Empresas

Comunicación y conectividad | Cloud | IoT | Seguridad

Administración de contenido móvil.

VMware Workspace ONE UEM sevices

vmware

Puede encontrar la documentación técnica más actualizada en el sitio web de VMware:

https://docs.vmware.com/es/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Spain, S.L.
Calle Rafael Boti 26
2.ª planta
Madrid 28023
Tel.: +34 914125000
www.vmware.com/es

Contenido

Introducción a la administración de correo electrónico móvil

1

Utilice Workspace ONE UEM powered by AirWatch para administrar la implementación de correo electrónico móvil.

Poder ver datos corporativos en su dispositivo ofrece comodidad y mejora la productividad, pero también presenta problemas de seguridad e implementación. Para hacer frente a estos problemas, la solución Workspace ONE UEM powered by AirWatch Mobile Email Management (MEM) le proporciona seguridad completa para la infraestructura de correo electrónico corporativo.

Desafíos

El correo electrónico móvil ofrece ventajas y, al mismo tiempo, presenta desafíos más importantes, como los siguientes:

- Aprovisionar el correo electrónico en distintos tipos de dispositivos, sistemas operativos y clientes de correo electrónico.
- Proteger el acceso al correo electrónico en redes que no son seguras.
- Proteger la información confidencial frente a aplicaciones de terceros.
- Impedir el acceso al correo electrónico a dispositivos no autorizados, extraviados o robados.
- Evitar la pérdida o circulación de archivos adjuntos de correo electrónico mediante aplicaciones de lectores de terceros cuando estos archivos son vistos.

Ventajas de la administración de correo electrónico móvil (MEM)

Workspace ONE UEM powered by AirWatch MEM ofrece todos los elementos clave necesarios para realizar una implementación de correo electrónico móvil segura y fluida. Las siguientes son algunas de las ventajas del uso de MEM:

- Establecimiento de seguridad SSL
- Configuración inalámbrica del correo electrónico
- Detección de dispositivos sin administrar
- Protección del correo electrónico contra la pérdida de datos

- Bloqueo de acceso al correo electrónico en dispositivos no administrados
- Permiso de acceso al correo electrónico solo para los dispositivos aprobados por la empresa
- Integración y revocación de certificados.

Requisitos de MEM

Verifique los requisitos del explorador que encontrará en esta sección antes de continuar con la solución® de administración de correo electrónico móvil® (MEM) de VMware AirWatch.

Descargo de responsabilidad

No se garantiza la integración con productos de terceros. La implementación depende del funcionamiento correcto de dichas soluciones de terceros.

Navegadores compatibles

La consola de Workspace ONE UEM es compatible con las últimas compilaciones estables de los siguientes navegadores web:

- Chrome
- Firefox
- Safari
- Internet Explorer 11
- Microsoft Edge

Nota Si utiliza IE para acceder a la consola UEM, navegue a **Panel de control > Ajustes > Opciones de Internet > Seguridad** y asegúrese de que su nivel de seguridad o el nivel de seguridad personalizado tenga **Habilitada** la opción de **Descarga de fuentes**.

Si utiliza un navegador más antiguo que los mencionados, actualice el navegador para garantizar el rendimiento de la consola de Workspace ONE UEM. Se han realizado pruebas integrales de las plataformas para garantizar la funcionalidad de estos navegadores web. Si decide utilizar un navegador no certificado, es posible que tenga algunos problemas menores con la consola de UEM.

Modelos de implementación para la administración de la infraestructura de correo electrónico

2

Workspace ONE UEM ofrece dos tipos de modelos de implementación para proteger y administrar su infraestructura de correo electrónico, el modelo de proxy y el modelo directo.

Puede utilizar cualquiera de los siguientes modelos de implementación de correo electrónico, junto con las políticas de correo electrónico que defina en la consola UEM para administrar de forma eficaz sus dispositivos móviles.

- En el modelo de implementación de proxy, un servidor independiente llamado servidor de proxy Secure Email Gateway (SEG) se coloca entre el servidor de Workspace ONE y el servidor de correo electrónico corporativo. Este servidor de proxy filtra todas las solicitudes de los dispositivos al servidor de correo y transmite el tráfico únicamente desde los dispositivos aprobados. De este modo el servidor de correo electrónico corporativo está protegido, ya que no se comunica de forma directa con los dispositivos móviles.
- En el modelo de implementación directa, no hay ningún servidor de proxy implicado y Workspace ONE UEM se comunica directamente con los servidores de correo electrónico. La ausencia de servidor de proxy simplifica la instalación y la configuración en este modelo.

Nota El modelo de implementación de proxy tiene dos variantes: las plataformas clásica y SEG V2. La plataforma SEG clásica ya no se admite, ya que la plataforma SEG V2 garantiza un rendimiento mayor que el que ofrece la plataforma clásica. La plataforma SEG V2 se puede instalar en un servidor SEG existente con un tiempo de inactividad mínimo y durante una actualización, sin que sea necesario realizar ningún cambio de perfil ni interactuar con el usuario final.

Modelo de implementación	Modo de configuración	Infraestructura de correo
Modelo de implementación de proxy	Microsoft Exchange 2010/2013/2016 Exchange Office 365	Microsoft Exchange 2010/2013/2016/2019 Exchange Office 365 HCL Domino con HCL Gmail
Modelo de implementación directa: PowerShell	Modelo PowerShell	Microsoft Exchange 2010/2013/2016/2019 Microsoft Office 365
Modelo de implementación directa: Gmail	Gmail	

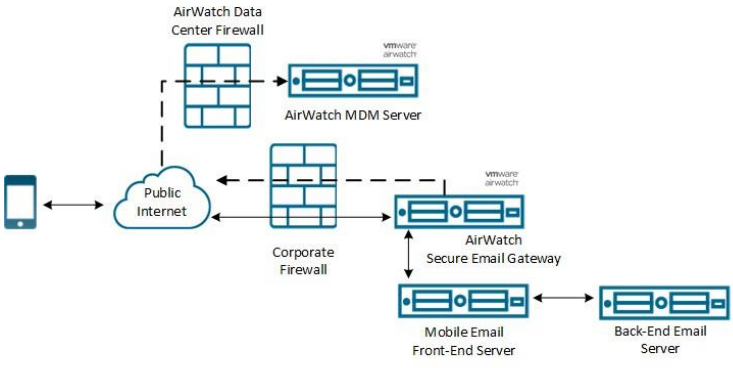
Nota Workspace ONE UEM solo ofrece soporte para las versiones de servidores de correo de terceros con soporte por parte del proveedor. Cuando el proveedor declara una versión de servidor como obsoleta, Workspace ONE UEM deja de ofrecer integración con esa versión.

Modelo Proxy SEG (Secure Email Gateway)

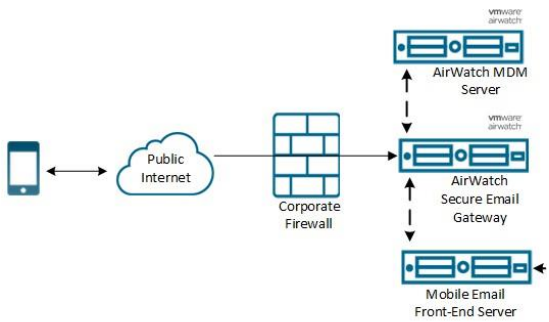
El servidor de proxy SEG (Secure Email Gateway) es un servidor independiente que se instala conforme a su servidor de correo electrónico para que todo el tráfico de correo electrónico hacia los dispositivos móviles pase por el proxy. Según la configuración que se defina en la consola de UEM, el servidor de proxy SEG toma decisiones de “permitir” o “bloquear” para cada dispositivo móvil que administra.

El servidor de proxy SEG filtra todas las solicitudes de comunicación enviadas al servidor de correo electrónico corporativo y solo transmite el tráfico de los dispositivos aprobados. La retransmisión protege el servidor de correo electrónico corporativo, ya que no permite que ningún dispositivo se comunique con él.

Instale el servidor SEG en su red para que esté conforme con el tráfico de correo electrónico corporativo. También puede instalarlo en una red de perímetro (DMZ) o detrás de un proxy inverso. Debe instalar el servidor SEG en el centro de datos, sin importar si su servidor de MDM de Workspace ONE se encuentra en la nube o en la sede.



Cloud Architecture

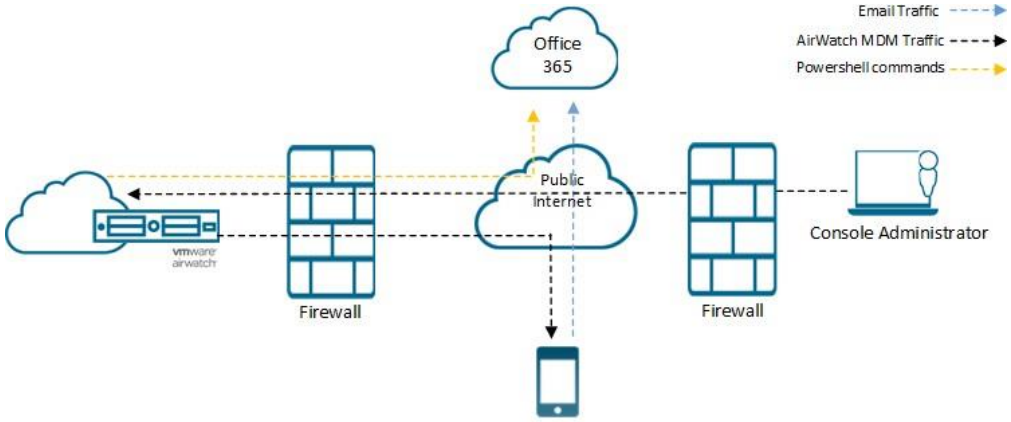


On-premise Architecture

Modelo PowerShell de implementación directa

En el modelo PowerShell, Workspace ONE UEM adopta el rol administrativo de PowerShell y envía comandos a la infraestructura de Exchange ActiveSync (EAS) para permitir o prohibir el acceso al correo electrónico según las políticas definidas en UEM console. Las implementaciones de PowerShell no requieren un servidor de proxy de correo electrónico independiente y el proceso de instalación es más simple.

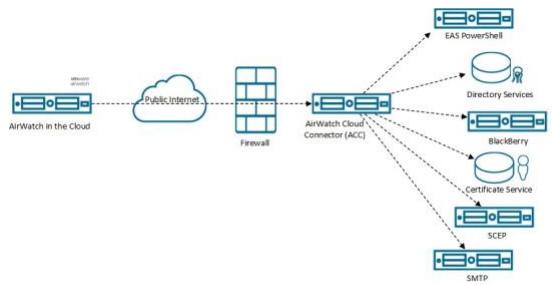
Las implementaciones de PowerShell están destinadas a las organizaciones que utilizan Microsoft Exchange 2010, 2013, 2016, 2019 u Office 365.



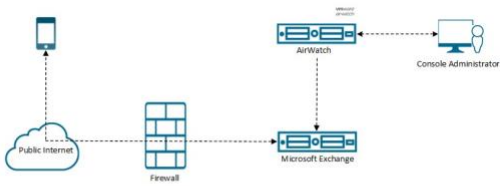
Microsoft Office 365

Hay dos formas en las que se emiten los comandos de PowerShell en función de dónde se encuentran el servidor de Workspace ONE UEM y el servidor de Exchange:

- El servidor de Workspace ONE se encuentra en la nube y el servidor de Exchange se encuentra en la sede: el servidor de Workspace ONE UEM emite los comandos de PowerShell. El VMware Enterprise Systems Connector configura la sesión de PowerShell con el servidor de correo electrónico.
- El servidor de Workspace ONE UEM y el servidor de correo electrónico se encuentran en la sede: el servidor de Workspace ONE UEM configura la sesión de PowerShell directamente con el servidor de correo electrónico. Aquí no se requiere el servidor de VMware Enterprise Systems Connector, a menos que el servidor de Workspace ONE UEM no pueda comunicarse directamente con el servidor de correo electrónico.



Microsoft Exchange 2010 with AirWatch Cloud



Microsoft Exchange 2010 with AirWatch On-Prem

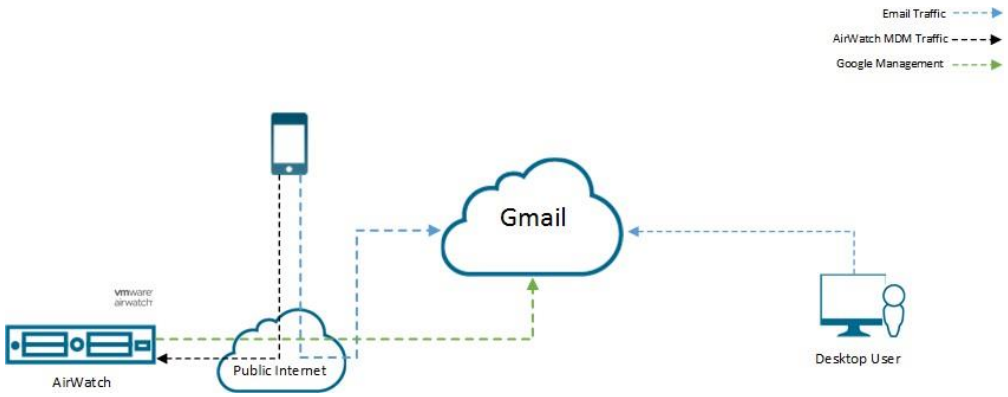
Para obtener ayuda para elegir entre los modelos de implementación de PowerShell y Secure Email Gateway, consulte la sección de recomendaciones de Workspace ONE UEM.

Modelo Gmail directo

Integrar servidor de Workspace ONE UEM con Google.

Es posible que las organizaciones que utilizan la infraestructura de Gmail estén familiarizadas con los retos que implica proteger los extremos de correo electrónico de Gmail y evitar que los correos circunvalen los extremos seguros. Workspace ONE UEM facilita la tarea con un método flexible y seguro para integrar la infraestructura de correo electrónico.

En el modelo de implementación de Gmail directo, el servidor de Workspace ONE UEM se comunica directamente con Google. En función de las necesidades de seguridad, Workspace ONE puede administrar la contraseña de Google de un usuario y controlar el acceso al buzón de correo del usuario.



Llamadas de la API a Google Suite: puede personalizar los atributos utilizados en las llamadas de la API a Google Suite especificando un atributo alternativo en lugar de la dirección de correo electrónico del usuario. De forma predeterminada, se utiliza la dirección de correo electrónico del usuario. Para obtener más información sobre cómo configurar el modelo Gmail directo, consulte *Cómo integrar el modelo directo utilizando administración de contraseñas*.

Matriz de los modelos de implementación de MEM

Utilice la matriz siguiente para comparar las características disponibles en los diferentes modelos de implementación de MEM.

Office 365 requiere configuración adicional para el modelo Proxy SEG. Workspace ONE UEM recomienda el modelo directo de integración para los servidores de correo electrónico en la nube. Consulte la sección de recomendaciones de Workspace ONE UEM para obtener más información.

✓	Compatible	□	No compatible con Workspace ONE UEM
X	La función no está disponible	N/A	No aplicable

Tabla 2-1. Matriz de implementación

	Modelo Proxy SEG			Modelo directo		
	Exchange 2010/2013/2016/2019 Office 365	HCL Notes Traveler	Google	Office 365(PowerShell)	Exchange 2010/2013/2016/2019 (PowerShell)	Gmail
Herramientas de seguridad de correo electrónico						
Ajustes de seguridad obligatorios						
Uso de firmas digitales a través de la capacidad de S/MIME	✓	□	□	✓	✓	N/A
Protección de datos confidenciales por medio de cifrado obligatorio	✓	✓	✓	✓	✓	✓
Exigir seguridad SSL	✓	✓	✓	✓	✓	✓
Seguridad de hipervínculos y archivos adjuntos de correo electrónico						
Establezca que los archivos adjuntos y los hipervínculos se abran solo en VMware AirWatch Content Locker o Workspace ONE Web	✓	✓	✓	x	x	x
Configuración automática del correo electrónico						
Configuración inalámbrica del correo electrónico en el dispositivo	✓	✓	✓	✓	✓	✓

Tabla 2-1. Matriz de implementación (continuación)

	Modelo Proxy SEG			Modelo directo		
	Exchange 2010/2013/2016/2019 Office 365	HCL Notes Traveler	Google	Office 365(PowerShell)	Exchange 2010/2013/2016/2019 (PowerShell)	Gmail
Control de acceso al correo electrónico						
Bloqueo de acceso al correo electrónico en dispositivos no administrados	✓	✓	✓	✓	✓	✓
Detección de dispositivos sin administrar	✓	✓	✓	✓	✓	N/A
Acceso al correo electrónico por medio de políticas de conformidad personalizables	✓	✓	✓	✓	✓	✓
Requerir el cifrado del dispositivo para acceder al correo electrónico	✓	✓	✓	✓	✓	✓
Restringir dispositivos comprometidos a la hora de acceder al correo electrónico	✓	✓	✓	✓	✓	✓
Permitir/bloquear correo electrónico - Cliente de correo	✓	✓	✓	✓	✓	x
Control de acceso al correo electrónico						
Permitir/bloquear correo electrónico - Usuario	✓	✓	✓	✓	✓	x

Tabla 2-1. Matriz de implementación (continuación)

	Modelo Proxy SEG			Modelo directo		
	Exchange 2010/2013/2016/2019 Office 365	HCL Notes Traveler	Google	Office 365(PowerShell)	Exchange 2010/2013/2016/2019 (PowerShell)	Gmail
Permitir/bloquear correo electrónico - Modelo del dispositivo	✓	✓	✓	✓	✓	✓
Permitir/bloquear correo electrónico - Dispositivo OS	✓	✓	✓	✓	✓	✓
Permitir/bloquear correo electrónico - Tipo de dispositivo EAS	✓	✓	✓	✓	✓	x
Visibilidad de la administración						
Estadísticas del tráfico de correo electrónico	✓	✓	✓	x	x	x
Estadísticas de los clientes de correo electrónico	✓	✓	✓	x	x	x
Administración de certificados						
Integración/ revocación de CA	✓	□	□	✓	✓	N/A
Arquitectura						
Puerta de enlace en línea (proxy)	✓	✓	✓	N/A	N/A	✓
PowerShell de Exchange	N/A	N/A	N/A	✓	✓	N/A
Administración de contraseñas para Gmail	N/A	N/A	✓	N/A	N/A	✓
Integración de API de directorio para Gmail	N/A	N/A	N/A	N/A	N/A	✓
Compatible						

Tabla 2-1. Matriz de implementación (continuación)

	Modelo Proxy SEG			Modelo directo		
	Exchange 2010/2013/2016/2019 Office 365	HCL Notes Traveler	Google	Office 365(PowerShell)	Exchange 2010/2013/2016/2019 (PowerShell)	Gmail
Workspace ONE Boxer para iOS y Android [^]	✓	✓	✓	✓	✓	✓
Cliente nativo de correo electrónico de iOS	✓	✓	✓	✓	✓	✓
Cliente nativo de correo electrónico de Android (Gmail)	✓	✓	✓	✓	✓	✓
Cliente de HCL Notes de Android*	N/A	✓	N/A	N/A	N/A	N/A

*La seguridad de archivos adjuntos e hipervínculos de correo electrónico no es compatible con el cliente de HCL Notes de Android.

+ Exchange 2003 no es compatible

^ Exchange 2003, Requerir perfil de ActiveSync y MEM múltiples no son compatibles con Workspace ONE Boxer.

Recomendaciones de Workspace ONE UEM

En esta sección, se enumeran las características compatibles con Workspace ONE UEM y los tamaños de implementación adecuados. Utilice la matriz de decisión para elegir la implementación que más se ajuste a sus necesidades.

Cifrado de los archivos adjuntos

Gracias al cifrado obligatorio de archivos adjuntos de sus dispositivos móviles, Workspace ONE UEM puede ayudarle a mantener sus archivos adjuntos de correo electrónico protegidos sin que ello afecte a la experiencia de los usuarios finales.

	Nativo	Traveler	Workspace ONE Boxer
iOS	✓		
Android	✓		
SEG solo admite el cifrado de archivos adjuntos y la transformación de hipervínculos en Workspace ONE Boxer si estas funciones están habilitadas en la configuración de la aplicación Boxer en la consola de UEM. SEG admite el cifrado de archivos adjuntos con Exchange 2010/2013/2016/2019 y Office 365.			

Nota SEG no cifra los archivos adjuntos para Workspace ONE Boxer, pero DLP se puede aplicar a nivel de aplicación.

Administración de correo electrónico

La lista le proporciona el mayor nivel de seguridad con la implementación y la administración más sencillas posibles.

Infraestructura del correo electrónico	Gmail	PowerShell	SEG (Secure Email Gateway)
Infraestructura de correo en la nube			
Office 365		✓	✓
Gmail	✓		✓
Infraestructura de correo en la sede			
Exchange 2010		✓	✓
Exchange 2013		✓	✓
Exchange 2016		✓	✓
Exchange 2019		✓	✓
HCL Notes			✓

^Utilice Secure Email GatewaySecure Email Gateway (SEG) para todas las infraestructuras de correo en la sede cuyas implementaciones tengan más de 100 000 dispositivos. Para las implementaciones con menos de 100 000 dispositivos, también tiene la opción de utilizar PowerShell para la administración de correo electrónico. Consulte la Matriz de decisión de Secure Email Gateway frente a PowerShell.

**El umbral para las implementaciones de PowerShell está basado en el conjunto de pruebas de rendimiento más recientes y puede cambiar con cada versión. Para las implementaciones de hasta 50 000 dispositivos, los procesos de sincronización y de ejecución de conformidad pueden ser relativamente rápidos (menos de tres horas). A medida que el tamaño de la implementación se acerca a los 100 000 dispositivos, los administradores deben tener en cuenta que el tiempo de los procesos de sincronización y de ejecución de conformidad puede aumentar de 3 a 7 horas.

Matriz de decisión de Secure Email Gateway frente a PowerShell

Esta matriz le presenta información sobre las funciones de implementación de SEG y PowerShell para ayudarle a elegir la implementación que mejor se ajuste a sus necesidades.

	Ventajas	Desventajas
SEG	■ Conformidad en tiempo real ■ Cifrado de archivos adjuntos ■ Transformación de hipervínculos	■ Se requieren servidores adicionales
PowerShell	■ No se requiere un servidor en la sede adicional para la administración de correo electrónico ■ El tráfico de correo no pasa por un servidor en la sede antes de ir a Office 365, por lo que no se necesita ADFS	■ Sin sincronización de conformidad en tiempo real ■ No apto para implementaciones grandes (más de 100 000)
Microsoft aconseja utilizar los servicios de federación de Active Directory (ADFS) para evitar el acceso directo a las cuentas de correo electrónico de Office 365.		

Cómo migrar el correo electrónico a Workspace ONE UEM

3

Puede migrar su correo electrónico a un modelo de Administración de correo electrónico móvil (MEM) mediante Workspace ONE UEM

Si migra a uno de estos modelos MEM podrá aplicar políticas de control de acceso al correo electrónico para otorgar acceso al correo electrónico únicamente a los dispositivos y usuarios aprobados:

- Secure Email Gateway (SEG)
- PowerShell
- Gmail

Cómo migrar a Secure Email Gateway

La migración del correo electrónico a Secure Email Gateway (SEG) permite a los usuarios acceder a los mensajes de correo electrónico solo a través del proxy SEG.

El uso de SEG exige las políticas de control de acceso de correo electrónico para proveer acceso solo a los usuarios y dispositivos aprobados. Las directivas de cifrado de archivos adjuntos garantizan la seguridad de los datos.

1 Configure SEG en su grupo organizativo requerido en Global en Consola Workspace ONE UEM. .

2 Descargue e instale SEG..

3 Pruebe la funcionalidad de SEG utilizando la política de conformidad de correo electrónico.

   a Desactive temporalmente todas las políticas de conformidad.

   b Pida a todos los usuarios que inscriban sus dispositivos en Workspace ONE UEM.

   c Proporcione a todos los dispositivos inscritos un nuevo perfil de correo electrónico (con la dirección URL del servidor de SEG como el nombre de host).

   d Recuerde periódicamente a los usuarios de dispositivos sin administrar que deben inscribirse en Workspace ONE UEM.

   e Para bloquear el acceso de EAS al servidor de correo en una fecha específica, modifique las reglas de firewall (o Threat Management Gateway). Así garantiza que los dispositivos móviles no puedan acceder al servidor de correo directamente.

f Habilite todas las políticas de conformidad.

Nota Webmail, Outlook Web Access (OWA) y otros clientes de correo que estén en uso mantendrán el acceso al servidor de correo.

Cómo migrar a PowerShell

Puede proteger sus dispositivos y sincronizar los dispositivos con Exchange u Office 365 para correos electrónicos si migra a PowerShell.

PowerShell detecta los dispositivos administrados y sin administrar y, con la ayuda de las políticas de control de acceso al correo electrónico, proporciona acceso únicamente a los usuarios y dispositivos aprobados.

1 Configure la integración de PowerShell en el grupo organizativo apropiado bajo "Global" en Workspace ONE UEM Console.

2 Configure la integración con los grupos de usuarios (ya sean personalizados o predefinidos).

3 Pruebe la funcionalidad de PowerShell con un subconjunto de usuarios (usuarios de prueba, por ejemplo) para comprobar que las siguientes funciones se ejecutan correctamente:

   a Sincronización con el servidor de correo electrónico para detectar dispositivos.

   b Control de acceso en tiempo real.

4 Desactive temporalmente todas las políticas de conformidad.

5 Proporcione un nuevo perfil de correo electrónico a todos los dispositivos que se hayan inscrito en Workspace ONE UEM con el nombre de host del servidor de correo electrónico.

6 Realice una sincronización con el servidor de correo electrónico para detectar todos los dispositivos (administrados y sin administrar) que se estén sincronizando para recibir el correo electrónico.

7 Recuerde periódicamente a los usuarios de dispositivos sin administrar que deben inscribirse en Workspace ONE UEM.

8 Active e imponga reglas de conformidad para bloquear el acceso al correo electrónico de todos los dispositivos que no estén conformes en alguna fecha determinada, inclusive de los dispositivos sin administrar.

9 Configure el servidor de correo electrónico para que bloquee todos los dispositivos de forma predeterminada.

Nota El panel de control del correo electrónico muestra la lista de dispositivos sin administrar como bloqueados y los dispositivos administrados que están permitidos para correo electrónico.

Integración de Gmail con Workspace ONE UEM

Si migra a Gmail, puede sincronizar sus dispositivos con el servidor de Gmail. Puede integrar su Gmail con o sin Secure Email Gateway (SEG) o directamente con las API de directorio.

1 Habilite la opción de inicio de sesión único (SSO) en Gmail o cree un certificado de cuenta de servicio.

2 Configure la integración de Gmail en la Consola Workspace ONE UEM con el asistente de configuración de MEM.

3 Proporcione a los usuarios perfiles de EAS con las nuevas contraseñas aleatorias. Los dispositivos que no reciban el perfil se bloquearán automáticamente y no podrán acceder a Gmail.

Cómo migrar dispositivos

Puede migrar dispositivos entre grupos organizativos e implementaciones de MEM usando Workspace ONE UEM.

1 En Consola Workspace ONE UEM, navegue a **Tablero de correo electrónico**.

2 Filtre los dispositivos administrados que estén en su “Implementación de MEM” actual.

3 En la página **Vista de lista**, seleccione todos los dispositivos y seleccione la opción **Migrar dispositivos** en el menú desplegable **Administración**.

4 En la página **Confirmación para migrar dispositivos**, introduzca el código de clave indicado para confirmar la migración y seleccione la configuración en la que desea implementar los dispositivos.

5 Seleccione **Continuar**.

Resultados

Después de completar estos pasos, Workspace ONE UEM elimina automáticamente el perfil de Exchange ActiveSync (EAS) anterior y envía el nuevo perfil de EAS al grupo de implementación de destino. Entonces el dispositivo se conecta a su nuevo grupo de implementación. El nombre de configuración MEM actualizado del dispositivo se muestra en el Panel de control de correo electrónico.

Configuración de la implementación de la administración de correo electrónico móvil

4

Integre su infraestructura de correo electrónico en pocos pasos con el asistente de configuración de Administración de correo electrónico móvil (MEM).

MEM solo puede configurarse en un grupo organizativo primario y no se puede reemplazar desde un grupo organizativo secundario. Puede asociar una configuración de MEM a uno o varios perfiles de Exchange ActiveSync (EAS).

1 Navegue a **Correo electrónico** > **Ajustes** y, a continuación, seleccione **Configurar**.

2 Seleccione el modelo de implementación y, a continuación, elija el tipo de correo electrónico. Seleccione **Siguiente**.

a Si el modelo de implementación es Proxy, seleccione el tipo de correo electrónico.

Puede elegir:

- Exchange
- Google
- HCL Notes

b Si el modelo de implementación es Directo, seleccione el tipo de correo electrónico.

Puede elegir:

- Exchange
- Google Apps con integración directa de API
- Google Apps con aprovisionamiento de contraseña: seleccione “Con retención de contraseña” o “Sin retención de contraseña” como tipo de implementación de Gmail

Para más información sobre los niveles de implementación, consulte la sección tipo de implementación de correos electrónicos.

3 Introduzca los detalles del tipo de implementación que haya seleccionado.

Puede elegir:

- Para las implementaciones de SEG:

1 Introduzca el nombre descriptivo de esta implementación.

2 Introduzca los datos del servidor de proxy de SEG.

- Para las implementaciones de PowerShell:
  1 Introduzca el nombre descriptivo de esta implementación.
  2 Introduzca los detalles del servidor de PowerShell, la autenticación y los ajustes de sincronización.
- Para Gmail:
  1 Introduzca el nombre descriptivo de esta implementación.
  2 Introduzca los detalles de los ajustes de Gmail, la autenticación, la integración API del directorio de Gmail y los ajustes de Proxy SEG.

4 Asocie un perfil de EAS de plantilla a la implementación de MEM y seleccione **Siguiente**.

a Cree un perfil de EAS de plantilla para esta implementación.

Los nuevos perfiles de plantilla no se publican automáticamente a los dispositivos. Puede publicar perfiles en sus dispositivos desde la página Perfiles.

b (Opcional) Asocie un perfil existente a esta implementación si se va a configurar más de una implementación de MEM en un solo grupo organizativo.

La página **Resumen de configuración MEM** muestra los detalles de configuración.

5 Seleccione **Guardar**.

6 Después de seleccionar “Guardar”, puede agregar ajustes avanzados a la implementación.

a Seleccione el icono **Avanzado**  que corresponda a su implementación.

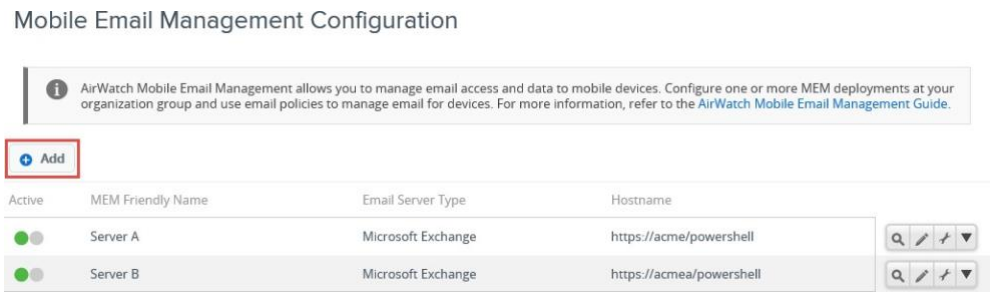
b Configure los ajustes disponibles para los buzones de los usuarios según los requisitos que aparezcan en la página **Configuración avanzada de la administración de correo electrónico móvil**.

c Seleccione **Guardar**.

Pasos siguientes

Para configurar varias implementaciones de MEM, seleccione **Agregar** (disponible en la página principal de **Configuración de administración de correo electrónico móvil**) y lleve a cabo los pasos 2–7.

En la implementación de SEG, puede asignar una configuración particular como la predeterminada por medio de la opción **Establecer como predeterminado** disponible en  .



Nota

- Debe crear grupos de usuarios cuyos miembros pertenezcan solo a uno de los dos grupos si va a conectar varios entornos de PowerShell al mismo servidor de Exchange.
- Utilice dominios diferentes en la configuración si va a conectar entornos de Gmail.
- Contemple la posibilidad de conectar la integración de SEG y PowerShell al mismo entorno de correo electrónico solo durante la migración de implementaciones de MEM con los ajustes apropiados. El Soporte de Workspace ONE puede ayudarle con esta implementación.

Cómo habilitar el correo electrónico basado en certificados

El uso de certificados con las credenciales de nombre de usuario y contraseña estándar tiene algunas ventajas, ya que los certificados mejoran la autenticación frente al acceso no autorizado. También evita que los usuarios tengan que introducir una contraseña o tengan que renovarla todos los meses. Los correos electrónicos confidenciales entre destinatarios pueden cifrarse a través de S/MIME o verificar su identidad por medio de una firma de mensaje.

1 Navegue a **Dispositivos > Perfiles y recursos > Perfiles**.

2 Seleccione **Agregar > Agregar perfil** y, después, seleccione la plataforma requerida.

3 Elija el ajuste del perfil **Credenciales** y configúrelo.

   a En **Fuente de credenciales**, seleccione cualquiera de las que aparecen en la lista.

   Puede elegir:

   - **Cargar**: cargue un certificado e introduzca el nombre del mismo.
   - **Entidad definida de certificación**: seleccione la entidad de certificación y la plantilla de certificado en el menú desplegable de su grupo organizativo.

     Las entidades de certificación y plantillas se agregan al grupo organizativo en **Dispositivos > Certificados > Entidades de certificación**.

4 Seleccione la opción para **Guardar y publicar** los ajustes.

Configuración del atributo de usuario para llamadas de MEM a Google Suite

Las implementaciones de Gmail, de manera predeterminada, usan las API de Google para administrar el acceso a Gmail. Puede identificar el usuario de inscripción con la dirección de correo electrónico de este mientras envía comandos a Google. Además, un administrador también puede seleccionar un atributo personalizado de Active Directory en lugar de la dirección de correo electrónico del usuario para identificar al usuario en Google.

Este atributo personalizado se puede utilizar cuando la dirección de correo electrónico de Google se encuentre en un campo de atributo personalizado de Active Directory del cliente. Los ajustes de los atributos personalizados se aplican a Google Apps mediante el aprovisionamiento de contraseñas, Google Apps con integración directa de API, así como SEG V2 con métodos automáticos de implementación de aprovisionamiento de contraseñas.

1 Vaya a **Cuentas > Administradores > Configuración de administradores > Servicios de directorio > Usuario**. El administrador de Workspace ONE UEM puede asignar los valores de los atributos personalizados y utilizar el valor de asignación de Active Directory de los clientes.

2 Habilite el atributo personalizado en la página **Servicio de directorio**, introduzca un valor de asignación y sincronice a los usuarios de Active Directory para actualizar el atributo personalizado del usuario de inscripción. Para obtener más información sobre cómo habilitar el atributo personalizado, consulte el tema sobre la asignación de la información del usuario de servicios de directorio en la guía Integración del servicio de directorio.

3 Vaya a **Correo electrónico > Ajustes de correo electrónico** y seleccione **Configurar**. Configure la puerta de enlace de la plataforma y seleccione **Siguiente**.

4 En la Página **Agregar configuración de correo electrónico**, seleccione el modelo de implementación como **Directo**, el tipo de correo electrónico como **Google Apps con integración directa de API** y seleccione **Siguiente**.

5 Escriba un nombre descriptivo para esta implementación en la página implementación. Introduzca los detalles de los ajustes de Gmail, la autenticación, la integración API del directorio de Gmail y los ajustes de Proxy SEG.

6 Introduzca un valor en **Dirección de correo electrónico de usuario de Google**. El valor predeterminado de Dirección de correo electrónico de usuario de Google es Dirección de correo electrónico. Un administrador puede seleccionar un atributo personalizado en lugar de la dirección de correo electrónico predeterminada.

7 Configure los perfiles de correo electrónico. Consulte Capítulo 6 Configuración de los perfiles de correo electrónico .

Resultados:

Puede utilizar el atributo personalizado cuando la dirección de correo electrónico de Google se encuentre en un campo de atributo personalizado del Active Directory del cliente.

Asignación del dispositivo a la administración de correo electrónico móvil

5

La inscripción de dispositivos, la asignación de perfiles de correo electrónico en dispositivos y las modificaciones en el estado de conformidad del dispositivo influyen. Las configuraciones de MEM se asignan a los dispositivos en función de los perfiles de EAS presentes en los dispositivos. Las políticas de conformidad de los perfiles administrados y requeridos de ActiveSync garantizan que las configuraciones manuales y sin administrar siguen restringidas.

Dispositivos con perfil de Exchange Active Sync (EAS)

Cuando un dispositivo con un perfil de EAS se asocia con una configuración de MEM en concreto, Workspace ONE UEM envía actualizaciones de la política a dicha configuración de MEM. Esta función facilita las migraciones y varias configuraciones de MEM en las que se administran uno o varios entornos de correo electrónico.

Independiente de cuál sea el cliente de correo, todos los modelos de Google de MEM requieren un perfil de EAS. Si se trata de nuevas instalaciones, es obligatorio asociar un perfil de EAS a una configuración de MEM. Para las actualizaciones, un administrador tiene que asociar un perfil de EAS a la configuración de MEM al momento de terminar el proceso de actualización.

Integración de proxy SEG

Workspace ONE UEM transmite un mensaje a todas las configuraciones de MEM del grupo organizativo en el que está inscrito el dispositivo. Este mensaje describe el estado de conformidad del dispositivo. Si la conformidad cambia, se envía un mensaje actualizado. Cuando el dispositivo se conecta a un servidor SEG determinado, SEG reconoce el dispositivo gracias al mensaje transmitido anteriormente. El proxy SEG informa a VMware AirWatch de que el dispositivo ha sido detectado. Entonces, Workspace ONE UEM asocia el dispositivo a la configuración de MEM para el SEG y lo muestra en el Tablero de correo electrónico.

Si hay varios servidores SEG que tienen las cargas repartidas, los mensajes de transmisión de una sola política se aplicarán a un solo SEG. Aquí se incluyen los mensajes enviados desde la Consola Workspace ONE UEM a SEG tras la inscripción o cuando se infringe o corrige la conformidad. Utilice la sincronización delta con un intervalo de actualización de diez minutos para facilitar los dispositivos que se acaban de inscribir o que están conformes. Estos dispositivos tienen un periodo de espera de un máximo de diez minutos antes de que el correo electrónico comience a sincronizarse.

Ventajas:

- Políticas actualizadas de la misma fuente de API para todos los servidores SEG.
- Efecto menor sobre el rendimiento del servidor de API.
- Implementación o mantenimiento más sencillo en comparación con el modelo SEG de agrupación.
- Menos puntos de error, ya que cada SEG se encarga de su propio conjunto de políticas.
- Mejor experiencia de usuario.

Integración de PowerShell

Las configuraciones de MEM de PowerShell se comportan de la misma manera que el SEG en lo que se refiere a las actualizaciones de las políticas. Para las migraciones a PowerShell, es importante que los nuevos perfiles se asocien a la configuración de MEM de PowerShell. La asociación de un nuevo perfil reduce la comunicación innecesaria con la anterior configuración de MEM.

Integración de Gmail

En este tipo de implementación se necesitan perfiles, excepto cuando se integra con las API del directorio de Google. A menos que los dispositivos se suministren con los perfiles, la implementación configurada de Gmail no los identifica o administra.

Sincronizar dispositivos

Utilice MEM para sincronizar los dispositivos asociados con un grupo organizativo.

Una vez configurada la implementación de administración de correo electrónico móvil (MEM), los dispositivos del grupo organizativo asociado se sincronizarán con MEM. Puede ver el estado de los dispositivos y otros detalles en la página del **Tablero de correo electrónico** de la Consola Workspace ONE UEM.

La aparición de los dispositivos en el tablero dependerá de los modelos de implementación a los que se asignen los dispositivos.

- SEG Proxy: los dispositivos administrados con el proxy SEG aparecen en el tablero cuando el proxy SEG informa de que están conectados y administrados.
- PowerShell: los dispositivos administrados con PowerShell aparecen en el tablero cuando Workspace ONE UEM envía un cmdlet de PowerShell para permitir que el dispositivo se conecte al correo electrónico.
- Gmail: los dispositivos administrados con Gmail aparecen en el tablero cuando el perfil de EAS de Workspace ONE UEM se coloca en la cola para el dispositivo.

El Tablero de correo electrónico muestra uno de los siguientes estados:

- **Administrado y asignado**: dispositivos inscritos con un *memconfigID* identificado.

- **Administrado y sin asignar**: dispositivos inscritos para los que todavía no se ha identificado el *memConfigID* ni con la asignación de perfil ni con la detección automática.
- **Sin administrar y detectado**: dispositivos que aún no están inscritos en Workspace ONE UEM, pero que han sido detectados por una configuración de MEM específica en el grupo organizativo.

Configuración de los perfiles de correo electrónico

6

Para implementar el correo de EAS con el cliente de correo nativo (Android), cree un perfil de configuración para el cliente de Gmail.

1 Navegue a **Dispositivos > Perfiles y recursos > Perfiles > Agregar > Agregar perfil > Android**.

2 Seleccione **Dispositivo** para implementar su perfil en un dispositivo.

3 Configure los ajustes de la sección **General** del perfil. Estos ajustes determinan la forma en la que se implementa el perfil y los usuarios que lo recibirán.

4 Seleccione la carga útil de **Exchange ActiveSync**.

5 Configure los ajustes de **Exchange ActiveSync**.

Ajustes	Descripción
Cliente de correo	Seleccione **Gmail** como el tipo de cliente de correo.
Nombre de la cuenta	Introduzca la descripción de la cuenta de correo.
Host de Exchange ActiveSync	Introduzca la dirección URL externa del servidor de ActiveSync de la compañía. El servidor de ActiveSync puede ser cualquier servidor de correo que implemente el protocolo de ActiveSync, tales como HCL Notes Traveler, Novell Data Synchronizer y Microsoft Exchange. Para las implementaciones de Secure Email Gateway (SEG), utilice la dirección URL de SEG y no la del servidor de correo.
Ignorar errores de SSL	Habilite esta opción para permitir que el dispositivo ignore los errores de SSL de los procesos del Workspace ONE Intelligent Hub.
Dominio	Introduzca el dominio del usuario final. Puede utilizar los valores de búsqueda en vez de crear perfiles individuales para cada usuario final.
Usuario	Introduzca el nombre de usuario del usuario final. Puede utilizar los valores de búsqueda en vez de crear perfiles individuales para cada usuario final.

Ajustes	Descripción
Dirección de correo electrónico	Introduzca la dirección de correo electrónico del usuario final. Puede utilizar los valores de búsqueda en vez de crear perfiles individuales para cada usuario final. **Nota** Si utiliza el atributo personalizado para GSuite, debe usar el valor de búsqueda de atributos personalizados para el campo **Dirección de correo electrónico** en el perfil de correo electrónico de Exchange ActiveSync. Consulte Configuración del atributo de usuario para llamadas de MEM a Google Suite.
Contraseña	Introduzca la contraseña del usuario final. Puede utilizar los valores de búsqueda en vez de crear perfiles individuales para cada usuario final.
Certificado de identidad	Seleccione (si lo desea) un certificado de identidad en el menú desplegable si requiere que el usuario final presente un certificado para conectarse a Exchange ActiveSync, de lo contrario, seleccione **Ninguno** (opción predeterminada). Para obtener la información adicional necesaria para seleccionar un certificado para esta carga útil, consulte Cómo implementar credenciales.
Número de días trascurridos de correo para sincronizar	Seleccione el número de días transcurridos de correo para sincronizar con el dispositivo.
Número de días transcurridos de calendario para sincronizar	Seleccione el número de días transcurridos en el calendario del dispositivo para sincronizar.
Sincronizar calendario	Habilite esta opción para que los calendarios se sincronicen con el dispositivo.
Sincronizar contactos	Habilite esta opción para que los contactos se sincronicen con el dispositivo.
Permitir sincronización de las tareas	Habilite esta opción para permitir la sincronización de las tareas con el dispositivo.
Tamaño máximo de truncamiento del correo electrónico	Defina el tamaño máximo antes de truncar los mensajes de correo electrónico cuando se sincronizan con los dispositivos.
Firma de correo electrónico	Introduzca la firma de correo electrónico que se mostrará en los correos que se envíen.
Permitir archivos adjuntos	Habilite esta opción para permitir los archivos adjuntos en los correos electrónicos.
Tamaño máximo de archivos adjuntos	Defina el tamaño máximo de los archivos adjuntos en MB.
Permitir el reenvío de correo electrónico	Habilite esta opción para permitir el reenvío de los correos electrónicos.

Ajustes	Descripción
Permitir formato HTML	Permite determinar si los correos electrónicos que se sincronizan con el dispositivo pueden estar en formato HTML. Si no se habilita este ajuste, todos los correos electrónicos se convertirán en texto sin formato.
Inhabilitar capturas de pantalla	Habilite esta opción para impedir que se tomen capturas de pantalla en el dispositivo.
Intervalo de sincronización	Introduzca el número de minutos entre sincronizaciones.
Días pico para programación de sincronización	■ Programe los días pico de la semana para la sincronización y la **Hora de inicio** y la **Hora de finalización** para la sincronización en los días seleccionados. ■ Defina la frecuencia de la **Sincronización en horario pico** y la **Programación de la sincronización fuera de horas pico**. ■ Al seleccionar **Automático**, se sincroniza el correo electrónico durante todas las actualizaciones. ■ Al seleccionar **Manual**, solo se sincroniza el correo electrónico cuando se selecciona. ■ Al seleccionar un valor de tiempo, se sincroniza el correo electrónico según un programa definido. ■ Habilite las opciones **Utilizar SSL**, **Utilizar TLS** y **Cuenta predeterminada**, si así lo desea.
Ajustes de S/MIME	Seleccione **Utilizar S/MIME**. Ahí puede seleccionar un certificado S/MIME que usted asocia como **Certificado de usuario** en la carga útil de **Credenciales**. ■ **Certificado S/MIME** – Seleccione el certificado que se utilizará. ■ **Requerir mensajes S/MIME cifrados** – Habilite esta opción para requerir el cifrado. ■ **Requerir mensajes S/MIME firmados**: habilite esta opción para requerir mensajes S/MIME firmados. Indique un **Host de migración** si utiliza los certificados S/MIME para el cifrado. Seleccione **Guardar** para guardar los ajustes o **Guardar y publicar** para guardar y enviar los ajustes del perfil al dispositivo requerido.

6 Seleccione **Guardar** para guardar los ajustes o **Guardar y publicar** para guardar y enviar los ajustes del perfil al dispositivo requerido.

Cómo configurar un perfil de correo de EAS para el cliente de correo nativo

Cree un perfil de configuración de correo electrónico para el cliente de correo nativo en dispositivos iOS.

1 Navegue a **Dispositivos > Perfiles y recursos > Perfiles > Agregar.**Seleccione **Apple iOS**.

2 Configure los ajustes de la sección **General** del perfil.

3 Seleccione la carga útil de **Exchange ActiveSync**.

4 Seleccione **Cliente de correo nativo** para el **Cliente de correo**. Complete el cuadro de texto **Nombre de la cuenta** con la descripción de esta cuenta de correo. Introduzca la dirección URL del servidor de ActiveSync de la empresa en el campo **Host de Exchange ActiveSync**.

Nota El servidor de ActiveSync puede ser cualquier servidor de correo que implemente el protocolo de ActiveSync, tales como HCL Notes Traveler, Novell Data Synchronizer y Microsoft Exchange. Para las implementaciones de Secure Email Gateway (SEG), utilice la dirección URL de SEG y no la del servidor de correo electrónico.

5 Marque la casilla **Utilizar SSL** para habilitar el uso de la capa de sockets seguros (SSL) para los correos electrónicos entrantes.

6 Seleccione la casilla **S/MIME** para utilizar otros certificados de cifrado. Antes de habilitar esta opción, asegúrese de haber cargado los certificados necesarios en los ajustes de perfil de **Credenciales**.

   a Seleccione el **Certificado S/MIME** para firmar los mensajes de correo electrónico.

   b Seleccione el **Certificado de cifrado S/MIME** para firmar y cifrar los mensajes de correo electrónico.

   c Marque la casilla de **Habilitar conmutador de "Por mensaje"** para permitirles a los usuarios finales que escojan los mensajes individuales de correo electrónico que vayan a firmar y cifrar utilizando el cliente de correo nativo de iOS (solo dispositivos iOS 8+ supervisados).

7 Rellene la **Información de inicio de sesión**, entre la que se incluyen los valores de búsqueda **Nombre de dominio, Nombre de usuario y Dirección de correo electrónico**. Los valores de búsqueda obtienen la información directamente del registro de la cuenta de usuario. Para utilizar los valores de búsqueda {EmailDomain}, {EmailUserName} y {EmailAddress}, asegúrese de que las cuentas de usuario de Workspace ONE UEM tengan una dirección de correo electrónico y un nombre de usuario de correo electrónico definidos.

8 Deje el campo **Contraseña** vacío para pedirle al usuario que introduzca una contraseña.

9 Seleccione el **Certificado de carga útil** para definir un certificado para la autenticación basada en el certificado después de haberlo agregado en la carga útil de **Credenciales**.

10 Configure los siguientes ajustes opcionales de **Ajustes y seguridad** según proceda:

a **Número de días transcurridos de correo para sincronizar** – Se descarga la cantidad definida de correo. Tenga en cuenta que cuanto más largo sea el periodo de tiempo, más datos se consumirán durante la descarga del correo.

b **Impedir mover mensajes** – Le impide al usuario mover correos del buzón de Exchange a cualquier otro buzón en el dispositivo.

c **Prevenir el uso en aplicaciones de terceros** – Le impide a otras aplicaciones el uso del buzón de Exchange para enviar mensajes.

d **Prevenir sincronización de las direcciones recientes**: desactiva las sugerencias de contactos cuando envía un correo en Exchange.

e **Bloquear Mail Drop**: desactiva el uso de la función de Mail Drop de Apple.

f **Habilitar correo**: habilita la configuración de una aplicación de correo independiente para la cuenta de Exchange (iOS 13).

g **Permitir la alternancia de correo**: si está desactivada, evita que el usuario active o desactive el correo (iOS 13).

h **Habilitar contactos**: habilita la configuración de una aplicación de contactos independiente para la cuenta de Exchange (iOS 13).

i **Permitir la alternancia de contactos**: si está desactivada, evita que el usuario active o desactive los contactos (iOS 13).

j **Habilitar calendarios**: habilita la configuración de una aplicación de calendario independiente para la cuenta de Exchange (iOS 13).

k (iOS 13) **Permitir la alternancia de calendarios**: si está desactivada, evita que el usuario active o desactive los calendarios.

l **Habilitar notas**: habilita la configuración de una aplicación de notas independiente para la cuenta de Exchange.

m **Permitir la alternancia de notas**: si está desactivada, evita que el usuario active o desactive las notas (iOS 13).

n (iOS 13) **Habilitar recordatorios**: habilita la configuración de una aplicación de recordatorios independiente para la cuenta de Exchange.

o **Permitir la alternancia de recordatorios**: si está desactivada, evita que el usuario active o desactive los recordatorios (iOS 13).

11 Asigne la **Default Audio Call App** que su cuenta EAS nativa utilizará para realizar llamadas cuando seleccione un número de teléfono en un mensaje de correo electrónico.

12 Seleccione **Guardar y publicar** para enviar el perfil a los dispositivos disponibles.

Perfiles de Exchange ActiveSync (escritorio de Windows)

Los perfiles de Exchange ActiveSync le permiten configurar los dispositivos de escritorio de Windows para que accedan a su servidor de Exchange ActiveSync y utilicen el correo electrónico y el calendario.

Utilice certificados firmados por una autoridad de certificado de terceros de confianza (CA). Cualquier error en sus certificados hace que las conexiones seguras se vuelvan vulnerables a posibles ataques de tipo “Man in the middle” (ataques de intermediarios). Ese tipo de ataques afectan negativamente la confidencialidad y la integridad de los datos que se transmiten entre los componentes del producto, y también les dan la oportunidad a los intrusos de interceptar o alterar los datos mientras están en tránsito.

El perfil de Exchange ActiveSync es compatible con el cliente de correo nativo para escritorio de Windows. La configuración varía según el cliente de correo que utilice.

Eliminación de un perfil o eliminación empresarial

Si se elimina el perfil con un comando de eliminación de perfil, una política de conformidad o una eliminación empresarial, se eliminan todos los datos de correo electrónico, tales como:

- La información de la cuenta de usuario/inicio de sesión.
- Datos de los mensajes de correo electrónico
- Información de los contactos y el calendario.
- Adjuntos guardados en el almacenamiento interno de la aplicación.

Nombre de usuario y contraseña

Si tiene nombres de usuarios de correo electrónico que difieren de las direcciones de correo de los usuarios, puede utilizar el cuadro de texto **{EmailUserName}**, que corresponde a los nombres de usuarios de correo electrónico que se importaron durante el proceso de integración del servicio de directorio. Incluso aunque los nombres de usuario coincidan con las direcciones de correo electrónico, use el cuadro de texto **{EmailUserName}**, ya que este utiliza la dirección de correo importada a través de la integración del servicio de directorio.

Configuración de un perfil de Exchange ActiveSync (escritorio de Windows)

Cree un perfil de Exchange ActiveSync para ofrecer a los dispositivos con escritorio de Windows acceso a su servidor de Exchange ActiveSync para usar el correo electrónico y el calendario.

Nota Workspace ONE UEM no es compatible con Outlook 2016 para los perfiles de Exchange ActiveSync. La configuración del perfil de Servicios Web Exchange (EWS) para la aplicación Outlook en un dispositivo de escritorio de Windows a través de Workspace ONE UEM ya no es compatible con la versión 2016 de Microsoft Exchange.

1 Navegue a **Dispositivos > Perfiles > Vista en lista > Agregar** y seleccione **Agregar perfil**.

2 Seleccione **Windows** y luego la plataforma de **Escritorio de Windows**.

3 Seleccione **Perfil de usuario**.

4 Configure los ajustes de la sección **General** del perfil.

5 Seleccione la carga útil de **Exchange ActiveSync**.

6 Configure los ajustes de Exchange ActiveSync:

Ajustes	Descripción
Cliente de correo	Seleccione el cliente de correo que configura el perfil de EAS. Workspace ONE UEM es compatible con el cliente de correo nativo.
Nombre de la cuenta	Introduzca el nombre para la cuenta de Exchange ActiveSync.
Host de Exchange ActiveSync	Introduzca la dirección URL o la dirección IP del servidor que hospeda el servidor EAS.
Utilizar SSL	Habilite esta opción para enviar todas las comunicaciones a través de la capa de sockets seguros (SSL).
Dominio	Introduzca el dominio de correo electrónico. El perfil es compatible con los valores de búsqueda para agregar la información de inscripción e inicio de sesión del usuario. Para obtener más información, consulte la sección Nombre de usuario y contraseña en la parte inferior de la página.
Nombre de usuario	Introduzca el nombre de usuario del correo electrónico.
Dirección de correo electrónico	Introduzca la dirección de correo electrónico. Este es un campo requerido.
Contraseña	Introduzca la contraseña de correo electrónico.
Certificado de identidad	Seleccione el certificado de la carga útil de EAS. Consulte Configurar una carga útil de credenciales para obtener más información.
El próximo intervalo de sincronización (min)	Seleccione la frecuencia, en minutos, con la que el dispositivo se sincroniza con el servidor de EAS.
Número de días trascurridos de correo para sincronizar	Seleccione cuántos días de correos electrónicos anteriores se sincronizan con el dispositivo.
Registro de diagnósticos	Habilite esta opción para registrar la información con fines de solución de problemas.
Exigir la protección de datos cuando el dispositivo esté bloqueado	Habilite esta opción para exigir que los datos estén protegidos cuando el dispositivo esté bloqueado.
Permitir la sincronización del correo electrónico	Habilite esta opción para permitir la sincronización de los mensajes de correo electrónico.

Ajustes	Descripción
Permitir la sincronización de los contactos	Habilite esta opción para permitir la sincronización de los contactos.
Permitir la sincronización del calendario	Habilite esta opción para permitir la sincronización de los eventos del calendario.

7 Seleccione **Guardar** para mantener el perfil en la consola de Workspace ONE UEM o **Guardar y publicar** para enviarlo a los dispositivos.

Aplicación del control de acceso de correo electrónico 7

Cómo configurar el control de acceso para proporcionar acceso seguro a su infraestructura de correo electrónico.

Políticas de conformidad de correo electrónico

Después de la implementación del correo electrónico, puede aumentar la seguridad del correo móvil con el control de acceso. La función de control de acceso limita el acceso a la infraestructura de correo a solo los dispositivos seguros y que estén en estado de conformidad. El control de acceso se aplica con la ayuda de las políticas de conformidad de correo electrónico.

Las políticas de conformidad de correo electrónico mejoran la seguridad al restringir el acceso al correo electrónico a los dispositivos no conformes, sin cifrar, inactivos o sin administrar. Estas políticas le permiten limitar el acceso al correo electrónico a solo los dispositivos requeridos y aprobados. Las políticas de correo electrónico también restringen el acceso al correo electrónico según el modelo del dispositivo y el sistema operativo.

Estas políticas están categorizadas como Políticas generales de correo electrónico, Políticas de dispositivos administrados y Políticas de seguridad de correo electrónico. En la tabla se muestran las diferentes políticas que pertenecen a cada categoría y las implementaciones a las que se aplican.

En la siguiente tabla, se enumeran las directivas de cumplimiento de correo electrónico compatibles.

Tabla 7-1. Directivas de cumplimiento de correo electrónico

	SEG (Exchange, HCL Traveler, G Suite)	PowerShell (Exchange)	Administración de contraseñas (Gmail)	Integración directa (Gmail)
Políticas generales de correo electrónico				
Sincronizar ajustes	S	N		
Dispositivo administrado	S	S		
Cliente de correo	S	S		
Usuario	S	S		

Tabla 7-1. Directivas de cumplimiento de correo electrónico (continuación)

	SEG (Exchange, HCL Traveler, G Suite)	PowerShell (Exchange)	Administración de contraseñas (Gmail)	Integración directa (Gmail)
Tipo de dispositivo EAS	S	S		
Políticas de dispositivos administrados				
Inactividad	S	S		
Dispositivo comprometido	S	S		
Cifrado	S	S		
Modelo	S	S		
Sistema operativo	S	S		
Requerir perfil de ActiveSync	S	S		
Políticas de seguridad de correo electrónico				
Clasificación de seguridad del correo electrónico	S	N		
Adjuntos (dispositivos administrados)	S	N		
Adjuntos (dispositivos sin administrar)	S	N		
Hipervínculo	S	N		

Cómo activar una política de conformidad de correo electrónico

Las políticas de conformidad de correo electrónico disponibles en la Consola Workspace ONE UEM son Políticas generales de correo electrónico, Políticas de dispositivos administrados y Políticas de seguridad de correo electrónico. Puede activar cualquiera de estas políticas de conformidad de correo electrónico o editar las reglas para que estas políticas de correo electrónico permitan o bloqueen los dispositivos.

1 Navegue a **Correo electrónico > Políticas de conformidad**.

2 Utilice el icono de editar política, ubicado en la columna **Acciones**, para editar cualquiera de las reglas para una política.

Nota **Políticas generales de correo electrónico** exige el cumplimiento de las políticas en todos los dispositivos que acceden al correo electrónico. Si selecciona un grupo de usuarios, la política se aplica a todos los usuarios de ese grupo.

Política de correo electrónico	Descripción
Sincronizar ajustes	Impida que el dispositivo se sincronice con carpetas de EAS específicas. ■ Workspace ONE UEM evitará que los dispositivos se sincronicen con las carpetas seleccionadas sin importar qué otras políticas de conformidad estén vigentes. ■ Para que la política tome efecto, es necesario que se vuelva a publicar el perfil de EAS a los dispositivos (así se obliga a que el dispositivo se sincronice de nuevo con el servidor de correo electrónico).
Dispositivo administrado	Restrinja el acceso al correo electrónico solo a los dispositivos administrados.
Cliente de correo	Restrinja el acceso al correo electrónico a un conjunto de clientes de correo electrónico. ■ Puede permitir o bloquear clientes de correo electrónico según el tipo de cliente, como **Personalizado** y **Detectado** ■ También puede establecer acciones predeterminadas para el cliente de correo y para aquellos clientes de correo recién detectados que no se muestran en el menú desplegable de "Cliente de correo". Para el tipo de cliente personalizado, puede utilizar comodines (*) o la función de autocompletar.

Política de correo electrónico	Descripción
Usuario	Restrinja el acceso al correo electrónico a un conjunto de usuarios. Puede permitir o bloquear los tipos de usuarios que incluyan “Personalizado”, “Detectado”, “Cuenta de usuario de Workspace ONE UEM” y “Grupo de usuarios”. También puede establecer acciones predeterminadas para los nombres de usuario de correo electrónico que no se muestran en el campo desplegable "Nombre de usuario" o "Grupo". Para el tipo de usuario personalizado puede utilizar comodines (*) o la función de autocompletar.
Tipo de dispositivo EAS	Asigne dispositivos a las listas de permitidos o de no permitidos según el atributo Tipo de dispositivo EAS proporcionado por el dispositivo del usuario final. Puede permitir o bloquear dispositivos según el tipo de cliente de correo, como Personalizado y Detectado. También puede establecer acciones predeterminadas para los tipos de dispositivo EAS que no se muestren en el campo desplegable “Tipo de dispositivo”. Para el tipo de cliente personalizado, puede utilizar comodines (*) o la función de autocompletar.

Políticas de dispositivos administrados exige el cumplimiento de políticas en los dispositivos administrados que accedan al correo electrónico.

Política de correo electrónico	Descripción
Inactividad	Impida que los dispositivos administrados inactivos accedan al correo electrónico. Puede determinar la cantidad de días que un dispositivo aparece como inactivo (es decir, que no realiza una verificación de estado en VMware AirWatch) antes de que Workspace ONE UEM le bloquee el acceso al correo electrónico. El valor mínimo es 1 y el máximo 32767.
Dispositivo comprometido	Impida que los dispositivos en peligro accedan al correo electrónico. Esta política no bloquea el acceso al correo electrónico de los dispositivos que no hayan informado del estado comprometido a AirWatch.
Cifrado	Impida que los dispositivos sin cifrar accedan al correo electrónico. Esta política solo se aplica a los dispositivos que hayan informado a VMware AirWatch sobre el estado de la protección de datos.
Modelo	Restrinja el acceso al correo electrónico según la plataforma y el modelo del dispositivo.

Política de correo electrónico	Descripción
Sistema operativo	Restrinja el acceso al correo electrónico a un conjunto de sistemas operativos para determinadas plataformas.
Requerir perfil de ActiveSync	Restrinja el acceso al correo electrónico a los dispositivos sin administrar con un perfil de Exchange ActiveSync. Para los clientes de correo electrónico configurados a través de una configuración de la aplicación en lugar de a través del perfil de ActiveSync, el envío de una configuración de la aplicación a un cliente de correo electrónico administrado garantiza que el cliente de correo electrónico cumpla con la política de conformidad.

Políticas de seguridad de correo electrónico exige el cumplimiento de políticas para los archivos adjuntos e hipervínculos. Esta política se aplica solamente a las implementaciones de SEG. Para obtener más información, consulte la sección *Configuración de la aplicación del control de acceso de correo electrónico*.

Política de correo electrónico	Descripción
Clasificación de seguridad del correo electrónico	Defina la política para que SEG acepte correos electrónicos con y sin etiquetas. Puede utilizar las etiquetas predefinidas o crear etiquetas con la opción de personalización. Según la clasificación, puede permitir o bloquear el correo electrónico en clientes de correo.
Adjuntos (dispositivos administrados)	Cifre los elementos adjuntos de correo electrónico de los tipos de archivo seleccionados. Los archivos adjuntos están protegidos en el dispositivo y solo se pueden ver dentro de VMware AirWatch Content Locker. En estos momentos, la función solo está disponible para los dispositivos iOS y Android administrados que tengan la aplicación VMware AirWatch Content Locker. Para otros dispositivos administrados, puede elegir que se permitan archivos adjuntos cifrados, que se bloqueen todos los archivos adjuntos o que se permitan archivos adjuntos sin cifrar.

Política de correo electrónico	Descripción
Adjuntos (dispositivos sin administrar)	Cifre y bloquee los archivos adjuntos o permita los archivos adjuntos sin cifrar en los dispositivos sin administrar. Los archivos adjuntos cifrados no se pueden ver en dispositivos sin administrar. El propósito de esta función es mantener la integridad del correo electrónico. Si se reenvía un correo electrónico que tiene un archivo adjunto cifrado desde un dispositivo sin administrar, el destinatario podrá verlo en un PC u otro dispositivo móvil.
Hipervínculo	Permita que los usuarios de los dispositivos abran los hipervínculos de los correos electrónicos directamente en VMware Browser. El Secure Email Gateway modifica de forma dinámica el hipervínculo para abrirlo en VMware Browser. Puede escoger uno de los siguientes Tipos de modificación: ■ Todo: seleccione este tipo si desea abrir todos los hipervínculos en VMware Browser. ■ Excluir: seleccione este tipo si no desea que los usuarios de los dispositivos abran los dominios indicados en VMware Browser. Enumere los dominios excluidos en el campo **Modificar todos los hipervínculos excepto estos dominios**. También puede cargar los nombres de dominio en masa desde un archivo `.csv`. ■ Incluir: seleccione este tipo si desea que los usuarios de los dispositivos abran los hipervínculos de los dominios especificados en VMware Browser. Enumere los dominios incluidos en el campo **Solo modificar hipervínculos para estos dominios**. También puede cargar los nombres de dominio en masa desde un archivo `.csv`.

3 Cree la regla de conformidad y seleccione **Guardar**.

4 Seleccione el círculo gris de la columna **Activo** para activar la política de conformidad. Aparecerá una página en la que se mostrará un código de clave.

5 Introduzca el código de clave en el campo correspondiente y seleccione **Continuar**.

Resultados: la política se activa y aparece un círculo de color verde en la columna **Activo**.

Protección del contenido de los correos electrónicos, los archivos adjuntos y los hipervínculos

Proteja el correo electrónico usando Workspace ONE UEM Web y Workspace ONE UEM Content.

Workspace ONE UEM le ayuda a proteger y controlar los archivos adjuntos de correo electrónico móvil más vulnerables a la pérdida de datos en el caso de los dispositivos administrados y no administrados. Workspace ONE UEM permite que los usuarios de los dispositivos abran los hipervínculos de los correos electrónicos directamente en el Workspace ONE Web presente en el dispositivo. El Secure Email Gateway modifica de forma dinámica el hipervínculo para abrirlo en Workspace ONE Web.

Debe tener instaladas las aplicaciones siguientes antes de comenzar con la protección de los archivos adjuntos:

- Secure Email Gateway (SEG)
- VMware Content Locker (iOS y Android)
- Compatibilidad con Microsoft Exchange 2010/2013/2016/2019, HCL Notes, Novell GroupWise y Gmail

Cómo habilitar la clasificación de seguridad del correo electrónico

Seleccione las clasificaciones de seguridad en la consola UEMConsola Workspace ONE UEM para los que desea que Secure Email Gateway tome medidas.

Existe una lista de clasificaciones de seguridad predefinidas disponible, así como la opción de crear su propia clasificación personalizada.

1. Navegue a **Correo electrónico > Políticas de conformidad > Políticas de seguridad de correo electrónico**.
2. Seleccione el círculo de color gris en la columna **Activo** de la política de conformidad **Clasificaciones de seguridad del correo electrónico**. Aparecerá una página en la que se mostrará un código de clave.
3. Introduzca el código de clave en el campo correspondiente y seleccione **Continuar**. La política se activa y se indica con un círculo de color verde en la columna **Activo**.
4. Seleccione la opción **Editar** en la columna **Acciones**.
5. Seleccione **Agregar** y, a continuación, el tipo de etiqueta en el menú desplegable **Tipo**.

   Las opciones disponibles son “Predefinido“ y “Personalizado”. Puede elegir:

   - Seleccione el tipo de etiqueta “predefinido” para obtener una lista de las etiquetas disponibles en el menú desplegable **Clasificación de seguridad**.
   - Seleccione el tipo de etiqueta “personalizado” para introducir su propia etiqueta personalizada en el campo **Clasificación de seguridad**.
6. Introduzca la **Descripción** para la etiqueta y seleccione **Siguiente**.
7. Configure las medidas que SEG debe adoptar contra los correos electrónicos marcados o sin marcar con una etiqueta. Seleccione **Siguiente**.

Puede decidir si permitirá o bloqueará los correos electrónicos en clientes de correo.

8 Vea el **Resumen** y seleccione **Guardar**.

Cómo habilitar la protección de archivos adjuntos de correo electrónico

Proteger archivos adjuntos de correo electrónico mediante Workspace ONE UEM.

Los archivos adjuntos de correo electrónico corresponden a diferentes tipos de archivo. En la consola de UEM, puede seleccionar los tipos de archivo cuyos archivos adjuntos de correo electrónico deben cifrarse a través de Secure Email Gateway. Estos archivos adjuntos cifrados están protegidos en los dispositivos móviles y pueden verse utilizando la aplicación VMware AirWatch Content Locker.

Ajustes detallados para dispositivos iOS y Android administrados. Para otros dispositivos administrados y todos los dispositivos sin administrar, se puede impedir que los archivos adjuntos (en masa) se abran en aplicaciones de terceros.

1 Navegue a **Correo electrónico > Políticas de conformidad > Políticas de seguridad de correo electrónico**.

2 Seleccione el círculo de color gris de la columna **Activo** de la política de conformidad de **Adjuntos (dispositivos administrados)** o **Adjuntos (dispositivos sin administrar)**.

Resultados: aparecerá una página en la que se mostrará un código de clave.

3 Introduzca el código de clave en el campo correspondiente y seleccione **Continuar**.

Resultados: la política se activa y aparece un círculo de color verde en la columna **Activo**.

4 Seleccione la opción **Editar** en la columna **Acciones**.

5 Seleccione si desea "cifrar y permitir" o "bloquear y permitir sin cifrar" el adjunto para cada categoría de archivo (solo para dispositivos iOS y Android administrados).

6 Marque la casilla **Permitir que se guarden archivos adjuntos en Content Locker** para guardar los archivos adjuntos en Content Locker.

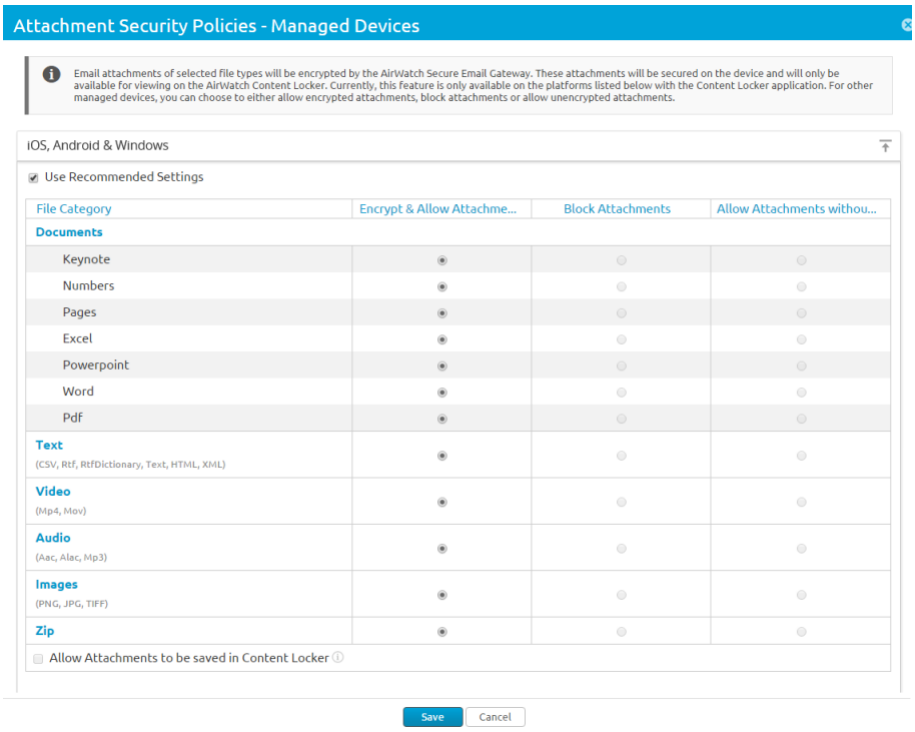
Resultados: los archivos adjuntos permanecen cifrados y las políticas de Content Locker aún se aplican.

7 Seleccione la política para **Otros archivos** que no se mencionan aquí.

8 Introduzca las extensiones de archivo que se deben excluir de las acciones configuradas en **Otros archivos** para la **Lista de exclusión**.

9 Introduzca el **Mensaje personalizado para archivos adjuntos bloqueados** para informar al destinatario de que se bloqueó un archivo adjunto.

10 Seleccione **Guardar**.



Cómo habilitar la protección del hipervínculo

Con la política de seguridad de correo electrónico de hipervínculos, podrá controlar los hipervínculos de los correos electrónicos que desean modificarse para que puedan abrirse directamente con Workspace ONE Web.

1 Navegue a **Correo electrónico > Políticas de conformidad > Políticas de seguridad de correo electrónico**.

2 Seleccione el círculo de color gris de la columna **Activo** de la política de conformidad **Hipervínculo**.

Resultados: aparecerá una página en la que se mostrará un código de clave.

3 Introduzca el código de clave en el campo correspondiente y seleccione **Continuar**.

Resultados: la política se activa y aparece un círculo de color verde en la columna **Activo**.

4 Seleccione la opción **Editar** en la columna **Acciones**.

5 Seleccione la plataforma en la que desee ignorar las transformaciones de hipervínculos.

6 Seleccione un **Tipo de modificación**.

Puede elegir:

- **Todo**: seleccione este tipo si desea abrir todos los hipervínculos en Workspace ONE Web.

- **Incluir**: seleccione este tipo si desea que los usuarios de los dispositivos abran los hipervínculos de los dominios especificados en Workspace ONE Web. Enumere los dominios incluidos en el campo **Solo modificar hipervínculos para estos dominios**. También puede cargar los nombres de dominio en masa con un archivo CSV.
- **Excluir**: seleccione este tipo si no desea que los usuarios de los dispositivos abran los dominios indicados en Workspace ONE Web. Enumere los dominios excluidos en el cuadro de texto **Modificar todos los hipervínculos excepto estos dominios**. También puede cargar los nombres de dominio en masa con un archivo CSV.

7 Seleccione **Guardar**.

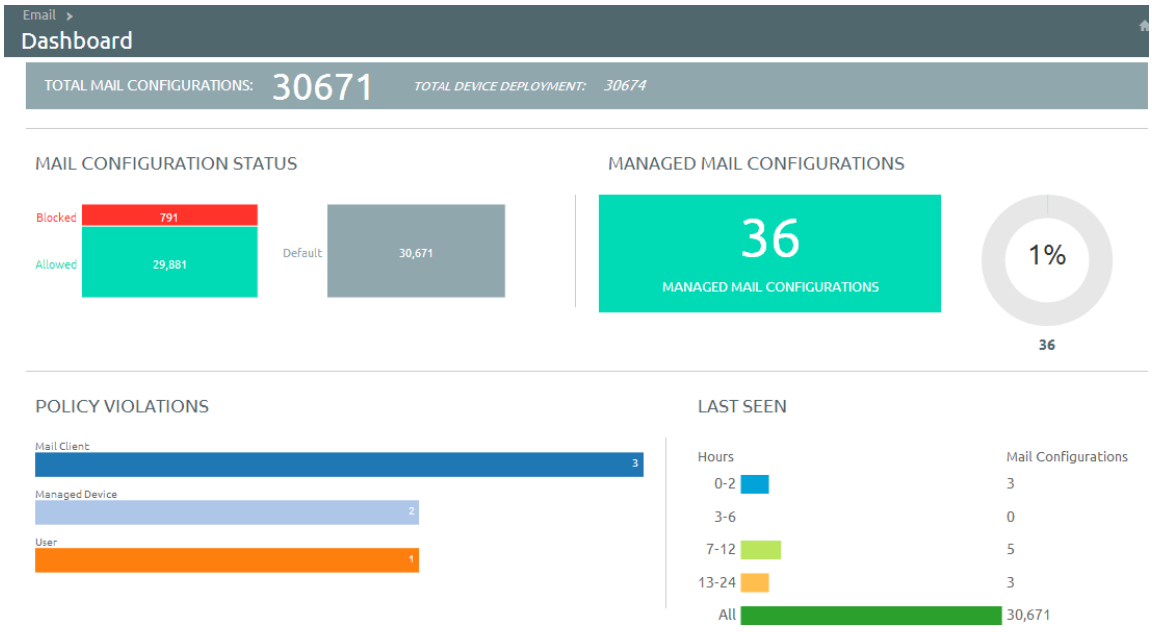
Supervisión del tráfico de correo electrónico

8

Supervise el tráfico de correo electrónico y los dispositivos del grupo de usuarios en el **Tablero de correo electrónico**.

Correo electrónico > Tablero le proporciona un resumen del estado de los dispositivos conectados al servidor de correo electrónico.

También puede utilizar las gráficas disponibles para filtrar su búsqueda. Por ejemplo, si desea ver todos los dispositivos administrados de un grupo organizativo, seleccione la gráfica Dispositivos administrados. Los resultados se mostrarán en la página “Vista de lista”.



Vea la información detallada del dispositivo y la información específica del usuario.

Puede ver todas las actualizaciones en tiempo real de los dispositivos de los usuarios finales que administra con administración de correo electrónico móvil (MEM) desde la página de **Correo electrónico > Vista de lista**.

Cambie entre las pestañas **Dispositivo** y **Usuario** para ver la información del usuario y del dispositivo. Para ver la lista resumida o personalizada de la información, cambie el Diseño.

- Vea los dispositivos administrados, sin administrar, conformes, no conformes, bloqueados o permitidos.
- Vea la dirección IP del dispositivo.

Nota Para Workspace ONE UEM versión 2107 y versiones posteriores, los detalles del dispositivo, como el SO, modelo, plataforma, número de teléfono, IMEI, etc., no se muestran en la página **Vista de lista**.

Puede ver el dispositivo o información específica sobre el usuario como lista resumida o personalizada según sus requisitos.

La página **Vista de lista** proporciona la siguiente información detallada:

Ajustes	Descripción
Última solicitud	El último cambio de estado del dispositivo de Workspace ONE UEM o de Exchange en la integración de PowerShell. En la integración de SEG, esta columna muestra la última vez que un dispositivo sincronizó el correo electrónico.
Usuario	El nombre de la cuenta de usuario.
Nombre descriptivo	El nombre descriptivo del dispositivo.
Configuración de MEM	La implementación de MEM configurada que administra el dispositivo.
Dirección de correo electrónico	La dirección de correo electrónico de la cuenta de usuario.
Identificador	El código de identificación alfanumérico único asociado al dispositivo.
Cliente de correo	El cliente de correo que sincroniza los correos electrónicos en el dispositivo.
Último comando	El último cambio de estado del dispositivo. Se rellena la columna **Última solicitud**.
Último servidor de Gateway	El servidor al que el dispositivo está conectado.

Ajustes	Descripción
Estado	El estado, en tiempo real, del dispositivo y si el correo electrónico del mismo está bloqueado o permitido según la política definida.
Razones	El código de razón para permitir o bloquear el correo electrónico en un dispositivo. ■ El código de razón aparece como “Global” si la política predeterminada de la organización para bloquear/ permitir/poner en cuarentena define el estado de acceso. El código de razón aparece como “Individual” si el administrador de Exchange o Workspace ONE UEM configura el ID del dispositivo explícitamente para un determinado buzón. El código de razón es “Política” si alguna política de EAS bloquea el dispositivo. ■ Workspace ONE UEM le ofrece la opción de bloquear los correos electrónicos en los dispositivos no conformes (por ejemplo, dispositivos con aplicaciones en la lista de no permitidos). Los correos electrónicos se habilitan cuando los dispositivos vuelven a estar en conformidad. Puede ver la lista de dispositivos no conformes en el **Tablero de correo electrónico** marcados con la etiqueta de razón “Conformidad de MDM”.

- **Dirección IP**: la dirección IP del dispositivo.

  Nota Para Workspace ONE UEM versión 2107 y versiones posteriores, los detalles del dispositivo, como el SO, modelo, plataforma, número de teléfono, IMEI, etc., no se muestran en la página **Vista de lista**.

- **Identidad del buzón**: la ubicación del buzón del usuario en el Active Directory.

Filtros

Reduzca la búsqueda de dispositivos usando la opción **Filtro** en la página “Vista de lista”.

Ajustes	Descripción
Última detección	Todo, menor que, 24 horas, 12 horas, 6 horas, 2 horas.
Administrado/a(s)	Todo, administrado/a(s), sin administrar.
Tipos de propiedad	Todo, permitido(s), bloqueado(s).
Reemplazo de la política	Todo, Lista de no permitidos, Lista de permitidos, Predeterminado.
Infracción de política	Comprometido, dispositivo inactivo, sin datos protegidos/inscrito/conforme con MDM, tipo de dispositivo EAS no aprobado/cuenta de correo electrónico/cliente de correo/modelo/SO.
Configuración de MEM	Filtrar dispositivos según las implementaciones de MEM configuradas.
Tipo de dispositivo EAS	Filtrar según el tipo de dispositivo.

Dirección de correo electrónico	Filtrar según la dirección de correo electrónico.
Último servidor de Gateway	Filtrar según el servidor Secure Email Gateway disponible.

Acciones del correo electrónico

Los menús desplegables **Reemplazar**, **Acciones** y **Administración** proporcionan un solo lugar donde se pueden realizar varias acciones en el dispositivo.

Importante Estas acciones no se pueden anular.

Reemplazar

Seleccione la casilla de algún dispositivo para aplicarle una acción. Coloque un dispositivo en la lista de permitidos o en la lista de no permitidos sin importar la política de conformidad y restituya la política cuando la necesite.

- **Lista de permitidos**: permite que un dispositivo reciba correos electrónicos.
- **Lista de no permitidos**: bloquea un dispositivo para que no reciba correos electrónicos.
- **Predeterminado**: permite o bloquea un dispositivo según el estado de conformidad o no conformidad.

Acciones

- **Sincronizar los buzones**: manda una consulta al servidor de Exchange para obtener una lista actualizada de los dispositivos que han intentado sincronizar el correo electrónico (modelo PowerShell directo). Si no selecciona esta opción, la lista de dispositivos sin administrar no cambiará a menos que uno de ellos se inscriba en Workspace ONE UEM o se añada a una lista de permitidos o lista de no permitidos manualmente y, por ende, inicie el comando para cambiar el estado.

  Workspace ONE UEM ofrece la opción de "Sincronización de correo electrónico" en el Portal de autoservicio (SSP) para que los usuarios puedan sincronizar los dispositivos con el servidor de correo electrónico y puedan también ejecutar políticas de conformidad preconfiguradas en todos sus dispositivos. Por lo general, el proceso es mucho más rápido que la sincronización en masa que se realiza en todos los dispositivos.
- **Ejecutar la conformidad**: provoca que el motor de conformidad ejecute la configuración de MEM seleccionada. Este comando se ejecuta de otra manera cuando se usa el modelo PowerShell en lugar del modelo SEG.
  - Si el SEG está configurado, este comando actualiza el SEG con las políticas de conformidad más recientes.
  - Si el modelo PowerShell está configurado, este comando ejecuta una comprobación de conformidad manualmente en todos los dispositivos y les bloquea o permite el acceso al correo electrónico.

Cuando se ha configurado el modelo Direct PowerShell, Workspace ONE UEM se comunica directamente con la matriz CAS utilizando sesiones de PowerShell firmadas de forma remota establecidas desde el servidor de la consola o VMware Enterprise Systems Connector (dependiendo de la arquitectura de implementación). Por medio de las sesiones firmadas de forma remota, los comandos de PowerShell se envían para añadir el ID de un dispositivo a la lista de no permitidos y a la lista de permitidos del buzón CAS de ciertos usuarios en Exchange 2010/2013 según el estado de conformidad del dispositivo en Workspace ONE UEM.

- **Habilitar el modo de prueba**: prueba las políticas de correo electrónico sin aplicárselas a los dispositivos de implementaciones integradas con SEG.

Administración

Seleccione la casilla de algún dispositivo para aplicarle una acción.

Ajustes	Descripción
Correo electrónico de inscripción	Envía al usuario un correo electrónico que contiene todos los detalles que necesita para la inscripción. Cuando detecte que hay algún dispositivo sin administrar, envíe un correo electrónico de inscripción para solicitarle al usuario que inscriba el dispositivo (PowerShell solamente).
Modo Dx activado	Ejecuta el diagnóstico en el buzón del usuario seleccionado para obtener el historial de la actividad del dispositivo. Esta opción solo está disponible para SEG.
Modo Dx desactivado	Desactiva el diagnóstico en el buzón del usuario seleccionado.
Actualizar la clave de cifrado	Restablece el cifrado y vuelve a sincronizar los correos electrónicos de los dispositivos seleccionados.
Eliminación total remota	Restablece el dispositivo a los ajustes de fábrica. Realice el restablecimiento empresarial (restablece los ajustes de fábrica) en los dispositivos perdidos o robados que contengan información confidencial (solo PowerShell).
Eliminar dispositivos sin administrar	Elimina del tablero el registro del dispositivo sin administrar que haya seleccionado.
Cómo migrar dispositivos	Migra los dispositivos entre grupos organizativos e implementaciones de MEM.
Sincronizar el buzón seleccionado	Sincroniza el buzón del dispositivo seleccionado. Solo puede sincronizar un buzón de dispositivo a la vez.

Nota Este registro podría volver a aparecer tras la próxima sincronización.

Cómo comprobar la presencia de dispositivos sin administrar

Para asegurarse de que los dispositivos están administrados y supervisados, navegue a la página “Vista de lista”. Desde la página Vista de lista, aplique un filtro para ver los dispositivos sin administrar y envíeles un correo de inscripción desde el menú desplegable Administración.