Secure Mail

Contents

Introducción a Secure Mail

April 12, 2019

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 1
- Exchange Server 2016 Cumulative Update 12
- Exchange Server 2013 Cumulative Update 22
- Exchange Server 2016 Cumulative Update 11
- Exchange Server 2016 Cumulative Update 10
- Exchange Server 2016 Cumulative Update 9
- Exchange Server 2016 Cumulative Update 8
- Exchange Server 2013 Cumulative Update 21
- Exchange Server 2013 Cumulative Update 19
- Exchange Server 2010 SP3 Update Rollup 26
- Exchange Server 2010 SP3 Update Rollup 24
- Exchange Server 2010 SP3 Update Rollup 19
- Exchange Server 2010 SP3 Update Rollup 22
- IBM Domino Mail Server versión 9.0.1 FP10 HF197
- IBM Domino Mail Server 9.0.1 FP9
- IBM Lotus Notes Traveler 9.0.1.21
- IBM Lotus Notes Traveler 9.0.1.9
- 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.

Novedades en Secure Mail

May 17, 2019

Las funciones siguientes son nuevas en Secure Mail:

Secure Mail 19.5.0

Secure Mail para Android

Administrar 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. 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.

Novedades en versiones anteriores

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 en el icono **Contactos** para modificar la lista de correo.

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

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 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

La versión 19.2.0 de Secure Mail 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

- **Mejoras en Contactos.** En Secure Mail para Android, cuando toca en **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:
  - **Adjuntar a correo**
  - **Compartir**
  - **Eliminar**

  En la ficha **Organización**, puede tocar el icono Más situado a la derecha de **ADMINISTRADOR**, **COLABORADORES DIRECTOS**, o **COMPAÑEROS**, para crear 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**, **COLABORADES 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 en **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:

- 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; de lo contrario, aparece 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 iOS, se agrega un nuevo 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

La versión 18.12.0 de Secure Mail 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 18.11.5

Secure Mail para Android

- **Notificar sobre mensajes de phishing con encabezados ActiveSync.** En Secure Mail para Android, cuando un usuario informa sobre 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 correo notificado.

  Para habilitar esta función, un administrador debe configurar la directiva **Direcciones para notificar correo 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 mensaje de phishing (en calidad de archivo adjunto).

- **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 en **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 dependiendo de 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 en **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 Web 18.10.5

- **Integración de Secure Mail en Slack (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 en Slack (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 notificaciones para administrar la forma en que se manejan sus notificaciones de correo electrónico y calendario. Esta característica 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 correo de phishing" y definir el **Mecanismo para notificar phishing** en **Notificar mediante reenvío**. Para obtener información detallada, consulte Notificar mensaje de phishing en calidad de reenvío.

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):**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 correo de phishing" y definir el "Mecanismo para notificar phishing" en **Notificar mediante reenvío**. Para obtener información detallada, consulte Notificar mensaje de phishing en calidad de reenvío.

- **Mejoras en las tarjetas Feed:** 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 en **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 "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 en 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 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**.

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 en el icono de tres líneas y, a continuación, toque en 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 en 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 en el icono para buscar un correo electrónico concreto.
- **Icono de vista de clasificación:** Toque en 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 en el icono para destacar un correo electrónico.
  - **Marcar como no leído:** Toque en el icono para marcar el correo electrónico como no leído.
  - **Eliminar:** Toque en el icono para eliminar el correo electrónico.
  - **Más opciones:** Toque en 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 en el icono para ver los eventos de hoy.
  - **Buscar:** Toque en 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:

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

  En dispositivos iOS:

  - **Editar:** Toque en el icono para modificar los datos del contacto.
  - **Compartir:** Toque en 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 en **Editar** y luego toque en **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 en el icono **Ordenar** y elija los filtros apropiados para ordenar los adjuntos.
- **Buscar:** Toque en 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 usando aplicaciones empresariales Android 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. Se incluye respaldo de 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

- **Respaldo 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 respalda 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).

  > 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.

  Para obtener información detallada, consulte Autenticación moderna con Microsoft Office 365.

Problemas conocidos y problemas resueltos

May 17, 2019

Problemas conocidos en la versión 19.5.0

En dispositivos con iOS, puede conectarse a redes Wi-Fi fuera de las redes Wi-Fi permitidas definidas en la directiva MDX **Redes Wi-Fi permitidas**. Esto le permite abrir Secure Mail y Secure Web para iOS a través de redes que no figuran en la directiva MDX. [CXM-66730]

Problemas resueltos en la versión 19.5.0

- En Secure Mail para Android, no puede pegar direcciones de correo electrónico en los campos **Para:** o **Cc/Bcc:** cuando está escribiendo un correo electrónico. Sin embargo, puede pegar direcciones de correo electrónico en los campos **Para:** o **Cc/Cco:** cuando responda a un correo electrónico. [CXM-64752]
- En Secure Mail para Android, no puede guardar la configuración de la cuenta cuando inscribe dispositivos Android Enterprise. [CXM-65138]

Problemas conocidos y resueltos en Secure Mail para Android versión 19.4.6

No hay problemas conocidos ni resueltos en esta versión.

Problemas resueltos y conocidos en versiones anteriores

Problemas conocidos en la versión 19.4.5

No hay ningún problema conocido en esta versión.

Problemas resueltos en la versión 19.4.5

- En Secure Mail para iOS, cuando envía una invitación de reunión en Outlook y la modifica en Secure Mail, la reunión no se actualiza en Outlook. Los destinatarios tampoco reciben la actualización. Este problema también ocurre cuando crea una invitación de reunión en Secure Mail y la modifica en Secure Mail. [CXM-62511]
- En Secure Mail para iOS, el calendario no se sincroniza y aparece el siguiente error: "No se pudo sincronizar el calendario". [CXM-62796]
- En Secure Mail para Android, algunas invitaciones de reunión que crea con Outlook no se reflejan en el calendario de Secure Mail. [CXM-63552]
- En Secure Mail para Android, las reuniones recurrentes aparecen con retraso y las actualizaciones realizadas en las reuniones no se sincronizan correctamente. [CXM-65263]

Problemas conocidos en la versión 19.3.5

No hay ningún problema conocido en esta versión.

Problemas resueltos en la versión 19.3.5

- En Secure Web para iOS, no puede pegar la URL bitly en el explorador. [CXM-56276]

- En Secure Mail para iOS, aparece este mensaje de error para cada correo recibido: No se puede obtener el mensaje. Abra Secure Mail. [CXM-56418]
- Cuando el usuario abre la aplicación e introduce su PIN en Secure Mail para iOS, a menudo aparece el mensaje de error “Red de la empresa no disponible”. [CXM-59776]
- Secure Mail para iOS no se sincroniza tras cambiar a la autenticación de varios factores. [CXM-62176]

Problemas conocidos en Secure Mail 19.3.0

No hay problemas conocidos en esta versión.

Problemas resueltos en la versión 19.3.0

Secure Mail para iOS

En Secure Mail para iOS, cuando hay un tiempo de espera de solicitud debido a una sesión de red no válida, la siguiente pancarta de notificación aparece intermitentemente cuando recibe un correo electrónico: **Secure Mail no puede obtener el mensaje porque se excedió el tiempo de espera de la solicitud**. [CXM-62561]

Secure Mail para Android

- En Secure Mail para Android, no puede recibir notificaciones de Firebase Cloud Messaging (FCM) de mozaiekwonen.xm.cloud.com. [CXM-62146]
- En Secure Mail para Android, cuando actualiza un evento de calendario, los cambios no se sincronizan con Outlook Office 365. [CXM-62227]
- En Secure Mail para Android, los correos electrónicos que contienen datos adjuntos no se envían cuando hay una conectividad de red deficiente o no hay conectividad. Estos correos electrónicos permanecen en la bandeja de salida incluso después de restaurar la conectividad de red. [CXM-64297]

Problemas conocidos en la versión 19.2.0

En Secure Mail para iOS, cuando el certificado tiene habilitada la opción de transparencia de certificado con el grapado del protocolo OCSP, la configuración de Secure Mail falla en iOS 12.1.1 y versiones posteriores.

Problemas resueltos en la versión 19.2.0

Secure Mail para iOS

En Secure Mail para iOS, no puede copiar el texto del campo “asunto” de Secure Mail a Secure Notes versión 10.8.6.6. [CXM-61060]

Secure Mail para Android

- En Secure Mail para Android, si el texto predictivo está habilitado en dispositivos Samsung, la última palabra del texto aparece subrayada. La última palabra de la firma se guarda con un subrayado cuando no se deja espacio, y el destinatario también puede verla. [CXM-60894]
- Al recibir un resumen de correo electrónico en Secure Mail para Android, las imágenes no se muestran. [CXM-62280]
- Secure Mail para Android se bloquea al iniciarse cuando se instala la versión 5.0.4324.0 del Portal de empresa de Intune. Para obtener más detalles, consulte este artículo de Citrix Support Knowledge Center. [CXM-62516]

Problemas conocidos y resueltos en Secure Mail para iOS versión 19.1.6

No hay problemas conocidos ni resueltos en la versión 19.1.6.

Se han corregido los problemas siguientes en las versiones anteriores:

Problemas conocidos en la versión 19.1.5

No hay problemas conocidos en la versión 19.1.5.

Problemas resueltos en la versión 19.1.5

Se han corregido los siguientes problemas en la versión 19.1.5:

- En Secure Mail para iOS, aparece este mensaje de error para cada correo recibido: **No se puede obtener el mensaje. Abra Secure Mail** [CXM-56418]
- En Secure Mail para iOS, cuando los usuarios abren la aplicación y escriben el PIN, reciben con frecuencia el mensaje de red de empresa no disponible. [CXM-59766]
- En aplicaciones Android empaquetadas, la cadena UserAgent se agrega varias veces, lo que hace que aumente el tamaño del encabezado. Este comportamiento da como resultado un error y la página no se carga. [CXM-59869]

Problemas resueltos en la versión 19.1.0

Secure Mail para iOS

- Cuando Secure Mail no se conecta a Exchange Server, aparece el siguiente mensaje en la pancarta de notificación de correo electrónico:

  "No podemos obtener este mensaje porque su sesión ha caducado. Abra Secure Mail para renovar la sesión".

  Este problema se corrige y el mensaje se actualiza de la siguiente manera:

  "Secure Mail no puede conectarse a la red de su organización. Contacte con su administrador". [CXM-59128]

- Si un usuario que ejecuta buzones de correo O365, realiza repetidamente acciones de respuesta de notificación como **Sí; No; Puede ser; o Eliminar** puede haber una limitación de Office 365 y aparece el siguiente mensaje de error:

  "El servidor está ocupado. Vuelva a intentarlo". [CXM-60123]

Secure Mail para Android

- En Secure Mail para Android, si usa el idioma turco, no puede enviar correos electrónicos a destinatarios cuya dirección contenga el carácter "I". [CXM-59093]
- En Secure Mail para Android, los usuarios no pueden seleccionar y resaltar la línea de asunto de un correo electrónico. [CXM-59185]
- En Secure Mail para Android, el inicio de sesión falla si la contraseña contiene el carácter €. [CXM-59654]
- En Secure Mail para Android, cuando el parámetro **Sincronizar con contactos locales** está habilitado, todos los contactos se exportan a sus contactos nativos. Después de la sincronización, los campos de teléfono como Móvil, Trabajo, Casa, Fax de trabajo y Fax de casa, no aparecen en el orden correcto. Por ejemplo, en los contactos nativos, el número de fax aparece encima del número de móvil. El usuario no puede cambiar este orden. [CXM-57994]

Problemas resueltos en la versión 18.12.0

Secure Mail para iOS

- En Secure Mail para iOS, cuando recibe un correo en formato de texto enriquecido (RTF), ciertos tipos de datos adjuntos integrados con el texto y el símbolo de archivo adjunto no son visibles. [CXM-59121]
- En Secure Mail para iOS, cuando se habilitan las notificaciones push enriquecidas y se desactivan y activan las **Notificaciones de correo**, la opción **Tipo de correo** aparece de forma intermitente. [CXM-59122]

Secure Mail para Android

- Si está ejecutando el mecanismo de autenticación basada en cliente en su entorno, Secure Mail no puede sincronizar automáticamente los mensajes de correo electrónico de forma intermitente. Al realizar una sincronización manual, sólo se obtienen algunos correos electrónicos. [CXM-59650]

Problema resuelto en la versión 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]

Problemas resueltos en la versión 18.11.0

- En Secure Mail para Android, las imágenes incrustadas no se ven en un correo electrónico. [CXM-53556]
- Secure Mail para Android se bloquea al abrir un correo electrónico cuya firma contiene una URL incrustada, como `file://C:\...jpg`. [CXM-58219]

Problemas resueltos en la versión 18.10.5

Secure Mail para iOS

- Cuando se habilita la política MDX Habilitar protección de datos de iOS, se envía la notificación "Tiene un nuevo correo electrónico" de manera intermitente. [CXM-55491]
- En el iPhone XS, los archivos adjuntos no se pueden descargar o enviar y las imágenes descargadas no se pueden visualizar. [CXM-57030]

Secure Mail para Android

- Cuando los usuarios modifican una reunión recurrente para las cuentas que ejecutan Exchange ActiveSync versión 16 y posteriores, la reunión no se actualiza en Exchange Server. Como resultado, la reunión no se sincroniza entre Secure Mail y Outlook. [CXM-57200]

Problemas resueltos en la versión 18.10.0

- En Secure Mail para Android, los usuarios no pueden ver imágenes alineadas que apunten a servidores que no sean Exchange. [CXM-56736] [CXM-55843]
- En Secure Mail para Android, el número de PIN no se añade al número de acceso telefónico al unirse a reuniones de WebEx. Hay que escribir manualmente el número de PIN. [CXM-56002]

- Si el calendario personal del usuario no está configurado, Secure Mail para Android se bloquea al intentar exportar su propio calendario. [CXM-56264]
- En el iPhone XS, en Secure Mail para iOS, los archivos adjuntos no se pueden descargar o enviar y las imágenes descargadas no se pueden visualizar. [CXM-57030]

Problemas resueltos en la versión 18.9.0

Secure Mail para Android

- La estación de trabajo cliente cambia aleatoriamente con cada solicitud de autenticación de NT LAN Manager (NTLM). [CXM-55177]
- En Android P, la sincronización de Secure Mail deja de funcionar intermitentemente cuando el dispositivo está en modo de ahorro de batería. [CXM-55441]
- Si el calendario personal del usuario no está configurado, Secure Mail se bloquea al intentar exportar su propio calendario. [CXM-56264]

Problemas resueltos en la versión 10.8.65

Secure Mail para iOS

- Cuando FIPS está habilitado y los usuarios ejecutan Secure Mail para iOS en un dispositivo iOS 11.3, las directivas MDX para cortar, copiar y pegar elementos no funcionan según lo esperado. [CXM-53993]
- Cuando se utiliza Secure Mail para iOS en dispositivos compartidos, los usuarios nuevos pueden ver los correos electrónicos de un usuario anterior a pesar de que este haya cerrado la sesión. Si los usuarios nuevos tocan en una carpeta para actualizar la pantalla, ya no aparecen los correos electrónicos de los usuarios anteriores. [CXM-55176]

Problemas resueltos en la versión 10.8.60

> Nota:
>
> Las versiones de Secure Mail de 10.8.25 a 10.8.60 no presentan problemas conocidos.

- En Secure Mail para iOS que se ejecuta en servidores IBM Lotus Domino, no se puede usar el icono de búsqueda en la bandeja de entrada. [CXM-53782]
- Cuando los usuarios inscriben un dispositivo que ejecuta Secure Mail para Android en el Portal de empresa de Intune, Secure Mail deja de funcionar. [CXM-54178]
- Secure Mail para iOS se bloquea al sincronizar una gran cantidad de carpetas de correo con el servidor durante un flujo de usuario inicial. [CXM-54371]
- En Secure Mail para iOS, la vista previa de impresión de los archivos PDF aparece más pequeña. [CXM-54482]

- En Secure Mail para Android, varios ID de correos electrónicos no se completan automáticamente al responder a correos electrónicos. [CXM-54811]

Problemas resueltos en la versión 10.8.55

- En Secure Mail para iOS, la vista semanal del calendario se representa incorrectamente en un iPad Pro cuando se ve en el modo horizontal. [CXM-53723]

Problemas relacionados con MDX resueltos en la versión 10.8.55

- En Android, Secure Mail se bloquea cuando los usuarios se desconectan de Secure Hub. [CXM-53930]
- En dispositivos iOS, Secure Web y Secure Mail 10.8.45 se bloquean al iniciarse. [CXM-54089]

Problemas resueltos en la versión 10.8.50

- Secure Mail para iOS no puede guardar archivos de vídeo en ShareFile. [CXM-42238]
- Cuando habilita las notificaciones push en Secure Mail para Android, no recibe notificaciones de nuevos correos electrónicos. Este problema se produce de forma intermitente. [CXM-53135]

Problemas resueltos en la versión 10.8.45

Secure Mail 10.8.45 no contiene problemas resueltos.

Problemas resueltos en la versión 10.8.40

En Secure Mail para iOS, aparece, de forma intermitente, una notificación duplicada por cada correo electrónico nuevo recibida. [CXM-51473]

Problemas resueltos en la versión 10.8.35

- En Secure Mail para Android, la sincronización automática se detiene de forma intermitente. Los usuarios deben sincronizar manualmente la configuración para que algunos mensajes nuevos de servidores de Office 365 aparezcan en Secure Mail. [CXM-49354, CXM-52716]
- En Secure Mail para Android, aunque inhabilite las notificaciones para los eventos de correo electrónico y calendario, esas notificaciones siguen apareciendo y cada notificación genera un sonido. [CXM-50479]

- Cuando crea un evento de Todo el día utilizando Secure Mail para Android, se muestran fechas incorrectas en el calendario de Outlook. [CXM-50612]
- En Secure Mail para Android, los grupos de contactos personales de Exchange no se sincronizan con la aplicación. [CXM-51190]
- Cuando el inicio SSO está configurado, este inicio falla cuando Secure Mail para Android quiere iniciar sesión en Exchange. A los usuarios se les solicita una contraseña para iniciar sesión. [CXM-51343]

Problemas resueltos en la versión 10.8.25

- En Secure Mail para Android, se produce un retraso cuando los usuarios sincronizan una invitación de calendario con Office 365. El problema ocurre cuando se crea o se actualiza una invitación de calendario. [CXM-49596]
- En Secure Mail para Android, cuando los usuarios escriben una sola letra en el campo "CC:" y luego tocan en **Enviar**, Secure Mail envía el mensaje al primer usuario de la lista de destinatarios frecuentes. En vez de ello, debería aparecer una notificación de que los datos que contiene el campo "CC:" no son válidos. [CXM-50476]
- En los dispositivos Zebra T51 con Android 7, los usuarios no pueden instalar la aplicación Citrix Launcher. [CXM-50621]
- Cuando NetScaler Gateway se configura con la autenticación basada en certificados: en Secure Mail para iOS, cada vez que los usuarios reciben un correo nuevo, aparece el mensaje "Tiene mensajes nuevos". Sin embargo, la notificación debería incluir el nombre del remitente, el asunto y la vista previa del cuerpo. [CXM-51075]

Problemas resueltos en la versión 10.8.20

- En Endpoint Management, si la aplicación Portal de empresa de Intune está instalada en dispositivos Android inscritos en el modo solo MAM, Secure Mail intenta redirigir a la página de inicio de sesión de Microsoft. Aparece el mensaje de error: "No se ha recibido la configuración de la aplicación. Contacte con su administrador para configurar la aplicación". [CXM-48135]
- En Secure Mail para Android, el inicio de sesión falla si su nombre de usuario o contraseña contienen caracteres especiales como ä, ö, ü o €. [CXM-48197]
- En dispositivos Android, un reinicio permite omitir la autenticación para acceder a Secure Mail. [CXM-48444]
- En Secure Mail para Android, cuando responde correos electrónicos antes de que se descarguen las imágenes integradas, los correos se quedan atascados en la bandeja de salida. Este problema ocurre cuando el parámetro **Mostrar imágenes** está habilitado en la configuración. [CXM-49222]

- En Secure Mail para iOS, si la directiva IRM está **activada** y la clasificación de correo electrónico está establecida en **Protegida**, no podrá ver los archivos adjuntos cuando descargue el correo completo. [CXM-49544]

Problemas resueltos en la versión 10.8.10

Secure Mail para iOS

- Después de actualizar a Secure Mail 10.7.25 para iOS, faltan los corchetes (<y>) en el encabezado Message-ID. [CXM-46029]
- En Secure Mail para iOS, después de que los usuarios agregan una invitación de calendario desde Outlook, la aplicación falla intermitentemente. Este problema ocurre si la invitación de calendario contiene un emoji. [CXM-46250]
- En iOS, después de actualizar las aplicaciones móviles de productividad a 10.7.30, si "Nivel de registro" está establecido en 11 o más, Secure Mail se vuelve lento y se bloquea si se deja abierto. [CXM-46721]
- En Secure Mail para iOS, aparecen de vez en cuando notificaciones duplicadas si la directiva "Control de notificaciones en pantalla bloqueada" tiene el valor **Solo recuento**. [CXM-47461]

Secure Mail para Android

En Secure Mail para Android, cuando los usuarios copian y pegan cuatro o más direcciones de correo electrónico en el campo Para:, la aplicación se bloquea. [CXM-46578]

Problemas conocidos en la versión 19.1.0

No hay ningún problema conocido en la versión 19.1.0

Implementar Secure Mail

March 11, 2019

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 ver información detallada, consulte Integrar con 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 respalda 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 más información acerca de las limitaciones conocidas con IBM/Lotus Notes, consulte esta entrada de 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 más detalles, 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 más información, consulte [Agregar aplicaciones].(/es-es/citrix-endpoint-management/apps.html)

> 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 la **recopilación completa**.

Configurar Secure Mail

February 11, 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 con 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

February 22, 2019

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 definir cómo se integra Endpoint Management en 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 más información, consulte Para 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

February 11, 2019

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 más detalles, consulte la documentación de Microsoft en URL e intervalos 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.

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.

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 más información sobre las notificaciones push enriquecidas, consulte Notificaciones push en 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/d	n/d

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
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.

> **Nota:**
>
> Configure los servicios de red en segundo plano solo si su servidor de correo y AD FS son internos.

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

April 29, 2019

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 (anteriormente 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 utilizando las credenciales de administrador.
2. En la consola, haga clic en la pestaña **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 al correo seguro es **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, 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

February 11, 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.

- Si quiere configurar los servicios en segundo plano para Secure Mail, consulte Servicios en segundo plano para Secure Mail.
- Si quiere 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 respalda 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 más información acerca de las limitaciones conocidas con IBM/Lotus Notes, consulte esta entrada de 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 más detallada, consulte Fin de vida y aplicaciones obsoletas.

- 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 MDX para configurar 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 usando 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 más información 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 recibe respaldo en el puerto 443. Sin SSL recibe respaldo, 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 ver más información sobre esta revisión, 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 información actualizada 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 respaldados para 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 respaldados para 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
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

March 12, 2019

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 ver información detallada, consulte Integrar con un proveedor de identidades digitales.	X	
Respaldo a credenciales derivadas	Secure Mail admite credenciales derivadas como origen de certificado. Para obtener más información acerca de 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 más información, 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 la tienda 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 de ambos procedimientos se indican 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 acerca de 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 más información, consulte Directiva de 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

April 29, 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 Apple App Store (iOS) o Google Play Store (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 Apple App Store (iOS) o Google Play Store (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

March 11, 2019

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, el respaldo para IRM está **desactivado**. 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 el usuario recibe un correo con contenido protegido, ve 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 usando 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: Planificación [SEC = PROTEGIDO, DLM = Reservado]
- Asunto: Planificación [DLM = Reservado]
- Asunto: Planificación [SEC = NO CLASIFICADO]

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: Planificación [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. El valor predeterminado es **No**.

- **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 añadido 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, éste aplica el nivel de protección de Clase A a todos los archivos del sandbox. Para obtener más información sobre la protección de los datos en Secure Mail, consulte Proteger 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 la tienda de aplicaciones de Endpoint Management.

Protección de datos del Australian Signals Directorate

Secure Mail respalda 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 Android

May 17, 2019

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

Administrar sus feeds

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

Las mejoras a los feeds incluyen las siguientes opciones:

- Agregar hasta tres carpetas de correo electrónico.
- Agregue tarjetas para sus colegas y colaboradores directos, o carpetas como VIP y Marcado.
- Buscar tarjetas o carpetas.
- Reordenar las tarjetas existentes.
- Eliminar una tarjeta existente.

Puede administrar sus tarjetas pulsando el botón **Administrar feeds** en la vista de **Feeds**.

Si lo prefiere, puede pulsar la opción **Administrar feeds** en **CORREO** desde la pantalla Parámetros para administrar sus tarjetas.

Puede añadir, reordenar o eliminar tus tarjetas según sus preferencias.

Para agregar una tarjeta

1. Toque en la ficha **Todas las tarjetas** o **Todas las carpetas**.
2. Toque en el icono **Añadir** (+) en la parte superior derecha de la pantalla para seleccionar las tarjetas que elija.
3. Toque en **Listo**.

Las cartas que ha seleccionado se añaden y aparecen en sus feeds.

Para reordenar sus tarjetas

1. Toque en el botón **Administrar feeds**.
2. En las tarjetas disponibles, mantenga pulsado para seleccionar una tarjeta.
3. Mueva la tarjeta a la ubicación deseada.

Para eliminar una tarjeta

1. Toque en el botón **Administrar feeds**.
2. Toque el icono **-** junto a las tarjetas.
3. Toque en **Listo**.

Las tarjetas se eliminan de tus feeds.

Visualizar datos adjuntos

En Secure Mail para Android, es fácil visualizar archivos adjuntos de correo y calendario. El archivo adjunto se abre directamente dentro de la aplicación o se muestra una lista de aplicaciones compatibles. Puede seleccionar la aplicación necesaria para ver los datos adjuntos.

Secure Mail admite la visualización de los siguientes formatos de archivo de contacto: .txt, word, audio, vídeo, html, archivos. zip, imágenes, archivos. eml y .vcf.

Requisitos previos

Asegúrese de que un administrador configure las siguientes directivas MDX en la consola de Citrix Endpoint Management:

- La directiva “Intercambio de documentos (Abrir en)” debe estar establecida en **Restringida**.
- La directiva “Permitir documentos sin conexión” debe estar establecida en **Sin límite**.

Para obtener información sobre esas directivas, consulte las directivas MDX en Interacción entre aplicaciones.

Acciones para visualizar datos adjuntos

Puede hacer lo siguiente para ver los datos adjuntos:

- Seleccionar un mensaje existente en un buzón para adjuntarle un archivo.
- Crear un mensaje al que adjuntar un archivo
- Guardar los datos adjuntos para acceder a ellos sin conexión.
- Eliminar los datos adjuntos de archivos sin conexión.
- Abrir los datos adjuntos utilizando una aplicación diferente cuando se le solicite.
- Ver el evento de calendario o el mensaje de correo electrónico de origen de los datos adjuntos.

Puede previsualizar los datos adjuntos mientras:

- Visualiza un mensaje.
- Redacta un mensaje nuevo.
- Reenvía un mensaje.

También puede previsualizar los datos adjuntos desde:

- La carpeta de datos **Adjuntos**.
- Los eventos de calendario.

Adjuntar archivos a un correo electrónico existente o a un nuevo correo electrónico

Puede adjuntar archivos a un correo electrónico existente o puede crear un correo electrónico para adjuntar archivos.

1. Toque en la carpeta **Adjuntos** y mantenga pulsada la opción para seleccionar varios adjuntos, o simplemente toque para seleccionar un archivo adjunto.
2. Toque en el icono **Adjuntar** en la pantalla. Aparece el buzón.

3. Puede realizar una de las siguientes acciones:
    - Para adjuntar el archivo a un correo electrónico existente, seleccione un mensaje existente.
    - Para adjuntar el archivo a un nuevo correo electrónico, toque en **Mensaje nuevo**.

Para guardar los datos adjuntos para acceder a ellos sin conexión

1. Abra los datos adjuntos.
2. Toque en el icono **Más** en la parte superior derecha de la página y, a continuación, toque en **Guardar sin conexión**.

Para eliminar los datos adjuntos de archivos sin conexión

1. Abra los datos adjuntos.
2. Toque en el icono **Más** en la parte superior derecha de la página y, a continuación, toque en **Quitar de archivos sin conexión**.

Para abrir el archivo adjunto mediante diferentes aplicaciones

1. Abra los datos adjuntos.
2. Toque en el icono **Más** en la parte superior derecha de la página y luego en **Abrir con**.
3. En las opciones que aparecen, toque la aplicación que quiera usar para abrirlo.
4. También puede deslizar el dedo hacia la izquierda para ver la lista de Acciones que se pueden utilizar para ver o abrir los datos adjuntos.

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

1. Toque en el icono **Adjuntos** situado en la parte inferior derecha de la pantalla.
2. Toque en uno de los datos adjuntos y luego toque en el icono **Más** en la parte superior derecha de la pantalla.
3. Toque en **Ver mensaje original** o en **Ver calendario original** para ver el origen de un correo electrónico o de un evento del calendario.

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 capacidad de impresión presenta las siguientes limitaciones conocidas:
>
> - Las imágenes alineadas solo se imprimen si las ha descargado tocando en **Mostrar imágenes**. Si no toca en **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 en **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 en 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 en **Imprimir**. Aparecerá una vista previa del correo electrónico.

2. Toque en la lista y aparecerán las siguientes opciones:
    - Guardar en PDF
    - Todas las impresoras
3. Toque en **Guardar en PDF** para guardar el correo electrónico en formato PDF.
4. Toque en **Todas las impresoras**. Instale la impresora que más se ajuste a sus necesidades.
5. Una vez instalada la impresora, toque en **Select Printer** 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 en el icono “Imprimir” de la pantalla.

Para imprimir una imagen alineada

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

Notificar sobre mensajes de phishing con encabezados ActiveSync

En Secure Mail para Android, cuando un usuario informa sobre 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 correo notificado.

Para habilitar esta función, un administrador debe configurar la directiva “Direcciones para notificar correo 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 mensaje de phishing (en calidad de archivo adjunto).

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 en **Notificaciones**.
2. En la pantalla **Notificaciones**, toque en **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 característica 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.

Adjuntar archivos 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 Note 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 carpeta 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 pueden ahora adjuntar una imagen desde la aplicación Galería de sus dispositivos.

Formatos de archivo respaldados

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

Formato	iOS	Android
3GP	X	X
Flac		X
AAC	X	X
M4A	X	X
3GP(AMR-NB)	X	X
MP3	X	X
WAV	X	X
OGG		X
ICO	X	X
JPEG	X	X
PNG	X	X
TIF (de página única)	X	
BMP	X	X
GIF	X	X
WebP		X
.dot	X	X
PDF	X	
PPT	X	X
PPTX	X	X
DOC	X	X
DOCX	X	X
XLS	X	X
XLSM	X	X
XLSX	X	X
TXT	X	X
POT	X	X
HTM	X	X
HTML	X	X
ZIP	X	X

Formato	iOS	Android
EML	X	X

Varias cuentas de Exchange para Android

Desde **Parámetros** en Secure Mail, ahora 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.

Requisitos previos

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.
- 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 respalda solo servidores de correo de Exchange y Office 365.

Para agregar una cuenta de correo electrónico de Exchange en Android

1. Abra Secure Mail, toque en el icono de tres líneas y en el icono **Parámetros**.
2. En **Cuentas**, toque en **Agregar cuenta**.
3. En la pantalla **Agregar cuenta**, escriba las credenciales para la nueva cuenta.

   Si lo prefiere, puede establecer los valores de los siguientes parámetros:

   - **Periodo de sincronización de correo:** Toque para seleccionar un valor para el periodo de sincronización de correo. El valor que establezca indicará la cantidad de días de correo que va a sincronizar Secure Mail. El administrador establece el valor predeterminado.
   - **Hacer cuenta predeterminada:** Toque para establecer la nueva cuenta como la cuenta predeterminada. El valor es **No** de forma predeterminada.
4. Toque en **Iniciar sesión** para crear la cuenta.

   La nueva cuenta se muestra en la pantalla **Parámetros** del menú **Cuentas**.

> **Nota:**
>
> Las cuentas adicionales deben usar la autenticación por Active Directory. Secure Mail no respalda la autenticación basada en certificados cuando se configuran varias cuentas.

Para modificar una cuenta

Puede modificar la descripción y la contraseña pertenecientes a la cuenta de correo electrónico en Android.

1. Abra Secure Mail, toque en el icono de tres líneas y en el icono **Parámetros**.
2. En **Cuentas**, toque en la cuenta que quiere modificar.
3. En la pantalla **Cuenta**, modifique los campos.
4. Toque en **Guardar** para confirmar la acción o en **Cancelar** para volver a la pantalla **Parámetros**.

Para eliminar una cuenta en Android

1. Abra Secure Mail, toque en el icono de tres líneas y en el icono **Parámetros**.
2. En **Cuentas**, toque en la cuenta que quiere eliminar.
3. En la pantalla **Detalles de la cuenta**, toque en **Eliminar cuenta** en la parte inferior de la pantalla, o toque en **Cancelar** para volver a la pantalla **Parámetros**.
4. Toque en **ELIMINAR** para confirmar la acción.

> Nota:
>
> Si elimina la cuenta predeterminada, la cuenta siguiente se convertirá en la cuenta predeterminada.

Para definir una cuenta predeterminada en Android

Secure Mail usa la cuenta predeterminada en las siguientes situaciones:

- **Redactar correos:** El campo **De:** se rellena automáticamente con el ID de correo de la cuenta predeterminada.
- **Crear eventos de calendario:** El campo **Organizador** se rellena automáticamente con el ID de correo de la cuenta predeterminada.

Cuando se agregan una o varias cuentas de correo electrónico, la primera cuenta que cree es la cuenta predeterminada. Para cambiar la cuenta predeterminada, vaya a **Parámetros** y toque en **Predeterminado**, en **General**.

En la pantalla **Cuenta predeterminada**, toque en la cuenta que quiere establecer como predeterminada.

Parámetros para varias cuentas de Exchange en Android

Si ha configurado varias cuentas de Exchange, algunos de los parámetros de Secure Mail estarán disponibles para cada una de estas cuentas de forma individual, mientras que los demás parámetros serán globales. Los siguientes parámetros son específicos de la cuenta:

- Predeterminado
- Notificaciones
- Fuera de la oficina
- Frecuencia de sincronización de la bandeja de entrada
- Periodo de sincronización
- Sincronizar correo
- S/MIME
- Archivos sin conexión
- Firma
- Respuestas rápidas
- Sincronizar calendario
- Sincronizar contactos
- Sincronizar contactos locales
- Exportar parámetros

Estos parámetros aparecen con el icono >. Toque en el icono > para ver las cuentas que contiene el dispositivo.

Para aplicar la configuración a una cuenta específica, expanda el parámetro tocando en **>** y, a continuación, seleccione la cuenta de correo electrónico en sí.

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.

Para ver los buzones, abra Secure Mail y toque en el icono de tres líneas. En la pantalla **Buzones**, toque en la cuenta para ver más opciones disponibles.

Aunque la vista **Todas las cuentas** muestra los mensajes de correo electrónico de varias cuentas de forma colectiva, en las siguientes acciones se usa 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

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.

Las siguientes acciones están limitadas a las cuentas individuales:

- Mover elementos.
- Redactar mensajes de correo electrónico desde la vista de conversación.
- Guardar contactos.

Contactos

Toque en el icono **Contactos** desde la barra de la ficha y, a continuación, toque en el icono de tres líneas en la parte superior derecha de la pantalla. La pantalla **Contactos** muestra los siguientes elementos:

- **Todos los contactos:** Muestra todos los contactos de varias cuentas de correo electrónico. Esta opción solo aparece si se configuran varias cuentas de correo electrónico.
- **Cuenta individual de correo electrónico:** Muestra los contactos que pertenecen a la cuenta individual de correo electrónico que esté configurada.
- **Categorías:** Muestra las categorías de contacto que puede haber creado o seleccionado de la lista predefinida para agrupar contactos.

Para ver la carpeta de contactos

> Nota:
>
> No se admiten las subcarpetas de contactos en Secure Mail para Android. Si ha creado carpetas o subcarpetas para sus contactos usando Microsoft Outlook, no podrá verlas en Secure Mail.

1. En la pantalla de contactos:

- Toque en “Todos los contactos” para ver todos los contactos de varias cuentas de correo electrónico.
- Toque en una cuenta individual de correo electrónico para ver los contactos asociados a esa cuenta de correo electrónico en particular.

2. Toque en “Categorías” para ver los contactos agrupados por categorías específicas. Puede optar por agrupar los contactos en función de una categoría que haya creado, o bien, puede agruparlos en una categoría proveniente de una lista predefinida.

Puede sincronizar los contactos de una cuenta individual con los contactos locales.

Para sincronizar contactos locales

1. Abra Secure Mail.
2. Toque en el icono “Parámetros” y vaya a **Contactos > Sincronizar contactos locales**. A continuación, toque en > para expandir el menú.
3. En la pantalla **Sincronizar contactos locales**, habilite la cuenta cuyos contactos quiere sincronizar.
4. Toque en **Aceptar**.
5. Cuando se le solicite si permitir que Secure Mail acceda a sus contactos, toque en **Aceptar**.

Ahora habrá exportado correctamente contactos de la cuenta.
Para deshacer esta acción, vaya a **Parámetros > Contactos > Sincronizar contactos locales** y, a continuación, toque en el conmutador situado junto a la cuenta para inhabilitar esta característica. Toque en **Aceptar** para confirmar la acción.

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 en el icono **Calendario** en la barra al pie de página y luego toque en el icono de tres líneas en la parte superior izquierda.
   La pantalla **Calendarios** muestra todas las cuentas configuradas.

2. Toque en 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 en **Guardar**.
4. Para volver a la pantalla anterior, toque en **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 en 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.

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 características de Secure Mail que son compatibles con Android Enterprise.

Función	Respaldo
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 características de Secure Web que son compatibles con Android Enterprise.

Función	Respaldo
Modo de exploración segura	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.

Integrar Secure Mail en Slack (Preview)

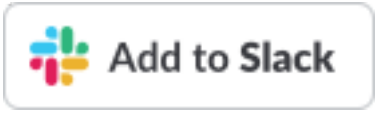
April 12, 2019

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 característica 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 característica

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

January 25, 2019

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, incluso aunque los usuarios tengan configurado Hotmail o Exchange 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 debe anular 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. El valor predeterminado es **Sí**.

Notificaciones de Secure Mail

En la siguiente tabla, se resume 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 información acerca de la configuración, consulte Notificaciones push en Secure Mail para iOS.

Notificaciones push enriquecidas

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”.
- La directiva “Control de notificaciones en pantalla bloqueada” está establecida en **Permitir** o **Remitente del correo o título del evento**.

- Vaya a **Secure Mail > Parámetros > Notificaciones** y habilite **Notificaciones de correo**.

Esta característica no se admite con alguna de estas configuraciones:

- Autenticación moderna en Microsoft Office 365 (Oauth)
- Aplicaciones que administra la integración de Endpoint Management en Microsoft Intune/EMS
- Dispositivos inscritos mediante credenciales derivadas

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 de 30 segundos necesario para obtener los detalles del mensaje.

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 también 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 aún 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.

Notificaciones push para Secure Mail

March 12, 2019

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 respalda notificaciones recibidas mediante la funcionalidad de "Actualización en segundo plano" o notificaciones push suministradas por el servicio APNs (Apple Push Notification service). Secure Mail para Android respalda notificaciones recibidas a través del servicio Firebase Cloud Messaging (FCM).

Cómo funcionan las notificaciones push

Secure Mail envía notificaciones push para las siguientes actividades de la bandeja de entrada:

- **Nuevo mensaje de correo, invitaciones de reunión, cancelaciones de reunión, actualizaciones de reunión:** Cuando APNs envía notificaciones a una bandeja de entrada, Secure Mail actualiza todas las carpetas, incluido el Calendario, para que los cambios de las reuniones se reflejen inmediatamente en los calendarios de los usuarios.
- **En iOS, el estado de Secure Mail cambia de leído a no leído y viceversa.** 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.

  Para iOS, Secure Mail sigue ofreciendo el recuento de los mensajes de correo electrónico no leídos en 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.

  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.

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 la tienda 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 el 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 más información acerca de la configuración de proxys, consulte Configurar un 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 más información, consulte el artículo Conceptos avanzados de Endpoint Management.

Configuración de Citrix Gateway

Mientras el servidor Exchange debe permitir el tráfico dirigido hacia el servicio de escucha, Citrix ADC debe permitir el tráfico dirigido 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.

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.

Si surgen otros problemas, intente solucionarlos con la herramienta de prueba Secure Mail Test Tool.

Preguntas frecuentes sobre las notificaciones push de Secure Mail

Cuándo entrega iOS las notificaciones a Secure Mail

Si Secure Mail se ejecuta en primer plano, las notificaciones se entregan *siempre* a Secure Mail. Esta es la única vez que Citrix puede garantizar que las notificaciones se entregarán. Cuando Secure Mail se coloca en segundo plano, la etiqueta de recuento de la aplicación siempre las actualiza. Sin embargo, las notificaciones (en la pantalla de bloqueo y en pancarta) dependen de la funcionalidad de Actualización en segundo plano. En concreto, cuando iOS suspende o termina la aplicación, no hay total seguridad de que se envíen notificaciones. Los siguientes factores quedan fuera del control de Citrix.

Las situaciones siguientes pueden afectar a la entrega de notificaciones:

- Cuando queda poca batería.
- Cuando Secure Mail no se utiliza con frecuencia (rara vez se pone en primer plano).
- Cuando se reciben correos electrónicos fuera de las horas de uso principales y la aplicación se suspende durante un tiempo en segundo plano: por ejemplo, entre medianoche y las 6 de la mañana.

Las notificaciones *no se entregan* a Secure Mail en los casos siguientes:

- Si el usuario cierra Secure Mail, hasta que el usuario vuelve a abrir la aplicación manualmente.
- Si el sistema ha finalizado Secure Mail y la aplicación no se ha reiniciado automáticamente.
- Cuando Secure Mail no está activo.

> **Importante:**
>
> Las notificaciones no pueden entregarse a Secure Mail cuando éste no está activo por varios motivos, incluidos los siguientes:
>
> - Si el dispositivo está en modo de bajo consumo y Secure Mail está en segundo plano. Este es la situación más frecuente en 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. Este parámetro lo controlan los propios usuarios.
> - Si el dispositivo tiene problemas de conectividad de red. Esta situación depende totalmente del dispositivo iOS.

Cuando Secure Mail no recibe una notificación, Secure Mail no sincroniza los nuevos datos en el dispositivo. Como consecuencia de ello, pueden darse las siguientes situaciones:

- Secure Mail solo sincroniza datos cuando los usuarios traen la aplicación al primer plano.
- Dejan de recibirse notificaciones de correo nuevo en la pantalla de bloqueo. No obstante, los avisos de calendario siguen apareciendo.

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, no aparecen las notificaciones de 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 usando APNs y cuando las notificaciones APNs se entreguen a Secure Mail. Cuando iOS enruta las notificaciones APNs a Secure Mail, la aplicación inmediatamente sincroniza los datos desde el servidor y 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 consecuencia de esto, puede transcurrir cierto tiempo desde el momento en que un correo electrónico llega a la bandeja de entrada de Exchange y el momento en que 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 usando 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 muy importante, y que puede causar confusión, es que Secure Mail no siempre muestra el correo nuevo en tiempo real en la pantalla de bloqueo del mismo modo que lo hacen otras aplicaciones como Gmail o Microsoft Outlook. El motivo principal de esta diferencia es la seguridad. Para alinearse con el comportamiento de las otras aplicaciones, el servicio de escucha de Citrix necesitaría las credenciales del usuario para autenticarse con Exchange y obtener el contenido del correo electrónico, y pasar este contenido de correo electrónico a través del servicio de escucha de Citrix, además del 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. Esto 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 usando 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, porque Outlook para iOS utiliza un modelo en el cual Microsoft almacena las credenciales del 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 forma similar al modelo de Gmail, donde 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 necesitan confiar las contraseñas de los usuarios a Microsoft, de modo que Microsoft pueda acceder a los buzones de correo, lo que supone un riesgo para la seguridad. Para obtener más información sobre cómo administra Microsoft las contraseñas de los usuarios, consulte este artículo de Microsoft TechNet.

Para ver las preguntas frecuentes específicas de administradores sobre notificaciones push, consulte este artículo del Support Knowledge Center. Para ver más preguntas frecuentes relacionadas con los usuarios, consulte este artículo del Support Knowledge Center.

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

February 11, 2019

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 editar 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 funcionalidades de Secure Mail en cada plataforma, consulte Funciones desglosadas por plataforma.

Probar Secure Mail y solucionar problemas de Secure Mail

March 12, 2019

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 más información, 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 más información sobre la configuración de las 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 **Enviar**.

   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 reciben respaldo. Verifique que las versiones de Secure Mail y MDX Toolkit utilizados son las más recientes y son compatibles. Para obtener más información, 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.

Para obtener más detalles, consulte la entrada del blog TechNet Under The Hood: Exchange ActiveSync Mailbox Log Analysis

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