participante: 9999999 |
| | PIN de participante | 1-888-999-9999 PIN de participante: 99999999 |
| | Código de invitado | 1-888-999-9999 Código de invitado: 99999999 |
| | PIN de invitado | 1-888-999-9999 PIN de invitado: 99999999 |
| | Código de participante o invitado | 1-888-999-9999 Código de participante o invitado: 99999999 |
| | Código de presidencia | 1-888-999-9999 Código de presidencia: 99999999 |
| | PIN de presidencia | 1-888-999-9999 PIN de presidencia: 99999999 |
| | Código de presidente | 1-888-999-9999 Código de presidente: 99999999 |
| | PIN de presidente | 1-888-999-9999 PIN de presidente: 99999999 |
| | PIN de organizador | 1-888-999-9999 PIN de organizador: 99999999 |
| | PIN | 1-888-999-9999 PIN:99999999 |

| Formatos de número de teléfono admitidos | Separador de código de conferencia | Ejemplo |
|---|---|---|
| | Código de acceso | 1-888-999-9999 Código de acceso: 99999999 |
| | Código | 1-888-999-9999 Código: 99999999 |
| | Código de conferencia | 1-888-999-9999 Código de conferencia: 99999999 |
| | ID de conferencia | 1-888-999-9999 ID de conferencia: 99999999 |
| | , | +1 (631) 992-3240,958209234# |
| | „ | +1 (631) 992-3240„958209234# |
| | „, | +1 (631) 992-3240„,958209234# |
| | „„ | +1 (631) 992-3240„„958209234# |
| | código de acceso | +1 (631) 992-3240 código de acceso 958209234# |
| | ext: | +1 (631) 992-3240 ext:958209234# |
| | 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# |

| Formatos de número de teléfono admitidos | Separador de código de conferencia | Ejemplo |
|---|---|---|
| | PC | +1 (631) 992-3240 PC 958209234# |
| | pc | +1 (631) 992-3240 pc 958209234# |

### Superponer calendarios personales

En dispositivos iOS y Android, puede importar su calendario personal desde la aplicación nativa de calendario y ver los eventos personales en Secure Mail. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Ver los eventos de su calendario personal.

### Insertar una imagen alineada

En el siguiente procedimiento se describe cómo insertar una imagen alineada.

1. Para adjuntar una imagen alineada a su correo electrónico, mantenga pulsado el cuerpo del mensaje. En las opciones que aparecerán, toque **Insertar imagen**.
2. Secure Mail puede solicitarle acceso a sus fotos. Aparecerá la Galería de fotos. Vaya a la galería y toque la imagen que quiera insertar.
3. El correo contendrá la imagen que haya seleccionado.

### Acciones de deslizamiento

En dispositivos iOS y Android, al deslizar un mensaje de correo electrónico a la izquierda o a la derecha, se realizan determinadas acciones. Para ver documentación de ayuda para usuarios sobre esta función, consulte el artículo del Centro de ayuda para usuarios de Citrix Usar acciones de deslizamiento.

### Unirse a reuniones de Skype Empresarial en iOS o Android

Puede unirse a las reuniones de Skype Empresarial sin problemas a través de Secure Mail. Esta función requiere que la aplicación Skype Empresarial esté instalada en su dispositivo.

#### Para unirse a una reunión de Skype Empresarial

1. Toque el recordatorio de reunión o en el evento del calendario de Skype Empresarial.

2. En la pantalla **Detalles del evento**, toque la opción **Asistir a la reunión** de Skype. La reunión de Skype Empresarial comienza en una nueva ventana.

   Si no ha instalado Skype Empresarial en el dispositivo, toque **Instalar Skype** para instalar la aplicación.

### Vista previa de datos adjuntos en la aplicación y otras mejoras

Ahora puede obtener una vista previa de los datos adjuntos (MS Office e imágenes) en Secure Mail dentro de la aplicación, en lugar de abrirlos con aplicaciones de terceros, como QuickEdit.

Puede hacer lo siguiente para ver los datos adjuntos:

- Seleccionar un mensaje existente en un buzón para adjuntarle un archivo.
- Seleccionar un mensaje nuevo para adjuntarle un archivo.
- Guardar los datos adjuntos para acceder a ellos sin conexión.
- Eliminar los datos adjuntos de archivos sin conexión.
- Abrir los datos adjuntos mediante una aplicación diferente.
- Ver el evento de calendario o el mensaje de correo electrónico de origen de los archivos adjuntos.

> **Nota:**
>
> Solamente se puede ver el evento de calendario o el mensaje de correo electrónico de origen cuando se ven los datos adjuntos desde el repositorio **Datos adjuntos**.

También puede obtener una vista previa de los datos adjuntos en los siguientes casos:

- Al ver un mensaje.
- Al redactar un mensaje nuevo.
- En carpeta de datos Adjuntos.
- Eventos de calendario.

#### Para seleccionar un mensaje al que adjuntar un archivo

1. Abra el correo electrónico con los datos adjuntos.
2. Toque el archivo adjunto.
3. Toque el icono **Adjuntar**.

   Aparecerá la Bandeja de entrada.
4. Seleccione un mensaje para adjuntarle este archivo, o toque **Nuevo mensaje** para adjuntarlo a un mensaje nuevo.

**Para guardar los datos adjuntos para acceder a ellos sin conexión**

1. Abra los archivos adjuntos.
2. Toque el icono **Más** en la parte superior derecha de la página y en **Guardar sin conexión** para guardar el archivo adjunto para el acceso sin conexión.

**Para eliminar los archivos adjuntos de archivos sin conexión**

1. Abra los archivos adjuntos.
2. Toque el icono **Más** en la parte superior derecha de la página y **Quitar archivos sin conexión** para eliminar el archivo adjunto de los archivos sin conexión.

**Para abrir datos adjuntos con otra aplicación**

1. Abra los archivos adjuntos.
2. Toque el icono **Más** en la parte superior derecha de la página y en **Abrir con**. para abrir los datos adjuntos con otra aplicación.
3. En las opciones que aparecen, toque la que quiera usar para abrirlo.

**Para ver el evento de calendario o el mensaje de correo electrónico de origen de los datos adjuntos**

1. Toque el icono **Adjuntos** situado en la parte inferior derecha de la pantalla.
2. Toque **Sin conexión**.
3. Toque uno de los archivos adjuntos y luego toque el icono **Más** en la parte superior derecha de la pantalla.
4. Aparecerá el mensaje de correo electrónico de origen.

## Migrar nombres de usuario a direcciones de correo electrónico (UPN)

En Secure Mail para iOS y Android, puede migrar desde la autenticación con nombre de usuario y contraseña de Exchange a la autenticación con nombre UPN y contraseña.

Con esta función habilitada, no tendrá que:

- Reinstalar Secure Mail.
- Eliminar y agregar la cuenta en Secure Mail.
- Cambiar el nombre de usuario en Secure Mail.

**Requisitos previos**

Para poder proceder a esta migración, los usuarios deben ejecutar Secure Mail 10.7.25 o una versión posterior.
Para usar esta función, debe habilitar la directiva “Intentar migración de nombre de usuario en caso de fallo de autenticación”.

**Para migrar a la autenticación por nombre UPN**

1. Habilite la directiva “Intentar migración de nombre de usuario en caso de fallo de autenticación” en Endpoint Management.
2. Migre su cuenta de usuario de Exchange a un nuevo nombre UPN que coincida con la dirección de correo electrónico SMTP principal del usuario.
   Eso desencadena un error de autenticación. Secure Mail intentará la autenticación mediante la dirección de correo electrónico SMTP principal.

En caso de una autenticación correcta, la cuenta de usuario se migra al nombre UPN actualizado.

**Para verificar la migración**

**En dispositivos iOS:** Vaya a **Ajustes** y toque la cuenta para ver los detalles. En caso de una migración correcta, la dirección de correo electrónico SMTP principal aparece en el campo **Nombre de usuario** de la pantalla **CUENTA**.

**En dispositivos Android:** Vaya a **Ajustes** y toque la cuenta para ver los detalles. En caso de una migración correcta, la dirección de correo electrónico SMTP principal aparece en el campo **Nombre de usuario** de la pantalla **Detalles de la cuenta**.

**Listas de distribución personales**

**Requisitos previos**

- Los servicios web de Exchange (EWS) están habilitados en su servidor de Exchange.
- Microsoft Exchange Server 10 SP1 o versiones posteriores.

Secure Mail para iOS y Android admite grupos de contactos personales. En Secure Mail, aparecen los grupos de contactos que haya creado en su cliente de escritorio de Outlook. Los grupos de contactos que haya creado aparecen en Contactos en Secure Mail.

> **Nota:**
>
> No puede ver los miembros de un grupo de contactos anidado en Secure Mail.

Puede usar las listas de distribución personales cuando redacta un correo electrónico o crea un evento de calendario. Si ha creado un grupo de contactos personales (lista de distribución) mediante Exchange, esa lista aparece en Secure Mail.

**Para ver una lista de distribución personal**

1. En Secure Mail, abra **Contactos**.
2. Escriba el nombre del grupo de contactos.
   El grupo aparece en los resultados de búsqueda.
3. Toque el grupo de contactos para ver los miembros que lo componen.

> **Nota**:
>
> No puede modificar un grupo de contactos en Secure Mail.

**Para redactar un correo para un grupo de contactos**

1. Abra Secure Mail y toque el botón de acción flotante **Modificar** para redactar un correo.
2. En la pantalla **Nuevo mensaje**, escriba el nombre del grupo de contactos en el campo **Para:**.
3. De la lista de contactos que aparece, seleccione el grupo de contactos.

   Los grupos de contactos se indican con el siguiente icono:

**Para enviar una invitación de calendario a un grupo de contactos**

1. Abra Secure Mail y vaya a **Calendario**.
2. Toque el icono **+** para crear un evento de calendario.
3. En la pantalla **Nuevo evento**, toque **Invitados** para agregar nuevos miembros.
4. Escriba el nombre del grupo de contactos para enviar la invitación al grupo.
5. De la lista de contactos que aparece, seleccione el grupo de contactos.

## Firmas de texto enriquecido

En Secure Mail para iOS y Android, puede usar imágenes o enlaces en su firma de correo electrónico. Para actualizar su firma, simplemente copie y pegue imágenes o enlaces en el campo de firma.

**Para agregar una firma de texto enriquecido**

1. Copie la imagen o URL que quiere usar.
2. Vaya a **Secure Mail > Parámetros > Firma**.
3. Pegue la imagen o URL.

Alternativamente, en dispositivos iOS, puede presionar prolongadamente en el campo de la firma y tocar en **Insertar imagen** para seleccionar una imagen de su galería.

## Sincronización de carpeta

En Secure Mail para iOS y Android, puede tocar el icono **Sincronizar** para actualizar todo el contenido de Secure Mail. Encontrará el icono **Sincronizar** en los paneles deslizables de Secure Mail como Buzones, Calendarios, Contactos y Archivos adjuntos. Cuando toca el icono **Sincronizar**, se actualizan las carpetas que haya configurado para la actualización automática, como Buzones, Calendarios y Contactos. La marca de hora de la última sincronización aparece junto al icono **Sincronizar**.

**Para sincronizar sus carpetas**

1. Abra Secure Mail.
2. Desde las carpetas disponibles en la barra de fichas del pie de página, toque la carpeta que desea sincronizar.
3. Toque el icono de tres líneas situado en la esquina superior izquierda de su pantalla.
4. Toque el icono **Sincronizar** en la parte inferior izquierda de tu pantalla.
5. Se sincronizará la carpeta y su contenido se actualizará. La marca de hora aparece junto al icono **Sincronizar**.

## Mejoras para adjuntar fotos

En Secure Mail para iOS y Android, puede adjuntar fotos fácilmente al tocar en el nuevo icono **Galería**.

**Para adjuntar fotos a su correo electrónico**

1. Abra Secure Mail.
2. Toque **Redactar** para crear un correo o toque el botón de acción flotante **Responder** para responder a un correo electrónico.
3. Toque el icono **Galería** al lado del icono de **Archivos Adjuntos** en la parte inferior derecha de su pantalla.

4. Su galería aparecerá en la parte inferior de la pantalla junto con los iconos **Cámara** y **Recientes**.
5. Navegue y seleccione las imágenes que desea adjuntar desde su galería o toque el icono **Cámara** para tomar una foto.

> **Nota:**
>
> Cuando toque el icono **Archivos Adjuntos**, aparecerán las siguientes opciones:
>
> - Archivos
> - ShareFile (ahora Citrix Files)
> - De datos adjuntos de correo

### Secure Mail genera los recursos incrustados cuando se consulta un correo electrónico

Si los recursos están presentes en su red interna (como correos electrónicos con URL de imágenes que son enlaces internos), Secure Mail se conecta a la red interna para obtener el contenido y generarlo.

### Compatibilidad con la autenticación moderna

La autenticación moderna es una autenticación OAuth basada en token con nombre de usuario y contraseña. Esto admite Office 365 para servicios de federación de Active Directory (AD FS) externos e internos, así como proveedor de identidades (IdP).

### Permitir directiva MDX de dominios de Secure Web para Secure Mail

En Secure Mail, algunas URL externas deben abrirse en un explorador nativo en lugar de en Secure Web. Como resultado, de forma predeterminada, todas las URL se abren en un explorador nativo. Sin embargo, puede crear una lista de direcciones URL que quiera abrir específicamente en Secure Web. Para ello, configure una directiva MDX en la consola de Citrix Endpoint Management denominada Dominios permitidos de Secure Web.

Una vez implementada la directiva, se coteja una lista de dominios de host de URL, separados por comas, con la parte de nombre de host de una URL que la aplicación normalmente quiere enviar a un programa externo. Por lo general, esta directiva se configura como una lista de dominios internos de los que debe ocuparse Secure Web.

Si deja vacía la directiva, que es la configuración predeterminada, todo el tráfico web se envía a Secure Web hasta que excluya explícitamente las direcciones URL del filtrado o las redirija. Para redirigir las direcciones URL, configure la directiva Excluir filtro de URL para dominios. Esta directiva indica las direcciones URL que deben abrirse en el explorador nativo. Esta directiva tiene prioridad sobre la directiva de dominios de Secure Web.

Puede configurar estas directivas MDX para Android e iOS.

#### Ejemplo de configuración de la directiva de dominios de Secure Web

Los siguientes procedimientos muestran cómo Secure Mail para Android solicita a los usuarios que abran las URL en el explorador Chrome nativo o en Secure Web. En iOS, los pasos muestran que las URL que normalmente se abrirían en un explorador Safari se abren automáticamente en Secure Web.

#### Para Secure Mail para Android

1. En la lista de directivas de interacción entre aplicaciones, en la lista de excepciones de apertura restringida, escriba *{package = com.android.chrome}*.
2. En la lista de directivas de interacción entre aplicaciones (URL de salida), vaya a **Permitir dominios de Secure Web** y agregue el sufijo DNS del sitio web.

Para otros exploradores de terceros, utilice el siguiente formato, según corresponda:

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

#### Para Secure Mail para iOS

1. En la lista de directivas de interacción entre aplicaciones (URL de salida), en **URL permitidas**, agregue + ^ *safari:*
2. En los **esquemas de URL de aplicaciones**, agregue *safari:*
3. Vaya a **Permitir dominios de Secure Web** y agregue el sufijo DNS del sitio web.

## Integrar Secure Mail con Slack (Tech Preview)

June 18, 2019

Ahora puede llevar su conversación por correo electrónico a la aplicación Slack en dispositivos iOS o Android.

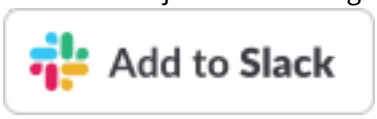
Una vez que habilite esta función, podrá hacer lo siguiente:

- Cambie sin problemas de correos electrónicos a conversaciones de Slack.
- Cree una conversación grupal de Slack con sus destinatarios de correo electrónico.
- Cree un mensaje directo en Slack para su destinatario de correo electrónico.

### Requisitos previos

- Para administradores:

  - Debe haber instalado Secure Mail en su espacio de trabajo de Slack. Haga clic en el siguiente botón **Add to Slack** (Agregar a Slack). 

  - Compruebe que la directiva **Enable Slack** está **activada**. Para obtener detalles sobre la directiva, consulte:
    * Habilitar la directiva de Slack para iOS
    * Habilitar la directiva de Slack para Android
- Para los usuarios: antes de continuar, asegúrese de tener una cuenta de Slack y de que la aplicación de Slack esté instalada en su dispositivo.

### Para habilitar esta función en el dispositivo

1. Abra Secure Mail y toque en el icono de tres líneas.
2. En la pantalla **Buzones**, toque en el icono de parámetros situado en la esquina inferior derecha de la pantalla.
3. En la pantalla **Parámetros**, toque en **Slack**, que aparece listado en **Integraciones**.
4. Proporcione la URL de su espacio de trabajo de Slack y luego toque en **Continuar**.
5. Proporcione sus credenciales y toque en **Iniciar sesión**.
6. Cuando se le solicite que autorice el acceso de Secure Mail a la información, toque en **Autorizar**.

Ahora está conectado a Slack.

### Para usar esta función

1. Abra una conversación de correo electrónico en Secure Mail y toque en el botón de acción flotante.
2. Desde las opciones disponibles, toque en **Chatear en Slack**.
3. La conversación cambiará a Slack con los destinatarios de su correo electrónico.

**Tenga en cuenta lo siguiente:**

- En los dispositivos que ejecutan Secure Mail para iOS o Android, puede crear una conversación de Slack con un máximo de ocho destinatarios de su correo electrónico. Si tiene más de ocho destinatarios de correo electrónico, de forma predeterminada, Secure Mail selecciona los primeros ocho destinatarios presentes en su conversación de correo electrónico.

# Notificaciones y sincronización

July 17, 2020

En este artículo se describe el funcionamiento de las notificaciones y la sincronización de correo electrónico, así como los parámetros que ofrece Secure Mail para ello.

## Actualización en segundo plano de Secure Mail para iOS

Cuando Secure Mail para iOS está configurado para proporcionar notificaciones a través de la función Actualización en segundo plano de iOS (y no mediante APNs), la actualización del correo en Secure Mail funciona de este modo:

- Cuando los usuarios habilitan la función **Actualización en segundo plano** en el dispositivo desde el menú **Ajustes** y Secure Mail se está ejecutando en segundo plano, el correo se sincroniza con el servidor. La frecuencia de sincronización depende de una serie de factores.
- Si el usuario inhabilita la función **Actualización en segundo plano**, la aplicación nunca recibe el correo electrónico mientras se ejecute en segundo plano.
- Cuando los usuarios mueven Secure Mail al segundo plano, la aplicación continúa ejecutándose durante un período de gracia antes de suspenderse.
- Mientras se ejecuta en el primer plano, Secure Mail muestra actividad de correo en tiempo real, independientemente de cómo esté configurado el parámetro **Actualización en segundo plano**.

## Secure Mail y ActiveSync

Secure Mail se sincroniza con Exchange Server a través del protocolo de mensajería de ActiveSync. Esta función permite a los usuarios acceder en tiempo real a su información de Outlook: correo, contactos, eventos de calendario, buzones de correo generados automáticamente y carpetas creadas por cada usuario.

> **Nota:**
>
> ActiveSync no admite la sincronización de carpetas públicas de Exchange. En Exchange Server 2013, ActiveSync tampoco sincroniza la carpeta Borradores.

Para sincronizar las carpetas creadas por el usuario, siga estos pasos:

### iOS

1. Vaya a **Ajustes > Actualización automática**.
2. **Active** la **Actualización automática**.
3. Toque en **Sí**. Aparecerá una lista con todos los buzones de correo.

4. Toque en las carpetas que quiera sincronizar.

**Android**

1. Vaya a la lista de buzones de correo.
2. Toque en el buzón que quiera sincronizar.
3. Toque en el icono Más en la esquina inferior derecha.
4. Toque en **Opciones de sincronización**.
5. En **Frecuencia de comprobación**, seleccione la frecuencia con la que se sincronizará la carpeta.

## Exportar contactos en Secure Mail

Los usuarios de Secure Mail pueden sincronizar continuamente sus contactos con la libreta de direcciones del teléfono, exportar en una vez un contacto concreto a la libreta de direcciones, o bien compartir un contacto como archivo adjunto de vCard.

Para permitir esas funciones, **active** la directiva "Exportar contactos" para Secure Mail en la consola de Endpoint Management.

Cuando la directiva está **activada**, se habilitan las siguientes opciones en Secure Mail:

- **Sincronizar contactos locales** en Parámetros
- Exportar contactos individuales
- Compartir contactos como datos adjuntos de vCard

Cuando la directiva "Exportar contactos" está **desactivada**, esas opciones no aparecen en la aplicación.

Una vez habilitada la directiva, para sincronizar contactos ininterrumpidamente desde el servidor de correo a la libreta de direcciones del teléfono, los usuarios deben establecer **Sincronizar contactos locales** en **Sí**. Mientras **Sincronizar contactos locales** esté **activada**, cualquier actualización de los contactos en Exchange o Secure Mail conllevará una actualización de los contactos locales.

Debido a limitaciones de Android, si una cuenta de Exchange o Hotmail ya está establecida para sincronizarse con los contactos locales, Secure Mail no podrá sincronizar los contactos.

En iOS, los contactos de Secure Mail pueden exportarse y sincronizarse con los contactos del teléfono. Los contactos se pueden exportar y sincronizar, incluso aunque los usuarios tengan Hotmail o Exchange configurados en el dispositivo. Configure esta función en Endpoint Management a través de la directiva "Omitir comprobación de contactos nativos" de Secure Mail. Esta directiva determina si Secure Mail anula la comprobación de contactos desde una cuenta de Exchange o Hotmail configurada en la aplicación nativa de contactos. Si está **activada**, la aplicación sincroniza los contactos con el dispositivo, incluso aunque la aplicación nativa de contactos esté configurada con una cuenta de Exchange o Hotmail. Si tiene el valor **No**, la aplicación seguirá bloqueando la sincronización de contactos. Este parámetro está **activado** de forma predeterminada.

### Notificaciones de Secure Mail

En la siguiente tabla, se indica cómo se gestionan las notificaciones en los dispositivos móviles compatibles cuando Secure Mail se ejecuta en primer plano o en segundo plano.

| Con Secure Mail ejecutándose en primer o segundo plano: | Se tratan las notificaciones para iOS | Se tratan las notificaciones para Android |
|---|---|---|
| Primer plano | Secure Mail mantiene una conexión persistente con ActiveSync para sincronizar la actividad del correo electrónico y del calendario. | Secure Mail mantiene una conexión persistente con ActiveSync para sincronizar la actividad del correo electrónico y del calendario. |
| Segundo plano (o cerrado) | Secure Mail recibe notificaciones mediante la funcionalidad “Actualización de aplicaciones en segundo plano” de iOS o, si está configurado, a través de APNs. | Secure Mail mantiene una conexión persistente con ActiveSync. |

Para obtener detalles sobre la configuración, consulte Notificaciones push en Secure Mail para iOS.

## Notificaciones push para Secure Mail

July 6, 2020

Secure Mail para iOS y Secure Mail para Android pueden recibir notificaciones sobre actividades del calendario y del correo electrónico cuando la aplicación se ejecuta en segundo plano o está cerrada. Secure Mail para iOS admite notificaciones recibidas mediante la función de notificaciones push remotas, suministrada por el servicio APNs (Apple Push Notification service). Secure Mail para Android admite notificaciones recibidas a través del servicio Firebase Cloud Messaging (FCM).

### Cómo funcionan las notificaciones push

Para proporcionar notificaciones push en dispositivos iOS y Android, Citrix aloja un servicio de escucha en Amazon Web Services (AWS) para:

- Escucha de notificaciones push de los servicios web de Exchange (EWS) enviados por los servidores Exchange cuando hay actividad de la Bandeja de entrada. Exchange no envía ningún

contenido de correo al servicio de Citrix.

No hay información de identificación personal almacenada en el servicio de Citrix. En su lugar, hay un token de dispositivo y un ID de suscripción para identificar al dispositivo y la carpeta de la Bandeja de entrada específicos que se actualizan dentro de Secure Mail.

- Enviar notificaciones APNs, que solo contienen indicadores numéricos, a Secure Mail en dispositivos iOS.
- Enviar notificaciones FCM a Secure Mail en dispositivos Android.

El servicio de escucha de Citrix no afecta al tráfico de datos de correo, que continúa fluyendo entre los dispositivos de usuario y los servidores Exchange Server a través de ActiveSync. El servicio de escucha, que está configurado para alta disponibilidad y recuperación ante desastres, está disponible en tres regiones:

- América
- Europa, Medio Oriente y África (EMEA)
- Asia-Pacífico (APAC)

### Requisitos del sistema para notificaciones push

Si la configuración de Citrix Gateway incluye Secure Ticket Authority (STA) y el túnel dividido está desactivado, Citrix Gateway debe permitir el tráfico (cuando se tuneliza desde Secure Mail) hacia las siguientes direcciones URL del servicio de escucha de Citrix:

| Región | dirección URL | Dirección IP |
|---|---|---|
| América | `https://us-east-1.pushreg.xm.citrix.com` | 52.7.65.6; 52.7.147.0 |
| Europa-Oriente Medio-África | `https://eu-west-1.pushreg.xm.citrix.com` | 54.154.200.233; 54.154.204.192 |
| Asia-Pacífico | `https://ap-southeast-1.pushreg.xm.citrix.com` | 52.74.236.173; 52.74.25.245 |

### Configurar Secure Mail para notificaciones push

Para configurar APNs o FCM en Secure Mail para la distribución desde el almacén de aplicaciones, en la consola de Endpoint Management, **active** las notificaciones push y seleccione su región. En esta imagen se muestra la configuración para iOS.

En caso de Android, en esta imagen se muestra la misma **configuración de notificaciones push** que

en iOS. Además, si el servicio EWS está alojado en otra región que no sea la del servidor de correo, rellene el campo **Nombre de host EWS**. El valor predeterminado está vacío. Si no define la configuración, Endpoint Management usa el nombre de host del servidor de correo.

Necesita configurar Exchange y Citrix ADC para permitir el flujo de tráfico hacia el servicio de escucha.

### Configurar Exchange Server

Permitir SSL de salida (en el puerto 443) desde el firewall a la URL del servicio de escucha de Citrix para la región donde se encuentra el servidor Exchange Server. Por ejemplo:

| Región | dirección URL | Dirección IP |
|---|---|---|
| América | `https://us-east-1.mailboxlistener.xm.citrix.com` | 52.6.252.176; 52.4.180.132 |
| Europa-Oriente Medio-África | `https://eu-west-1.mailboxlistener.xm.citrix.com` | 54.77.174.172; 52.17.147.220 |
| Asia-Pacífico | `https://ap-southeast-1.mailboxlistener.xm.citrix.com` | 52.74.231.240; 54.169.87.20 |

Si tiene un servidor proxy entre el dispositivo de escucha de Citrix y Exchange Web Services (EWS), puede seguir uno de estos procedimientos.

- Enviar tráfico EWS a través del proxy y, a continuación, al dispositivo de escucha.
- Omitir el proxy y enrutar el tráfico EWS al dispositivo de escucha directamente.

Para enviar el tráfico de EWS a través del servidor proxy, configure el archivo web.config de EWS en la carpeta ClientAccess\exchweb\ews, como sigue:

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

Para obtener información detallada sobre la configuración de proxies, consulte Configuración de proxy.

Para entornos de Exchange 2013, debe agregar manualmente la sección `system.net` al archivo web.config. Por lo demás, las configuraciones que se describen aquí deben funcionar para Exchange 2013. Para solucionar problemas, póngase en contacto con el administrador de Exchange.

Para omitir el servidor proxy, configure la lista de omisión para permitir que Exchange haga conexiones con el servicio de escucha de Citrix.

Cuando Secure Hub se inscribe con la autenticación por certificados, también debe configurar el servidor Exchange Server para la autenticación por certificados. Para obtener información detallada, consulte el artículo Conceptos avanzados de Endpoint Management.

### Configurar Citrix Gateway

Aunque el servidor Exchange necesite permitir el tráfico hacia el servicio de escucha, Citrix ADC debe permitir el tráfico al servicio de registro. De este modo, los dispositivos pueden conectarse y registrarse para las notificaciones push.

Si sus servidores de EWS y ActiveSync son diferentes, configure la directiva de tráfico de Citrix ADC para permitir el tráfico de EWS. Para obtener más información sobre la integración de Citrix Endpoint Management en Citrix Gateway, consulte la sección Integración con Citrix Gateway y Citrix ADC.

### Solucionar problemas

Para solucionar problemas de conexiones salientes, compruebe los registros de eventos de Exchange, que incluyen entradas de registros cuando una solicitud de suscripción o la notificación de una suscripción no son válidas o fallan. También puede ejecutar seguimientos de Wireshark en el servidor Exchange Server para controlar el tráfico de salida para el servicio de escucha de Citrix.
Para ver otros problemas, utilice Secure Mail Test Tool.

### Preguntas frecuentes sobre las notificaciones push de Secure Mail

#### Cuándo entrega Android las notificaciones a Secure Mail

En Android, las notificaciones siempre se entregan a Secure Mail.

#### Cómo afecta FCM a las notificaciones de correo electrónico que aparecen en la pantalla de bloqueo

Las notificaciones de correo nuevo que aparecen en la pantalla de bloqueo se generan en función de los datos que Secure Mail sincroniza en el dispositivo. Es importante tener en cuenta que esta

información no proviene del servicio de escucha.

Para mostrar notificaciones de correo nuevo, Secure Mail necesita poder sincronizar datos desde Exchange para tener la información disponible y crear las notificaciones.

Cuando recibe un nuevo correo, aparece la notificación FCM **Tiene mensajes nuevos**. Una vez que la sincronización del correo electrónico se complete en segundo plano, el correo nuevo aparece en Secure Mail.

#### Cómo afecta la función Actualización en segundo plano a Secure Mail y APNs

Si el usuario desactiva la función Actualización en segundo plano, se dan las siguientes situaciones:

- Secure Mail no recibe notificaciones cuando Secure Mail no es la aplicación en segundo plano.
- Secure Mail no actualiza la pantalla de bloqueo con notificaciones de correo nuevo.

La inhabilitación de la función Actualización en segundo plano tiene un efecto importante en el comportamiento de Secure Mail. Como se ha indicado anteriormente, las actualizaciones de las insignias de notificaciones basadas en el servicio APNs siguen sucediendo, pero en este modo no se sincroniza el correo electrónico en el dispositivo.

#### Cómo afecta la función Modo de bajo consumo a Secure Mail y APNs

El comportamiento del sistema con respecto a Secure Mail es el mismo cuando se usa el Modo de bajo consumo que cuando la función Actualización en segundo plano está inhabilitada. En modo de bajo consumo, el dispositivo no reactiva las aplicaciones para una actualización periódica y no entrega notificaciones a aplicaciones en segundo plano. Los efectos secundarios son, por lo tanto, los mismos que los indicados en la sección Actualización en segundo plano, más arriba. Tenga en cuenta que, en el Modo de bajo consumo, las insignias de recuento se siguen actualizando basándose en las notificaciones de APNs.

#### Cómo afecta APNs a las notificaciones de correo electrónico que aparecen en la pantalla de bloqueo

Las notificaciones de correo nuevo que aparecen en la pantalla de bloqueo se generan en función de los datos que Secure Mail sincroniza en el dispositivo. Es importante tener en cuenta que esta información no proviene del servicio de escucha.

Para mostrar notificaciones de correo nuevo, Secure Mail necesita poder sincronizar datos desde Exchange, de forma que Secure Mail tenga la información disponible para crear las notificaciones.

Si las notificaciones de APNs no se entregan a Secure Mail en segundo plano, Secure Mail no detecta las notificaciones y, por tanto, no sincroniza los datos nuevos. Puesto que no hay datos nuevos para

Secure Mail, no se generan notificaciones de correo electrónico nuevo en la pantalla de bloqueo del dispositivo, incluso aunque no se hayan entregado notificaciones APNs.

### Qué otros problemas pueden provocar que falle la sincronización iniciada por FCM en segundo plano

Hay una serie de problemas que pueden hacer que las solicitudes de sincronización de FCM fallen, entre otros:

- Un tíquet no válido de STA.
- Cuando Secure Mail se reactiva tras haber estado suspendido, la aplicación tiene 10 segundos para sincronizar todos los datos desde el servidor.

Si se da alguna de las condiciones anteriores, Secure Mail no puede sincronizar datos. En consecuencia, las notificaciones no aparecen en la pantalla de bloqueo.

### Qué otros problemas pueden provocar que falle la sincronización iniciada por APNs en segundo plano

Hay una serie de problemas que pueden hacer que las solicitudes de sincronización de APNs fallen, entre otros los siguientes:

- Un tíquet no válido de STA.
- Una conexión de red lenta. Cuando Secure Mail se reactiva en segundo plano, la aplicación tiene 30 segundos para sincronizar todos los datos desde el servidor.
- Si la directiva de protección de datos está habilitada y una notificación de APNs reactiva Secure Mail, cuando se bloquea el dispositivo Secure Mail no puede acceder al almacén de datos y la sincronización no tiene lugar. Tenga en cuenta que esto solo ocurre cuando el sistema intenta iniciar Secure Mail “en frío”. Si un usuario ya ha iniciado Secure Mail en algún momento después de desbloquear el dispositivo, la sincronización por APNs se realiza correctamente incluso cuando el dispositivo está bloqueado.

Si se da alguna de las condiciones anteriores, Secure Mail no puede sincronizar los datos y, por lo tanto, no puede mostrar notificaciones en la pantalla de bloqueo.

### De qué otro modo genera Secure Mail notificaciones en la pantalla de bloqueo cuando no se entregan o no se usa APNs

Aunque APNs esté inhabilitado, Secure Mail aún se reactiva por eventos periódicos de Actualización en segundo plano de iOS, siempre que está opción esté habilitada y si el modo de bajo consumo está desactivado.

Durante estos eventos de reactivación, Secure Mail sincroniza los nuevos mensajes de correo electrónico desde Exchange Server. El nuevo correo puede usarse entonces para generar notificaciones de correo electrónico en la pantalla de bloqueo. Por lo tanto, aunque las notificaciones APNs no se entreguen o APNs esté inhabilitado, Secure Mail puede sincronizar los datos en segundo plano.

Es importante tener en cuenta que esto ocurrirá menos en tiempo real cuando se esté mediante APNs y cuando las notificaciones APNs se entreguen a Secure Mail. Cuando iOS enruta las notificaciones APNs a Secure Mail, la aplicación sincroniza inmediatamente los datos desde el servidor, por lo que las notificaciones de la pantalla de bloqueo parecen ser en tiempo real.

En el caso de que se requieran eventos de Actualización en segundo plano, las notificaciones de la pantalla de bloqueo no tienen lugar en tiempo real. En este caso, Secure Mail se reactiva con la frecuencia que determine únicamente iOS. Como tal, puede transcurrir un tiempo entre estas dos situaciones:

- Cuando un correo electrónico llega a la Bandeja de entrada de un usuario en Exchange.
- Cuando Secure Mail sincroniza ese mensaje y genera la notificación en la pantalla de bloqueo.

Tenga en cuenta que Secure Mail recibe estas reactivaciones periódicamente incluso aunque no se esté mediante el servicio APNs. En todos los casos en que la función de Actualización en segundo plano reactiva Secure Mail, Secure Mail intenta sincronizar los datos desde Exchange.

### Cómo difiere Secure Mail de otras aplicaciones que también muestran contenido en la pantalla de bloqueo

Una diferencia importante, que puede provocar confusión, es que Secure Mail no siempre muestra los correos electrónicos nuevos en tiempo real en la pantalla de bloqueo. Este comportamiento difiere de Gmail, Microsoft Outlook y otras aplicaciones. El motivo principal de esta diferencia es la seguridad. Para que el comportamiento sea el mismo que el de las demás aplicaciones, el servicio de escucha de Citrix requiere las credenciales de usuario para autenticarse en Exchange. Las credenciales son necesarias para obtener el contenido de correo electrónico. Las credenciales también son necesarias para pasar este contenido de correo electrónico a través del servicio de escucha de Citrix al servicio APNs de Apple. El enfoque de Citrix para notificaciones APNs no requiere que el servicio de escucha de Citrix adquiera ni almacene la contraseña del usuario. El servicio de escucha no tiene acceso al buzón de correo ni a la contraseña del usuario.

Nota sobre la aplicación de correo nativa de iOS: iOS permite que su propia aplicación de correo electrónico mantenga una conexión persistente con el servidor de correo, lo que garantiza que las notificaciones se entreguen siempre. No se permite esta capacidad a aplicaciones de terceros que no sean la aplicación de correo nativa.

**Comportamiento de la aplicación Gmail:** Google controla, como propietario, tanto la aplicación Gmail como el servidor Gmail. Este comportamiento significa que Google puede leer el contenido de los mensajes e incluir dicho contenido en la carga de la notificación APNs. Cuando iOS recibe esta notificación APNs desde Gmail, iOS hace lo siguiente:

- Establece la insignia de la aplicación con el valor especificado en la carga de la notificación.
- Muestra la notificación en la pantalla de bloqueo mediante el texto del mensaje contenido en la carga de la notificación.

Esta es una diferencia importante: Es iOS, no la aplicación Gmail, el que muestra la notificación en la pantalla de bloqueo, en función de los datos contenidos en la carga de la notificación. De hecho, es posible que iOS nunca reactive la aplicación Gmail, de la misma forma que iOS puede no reactivar Secure Mail cuando llega una notificación. Sin embargo, debido a que la carga contiene un fragmento de mensaje, iOS puede mostrar la notificación de la pantalla de bloqueo sin necesidad de sincronizar los datos de correo en el dispositivo.

En Secure Mail, esta situación es diferente. Secure Mail debe sincronizar primero los datos del mensaje desde Exchange para que la aplicación pueda después mostrar la notificación en la pantalla de bloqueo.

**Comportamiento de la aplicación Outlook para iOS:** Microsoft controla Outlook para iOS. No obstante, la organización a la que pertenece el usuario controla los servidores Exchange desde donde se obtienen los datos. A pesar de esta configuración, Outlook puede mostrar notificaciones en la pantalla de bloqueo en función de los datos que proporciona Microsoft en la notificación APNs. Este comportamiento se debe a que Outlook para iOS utiliza un modelo en el que Microsoft almacena las credenciales de usuario. Microsoft accede directamente al buzón del usuario desde su servicio de nube y determina si existe correo nuevo.

Si hay correo nuevo, el servicio de nube de Microsoft genera una notificación APNs que contiene los datos del nuevo correo. Este modelo funciona de manera similar al modelo de Gmail. En el modelo de Gmail, iOS simplemente toma los datos y genera una notificación en la pantalla de bloqueo basada en esos datos. La aplicación Outlook de iOS no está involucrada en este proceso.

**Nota de seguridad importante sobre Outlook para iOS:** El enfoque de Outlook para iOS tiene ciertas consecuencias para la seguridad. Las organizaciones deben confiar a Microsoft las contraseñas de sus usuarios. Esta confianza permite a Microsoft tener acceso al buzón del usuario, lo que supone un riesgo para la seguridad.

Para ver más preguntas frecuentes específicas de los administradores sobre notificaciones push, consulte este artículo de Citrix Support Knowledge Center. Para ver más preguntas frecuentes relacionadas con los usuarios, consulte este artículo de Citrix Support Knowledge Center.

## Notificaciones push enriquecidas en Secure Mail para iOS

July 17, 2020

Secure Mail para iOS admite las notificaciones push enriquecidas. Con las notificaciones enriquecidas, se reciben notificaciones en la bandeja de entrada de un dispositivo bloqueado, incluso aunque

Secure Mail no se esté ejecutando en segundo plano. Esta función se admite con autenticaciones por contraseña y autenticaciones basadas en el cliente.

> **Nota:**
>
> Debido al cambio en la arquitectura para admitir la función de notificaciones push enriquecidas, la función de notificaciones de correo Solo VIP ya no está disponible.

Para habilitar la función de notificaciones push enriquecidas, debe cumplir los siguientes requisitos previos:

- En la consola de Endpoint Management, **active** las notificaciones push.
- La directiva "Acceso de red" está establecida en **Sin restricciones** o **Túnel a la red interna**. Si la directiva "Acceso de red" está establecida en **Túnel a la red interna**, compruebe que el host de servicios web Exchange (EWS) está configurado en la directiva "Servicios de red en segundo plano". Si EWS y ActiveSync tienen el mismo host, el host de ActiveSync debe estar definido en la directiva "Servicios de red en segundo plano".
- Establezca la directiva Control de notificaciones en pantalla bloqueada en **Permitir** o **Remitente del correo o título del evento**.
- Vaya a **Secure Mail > Parámetros > Notificaciones** y habilite **Notificaciones de correo**.

Esta función no se admite con alguna de estas configuraciones:

- Autenticación moderna en Microsoft Office 365
- Aplicaciones que administra la integración de Endpoint Management en Microsoft Intune/EMS
- Dispositivos inscritos mediante credenciales derivadas

### Cómo funcionan las notificaciones push en Secure Mail para iOS

Secure Mail recibe notificaciones push para las siguientes actividades de la bandeja de entrada:

- **Correo nuevo, convocatorias de reunión, cancelaciones o actualizaciones de reuniones**: Cuando APNs envía notificaciones remotas a Secure Mail para iOS y Secure Mail actualiza todas las carpetas marcadas para la actualización automática.

  > **Nota:**
  >
  > De forma predeterminada, las carpetas Bandeja de entrada, Calendario y Contactos están marcadas para la actualización automática. Los usuarios pueden seleccionar cualquier otra carpeta de correo para la actualización automática en **Secure Mail** > **Parámetros** > **Actualización automática**.

- El icono de Secure Mail muestra la cantidad total de mensajes nuevos y no leídos solamente en la carpeta Bandeja de entrada de Exchange. Secure Mail actualiza el icono una vez que el usuario lee los mensajes en un escritorio o un equipo portátil.

- Durante una instalación o actualización, Secure Mail para iOS solicita a los usuarios que permitan las notificaciones push. Los usuarios también pueden permitir notificaciones push más adelante desde los ajustes del sistema de iOS.

### Comportamiento de notificaciones push cuando no se admiten notificaciones push enriquecidas

Para configuraciones que no admiten la función de notificaciones push enriquecidas para iOS, Secure Mail ofrece el recuento de correos electrónicos no leídos de la Bandeja de entrada durante el período de sincronización. Si la directiva **Control de notificaciones en pantalla bloqueada** está **activada**, aparecen notificaciones push en una pantalla de dispositivo bloqueada después de que iOS reactive Secure Mail para realizar una sincronización.

### Preguntas frecuentes sobre las notificaciones push de Secure Mail para iOS

Cuándo entrega iOS las notificaciones a Secure Mail

Cuando se habilita la función de notificaciones push enriquecidas, iOS entrega notificaciones remotas a Secure Mail. Estas notificaciones se producen incluso aunque la aplicación no se esté ejecutando en segundo plano o aunque esté en modo de bajo consumo.

> **Nota:**
>
> Cuando la función de notificaciones push enriquecidas no está habilitada, es posible que las notificaciones no se entreguen a Secure Mail cuando Secure Mail no está activo. Esta situación se produce por muchos motivos, entre otros:

- Si el dispositivo está en modo de bajo consumo y Secure Mail está en segundo plano. Este es el caso más frecuente en el que no se entregan notificaciones.
- Si la función **Actualización en segundo plano** está **desactivada** para Secure Mail y Secure Mail se encuentra en segundo plano. Tenga en cuenta que son los usuarios los que controlan este parámetro.
- Si el dispositivo tiene una conectividad de red deficiente. Esta situación depende del dispositivo iOS.

### Razones para que aparezca la notificación “Tiene mensajes nuevos” en dispositivos iOS

La notificación “Tiene mensajes nuevos” aparece en los dispositivos iOS cuando Secure Mail no recibe ninguna respuesta de los servicios web Exchange (EWS) durante el tiempo especificado. El tiempo necesario para obtener los datos del mensaje es de 30 segundos.

Este comportamiento también puede darse en el dispositivo cuando hay mala conectividad Wi-Fi o de datos.

Además de este motivo de respuesta con retraso por parte de EWS, Secure Mail muestra la notificación "Tiene mensajes nuevos" en las siguientes situaciones:

- Cuando Secure Mail no puede leer la información requerida proveniente del contenedor seguro. Este caso suele ocurrir después de reiniciar el dispositivo y antes de desbloquearlo.
- Cuando Secure Mail no puede conectarse o configurar un canal seguro con Citrix Gateway o EWS.
- Cuando las credenciales han caducado o se han modificado, pero no se han actualizado en Secure Mail. En la siguiente imagen se muestra cómo aparece la notificación en este caso.
- Cuando Secure Mail recibe una respuesta inesperada de Exchange Server para una solicitud válida de Secure Mail. Para obtener más información sobre los códigos de respuesta de EWS, consulte la documentación de desarrollo de Microsoft.

### Mensajes de error de notificación push en Secure Mail para iOS

En Secure Mail para iOS, los mensajes de error de notificación push aparecen en el centro de notificaciones correspondiente del dispositivo. Estas notificaciones aparecen en función del tipo de error de la notificación.

Aparecen los siguientes mensajes de notificación en función de los diferentes casos de error:

- **Secure Mail no puede conectarse a la red de su organización**. Esta notificación aparece cuando Secure Mail no puede establecer conexiones SOCKS5 con Citrix Gateway.
- **Secure Mail no puede conectarse a la red de su organización. Contacte con su administrador.** Esta notificación aparece cuando no se puede acceder a Citrix Gateway. Compruebe que Citrix ADC está configurado correctamente y es accesible desde redes externas.
- **Secure Mail no puede conectarse de forma segura a la red de su organización. Contacte con su administrador.** Esta notificación aparece cuando Secure Mail no puede establecer conexiones SSL con Citrix Gateway. Compruebe que el certificado SSL es válido.
- **Secure Mail no puede conectarse de forma segura a su servidor de correo. Contacte con su administrador.** Esta notificación aparece cuando Secure Mail no puede establecer conexiones SSL con Exchange Server. Compruebe que es válido el certificado SSL presente en su Exchange Server. Si quiere que la aplicación se conecte a Exchange Server a pesar de que este servidor no tenga un certificado válido, debe habilitar la directiva MDX "Aceptar todos los certificados SSL".
- **Secure Mail no puede obtener el mensaje debido a un error del servidor de correo. Contacte con su administrador.** Esta notificación aparece cuando Secure Mail no puede analizar la respuesta de EWS proveniente de Exchange Server.

- **Secure Mail no puede obtener el mensaje porque se excedió el tiempo de espera de la solicitud.** Esta notificación aparece cuando Secure Mail no recibe respuesta del servidor en un plazo de 30 segundos. Esta notificación podría aparecer debido a una mala conexión inalámbrica o de datos en el dispositivo. Inténtelo de nuevo después de esperar un momento.
- **No se puede obtener el mensaje. Abra Secure Mail**. Esta notificación aparece cuando Secure Mail no puede leer las credenciales desde el contenedor seguro. Esta notificación puede aparecer cuando el dispositivo se ha reiniciado pero aún no se ha desbloqueado. Desbloquee el dispositivo para permitir automáticamente el acceso de Secure Mail al contenedor seguro. Si sigue recibiendo esta notificación, abra Secure Mail para actualizar automáticamente las credenciales en el contenedor seguro.

## Interactividad de Secure Mail con otras aplicaciones móviles de productividad y Citrix Files

August 21, 2020

Gracias a la interactividad de Secure Mail con otras aplicaciones móviles de productividad y con Citrix Files, los usuarios pueden acceder, modificar, compartir y guardar documentos sin tener que salir en ningún momento del entorno seguro definido por las directivas de la empresa. Por ejemplo, al tocar en un enlace de Secure Mail, el sitio se abre en Secure Web. Los usuarios pueden abrir y modificar datos adjuntos con Citrix QuickEdit para Endpoint Management. Los datos adjuntos se descargan en el espacio que tenga asignado el usuario en Citrix Files para Endpoint Management.

Para obtener una lista completa de las funciones de Secure Mail para cada plataforma, consulte Funciones desglosadas por plataforma.

## Probar Secure Mail y solucionar problemas de Secure Mail

July 17, 2020

Cuando Secure Mail no funciona correctamente, normalmente se debe a problemas de conexión. En este artículo se describe cómo evitar problemas de conexión. Si se producen problemas, en este artículo se describe cómo solucionarlos.

## Probar las conexiones de ActiveSync, la autenticación de usuarios y la configuración de APNs

Puede usar Endpoint Management Analyzer para realizar comprobaciones del servicio de detección automática de Secure Mail. Esta herramienta es una guía para la descarga de la aplicación de pruebas Endpoint Management Exchange ActiveSync Test. La prueba de correo (la opción "Mail test") verifica los parámetros básicos de conexión con el servidor de correo. Esta herramienta también detecta problemas en los servidores ActiveSync si no están preparados para implementarse en un entorno de Endpoint Management. Para obtener información detallada, consulte Herramienta Endpoint Management Analyzer.

La opción "Mail test" en el Analyzer verifica lo siguiente:

- Las conexiones de los dispositivos iOS y Android con servidores Microsoft Exchange Server o IBM Traveler Server.
- Autenticación de usuario.
- La configuración de las notificaciones push para iOS, incluidos Exchange Server, Servicios web de Exchange (EWS), Citrix Gateway, certificados APNs y Secure Mail. Para obtener información sobre cómo configurar notificaciones push, consulte Notificaciones push en Secure Mail para iOS.

La herramienta proporciona una lista completa de recomendaciones para corregir los problemas.

> Nota:
>
> La aplicación Mail test, MailTest.ipa, ha quedado obsoleta. En su lugar, puede acceder a la misma funcionalidad en Endpoint Management Analyzer.

### Requisitos previos para las pruebas

- Compruebe que la directiva "Acceso de red" no esté bloqueada.
- **Desactive** la directiva "Bloquear redacción de correo electrónico".

## Usar registros de Secure Mail para solucionar problemas de conexión

Para obtener los registros de Secure Mail, haga lo siguiente:

1. Vaya a **Secure Hub > Ayuda > Notificar problema**.
2. Seleccione **Secure Mail** de la lista de aplicaciones.

   Se abrirá un mensaje de correo electrónico dirigido al servicio de asistencia.
3. Introduzca el asunto y describa brevemente el problema en el cuerpo del mensaje.
4. Seleccione el momento en que ocurrió.

5. Cambie la configuración de registros solo si el equipo de asistencia se lo indica.
6. Haga clic en **Send**.

   Se abrirá el mensaje escrito con registros comprimidos como archivos adjuntos.
7. Vuelva a hacer clic en **Enviar**.

   Los archivos ZIP enviados incluyen los siguientes registros:

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

Los registros de información de la aplicación incluyen información acerca del dispositivo y la aplicación. Verifique que el modelo de hardware y la versión de la plataforma utilizados sean compatibles. Verifique que las versiones de Secure Mail y MDX Toolkit utilizados son las más recientes y son compatibles. Para obtener información detallada, consulte Requisitos del sistema para Secure Mail y Compatibilidad de Endpoint Management.

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

Los registros de configuración de VPN solo se facilitan para Secure Hub. Compruebe la versión de Citrix ADC `ServerBuildVersion` para asegurarse de que se está utilizando la versión más reciente de Citrix ADC. Compruebe los parámetros `SplitDNS` y `SplitTunnel` de la siguiente manera:

- Si "DNS dividida" está establecida en **Remoto**, **Local** o **Ambos**, verifique que el FQDN del servidor de correo se esté resolviendo correctamente a través de DNS. (DNS dividida está disponible para Secure Hub en Android.)
- Si "Túnel dividido" está **activado**, compruebe que el servidor de correo está en la lista de aplicaciones de Internet accesibles en el back-end.
- CtxLog_AppPolicies.xml (iOS), Policy.xml (Android y Windows Phone)

Los registros de directivas proporcionan los valores de todas las directivas MDX que se estaban aplicando en Secure Mail en el momento de obtener los registros. Para ver los problemas de conexión, verifique los valores de las directivas `<BackgroundServices>` y `<BackgroundServicesGateway>`.

- Registros de diagnóstico (en la carpeta de diagnósticos)

En configuraciones iniciales de Secure Mail, el problema más común es: "La red de su empresa no está disponible en este momento". Si quiere usar los registros de diagnóstico para solucionar los problemas de conexión, haga lo siguiente.

Las columnas de clave en los registros de diagnóstico son: Timestamp, Message Class y Message. Cuando aparece un mensaje de error en Secure Mail, tome nota de la hora para poder encontrarlo rápidamente en las entradas del archivo de registro en la columna **Timestamp**.

Para determinar si la conexión desde dispositivo hacia Citrix Gateway se realizó correctamente, revise las entradas de AG Tunneler. Los siguientes mensajes indican que la conexión se realizó correctamente:

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

Para determinar si la conexión desde Citrix Gateway hacia Endpoint Management se realizó correctamente (y, por tanto, se puede validar el tíquet de STA), vaya a los registros de diagnóstico de Secure Hub y revise las entradas de INFO (4) en el epígrafe Message Class, correspondientes a la hora en que se inscribió el dispositivo. Los siguientes mensajes indican que Secure Hub obtuvo un tíquet de STA desde Endpoint Management:

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

> Nota:
>
> Durante la inscripción, Secure Hub envía una solicitud a Endpoint Management para pedir un tíquet de STA. Endpoint Management envía el tíquet de STA al dispositivo, donde este tíquet se almacena y se agrega a la lista de tíquets de STA de Endpoint Management.

Para determinar si Endpoint Management emitió un tíquet de STA a un usuario, consulte el archivo UserAuditLogFile.log, incluido en el paquete de asistencia. Para cada tíquet, se muestra la hora de emisión, el nombre de usuario, los dispositivos de usuario y el resultado. Por ejemplo:

**Hora:** 2015-06-30T 12:26:34.771-0700

**Usuario:** 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’ (Tíquet de STA generado correctamente para el usuario “user2” y la aplicación “Secure Mail”.)

Para verificar que se puede establecer la comunicación desde Citrix Gateway hacia el servidor de correo, debe comprobar si la red y DNS están configurados correctamente. Para ello, use Secure Web para acceder a Outlook Web Access (OWA). Al igual que Secure Mail, Secure Web puede usar un micro túnel VPN para establecer conexión con Citrix Gateway. Secure Web actúa como proxy del tráfico hacia el recurso interno o externo al que accede la aplicación. En la mayoría de los casos, especialmente en un entorno de Exchange, OWA está alojado en el servidor de correo.

Para probar la configuración, abra Secure Web y escriba el nombre de dominio completo (FQDN) de la página de OWA. Esa solicitud toma la misma ruta y la misma resolución DNS que la comunicación entre Citrix Gateway y el servidor de correo. Si la página de OWA se abre, significa que Citrix Gateway se está comunicando con el servidor de correo.

Si las comprobaciones anteriores indican que la comunicación es correcta, significa que el problema no está en la configuración de Citrix. El problema es de los servidores Exchange o Traveler.

En este caso, puede recopilar información para los administradores de Exchange o Traveler. En primer lugar, compruebe si hay problemas de HTTP en los servidores Exchange o Traveler. Para ello, busque la palabra "Error" en los registros de diagnóstico de Secure Mail. Si los errores encontrados incluyen códigos HTTP y cuenta con varios servidores Exchange o Traveler, investigue cada servidor. Exchange y Traveler tienen registros HTTP que muestran las solicitudes y respuestas HTTP desde los dispositivos cliente. El registro de Exchange es C:\inetpub\LogFiles\W3SVC1\U_EX.log. El registro de Traveler es IBM_TECHNICAL_SUPPORT>HTTHR.log.

### Para obtener registros de bloqueos desde un dispositivo Secure Mail para iOS

1. En el dispositivo iOS, vaya a **Ajustes** > **Privacidad** > **Análisis** > **Datos de análisis**.
2. En la lista **Datos**, haga clic en el nombre de la aplicación y en la marca de tiempo correspondiente. Aparecerán los registros.

### Solucionar problemas con el correo electrónico, los contactos o el calendario

Puede solucionar problemas de Secure Mail; por ejemplo, correos electrónicos atascados en borradores, contactos que faltan o elementos de calendario que no se sincronizan. Para resolver estos problemas, use los registros de buzón de Exchange ActiveSync. Los registros muestran las solicitudes entrantes enviadas por los dispositivos y las respuestas salientes enviadas desde el servidor de correo.

### Prácticas recomendadas para la sincronización ilimitada

Cuando los usuarios establezcan su período de sincronización de correo en **Todo**, tendrán sincronización ilimitada. Con una sincronización ilimitada, se asume que los usuarios administran el tamaño de su buzón de correo, que es la Bandeja de entrada y todas las subcarpetas sincronizadas. A continuación, dispone de algunos aspectos a tener en cuenta para obtener el mejor rendimiento.

1. Si el tamaño del buzón de correo supera los 18 000 mensajes o 600 MB de tamaño total, la sincronización del correo electrónico puede ralentizarse.
2. No se recomienda habilitar **Cargar adjuntos en Wi-Fi** con la sincronización ilimitada. Esta opción puede provocar que el tamaño del correo electrónico se dispare rápidamente en el dispositivo.
3. Para impedir que los usuarios finales tengan la opción de una sincronización ilimitada, establezca la directiva **Intervalo máximo de sincronización** en un valor que no sea **Todo**.
4. No se recomienda establecer **Todo** en **Intervalo de sincronización predeterminado** para los usuarios.

**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