Empresas

Comunicación y conectividad | Cloud | IoT | Seguridad

Administración de dispositivos Android

VMware Workspace ONE UEM service

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

Cómo integrar Workspace ONE UEM con Android

Workspace ONE UEM con tecnología AirWatch le proporciona un conjunto de soluciones robustas de administración móvil para la inscripción, la protección, la configuración y la administración de su implementación de dispositivos Android. A través de Workspace ONE UEM console, tiene varias herramientas y funciones a su disposición para la administración de todo el ciclo de vida de los dispositivos personales y corporativos.

En la guía se explica cómo integrar Workspace ONE UEM como Administrador de movilidad empresarial (EMM) con los dispositivos Android.

Términos clave para Android

Estos términos clave asociados a Android le ayudarán a comprender cómo configurar e implementar los ajustes para los usuarios.

- Perfil de trabajo: el modo Perfil de trabajo, también conocido como Propietario del perfil, crea un contenedor dedicado en el dispositivo únicamente para el contenido y las aplicaciones empresariales. El modo Perfil de trabajo permite a las organizaciones administrar los datos y las aplicaciones empresariales, pero sin acceder a las aplicaciones y los datos personales del usuario. Las aplicaciones Android se indican con un icono de maletín para distinguirlas de las aplicaciones personales.
- Administrado de trabajo: el modo administrado de trabajo, también conocido como modo de propietario del dispositivo o modo totalmente administrado, bloquea todo dispositivo. Los usuarios tendrán acceso a las aplicaciones corporativas, pero no a las aplicaciones personales, a través de la tienda Google Play.
- Corporativo habilitado de forma personal: Corporativo habilitado de forma personal (COPE) se refiere a los dispositivos propiedad de la empresa. Se trata de algo similar al dispositivo administrado de trabajo, pero los usuarios reciben un perfil de trabajo para acceder a las aplicaciones corporativas. Siguen teniendo acceso a su tienda Google Play personal fuera del perfil de trabajo. COPE solo está disponible en dispositivos Android 8.0 o versiones posteriores.
- Cuenta de Google administrada: se refiere a la cuenta de Google registrada en el dispositivo utilizado para Android y ofrece la administración de aplicaciones de Android a través de Google Play. Esta cuenta está administrada por el dominio que administra su configuración de Android.
- Cuenta de Google Play administrada: para las organizaciones que desean configurar Android, pero no tienen cuentas de G Suite ni cuentas de Google administradas.
- Cuenta de servicio de Google: la cuenta de servicio de Google es una cuenta de Google

especial que utilizan las aplicaciones para acceder a las API de Google recomendadas para clientes de G Suite.

- Token de EMM: ID único que utiliza Workspace ONE UEM para conectar Workspace ONE UEM console a la cuenta de Google administrada.
- Dominio de Google administrado: dominio que se reclama para habilitar el Android asociado a su empresa.
- Configuración de dominio de Google: proceso de Google para reclamar un dominio de Google administrado.
- AirWatch Relay: la aplicación de Workspace ONE UEM que utilizan los administradores para inscribir en masa dispositivos Android en Workspace ONE UEM.
- Bump de NFC: tecnología de comunicación que permite que los dispositivos intercambien información al colocarlos al lado unos de otros, lo que se conoce como un "bump". Se realiza al utilizar la aplicación AirWatch Relay para pasar información del dispositivo primario al dispositivo secundario.
- AOSP/Red cerrada: el proyecto de código abierto de Android (Android Open Source Project, AOSP) o Red cerrada se refiere a dispositivos Android sin servicios móviles de Google (GMS) y entornos de Console sin acceso a Google. Con este modo de inscripción no se crea ninguna cuenta de Google.
- Inscripción basada en el usuario: cuando se inscribe un dispositivo, la cuenta de Google que se crea es la misma en todos los dispositivos inscritos por este empleado. Este método de inscripción es ideal cuando se asignan empleados a dispositivos sin inscripción preparada.
- Inscripción basada en dispositivos: la cuenta de Google generada es única para cada dispositivo inscrito por el mismo usuario. Esto es ideal para un dispositivo de inscripción preparada o dispositivos dedicados.
- Implementación progresiva: la implementación progresiva le permite seguir utilizando la implementación actual del dispositivo a medida que realiza la transición de Android (heredado) a Android Enterprise. Todas las implementaciones de dispositivos nuevas pueden estar inscritas en Android Enterprise y administrarse con dispositivos más antiguos.

Requisitos para usar Android con Workspace ONE UEM

Antes de implementar dispositivos Android, debe tener en cuenta los siguientes requisitos previos, requisitos para la inscripción, materiales complementarios y sugerencias útiles del equipo de Workspace ONE UEM.

Sistemas operativos compatibles

Android 5.X.X (Lollipop)

Android 6.X.X

Android 7.X.X

Android 8.X.X

Android 9.X.X

Aviso: LG Service Application ya no es compatible con los dispositivos LG que ejecutan Android 9 y versiones posteriores con implementaciones de Android (heredado). Si utiliza dispositivos LG con Android 9 o posterior mediante el método de inscripción de Android (heredado), debería considerar la posibilidad de migrar a Android Enterprise.

Android 10.X.X

Android 11.X.X

Android 12.X.X

Android 13.X.X

Aviso: Los clientes podrán acceder a un conjunto de funciones de privacidad actualizadas cuando se actualice un dispositivo de inscripción COPE de Android 10 a Android 11. En Descripción de los modos de dispositivos Android encontrará un resumen de las funciones clave y la funcionalidad de los dispositivos COPE.

Aviso: Si su organización requiere más tiempo para completar las pruebas, existen dos opciones para retrasar la actualización de los dispositivos a Android 11. Consulte Administrar actualizaciones de sistema para dispositivos Android.

Si los dispositivos no admiten la integración de Google Play EMM, consulte la implementación de Android (heredado) o use una configuración de AOSP/Red cerrada.

Para obtener más información sobre AOSP/Red cerrada, consulte Descripción de los modos de dispositivos Android.

Compatibilidad con Android GO

Workspace ONE UEM solo admite dispositivos que ejecutan Android GO en modo administrado de trabajo. Para estos dispositivos, se admiten todas las capacidades de administración de dispositivos para el modo administrado de trabajo, excepto las siguientes:

- Workspace ONE Launcher
- Funciones de aprovisionamiento de productos que requieren acceso o modificación de archivos o directorios en el dispositivo
    - Archivos/Acciones: solo se admiten Reiniciar y Ejecutar acciones de intención
    - Condiciones: se admiten todas las condiciones excepto Launcher
    - Evento/Acciones: se admiten todas las acciones excepto Aplicar ajustes personalizados

Requisitos de red para Android

Los dispositivos de los usuarios finales deben poder comunicarse con ciertos endpoints para acceder a las aplicaciones y los servicios. Los requisitos de red para Android son una lista de endpoints conocidos para las versiones actuales y anteriores de las API de administración empresarial.

A fin de alcanzar correctamente todos los endpoints, se necesita una conexión directa. Si los dispositivos están conectados detrás de un proxy, no se puede establecer comunicación directa y se produce un error en ciertas funciones.

Host de destino	Puertos	Fin

play.google.com,android.com,google-analytics.com, *.googleusercontent.com,*gstatic.com,*gvt1.com*, *ggpht.com,dl.google.com,dl-ssl.google.com, android.clients.google.com,*gvt2.com,*gvt3.com	TCP/443TCP, UDP/5228-5230	Google Play y updatesgstatic.com,* googleusercontent.com: contiene contenido generado por el usuario (por ejemplo, iconos de aplicaciones en la tienda)*gvt1.com, *.ggpht, dl.google.com,dl-ssl.google.com,android.clients.google.com: descarga de aplicaciones y actualizaciones, API de PlayStore, gvt2.com y gvt3.com se usan para reproducción, conectividad, supervisión y diagnóstico.
*.googleapis.com	TCP/443	EMM/API de Google/API de PlayStore
accounts.google.com, accounts.google.[country]	TCP/443	Autenticación para accounts.google.[country]. Use el dominio local de nivel superior para [country]. Por ejemplo, para Australia, utilice accounts.google.com.au y, para Reino Unido, use accounts.google.co.uk.
fcm.googleapis.com, fcm-xmpp.googleapis.com	TCP/443, 5228-5230	Firebase Cloud Messaging (por ejemplo, Buscar mi dispositivo, consola de EMM <-> comunicación DPC, como la inserción de configuraciones). Esto no funciona con proxies (consulte los detalles aquí).
pki.google.com, clients1.google.com	TCP/443	Búsqueda en la lista de revocación de certificados de certificados emitidos por Google
clients2.google.com, clients3.google.com. clients4.google.com, clients5.google.com, clients6.google.com	TCP/443	Dominios compartidos por varios servicios de back-end de Google, como informes de bloqueo, sincronización de marcadores de Chrome, sincronización de hora (tlsdate) y muchos otros.
omahaproxy.appspot.com	TCP/443	Actualizaciones de Chrome
android.clients.google.com	TCP/443	URL de descarga de CloudDPC utilizada en el aprovisionamiento de NFC
connectivitycheck.android.com, www.google.com	TCP/443	La prueba de conectividad anterior a la prueba de conectividad de Android CloudDPC v470 que empieza con N MR1 requiere que el acceso a https://www.google.com/generate _204 esté disponible o que la red Wi-Fi proporcionada apunte a un archivo PAC al que se pueda acceder. También se requiere para dispositivos AOSP que ejecuten Android 7.0 o una versión posterior.
www.google.com, www.google.com/generate_204		Dispositivos AOSP que ejecuten Android 7.0 o una versión posterior
android-safebrowsing.google.com, safebrowsing.google.com	TCP/443	Verificación de aplicaciones de Android.

Requisitos del proxy de servicios de dispositivos

La aplicación de servicios de dispositivos Workspace ONE UEM utiliza la API de atestación de SafetyNet de Google para verificar la integridad de los dispositivos Android y garantizar que no estén comprometidos. Para ello, realiza llamadas de API salientes a los servidores de Google. En entornos locales, las organizaciones pueden optar por solo permitir que la aplicación de servicios de dispositivos establezca conexiones salientes a través de un proxy. En estos casos, además de configurar los ajustes de proxy en el nivel de la aplicación a través de Workspace ONE UEM Console, los clientes también deben configurar este proxy saliente en el nivel del sistema para el

servidor Windows que aloja la aplicación de servicios de dispositivos. Si el servidor Windows no puede establecer conexiones salientes con los endpoints de Google requeridos, se producirá un error en la atestación de estado de SafetyNet.

Reglas del firewall para las consolas

Si la consola de EMM se encuentra ubicada a nivel local, será necesario que se pueda acceder a los destinos que aparecen a continuación desde la red para crear una empresa de Google Play administrada y para acceder al iFrame de Google Play administrado.

Estos requisitos reflejan los requisitos actuales de Google Cloud y están sujetos a cambios.

Host de destino	Puertos	Fin
play.google.com, www.google.com	TCP/443	Nueva inscripción en Play Enterprise, Google Play Store
fonts.googleapis.com*, .gstatic.com	TCP/443	iFrame JS, fuentes de Google, contenido generado por el usuario (por ejemplo, iconos de aplicaciones en la tienda)
accounts.youtube.com, accounts.google.com, accounts.google.com.*	TCP/443	Autenticación de cuenta, authdomains de cuenta específicos del país
apis.google.com, ajax.googleapis.com	TCP/443	GCM, otros servicios web de Google e iFrame JS
clients1.google.com, payments.google.com, google.com	TCP/443	Aprobación de aplicaciones
ogs.google.com	TCP/443	elementos de interfaz de usuario de iFrame
notifications.google.com	TCP/443	Notificaciones de escritorio/móvil

Requisitos de inscripción

Cada dispositivo Android implementado en su organización debe estar inscrito para poder comunicarse con Workspace ONE UEM y tener acceso al contenido y las funciones internas. La siguiente información es necesaria para poder inscribir un dispositivo Android.

Si hay un dominio de correo electrónico asociado al entorno. Si utiliza la detección automática:

- Dirección de correo electrónico: este es el correo electrónico asociado a la organización. Por ejemplo, JohnDoe@acme.com.
- Credenciales: esta combinación de nombre de usuario y contraseña le permite tener acceso a su entorno de Workspace ONE UEM. Estas credenciales pueden ser las mismas que las de sus servicios de directorio de red o pueden definirse en exclusiva en Workspace ONE UEM console.

Si hay un dominio de correo electrónico no asociado al entorno. Si no utiliza la detección automática:

Si un dominio no está asociado con su entorno, se le pedirá igualmente que introduzca su dirección de correo electrónico. Dado que la detección automática no está habilitada, se le pedirá la siguiente información:

- ID de grupo: el ID de grupo asocia su dispositivo a su rol corporativo, y está definido en Workspace ONE UEM console.
- Credenciales: la combinación única del nombre de usuario y la contraseña le permite acceder a su entorno de AirWatch. Estas credenciales pueden ser las mismas que las de sus servicios de directorio de red o pueden definirse en exclusiva en Workspace ONE UEM console.

Para descargar Workspace ONE Intelligent Hub y, posteriormente, inscribir un dispositivo Android, debe completar uno de los siguientes pasos:

- Vaya a https://www.getwsone.com y siga las indicaciones.
- Descargue Workspace ONE Intelligent Hub desde la tienda Google Play.

Restricciones de inscripción para Android

Las restricciones de inscripción le permiten aprovisionar la inscripción, por ejemplo, al restringir las inscripciones a usuarios conocidos, grupos de usuarios y varios dispositivos inscritos permitidos.

Estas opciones están disponibles si accede a Grupos y ajustes > Todos los ajustes > Dispositivos y usuarios > General > Inscripción. Además, seleccionando la pestaña Restricciones podrá personalizar las políticas de restricción de inscripción por grupo organizativo y funciones de grupo de usuarios.

Puede crear restricciones de inscripción basadas en:

- El fabricante y el modelo de Android para garantizar que solo los dispositivos aprobados se inscriban en Workspace ONE UEM. Cuando se inscribe un dispositivo Android, los criterios de restricción de inscripción y grupo inteligente se actualizan para incluir la nueva marca y el modelo del dispositivo.

  Aviso: Algunos dispositivos están fabricados por otros proveedores. Puede crear una política con el fabricante real del dispositivo para que las políticas surtan efecto. A continuación, se enumeran algunas maneras de identificar la fabricación del dispositivo:

  - Desplácese hasta la página Acerca de en los ajustes del dispositivo.
  - Con un comando adb: `adb shell getprop | grep "manufacturer"`.
- Dispositivos incluidos en listas de admitidos y bloqueados por UDID, IMEI y número de serie.

  Aviso: Al inscribir dispositivos con Android 10 o versiones posteriores en el modo de Perfil de trabajo, los dispositivos se mantienen en un estado pendiente hasta que UEM Console pueda recuperar el IMEI o número de serie de los dispositivos para ver si están en la lista de admitidos o de bloqueados. Hasta que esto se compruebe, el dispositivo no se inscribirá totalmente ni se enviará ningún dato de trabajo hasta que se complete la inscripción.

Descripción de los modos de dispositivo Android

Las características de administración integradas de Android permiten a los administradores de TI administrar los dispositivos que se utilizan exclusivamente para trabajo.

Android ofrece varios modos según el tipo de propiedad del dispositivo que se utilice dentro de su organización:

- Perfil de trabajo: Crea un espacio dedicado en el dispositivo únicamente para aplicaciones y

datos de trabajo. Se trata de la implementación ideal para aplicaciones del "programa de uso de dispositivos personales" (BYOD).

- Dispositivo administrado de trabajo: Permite a Workspace ONE UEM y a los administradores de TI controlar todo el dispositivo y aplicar un amplio rango de controles de directivas no disponibles para los perfiles de trabajo, pero restringe el dispositivo a un uso corporativo únicamente
    - Dispositivo corporativo habilitado de forma personal: Se refiere a los dispositivos que son propiedad de la empresa. Se trata de algo similar al dispositivo administrado de trabajo, pero se aprovisiona con un perfil de trabajo para uso personal y corporativo.
    - Dispositivo administrado de trabajo sin servicios de Google Play: Si utiliza Workspace ONE UEM en dispositivos del proyecto de código abierto de Android (Android Open Source Project, AOSP), dispositivos que no sean de GMS o con redes cerradas dentro de su organización, puede inscribir sus dispositivos con Android mediante el flujo de inscripción de dispositivos administrados de trabajo sin servicios de Google Play

Funcionalidad del modo Perfil de trabajo

Las aplicaciones del Perfil de trabajo se diferencian por un icono de maletín rojo, se denominan aplicaciones distintivas y se muestran en un iniciador unificado con las aplicaciones personales del usuario. Por ejemplo, el dispositivo muestra un icono personal para Google Chrome y un icono independiente para Chrome de trabajo, que se indican con el distintivo. Desde la perspectiva del usuario final, parece que son dos aplicaciones diferentes, pero la aplicación solo se instala una vez con los datos empresariales almacenados independientemente de los datos personales.

Workspace ONE Intelligent Hub se encuentra identificado y existe solo dentro del espacio de los datos del perfil de trabajo. No hay ningún tipo de control sobre las aplicaciones personales y Workspace ONE Intelligent Hub no tiene acceso a la información personal.

Hay una serie de aplicaciones del sistema que se incluyen con el Perfil de trabajo de forma predeterminada como Chrome de trabajo, Google Play, ajustes de Google, Contactos y Cámara, que se pueden ocultar utilizando un perfil de restricciones.

Ciertos ajustes muestran la separación entre las configuraciones personal y de trabajo. Los usuarios ven configuraciones independientes para los siguientes ajustes:

- Credenciales: ver certificados corporativos para la autenticación del usuario en los dispositivos administrados.
- Cuentas: ver la cuenta de Google administrada unida al Perfil de trabajo.
- Aplicaciones: enumera todas las aplicaciones instaladas en el dispositivo.
- Seguridad: muestra el estado de cifrado del dispositivo.

Funcionalidad del modo Dispositivo administrado de trabajo

Cuando se inscriben los dispositivos en el modo Dispositivo administrado de trabajo, se crea un modo integral de propiedad corporativa. Workspace ONE UEM controla todo el dispositivo y no hay separación de datos personales y de trabajo.

Hay ciertos factores importantes que cabe tener en cuenta para el modo administrado de trabajo:

- La pantalla principal no muestra aplicaciones distintivas como el modo Perfil de trabajo.
- Los usuarios tienen acceso a diferentes aplicaciones previamente cargadas al realizar la activación del dispositivo. Las aplicaciones adicionales solo se pueden aprobar y agregar a través de Workspace ONE UEM console.
- Workspace ONE Intelligent Hub está establecido como el administrador del dispositivo en los ajustes de seguridad y no se puede deshabilitar.
- Si se cancela la inscripción del dispositivo desde el modo de tareas administradas de trabajo, se iniciará el restablecimiento de fábrica del dispositivo.

Dispositivo administrado de trabajo sin servicios de Google Play

Si utiliza Workspace ONE UEM en dispositivos del proyecto de código abierto de Android (Android Open Source Project, AOSP), dispositivos que no sean de GMS o con redes cerradas dentro de su organización, puede inscribir sus dispositivos con Android mediante el flujo de inscripción de dispositivos administrados de trabajo sin servicios de Google Play. Puede alojar aplicaciones en la intranet de su organización y utilizar métodos de inscripción específicos de OEM para la implementación.

Deberá especificar en la consola de UEM que está utilizando AOSP/Red cerrada durante el registro de EMM para Android.

Aspectos que se deben tener en cuenta al utilizar un dispositivo administrado de trabajo sin servicios de Google Play en implementaciones de AOSP/Red cerrada:

- Si ya configuró Android en un grupo organizativo superior y desea implementar AOSP/Red cerrada solo en un grupo organizativo secundario específico, el administrador de la consola de UEM tiene una opción para especificar que las inscripciones listas para usar en el grupo organizativo secundario no tengan una cuenta gestionada de Google. Para obtener más información, consulte Ajustes de inscripción en el registro de EMM para Android.
- Si va a implementar dispositivos mediante Workspace ONE UEM 1907 y versiones anteriores, no es necesario llevar a cabo la configuración de UEM Console.
- Si va a implementar dispositivos mediante Workspace ONE UEM 1908 y versiones posteriores, debe configurar los ajustes en la página de registro de EMM para Android.
- Los métodos de inscripción admitidos son los siguientes:
    - Código QR
    - StageNow para dispositivos Zebra
    - Honeywell Enterprise Provisioner para dispositivos Honeywell
- La inscripción a través del identificador de Workspace ONE Intelligent Hub no es compatible con los dispositivos del AOSP.
- No se admite el perfil de actualización automática pública. Este perfil se aplica específicamente a las aplicaciones públicas y no funciona en los dispositivos del AOSP o redes cerradas.
- No se admite el perfil de protección de restablecimiento de fábrica.
- Las aplicaciones internas (alojadas en Workspace ONE UEM Console) se implementarán

silenciosamente en los dispositivos del AOSP/Red cerrada.

- Los dispositivos administrados para el trabajo inscritos sin una cuenta gestionada de Google no deben asignarse a ninguna aplicación pública y no deben tenerse en cuenta en el recuento de dispositivos de asignación de aplicaciones públicas.
- Versión de SO y requisitos de OEM para el Dispositivo administrado de trabajo sin servicios de Google Play:
    - AOSP (no GMS)
        - Zebra y Honeywell: debe ser una versión de SO que admita la inscripción de StageNow o de Honeywell Enterprise Provisioner.
        - Otros OEM: no son compatibles a menos que el OEM desarrolle compatibilidad para el mismo a través de un cliente como StageNow o permitiendo que los usuarios accedan a la inscripción del código QR.
    - Red cerrada
        - Zebra y Honeywell: Android 7.0 y versiones posteriores, o deben ejecutarse en una versión de sistema operativo que admita la inscripción de StageNow (también 7.0 o posterior) o Honeywell Enterprise Provisioner.
        - Otros OEM: Android 7.0 o versiones posteriores, ya que la inscripción del código QR es el único método admitido.
- Cuando se configura un dispositivo administrado de trabajo sin servicios de Google Play, Workspace ONE Intelligent Hub debe configurarse para utilizar AWCM en lugar de Firebase Cloud Messaging. Sin esta actualización, los dispositivos no recibirán notificaciones mediante push desde Console.

Modo Dispositivo corporativo habilitado de forma personal (COPE)

Cuando los dispositivos se inscriben utilizando el modo COPE el usuario sigue teniendo control sobre todo el dispositivo. La capacidad única del modo COPE es que permite aplicar dos conjuntos de directivas distintos, como las restricciones, para el dispositivo y dentro de un perfil de trabajo.

El modo COPE solo está disponible en dispositivos Android 8.0 +. Si inscribe dispositivos Android de una versión anterior a Android 8.0, el dispositivo se inscribe automáticamente como Dispositivo completamente administrado.

Existen algunas advertencias a tener en cuenta al inscribir los dispositivos en modo COPE:

- Para las nuevas inscripciones con Android 11 se debe utilizar Workspace ONE Intelligent Hub 20.08 para Android y Workspace ONE UEM Console 2008. Para obtener información específica, consulte Cambios en el dispositivo corporativo habilitado personalmente (COPE) en Android 11.
- El cifrado con PIN y el inicio de sesión único de Workspace ONE UEM mediante SDK no son compatibles con los dispositivos corporativos habilitados de forma personal. Se puede aplicar un código de acceso de trabajo para garantizar que el uso de aplicaciones de trabajo requiere el uso de un código de acceso.
- La inscripción preparada para dispositivos de un usuario único y la inscripción preparada para dispositivos de múltiples usuarios no se admiten para las inscripciones COPE.
- Las aplicaciones internas (alojadas en Workspace ONE UEM) y las aplicaciones públicas

implementadas en los dispositivos COPE se muestran en el catálogo de la aplicación en el perfil de trabajo.

- De forma similar a las inscripciones que son solo de perfil de trabajo, los dispositivos corporativos habilitados de forma personal proporcionan a los usuarios la opción para inhabilitar el perfil de trabajo (por ejemplo, si el usuario está de vacaciones). Cuando se inhabilita el perfil de trabajo, las aplicaciones de trabajo ya no presentan notificaciones y no se pueden iniciar. El estado (habilitado o inhabilitado) del perfil de trabajo se presenta al administrador en la página de detalles del dispositivo. Cuando el perfil de trabajo está inhabilitado, la información más reciente de la aplicación y del perfil no puede recuperarse desde el perfil de trabajo.
- Workspace ONE Intelligent Hub ya existe en las secciones del perfil totalmente administrado y de trabajo del dispositivo corporativo habilitado de forma personal. Al existir tanto dentro como fuera del perfil de trabajo, las políticas de administración se pueden aplicar al perfil de trabajo y a todo el dispositivo. Sin embargo, Workspace ONE Intelligent Hub solo está visible en el perfil de trabajo.
- Cuando se envían notificaciones mediante push al dispositivo, el Workspace ONE Intelligent Hub que se encuentra fuera del perfil de trabajo está disponible temporalmente para que el usuario vea los mensajes, garantizando que los mensajes importantes lleguen al usuario, incluso si el perfil de trabajo está inhabilitado temporalmente.
- Los perfiles asignados pueden verse a través de Workspace ONE Intelligent Hub en el perfil de trabajo.
- Las políticas de conformidad para la administración de aplicaciones (como bloquear/eliminar aplicaciones) solo se admiten para las aplicaciones que están dentro del perfil de trabajo. Las aplicaciones pueden estar en la lista negra en el dispositivo (fuera del perfil de trabajo) utilizando perfiles de control de aplicaciones.
- En dispositivos COPE con Android 11 o posterior, puede optar por realizar una eliminación empresarial en lugar de realizar una eliminación total del dispositivo. Puede seguir utilizando el comando Eliminación total del dispositivo para realizar una eliminación total. Cuando realiza una eliminación empresarial, el dispositivo elimina el perfil de trabajo y devuelve la propiedad del dispositivo al usuario. Los datos personales de los usuarios están intactos.
- No se admite el aprovisionamiento de productos en las inscripciones COPE.
- Cambios específicos en Android 11:
    - Las aplicaciones internas (alojadas en Workspace ONE UEM) ya no se pueden insertar en la parte personal del dispositivo. Las aplicaciones internas (tales como aplicaciones privadas) y las aplicaciones públicas deben implementarse solo en el perfil de trabajo.
        - Cualquier otra funcionalidad, como las reglas de conformidad que dependen de las aplicaciones internas, también dejará de ser compatible.
    - Ya no se admite el método de inscripción afw#hub.
        - Considere la posibilidad de usar el código QR o la inscripción automatizada en su lugar.
    - Si su organización requiere más tiempo para completar las pruebas, existen dos opciones para retrasar la actualización de los dispositivos a Android 11. Para obtener

información específica, consulte Cambios en el dispositivo corporativo habilitado personalmente (COPE) en Android 11.

Migración de Android heredado

Android (heredado), también conocido como Administrador de dispositivos, es el método heredado de inscripción de dispositivos Android con Workspace ONE UEM Console, ya que los modos de perfil de trabajo y administrado de trabajo de Android se introdujeron en Android 5.0. Los clientes que se inscriben en Workspace ONE UEM mediante la implementación de Android (heredado) pueden migrar a Android Enterprise para aprovechar la funcionalidad del dispositivo para la empresa.

Esta sección proporciona información y prácticas recomendadas sobre cómo pasar de la implementación de Android (heredado) a Android Enterprise.

Google dejó de utilizar ciertas API de administrador de dispositivos en favor de una actualización de la funcionalidad del dispositivo, ya que el administrador del dispositivo no es adecuado para admitir los requisitos actuales de la empresa. Los clientes de Workspace ONE UEM pueden adoptar los modos Administrado de trabajo (ideal para dispositivos de propiedad corporativa), Perfil de tarea (ideal para implementaciones de BYOD) y Dispositivo corporativo habilitado de forma personal (COPE) para administrar sus dispositivos Android mediante la migración de Android (heredado) a Android Enterprise.

Prácticas recomendadas para la migración de Android (heredado)

El momento de efectuar la migración a Android Enterprise queda al criterio de las necesidades de su negocio y el calendario de la migración real depende de los casos de uso de la organización. Estas son algunas consideraciones:

- Si es improbable que sus dispositivos actuales reciban Android 10 o si la organización controla las actualizaciones del sistema operativo, no es necesario migrar estos dispositivos. Puede implementar Android Enterprise para los dispositivos recién adquiridos.
- Los dispositivos BYOD son los más vulnerables, ya que es probable que los usuarios finales actualicen sus dispositivos al sistema operativo más reciente. Se puede lograr una migración de administrador de dispositivo a perfil de trabajo mediante la función de migración heredada de Android en Workspace ONE UEM Console.

Cómo migrar entre modos de dispositivo

Migración del modo administrado de trabajo

Los dispositivos Zebra que ejecutan Android 7 y versiones posteriores y MXMF 7 y versiones posteriores son compatibles con la migración de Android (heredado) al modo administrado de trabajo de Android Enterprise. Póngase en contacto con el servicio de asistencia de Zebra para recuperar un certificado para su empresa, que será necesario desde una perspectiva de seguridad

para garantizar la integridad de la migración. Los certificados suelen tener un ciclo de vida útil corto (de 30 a 90 días). El certificado debe tener un formato `.pem`.

Zebra puede solicitar la siguiente información para la generación de un certificado:

- Aplicación que realiza la migración: Zebra MX Service
- La aplicación se está migrando a Administrado de trabajo: Workspace ONE Intelligent Hub para Android
- Nombre del cliente

Los requisitos y funciones de migración desde este flujo incluyen:

- VMware Workspace ONE UEM 2006 o versión posterior
- Workspace ONE Intelligent Hub 20.05 para Android y Zebra MX Service 4.8 para Android.
- Si utiliza archivos APF para la inscripción o la actualización de Hub, deberá usar la versión de administrador del dispositivo (Android (heredado)), mostrado como DA, del archivo APF para la inscripción y la versión administrada de trabajo (Android Enterprise), mostrado como DO, para la actualización.
- La migración se realiza de forma remota y silenciosa.
- Las cuentas de Google no pueden estar presentes en el dispositivo, ya que esto podría provocar un error en la migración. Elimine todas las cuentas de Google antes de realizar la migración.
- Los dispositivos no se apagan, reinician ni restablecen durante la migración, lo que garantiza que los datos de las aplicaciones se mantengan intactos.
- La conectividad Wi-Fi se mantiene durante la migración.
- Los productos que no contienen perfiles permanecen instalados.
- La migración al modo AOSP/Red cerrada es totalmente compatible.
- Antes de la migración, revise la política de restricciones de la Play Store. Si la Play Store está bloqueada antes de la migración, los dispositivos se considerarán dispositivos administrados de trabajo en AOSP y no admitirán la administración de aplicaciones públicas. Si desea implementar aplicaciones desde la Play Store después de migrar a Administrado de trabajo, asegúrese de que la Play Store no esté bloqueada en los dispositivos inscritos heredados antes de la migración.

Registro de EMM para Android

Configure el registro de EMM para Android en su entorno para habilitar la inscripción y la migración de los dispositivos en Android Enterprise.

Elegibilidad de la migración

Dos nuevos atributos personalizados, `migration.do.eligible` y `migration.do.ineligibilityReason`, se notificarán a Console. Si `migration.do.eligible` tiene un valor "true", el dispositivo podrá realizar la migración. Console comprobará automáticamente este atributo antes de enviar un comando de migración al dispositivo. Si el valor es "false", compruebe `migration.do.ineligibilityReason` para obtener más información.

Migración de perfil de trabajo

Workspace ONE UEM Console proporciona un proceso sencillo que le ayuda a migrar todos los dispositivos de Android (heredado) a un Perfil de tarea de Android Enterprise. Las funciones de migración de la consola de UEM le ayudan a asegurarse de que:

- La administración heredada permanece intacta hasta que se complete la migración.
- Los dispositivos que no se migren nunca se verán afectados.
- Supervise cuáles son los dispositivos que están completos, en curso y asignados.
- Cree grupos inteligentes provisionales o de prueba para garantizar que los dispositivos de usuarios se migren correctamente antes de migrar toda la flota de dispositivos.

Migración de dispositivos corporativos

Puede migrar de Android (heredado) a Android Enterprise con los dispositivos de propiedad corporativa en los modos Administrado de trabajo o Dispositivo corporativo habilitado de forma personal (COPE). Las opciones de inscripción y migración varían en función del sistema operativo Android, del tipo de dispositivo y de si los dispositivos tienen acceso a los servicios de Google. Este escenario es el mejor para realizar la migración a dispositivos que no sean Android Zebra.

Las opciones de migración e inscripción son las siguientes:

- Use la inscripción totalmente administrada para dispositivos con Android 8.0 o posterior.
- Utilice la inscripción Knox Mobile para los dispositivos Samsung con Android 8.0 o posterior.
- Siga las estrategias de implementación progresiva de dispositivos y continúe utilizando sus dispositivos Android actuales inscritos a través de Android (heredado). Una estrategia de implementación progresiva de dispositivos significa que todas las implementaciones de dispositivos nuevas se inscriben automáticamente en Android Enterprise y se administran simultáneamente con implementaciones más antiguas (Android, heredado) hasta que la organización esté lista para traspasar todos los dispositivos a Android Enterprise.

Migración de Android sin Google Services

Si está inscrito en Workspace ONE UEM con dispositivos Android implementados a través de Android (heredado) y desea cambiar a Android Enterprise sin Google Services, ofrecemos compatibilidad con red cerrada para los dispositivos de propiedad corporativa e inscripción no administrada para dispositivos BYOD.

Si tiene un dispositivo que no tiene conectividad de red o si el dispositivo se puede conectar a una red pero no tiene Google Services (un dispositivo certificado sin GMS), puede inscribir estos dispositivos en Android Enterprise en el modo Administrado de trabajo e implementar aplicaciones internas y aplicar directivas con perfiles de Android.

Si tiene un dispositivo con conectividad de red pero que tiene restricciones para Google Services, por ejemplo, en el caso de dispositivos ubicados en China, puede usar la compatibilidad de red cerrada para los dispositivos corporativos. Para dispositivos BYOD, puede usar el modo único MAM basado en SDK denominado Modo registrado para habilitar la inscripción no administrada para dispositivos Android.

Migración en modo totalmente administrado mediante la

inscripción automatizada

El aprovisionamiento automático permite que los dispositivos Android se configuren de forma masiva con Workspace ONE UEM como proveedor EMM listo para usar sin tener que configurar manualmente cada dispositivo. El uso del aprovisionamiento automático con la migración de Android (heredado) le permite trasladar sus dispositivos al modo totalmente administrado con facilidad y garantizar que la migración se completa de forma segura.

1. Configure Workspace ONE UEM Console completando los requisitos previos para la migración en Android (heredado).
2. Complete el aprovisionamiento automático para que los dispositivos se agreguen al portal automatizado.
3. Pruebe y asegúrese de que el flujo de migración funciona con los dispositivos de prueba. Recuerde que se debe crear un perfil de Wi-Fi para que la migración se realice correctamente.
4. Envíe un comando "Eliminación total del dispositivo" a los dispositivos administrados anteriormente en Android (heredado).

Impacto en las API

Google dejó de utilizar ciertas API de administrador de dispositivos en favor de una actualización de la funcionalidad del dispositivo, ya que el administrador del dispositivo no es adecuado para admitir los requisitos actuales de la empresa. Las siguientes API disponibles con el administrador del dispositivo ya no funcionan en dispositivos que ejecuten Android 10 y versiones posteriores. El resto de dispositivos con Android 9.0 o versiones anteriores no se verán afectados:

- USES_POLICY_DISABLE_CAMERA
- USES_POLICY_DISABLE_KEYGUARD_FEATURES
- USES_POLICY_EXPIRE_PASSWORD
- USES_POLICY_LIMIT_PASSWORD

Preguntas más frecuentes sobre la migración en Android (heredado)

Para ayudarle a comprender mejor la migración en Android (Legacy), estas son algunas de las preguntas más frecuentes y las prácticas recomendadas para realizar una migración correcta.

- Al habilitar Android Enterprise en un grupo organizativo, ¿podría afectar a mis inscripciones de administrador en los dispositivos existentes?
    - Las inscripciones del administrador del dispositivo actual permanecerán inscritas y recibirán todos los perfiles y las aplicaciones asignados. Al habilitar Android Enterprise solo se verán afectadas las nuevas inscripciones. Cuando inscriba un nuevo dispositivo compatible con Android Enterprise, utilice Android Enterprise. Si un dispositivo no es compatible con Android Enterprise, se inscribirá mediante el administrador de dispositivos.
- ¿Pueden el administrador del dispositivo y Android Enterprise coexistir en la misma

UEM Console?

- Las inscripciones de los administradores de dispositivos y las inscripciones de Android Enterprise pueden coexistir en el mismo grupo de organización. La administración de perfiles se separa como Android y Android (heredado) para las inscripciones de los administradores de dispositivos y Android Enterprise, respectivamente.

  Además, con UEM Console v9.2.0 o posterior es posible reemplazar las inscripciones empresariales de Android en grupos de organización específicos, o incluso limitarla a grupos inteligentes específicos.

- ¿Puedo usar el aprovisionamiento de productos con Android Enterprise?
  - El aprovisionamiento de productos es compatible con dispositivos completamente administrados.
- ¿Hay capacidades de administración específicas de OEM disponibles en los dispositivos inscritos a través de Android Enterprise?
  - Las capacidades de administración específicas de OEM están disponibles a través de OEMConfig. Los OEM tales como Samsung y Zebra han creado aplicaciones públicas que se pueden agregar a la consola de Workspace ONE UEM. Estas aplicaciones proporcionan pares clave-valor de configuración de aplicaciones que pueden alterar las capacidades de los dispositivos.
- ¿Es compatible Workspace ONE Assist con Android Enterprise?
  - Workspace ONE Assist es compatible con todas las opciones de inscripción en Android Enterprise.
- ¿Pueden usar los clientes nuevos Android (heredado)?
  - Los clientes nuevos de Workspace ONE UEM deben configurar Android Enterprise para implementar dispositivos Android.
  - Los clientes existentes pueden deshabilitar y volver a habilitar Android (heredado) tal como deseen.

Ahora que ya conoce la migración de Android (heredado), puede continuar con los requisitos previos para comenzar la migración.

Requisitos previos para la migración a Android

Para proporcionar una experiencia de usuario final intuitiva para la migración, esta página le guiará a través de una migración correcta. Si no se completan estos pasos, podrían producirse errores en la migración o los usuarios no podrían acceder a todas las aplicaciones que necesiten.

Elegibilidad del dispositivo

El dispositivo debe ser apto para la migración. Por ejemplo. No se pueden migrar los dispositivos Samsung con el contenedor de Knox habilitado.

Para comprobar la idoneidad de la migración, vaya a Detalles del dispositivo > Atributos personalizados y haga que el atributo `sure migration.eligible` tenga el valor `True`.

Crear un grupo inteligente para migrar desde Android (heredado)

Antes de migrar, tendrá que crear grupos inteligentes para todos los dispositivos que se van a migrar. Puede crear grupos independientes para ensayar en una pequeña cantidad de dispositivos con fines de prueba antes de realizar la implementación en todos los dispositivos.

Workspace ONE UEM console proporciona un proceso sencillo que le ayuda a crear grupos inteligentes para migrar todos los dispositivos de Android (heredado) a la implementación de perfiles de trabajo de Android.

1. Seleccione el **grupo organizativo (GO)** que proceda, al que se aplicará el nuevo grupo inteligente y desde el que podrá administrarse. La selección de un GO es opcional.
2. Navegue a Grupos y ajustes > Grupos > Grupos de asignación y luego seleccione Agregar grupo inteligente
3. Introduzca el Nombre del grupo inteligente.
4. Configure el tipo de grupo inteligente:
    - Criterios: Esta opción funciona mejor con aquellos grupos con un mayor número de dispositivos (más de 500) que reciben actualizaciones generales. Este método funciona mejor porque los detalles heredados de estos grupos pueden llegar a todos los extremos de su flota móvil.
    - Dispositivos o usuarios: Esta opción funciona mejor con aquellos grupos con un menor número de dispositivos (500 o menos) que reciben actualizaciones importantes, pero esporádicas. Este método funciona mejor debido al nivel detallado al que puede seleccionar miembros del grupo. Aviso: Al cambiar entre los dos tipos de grupos inteligentes se borrarán las entradas y selecciones que haya realizado.

    Se debe seleccionar al menos un dispositivo implementado como Android (heredado) como apto para la migración o se producirán errores durante la configuración de la migración.
5. Seleccione Guardar.

Volver a crear perfiles para Android

Los perfiles de Android Enterprise son independientes de los perfiles de administrador de dispositivos o de Android (heredado). Debe volver a crear los perfiles para Android Enterprise. Estos perfiles están disponibles para la configuración después de completar el registro de Android Enterprise.

En las consolas UEM Console de versiones anteriores a la 9.4.0, los perfiles de Android Enterprise están disponibles en Dispositivos > Perfiles y recursos > Perfiles > Agregar > Agregar perfil > Android > Android for Work.

En las consolas UEM Console versión 9.4.0 y superiores, los perfiles de Android Enterprise están disponibles en Dispositivos > Perfiles y recursos > Perfiles > Agregar > Agregar perfil > Android.

Aviso: Si el perfil de Wi-Fi se configuró para la implementación de Android (heredado), debe crear y asignar un perfil de Wi-Fi de Android a los dispositivos seleccionados para la migración antes de poder crear una migración.

Los perfiles de dispositivos Android garantizan el uso adecuado de los dispositivos, la protección de los datos confidenciales y la funcionalidad del entorno de trabajo. Los perfiles sirven para distintos propósitos que van desde permitirle exigir reglas y procedimientos corporativos hasta adaptar y preparar los dispositivos Android para la forma en la que se utilizan.

Configurar la administración de aplicaciones

Una vez que se agrega una aplicación a Workspace ONE UEM Console, se puede distribuir al administrador del dispositivo, también denominado Android (heredado) y Android Enterprise. Si se ha agregado una aplicación pública a la consola de UEM antes del registro de Android Enterprise, la sección Administración de aplicaciones de esta guía le ayudará a configurar los ajustes para que no se interrumpan las asignaciones de aplicaciones existentes.

Las aplicaciones internas no pueden administrarse para el modo de administración de perfiles de trabajo en Android Enterprise. Para asegurarse de que las aplicaciones internas estén disponibles para los dispositivos que se han migrado al perfil de trabajo, debe cargar la aplicación en la consola de Google administrada como una aplicación privada antes de la migración.

Utilice Workspace ONE UEM para administrar la implementación y el mantenimiento de las aplicaciones móviles disponibles públicamente en la tienda Google Play. Asegúrese de que cada aplicación pública esté aprobada para su organización a fin de garantizar una migración sin problemas.

Aviso: Si va a migrar a dispositivos administrados de trabajo, revise la política de restricciones de la Play Store antes de la migración. Si la Play Store está bloqueada antes de la migración, los dispositivos se considerarán dispositivos administrados de trabajo en AOSP y no admitirán la administración de aplicaciones públicas. Si desea implementar aplicaciones desde la Play Store después de migrar a Administrado de trabajo, asegúrese de que la Play Store no esté bloqueada en los dispositivos inscritos heredados antes de la migración a Administrado de trabajo.

Administrar aplicaciones públicas para la migración de Android (heredado)

Si se ha agregado una aplicación pública a UEM Console antes de la migración de Android (heredado) y el registro de Android Enterprise, esta tarea le ayudará a asegurarse de que todas las aplicaciones se importen después de la migración.

Estos pasos simplemente garantizan que la consola de UEM sepa que la aplicación se ha aprobado en Google Play administrado. Ahora es posible asignar esta aplicación a inscripciones de Android Enterprise una vez finalizada la migración.

1. Navegue a https://play.google.com/work (inicie sesión con la misma cuenta de Gmail utilizada para configurar Android Enterprise), busque la aplicación apruébela para su organización.
2. En UEM Console, desplácese a Aplicaciones y libros > Nativas > Públicas > Agregar aplicación > Android > Importar desde Play.
3. Seleccione Importar cuando se muestre la lista de aplicaciones aprobadas.

   Tras la migración, la memoria caché de la aplicación se borra y los usuarios tendrán que volver a introducir las credenciales.

Verificar los ajustes de red

Los requisitos de red para Android son una lista de endpoints conocidos para las versiones actuales y anteriores de las API de administración empresarial. Compruebe los ajustes de red para asegurarse de que hay conexión entre Workspace ONE, la tienda Google Play y los dispositivos Android.

Una vez que haya llevado a cabo los requisitos previos, estará preparado para continuar con la migración con el modo de dispositivo deseado.

Migración desde Android (heredado) mediante la herramienta de migración

Workspace ONE UEM Console proporciona una herramienta de migración que le permite completar todos los requisitos previos, seleccionar grupos inteligentes, configurar un mensaje personalizado para sus usuarios y acceder a un panel donde ver una página de resumen de los dispositivos migrados, incluidos el estado de idoneidad y detalles de la ejecución correcta o con errores.

Asegúrese de haber completado las condiciones previas para evitar una migración con errores o que los usuarios no puedan acceder a todas las aplicaciones que necesiten.

1. Vaya a Dispositivos > Ciclo de vida > Migración de Android heredado y seleccione Nueva migración.
2. Seleccione el modo deseado en la ventana Seleccionar tipo de migración.
3. Complete las condiciones previas y seleccione Siguiente para pasar a la pestaña Detalles.

Detalles	La pestaña Detalles le permite seleccionar los grupos inteligentes que desea migrar.
Nombre	Introduzca un nombre descriptivo para el grupo de migración.
Descripción	Introduzca una descripción detallada del grupo de migración.
Grupos inteligentes	Especifique los grupos inteligentes que recibirán la migración. Los grupos inteligentes deben incluir implementaciones de Android (heredado). Recibirá un mensaje de error si un grupo inteligente no es apto para ser incluido en la migración.
Mensaje	Después de que los usuarios hayan elegido actualizar a Android Enterprise, este mensaje les informará sobre la migración y les pedirá que realicen acciones para continuar.

4. Seleccione Validar. Al seleccionar Validar, se recupera el número de dispositivos aptos para la migración.
5. Seleccione Continuar una vez que se validen todos los dispositivos para la migración. No podrá continuar hasta que se seleccione un grupo inteligente válido.

   Se muestra una página de Resumen que muestra detalles tales como la lista de dispositivos, la idoneidad de la migración y el motivo por el cual el dispositivo no cumple los requisitos, cuando proceda
6. Seleccione Crear para crear la migración.

   Se envía una notificación a los dispositivos aptos en los grupos inteligentes seleccionados que informan a los usuarios sobre la migración y que les solicitan que realicen las acciones

necesarias para continuar. Puede supervisar el progreso en la página Migración de Android heredado. Desde esta página, puede seleccionar las migraciones de la vista de lista para mostrar la página Detalles de la migración.

Aviso: Durante la migración de Android (heredado) a Android Enterprise, en función de la configuración del programador, el comando de migración se envía automáticamente para el primer tamaño de lote (300) de dispositivos de forma instantánea. Después de los primeros 300 dispositivos, el resto de los dispositivos recibirán el comando a los intervalos determinados. Puede ver la configuración de la consola de UEM en Administrador > Programador.

Consulte la página de detalles de la migración para obtener más información

Página de detalles de la migración

Las páginas de Detalles de la migración permiten realizar un seguimiento de la migración por grupo de migración, detalles, estado y vista de lista de los dispositivos incluidos en la migración.

Vista de lista de la migración de Android heredado

La Vista de lista de la migración de Android heredado se muestra automáticamente después de crear una nueva página de migración. La vista de lista le ayuda a ver todas las actualizaciones en tiempo real de los dispositivos de usuario final que va a migrar con Workspace ONE UEM console. La vista de lista le permite:

- Editar migraciones específicas; para ello, seleccione el botón de opción en el nombre descriptivo de la migración que desee. Puede actualizar la migración de nuevos dispositivos agregados al grupo inteligente mediante Editar.
- Retire la notificación persistente para eliminar los grupos de migración que evitan que los dispositivos en cola se migren desde un dispositivo de Android heredado. El perfil de Android Work no se elimina de los dispositivos que ya se han migrado.
- Busque y delimite un dispositivo mediante la opción de búsqueda.

Página de detalles de la migración de Android heredado

Para acceder a la página Detalles de la migración, seleccione un nombre descriptivo de migración de la Vista de lista de la migración de Android heredad con Workspace ONE UEM console para revisar el estado de la migración. Puede ver un resumen gráfico, el estado y los motivos de la ejecución correcta o incorrecta de la migración.

Utilice la página Detalles de la migración para insertar el comando de migración en el dispositivo con el botón Volver a intentar si se produce un error en la migración.

Personalice un mensaje para los dispositivos en el lote de migración con el botón Notificar. Configure el campo como sigue:

- Tipo de mensaje: Seleccione el tipo de mensaje (correo electrónico, SMS o inserción) que Workspace ONE UEM utiliza para esta plantilla.
- Asunto: Introduzca el asunto del mensaje.
- Cuerpo del mensaje: Escriba el mensaje que Workspace ONE UEM muestra en los

dispositivos de los usuarios finales para cada tipo de mensaje.

Cómo registrar Android con Workspace ONE UEM

Para empezar a administrar los dispositivos Android, deberá registrar Workspace ONE UEM como su proveedor de administración de movilidad empresarial (EMM) con Google. La página de Primeros pasos de Workspace ONE UEM console proporciona una solución paso a paso para ayudar a configurar las herramientas de administración empresarial necesarias para proteger y administrar su flota de dispositivos.

Hay dos formas de configurar Android: mediante una cuenta de Google Play administrada (opción preferida) o mediante un dominio de Google administrado (recomendado por Google para los clientes de G Suite). Si su empresa no utiliza G Suite y permite varias configuraciones de Android dentro de la organización mediante una cuenta de Google personal, se utiliza una cuenta de Google Play administrada. Workspace ONE UEM administra esta cuenta y no requiere ninguna sincronización de directorio activo ni la verificación de Google.

Para configurar Android con un dominio de Google administrado (G Suite) es necesario que su empresa configure un dominio de Google, y deberá seguir un proceso de verificación para demostrar que el dominio es de su propiedad. Este dominio solo puede vincularse a una cuenta de EMM verificada. La instalación incluye la creación de una cuenta de servicio de Google y la configuración de Workspace ONE UEM como su proveedor de EMM. Considere la opción de crear una cuenta de Google específicamente para Android para su organización, de modo que al utilizarla no entre en conflicto con ninguna cuenta de Google existente.

Importante: Cuando se crea una cuenta de Google para el dominio de Google administrado, se considerará la cuenta de administrador para el dominio. Considere la posibilidad de agregar más usuarios (cuentas de Google) para ayudarle a administrar tareas en la Google Play administrada. Puede ser útil agregar más cuentas de Google en caso de que la cuenta principal de Google quede inactiva. Si esto ocurre, podrá seguir accediendo al dominio de Google administrado y evitar comportamientos no deseados. Además, no elimine la cuenta de administrador de Google ni el EnterpriseID asociado al registro de EMM de Android. La eliminación puede provocar errores en el registro de EMM de Android.

Puede crear y asignar funciones para el dominio de Google administrado. Consulte Asignar funciones en Enterprise.

La cuenta de servicio de Google es una cuenta de Google especial que utilizan las aplicaciones para acceder a las API de Google, y es necesaria a la hora de configurar Android con el método de dominio de Google administrado para su empresa. Las credenciales de la cuenta de servicio de Google se rellenan automáticamente a la hora de configurar cuentas de Android al registrarse utilizando una cuenta de Google Play administrada. Si se produce un error al configurar las cuentas de Android, borre la configuración en Workspace ONE UEM console y vuelva a intentarlo o cree la cuenta de forma manual. En las cuentas de Google, considere la posibilidad de crear la cuenta de servicio de Google antes de cualquier método de instalación.

Para cambiar la cuenta de Google o realizar cambios en la configuración de administración, debe desenlazar la cuenta desde Workspace ONE UEM console.

Importante: La configuración de Android incluye la integración con herramientas de terceros que no están administradas por VMware. La información que aparece en esta guía para la consola de administración de Google y la consola de desarrolladores de Google se ha documentado con la versión disponible a fecha de enero de 2018. No se garantiza la integración con productos de terceros, y la implementación depende del funcionamiento correcto de dichas soluciones de terceros.

RCómo registrar EMM de Android con la cuenta de Google Play gestionada

Workspace ONE UEM console le permite completar un proceso de configuración simplificada para enlazar la consola de UEM a Google como su proveedor de EMM.

Requisitos previos

Si la página de registro de EMM de Android está bloqueada, asegúrese de haber habilitado las direcciones URL de Google en su arquitectura de red para comunicarse con endpoints internos y externos.

Procedimiento

1. Desplácese a Introducción > Workspace ONE > Registro de EMM de Android.
2. Seleccione Configurar y se le redirigirá a la página de registro de EMM de Android.
3. Seleccione Registrar con Google. Si ya ha iniciado sesión con sus credenciales de Google, se le redirigirá a la página "Comenzar" de Google.

   Si su organización utiliza más de un dominio, tendrá que registrar dominios independientes.
4. Seleccione Inicio de sesión, si no la ha iniciado aún, escriba sus credenciales de Google y, a continuación, seleccione Comenzar.
5. Introduzca el Nombre de la organización. El campo de proveedor de administración de movilidad empresarial (EMM) se rellena automáticamente como VMware Workspace ONE UEM.
6. Seleccione Confirmar > Completar registro. Se le redirige a Workspace ONE Console y se rellenan automáticamente sus credenciales de cuenta de servicio de Google.
7. Seleccione Guardar > Probar conexión para asegurarse de que la cuenta de servicio está configurada y conectada correctamente.

Si se ha borrado su configuración en la consola de UEM, cuando navegue para registrarse en Google verá un mensaje donde se le solicita que complete la instalación. Se le redirigirá de nuevo a Workspace ONE UEM Console para finalizar la instalación.

Cómo registrar EMM de Android con un dominio de Google gestionado (clientes de G-Suite)

Para configurar su cuenta con el dominio de Google administrado es necesario que la organización

configure un dominio de Google si no utiliza uno todavía. Deberá llevar a cabo varias tareas manuales, como comprobar la propiedad del dominio en Google, obtener un token de EMM y crear una cuenta de servicio de empresa para utilizar este tipo de instalación.

1. Desplácese a Introducción > Workspace ONE > Registro de EMM de Android.
2. Seleccione Registrar y se le redirigirá al Asistente de instalación de Android para llevar a cabo tres pasos:
    1. Generar token: Para obtener el token empresarial, registre su dominio empresarial en Google.
    2. Cargar token: Introduzca el Token de EMM en el Asistente de configuración de Android.
    3. Configurar usuarios: Configure cómo se van a crear los usuarios para toda la empresa.
3. Seleccione Ir a Google. Se le redirige al sitio de G Suite.
4. Registre su empresa y compruebe el dominio.

Configuración de cuenta de servicio de Google

La cuenta de servicio de Google es una cuenta de Google especial que utilizan las aplicaciones para acceder a las API de Google. Debe crear esta cuenta después de generar el token de EMM para poder cargar toda la información a la vez.

1. Vaya a la Google Cloud Platform - consola de los desarrolladores de Google .
2. Inicie sesión con sus credenciales de Google.

    Las credenciales de administrador de Google no tienen que estar asociadas a su dominio empresarial. Considere la opción de crear una cuenta de Google específicamente para Android para su organización, de modo que al utilizarla no entre en conflicto con ninguna cuenta de Google existente.

    Aviso: Considere la posibilidad de agregar más cuentas para que, si una cuenta queda inactiva, disponga de cuentas adicionales para iniciar sesión y acceder a su cuenta de servicio de Google.
3. Utilice el menú desplegable del menú Seleccionar un proyecto y seleccione Nuevo proyecto.
4. Introduzca un Nombre de proyecto para crear un proyecto de API en la ventana Nuevo proyecto. Considere el uso de EMM Android-NombreCompañía como convención de nomenclatura.
5. Acepte los términos y condiciones y seleccione Crear.

    El proyecto se genera y la consola de los desarrolladores de Google le redirige a la página Administrador de API.
6. Seleccione Habilitar API y servicios para Android desde el Panel de control de servicios y API.
7. Busque y habilite las siguientes API: API de EMM de Google Play y SDK de administrador.

    Después de crear su proyecto y habilitar las API, cree su cuenta de servicio en la consola de

desarrolladores de Google.

8. Desplácese a API y servicios > Credenciales > Crear credenciales > Clave de cuenta de servicio > Nueva cuenta de servicio.
9. Defina el Nombre de cuenta de servicio para su cuenta de servicio. Considere la opción de seguir la convención de nomenclatura de Android y asegúrese de anotar el nombre que elija, ya que lo necesitará en pasos siguientes.
10. Utilice el menú desplegable para seleccionar Función > Proyecto como Propietario.
11. Seleccione el Tipo de clave como P12.
12. Seleccione Crear. El certificado de identidad se genera automáticamente y se descarga en la unidad local. Asegúrese de guardar el certificado de identidad y la contraseña para cuando se cargue el certificado en Workspace ONE UEM console.
13. Seleccione Administrar cuentas de servicio de la lista Claves de cuenta de servicio que abre la página Cuentas de servicio.
14. Seleccione el botón de menú (tres puntos verticales) situado junto a su cuenta de servicio y seleccione Editar.
15. Seleccione Habilitar delegación en todo el dominio de G Suite.
16. Introduzca un Nombre de producto para cambiar la configuración del dominio de G Suite. Considere el uso de EMMAndroid-NombreCompañía como convención de nomenclatura.
17. Seleccione Guardar.
18. Seleccione ID de View Client en el campo Delegación en todo el dominio. Se muestran los detalles de su cuenta de servicio. Desde aquí, abandonará la consola de desarrolladores y deberá introducir sus credenciales en la consola de administración de Google.

    No olvide guardar su ID de cliente antes de salir de la consola de desarrolladores. También utilizará estas credenciales en Workspace ONE UEM console al cargar el token de EMM.

Configuración de la consola de administración de Google

La consola de administración de Google es la herramienta que utilizan los administradores para administrar los servicios de Google para los usuarios de una organización. Workspace ONE UEM utiliza la consola de administración de Google para la integración con Android y Chrome OS.

La página de Administrar el acceso del cliente de API le permite controlar el acceso de la aplicación interna personalizada y la aplicación de terceros a las API de Google compatibles (ámbitos).

1. Inicie sesión en la consola de administración de Google y desplácese hasta Seguridad > Ajustes avanzados > Administrar el acceso de cliente de API.
2. Rellene los siguientes datos:

Ajustes	Descripción
Nombre del cliente	Introduzca el ID de cliente generado al crear la cuenta de servicio de Google
Uno o más ámbitos de API	Copie y pegue los siguientes ámbitos de API de Google para Android: https://www.googleapis.com/auth/admin.directory.user

3. Seleccione Autorizar.

Generar Token de EMM

El token único de EMM vincula su dominio para la administración de Android al Workspace ONE UEM activado mediante AirWatch. Se le dirige al sitio de configuración de G Suite después de seleccionar Ir a Google desde la tarea anterior para comenzar.

Los pasos que se describen en la tarea son para generar un token de EMM para un dominio nuevo. La tarea para generar el token de EMM es diferente en función de si se registra con un dominio nuevo o existente.

Si va a generar un token para un dominio existente, simplemente desplácese a Seguridad > Proveedor de EMM administrado para Androidy seleccione Generar token de EMM, continúe después con el paso 5.

1. Rellene los siguientes campos:
    1. Acerca de usted: introduzca la información de contacto del administrador.
    2. Acerca de su empresa: rellene la información de su compañía.
    3. Su cuenta de administrador de Google: cree una cuenta de administrador de Google.
    4. Finalizar: introduzca los datos de comprobación de seguridad.
2. Seleccione Aceptar y crear su cuenta después de leer y aceptar los términos establecidos por Google.
3. Siga las indicaciones restantes para Comprobar la propiedad del dominio y Conectar con su proveedor. Una vez comprobado, esto se convierte en su dominio de Google administrado.

    Para comprobar la propiedad del dominio, están disponibles las siguientes opciones: agregar una etiqueta meta a la página de inicio, agregar un registro de host del dominio, o bien cargar un archivo HTML al sitio del dominio. Configure los ajustes para las opciones disponibles.
4. Seleccione Comprobar para continuar. Si este proceso se realiza correctamente, en la sección Conectar con su proveedor aparece su token de EMM. Este token tiene una validez de 30 días. Si tiene problemas durante este paso, consulte con el soporte de Google a través del número de soporte y el PIN único que se indica.
5. Copie el token de EMM generado y seleccione Finalizar.

Workspace ONE UEM recomienda crear la cuenta de servicio de Google antes de volver a Workspace ONE UEM Console para cargar el token de EMM, de modo que pueda cargar todas las credenciales al mismo tiempo.

Generar token de EMM para el dominio existente

El token único de EMM vincula su dominio para la administración de Android al Workspace ONE UEM activado mediante AirWatch. En el caso del dominio existente, se le dirige a la consola de administración de Google para generar el token de EMM. Los pasos que se describen en la tarea son para generar un token de EMM para un dominio existente. La tarea para generar el token de

EMM es diferente en función de si se registra con un dominio nuevo o existente. Para obtener información sobre la generación de un token de EMM para un nuevo dominio, consulte Generar token de EMM. Inicie sesión en la consola de administración de Google con las credenciales de administrador de Google. Desplácese a Seguridad > Proveedor de EMM administrado para Android y seleccione Generar token de EMM. Copie y pegue el token en Workspace ONE UEM Console.

Los pasos que se describen en la tarea son para generar un token de EMM para un dominio existente. La tarea para generar el token de EMM es diferente en función de si se registra con un dominio nuevo o existente.

1. Inicie sesión en la consola de administración de Google con las credenciales de administrador de Google.
2. Navegue a Seguridad > Administrar proveedor de EMM de Android y seleccione Generar token de EMM.
3. Copie y pegue el token en Workspace ONE UEM Console.

Cargar el Token de EMM

Introduzca la información que ha obtenido de Google durante el registro. Esto incluye el dominio registrado, el token de empresa y la dirección de correo electrónico de administrador de Google que haya creado.

También puede obtener el token de empresa si inicia sesión en https://admin.google.com con su dirección de correo electrónico de administrador de Google en Seguridad→Administrar proveedor de EMM de Android.

1. Desplácese a Introducción > Workspace ONE > Registro de EMM de Android. Si ha cerrado la ventana o no se le redirecciona automáticamente a Workspace ONE UEM.
2. Seleccione Registrar y se le redirigirá al asistente de configuración de Android.
3. Seleccione Cargar Token en el asistente de configuración de Android.

   Esto también se conoce como el token de empresa.
4. Rellene los siguientes campos:

Ajustes	Descripción
Dominio	Dominio reclamado para habilitar Android asociado con su empresa.Importante: Si su dominio ya se ha registrado con otro proveedor de EMM, no podrá cargar un nuevo token de EMM.
Token de empresa de EMM	Token generado en la consola de administración de Google.
Correo electrónico del administrador de Google	Se trata de la cuenta de administrador que se usa para el registro de dominios, la consola para desarrolladores de Google y la consola de administración de Google.
ID de cliente	ID de cliente generado al crear la cuenta de servicio de Google. Este ID se recupera a partir de los Ajustes de la consola para desarrolladores de Google.
Dirección de correo electrónico de la cuenta de Google Service	Correo electrónico generado a partir de la creación de la cuenta de servicio de Google. Este ID se recupera a partir de los Ajustes de la consola para desarrolladores de Google.

Ajustes	Descripción
ID de certificado	Cargue el certificado P12 creado al generar la cuenta de servicio de Google. Requiere una contraseña. Este ID se recupera a partir de los Ajustes de la consola para desarrolladores de Google.

5. Seleccione Siguiente para configurar usuarios.

Configurar usuarios

Todos los usuarios en su empresa que utilicen Android necesitarán cuentas de Google creadas para conectarse con sus dispositivos. Este último paso en el asistente de registro de EMM de Android le permite determinar qué método de instalación prefiere para crear usuarios.

Los administradores tienen dos opciones para crear usuarios en Android:

- Permitir que Workspace ONE UEM cree automáticamente las cuentas de Google durante la inscripción.
- Crear usuarios de forma manual iniciando sesión en la consola de administración de Google, o bien utilizando la herramienta de sincronización de directorio activo de Google (GADS).

El formato para el nombre de usuario es nombredeusuario@ <su_dominiode_empresa>.com.

1. Habilitar una de las siguientes opciones para determinar cómo se configuran los usuarios:
    - Crear una cuenta de Google durante la inscripción basada en la dirección de correo electrónico del usuario inscrito.
    - Usar SAML para habilitar la autenticación SAML en el proceso de inscripción.
    - Usar SAML para la autenticación de la cuenta de Google. Para utilizar este método, configure el inicio de sesión único navegando hasta Seguridad > Inicio de sesión único en la consola de administración de Google. Si no se habilita la creación automática de usuarios con uno de los métodos anteriores, Workspace ONE UEM Console le dirigirá al método alternativo de creación de cuentas de Google mediante la herramienta Google Active Directory Sync o la consola de administración de Google.
2. Utilice la opción Probar conexión, que comprueba si la comunicación es correcta con Google.
    - Acceso a la API de Play: Valida que la API del EMM de Google esté habilitada y que se pueden instalar las aplicaciones.
    - Acceso a la API de directorio: Valida que la API del SDK de administración está habilitada y que el ámbito de https://www.googleapis.com/auth/admin.directory.user está autorizado en la consola de administración de Google.
3. Seleccione Guardar.

Creación de usuarios de inscripción de Android

VMware le sugiere que cree usuarios para Android automáticamente durante la inscripción. El asistente de configuración de Android le permite especificar si desea crear automáticamente las cuentas de usuario durante la inscripción y, si es así, utilizar SAML para autenticar las cuentas. Si no

ha configurado SAML anteriormente, el asistente mostrará un vínculo que le dirige para configurar sus ajustes.

Creación de usuarios de forma automática

1. Seleccione Sí para Crear cuentas de Google durante la inscripción basadas en los correos electrónicos de los usuarios inscritos.
2. Seleccione Sí para Usar extremo de SAML para autenticar cuentas.

   Si no ha configurado SAML, el asistente le pedirá que configure la autenticación de SAML.
3. Seleccione Sí para Usar SAML para la autenticación de la cuenta de Google que requiere que configure el inicio de sesión único en la consola de administración de Google.
4. Seleccione Guardar para completar la instalación de Android.

Creación de usuarios de forma manual

Puede crear manualmente cuentas de usuario para toda la empresa fuera de Workspace ONE UEM console mediante la herramienta de sincronización de directorio de nube de Google (GCDS) o la consola de administración de Google. Para acceder a la consola de administración de Google, puede hacer clic en el vínculo incluido en el asistente de configuración. Deberá ponerse en contacto con Google para obtener más instrucciones para el uso de la consola.

El método GCDS requiere que use una configuración similar a la de los servicios de directorio de AirWatch. Acceda a la configuración de los servicios de directorio navegando hasta Grupos y ajustes ► Todos los ajustes ► Sistema ► Integración empresarial ► Servicios de directorio.

Puede acceder a la herramienta GCDS haciendo clic en el vínculo publicado en el asistente de configuración o bien descargando la herramienta directamente en el equipo desde la página de Soporte de Google .

La herramienta GDCS le permite crear manualmente cuentas de Google para cada empleado de su empresa mediante una sola tarea de creación en masa. Las cuentas se crean mediante la sincronización con la información almacenada desde VMware Workspace ONE Directory Services.

Aviso: La información que se proporciona en el presente documento está actualizada a fecha de la versión más reciente de GCDS v.4.4.0, de marzo de 2017.

1. Seleccione el vínculo en el asistente de configuración o descargue la herramienta GDCS directamente desde Google.
2. Abra la herramienta desde su escritorio y seleccione las Cuentas de usuario y los Grupos que desea sincronizar.
3. Seleccione la pestaña Configuración de dominio de Google e introduzca lo siguiente:
   1. Introduzca el Nombre de dominio principal.
   2. Seleccione esta opción para Reemplazar los nombres de dominio en la dirección de correo electrónico LDAP (de usuarios y grupos) por este nombre de dominio. Así se asegurará de que todas las direcciones de correo electrónico del usuario coincidan con el nombre de dominio.
4. Seleccione el botón Autorizar ahora.
5. Siga los pasos para continuar el proceso de autorización cuando aparezca el cuadro de

diálogo Autorizar sincronización del directorio de aplicaciones de Google.

1. Inicie sesión en su cuenta de administrador de Android.
2. Introduzca la verificación recibida por correo electrónico.
3. Seleccione Validar para confirmar estos ajustes.

6. Seleccione la pestaña Configuración de LDAP para especificar la configuración de conexión para sincronizar los servicios de directorio de AirWatch con Google. Desde aquí, puede introducir la misma configuración guardada en los servicios de directorio de AirWatch para sincronizarla con esta herramienta. Para acceder a estos ajustes, navegue a Grupos y ajustes ► Todos los ajustes ► Sistema ► Integración empresarial ► Servicios de directorio.
7. Seleccione Probar conexión. Si la sincronización se realiza correctamente, se crearán automáticamente las cuentas de directorio activo vinculadas y las cuentas de Google corporativas en Google.

   Se le dirigirá de nuevo al asistente de configuración para finalizar la instalación.

Cómo desenlazar el dominio de Workspace ONE UEM

Puede desenlazar la cuenta de administrador de Android en Workspace ONE UEM console en caso de que necesite realizar un cambio o modificar las cuentas de Google.

1. Desplácese a Dispositivos > Ajustes del dispositivo > Dispositivos y usuarios > Android > Registro de EMM de Android
2. Seleccione Borrar configuración de la página de registro de EMM de Android.

Resumen de la inscripción de dispositivos Android

Cada dispositivo Android implementado en su organización debe estar inscrito para poder comunicarse con Workspace ONE UEM Console y tener acceso al contenido y las funciones internas.

Workspace ONE Intelligent Hub proporciona un recurso único para inscribir el dispositivo y proporciona también los detalles del dispositivo y la conexión. La inscripción con el Hub le permite:

- Autenticar usuarios por medio de servicios básicos o de directorio, tales como AD/LDAP/Domino, SAML, tokens o proxy.
- Registrar dispositivos en masa o permitir que los usuarios se registren automáticamente.
- Definir versiones y modelos de SO aprobados y el número máximo de dispositivos permitidos para cada usuario.
- Autentique la inscripción mediante Workspace ONE Access durante la inscripción automática.

Dispositivos y usuarios/Android/Registro de EMM de Android

La página de registro de EMM de Android le permite configurar las diversas opciones para la inscripción con Android. Esta página usa un asistente que le ayudará a configurar la integración de los dispositivos. Si es la primera vez que utiliza el registro de EMM de Android, consulte la página Registrar Android con Workspace ONE UEM para configurar los ajustes.

Automatizado

La inscripción automatizada permite configurar dispositivos que ejecutan Android con Workspace ONE UEM como proveedor de administración de movilidad empresarial desde el primer momento.

Si el dispositivo está conectado a Internet durante la configuración del dispositivo, se descarga automáticamente Workspace ONE Intelligent Hub y se pasan automáticamente los detalles de la inscripción para inscribir el dispositivo sin la interacción del usuario. Puede utilizar esta página en el registro de EMM de Android para configurar los ajustes predeterminados de los nuevos dispositivos agregados a las cuentas automatizadas vinculadas.

Ajustes	Descripción

Especificar grupo organizativo	Habilite esta opción para seleccionar un grupo organizativo específico. Cuando esta opción no está activada, los ajustes se aplican a todos los grupos.
DPC adicionales	Utilice los campos Clave de configuración y Valor de configuración para incluir marcas de inscripción adicionales. Para obtener información sobre las marcas, consulte Indicadores de inscripción adicionales admitidos para la inscripción de Android.

Para realizar la inscripción automatizada, consulte Inscribir dispositivos Android mediante el portal automatizado.

Ajustes de inscripción

Ajustes	Descripción
Modo de administración para dispositivos corporativos	Elija si los dispositivos deben asociarse como Administrado de trabajo o Corporativo habilitado de forma personal.
	Si está trabajando en una red cerrada o no puede comunicarse con Google Play, seleccione AOSP/Red cerrada. No se crea una cuenta de Google en estos dispositivos. La administración de aplicaciones públicas mediante Google Play administrado no está disponible mediante el uso de la inscripción con AOSP/Red cerrada. Esta opción solo se aplicará a los dispositivos inscritos con ese grupo organizativo. La organización principal puede aún tener dispositivos en la inscripción de trabajo administrado mediante una cuenta de Google.
	En algunos casos, es posible que desee inscribir dispositivos GMS y no GMS en el mismo grupo organizativo sin tener que crear varios grupos organizativos para la administración de dispositivos. Si utiliza la inscripción de código QR para estos dispositivos, puede configurar el asistente de configuración de inscripción para forzar la inscripción de AOSP o red cerrada, independientemente del tipo de inscripción establecido en este campo.
	Si se selecciona Basado en dispositivo, solo se deben utilizar cuentas basadas en dispositivos, lo que se aplica a COPE en Android 8.0. Dispositivos Android 10 y Android 11. Esto resulta útil para la inscripción provisional y escenarios de un solo uso, tales como dispositivos de quiosco.
Generación de cuentas de Google para dispositivos corporativos	Seleccione cómo se crearán sus cuentas de Google. Este campo es solo para cuentas de Google administradas y no para cuentas de Google Workspace o G Suite.
Mensaje de usuario sobre la eliminación empresarial de perfil de trabajo	Personalice un mensaje de aviso que se muestre en los dispositivos de los usuarios cuando realice una eliminación empresarial desde la consola de UEM. Al realizar una eliminación empresarial desde la página Detalles del dispositivo, también se genera el mensaje. El usuario no necesita realizar ninguna acción en su dispositivo. El mensaje se mostrará al finalizar la eliminación empresarial.

Restricciones de inscripción

Ajustes	Descripción
Defina el método de inscripción para este grupo organizativo	Seleccione si desea Usar siempre Android o Usar siempre Android (heredado), Definir grupo de asignación que utiliza Android.
	Si selecciona Definir grupo de asignación que utiliza Android, todos los dispositivos sin asignar utilizarán Android (heredado) de forma predeterminada.
Grupos de asignación	Seleccione un grupo inteligente del menú desplegable.
	Cuando se selecciona un grupo inteligente, los dispositivos o usuarios que no pertenezcan a esos grupos tendrán que realizar una inscripción en Android heredado (administrador del dispositivo). Los dispositivos que pertenecen al grupo inteligente se inscribirán en el Perfil de trabajo o en Dispositivo administrado de trabajo, suponiendo que sean compatibles con estos modos de inscripción.
Permitir inscripción de perfil de trabajo	Utilice este ajuste para impedir que los dispositivos que son propiedad de los empleados se inscriban en el modo de perfil de trabajo.

Protección de dispositivo para dispositivos Android

Android OS 5.1 y las versiones posteriores cuentan con una función denominada Protección del dispositivo que requiere la introducción de credenciales de Google antes y después del restablecimiento de un dispositivo. Cuando un dispositivo está listo para ser inscrito como dispositivo administrado de trabajo para Android, el dispositivo debe ser un restablecimiento de fábrica.

Es necesario eliminar del dispositivo todas las cuentas de Google existentes y deshabilitar la pantalla de bloqueo seguro para evitar activar la Protección de dispositivo y permitir la instalación de Workspace ONE Intelligent Hub durante la inscripción. Utilizar el dispositivo desde el estado de restablecimiento de fábrica también impide que se bloquee al nuevo usuario en el dispositivo.

Si el propietario anterior había cambiado la contraseña de la cuenta de Google, deberá esperar tres días antes de realizar el restablecimiento de fábrica de cualquiera de sus dispositivos Android 5.1 o posterior para la inscripción, a menos que haya deshabilitado explícitamente la Protección de dispositivo de Android en los mismos. Si realiza el restablecimiento de fábrica de uno de los dispositivos Android antes de que pasen esos tres días y trata de iniciar sesión en ese dispositivo con su cuenta de Google, le aparecerá un mensaje de error y no podrá acceder al dispositivo con ninguna cuenta hasta que pasen 72 horas desde el cambio de contraseña.

Habilitar la inscripción sin administrar para dispositivos Android

Para permitir que algunos dispositivos Android se inscriban en Workspace ONE UEM sin los servicios de Google, debe habilitar el modo registrado

Los dispositivos inscritos a través de la aplicación Intelligent Hub se administran a través de MDM de forma predeterminada. Con el objeto de permitir que algunos dispositivos Android se inscriban sin

ser administrados a través de MDM, debe habilitar el modo no administrado para un grupo inteligente.

Los criterios de selección disponibles son la versión del SO, el tipo de propiedad y el grupo de usuarios.

En la inscripción sin administrar, los usuarios pueden acceder a las aplicaciones que requieren un nivel básico de seguridad. Cuando los usuarios intentan acceder a una aplicación que requiere administración, los usuarios son guiados a través del proceso de inscripción de MDM. Las directivas de la aplicación de administración adaptativa se utilizan para controlar los niveles de administración de dispositivos para dispositivos Android inscritos sin administración.

1. En Workspace ONE UEM Console, seleccione el grupo organizativo que desea habilitar con la inscripción sin administrar y desplácese a la página Dispositivos > Ajustes del dispositivo > Dispositivos y usuarios > General > Inscripción > Modo de administración.
2. En Ajustes actuales, haga clic en Anular.
3. Para Android, seleccione Habilitado.
4. En Grupos inteligentes, agregue el grupo inteligente que está habilitado para las inscripciones sin administrar.
5. Haga clic en Guardar.

Los usuarios con dispositivos Android del grupo inteligente configurado tienen derechos de acceso sin administrar a las aplicaciones. Los usuarios pueden utilizar la aplicación Workspace ONE Intelligent Hub para acceder a las aplicaciones que requieren un nivel básico de seguridad sin que el dispositivo se inscriba en la administración de dispositivos móviles de Workspace ONE UEM.

Inscripción por detección automática

Workspace ONE UEM con tecnología AirWatch facilita el proceso de inscripción mediante el uso de un sistema de detección automática para inscribir dispositivos en entornos y grupos organizativos (GO). También puede utilizar la detección automática para permitir que los usuarios finales se autentiquen en el Portal de autoservicio (SSP).

Aviso: Para habilitar la detección automática en los entornos de la sede, debe asegurarse de que los entornos puedan comunicarse con los servidores de detección automática de Workspace ONE UEM.

Registro de la inscripción por detección automática

El servidor verifica la singularidad del dominio del correo electrónico y permite que solamente se registre un dominio en un grupo organizativo en un entorno. Debido a esta comprobación del servidor, debe registrar el dominio en el grupo organizativo del nivel principal.

El sistema de detección automática se configura automáticamente para los nuevos clientes de software como servicio (SaaS).

Cómo configurar la inscripción por detección automática desde un grupo organizativo primario

La inscripción por detección automática simplifica el proceso de inscripción al inscribir los dispositivos en los entornos y grupos organizativos (GO) deseados utilizando las direcciones de correo electrónico de los usuarios finales.

Configure una inscripción por detección automática desde un GO primario siguiendo los pasos que se indican a continuación.

1. Desplácese a Grupos y ajustes > Todos los ajustes > Administrador > Cloud Services y habilite la opción Detección automática. Introduzca la dirección de correo electrónico de inicio de sesión en ID de AirWatch para detección automática y seleccione Establecer identidad.
    1. Si es necesario, vaya a https://my.workspaceone.com/set-discovery-password para definir la contraseña para el servicio de detección automática. Una vez que se haya registrado y seleccione Establecer identidad, el Token HMAC se rellena automáticamente. Haga clic en Probar conexión para asegurarse de que la conexión está funcionando.
2. Habilite la opción Fijación de certificados de detección automática para cargar su propio certificado y adjuntarlo a la función de detección automática. Puede revisar las fechas de validez y otra información de los certificados existentes y también puede Reemplazar y Borrar estos certificados existentes.
3. Seleccione Agregar un certificado y, a continuación, se muestra la configuración de Nombre y Certificado. Introduzca el nombre del certificado que desea cargar, seleccione el botón Cargar y seleccione el certificado en el dispositivo.
4. Seleccione Guardar para completar la configuración de la detección automática.

Indique a los usuarios finales que se inscriban por sí mismos que seleccionen la opción de dirección de correo electrónico para poder autenticarse, en vez de introducir un ID de grupo o una dirección URL del entorno. Cuando los usuarios inscriben sus dispositivos con una dirección de correo electrónico, se inscribirán en el mismo grupo mostrado en el campo Grupo organizativo para la inscripción de la cuenta de usuario asociada.

Cómo inscribirse con el sistema de detección automática desde un grupo organizativo secundario

Puede configurar la inscripción por detección automática desde un grupo organizativo secundario en el grupo organizativo para la inscripción. Para poder realizar una inscripción por detección automática de este modo, deberá pedir a los usuarios que seleccionen un ID de grupo durante la inscripción.

Haga que los usuarios seleccionen un ID de grupo durante las inscripciones.

1. Desplácese a Dispositivos > Ajustes del dispositivo > General > Inscripción y seleccione la pestaña Agrupación.
2. Seleccione Pedirle al usuario que seleccione el ID de grupo.
3. Seleccione Guardar.

Cómo configurar la inscripción de dispositivos administrados de trabajo

El modo Dispositivo administrado de trabajo de Android otorga a Workspace ONE UEM el control de todo el dispositivo. El uso de un dispositivo de restablecimiento de fábrica ayuda a garantizar que los dispositivos no estén configurados para uso personal.

Existen varias formas de inscribir los dispositivos administrados de trabajo:

- Utilizando AirWatch Relay para realizar un bump de NFC
- Utilizando un identificador exclusivo o un código de token
- Escaneando un código QR
- Cómo utilizar la inscripción automatizada
- Usando Knox Mobile Enrollment para dispositivos Samsung. Puede obtener más información en la documentación de Knox Mobile Enrollment.

Los requisitos de su empresa determinan los métodos de inscripción que le conviene utilizar. No puede inscribir los dispositivos hasta que haya finalizado el registro de EMM de Android.

Si los dispositivos Android que utiliza están en una red cerrada no se pueden comunicar con Google Play o ejecutan Android 5.0 o versiones anteriores, puede inscribirse mediante la inscripción Dispositivo administrado para el trabajo para la compatibilidad con AOSP/Red cerrada. La administración de aplicaciones públicas mediante Google Play administrado no estará disponible.

Cómo inscribir con AirWatch Relay

AirWatch Relay es una aplicación que transmite información de dispositivos primarios a todos los dispositivos secundarios que están inscritos en Workspace ONE UEM con Android.

Aviso: AirWatch Relay no es compatible con Android 10.

Este proceso se realiza a través de un bump de NFC y permite a los dispositivos secundarios:

- Copiar la red Wi-Fi del dispositivo principal y la configuración regional, como la fecha, la hora y la ubicación del dispositivo.
- Descargue la última versión de producción de Workspace ONE Intelligent Hub para Android.
- Configure de forma silenciosa Workspace ONE Intelligent Hub como administrador del dispositivo.
- Inscribir automáticamente en Workspace ONE UEM.

AirWatch Relay le permite inscribir en masa todos los dispositivos secundarios antes de implementarlos para los usuarios finales, y evita a los usuarios finales tener que inscribir sus propios dispositivos. Todos los dispositivos secundarios deben estar en modo de restablecimiento de fábrica y tener la NFC habilitada de forma predeterminada para ser inscritos como dispositivos administrado de trabajo para Android.

El proceso de bump de NFC depende del sistema operativo Android. Los dispositivos que ejecutan Android 6.0 o superior realizan un bump para conectar e inscribir dispositivos secundarios en un solo paso. Los dispositivos que ejecutan versiones de SO Android entre v5.0 y v6.0 realizan dos bumps de NFC. El primer bump es para conectar el dispositivo secundario a la red Wi-Fi y a la configuración regional, incluida la fecha, la hora y la ubicación del dispositivo, y descargar Workspace ONE Intelligent Hub. El segundo bump de NFC es para inscribir todos los dispositivos secundarios antes de implementarlos para los usuarios finales.

Cómo realizar la inscripción con VMware Workspace ONE Intelligent Hub Identifier

El método de inscripción de VMware Workspace ONE Intelligent Hub Identifier es una opción simplificada para la inscripción de dispositivos administrados de trabajo para Android 6.0 o superior. Introduzca un identificador simple, o un valor hash, en un dispositivo de restablecimiento de fábrica. Después de introducir el identificador, la inscripción se automatiza mediante la inserción de Workspace ONE Intelligent Hub. El usuario solo debe introducir los detalles del servidor, el nombre de usuario y la contraseña.

Con el identificador, también puede inscribir en nombre del usuario final mediante una Inscripción preparada de dispositivos de usuario único. Este método es útil para aquellos administradores que configuran varios dispositivos para todo un equipo o para miembros específicos del equipo. Gracias a este método, los usuarios finales se ahorran el tiempo y el esfuerzo que conlleva inscribir sus propios dispositivos.

Para obtener más información sobre la inscripción provisional de dispositivos de usuario único, consulte Inscripción provisional de dispositivos de usuario único en la documentación de Administración de dispositivos móviles (MDM).

Cómo inscribir con código QR

El aprovisionamiento de código QR es una forma sencilla de inscribir una flota de dispositivos que no admiten NFC ni el bump de NFC. El código QR contiene una carga útil de pares de clave-valor con toda la información que se necesita para la inscripción del dispositivo. Cree el código QR antes de iniciar la inscripción. Puede usar cualquier generador de código QR en línea, como Web Toolkit Online, para crear un código QR único. El código QR incluye la información de dirección URL del servidor y el ID de grupo. También puede incluir el nombre de usuario y contraseña, o bien el usuario tiene que introducir sus credenciales.

Este es el formato del texto que debe copiarse en el generador:

```
{"android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"com.airwatch.androidagent/com.airwatch.agent.DeviceAdministratorReceiver","android.ap
p.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":
"6kyqxDOjgS30jvQuzh4uvHPk-0bmAD-1QU7vtW7i_o8=\n","android.app.extra.PROVISIONING_DEVIC
E_ADMIN_PACKAGE_DOWNLOAD_LOCATION":"https://getwsone.com/mobileenrollment/airwatchagen
t.apk",
"android.app.extra.PROVISIONING_SKIP_ENCRYPTION":      false,"android.app.extra.PROVISIONIN
G_WIFI_SSID":  "Your_SSID","android.app.extra.PROVISIONING_WIFI_PASSWORD":  "Password",
"android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
{"serverurl": "Server URL",
"gid": "Group ID",
"un":"Username",
"pw":"Password"}
```

Inscripción automatizada

La inscripción automatizada permite configurar dispositivos que ejecutan Android 9.0 o posterior con Workspace ONE UEM como proveedor de administración de movilidad empresarial desde el primer

momento.

Si el dispositivo está conectado a Internet durante la configuración del dispositivo, se descarga automáticamente Workspace ONE Intelligent Hub y se pasan automáticamente los detalles de la inscripción para inscribir el dispositivo sin la interacción del usuario. Una vez que configure la inscripción automatizada, puede administrar los dispositivos automatizados de su organización desde la página de registro de EMM de Android.

La inscripción automatizada solo es compatible con un número limitado de operadores móviles y OEM. Los clientes deberán consultar con sus operadores para saber si admiten el aprovisionamiento automatizado. Puede obtener más información sobre los operadores y dispositivos compatibles en el sitio web de Google.

Para obtener información adicional sobre la inscripción automatizada, consulte el Artículo de soporte de Android.

Aviso: La inscripción automatizada solo es compatible en los dispositivos con Android 8.0 (Oreo) o una versión posterior.

Inscripción de dispositivos mediante Workspace ONE Access

Workspace ONE Access proporciona autenticación multifactor, acceso condicional e inicio de sesión único en SaaS, web y aplicaciones móviles nativas. Puede utilizar Workspace ONE Access para autenticar dispositivos en lugar de Workspace ONE Intelligent Hub. Cuando haya habilitado Workspace ONE Access como método de autenticación, podrá utilizar métodos de inscripción automática como NFC, códigos QR, automatizados y la inscripción mediante Samsung Knox Mobile.

Cómo inscribir dispositivos administrados de trabajo mediante AirWatch Relay

La inscripción del modo Dispositivo administrado de trabajo mediante AirWatch Relay varía en función de la versión del sistema operativo Android.

Aviso: AirWatch Relay no es compatible con Android 10 ni versiones posteriores.

Cómo inscribir dispositivos Android con AirWatch Relay para Android 6.0 o superior

En Android 6.0 o superior, la aplicación AirWatch Relay proporciona una opción de un solo bump para configurar la región, la red Wi-Fi, los ajustes de aprovisionamiento y los ajustes de inscripción en ese único bump.

Procedimiento

1. Descargue la aplicación AirWatch Relay desde la tienda Google Play en el dispositivo primario e inicie la aplicación una vez finalizada.
2. Revise la pantalla "Para administradores de AirWatch" y seleccione Siguiente para continuar con el asistente. Esta pantalla le permitirá ver u omitir un asistente de instalación que proporciona descripciones acerca del propósito de la aplicación e incluye un tutorial del bump de NFC.
3. Toque en Configuración en los dispositivos de aprovisionamiento en un único bump

(Android 6.0 o superior).

4. Desde el dispositivo primario, defina los siguientes ajustes:

Ajustes	Descripción
Hora local	Habilite este campo para que el dispositivo se configure automáticamente con la hora local.
Zona horaria	Seleccione la zona horaria.
Región	Seleccione la ubicación en la que se va a habilitar su dispositivo.
Red Wi-Fi	Especifique la red de Wi-Fi a la que se va a conectar el dispositivo.
Tipo de seguridad	Determine el tipo de cifrado para la conexión.
Contraseña Wi-Fi	Introduzca la contraseña de Wi-Fi.
Cifrar dispositivo	Deshabilite esta configuración para omitir el cifrado del dispositivo como parte del aprovisionamiento de dispositivos administrados de trabajo.
Deshabilitar aplicaciones del sistema	Cuando está habilitada, Workspace ONE Intelligent Hub deshabilita las aplicaciones de sistema durante la instalación.
Servidor	Introduzca la dirección URL del servidor o el nombre de host.
ID del grupo	Introduzca un identificador para el grupo organizativo, que los usuarios utilizarán para que los dispositivos inicien sesión.
Nombre de usuario	Introduzca las credenciales para el usuario del dispositivo secundario que se va a inscribir.
Contraseña	Introduzca las credenciales para el usuario del dispositivo secundario que se va a inscribir.

5. Toque en Listo desde el dispositivo primario.

6. Toque en el dispositivo principal y secundario consecutivamente para llevar a cabo el bump de NFC. El dispositivo secundario debe estar en modo de restablecimiento de fábrica para asegurarse de que no esté configurado para uso personal. Antes de realizar un restablecimiento de fábrica en los dispositivos secundarios (si el dispositivo no está recién sacado de la caja), deshabilite la pantalla de bloqueo y elimine todas las cuentas de Google existentes configuradas en el dispositivo. La protección de dispositivos es una función para Android 5.1 y posterior que requiere que el usuario introduzca las credenciales de la cuenta de Google antes de realizar un restablecimiento de fábrica. Si deshabilita el bloqueo de pantalla y elimina la cuenta de Google existente, no se le pedirán las credenciales y no se dificultará la inscripción.

7. Toque en Tocar para emitir en el dispositivo primario con los dispositivos aún juntos.

8. Toque en Cifrar en el dispositivo secundario con los dispositivos aún juntos. Este paso solo se aplica si no se ha habilitado la opción Cifrar dispositivo. De lo contrario, se aceptará automáticamente. Automáticamente, el dispositivo secundario:

```
Connects to the Wi-Fi network defined in the AirWatch Relay app.
Downloads and silently installs the Workspace ONE Intelligent Hub.
Sets the Workspace ONE Intelligent Hub as device administrator.
```

```
Resets the device.
```

Una vez restablecido el dispositivo secundario, el dispositivo se aprovisiona para el modo administrado de trabajo. Aparece una pantalla de bienvenida en el dispositivo secundario. Para comprobar lo mencionado desde el dispositivo secundario, desplácese a Ajustes del dispositivo > Seguridad > Administradores del dispositivo para ver que Workspace ONE Intelligent Hub aparece como el administrador del dispositivo. Los usuarios finales no podrán desactivar esta opción.

También se pueden observar en la pantalla principal del dispositivo las aplicaciones previamente descargadas permitidas. Cualquier otra aplicación deberá ser aprobada por el administrador de Workspace ONE UEM console.

Si tiene varios dispositivos para inscribir en su flota de dispositivos, repita a continuación el primer bump de NFC en cada dispositivo secundario para aprovisionarlos en el modo Dispositivo administrado de trabajo.

Resultados

Si la inscripción se ha realizado correctamente, se mostrará la página Mi dispositivo en el dispositivo secundario. Todas las aplicaciones y los perfiles comenzarán a enviarse automáticamente al dispositivo. Deberá repetir los pasos de inscripción para cada dispositivo que necesite inscribir en su flota de dispositivos.

La consola de Workspace ONE UEM informa del estado de Android en los dispositivos de los usuarios. Puede consultar la página Vista de detalles para comprobar que el dispositivo está inscrito correctamente en el modo administrado de trabajo.

Cómo inscribir dispositivos administrados de trabajo mediante AirWatch Relay para Android 5.0 y Android 6.0

Para Android v5.0 y Android v6.0, la aplicación AirWatch Relay ofrece una opción de bump de NFC que permite configurar automáticamente os ajustes de región, Wi-Fi, aprovisionamiento e inscripción.

Procedimiento

1. Descargue la aplicación AirWatch Relay desde la tienda Google Play en el dispositivo primario e inicie la aplicación una vez finalizada.
2. Revise la pantalla "Para administradores de AirWatch" y seleccione Siguiente para continuar con el asistente. Esta pantalla le permitirá ver u omitir un asistente de instalación que proporciona descripciones acerca del propósito de la aplicación e incluye un tutorial del bump de NFC.
3. Toque Configuración en la opción que desee para aprovisionar dispositivos en 2 bumps (se puede realizar en Android 5.0 para dispositivos Android 6.0).
4. Desde el dispositivo primario, defina los siguientes ajustes:

Ajustes	Descripción
Hora local	Habilite este campo para que el dispositivo se configure automáticamente con la hora local.
Zona horaria	Seleccione la zona horaria.

Ajustes	Descripción
Región	Seleccione la ubicación en la que se va a habilitar su dispositivo.
Red Wi-Fi	Especifique la red de Wi-Fi a la que se va a conectar el dispositivo.
Tipo de seguridad	Determine el tipo de cifrado para la conexión.
Contraseña Wi-Fi	Introduzca la contraseña de Wi-Fi.
Cifrar dispositivo	Habilite este campo para indicar que el cifrado de dispositivo puede omitirse dentro del aprovisionamiento de dispositivos administrados de trabajo.
Deshabilitar aplicaciones del sistema	Si este campo está habilitado, Workspace ONE Intelligent Hub deshabilita las aplicaciones del sistema durante la configuración.

5. Haga clic en Listo desde el dispositivo primario para realizar el primer bump.
6. Haga clic en el dispositivo principal y secundario consecutivamente para llevar a cabo el primer bump de NFC. El dispositivo secundario debe estar en modo de restablecimiento de fábrica para asegurarse de que no esté configurado para uso personal.

   Antes de realizar un restablecimiento de fábrica en los dispositivos secundarios (si el dispositivo no está recién sacado de la caja), deshabilite la pantalla de bloqueo y elimine todas las cuentas de Google existentes configuradas en el dispositivo. Protección de dispositivo es una función para Android 5.1 que requiere que el usuario introduzca las credenciales de la cuenta de Google antes de realizar un restablecimiento de fábrica. Si deshabilita el bloqueo de pantalla y elimina la cuenta de Google existente, no se le pedirán las credenciales y no se dificultará la inscripción.
7. Toque en Tocar para emitir en el dispositivo primario con los dispositivos aún juntos.
8. Toque en Cifrar en el dispositivo secundario con los dispositivos aún juntos. Este paso solo se aplica si no se ha habilitado Cifrar dispositivo, de lo contrario, se aceptará automáticamente.

   Automáticamente, el dispositivo secundario:

```
Connect to the Wi-Fi network defined in the AirWatch Relay app.
Download and silently install the Workspace ONE Intelligent Hub.
Set the Workspace ONE Intelligent Hub as device administrator.
Reset the device.
```

   Una vez restablecido el dispositivo secundario, el dispositivo se aprovisiona para el modo administrado de trabajo y se completa el primer bump. Aparece una pantalla de bienvenida en el dispositivo secundario. Para comprobar lo mencionado desde el dispositivo secundario, desplácese a Ajustes del dispositivo > Seguridad > Administradores del dispositivo para ver que Workspace ONE Intelligent Hub aparece como el administrador del dispositivo. Los usuarios finales no podrán desactivar esta opción.

   También se pueden observar en la pantalla principal del dispositivo las aplicaciones previamente descargadas permitidas. Cualquier otra aplicación deberá ser aprobada por el administrador de Workspace ONE UEM console.

   Si tiene varios dispositivos para inscribir en su flota de dispositivos, repita a continuación el

primer bump de NFC en cada dispositivo secundario para aprovisionarlos en el modo Dispositivo administrado de trabajo. Si no es así, continúe con la inscripción.

Si lo prefiere, puede elegir inscribir los dispositivos secundarios manualmente y omitir los pasos del segundo bump de NFC que se detallan a continuación. Deberá introducir los datos de la inscripción manualmente en cada dispositivo. Para los flujos de inscripción adicionales, consulte Flujos de trabajo de inscripción adicionales en la documentación de Administración de dispositivos móviles (MDM).

9. Vuelva a la aplicación AirWatch Relay desde el dispositivo primario y haga clic en Inscribir.
10. Defina los ajustes de inscripción. Estos ajustes se utilizarán para automatizar la inscripción de los dispositivos secundarios.

Ajustes	Descripción
Servidor	Introduzca la dirección URL del servidor o el nombre de host.
ID del grupo	Introduzca un identificador para el grupo organizativo, que los usuarios utilizarán para que los dispositivos inicien sesión.

11. Toque Listo.
12. Realice el segundo bump de NFC colocando juntos el dispositivo principal y el secundario y haga clic en Tocar para emitir en el dispositivo secundario e iniciar la inscripción. El segundo bump de NFC debe realizarse una vez que finalice el asistente de configuración. Espere hasta que el asistente de instalación haya finalizado y le dirija a la página de inicio del dispositivo para realizar el segundo bump de NFC para configurar Workspace ONE Intelligent Hub.
13. Introduzca las credenciales de la cuenta de Google corporativa asociada al usuario. Le aparecerá la pantalla de contraseña de la cuenta de Google. Si se inscribe como una cuenta de Google Play administrada, esta pantalla no se mostrará.
14. Toque Siguiente para ir a la página Mi dispositivo.

Pasos siguientes Si la inscripción se ha realizado correctamente, se mostrará la página Mi dispositivo en el dispositivo secundario (mostrado anteriormente). Todas las aplicaciones y los perfiles comenzarán a enviarse automáticamente al dispositivo. Deberá repetir los pasos de inscripción para cada dispositivo que necesite inscribir en su flota de dispositivos.

Cómo inscribir dispositivos Android con VMware Workspace ONE Intelligent Hub Identifier

Durante la inscripción de un dispositivo administrado de trabajo y corporativo habilitado de forma personal (COPE), el usuario introduce un token de identificador específico de DPC especial cuando se le pide que agregue una cuenta. El token de Workspace ONE UEM es "afw#hub", que identifica automáticamente a Workspace ONE UEM como su proveedor de EMM.

Importante: Este flujo de inscripción solo es compatible con dispositivos Android 6.0 Marshmallow o versiones posteriores.

1. Haga clic en Primeros pasos en su dispositivo con restablecimiento de fábrica.
2. Seleccione la red Wi-Fi e inicie sesión con sus credenciales para conectar el dispositivo.

3. Introduzca el identificador "afw#hub" cuando se le pida que agregue una cuenta de Google. El asistente de configuración agrega una cuenta de Google temporal al dispositivo. Esta cuenta solo se usa para descargar el DPC desde Google Play y se elimina una vez que finaliza.

   Si se introduce el identificador de forma incorrecta, se le pedirá que lo vuelva a introducir.

4. Toque Instalar para comenzar la configuración de Workspace ONE Intelligent Hub en el dispositivo. El Hub se abrirá automáticamente una vez completada la instalación.

5. Elija el Método de autenticación para continuar con la inscripción:

   1. Introduzca la Dirección de correo electrónico si ha configurado el modo Detección automática. Además, es posible que se le solicite seleccionar el ID de grupo de una lista o elegir Detalles del servidor e introducir el servidor, el ID de grupo y las credenciales de usuario.
   2. Elija Código QR si ha creado un código QR en la consola de UEM.

6. Siga las instrucciones restantes para completar la inscripción.

   Aviso: Puede consultar la página Vista de detalles para comprobar que el dispositivo está inscrito correctamente en el Modo administrado de trabajo.

Inscribir un dispositivo administrado de trabajo mediante un código QR

El método de inscripción con código QR instala y configura los modos Dispositivo administrado de trabajo y Corporativo habilitado de forma personal (COPE) mediante el escaneado de un código QR generado con el asistente de configuración de la inscripción o desde cualquier generador de códigos QR, como Web Toolkit Online.

Para usar UEM Console con el fin de crear el código QR, consulte el Asistente de configuración de inscripción (Dispositivos > Ciclo de vida > Plataforma provisional > Vista de lista > Configurar inscripción).

Importante: Este flujo de inscripción está disponible para los usuarios de Google Play administrado y de dominio de Google administrado. Este flujo de inscripción es compatible con dispositivos que ejecutan Android 7.0 o superior.

1. Encienda el dispositivo con restablecimiento de fábrica o listo para usar. El asistente para instalación solicita al usuario que toque la pantalla de bienvenida seis veces. Los toques deben realizarse en el mismo lugar en la pantalla.

   - Para dispositivos con Android 8.0 o posterior, continúe con el paso 2 para poder descargar el lector del código QR.
   - Para dispositivos Android 9.0 +, la cámara se abrirá automáticamente después de completar los seis toques.

2. Conéctese a la red Wi-Fi y el asistente de configuración descargará automáticamente un lector de códigos QR. La aplicación de lector de código QR se inicia automáticamente una vez terminada la instalación. En dispositivos con Android 8.0 y 9.0, puede utilizar la conectividad móvil. En Android 10 o versiones posteriores, se requiere Wi-Fi.

3. Escanee el código QR. Para dispositivos con Android 9.0 o posterior, utilice la opción de

código QR de la cámara para escanear. Puede utilizar cualquier generador de códigos QR en línea, como Web Toolkit Online.

Para crear un código QR único, introduzca el siguiente código en el campo Formato de texto de código QR:

```
{"android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"com.airwatch.androidagent/com.airwatch.agent.DeviceAdministratorReceiver","android.ap
p.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":
"6kyqxDOjgS30jvQuzh4uvHPk-0bmAD-1QU7vtW7i_o8=\n","android.app.extra.PROVISIONING_DEVIC
E_ADMIN_PACKAGE_DOWNLOAD_LOCATION":"https://getwsone.com/mobileenrollment/airwatchagen
t.apk",
"android.app.extra.PROVISIONING_SKIP_ENCRYPTION":      false,"android.app.extra.PROVISIONIN
G_WIFI_SSID":  "Your_SSID","android.app.extra.PROVISIONING_WIFI_PASSWORD":  "Password",
"android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":
{"serverurl": "Server URL",
"gid": "Group ID",
"un":"Username",
"pw":"Password"}
}
```

1. El asistente para la instalación descarga automáticamente Workspace ONE Intelligent Hub y configura automáticamente la URL del servidor, el ID de grupo, el Nombre de usuario y la Contraseña tal como se ha especificado en el código QR generado.

   Aviso: Cuando se incluya el servidor, el ID de grupo, el nombre de usuario y la contraseña en la configuración, Hub omitirá cualquier solicitud de inscripción adicional

2. Introduzca las credenciales de usuario que no se han configurado previamente en el código QR.

   Si la inscripción se ha realizado correctamente, se mostrará la página Mi dispositivo en el dispositivo. Todas las aplicaciones y los perfiles comienzan a enviarse automáticamente al dispositivo.

   La consola de Workspace ONE UEM informa del estado de Android en los dispositivos de los usuarios. Puede consultar la página Vista de detalles para comprobar que el dispositivo está inscrito correctamente en el Modo administrado de trabajo.

Cómo generar un código QR con el Asistente de configuración de la inscripción

Cree un código QR que pueda escanear con los dispositivos con Android 7.0 o una versión posterior para realizar una copia intermedia del dispositivo rápidamente. El asistente simplifica el proceso de configuración de la inscripción preparada.

1. Desplácese hasta Dispositivos > Ciclo de vida > Plataforma provisional > Vista de lista > Configurar inscripción > Android > Código QR en Workspace ONE UEM Console.
2. Conecte el dispositivo a la red Wi-Fi antes de la inscripción mediante la activación del conmutador para Wi-Fi. Se muestran las siguientes opciones:

Ajustes	Descripción

SSID	Introduzca el identificador de red SSID, más comúnmente conocida por el nombre de red Wi-Fi.
Contraseña	Introduzca la contraseña Wi-Fi para el SSID introducido.

3. Seleccione Siguiente.
4. Seleccione el Workspace ONE Intelligent Hub que desea insertar en los dispositivos durante la inscripción provisional. La opción predeterminada es Usar el Workspace ONE Intelligent Hub más reciente.

   Si no ha añadido ningún Workspace ONE Intelligent Hub, seleccione Hospedado en una URL externa y escriba la dirección en el cuadro de texto URL para que apunte a un paquete de Workspace ONE Intelligent Hub hospedado de forma externa.
5. Seleccione Siguiente.
6. Configure las opciones de Detalles de la inscripción. Para utilizar la autenticación basada en tokens, deje ambas opciones deshabilitadas.

Ajustes	Descripción
Grupo organizativo	Habilite y seleccione el grupo organizativo del código QR que utiliza el paquete de inscripción preparada.
Nombre de usuario	Configure las credenciales de inicio de sesión. Introduzca el nombre de la cuenta de usuario de Workspace ONE UEM.
Contraseña	Introduzca la contraseña correspondiente.
Aplicaciones del sistema	Se aplica solo a los dispositivos administrados de trabajo. Puede Habilitar la opción para mantener las aplicaciones de sistema no críticas instaladas en su dispositivo administrado de trabajo. Seleccione Deshabilitar para eliminar estas aplicaciones.
Forzar la inscripción de AOSP / Red cerrada	Cuando este campo está habilitado, puede inscribir dispositivos GMS y no GMS en el mismo grupo organizativo, independientemente del tipo de inscripción de dispositivos administrados de trabajo establecido durante el registro de EMM de Android. - Si el indicador está configurado para usar GMS y UEM Console se establece en AOSP en la página de registro de EMM de Android, el dispositivo utilizará el indicador de UEM Console y se inscribirá sin cuenta de Google.
	Si el indicador está configurado para usar GMS y UEM Console se ha configurado en cuentas basadas en usuario o basadas en dispositivo, el Intelligent Hub intentará realizar un flujo de inscripción de GMS. Si el dispositivo no es GMS, se producirá un error en la inscripción.

7. Seleccione Siguiente.
8. La página Resumen le permite Descargar el archivo del documento PDF. Seleccione Ver PDF para ver una vista previa de las selecciones de Formato de código QR.

Inscribir dispositivos Android mediante el portal

automatizado

En el portal automatizado, añada las configuraciones de inscripción que deberían aplicarse en el dispositivo en cuanto se realice la descarga de Workspace ONE Intelligent Hub.

Aviso: La inscripción automatizada solo es compatible en los dispositivos con Android 9.0 o una versión posterior. Para los dispositivos Samsung, utilice Knox Mobile Enrollment.

Para comenzar en el portal automatizado:

1. Navegue hasta la pestaña Configuraciones y haga clic en +.
2. Introduzca los datos siguientes para la inscripción:

Ajustes	Descripción
Nombre de la configuración	Introduzca un nombre para esta configuración.
EMM DPC	Seleccione "Workspace ONE Intelligent Hub". De este modo se asegurará de que Workspace ONE Intelligent Hub se descargue dentro de la instalación de fábrica.
DPC adicionales	Introduzca las credenciales de inscripción que se configurarán en Workspace ONE Intelligent Hub. Puede incluir la dirección URL del servidor, el ID de grupo, el nombre de usuario de inscripción y la contraseña de Workspace ONE UEM console. Copie el texto con formato JSON desde la consola de EMM.
Nombre de la empresa	Introduzca el nombre de su organización.
Dirección de correo electrónico de soporte	Introduzca el correo electrónico con el que los usuarios finales deben ponerse en contacto si encuentran problemas.
Número de teléfono de soporte	Introduzca el número de teléfono al que deben llamar los usuarios finales si encuentran problemas.
Mensaje personalizado	Introduzca un mensaje personalizado para mostrar a los usuarios finales antes de descargar Workspace ONE Intelligent Hub.

Estos son algunos de los distintos escenarios que puede utilizar para configuraciones automatizadas:

Si los usuarios finales aprovisionan sus dispositivos

En este escenario, excluya el nombre de usuario y la contraseña; el usuario los introducirá durante la instalación del dispositivo cuando se le solicite.

{ “android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE”: { “serverurl”: “https://airwatch.console.com”, “gid”: “groupID”} }

Si va a realizar la asignación a usuarios provisionales y conoce las credenciales de usuario

Este escenario se recomienda si todos los dispositivos se están preparando para un solo usuario, o bien se conocen el nombre de usuario y la contraseña de inscripción.

{ “android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE”: { “serverurl”:

“https://airwatch.console.com”, “gid”: “groupID”, “un”:“username”, “pw”:“password” } }

1. Seleccione Aplicar.
2. Asigne configuraciones en la pestaña Dispositivos seleccionando la configuración de inscripción que deberá aplicarse al dispositivo.

   Deberá consultar con su operador o el distribuidor de su dispositivo para recuperar el IMEI y los números de serie de sus dispositivos.

Vincular una cuenta automatizada a Workspace ONE UEM

Una vez que haya configurado su cuenta y dispositivos automatizados en el portal automatizado, puede vincular su cuenta a UEM Console para administrar sus dispositivos automatizados dentro de las consolas. Al vincular su cuenta automatizada a UEM Console, puede ver los dispositivos asociados con la cuenta automatizada, establecer una configuración de inscripción predeterminada y editar la información de soporte a través de Workspace ONE UEM Console.

Para vincular una nueva cuenta automatizada en UEM Console:

1. Navegue a Grupos y ajustes > Todos los ajustes > Dispositivos y usuarios > Android > Registro de EMM de Android y seleccione Automatizado.
2. Antes de vincular la cuenta, especifique los parámetros para la configuración predeterminada de inscripción automatizada. Una vez que vincule la cuenta automatizada, Workspace ONE UEM establecerá estos parámetros como la configuración de inscripción predeterminada de la cuenta.

Aviso: Para cambiar la configuración predeterminada, desvincule la cuenta de inscripción automatizada y repita este proceso de vinculación.

```
- Enable **Specific Organization Group** to select a specific Organization Group. When
 this option is not turned on, the settings apply to all groups.
- Configure **DPC Extras** which allows you to configure the DPC and provisioning extr
as used during zero-touch device setup.
```

Consulte Indicadores de inscripción adicionales.

1. Seleccione Vincular cuentas automatizadas, que le permite vincular sus cuentas automatizadas.

Ahora ve las cuentas automatizadas, la configuración, los dispositivos y la información de soporte. También puede vincular cuentas de inscripción automatizadas adicionales.

Cómo configurar la inscripción corporativa habilitada de forma personal

El modo Corporativo habilitado de forma personal (COPE) de Android proporciona a Workspace ONE UEM control sobre todo el dispositivo mientras se implementa un perfil de trabajo para que el usuario utilice el dispositivo como un dispositivo personal. COPE es un híbrido entre los modos de perfil de trabajo y de dispositivo administrado de trabajo.

Aviso:

Android 8.0 + requiere utilizar la implementación COPE en su flota de dispositivos. Si intenta inscribir

un dispositivo que no está ejecutando Android 8.0, el dispositivo se inscribirá automáticamente como un dispositivo administrado de trabajo.

Existen varias formas de inscribir los dispositivos COPE:

- A través de un identificador único o un código de token (disponible en Android 10 o en versiones anteriores, tal como se ha señalado)
- Escaneando un código QR
- Usando el aprovisionamiento automático
- Usando Knox Mobile Enrollment para dispositivos Samsung. Puede obtener más información en la documentación de Knox Mobile Enrollment.

Los requisitos de su empresa determinan los métodos de inscripción que le conviene utilizar. No puede inscribir los dispositivos hasta que haya finalizado el registro de EMM de Android.

Cómo inscribir con AirWatch Relay

AirWatch Relay es una aplicación que transmite información de dispositivos primarios a todos los dispositivos secundarios que están inscritos en Workspace ONE UEM con Android. Este proceso se realiza a través de un bump de NFC y permite a los dispositivos secundarios:

- Conectarse al dispositivo primario para copiar la red Wi-Fi y la configuración regional, como la fecha, la hora y la ubicación del dispositivo.
- Descargue la última versión de producción de Workspace ONE Intelligent Hub para Android.
- Configure de forma silenciosa Workspace ONE Intelligent Hub como administrador del dispositivo.
- Inscribir automáticamente en Workspace ONE UEM.

AirWatch Relay le permite inscribir en masa todos los dispositivos secundarios antes de implementarlos para los usuarios finales, y evita a los usuarios finales tener que inscribir sus propios dispositivos. Todos los dispositivos secundarios deben estar en modo de restablecimiento de fábrica y tener la NFC habilitada de forma predeterminada para ser inscritos como dispositivos COPE.

El proceso de bump de NFC depende de la versión del sistema operativo Android. Dado que COPE solo se admite en Android 8.0 +, la inscripción con AirWatch Relay llevará a cabo un único bump para conectar e inscribir dispositivos secundarios en un solo paso.

Nota Android 11 no es compatible con la opción de bump de NFC de AirWatch Relay para COPE. Si intenta inscribir dispositivos con Android 11 mediante el bump de NFC, la inscripción se bloqueará puesto que Google dejó de utilizar esta función.

Inscribirse con VMware Workspace ONE Intelligent Hub Identifier

El método de inscripción con VMware Workspace ONE Intelligent Hub Identifier es un enfoque simplificado para la inscripción de dispositivos habilitados para COPE. Introduzca un identificador simple, o un valor hash, en un dispositivo de restablecimiento de fábrica. Después de introducir el identificador, la inscripción se automatiza mediante la inserción de Workspace ONE Intelligent Hub. El usuario solo debe introducir los detalles del servidor, el nombre de usuario y la contraseña.

Aviso: Este método de inscripción no está disponible en Android 11 para COPE. Si intenta inscribir dispositivos con Android 11, la inscripción se bloqueará puesto que Google dejó de utilizar esta función.

Cómo inscribir con código QR

El aprovisionamiento de código QR es una forma sencilla de inscribir una flota de dispositivos que no admiten NFC ni el bump de NFC. El código QR contiene una carga útil de pares de clave-valor con toda la información que se necesita para la inscripción del dispositivo. Cree el código QR antes de iniciar la inscripción. Puede generar el código QR mediante el asistente de configuración de inscripción en la consola de Workspace ONE UEM.

El código QR incluye la información de dirección URL del servidor y el ID de grupo. También puede incluir el nombre de usuario y contraseña, o bien el usuario tiene que introducir sus credenciales.

Este es el formato del texto que debe pegarse en el generador de código QR:

```
{

"android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":
"com.airwatch.androidagent/com.airwatch.agent.DeviceAdministratorReceiver",
"android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":
"6kyqxDOjgS30jvQuzh4uvHPk-0bmAD-1QU7vtW7i_o8=\n",
"android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":
"https://getwsone.com/mobileenrollment/airwatchagent.apk",
"android.app.extra.PROVISIONING_SKIP_ENCRYPTION": false,
"android.app.extra.PROVISIONING_WIFI_SSID": "ssid",
"android.app.extra.PROVISIONING_WIFI_PASSWORD":    "password",
"android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE": {
"serverurl": "deviceservices.myserver.com",
"gid": "group_id",
"un":"username",
"pw":"password"
}
}
```

Cómo inscribir de forma automatizada

El aprovisionamiento automático permite configurar dispositivos que ejecutan Android 8.0 superior con Workspace ONE UEM como proveedor de administración de movilidad empresarial desde el primer momento.

Si el dispositivo está conectado a Internet durante la configuración del dispositivo, se descarga automáticamente Workspace ONE Intelligent Hub y se pasan automáticamente los detalles de la inscripción para inscribir el dispositivo sin la interacción del usuario.

A continuación se describen algunos requisitos previos que deben considerarse:

El aprovisionamiento automático solo es compatible con un número limitado de operadores móviles y fabricantes de equipos originales. Los clientes deberán consultar con sus operadores para saber si admiten el aprovisionamiento automático. Puede obtener más información sobre los operadores y dispositivos compatibles en el sitio web de Google.

Indicadores de inscripción adicionales admitidos para la inscripción de Android (DPC adicionales)

En este tema, se explica cómo implementar indicadores de inscripción adicionales mediante código QR o inscripción con el portal automatizado.

Formato

En el siguiente ejemplo, la información en negrita indica Información necesaria al implementar el código QR o la inscripción mediante JSON.

Para los valores opcionales, a partir de `"android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":`, introduzca las credenciales de inscripción que se configurarán en Workspace ONE Intelligent Hub. Puede incluir la dirección URL del servidor, el ID de grupo, el nombre de usuario de inscripción y la contraseña de Workspace ONE UEM console.

Donde indica `"VMwareSpecificflags":"EnterValue"`, consulte los indicadores disponibles a continuación y utilice el valor correcto según sea necesario.

```
{
   **"android.app.extra.PROVISIONING\_DEVICE\_ADMIN\_COMPONENT\_NAME":"com.airwatch.an
droidagent/com.airwatch.agent.DeviceAdministratorReceiver",
   "android.app.extra.PROVISIONING\_DEVICE\_ADMIN\_SIGNATURE\_CHECKSUM":"6kyqxDOjgS30j
vQuzh4uvHPk-0bmAD-1QU7vtW7i\_o8=",
   "android.app.extra.PROVISIONING\_DEVICE\_ADMIN\_PACKAGE\_DOWNLOAD\_LOCATION":"",
   "android.app.extra.PROVISIONING\_SKIP\_ENCRYPTION":"false",**
   "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":{
      "serverurl":"",
      "gid":"",
      "un":"",
      "pw":"",
      "VMwareSpecificflags":"Value"
   }
}
```

Desanclar Hub en caso de error de inscripción por detección automática

Si se produce un error en algún paso durante la inscripción automática o se produce algún otro error, Hub puede solicitar al usuario que ejecute la acción de desanclar, lo que permitirá al usuario acceder a todo el dispositivo. La función de desanclar también se puede proteger con una contraseña opcional. Si se establece, el usuario debe introducir la contraseña para desanclar. El usuario tiene intentos ilimitados de introducir la contraseña.

Los siguientes DPC adicionales deben agregarse al "Paquete adicional para administrador" en el código QR de inscripción:

```
"android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":  {  "*allowUnpinning*":  "*true*",
*"unpinPassword":"1234"*  }
```

Deshabilitar SafeBoot

Determina si el usuario no podrá reiniciar el dispositivo en modo de arranque seguro durante la inscripción. Esto se aplica a todos los métodos de inscripción inmediatos, entre los que se incluyen: La inscripción móvil de Samsung Knox (KME), automatizada y mediante código QR. Configure el valor booleano reemplazando el valor "Boolean" por "true" o "false".

```
"disableSafeBoot":"Boolean"
```

Deshabilitar Depuración USB

Determina si un usuario no tendrá permiso para habilitar o acceder a las funciones de depuración. Configure el valor booleano reemplazando el valor "Boolean" por "true" o "false".

```
"disableUsbDebugging":"Boolean"
```

Deshabilitar Orígenes desconocidos

Determina si un usuario no tendrá permiso para instalar aplicaciones que no se encuentren en la tienda. Configure el valor booleano reemplazando el valor "Boolean" por "true" o "false".

```
"disableInstallUnknownSources":"Boolean"
```

Utilizar autenticación de UEM

Si los usuarios desean utilizar la autenticación de UEM a pesar de encontrarse en Workspace ONE Access, deberán notificarlo a través de un nuevo código QR, que también se utilizará en el portal de KME a través de un JSON personalizado. Configure el valor booleano reemplazando el valor "Boolean" por "true" o "false".

```
"useUEMAuthentication":"Boolean"
```

URL de detección automática local

Configure la URL de detección automática local reemplazando "String" en el ejemplo siguiente por una URL similar a "www.myautodiscoveryurl.com".

```
"localAutoDiscoveryUrl":"String"
```

Número de reintentos de detección

Configure el número de reintentos de detección con un valor entero. Use un número inferior a 10. A continuación se muestra un ejemplo de cómo introducir este valor correctamente, reemplazando "Integer" por el número que elija.

```
"discoveryRetryCount":"Integer"
```

Intervalo de detección en segundos

Configure el intervalo de reintento de detección en segundos. A continuación se muestra un ejemplo de cómo introducir este valor correctamente, reemplazando "Integer" por el número que elija.

```
"discoveryIntervalInSeconds":"Integer"
```

Inscripción de AOSP

Permita que el dispositivo omita la adición de una cuenta de trabajo. Configure el valor booleano reemplazando el valor "Boolean" por "true" o "false".

```
"aospenrollment":"Boolean"
```

Número de reintentos

Configure el número de veces que se debe volver a intentar la inscripción automática en caso de error. Considere la posibilidad de usar un valor inferior a 10. A continuación se muestra un ejemplo de cómo introducir este valor correctamente, reemplazando "Integer" por el número que elija.

```
"retrycount":"Integer"
```

Permitir desanclaje

Permitir que el usuario se desplace fuera de Hub durante la inscripción. Configure el valor booleano reemplazando el valor "Boolean" por "true" o "false".

```
"allowUnpinning":"Boolean"
```

Certificado de inscripción

El DPC adicional de aprovisionamiento de certificados de inscripción proporciona a Workspace ONE Intelligent Hub para Android una forma de instalar un certificado antes de la inscripción, lo que es ideal para entornos de red cerrada que utilizan certificados autofirmados.

Cuando el DPC adicional se incluye en el código QR, Hub inscribe automáticamente en modo de propietario del dispositivo (totalmente administrado), instala el certificado e inscribe el dispositivo.

Siga estos pasos para obtener los datos del certificado codificado:

1. Cargar el certificado en un perfil de credenciales de Android
2. Guarde el perfil. No asignarlo a ningún dispositivo
3. Seleccione el perfil y vea el XML del perfil. "CertificateData" en el XML del perfil es lo que se utiliza en el JSON a continuación.
4. Agregue la siguiente clave al Paquete adicional para administrador en el código QR que aprovisiona JSON: "workManagedCertData":"Datos de certificado codificados"

```
{
```

```
   "android.app.extra.PROVISIONING_DEVICE_ADMIN_COMPONENT_NAME":"com.airwatch.androida
gent/com.airwatch.agent.DeviceAdministratorReceiver",
   "android.app.extra.PROVISIONING_DEVICE_ADMIN_SIGNATURE_CHECKSUM":"6kyqxDOjgS30jvQuz
h4uvHPk-0bmAD-1QU7vtW7i_o8=",
   "android.app.extra.PROVISIONING_DEVICE_ADMIN_PACKAGE_DOWNLOAD_LOCATION":"",
   "android.app.extra.PROVISIONING_SKIP_ENCRYPTION":false,
   "android.app.extra.PROVISIONING_ADMIN_EXTRAS_BUNDLE":

{"serverurl":"","gid":"","un":"","pw":"","workManagedCertData":"encoded   certificate   da
ta"}
}
```


Aviso: Si UEM Console está configurado para el modo COPE, se produce un error en la inscripción de los dispositivos Android 11.

Cómo inscribir un dispositivo Android en modo Perfil de trabajo

El proceso de inscripción crea una conexión entre los dispositivos Android y su entorno de AirWatch. Workspace ONE Intelligent Hub facilita el proceso de inscripción y permite la administración en tiempo real y el acceso a la información relevante del dispositivo.

Siga estas instrucciones para instalar Workspace ONE Intelligent Hub y autenticar a los usuarios según el flujo de inscripción.

1. Descargue e instale Workspace ONE Intelligent Hub desde la tienda Google Play.
2. Inicie Workspace ONE Intelligent Hub.
    1. Si ha configurado la detección automática del correo electrónico, Workspace ONE Intelligent Hub le solicitará su dirección de correo electrónico. Además, es posible que tenga que seleccionar su ID de grupo en una lista.
    2. Si no ha configurado la detección automática de correo electrónico, seleccione el método de inscripción que desee.
3. Introduzca la dirección de correo electrónico o la URL de inscripción.
4. Introduzca el Nombre de usuario y Contraseña y haga clic en Continuar.
5. Acepte los Términos de uso.
6. Haga clic en el botón Cifrar y siga las indicaciones restantes para aceptar la configuración. Workspace ONE Intelligent Hub se cerrará después de aceptar los ajustes de cifrado. Toque la notificación Cifrado completo para regresar a Workspace ONE Intelligent Hub y continuar con la inscripción.

    La opción para cifrar el dispositivo depende de la versión de Android que ejecute el dispositivo. Los dispositivos que ejecutan Android Marshmallow están cifrados por defecto, por lo que esta opción no aparecerá durante la inscripción.
7. Haga clic en Configuración para configurar el Perfil de trabajo que se va a asociar con el dispositivo.
8. Haga clic en Aceptar en la política de privacidad. Las pantallas restantes de la inscripción variarán en función de cómo se creen los usuarios. Los ajustes empresariales de la Workspace ONE UEM console se enviarán al dispositivo. En este punto finaliza el registro

de dispositivos para cuentas de Google Play administradas.

9. Únicamente para las cuentas de Google, haga clic en Primeros pasos para crear el Perfil de trabajo y conectar la cuenta de Google administrada al dispositivo. Estos pasos varían en función del método de autenticación. Para continuar con la inscripción definida por el usuario:
    1. Cree la contraseña con sus credenciales de usuario y haga clic en Siguiente.
    2. Introduzca la Contraseña de la cuenta de Google administrada y haga clic en Siguiente.
10. Para continuar con la Sincronización del servicio de directorio:
    1. Introduzca su Contraseña y toque en Siguiente.
    2. Seleccione Continuar.
    3. Seleccione Salir.
11. Para seguir el flujo de inscripción de SAML:
    1. Introduzca el Nombre de usuario y la Contraseña y haga clic en Inicio de sesión. Se redirigirá al usuario a Workspace ONE Intelligent Hub.

Si se realiza correctamente, se configurará el Perfil de trabajo para el dispositivo y se mostrará la página de ajustes de Workspace ONE Intelligent Hub. El dispositivo queda listo para su uso según los ajustes de Android para el Perfil de trabajo.

StageNow de Zebra

El cliente de inscripción preparada StageNow es la solución Android de última generación de Zebra para realizar la inscripción preparada de dispositivos Zebra y prepararlos para su uso en producción.

- Los dispositivos Zebra deben ejecutar Android 7.0 MX versión 7.1 o posterior.
- Si desea inscribir sus dispositivos Zebra con un código de barras de Stage Now, debe tener cargada la versión 8.2 o posterior de Intelligent Hub para Android en Console como el paquete de Workspace ONE Intelligent Hub.
- Los dispositivos Zebra que ejecuten Android 6.0 y versiones anteriores deben seguir usando Rapid Deployment como cliente de inscripción preparada predeterminado.
- Solo se admiten servidores de retransmisión establecidos en modo pasivo. Los servidores de retransmisión en modo activo no son compatibles y no funcionan con el cliente de StageNow.
- Asegúrese de que la opción URL de Stage Now, que se encuentra en Grupos y ajustes > Todos los ajustes > Sistema > Avanzado > URL del sitio, esté configurada en la dirección URL adecuada.
    - Si su entorno local está configurando su propio servidor de StageNow, coloque la URL personalizada en este campo.
    - Si su entorno local no está configurando su propio servidor de StageNow, solo tiene que abrir las redes para permitir el acceso a la dirección URL que se muestra aquí.
    - En los entornos de SaaS no se necesita cambiar este cuadro de texto.

- No debe haber ninguna cuenta de Google presente en el dispositivo al intentar realizar la inscripción de StageNow en el modo administrado de trabajo.

Workspace ONE UEM admite StageNow dadas las siguientes condiciones y limitaciones.

Para obtener más información sobre Mobility de Zebra, consulte Mobility Extensions y Matriz completa de funciones de MX.

Si tiene pensado inscribir dispositivos Zebra en modo de dispositivo administrado de trabajo con un código de barras de StageNow, realice los siguientes pasos.

1. Use el selector Grupo organizativo para elegir el grupo que desea configurar para sus dispositivos Android.
2. Desplácese a Grupos y ajustes > Todos los ajustes > Dispositivos y usuarios > Android > Registros de EMM de Android y seleccione la pestaña Restricciones de inscripción.
3. Realice los siguientes ajustes.

Ajustes	Descripción
Configuración actual	Seleccione Reemplazar para aplicar los cambios al grupo organizativo que seleccionó en el paso 1.
Definir el método de inscripción para este grupo organizativo	Esta opción determina cómo trata este grupo organizativo los dispositivos Android.
	Seleccione entre los siguientes ajustes:
	Siempre utilizar Android: este ajuste permite deshabilitar el control deslizante Modo de Propietario del dispositivo de la pantalla Generar un código de barra de Stage Now y hace que no se pueda editar. Esto fuerza a todos los dispositivos Android que se inscriban en este grupo organizativo a estar en Modo de Propietario del dispositivo (o en Modo Dispositivo administrado de trabajo).
	Siempre utilizar Android (heredado): este ajuste permite deshabilitar el control deslizante Modo de Propietario del dispositivo de la pantalla Generar un código de barra de Stage Now y hace que no se pueda editar. Esto fuerza a todos los dispositivos Android que se inscriban en este grupo organizativo a estar en Modo de administrador de dispositivos.
	Definir grupos de asignación que utilicen Android: esta opción permite habilitar el control deslizante Modo de Propietario del dispositivo en la pantalla Generar un código de barra de Stage Now y lo hace editable, lo que le permite que pueda optar entre la inscripción de dispositivos Android en Modo de Propietario del dispositivo (Modo Dispositivo administrado de trabajo) o la anulación de inscripción en Modo de administrador de dispositivos de acuerdo con los Grupos de asignación seleccionados.

4. Dirija al usuario final para que realice los siguientes pasos para inscribir su dispositivo:
    1. Inicie el dispositivo desde el estado "ajustes de fábrica".
    2. Asegúrese de que no haya ninguna cuenta de Google en el dispositivo.

3. Siga los pasos del asistente de instalación o escanee el código de barras "Omitir el asistente de instalación" que le haya proporcionado Zebra.
4. Abra la aplicación StageNow.
5. Escanee el código de barras.

El dispositivo se inscribe automáticamente en el modo administrado de trabajo.

Cómo configurar los perfiles de Android

Los perfiles de Android garantizan el uso adecuado de los dispositivos y la protección de datos confidenciales. Los perfiles sirven para distintos propósitos que van desde permitirle exigir reglas y procedimientos corporativos hasta adaptar y preparar los dispositivos Android para la forma en la que se utilizan.

Android en comparación con los perfiles de Android heredado

Al implementar perfiles, existen dos tipos de perfiles de Android: Android y Android (heredado). Seleccione la opción de perfil de Android si ha completado el Registro de EMM de Android. Si no ha optado por el registro de EMM, tiene a su disposición los perfiles de Android (heredado). Si selecciona Android pero no ha llevado a cabo el registro de EMM de Android, aparece un mensaje de error que le pide que vaya a la página de configuración para completar el registro de EMM, o bien que continúe con la implementación del perfil de Android (heredado).

Modo de Perfil de trabajo frente a Dispositivo administrado de trabajo

Un perfil de trabajo es un tipo especial de administrador adaptado principalmente para un caso de uso de BYOD. Cuando el usuario ya tiene un dispositivo personal configurado con su propia cuenta de Google, la inscripción de Workspace ONE UEM crea un perfil de trabajo, donde instalará Workspace ONE Intelligent Hub. Workspace ONE UEM solo controla el perfil de trabajo. Las aplicaciones administradas se instalan dentro del perfil de trabajo y muestran una insignia de maletín naranja para diferenciarlas de las aplicaciones personales.

El dispositivo con la cuenta administrada de trabajo se aplica a los dispositivos que se inscriben desde un estado sin aprovisionar (restablecimiento de fábrica), recomendado para aquellos dispositivos propiedad de la empresa. Workspace ONE Intelligent Hub se instala durante el proceso de instalación y se configura como el propietario del dispositivo, lo que significa que Workspace ONE UEM tendrá el control total de todo el dispositivo.

Los perfiles de Android mostrarán las siguientes etiquetas: Perfil de trabajo y Dispositivo administrado de trabajo.

Las opciones de perfil con la etiqueta Perfil de trabajo solo se aplican a los ajustes y aplicaciones del perfil de trabajo y no afectan a las aplicaciones o ajustes personales del usuario. Por ejemplo, algunas restricciones deshabilitan el acceso a la cámara o la realización de capturas de pantalla. Estas restricciones solo afectan a las aplicaciones de insignia de Android que se encuentran dentro del perfil de trabajo y no afectarán a las aplicaciones personales. Las opciones de perfil configuradas para el Dispositivo administrado de trabajo se aplican a todo el dispositivo. Cada perfil que se describe en esta sección indica a qué tipo de dispositivo afecta el perfil.

Comportamiento de los perfiles

En ocasiones, es necesario implementar más de un perfil por diversos motivos. Cuando se implementan perfiles duplicados, la política más restrictiva tiene prioridad. Por lo tanto, si hay dos perfiles instalados, y uno de ellos indica que se bloquee la cámara y el otro indica que se permita la

cámara, Intelligent Hub for Android combina los perfiles y bloquea la cámara para elegir así la opción más segura.

configurar perfil

En Workspace ONE UEM Console, siga la misma ruta de navegación para cada perfil. La sección Vista previa muestra el Total de dispositivos asignados en una vista de lista. Puede ver los perfiles agregados en la pestaña Resumen.

Para configurar perfiles:

1. Desplácese a Dispositivos > Perfiles y recursos > Perfiles > Agregar > Agregar perfil > Android.
2. Configure los ajustes:

Ajustes	Descripción
Nombre	Establezca el nombre para su perfil y añada una descripción que le sea fácil de identificar.
Ámbito del perfil	Establezca cómo se utilizará el perfil en el entorno, ya sea en Producción, Provisional o Ambos.
Configuración de OEM	Active Ajustes de OEM para configurar ajustes específicos para los dispositivos Samsung o Zebra. Una vez que seleccione el OEM, verá los perfiles y ajustes adicionales que son exclusivos de cada OEM.

3. Seleccione el botón Añadir para el perfil deseado y configure los ajustes según sus preferencias. Puede utilizar los ajustes del perfil desplegable y de vista previa antes de seleccionar la opción de agregar.
4. Seleccione Siguiente para configurar los ajustes generales Asignación e Implementación del perfil según corresponda. Configure los siguientes ajustes:

Ajustes	Descripción
Grupo inteligente	
Permitir exclusión	Cuando esta opción está activada, aparece un nuevo cuadro Excluir grupo. Este cuadro le permite seleccionar aquellos grupos que desee excluir de la asignación del perfil de dispositivo.
Tipo de asignación	Determina la manera en que se implementará el perfil en los dispositivos: Automático: – – eEl perfil se implementará en todos los dispositivos. Opcional: Un usuario final puede optar por instalar el perfil desde el portal de autoservicio (SSP), o se puede implementar en cada dispositivo según el criterio del administrador. Los usuarios finales también pueden instalar perfiles que representen aplicaciones web, mediante la carga útil de un marcador o un web clip. Además, si configura la carga útil de forma que se muestre en el catálogo de aplicaciones, puede instalarla desde el mismo catálogo. Conformidad: el perfil se aplica al dispositivo mediante el motor de conformidad cuando el usuario no toma medidas correctivas para que su dispositivo esté en estado de conformidad.
Administrado por	El grupo organizativo con acceso administrativo al perfil.

Ajustes	Descripción
Instalación solamente por área	Active esta opción para mostrar la opción de geolocalización: Instalar solo en los dispositivos dentro de las zonas seleccionadas: Introduzca una dirección cualquiera de todo el planeta y un radio en kilómetros o millas para generar un perímetro de instalación de perfiles.
Programar la hora de instalación	Active esta opción para configurar los ajustes de programación: Activar la programación e instalar solo durante los periodos de tiempo seleccionados: especifique un horario configurado para que los dispositivos reciban el perfil solo en ese periodo de tiempo.

5. Seleccione Guardar y publicar.

Contraseña

La configuración de una política de código de acceso obliga a los usuarios finales a introducir un código de acceso, proporcionando así una primera capa de defensa para los datos confidenciales de los dispositivos.

Las políticas de código de acceso de perfil de Work se aplican únicamente a las aplicaciones corporativas para que los usuarios no tengan que introducir contraseñas complejas cada vez que desbloquean su dispositivo si están inscritos con un perfil de Work. Work mantiene la protección de los datos de la aplicación corporativa y permite que los usuarios finales accedan a las aplicaciones y datos personales de la manera que deseen. Para los dispositivos administrados de trabajo, esta política de código de acceso se aplica al dispositivo. El Código de acceso de Work está disponible en Android 7.0 (Nougat) y versiones posteriores para los dispositivos inscritos de Perfil de trabajo.

Las políticas de código de acceso del dispositivo se aplican a todo el dispositivo (inscritos con un perfil de Work o como administrado de Work). Este código de acceso debe introducirse cada vez que el dispositivo se desbloquea, y puede aplicarse además del código de acceso de Work.

De forma predeterminada, al crear perfiles nuevos, solo se activará el código de acceso de trabajo (se deshabilitará el código de acceso del dispositivo). El administrador tiene que activar el código de acceso del dispositivo de forma manual.

Aviso: Cuando el perfil de código de acceso está presente en el dispositivo y el usuario no establece el código de acceso, no se insertan aplicaciones ni perfiles en el dispositivo hasta que el dispositivo sea conforme.

Una vez que se establecen los ajustes del perfil de código de acceso, UEM Console notifica al usuario a través de una notificación persistente para actualizar los ajustes del código de acceso cuando dicho código alcanza la antigüedad mínima o requiere un cambio. Los usuarios no pueden utilizar Intelligent Hub hasta que configuran el código de acceso que se requiere en el perfil. En los dispositivos Samsung, el usuario queda bloqueado en el asistente de configuración de la pantalla de bloqueo hasta que establezca un código de acceso que cumpla con los requisitos de la directiva de código de acceso. Para los dispositivos administrados de trabajo, los usuarios no pueden utilizar el dispositivo. En el caso del perfil de trabajo y los dispositivos COPE, los usuarios no pueden acceder a las aplicaciones de trabajo.

A continuación se detallan los ajustes disponibles para el perfil Código de acceso.

Ajustes	Descripción
Activar la directiva de código de acceso de trabajo	Active esta opción para aplicar directivas de código de acceso únicamente a las aplicaciones distintivas de Android.
Longitud mínima del código de acceso	Establezca un número mínimo de caracteres para garantizar que los códigos de acceso sean lo suficientemente complejos.
Contenido de código de acceso	Asegúrese de que el contenido del código de acceso cumpla con sus requisitos de seguridad seleccionando para ello una de las siguientes opciones:Cualquiera, Numérico, Alfanumérico, Alfabético, Complejo, Complejo numérico o Biométrico débil en el menú desplegable.
	Utilice valores simples para acceder rápidamente o códigos de acceso alfanuméricos para mayor seguridad. También puede requerir un número mínimo de caracteres complejos (por ejemplo, @, #, &,! , ,?) para el código de acceso.
	El contenido de código de acceso con biométrica débil permite métodos de desbloqueo biométrico de seguridad baja, como el reconocimiento facial. Importante: Si el número mínimo de caracteres complejos de la contraseña es mayor que 4, se requiere al menos una letra minúscula y una mayúscula (solo en dispositivos SAFE v5.2).
Número máximo de intentos fallidos	Especifique el número de intentos permitidos antes de eliminar el contenido del dispositivo.
Vigencia máxima del código de acceso (días)	Especifique el número máximo de días que el código de acceso puede estar activo.
Alerta de cambio de código de acceso	Establezca la cantidad de tiempo antes de que caduque el código de acceso con que se le notifica al usuario que debe cambiarlo. Esta opción también está disponible en la directiva de código de acceso de dispositivos. Se le pedirá al usuario que cambie el código de acceso a través de un aviso en el dispositivo, pero podrá continuar con la realización de otras funciones en el dispositivo. Puede configurar una política de conformidad o utilizar los ajustes de Workspace ONE Intelligent Hub for Android para crear y exigir que el código de acceso se vuelva a agregar al dispositivo.
Historial del código de acceso	Especifique el número de veces que un código de acceso debe cambiarse antes de que un código de acceso anterior se pueda utilizar de nuevo.
Intervalo de tiempo de espera de bloqueo del perfil de trabajo (en minutos)	Configure el periodo de inactividad antes de que se bloquee automáticamente la pantalla del dispositivo.

Ajustes	Descripción
Intervalo de solicitud de contraseña (en minutos)	Configure la cantidad de tiempo después de desbloquear un dispositivo con un método de autenticación no seguro (por ejemplo, mediante huella digital o reconocimiento facial) antes de que se requiera un código de acceso. Esta opción también está disponible en la directiva de código de acceso de dispositivos.
Permitir Un bloqueo	Deshabilite esta opción para forzar un código de acceso independiente y más restrictivo para el código de acceso del perfil de trabajo y el código de acceso del dispositivo.
	La opción Un bloqueo está activada en segundo plano hasta que se crea un código de acceso del perfil de trabajo. Cuando los usuarios necesitan crear un código de acceso del dispositivo y del perfil de trabajo, el usuario puede elegir cuál crear en primer lugar, pero primero se aplicarán los requisitos más complejos.
	Aviso: Se aplica solo a dispositivos con Android 9.0 o posterior con perfil de trabajo y dispositivos COPE.
Permitir opciones biométricas	Active esta opción para permitir métodos de desbloqueo biométrico, como el reconocimiento facial.
Permitir sensor de huella digital	Active esta opción para permitir que los usuarios desbloqueen los dispositivos mediante la huella digital. Deshabilite esta opción para evitar el uso de su huella digital como método principal de autenticación y, en su lugar, exigir a los usuarios finales que introduzcan el tipo especificado de contraseña en el perfil.
Permitir escaneo facial	Deshabilite esta opción para impedir que el desbloqueo por reconocimiento facial se configure o se seleccione.Nota: Se aplica solo a los dispositivos administrados para el trabajo de Android 9.0+.
Permitir escaneo de iris	Deshabilite esta opción para impedir que el método de escáner de iris se configure o se seleccione.Nota: Se aplica solo a los dispositivos administrados para el trabajo de Android 9.0+.
Activar la directiva de código de acceso del dispositivo	Aplique las políticas de código de acceso para el dispositivo inscrito con un Perfil de trabajo. Este código de acceso deberá introducirse para desbloquear el dispositivo, y puede aplicarse además del código de acceso de trabajo. Para los dispositivos administrados de trabajo, esta política de código de acceso se aplica al dispositivo.
Longitud mínima del código de acceso	Establezca un número mínimo de caracteres para garantizar que los códigos de acceso sean lo suficientemente complejos.
Establecer el código de acceso inicial	Active esta opción para establecer un código de acceso inicial a nivel de dispositivo en todos los dispositivos implementados. Después de la implementación, se puede restablecer el código de acceso en el dispositivo. Aviso: Se aplica solo a los dispositivos administrados para el trabajo de Android 7.0+.
Contenido de código de acceso	Asegúrese de que el contenido del código de acceso cumpla con sus requisitos de seguridad al seleccionar una de las siguientes opciones desde el menú desplegable: Cualquiera, Numérico, Alfanumérico, Alfabético, Complejo o Numérico complejo.
Número máximo de intentos fallidos	Especifique el número de intentos permitidos antes de eliminar el contenido del dispositivo.

Ajustes	Descripción
Vigencia máxima del código de acceso (días)	Especifique el número máximo de días que el código de acceso puede estar activo.
Alerta de cambio de código de acceso	Establezca la cantidad de tiempo antes de que caduque el código de acceso con que se le notifica al usuario que debe cambiarlo.
Historial del código de acceso	Especifique el número de veces que un código de acceso debe cambiarse antes de que un código de acceso anterior se pueda utilizar de nuevo.
Intervalo de tiempo de espera de bloqueo del perfil de trabajo (en minutos)	Configure el periodo de inactividad antes de que se bloquee automáticamente la pantalla del dispositivo.
Permitir opciones biométricas	Active esta opción para permitir métodos de desbloqueo biométrico, como el reconocimiento facial.
Permitir el desbloqueo con la huella digital	Active esta opción para permitir que los usuarios desbloqueen los dispositivos mediante la huella digital, evitar que utilicen la huella digital como método principal de autenticación y, en su lugar, exigir a los usuarios finales que introduzcan el tipo especificado de contraseña en el perfil.
Permitir escaneo facial	Inhabilite esta opción para impedir que el desbloqueo por reconocimiento facial se configure o seleccione en el dispositivo Samsung.Nota: Se aplica solo a los dispositivos administrados para el trabajo de Android 9.0+.
Permitir escaneo de iris	Inhabilite esta opción para impedir que el escáner de iris se configure o seleccione en el dispositivo Samsung.Nota: Se aplica solo a los dispositivos administrados para el trabajo de Android 9.0+.
Código de acceso visible	Active esta opción para mostrar el código de acceso en la pantalla a medida que se introduce. Para dispositivos Samsung. Es necesario activar Ajustes de OEM en el perfil General y Samsung en el menú desplegable Seleccionar OEM.
Requerir el cifrado de la tarjeta SD	Indique si la tarjeta SD requiere cifrado. Para dispositivos Samsung, es necesario activar Ajustes de OEM en el perfil General y Samsung en el menú desplegable Seleccionar OEM.
Secuencia máxima de caracteres repetidos	Evite que los usuarios finales introduzcan códigos de acceso repetitivos fáciles de descubrir (por ejemplo "1111") mediante el establecimiento de un número máximo de caracteres repetidos. Para dispositivos Samsung.

Si selecciona Complejo en el cuadro de texto Contenido del código de acceso, se aplican los siguientes ajustes.

Ajustes	Descripción
Número mínimo de letras	Especifique el número de letras que pueden incluirse en el código de acceso.
Número mínimo de minúsculas	Especifique el número de letras en minúscula necesarias en el código de acceso.
Número mínimo de mayúsculas	Especifique el número de letras en mayúsculas necesarias en el código de acceso.
Número mínimo de caracteres que no son letras	Especifique el número de caracteres especiales necesarios en el código de acceso.
Número mínimo de dígitos numéricos	Especifique el número de dígitos numéricos necesarios en el código de acceso.
Número mínimo de símbolos	Especifique el número de símbolos necesarios en el código de acceso.

Los siguientes ajustes se aplican al configurar un código de acceso en un dispositivo Samsung.

Estas opciones solo se muestran cuando los Ajustes de OEM en el perfil General y en Samsung en el menú desplegable Seleccionar OEM están seleccionados.

Ajustes	Descripción
Código de acceso visible	Active esta opción para mostrar el código de acceso en la pantalla a medida que se introduce.
Permitir el desbloqueo con la huella digital	Active esta opción para permitir que los usuarios desbloqueen los dispositivos mediante la huella digital, evitar que utilicen la huella digital como método principal de autenticación y, en su lugar, exigir a los usuarios finales que introduzcan el tipo especificado de contraseña en el perfil.
Requerir cifrado de la tarjeta SD	Indique si la tarjeta SD requiere cifrado.
Requerir código de acceso	Requiere que el usuario introduzca el código de acceso para cifrar la tarjeta SD. Si se deja sin marcar, algunos dispositivos permiten que la tarjeta SD se cifre sin la interacción del usuario.
Secuencia máxima de caracteres repetidos	Evite que los usuarios finales introduzcan códigos de acceso repetitivos fáciles de descubrir (por ejemplo "1111") mediante el establecimiento de un número máximo de caracteres repetidos.
Longitud máxima de las secuencias numéricas	Establezca esta opción para evitar que el usuario final introduzca como código de acceso secuencias numéricas fáciles de descubrir, como “1234”. Para dispositivos Samsung.
Habilitar el escáner de iris	Inhabilite esta opción para impedir que el escáner de iris se configure o seleccione en el dispositivo Samsung.
Permitir desbloqueo facial	Inhabilite esta opción para impedir que el desbloqueo por reconocimiento facial se configure o seleccione en el dispositivo Samsung.

Ajustes	Descripción
Superposición de la pantalla de bloqueo	Active esta opción para enviar información a los dispositivos de usuario final y mostrarla sobre la pantalla de bloqueo.
	- Superposición de imagen: cargue imágenes para mostrarlas sobre la pantalla bloqueada. Puede cargar imágenes principales y secundarias, y determinar tanto la posición como la transparencia de las imágenes.
	- Información de compañía: especifique la información de la compañía para que aparezca en la pantalla bloqueada. Esta opción puede utilizarse para mostrar información de emergencia si el dispositivo se pierde o es objeto de robo.
	El ajuste "Superposición de la pantalla de bloqueo" solo está disponible en dispositivos Safe 5.0 y superior. El ajuste “Superposición de la pantalla de bloqueo” permanece configurado en el dispositivo mientras esté en uso y el usuario final no podrá modificarlo.

Cómo configurar la superposición de la pantalla de bloqueo (Android)

La opción Superposición de la pantalla de bloqueo del perfil de código de acceso le ofrece la posibilidad de superponer información sobre la imagen de la pantalla de bloqueo para proporcionar información al usuario final o a cualquiera que pueda encontrar un dispositivo bloqueado. La superposición de la pantalla de bloqueo es una parte del perfil de código de acceso.

La superposición de la pantalla de bloqueo es una funcionalidad nativa de Android y está disponible a través de varios OEM.

Los ajustes de Superposición de la pantalla de bloqueo para los perfiles de Android solo aparecen cuando el campo Ajustes de OEM está Activado y se ha seleccionado Samsung en el campo Seleccionar OEM. El campo de configuración de OEM en el perfil General solo se aplica a los perfiles de Android y no a las configuraciones de Android (heredado).

Configure los ajustes de Superposición de imagen según desee:

Ajustes	Descripción
Tipo de superposición de la imagen	Seleccione Imagen única o Imagen múltiple para determinar el número de imágenes de superposición requerido.
Imagen principal	Cargue un archivo de imagen.
Posición superior de imagen principal en porcentaje	Determine la posición de la imagen superior desde 0 hasta el 90 por ciento.
Posición inferior de imagen principal en porcentaje	Determine la posición de la imagen inferior desde 0 hasta el 90 por ciento.
Segunda imagen	Cargue una segunda imagen, si lo desea. Este campo solo se muestra si se ha seleccionado “Imagen múltiple” en el campo Tipo de superposición de la imagen.
Posición de la segunda imagen en porcentaje	Determine la posición de la imagen superior desde 0 hasta el 90 por ciento. Solo se aplica si se ha seleccionado “Imagen múltiple” en el campo Tipo de superposición de la imagen.
Posición inferior de la imagen secundaria en porcentaje	Determine la posición de la imagen inferior desde 0 hasta el 90 por ciento. Solo se aplica si se ha seleccionado “Imagen múltiple” en el campo Tipo de superposición de la imagen.

Ajustes	Descripción
Imagen de superposición	Determine la transparencia de su imagen como Transparente u Opaco.

Configure los ajustes de Información de compañía como desee.

Ajustes	Descripción
Nombre de la empresa	Introduzca el nombre de la compañía que desee mostrar.
Logotipo de la empresa	Cargue el logotipo de la empresa en un archivo de imagen.
Dirección de la compañía	Introduzca la dirección de la oficina de la empresa.
Número telefónico de la empresa	Introduzca el número de teléfono de la empresa.
Imagen de superposición	Determine la transparencia de su imagen como Transparente u Opaco.

Ajustes del navegador Chrome

El perfil Ajustes del navegador Chrome le ayuda a administrar la configuración de la aplicación Chrome de trabajo.

Chrome es el navegador web de Google. Chrome ofrece una serie de funciones, como búsqueda, omnibox (una casilla para buscar y navegar), autocompletar, almacenamiento de contraseñas e inicio de sesión en cuentas de Google para acceder de forma instantánea a las pestañas y búsquedas recientes en todos sus dispositivos. La aplicación Chrome de trabajo funciona del mismo modo que la versión personal de Chrome. Configurar este perfil no afectará a la aplicación personal de Chrome del usuario. Puede enviar este perfil junto con una VPN independiente o carga útil de credenciales + Wi-Fi para garantizar que los usuarios finales puedan autenticarse y acceder a los sistemas y sitios internos. Esto garantiza que los usuarios tengan que usar la aplicación de Chrome de trabajo para fines empresariales.

Matriz de ajustes del navegador Chrome (Android)

El perfil Ajustes del navegador Chrome le ayuda a administrar la configuración de la aplicación Chrome de trabajo. Configurar este perfil no afectará a la aplicación personal de Chrome del usuario. Puede enviar este perfil junto con una VPN independiente o carga útil de credenciales + Wi-Fi para garantizar que los usuarios finales puedan autenticarse y acceder a los sistemas y sitios internos.

Esta matriz detalla los ajustes disponibles en el perfil del navegador Chrome:

Ajustes	Descripción
**Permitir cookies	Seleccione esta opción para determinar los ajustes de las cookies del navegador.**
Permitir cookies en estos sitios web	Especifique las direcciones URL a las que se les permite el uso de cookies.
Bloquear cookies en estos sitios web	Especifique las direcciones URL a las que no se les permite el uso de cookies.
Permitir cookies solo para sesiones en estos sitios web	Especifique las direcciones URL a las que se les permite el uso de cookies solo para sesiones.

Ajustes	Descripción
**Permitir imágenes	Seleccione esta opción para determinar qué sitios pueden mostrar imágenes.
Permitir imágenes en estos sitios web	Especifique una lista de direcciones URL a las que se les permite mostrar imágenes.
Bloquear imágenes en estos sitios web	Especifique una lista de direcciones URL a las que no se les permite mostrar imágenes.
Permitir JavaScript	Seleccione los ajustes del navegador de JavaScript.
Permitir JavaScript en estos sitios web	Especifique los sitios que pueden ejecutar JavaScript.
Bloquear JavaScript en estos sitios web	Especifique los sitios que no pueden ejecutar JavaScript.
Permitir ventanas emergentes	Seleccione los ajustes del navegador para permitir ventanas emergentes.
Permitir elementos emergentes en estos sitios web	Seleccione la opción para determinar qué sitios tienen permiso para abrir ventanas emergentes.
Bloquear elementos emergentes en estos sitios web	Especifique los sitios que no pueden abrir ventanas emergentes.
Permitir rastrear ubicación	Defina si los sitios web pueden rastrear la ubicación física de los usuarios.
Modo Proxy	Especifique el servidor de proxy utilizado por Google Chrome y evite que los usuarios cambien los ajustes de proxy.
Dirección URL del servidor proxy	Especifique la dirección URL del servidor proxy.
URL de archivo PAC de proxy	Especifique una dirección URL para un archivo .pac de proxy.
Reglas de circunvalación del proxy	Especifique qué ajustes de proxy circunvalar. Esta directiva solo tiene efecto si ha seleccionado ajustes de proxy manuales.
Forzar Google SafeSearch	Active esta opción para forzar que las consultas de búsqueda en Google Web Search se realicen con SafeSearch.
**Forzar modo de seguridad de YouTube	Active esta opción para proporcionar a los usuarios la oportunidad de bloquear contenido explícito.
Activar Tocar para buscar	Active esta opción para utilizar Tocar para buscar en la vista de contenido de Google Chrome.
Activar proveedor de búsqueda predeterminado	Especifique el proveedor predeterminado de búsqueda.
Nombre del proveedor predeterminado de búsqueda	Especifique el nombre del proveedor predeterminado de búsqueda.

Ajustes	Descripción
Palabra clave del proveedor predeterminado de búsqueda	Especifique la palabra clave del proveedor predeterminado de búsqueda.
Dirección URL del proveedor predeterminado de búsqueda	Especifique la dirección URL del motor de búsqueda que se utiliza cuando se realiza una búsqueda de forma predeterminada.
Dirección URL sugerida del proveedor predeterminado de búsqueda	Especifique la dirección URL del motor de búsqueda que se utiliza para realizar sugerencias de búsqueda.
Dirección URL instantánea del proveedor predeterminado de búsqueda	Especifique los proveedores de búsqueda predeterminados cuando el usuario introduzca las consultas de búsqueda.
Icono del proveedor predeterminado de búsqueda	Especifique la dirección URL del icono del proveedor predeterminado de búsqueda.
Codificaciones del proveedor predeterminado de búsqueda	Especifique la codificación de caracteres admitida por el proveedor de búsqueda. Las codificaciones son nombres de la página de código, como UTF-8, GB2312 e ISO-8859-1. Si no se definen, se usará la predeterminada, es decir, UTF-8.
Lista de direcciones URL alternativas para el proveedor de búsqueda predeterminado	Especifique una lista de direcciones URL alternativas que puede utilizarse para extraer los términos de búsqueda del motor de búsqueda.
Buscar la clave de reemplazo de términos	Introduzca todas las claves de sustitución de términos de búsqueda.
Buscar la dirección URL de imágenes del proveedor de búsqueda	Especifique la dirección URL del motor de búsqueda que se utiliza para buscar imágenes.
URL de pestaña nueva	Especifique la dirección URL que utiliza el motor de búsqueda para abrir una página en una nueva pestaña.
Parámetros de búsqueda de la dirección URL de POST	Especifique los parámetros utilizados cuando se utiliza una dirección URL con POST.
Parámetros de búsqueda de sugerencias de POST	Especifique los parámetros utilizados cuando se realiza una búsqueda de imágenes con POST.

Ajustes	Descripción
Parámetros de búsqueda de imágenes de POST	Especifique los parámetros utilizados cuando se realiza una búsqueda de imágenes con POST.
Activar Administrador de contraseñas	Active la opción de guardar contraseñas del Administrador de contraseñas.
Activar páginas de error alternativas	Active esta opción para utilizar páginas de error alternativas integradas en Google Chrome (por ejemplo, "No se encontró la página").
Activar Autocompletar	Active esta opción para permitir que los usuarios completen automáticamente los formularios web a partir de la información guardada previamente, como la dirección o los datos de la tarjeta de crédito.
Activar impresión	Active esta opción para permitir la impresión en Google Chrome.
Activar la función de proxy de compresión de datos	Especifique una de las siguientes opciones para el proxy de compresión de datos: Activar siempre, Desactivar siempre. El proxy de compresión de datos puede reducir el uso de datos celulares y acelerar la navegación web móvil mediante el uso de servidores proxy alojados en Google para optimizar el contenido de los sitios web.
Activar Navegación segura	Active esta opción para activar la función Navegación segura de Google Chrome.
Deshabilitar la opción de guardar el historial del navegador	Active esta opción para deshabilitar el guardado del historial del navegador en Google Chrome.
Impedir el acceso tras la advertencia de navegación segura	Active esta opción para impedir que los usuarios accedan a sitios malintencionados desde de la página de advertencia.
Inhabilitar protocolo SPDY	Deshabilite el uso del protocolo SPDY en Google Chrome
Activar la predicción de red	Seleccione esta opción para permitir la predicción de red en Google Chrome.
Activar funciones obsoletas de la plataforma web temporalmente	Especifique una lista de funciones obsoletas de la plataforma web para volver a activarlas temporalmente.
Exigir búsqueda segura	Active esta opción para activar la búsqueda segura mientras utiliza el navegador web.
"Capacidad de ""Modo incógnito"""	Especifique si el usuario puede abrir las páginas en modo incógnito en Google Chrome.
Permitir el inicio de sesión en Chromium	Active esta opción para forzar a los usuarios de Chrome a iniciar sesión en el navegador si han iniciado sesión en Gmail en la web.
Activar sugerencias de búsqueda	Active las sugerencias de búsqueda en la omnibox de Google Chrome.
Activar Traductor	Active el servicio Traductor de Google integrado en Google Chrome.
Activar o desactivar la edición de marcadores	Active esta opción para permitir la adición, eliminación o modificación de marcadores.

Ajustes	Descripción
Marcadores administrados	Especifique una lista de marcadores administrados.
Bloquear acceso a una lista de direcciones URL	Introduzca la URL para evitar que el usuario cargue páginas web incluidas en la lista negra de direcciones URL.
Excepciones de la lista de URL bloqueadas	Introduzca las URL de excepciones de la lista de bloqueados. Puede separar la lista con comas.
Activar la versión mínima de SSL	Seleccione la versión mínima de SSL del menú desplegable.
Versión mínima de SSL a la que se puede recurrir	Seleccione la versión mínima de SSL a la que se puede recurrir del menú desplegable.

Restricciones

Los perfiles de restricciones en UEM Console bloquean la funcionalidad nativa de los dispositivos Android. Las restricciones disponibles y el comportamiento varían en función de la inscripción del dispositivo.

El perfil Restricciones muestra etiquetas que indican si se aplica la restricción seleccionada al Perfil de trabajo, al Dispositivo administrado de trabajo o a ambos; sin embargo, en el caso de los dispositivos del Perfil de trabajo estas solo afectan a aplicaciones distintivas de Android. Por ejemplo, al configurar restricciones para el Perfil de trabajo puede deshabilitar el acceso a la cámara de trabajo. Esto afecta únicamente a la cámara distintiva de Android y no a la cámara personal del usuario.

Tenga en cuenta que el Perfil de trabajo incluye por defecto una serie de aplicaciones del sistema, como Chrome de trabajo, Google Play, ajustes de Google, Contactos y Cámara; estas aplicaciones se pueden ocultar mediante el perfil de restricciones sin que esto afecte a la cámara personal del usuario.

Restricciones en el uso de cuentas de Google sin administrar

Puede que desee permitir a los usuarios agregar cuentas de Google personales o sin administrar, para leer, por ejemplo, los correos electrónicos personales, pero que al mismo tiempo se restrinja la instalación de aplicaciones en el dispositivo. Puede configurar una lista de cuentas que los usuarios puedan usar en Google Play en Workspace ONE UEM Console.

Implemente una carga útil de restricciones para proporcionar una mayor protección a los dispositivos Android. Los dispositivos de cargas útiles de restricciones pueden deshabilitar el acceso de los usuarios finales a las funciones del dispositivo para asegurarse de que no se manipulen los dispositivos.

Seleccione el perfil de Restricciones y configure los ajustes:

Ajustes	Descripción

Funcionalidad del dispositivo	Las restricciones a nivel del dispositivo pueden inhabilitar funcionalidades principales del dispositivo, como el uso de la cámara, las capturas de pantalla y el restablecimiento de fábrica, para mejorar la productividad y la seguridad. Por ejemplo, la inhabilitación de la cámara evita que los materiales confidenciales se fotografíen y transmitan fuera de su organización. La prohibición de las capturas de pantalla del dispositivo protege la confidencialidad del contenido corporativo en el dispositivo.
Aplicación	Las restricciones a nivel de las aplicaciones pueden deshabilitar determinadas aplicaciones tales como YouTube y el navegador nativo, lo cual le permite exigir el seguimiento de las directivas corporativas para el uso de dispositivos.
Sincronización y almacenamiento	Controle la forma en la que la información se almacena en los dispositivos, lo que le permitirá mantener el máximo equilibrio entre productividad y seguridad. Por ejemplo, la inhabilitación de la copia de seguridad en Google o USB mantiene los datos móviles corporativos contenidos en cada dispositivo administrado y fuera de las manos equivocadas.
Red	Evite que los dispositivos accedan a redes Wi-Fi y a conexiones de datos para garantizar que los usuarios finales no vean información confidencial a través de una conexión que no sea segura.
Trabajo y personal	Determine cómo se accede a la información o se comparte esta entre el contenedor personal y el contenedor de trabajo. Esta configuración se aplica únicamente al modo Perfil de trabajo.
Servicios de ubicación	Configure los ajustes de Servicios de ubicación para los dispositivos administrados de trabajo. Esta restricción se comporta de forma diferente entre distintas versiones de Android. En Android 8.0 y versiones anteriores, el comportamiento funciona de acuerdo con la configuración seleccionada en UEM Console. En Android 9.0 y versiones posteriores, cada configuración activa o desactiva los servicios de ubicación de la siguiente manera:Ninguna no hace nada. No permitir acceso a ninguna ubicación: desactiva los servicios de ubicación, Establecer ubicación de GPS solamente: activa los servicios de ubicación. Establecer la ubicación de ahorro de batería solamente: desactiva los servicios de ubicación. Establecer la ubicación de alta precisión solamente: desactiva los servicios de ubicación.
Samsung Knox	Configure restricciones específicas para dispositivos Android que ejecuten Samsung Knox. Esta sección solo está disponible cuando el campo Ajustes de OEM está activado en el perfil General y se ha seleccionado Samsung en el campo Seleccionar OEM.

Restricciones específicas para Android

Esta matriz proporciona un panorama representativo de las configuraciones de perfiles de restricción disponibles según el tipo de propiedad del dispositivo.

Función	Modo Dispositivo administrado de trabajo	Modo Perfil de trabajo
Funcionalidad del dispositivo		
Permitir el restablecimiento de fábrica	✓	✓
Permitir la captura de pantalla	✓	✓
Permitir agregar cuentas de Google	✓	✓
Permitir la eliminación de cuentas de Android Work	✓	
Permitir llamadas de teléfono salientes	✓	

Función	Modo Dispositivo administrado de trabajo	Modo Perfil de trabajo
Permitir que se envíen/reciban mensajes SMS	✓	
Permitir cambios de credenciales	✓	
Permitir todas las funciones de la pantalla de bloqueo	✓	
Permitir el uso de la cámara en la pantalla de bloqueo	✓	
Permitir las notificaciones en la pantalla de bloqueo	✓	
Permitir el identificador de huellas en pantalla de bloqueo	✓	✓
Permitir el estado de Hub de confianza en la pantalla de bloqueo	✓	✓
Permitir notificaciones completas en la pantalla de bloqueo	✓	✓
Forzar Pantalla activa al conectar con el cargador AC (Android 6.0 o superior)	✓	
Forzar Pantalla activa al conectar con el cargador USB (Android 6.0 superior)	✓	
Forzar Pantalla activa al conectar con el cargador inalámbrico (Android 6.0 o superior)	✓	
Permitir cambio de fondo de pantalla (Android 7.0 o superior)	✓	
Permitir barra de estado	✓	
Permitir pantalla de bloqueo (Android 6.0 o superior)	✓	
Permitir Agregar usuarios		
Permitir Eliminación de usuarios		
Permitir arranque seguro (Android 6.0 o superior)	✓	
Permitir cambio de fondo de pantalla (Android 7.0 o superior)		
Permitir cambio de icono de usuario (Android 7.0 o superior)	✓	✓
Permitir agregar/eliminar cuentas	✓	✓
Impedir el uso de la IU del sistema (avisos, actividades, alertas, errores, superposiciones, etc.)	✓	
Establecer el número máximo de días para deshabilitar el perfil de trabajo		✓
Aplicación		
Permitir cámara	✓	✓
Permitir Google Play	✓	✓
Permitir el navegador Chrome	✓	
Permitir la instalación de aplicaciones que no están en la tienda Google Play	✓	✓
Permitir modificación de aplicaciones en Ajustes	✓	
Permitir la instalación de aplicaciones	✓	✓

Función	Modo Dispositivo administrado de trabajo	Modo Perfil de trabajo
Permitir la desinstalación de aplicaciones	✓	✓
Permitir la verificación de inhabilitación de aplicaciones	✓	✓
Omitir el tutorial de usuario y las sugerencias introductorias	✓	✓
Permitir servicios de accesibilidad en la lista blanca	✓	
Restringir métodos de entrada	✓	✓
Sincronización y almacenamiento		
Permitir depuración USB	✓	
Permitir el almacenamiento en masa de USB✓		
Permitir el montaje de medios físicos de almacenamiento	✓	
Permitir transferencia USB de archivos	✓	
Permitir servicio de copia de seguridad (Android 8.0 o superior)		
Red		
Permitir cambios de Wi-Fi	✓	
Permitir el emparejamiento de Bluetooth	✓	
Permitir Bluetooth (Android 8.0 o superior)	✓	
Permitir uso compartido de contacto de Bluetooth (Android 8.0 o superior)*	✓	
Permitir conexiones salientes de Bluetooth*	✓	✓
Permitir anclaje de red	✓	
Permitir cambios VPN	✓	
Permitir cambios en la red móvil	✓	
Permitir NFC	✓	
Permitir cambios en el perfil de administración Wi-Fi (Android 6.0 o superior)	✓	
Trabajo y personal		

Permitir que se copie un portapapeles entre las aplicaciones personales y de trabajo	✓
Permitir que las aplicaciones de trabajo accedan a documentos de las aplicaciones personales	✓
Permitir que las aplicaciones personales accedan a documentos de las aplicaciones de trabajo	✓
Permitir que las aplicaciones personales compartan documentos con las aplicaciones de trabajo	✓
Permitir que las aplicaciones de trabajo compartan documentos con aplicaciones personales	

Función	Modo Dispositivo administrado de trabajo	Modo Perfil de trabajo
Permitir que la información del ID de llamada de contactos de trabajo se muestre en el marcador telefónico		✓
Permitir que los widgets de trabajo sean agregados a la pantalla principal personal		✓
Permitir contactos de trabajo en la aplicación de contactos personales (Android 7.0 o superior)		
Acceso al calendario entre perfiles (permite a los desarrolladores de aplicaciones de calendario de Android tener acceso a la información del calendario del perfil de trabajo mediante las API de Android 10. No se puede garantizar la compatibilidad de cada aplicación de calendario con estos métodos específicos de Android 10).		✓
Permitir la comunicación de aplicaciones entre perfiles		✓
Servicios de ubicación		
Permitir configuración de servicio de ubicación	✓	
Permitir al usuario modificar los ajustes de ubicación	✓	✓
Samsung Knox		
Funcionalidad del dispositivo		
Permitir el modo Avión	✓	
Permitir micrófono	✓	
Permitir ubicaciones ficticias	✓	
Permitir Portapapeles	✓	
Permitir apagar	✓	
Permitir tecla de Inicio	✓	
Permitir grabaciones de voz si el micrófono está permitido	✓	
Permitir grabaciones en video si la cámara está permitida.	✓	
Permitir la eliminación de la cuenta de correo electrónico	✓	
Permitir terminación de aplicación al estar inactiva	✓	
Permitir que el usuario establezca un límite de procesos en el fondo	✓	
Permitir auriculares	✓	

Sincronización y almacenamiento	
Permitir el cambio de la tarjeta SD	✓
Permitir actualización de forma inalámbrica (OTA)	✓
Permitir la sincronización automática de las cuentas de Google	✓
Permitir que se escriba en la tarjeta SD	✓

Función	Modo Dispositivo administrado de trabajo	Modo Perfil de trabajo
Permitir el almacenamiento del host USB	✓	
Permitir autocompletar (Android 8.0 o versiones posteriores)	✓	✓
Aplicación		
Permitir cambios a la configuración.	✓	
Permitir opciones de desarrollador	✓	
Permitir los datos en el fondo	✓	
Permitir marcación por voz	✓	
Permitir el informe de bloqueos de Google	✓	
Permitir S Beam	✓	
Permitir la solicitud de credenciales	✓	
Permitir S Voice	✓	
Permitir al usuario detener aplicaciones firmadas por el sistema	✓	
Bluetooth		
Permitir la conectividad del escritorio por Bluetooth	✓	
Permitir la transferencia de datos Bluetooth	✓	
Permitir llamadas salientes por Bluetooth	✓	
Permitir modo Bluetooth detectable	✓	
Activar el modo seguro de Bluetooth	✓	
Red		
Permitir Wi-Fi	✓	
Permitir los perfiles de Wi-Fi	✓	
Permitir Wi-Fi no segura	✓	
Permitir solo conexiones seguras de VPN	✓	

Permitir VPN	✓
Permitir conexión automática al Wi-Fi	✓
Permitir datos celulares	✓
Permitir Wi-Fi directo	✓
En roaming	
Permitir la sincronización automática mientras está en roaming	✓
Permitir sincronización automática cuando roaming está inhabilitado	✓

Función	Modo Dispositivo administrado de trabajo	Modo Perfil de trabajo
Permitir roaming de llamadas	✓	
Uso de datos en roaming	✓	
Permitir mensajes push mientras está en roaming	✓	
Teléfono y datos		
Permitir llamadas que no son emergencia	✓	
Permitir que el usuario establezca el límite de datos móviles	✓	
Permitir push WAP	✓	
Hardware		
Permitir tecla del menú	✓	
Permitir la tecla 'atrás'	✓	
Permitir la tecla de Búsqueda	✓	
Permitir el administrador de tareas	✓	
Permitir la barra del sistema	✓	
Permitir la tecla de Volumen	✓	
Seguridad		
Permitir los ajustes de bloqueo de pantalla	✓	
Permitir recuperación de firmware	✓	
Anclaje de red		
Permitir anclaje de red por USB	✓	
Restricciones de MMS		
Permitir entrada de MMS	✓	
Permitir salida de MMS	✓	
Misceláneo		
[illegible]		✓

Establecer el tamaño de texto en el dispositivo	✓
Permitir al usuario detener aplicaciones firmadas por el sistema	✓
Permitir solo conexiones seguras de VPN	✓

Exchange Active Sync

Workspace ONE UEM utiliza el perfil de Exchange ActiveSync (EAS) en los dispositivos Android para

garantizar una conexión segura con el correo electrónico interno, calendarios y contactos mediante clientes de correo. Por ejemplo, los ajustes de correo electrónico de EAS configurados para el Perfil de trabajo afectan a todas las aplicaciones de correo electrónico descargadas desde el catálogo de Workspace ONE UEM con el icono distintivo, y no al correo personal del usuario.

Una vez que el usuario tiene una dirección y un nombre de usuario, puede crear un perfil de Exchange Active Sync.

Aviso: El perfil de Exchange Active Sync se aplica a los modos Perfil de trabajo y Dispositivo administrado de trabajo.

Seleccione el perfil Exchange Active Sync y configure las siguientes opciones.

Ajustes	Descripción
Tipo de cliente de correo	Utilice el menú desplegable para seleccionar el cliente de correo que desea insertar en los dispositivos de usuario.
Host	Especifique la URL externa del servidor de ActiveSync de la compañía.
Tipo de servidor	Seleccione entre Exchange y Lotus.
Utilizar SSL	Active esta opción para cifrar los datos de EAS.
Deshabilitar comprobaciones de validación en los certificados SSL	Active esta opción para permitir certificaciones de Secure Socket Layer.
S-MIME	Active esta opción para seleccionar un certificado S/MIME que asocie como certificado de usuario en la carga útil Credenciales.
Certificado de firma de S/MIME	Seleccione el certificado para permitir el aprovisionamiento de certificados S/MIME para el cliente para la firma de mensajes.
Certificado de cifrado S/MIME	Seleccione el certificado para permitir el aprovisionamiento de los certificados S/MIME para el cliente para el cifrado de mensajes.
Dominio	Utilice los valores de búsqueda para usar el valor específico del dispositivo.
Nombre de usuario	Utilice los valores de búsqueda para usar el valor específico del dispositivo.
Dirección de correo electrónico	Utilice los valores de búsqueda para usar el valor específico del dispositivo.
Contraseña	Déjela en blanco para permitir que los usuarios finales establezcan sus propias contraseñas.
Certificado de inicio de sesión	Seleccione el certificado disponible en el menú desplegable.
Firma predeterminada	Especifique una firma de correo electrónico predeterminada para que se muestre en los mensajes nuevos.
Tamaño máximo de archivos adjuntos (MB)	Introduzca el tamaño máximo de archivos adjuntos que el usuario tiene permitido enviar.
Permitir la sincronización de Contactos y calendario	Active esta opción para permitir la sincronización de los contactos y el calendario con los dispositivos.

Actualización automática de aplicaciones públicas

El perfil de actualización automática de aplicaciones públicas le permite configurar actualizaciones automáticas y programar el mantenimiento de las aplicaciones Android públicas.

El perfil de actualización automática de aplicaciones públicas utiliza la API de Google para enviar los datos de perfil directamente a los dispositivos. Este perfil no se mostrará en VMware Workspace ONE Intelligent Hub.

Para configurar el perfil de actualización automática de aplicaciones públicas:

Aviso: Si un perfil contiene una carga útil de actualización de aplicaciones públicas, no puede contener otras cargas útiles.

Seleccione la actualización automática de aplicaciones públicas de la lista de carga útil y configure los ajustes de actualización:

- Política de actualización automática de aplicaciones públicas: Puede especificar el momento en el que Google Play admite la actualización automática. Seleccione Allow user to configure (Permitir al usuario configurar), Always auto update (Actualizar siempre automáticamente), Update on Wi-Fi only (Actualizar solamente en Wi-Fi) o Never auto upate (No actualizar nunca automáticamente).

La selección predeterminada es Allow user to configure (Permitir al usuario configurar).

- Hora de inicio: Puede configurar qué aplicaciones en hora local se pueden actualizar automáticamente en segundo plano a diario. Seleccione una hora entre las 00:30 y las 23:30.

Aviso: Solo es aplicable si se han seleccionado las opciones Actualizar solamente en Wi-Fi o Actualizar siempre automáticamente.

- Hora de finalización: Puede configurar qué aplicaciones en hora local se pueden actualizar automáticamente en segundo plano a diario. Seleccione una hora entre 30 minutos y 24 horas.

Aviso: Solo es aplicable si se han seleccionado las opciones Actualizar solamente en Wi-Fi y Actualizar siempre automáticamente.

En función del tiempo establecido, las aplicaciones solo se actualizarán automáticamente durante las horas de inicio y fin especificadas. Por ejemplo, debe establecer los dispositivos de quiosco para que solo se actualicen fuera de las horas de trabajo, con el fin de no interrumpir su uso.

Credenciales

Para obtener una seguridad más completa, puede implementar certificados digitales con los que proteger sus recursos corporativos. Para ello, primero debe definir una entidad de certificación y luego configurar una carga útil de Credenciales, junto con su carga útil de Exchange ActiveSync (EAS), Wi-Fi o VPN.

Cada carga útil tiene ajustes para asociar la entidad de certificación definida en la carga útil de Credenciales. Los perfiles de Credenciales implementan certificados corporativos para la autenticación del usuario en los dispositivos administrados. La configuración de este perfil varía según el tipo de propiedad del dispositivo. El perfil Credenciales se aplica a los modos Perfil de trabajo y Dispositivo administrado de trabajo.

Los dispositivos deben tener un código pin de dispositivo configurado para que Workspace ONE UEM pueda instalar los certificados de identidad con una clave privada.

Los perfiles de Credenciales implementan certificados corporativos para la autenticación del usuario

en los dispositivos administrados. La configuración de este perfil variará según el tipo de propiedad del dispositivo. El perfil Credenciales se aplicará a los modos de Perfil de trabajo y Dispositivo administrado de trabajo.

Seleccione el perfil Credenciales y seleccione Configurar.

Utilice el menú desplegable para seleccionar Carga o Entidad definida de certificación para la Fuente de credenciales. Las opciones de perfil restantes dependen de la fuente. Si selecciona Cargar, debe introducir un Nombre de credencial y cargar un nuevo certificado. Si selecciona Entidad definida de certificación, debe escoger una Entidad de certificación y una Plantilla predefinidas.

Administrar certificados con XML personalizado

Los certificados se pueden administrar a través de Workspace ONE Intelligent Hub for Android y a través de XML personalizados en UEM Console. Puede especificar nombres de paquetes que le permitan administrar sus certificados en dispositivos Android. Puede agregar los nombres de los paquetes a través de la configuración personalizada.

Para insertar estos paquetes:

1. Desplácese a Grupos y ajustes > Todos los ajustes > Aplicaciones > Ajustes y políticas > Ajustes > Ajustes personalizados.
2. Configure el XML personalizado según corresponda:

Ajustes	Descripción
Ajustes personalizados	Pegue el siguiente XML personalizado: { "AuthorizedCertInstaller" : “packagename” } y reemplace el marcador de posición "packagename" por el nombre del paquete real de la aplicación (normalmente en formato com.company.appname).

1. Guarde el XML personalizado.

Mensajes personalizados

El perfil Mensajes personalizados permite configurar los mensajes que se muestran en la pantalla principal del dispositivo cuando es necesario retransmitir información importante al usuario.

El perfil Mensajes personalizados permite establecer un mensaje para la pantalla de bloqueo, un mensaje que se mostrará cuando los usuarios intenten realizar una configuración bloqueada o la configuración del usuario del dispositivo.

Selecciona el perfil Mensajes personalizados y configure los ajustes de los mensajes:

|Configurar un mensaje para la pantalla de bloqueo|Introduzca un mensaje que se mostrará en la pantalla principal del dispositivo cuando el dispositivo esté bloqueado. Esto resulta útil para que los dispositivos perdidos o robados muestren la información de contacto del usuario.| |Configurar un mensaje breve para los ajustes bloqueados|Introduzca un mensaje que se mostrará cuando un usuario intente realizar acciones en un dispositivo bloqueado. Utilice el mensaje personalizado para explicar el motivo por el que la función está bloqueada.| |Configure un mensaje largo para que los usuarios puedan verlo en los ajustes|Los usuarios pueden ver este mensaje en su dispositivo en Ajustes > Seguridad > Administradores de dispositivo > Intelligent Hub.|

Control de aplicaciones

El perfil de control de aplicaciones le permite controlar las aplicaciones aprobadas e impedir la desinstalación de aplicaciones importantes. El motor de conformidad envía alertas y toma acciones administrativas cuando un usuario instala o desinstala ciertas aplicaciones y el control de aplicaciones previene que los usuarios lleven a cabo estas acciones en el primer lugar.

Solo las aplicaciones aprobadas por el administrador se mostrarán en la Play Store cuando se configure el perfil de control de aplicaciones. Por ejemplo, puede insertar automáticamente el navegador que desee en el dispositivo como una aplicación administrada y agregarlo al Grupo de aplicaciones de aplicaciones requeridas. Esta configuración combinada con la activación de la opción Impedir la desinstalación de aplicaciones requeridas en el perfil de control de aplicaciones impide desinstalar el navegador y cualquier otra aplicación requerida configurada en el Grupo de aplicaciones.

```
Warning: Enabling/ disabling critical system apps results in devices becoming unusable.
```

Para obtener más información sobre los grupos de aplicaciones, consulte la documentación de Administración de aplicaciones móviles.

Para controlar el acceso de las aplicaciones a sus dispositivos Android, cree un perfil que le permita incluir, evitar, desinstalar o activar aplicaciones del sistema con el perfil de control de aplicaciones.

Control de aplicaciones para dispositivos COPE

Si utiliza dispositivos inscritos con el método Dispositivo corporativo habilitado de forma personal, puede crear listas de permitidos o de no permitidos para las aplicaciones con el fin de evitar la instalación de aplicaciones no aprobadas en el perfil personal.

Ajustes	Descripción
Deshabilitar acceso a las aplicaciones no permitidas	Seleccione esta opción para desactivar el acceso a las aplicaciones que están en la lista de no permitidos definida en los grupos de aplicaciones. Si se activa, esta opción no desinstala la aplicación del dispositivo.
Impedir la desinstalación de aplicaciones requeridas	Active esta opción para evitar que el usuario o el administrador desinstalen las aplicaciones requeridas definidas en los Grupos de aplicaciones.
Activar aplicaciones del sistema	Active esta opción para mostrar las aplicaciones preinstaladas tal y como se ha definido en las aplicaciones de la lista blanca en los grupos de aplicaciones. Para COPE, la casilla de verificación "Administrado de trabajo" se aplica al lado personal y "Perfil de trabajo" se aplica al lado corporativo. Para dispositivos COPE en Android 10 y versiones anteriores.
Restricciones de la tienda Play Store personal	Seleccione Ninguna, Lista de permitidos o Lista de no permitidos para controlar qué aplicaciones se pueden instalar a través de Play Store en el lado personal de los dispositivos corporativos habilitados de forma personal. Las aplicaciones de la lista de no permitidos y la lista de permitidos se definen en los grupos de aplicaciones.

Ajustes de proxy

Los ajustes del proxy se configuran para garantizar que todo el tráfico de red HTTP y HTTPS solo

pasa a través de él. De este modo se garantiza la seguridad de los datos, ya que todos los datos personales y corporativos se filtrarán a través del perfil Ajustes del proxy.

Configure los ajustes de Proxy, como:

Ajustes	Descripción
Modo Proxy	Seleccione el tipo de proxy que desee.
URL de PAC Proxy	Especifique una dirección URL para un archivo .pac de proxy.
Servidor de proxy	Introduzca el nombre de host o la dirección IP del servidor proxy.
Lista de exclusión	Agregue nombres de host para evitar que se redirijan a través del proxy.

Actualizaciones del sistema

Utilice este perfil para administrar la forma en que se administran las actualizaciones de dispositivos Android cuando el dispositivo se inscribe en Workspace ONE UEM.

Seleccione el perfil de Actualizaciones del sistema.

Utilice el menú desplegable del campo Actualizaciones automáticas para seleccionar la política de actualización.

Ajustes	Descripción
Actualizaciones automáticas (dispositivos administrados de trabajo y COPE con Android 6.0 y posterior)	Instalar actualizaciones automáticamente: Instala actualizaciones automáticamente cuando están disponibles.
	Aplazar notificaciones de actualización: Aplaza todas las actualizaciones. Envía una política que bloquea las actualizaciones de SO por un período máximo de 30 días.
	Establecer plazo de actualización: Establezca un plazo diario en el que se actualizará el dispositivo.
Periodos de bloqueo de actualización anual del sistema (dispositivos administrados de trabajo y COPE con Android 9.0 y posterior)	Los propietarios de los dispositivos pueden posponer las actualizaciones de sistema inalámbricas (OTA) en los dispositivos durante un máximo de 90 días para bloquear la versión del SO que se ejecuta en estos dispositivos durante periodos críticos (por ejemplo, las vacaciones). El sistema aplica un búfer obligatorio de 60 días después de un periodo de bloqueo definido para evitar bloquear el dispositivo de forma indefinida.
	Durante un periodo de bloqueo:
	Los dispositivos no reciben ninguna notificación acerca de las actualizaciones OTA pendientes.
	Los dispositivos no instalan ninguna actualización OTA en el SO.
	Los usuarios del dispositivo no pueden comprobar manualmente si hay actualizaciones OTA.

Ajustes	Descripción
Periodo de bloqueo	Utilice este campo para establecer periodos de bloqueo, con el mes y el día, cuando no se puedan instalar actualizaciones. Cuando la hora del dispositivo se encuentre dentro de alguno de los periodos de bloqueo, todas las actualizaciones de sistema entrantes, incluidas las revisiones de seguridad, se bloquearán y no se podrán instalar. Cada periodo de bloqueo individual puede tener una duración máxima de 90 días y los periodos de bloqueo subsecuentes deben estar separados por al menos un periodo de 60 días.

Wi-Fi

La configuración de un perfil de Wi-Fi le permite conectar dispositivos a las redes corporativas, incluso si están ocultas, cifradas o protegidas.

El perfil de Wi-Fi puede ser útil para los usuarios finales que viajan a diferentes ubicaciones de la empresa, las cuales cuentan con sus propias redes inalámbricas únicas, o también para configurar automáticamente los dispositivos para conectarse a una red inalámbrica adecuada mientras están en una oficina.

Al enviar un perfil de Wi-Fi a los dispositivos que ejecutan Android 6.0+, si un usuario ya tiene su dispositivo conectado a una red Wi-Fi mediante la configuración manual, Workspace ONE UEM no podrá modificar la configuración Wi-Fi. Por ejemplo, si se ha cambiado la contraseña de la conexión Wi-Fi y envía el perfil actualizado a los dispositivos inscritos, algunos usuarios tendrán que actualizar su dispositivo manualmente con la nueva contraseña.

Para configurar el perfil:

Configure los ajustes de Wi-Fi:

Ajustes >	Descripción
Identificador de red	Proporcione el nombre de la red a la que se conecta el dispositivo.
Red oculta	Indique si la red Wi-Fi está oculta.
Establecer como red activa	Indique si el dispositivo se conectará a la red, sin interacción de parte de los usuarios finales.
Tipo de seguridad	Especifique el protocolo de acceso utilizado y si se requieren certificados. En función del tipo de seguridad seleccionado, se modificarán los campos obligatorios. Si se selecciona Ninguno, WEP, WPA/WPA 2 o Cualquiera (personal), se muestra el campo Contraseña. Si se selecciona WPA/WPA 2 Enterprise, se muestran los campos Protocolos y Autenticación.
	Protocolos
	- Usar autenticación de dos factores: cuando se activa, se muestra el campo TFA.
	- Tipo de SFA: elija un protocolo de autenticación. Las opciones disponibles son EAP-TLS, PEAP o EAP-TTLS.

Ajustes >	Descripción
	- Tipo de TFA: elija un método de autenticación interno. Las opciones disponibles son GTC, MSCHAP, MSCHAPv2 y PAP.
	Autenticación
	- Identidad: establezca la identidad y las credenciales que el dispositivo utilizará para conectarse a la red.
	- Certificado de identidad: seleccione el certificado de identidad para especificar una clave privada y una cadena de certificados de cliente para la autorización de cliente. Este certificado debe agregarse al perfil como parte de la carga útil Credenciales.
	- Certificado raíz: seleccione un certificado raíz que el dispositivo utilizará para la validación del certificado del servidor. El certificado raíz debe ser el certificado raíz de la CA del servidor. Esto se utiliza para la validación del certificado del servidor. Si no se especifica ningún certificado, se omite la validación del certificado del servidor. Este certificado debe agregarse al perfil como parte de la carga útil Credenciales.
	- Dominio: establezca una restricción para el nombre de dominio del servidor que se utilizará para validar el servidor de red. Si se establece, este FQDN se utiliza como requisito de coincidencia de sufijo para el certificado de servidor AAA en los elementos dNSName de SubjectAltName. Si se encuentra un dNSName coincidente, se cumple esta restricción. Si no hay valores de dNSName, esta restricción se compara con el CN de SubjectName mediante la misma comparación de coincidencia de sufijos.
	La coincidencia de sufijo en este contexto significa que el nombre de host/dominio se compara etiqueta por etiqueta, empezando por el dominio de nivel superior. Por ejemplo, si el dominio se establece en ejemplo.com, coincidirá con prueba.ejemplo.com, pero no con prueba-ejemplo.com.
Contraseña	Proporcione las credenciales requeridas para que el dispositivo se conecte a la red. El campo de la contraseña aparece cuando se selecciona WEP, WPA/WPA 2, Cualquier (Personal), WPA/WPA2 Enterprise en el campo Tipo de seguridad.
Incluir ajustes de Fusion	Active esta opción para ampliar las opciones de Fusion que podrá utilizar con adaptadores de Fusion para dispositivos Motorola. Los ajustes de Fusion se aplican solo a los dispositivos Motorola Rugged. Para obtener más información sobre la compatibilidad de VMware Support con dispositivos robustos Android, consulte la guía Rugged Android Platform Guide.
Establecer Fusion 802.11d	Active esta opción para utilizar Fusion 802.11d para configurar los ajustes de Fusion 802.11d.
Activar 802.11d	Active esta opción para utilizar la especificación inalámbrica 802.11d en dominios legales adicionales.
Establecer código de país	Active esta opción para establecer el Código de país que se utilizará en las especificaciones 802.11d.
Establecer banda RF	Active esta opción para elegir la banda de 2,4 GHz, la banda de 5 GHz o ambas bandas y las máscaras de canal aplicables.
Tipo de proxy	Active esta opción para configurar los ajustes del proxy de Wi-Fi.Nota: No se admite la configuración automática del proxy de Wi-Fi mediante la VPN por aplicación.

Ajustes >	Descripción
Servidor de proxy	Introduzca el nombre de host o la dirección IP del servidor proxy.
Puerto del servidor de proxy	Introduzca el puerto del servidor proxy.
Lista de exclusión	Introduzca los nombres de host que desea excluir del proxy. Los nombres de host introducidos aquí no se enrutarán a través del proxy. Utilice un "*" como carácter comodín para el dominio. Por ejemplo: *.air-watch.com o *air-watch.com.

VPN

Una red privada virtual (VPN) proporciona a los dispositivos un túnel seguro y cifrado para acceder a los recursos internos, como correo electrónico, archivos y contenido. Los perfiles de VPN permiten que cada dispositivo funcione como si estuviera conectado a través de la red en el sitio.

Dependiendo del tipo de conexión y del método de autenticación, utilice los valores de búsqueda para rellenar el nombre de usuario automáticamente y así simplificar el proceso de inicio de sesión.

Aviso: El perfil de VPN se aplica a los modos Perfil de trabajo y Dispositivo administrado de trabajo.

Configure los ajustes de VPN. La siguiente tabla define todos los ajustes que se pueden configurar en función del cliente de VPN.

Ajustes	Descripción
Tipo de conexión	Seleccione el protocolo utilizado para facilitar las sesiones de VPN. Cada tipo de conexión requiere que el cliente de VPN correspondiente esté instalado en el dispositivo para implementar el perfil de VPN. Estas aplicaciones deben asignarse a los usuarios y publicarse como aplicaciones públicas.
Nombre de la conexión	Introduzca el nombre asignado a la conexión creada por el perfil.
Servidor	Introduzca el nombre o la dirección del servidor que se utiliza para las conexiones de VPN.
Cuenta	Introduzca la cuenta de usuario para autenticar la conexión.
Siempre con VPN	Active esta opción para forzar la tunelización de todo el tráfico desde las aplicaciones de trabajo a través de VPN.
Bloqueo	Obliga a que las aplicaciones se conecten exclusivamente a través de la VPN. Si la VPN está desconectada o no está disponible, las aplicaciones no tendrán acceso a Internet.
Permitir que las aplicaciones omitan el bloqueo	Active esta opción para especificar que las aplicaciones continúen accediendo a Internet incluso cuando la VPN esté desconectada o no esté disponible.

Ajustes	Descripción
Lista de permitidos de bloqueo	Si la opción Lista de permitidos de bloqueo está activada con paquetes agregados, las aplicaciones enumeradas podrán conectarse directamente a Internet si se desconecta la VPN
Establecer como activo	Active esta opción para activar la VPN una vez que se aplique el perfil al dispositivo.
Reglas de VPN por aplicación	Active la opción VPN por aplicación, que le permite configurar reglas de tráfico de VPN basadas en aplicaciones específicas. Este cuadro de texto solo se muestra para proveedores de VPN compatibles. Aviso: No se admite la configuración automática del proxy de Wi-Fi mediante la VPN por aplicación.
Protocolo	Seleccione el protocolo de autenticación para la VPN. Disponible cuando se selecciona Cisco AnyConnect en el Tipo de conexión.
Nombre de usuario	Introduzca el nombre de usuario. Disponible cuando se selecciona Cisco AnyConnect en el Tipo de conexión.
Autenticación de usuario	Elija el método requerido para autenticar la sesión VPN.
Contraseña	Proporcione las credenciales requeridas para el acceso a la VPN del usuario final.
Certificado del cliente	Utilice el menú desplegable para seleccionar el certificado de cliente. Estas opciones se configuran en los perfiles de Credenciales.
Revocación de certificados	Active esta opción para activar la revocación de certificados.
Perfil de AnyConnect	Introduzca el nombre del perfil AnyConnect.
Modo FIPS	Active esta opción para activar el modo FIPS.
Modo estricto	Active esta opción para activar el modo estricto.
Claves de proveedor	Cree claves personalizadas que se incluirán en el diccionario de configuración del proveedor.
Clave	Introduzca la clave específica proporcionada por el proveedor.
Valor	Introduzca el valor de VPN para cada clave.
Certificado de identidad	Seleccione el certificado de identidad que se utilizará para la conexión VPN. Disponible cuando se selecciona Workspace ONE Tunnel en el Tipo de conexión.

Configurar reglas de VPN por aplicación

Puede forzar que las aplicaciones seleccionadas se conecten a través de su VPN corporativa. El proveedor de VPN debe admitir esta función y usted debe publicar las aplicaciones como aplicaciones administradas.

Aviso: No se admite la configuración automática del proxy de Wi-Fi mediante la VPN por aplicación.

1. Seleccione la carga útil de VPN de la lista.
2. Seleccione su proveedor de VPN en el campo Tipo de conexión.

3. Configure su perfil de VPN.
4. Seleccione Reglas de VPN por aplicación para activar la capacidad de asociar el perfil de VPN a las aplicaciones deseadas. Para el cliente de Workspace ONE Tunnel, esta selección está activada de forma predeterminada. Una vez activada la casilla de verificación, este perfil estará disponible para su selección en el menú desplegable de perfiles de tunelización de aplicaciones en la página Asignación de aplicaciones.
5. Seleccione Guardar y publicar.

   Si la opción Reglas de VPN por aplicación está activada como una actualización de un perfil de VPN existente, aquellos dispositivos o aplicaciones que anteriormente utilizaban la conexión de VPN se verán afectados. La conexión de VPN que anteriormente enrutaba todo el tráfico de las aplicaciones se desconectará y la VPN solo se aplicará a las aplicaciones asociadas con el perfil actualizado.

Para configurar las aplicaciones públicas para utilizar el perfil de VPN por aplicación, consulte Cómo agregar aplicaciones públicas para Android en Administración de aplicaciones para la publicación en Android.

Permisos

Workspace ONE UEM Console permite al administrador ver una lista de todos los permisos que utiliza una aplicación y establecer la acción predeterminada en tiempo de ejecución de la aplicación. El perfil Permisos está disponible en los dispositivos con Android 6.0 o superior que utilizan el dispositivo administrador de trabajo y el modo de perfil de trabajo.

Puede establecer directivas de permiso de tiempo de ejecución para cada aplicación de Android. Al configurar una aplicación en un nivel de aplicación individual, se obtienen los permisos más recientes.

Aviso: Todos los permisos que utiliza una aplicación aparecen cuando se selecciona la aplicación en la lista Excepciones; sin embargo, las políticas de permisos de Workspace ONE UEM console solo hacen referencia a permisos peligrosos, según el criterio de Google. Los permisos peligrosos abarcan áreas donde la aplicación solicita datos que incluyen información personal del usuario o que podrían afectar a los datos almacenados del usuario. Para obtener más información, consulte el sitio web de desarrolladores de Android.

Configure los ajustes de Permisos, entre los que se incluyen los siguientes:

Ajustes	Descripción
Política de permisos	Seleccione si desea Solicitar permiso al usuario, Otorgar todos los permisos, o Denegar todos los permisos para todas las aplicaciones de trabajo.
Excepciones	Busque aplicaciones que ya se han agregado a AirWatch (solo debe incluir aplicaciones aprobadas por Android) y realice una excepción a la política de permisos para la aplicación.

Modo de bloqueo de tarea

El modo de bloqueo de tarea permite que una aplicación se ancle a sí misma en primer plano, lo que permite un solo propósito, como el modo de quiosco. La aplicación admite el modo de bloqueo de tarea y se agrega a través del ajuste Aplicaciones y libros para que se muestre en Aplicaciones

en la lista blanca. El desarrollador de la aplicación configura el ajuste de bloqueo de tarea durante el desarrollo de la aplicación, mientras que los ajustes del perfil de bloqueo de tarea le permiten configurar los permisos y los ajustes.

Aviso: Para obtener información más específica sobre las aplicaciones admitidas, consulte el vínculo en el perfil del modo de bloqueo de tareas en Workspace ONE UEM Console, que le dirigirá al sitio de desarrolladores de Google.

Configure los ajustes del modo de bloqueo de tareas:

Ajustes	Descripción
Aplicaciones en la lista blanca	Seleccione las aplicaciones deseadas para bloquear el dispositivo en el modo de bloqueo de tareas.
Botón de inicio	Active esta opción para mostrar el botón de inicio en la pantalla para que el usuario pueda obtener acceso.
Botón de aplicaciones recientes	Active esta opción para mostrar un resumen de las aplicaciones utilizadas recientemente.
Acciones globales	Active esta opción para permitir que los usuarios presionen de manera sostenida el botón de encendido para ver acciones globales, tales como el botón de encendido u otras acciones comunes que se utilizan en el dispositivo.
Notificaciones de aplicaciones	Active esta opción para mostrar los iconos de notificación en la barra de estado.
Información del sistema en la barra de estado	Active esta opción para mostrar la barra de información del dispositivo con información tal como la duración de la batería, la conectividad y el volumen.
Bloquear pantalla	Active la pantalla de bloqueo.

Prácticas recomendadas para el modo de bloqueo de tarea

Considere la posibilidad de aplicar estas políticas y restricciones para garantizar la mejor experiencia y mantenimiento de su propósito único mediante políticas de modo de bloqueo de tarea. Estas recomendaciones son útiles si va a implementar un perfil de modo de bloqueo de tarea para dispositivos en casos prácticos de señalización digital y en modo quiosco, donde el usuario final no está asociado con el dispositivo.

Cree un perfil de "Restricciones" y configure los siguientes elementos en el perfil:

- Deshabilite las siguientes opciones en la Funcionalidad del dispositivo:
  - Permitir barra de estado: garantiza una experiencia inmersiva cuando el dispositivo está bloqueado en modo de bloqueo de tarea.
  - Permitir bloqueo: este modo garantiza que el dispositivo no se bloquee.
- Active las siguientes opciones en Funcionalidad del dispositivo:
  - Forzar Pantalla activa al conectar con el cargador AC
  - Forzar Pantalla activa al conectar con el cargador USB
  - Forzar encendido de pantalla al conectar un cargador inalámbricoEstas opciones garantizan que la pantalla del dispositivo siempre está activada para la interacción.

Implemente el perfil de Política de actualización del sistema para asegurarse de que el dispositivo

reciba las revisiones más recientes con una mínima intervención manual.

Fecha y hora para dispositivos Android

Configure los ajustes de sincronización de fecha y hora para garantizar que los dispositivos siempre tengan la hora correcta en diferentes regiones. Es compatible en dispositivos con Android 9.0 o versiones posteriores.

Configure los ajustes de Fecha / hora:

Ajustes	Descripción
Fecha / hora	Configure la fuente de datos desde la que los dispositivos obtendrán los ajustes de fecha y hora. Seleccione Automática, URL de HTTP o Servidor de SNTP.
	Automático: establece la fecha y la hora según los ajustes nativos del dispositivo.
	URL de HTTP: establece la hora en función de una URL. Esta dirección URL puede ser cualquier dirección URL. Por ejemplo, puede utilizar www.google.com como dirección URL.
	Servidor SNTP: Introduzca la dirección del servidor. Por ejemplo, puede utilizar time.nist.gov.
	En URL de HTTP y Servidor SNTP, configure los ajustes adicionales: Activar sincronización periódica: active esta opción para configurar el dispositivo de forma que sincronice la fecha y la hora periódicamente. Establecer zona horaria: especifique la zona horaria de entre las opciones disponibles.
Permitir al usuario cambiar la fecha y la hora	Active esta opción para permitir que los usuarios cambien manualmente la fecha y la hora del dispositivo.

Fecha y hora para dispositivos Samsung

Configure los ajustes de sincronización de fecha y hora para garantizar que los dispositivos siempre tengan la hora correcta en diferentes regiones.

Este perfil está disponible cuando el campo Ajustes de OEM está activado y el campo Seleccionar OEM se establece en Samsung en los ajustes del perfil General.

Aviso: El perfil Fecha/Hora solo se muestra cuando el campo Ajustes de OEM se establece en Activado

Configure los ajustes de Fecha / hora para Samsung, incluyendo:

Ajustes	Descripción
Formato de fecha	Cambiar el orden en el que se muestra Mes, Día y Año.
Formato de hora	Elegir entre formato de 12 o 24 horas.

Ajustes	Descripción	
Fecha / hora	Configure la fuente de datos desde la que los dispositivos obtendrán los ajustes de fecha y hora:	
	Automático: establece la fecha y la hora según los ajustes nativos del dispositivo.	
	Hora del servidor: establece la hora en función de la hora del servidor de Workspace ONE UEM Console en el momento en que se crea el perfil. Tenga en cuenta que esto puede hacer que el dispositivo tarde debido a la latencia a la hora de insertar perfiles.	Se mostrará un campo adicional, Establecer zona horaria, que le permite seleccionar la zona horaria.
	URL de HTTP: establece la hora en función de una URL. Esta dirección URL puede ser cualquier dirección URL. Por ejemplo, puede utilizar www.google.com como dirección URL.	
	Servidor SNTP: introduzca el servidor.	
	En URL de HTTP y Servidor SNTP, configure los ajustes adicionales: Activar sincronización periódica: active esta opción para configurar el dispositivo de forma que sincronice la fecha y la hora periódicamente. Establecer zona horaria: especifique la zona horaria de entre las opciones disponibles.	

Workspace ONE Launcher

Workspace ONE Launcher es un programa de inicio de aplicaciones que le permite bloquear dispositivos Android para casos prácticos individuales, así como personalizar la apariencia y el comportamiento de los dispositivos Android administrados. La aplicación Workspace ONE Launcher sustituye la interfaz de su dispositivo por una adaptada a sus necesidades empresariales.

Puede configurar Android 6.0 Marshmallow y dispositivos posteriores con el modo de propiedad corporativa, uso único (corporate-owned, single-use, COSU). El modo COSU le permite configurar dispositivos Android para un único propósito, como el modo quiosco, incluyendo aplicaciones internas y públicas admitidas en la lista blanca. El modo COSU es compatible con el modo de aplicación única, el modo de aplicaciones múltiples y el modo de plantilla. Para obtener más información sobre la implementación del perfil de Workspace ONE Launcher en modo COSU, consulte la publicación sobre Workspace ONE Launcher.

Para obtener una guía más completa sobre la configuración de Workspace ONE Launcher, consulte la publicación sobre Workspace ONE Launcher.

Firewall

La carga útil de Firewall permite a los administradores configurar las reglas de firewall para los dispositivos Android. Cada tipo de regla de firewall le permite agregar varias reglas.

Este perfil está disponible cuando el campo Ajustes de OEM está activado y el campo Seleccionar OEM se establece en Samsung en los ajustes del perfil General.

Aviso: La carga útil de Firewall solo se aplica a dispositivos SAFE 2.0+.

1. Desplácese a Recursos > Perfiles y líneas base > Perfiles > Agregar > Agregar perfil > Android.

El perfil Firewall solo se muestra para los perfiles de Android cuando el campo Ajustes de OEM está activado y Samsung está seleccionado en el campo Seleccionar OEM. El campo Ajustes de OEM en el perfil General solo se aplica a los perfiles de Android y no a las configuraciones de Android (heredado).

2. Seleccione Dispositivo para implementar el perfil.
3. Configure los ajustes del perfil General.

   Los ajustes de tipo General determinan de qué manera se implementa el perfil y qué usuarios lo recibirán.
4. Seleccione el perfil de Firewall.
5. Seleccione el botón Agregar debajo de la regla deseada para configurar los ajustes:

Ajustes	Descripción
Reglas de permiso	Permite que el dispositivo envíe y reciba desde una ubicación de red específica.
Reglas de prohibición	Evita que el dispositivo envíe y reciba tráfico desde una ubicación de red específica.
Reglas de desvío	Redirige el tráfico desde una ubicación de red concreta a una red alternativa. Si una página web permitida redirige a otra dirección URL, agregue todas las direcciones URL a las que se redirige a la sección de Permitir reglas para que se pueda acceder a ellas.
Reglas de excepción de redirecciona miento	Evita que el tráfico se redirija.

6. Seleccione Guardar y publicar.

APN

Configure el nombre de punto de acceso (APN) de los dispositivos Android para unificar la configuración del operador de la flota de dispositivos y corregir errores de configuración.

1. Desplácese a Recursos > Perfiles y líneas base > 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. El perfil APN solo se muestra cuando el campo Ajustes de OEM está Activado y se ha seleccionado Samsung en el campo Seleccionar OEM.

   Los ajustes de perfil General determinan de qué manera se implementa el perfil y qué usuarios lo recibirán.
4. Seleccione la carga útil de APN.
5. Configure los ajustes de APN:

Ajustes	Descripción

Nombre de la pantalla	Indique el nombre común del nombre de acceso.
Nombre del punto de acceso (APN)	Introduzca el APN proporcionado por su operador (por ejemplo, come.moto.cellular).
Tipo de punto de acceso	Especifica los tipos de comunicación de datos que debe utilizar esta configuración de APN.
Código móvil del país (MCC)	Introduzca el código de país de tres dígitos. Este valor comprueba si los dispositivos están en roaming en un operador distinto del que se ha introducido aquí. Esto se usa en combinación con un código de red móvil (MNC) para identificar de forma exclusiva a un operador de red móvil (operador) utilizando las redes móviles GSM (incluye GSM-R), UMTS y LTE.
Código de red móvil (MNC)	Introduzca el código de red de tres dígitos. Este valor comprueba si los dispositivos están en roaming en un operador distinto del que se ha introducido aquí. Esto se usa en combinación con un código de país móvil (MCC) para identificar de forma exclusiva a un operador de red móvil (operador) utilizando las redes móviles GSM (incluye GSM-R), UMTS y LTE.
Servidor MMS (MMSC)	Especifique la dirección del servidor.
Servidor proxy MMS	Introduzca el número del puerto MMS.
Puerto del servidor proxy MMS	Introduzca el puerto de destino para el servidor proxy.
Servidor	Introduzca el nombre o la dirección que se utilizan para la conexión.
Servidor de proxy	Introduzca los datos del servidor de proxy.
Puerto del servidor de proxy	Introduzca el puerto del servidor de proxy para todo el tráfico.
Nombre de usuario de punto de acceso	Especifique el nombre de usuario que se conecta al punto de acceso.
Contraseña de punto de acceso	Especifique la contraseña que autentica el punto de acceso.

Ajustes	Descripción
Tipo de autenticación	Seleccione el protocolo de autenticación.
Configurado como APN preferido	Active esta opción para garantizar que todos los dispositivos de usuario final tengan los mismos ajustes de APN y para evitar que se realicen cambios en el dispositivo o el operador.

6. Seleccione Guardar y publicar.

Protección de restablecimiento del estado de fábrica empresarial

La protección de restablecimiento de fábrica (FRP) es un método de seguridad de Android que impide el uso de un dispositivo después de un restablecimiento de datos de fábrica no autorizado.

Cuando se activa, el dispositivo protegido no se puede usar después de un restablecimiento de fábrica hasta que inicie sesión con la misma cuenta de Google configurada anteriormente.

Si un usuario ha activado FRP, cuando el dispositivo se devuelve a la organización (el usuario abandona la empresa, por ejemplo), es posible que no pueda volver a configurar el dispositivo debido a esta función del dispositivo.

El perfil de protección de restablecimiento de fábrica de la empresa utiliza un ID de usuario de Google que permite reemplazar la cuenta de Google después de un restablecimiento de fábrica para asignar el dispositivo a otro usuario. Para obtener este ID de usuario de Google, visite People:get.

Generar el ID de usuario de Google para el perfil de protección de restablecimiento de fábrica en dispositivos Android

Esta identificación de usuario de Google le permite restablecer el dispositivo sin la cuenta original de Google. Obtenga su identificador de usuario de Google mediante la API People:get para configurar el perfil. Antes de comenzar, debe obtener el ID de usuario de Google del sitio web People:get.

1. Desplácese a People:get.
2. En la ventana Probar esta API, configure los siguientes ajustes.

Ajustes	Descripción
resourceName	Introduzca people/me.
personFields	Introduzca metadata,emailAddresses
requestMask.includefield	Deje este campo vacío.
Credenciales	Active los campos Google OAuth 2.0 y Clave de API.

3. Seleccione Ejecutar.
4. Inicie sesión en su cuenta de Google si se le solicita. Esta es la cuenta que se utiliza para desbloquear los dispositivos cuando FRP está activado.

5. Seleccione Permitir para conceder permisos.
6. Seleccione 21 dígitos en la pestaña application/json en el campo id.
7. Vuelva a acceder a Workspace ONE UEM Console y configure el perfil de protección de restablecimiento de fábrica empresarial.

Configurar el perfil de protección de restablecimiento de fábrica empresarial para Android

Introduzca el ID de usuario de Google en el perfil de protección de restablecimiento de fábrica empresarial.

1. Desplácese a Recursos > Perfiles y líneas base > Perfiles > Agregar > Agregar perfil > Android.
2. Configure los ajustes del perfil en la sección General según sea necesario.
3. Seleccione la carga útil de Protección de restablecimiento de fábrica empresarial .
4. Configure los siguientes ajustes para establecer el nivel de control en sus implementaciones de aplicaciones:

Ajustes	Descripción
Identificadores de usuario de Google	Introduzca el identificador de usuario de Google obtenido de Google People:get.

5. Seleccione Guardar y publicar.

Zebra MX

El perfil Zebra MX le permite aprovechar las capacidades adicionales que se ofrecen con la aplicación de servicio Zebra MX en los dispositivos Android. La aplicación Zebra MX Service se puede enviar desde Google Play y desde My Workspace ONE distribuida como una aplicación interna en Workspace ONE UEM Console junto con este perfil.

1. Desplácese a Recursos > Perfiles y líneas base > Perfiles > Agregar > Agregar perfil > Android.
2. Configure los ajustes del perfil en la sección General según sea necesario. Active el campo Ajustes de OEM y seleccione Zebra en el campo Seleccionar OEM para activar el perfil Zebra MX.
3. Configure los ajustes del perfil Zebra MX:

Ajustes	Descripción
Incluir ajustes de Fusion	Active esta opción para ampliar las opciones de Fusion que podrá utilizar con adaptadores de Fusion para dispositivos Motorola.
Establecer Fusion 802. 11d	Active esta opción para utilizar Fusion 802.11d para configurar los ajustes de Fusion 802.11d.
Activar 802.11d	Active esta opción para utilizar la especificación inalámbrica 802.11d en dominios legales adicionales.

Ajustes	Descripción
Establecer código de país	Active esta opción para establecer el Código de país que se utilizará en las especificaciones 802.11d.
Establecer banda RF	Active esta opción para elegir la banda de 2,4 GHz, la banda de 5 GHz o ambas bandas y las máscaras de canal aplicables.
Permitir el modo Avión	Active esta opción para permitir el acceso a la pantalla de ajustes del modo Avión.
Permitir ubicaciones ficticias	Active o desactive las ubicaciones ficticias (en Ajustes > Opciones de desarrollador).
Permitir los datos en el fondo	Active o desactive los datos en segundo plano.
Mantener la conexión Wi-Fi activada durante el modo de suspensión	Siempre activada: la red Wi-Fi permanece habilitada cuando el dispositivo entra en el modo de suspensión. Solo si está enchufado: la red Wi-Fi permanece habilitada cuando el dispositivo entra en el modo de suspensión solo si se está cargando el dispositivo. Nunca activada: la red Wi-Fi se deshabilita cuando el dispositivo entra en el modo de suspensión.
Uso de datos en roaming	Active esta opción para permitir la conexión de datos cuando se está en roaming.
Forzar activación de Wi-Fi	Active esta opción para forzar la activación de la red Wi-Fi e impedir que los usuarios puedan desactivarla.
Permitir Bluetooth	Active esta opción para permitir el uso de Bluetooth.
Permitir Portapapeles	Active esta opción para permitir copiar y pegar.
Permitir notificación de seguimiento de redes	Active esta opción para permitir las notificaciones de advertencia del monitor de red, que suelen mostrarse tras la instalación de certificados.
Activar los ajustes de Fecha/Hora	Active esta opción para establecer los ajustes de Fecha/Hora
	Formato de fecha: Determina el orden en que se muestra el mes, día y año.
	Formato de hora: Elija 12 o 24 horas.
	Fecha/Hora: Configure la fuente de datos desde la que los dispositivos obtendrán los ajustes de fecha y hora:
	Automático: establece la fecha y la hora según los ajustes nativos del dispositivo.
	Hora del servidor: establece la hora según la hora del servidor de Workspace ONE UEM console.
	Establecer zona horaria: especifique la zona horaria.

Ajustes	Descripción
	URL de HTTP: Workspace ONE UEM Intelligent Hub accede a la URL y obtiene la marca de tiempo del encabezado HTTP. A continuación, aplica ese tiempo al dispositivo. No controla los sitios que se redirigen.
	Dirección URL: introduzca la dirección web para la programación de la fecha y la hora. Debe incluir http://. Ejemplo: http://www.google.com / No compatible con HTTPS.
	Activar sincronización periódica: active esta opción para configurar el dispositivo de forma que compruebe la fecha y la hora periódicamente.
	Establecer zona horaria: especifique la zona horaria.
	Servidor SNTP: - Los ajustes de NTP se aplican directamente al dispositivo.
	URL: introduzca la dirección web del servidor NTP/SNTP. Por ejemplo, puede utilizar time.nist.gov.
	Activar sincronización periódica: active esta opción para configurar el dispositivo de forma que compruebe la fecha y la hora periódicamente.
Activar Ajustes de sonido	Active Ajustes de sonido para configurar las opciones de audio en el dispositivo. - Música, video, juegos y otros elementos multimedia: Ajuste el control deslizante en el nivel de volumen que desee establecer en el dispositivo.
	Tonos de llamada y notificaciones: Ajuste el control deslizante en el nivel de volumen que desee establecer en el dispositivo.
	Llamadas de voz: Ajuste el control deslizante en el nivel de volumen que desee establecer en el dispositivo.
	Activar Notificaciones predeterminadas: Permite que suenen las notificaciones predeterminadas en el dispositivo.
	Activar Sonidos táctiles del teclado de marcación: Permite que suenen los tonos táctiles del teclado de marcado del dispositivo.
	Activar Sonidos táctiles: Permite que suenen los tonos táctiles del dispositivo.
	Activar Sonidos de bloqueo de pantalla: Permite que el dispositivo reproduzca un sonido al bloquearlo.
	Activar Vibrar al tocar**: Permite activar los ajustes de vibración.-
Activar Ajustes de pantalla	Active esta opción para definir los ajustes de pantalla: - Brillo de la pantalla: Ajuste el control deslizante en el nivel de brillo que desee establecer en el dispositivo.
	Activar Rotación automática de pantalla: Ajuste el control deslizante en el nivel de brillo que desee establecer en el dispositivo.
	Configurar modo de suspensión: Seleccione el periodo de tiempo que debe pasar para que la pantalla cambie al modo de suspensión.

4. Seleccione Guardar y publicar.

Ajustes personalizados

La carga útil de Ajustes personalizados puede utilizarse cuando se trata de nuevas funciones o versiones de la funcionalidad de Android que Workspace ONE UEM Console no admite actualmente a través de sus cargas útiles nativas. Utilice la carga útil Ajustes personalizados y el código XML para

activar o desactivar determinados ajustes manualmente.

1. Desplácese a Recursos > Perfiles y líneas base > Perfiles > Agregar > Agregar perfil > Android.
2. Configure los ajustes de la sección General del perfil.
3. Configure la carga útil apropiada (por ejemplo, Restricciones o Código de acceso).

   Puede trabajar con una copia del perfil, guardada en un grupo organizativo de "prueba", para evitar que haya usuarios afectados antes de que esté listo para guardar y publicar.
4. Utilice Guardar, pero no publique el perfil.
5. Seleccione el botón de radio de Perfiles > Vista en lista para la fila del perfil que desee personalizar.
6. Seleccione el botón XML situado en la parte superior para ver el perfil XML.
7. Para la carga útil de perfil que configuró anteriormente, copie la sección de código XML incluida enylas etiquetas (incluidas estas etiquetas). Si el perfil tiene varias cargas útiles, identifique lasetiquetas de la carga útil de la que desea copiar el código XML. Por ejemplo, un perfil de código de acceso tendrá unaetiqueta con un valor de "tipo" de com.airwatch.android.androidwork.apppasswordpolicy.
8. Copie esta sección de texto y cierre la vista de XML. Abra su perfil.
9. Seleccione la carga útil Ajustes personalizados y después Configurar. Pegue en el cuadro de texto el XML que ha copiado. El código XML que pegue debe contener el bloque completo de código, desde hasta.
   - Este XML debe contener el bloque de código completo que aparece en la lista para cada XML personalizado.
   - Los administradores deben configurar los ajustes desdehastacomo se desee.
   - Si se requieren certificados, configure una carga de certificado en el perfil y haga referencia a la PayloadUUID en la carga útil de ajustes personalizados.
10. Elimine la carga útil configurada originalmente seleccionando la sección de cargas útiles básicas y el botón menos [-]. Ahora puede mejorar el perfil agregando el código XML personalizado para la nueva funcionalidad.
    - Al aplicar ajustes personalizados para el perfil de Launcher, asegúrese de que está utilizando el tipo de característica adecuado para su tipo de perfil:
      - Para los perfiles de Android, use characteristic type = "com.airwatch.android.androidwork.launcher".
      - Para los perfiles de Android (heredado), use characteristic type = "com.airwatch.android.kiosk.settings".

    Cualquier dispositivo que no haya sido actualizado a la versión más reciente ignorará cualquier mejora que usted haya creado. Como el código está personalizado, debe probar dispositivos del perfil con versiones anteriores para verificar el comportamiento esperado.
11. Seleccione Guardar y publicar.

Envío de la configuración de la aplicación para las aplicaciones

Puede enviar pares clave-valor de configuración de la aplicación a través del perfil de ajustes personalizados de Android. Para ello, siga la siguiente plantilla y proporcione: - El ID de paquete de la aplicación - Para cada par clave-valor de configuración de la aplicación, el nombre de la clave, el valor y el tipo de datos de valor

```
    <characteristic   uuid="a0a4acc3-9de1-493b-b611-eb824ffed00f"   type="com.airwatch.and
roid.androidwork.app:packageID" target="1">
    <parm  name="key1"  value="string"  type="string"  />
    <parm  name="key2"  value="1"  type="integer"  />
    <parm  name="key3"  value="False"  type="boolean"  />
        </characteristic>
```

Ejemplo

```
<characteristic  uuid="a0a4acc3-9de1-493b-b611-eb824ffed00f"  type="com.airwatch.android
.androidwork.app:com.airwatch.testapp"  target="1">
    <parm  name="server_hostname"  value="test.com"  type="string"  />
    <parm  name="connection_timeout"  value="60"  type="integer"  />
    <parm  name="feature_flag"  value="True"  type="boolean"  />
</characteristic>
```

Aviso: La configuración de la aplicación se puede agregar durante la asignación de aplicaciones de Android. Consulte Agregar asignaciones y exclusiones a las aplicaciones para obtener más información.

Incluir una aplicación VPN en la lista de permitidos para VPN siempre activa

Para incluir en la lista de permitidos un cliente VPN para VPN siempre activa, envíe una carga útil de perfil de ajustes personalizados mediante el uso de esta plantilla y la provisión del ID de paquete de aplicación.

```
<characteristic  uuid="a0a4acc3-9de1-493b-b611-eb824ffed00f"  type="com.airwatch.android
.androidwork.app:packageID"  target="1">
    <parm  name="EnableAlwaysOnVPN"  value="True"  type="boolean"  />
</characteristic>
```

Aviso: Para enviar la configuración de la aplicación y activar VPN siempre activa para una aplicación, combine este par clave-valor con los pares clave-valor de configuración de la aplicación e impleméntelos como una única carga útil de ajustes personalizados.

XML personalizado para dispositivos Android

En Android 11, los clientes que utilizan atributos personalizados de terceros deben utilizar el perfil de ajustes personalizados para especificar una ubicación alternativa para almacenar los archivos de atributos personalizados. Las aplicaciones de los clientes también tendrán que dirigirse a la misma ubicación de la carpeta, que puede requerir cambios en su aplicación.

XML personalizado de ejemplo (el valor puede diferir en función de la preferencia del cliente):

```
<characteristic    type="com.android.agent.miscellaneousSettingsGroup"    uuid="2c787565-1c4
a-4eaa-8cd4-3bca39b8e98b">
<parm   name="attributes_file_path"   value="/storage/emulated/0/Documents/Attributes"/></
```

```
characteristic>
```

Funciones de perfiles específicos para Android

Estas matrices de funciones proporcionan un resumen de las funcionalidades clave disponibles para cada sistema operativo y destacan las funciones más importantes que se encuentran disponibles para la administración del dispositivo para Android.

Función	Perfil de trabajo	Dispositivo corporativo administrado
Control de aplicaciones		
Inhabilitar acceso a las aplicaciones en la lista negra	✓	✓
Impedir la desinstalación de aplicaciones requeridas	✓	✓
Activar directiva de actualización del sistema		✓
Administración de permisos en tiempo de ejecución	✓	✓
Browser		
Permitir Cookies	✓	✓
Permitir imágenes	✓	✓
Activar JavaScript	✓	✓
Permitir ventanas emergentes	✓	✓
Permitir rastrear ubicación	✓	✓
Configurar ajustes de proxy	✓	✓
Forzar Google SafeSearch	✓	✓
Forzar modo de seguridad de YouTube	✓	✓
Activar Tocar para buscar	✓	✓
Activar proveedor de búsqueda predeterminado	✓	✓
Activar Administrador de contraseñas	✓	✓
Activar páginas de error alternativas	✓	✓
Activar Autocompletar	✓	✓
Activar impresión	✓	✓
Activar la función de proxy de compresión de datos	✓	✓
Activar Navegación segura	✓	✓
Inhabilitar la opción de guardar el historial del navegador	✓	✓
Impedir el acceso tras la advertencia de navegación segura	✓	✓
Inhabilitar protocolo SPDY	✓	✓
Activar la predicción de red	✓	✓

Función	Perfil de trabajo	Dispositivo corporativo administrado
Activar funciones obsoletas de la plataforma web temporalmente	✓	✓
Exigir búsqueda segura	✓	✓
"Capacidad de ""Modo incógnito"""	✓	✓
Permitir el inicio de sesión en Chromium	✓	✓
Activar sugerencias de búsqueda	✓	✓
Activar Traductor	✓	✓
Permitir marcadores	✓	✓
Permitir el acceso a determinadas direcciones URL	✓	✓
Bloquear el acceso a determinadas direcciones URL	✓	✓
Establecer la versión mínima de SSL	✓	✓
Política de código de acceso		
Solicitar al usuario que establezca un nuevo código de acceso	✓	✓
Número máximo de intentos de contraseña fallidos	✓	✓
Permitir código de acceso simple	✓	✓
Contraseña alfanumérica permitida	✓	✓
Establecer tiempo de espera de bloqueo del dispositivo (en minutos)	✓	✓
Establecer la vigencia máxima del código de acceso	✓	✓
Extensión del historial de contraseña	✓	✓
Extensión del historial de contraseña	✓	✓
Establecer extensión mínima del código de acceso	✓	✓
Establecer número mínimo de dígitos numéricos	✓	✓
Establecer número mínimo de minúsculas	✓	✓
Establecer número mínimo de mayúsculas	✓	✓
Establecer número mínimo de mayúsculas	✓	✓
Establecer número mínimo de caracteres especiales	✓	✓
Establecer número mínimo de símbolos	✓	✓
Comandos		
Permitir eliminación de empresa	✓	✓
Permitir eliminación total		✓
Permitir contenedor o eliminación de perfil	✓	
Permitir eliminación de tarjeta SD		✓

Función	Perfil de trabajo	Dispositivo corporativo administrado
Bloquear dispositivo	✓	✓
Permitir contenedor de bloqueo o perfil		
Correo electrónico		
Configuración de correo electrónico nativo	✓	✓
Permitir la sincronización de Contactos y Calendario	✓	✓
Red		
Configurar tipos de VPN	✓	✓
Activar la VPN por aplicación (solo disponible para clientes VPN específicos)	✓	✓
Utilizar inicio de sesión web para la autenticación (solo disponible para los clientes VPN específicos)	✓	✓
Establecer proxy global de HTTP		✓
Permitir conexión de datos a Wi-Fi	✓	✓
Siempre con VPN	✓	✓
Cifrado		
Requerir cifrado de dispositivo completo	✓	✓
Notificar estado de cifrado		

Administración de dispositivos Android con Workspace ONE UEM

Una vez que los dispositivos se inscriban y configuren, adminístrelos a través de Workspace ONE UEM Console. Sus herramientas y funciones de administración le permiten supervisar los dispositivos y realizar funciones administrativas de forma remota.

Puede administrar todos los dispositivos desde la consola de UEM. El tablero permite realizar búsquedas y vistas personalizadas que puede utilizar para filtrar y encontrar dispositivos específicos. Esta función simplifica la ejecución de funciones administrativas en un conjunto determinado de dispositivos. La Vista de lista de dispositivos muestra todos los dispositivos que se encuentran actualmente inscritos en su entorno de Workspace ONE UEM, así como su estado. Puede filtrar la vista de lista específica de Android y ver cómo se administran los dispositivos en una misma ventana.

Cómo utilizar la página de Detalles del dispositivo

La página Detalles del dispositivo proporciona información específica de los dispositivos, como los perfiles, las aplicaciones, la versión de Workspace ONE Intelligent Hub y la versión de servicio OEM que está instalada en el dispositivo. También puede realizar acciones remotas en el dispositivo desde la página Detalles del dispositivo que sea específica para tal dispositivo.

Puede acceder a la página Detalles del dispositivo seleccionando el Nombre descriptivo del dispositivo en la página Búsqueda de dispositivos, en uno de los paneles de control disponibles o mediante el uso de cualquiera de las herramientas de búsqueda disponibles en Workspace ONE UEM Console.

Estado de inscripción en los detalles del dispositivo

En algunos casos, la página Detalles del dispositivo no actualiza el estado de inscripción debido a las acciones realizadas a nivel local en el dispositivo.

Estos son algunos de los escenarios posibles:

- Cuando un usuario realiza un restablecimiento de fábrica desde la aplicación Ajustes de su dispositivo, el estado de inscripción no se actualiza en UEM Console.
- Si un usuario elimina el perfil de trabajo de la aplicación Ajustes de su dispositivo, el estado de inscripción no se actualiza en UEM Console.
- El estado de inscripción no se actualiza tras alcanzar el límite del perfil de trabajo o el código de acceso del dispositivo con errores, lo que activa un perfil de trabajo o una eliminación total del dispositivo en función del modo de inscripción:
    - En el perfil de trabajo, se borra el perfil de trabajo.
    - En los dispositivos COPE y totalmente administrados, se elimina todo el dispositivo.

Si los dispositivos se encuentran en el modo de ahorro de energía

Los dispositivos Android que ejecutan Android M usan las opciones de ahorro de energía para las aplicaciones y los dispositivos inactivos. Si un usuario desenchufa un dispositivo y lo deja fijo, con la pantalla apagada, durante un periodo de tiempo, el dispositivo cambia al modo de espera, en el cual intenta mantener el dispositivo en un estado de suspensión. Durante este tiempo no habrá actividad de red.

Además, el modo Aplicación en espera permite al dispositivo determinar que una aplicación está inactiva cuando el usuario no la está utilizando de manera activa. Cuando los dispositivos están en alguno de estos estados, la consola administrativa de Workspace ONE UEM no recibe informes de los detalles del dispositivo. Cuando el usuario enchufe un dispositivo para cargarlo o abra una aplicación, el dispositivo reanudará las operaciones normales y la creación de informes desde las aplicaciones de AirWatch instaladas en el dispositivo para la consola de Workspace ONE UEM.

Arranque directo para dispositivos Android**

El modo de arranque directo es cuando el dispositivo se ha encendido pero el usuario no ha desbloqueado el dispositivo. En este estado, las aplicaciones no pueden ejecutarse con normalidad. Las aplicaciones, como Workspace ONE Intelligent Hub for Android, no pueden enviar muestras a UEM Console ni realizar funciones compatibles cuando el dispositivo se encuentra en este estado.

El arranque directo afecta a los dispositivos inscritos en el modo de perfil de trabajo de forma diferente. El perfil de trabajo seguirá estando bloqueado en el modo de arranque directo hasta que el perfil de trabajo se desbloquee introduciendo el código de acceso del perfil de trabajo, si existe uno. De esta manera, es posible que las aplicaciones fuera del perfil de trabajo puedan funcionar normalmente si el dispositivo está desbloqueado, pero es posible que las aplicaciones dentro del perfil de trabajo aún se bloqueen en el modo de arranque directo hasta que el usuario desbloquee el perfil de trabajo.

Cuando un dispositivo se bloquea durante el modo de inscripción Perfil de trabajo, la pantalla de bloqueo del perfil de trabajo admite el botón "Olvidé mi contraseña" para los dispositivos Android 11 que tienen contraseñas de dispositivo y de perfil de trabajo distintas.

Cuando un usuario selecciona "Olvidé mi contraseña", se le solicita que se ponga en contacto con su administrador de TI. Al seleccionar "Olvidé mi contraseña", el botón también inicia el perfil de trabajo en modo de arranque directo (bloqueado), lo que permite que su DPC lleve a cabo los pasos para realizar un restablecimiento seguro del código de acceso del perfil de trabajo.

Comandos de dispositivos Android compatibles por modo de inscripción

Esta matriz muestra los comandos de dispositivo disponibles por modo de inscripción.

Aviso: El comando Borrar código de acceso en el arranque directo solo es compatible con FCM (Firebase Cloud Messaging). AWCM no es compatible.

Aviso: El comando de bloqueo para dispositivos COPE con Android 11 o versiones posteriores solo bloquea el perfil de trabajo, no todo el dispositivo.

El asterisco indica qué comandos son compatibles mientras los dispositivos están en modo de arranque directo. La ejecución de comandos en el modo de arranque directo solo es compatible cuando Workspace ONE UEM utiliza FCM (Firebase Cloud Messaging) para la comunicación con los

dispositivos. Para obtener más información, consulte Ajustes de Android para Workspace ONE Intelligent Hub.

Comando de dispositivo	Modo Dispositivo administrado de trabajo	Perfil de trabajo	COPE (Android 8.0-Android 10)	COPE Android 11 o versión posterior
Consultar dispositivo	✓	✓	✓	✓
Enviar	✓	✓	✓	✓
Bloquear	✓	✓	✓	✓
Borrar código de acceso				
Borrar el código de acceso del dispositivo	✓*		✓	
Borrar el código de acceso del perfil de trabajo		✓	✓*	✓*
Generar token de la aplicación	✓	✓	✓	✓
Administración				
Cambiar el código de acceso del dispositivo	✓		✓	
Cambiar el código de acceso de trabajo		✓	✓	✓
Bloquear sesión de SSO	✓	✓	✓	✓
Reiniciar el dispositivo	✓			
Eliminación empresarial		✓*		✓
Borrar todo	✓*		✓*	✓*
Soporte				
Buscar dispositivo	✓	✓	✓	✓
Sincronizar dispositivo	✓	✓	✓	✓
Administración				
Cambiar grupo organizativo	✓	✓	✓	✓
Cómo administrar etiquetas	✓	✓	✓	✓
Editar dispositivo	✓	✓	✓	✓
Eliminar dispositivo	✓*	✓	✓*	✓*
Solicitar registro de dispositivos	✓	✓	✓	✓
Reemplazar nivel de registro del trabajo	✓			
Avanzado				

Comando de dispositivo	Modo Dispositivo administrado de trabajo	Perfil de trabajo	COPE (Android 8.0-Android 10)	COPE Android 11 o versión posterior
Iniciar/Detener AWCM	✓	✓	✓	✓
Sincronizar dispositivo	✓	✓	✓	✓

Utilice las pestañas del menú Detalles del dispositivo para acceder a información específica del dispositivo, como la siguiente:

- Resumen: consulte las estadísticas generales, tales como los estados de inscripción, la conformidad, la última detección, la plataforma/modelo/SO, el grupo organizativo, la información de contacto, el número de serie, el estado de alimentación incluido el estado de la batería, la capacidad de almacenamiento, la memoria física y la memoria virtual. Los dispositivos Zebra cuentan con un panel en el que se muestra información detallada de la batería. Podrá, asimismo, consultar Workspace ONE Intelligent Hub y qué versión del OEM correspondiente está instalada actualmente en el dispositivo. Aviso: Si los dispositivos Android informan sobre un fabricante y un modelo que se determina que no son válidos según los estándares de Android, el campo Modelo/SO del resumen de los dispositivos se muestra en Console como "Desconocido".
- Conformidad: vea el estado, el nombre de la política, la fecha de la prueba de conformidad anterior y la próxima prueba de conformidad, además de las acciones que ya se han realizado en el dispositivo.
- Perfiles: vea todos los perfiles de MDM que están actualmente instalados en el dispositivo.
- Aplicaciones: vea todas las aplicaciones actualmente instaladas en el dispositivo o que están a la espera de instalación en el mismo. Para las aplicaciones internas, se muestra el estado de instalación de todas las aplicaciones. En el caso de las aplicaciones públicas, solo se muestra el caso de las aplicaciones que tienen un icono que se puede iniciar en el dispositivo. No se muestrearán aplicaciones no administradas que no tengan un icono que se pueda iniciar.
- Contenido: vea el estado, el tipo, el nombre, la prioridad, la implementación, la última actualización, la fecha y la hora de las vistas, y proporcione una barra de herramientas para realizar acciones administrativas (instalar o eliminar contenido). Plataforma Android (heredado) VMware, Inc. 77
- Ubicación: vea la ubicación actual y el historial de ubicaciones del dispositivo. Si el dispositivo se encuentra en el modo de ahorro de energía, es posible que los datos de ubicación no se actualicen durante el modo de espera. Se solicita a los usuarios que activen Precisión de ubicación de Google en cualquier dispositivo en el que: La recopilación de datos de ubicación está habilitada en Ajustes de Intelligent Hub en el grupo organizativo del dispositivo o La recopilación de datos de ubicación está habilitada en Ajustes de privacidad del dispositivo (según el grupo organizativo y el tipo de propiedad). Se pedirá a los usuarios que concedan permisos de ubicación de Hub en el perfil de trabajo y los dispositivos COPE en Android 12 y versiones posteriores. Para obtener más información, consulte Ajustes de Android para Workspace ONE Intelligent Hub.
- Usuario: acceda a los detalles sobre el usuario de un dispositivo y también al estado de los otros dispositivos inscritos en ese mismo usuario. Puede acceder a las pestañas del menú seleccionando Más en la pestaña principal Detalles del dispositivo.

- Red: vea el estado de la red actual del dispositivo (Celular, Wi-Fi, Bluetooth). Aviso: Si los servicios de ubicación no están habilitados en un dispositivo, es posible que no se pueda recopilar e informar del SSID activo. En estos casos, el SSID se notifica como "SSID desconocido".
- Telecom: vea la cantidad de llamadas, datos y mensajes enviados y recibidos en el dispositivo.
- Notas: permite ver y agregar notas sobre el dispositivo. Por ejemplo, puede observar el estado de envío o si el dispositivo está en reparación o fuera de servicio.
- Certificados: permite identificar los certificados de dispositivos por nombre y emisor. Esta pestaña también proporciona información acerca de la fecha de caducidad del certificado.
- Productos: permite ver el historial y el estado de todos los paquetes que se han aprovisionado al dispositivo y cualquier error de aprovisionamiento.
- Atributos personalizados: permite utilizar la funcionalidad avanzada de aprovisionamiento de productos.
- Archivos/acciones: permite ver los archivos y el resto de acciones asociadas con el dispositivo.
- Acciones de evento: permite tomar medidas en un dispositivo cuando se cumplen las condiciones predeterminadas
- Registro del dispositivo compartido: permite ver el historial del dispositivo en términos de Dispositivo compartido, como las protecciones/desprotecciones anteriores y el estado actual.
- Solución de problemas: permite consultar la información de registro del Registro de eventos y los Comandos. Esta página muestra las funciones de exportación y búsqueda para que pueda realizar análisis y búsquedas detalladas.
- Registro de eventos: permite ver información detallada sobre la depuración de errores y los accesos al servidor, como un filtro por tipo de grupo de eventos, intervalo de fechas, gravedad, módulo y categoría. En la lista Registro de eventos, la columna Datos del evento puede presentar enlaces de hipertexto que abren una pantalla independiente con más detalles sobre el evento. Esta información permite realizar tareas avanzadas de solución de problemas, como determinar por qué el perfil no se puede instalar.
- Comandos – Vea una lista detallada de los comandos pendientes, en fila y completos que fueron enviados al dispositivo. Incluye un Filtro que le permite filtrar comandos según la Categoría, Estado y Comando específico.
- Detección de estado comprometido: permite ver los detalles relacionados con el estado comprometido del dispositivo, como el Motivo específico para ese estado y el nivel de gravedad del mismo.
- Historial de los estados: permite ver el historial del dispositivo en referencia al estado de inscripción.
- Registro especificado: permite ver los registros de Console, el catálogo, los servicios de dispositivos, la administración de dispositivos y el portal de autoservicio. Debe habilitar la opción Registro especificado en la configuración. Se proporciona un enlace para tal fin. A continuación, debe seleccionar el botón Crear registro y seleccionar el período de tiempo durante el que se recopilará el registro.

- Archivos adjuntos: utilice el espacio de almacenamiento del servidor para capturas de pantalla, documentos y enlaces, así como para solucionar problemas, entre otros usos, sin tener que utilizar el espacio del propio dispositivo.

Comportamiento de las direcciones MAC para Android

En los dispositivos que ejecutan Android 10 o superior, el sistema transmite direcciones MAC aleatorias de forma predeterminada. Esto es diferente de las versiones anteriores de Android.

La versión del sistema operativo Android y el tipo de inscripción determinan cómo recopilamos la dirección MAC de Wi-Fi:

- Los dispositivos totalmente administrados pueden recopilar la dirección MAC de Wi-Fi del hardware en todas las versiones del SO.
- Los dispositivos COPE pueden recopilar la dirección MAC de Wi-Fi del hardware en todos los sistemas operativos.
- Los dispositivos del perfil de trabajo pueden recopilar la dirección MAC de Wi-Fi del hardware en Android 9 y versiones anteriores.
- Los dispositivos del perfil de trabajo pueden recopilar la dirección MAC de Wi-Fi aleatoria para el SSID activo en Android 10 o versiones posteriores.

Puede encontrar la dirección MAC en la pestaña Red de Detalles del dispositivo.

Comandos de administración de dispositivos para dispositivos Android

El menú desplegable Más de la página Detalles del dispositivo le permite realizar acciones remotas de manera inalámbrica en el dispositivo seleccionado. Las acciones mencionadas a continuación varían en función de determinados factores como la plataforma del dispositivo, los ajustes de Workspace ONE UEM Console y el estado de inscripción.

Borrar código de acceso

- Borrar código de acceso (dispositivo): permite borrar el código de acceso del dispositivo. Se puede utilizar cuando el usuario haya olvidado el código de acceso del dispositivo.
- Generar token de la aplicación: puede generar el token de la aplicación para aquellos usuarios que olvidan su información de inicio de sesión de las aplicaciones creadas mediante Workspace ONE SDK.
- Borrar código de acceso de trabajo: permite borrar el código de acceso de trabajo o de contenedor. Se puede utilizar cuando el usuario haya olvidado el código de acceso del dispositivo.

Administración

- Cambiar el código de acceso del dispositivo: permite reemplazar cualquier código de acceso existente del dispositivo para acceder al dispositivo con uno nuevo.
- Cambiar código de acceso de trabajo: seleccione esta opción para eliminar amenazas a la seguridad del trabajo en el dispositivo. Para Android 8.0 o versiones posteriores.
- Bloquear SSO: permite bloquear al usuario del dispositivo para que no pueda utilizar el contenedor de Workspace ONE UEM ni ninguna otra aplicación.

- Reiniciar el dispositivo: permite reiniciar el dispositivo de forma remota para reproducir el efecto de apagarlo y encenderlo de nuevo.
- Eliminación total de los dispositivos: permite enviar un comando MDM para el borrado completo de todos los datos y el sistema operativo del dispositivo. Esta acción no se puede deshacer.
- Bloquear SSO: permite bloquear al usuario del dispositivo para que no pueda utilizar el contenedor de Workspace ONE UEM ni ninguna otra aplicación.
- Eliminación empresarial: elimina los datos empresariales del dispositivo sin afectar a los datos personales. En los dispositivos Android 11+ inscritos en COPE, la eliminación empresarial anula la inscripción del dispositivo, elimina el perfil de trabajo y deja el perfil personal en intacto.

Soporte

- Buscar dispositivo: permite enviar un mensaje de texto a la aplicación de Workspace ONE UEM correspondiente junto con un sonido audible diseñado para ayudar al usuario a ubicar un dispositivo que se haya perdido. Entre las opciones de sonido audible se incluye la reproducción de un sonido una cantidad configurable de veces y la duración del intervalo, en segundos, entre los sonidos.
- Sincronizar dispositivo: permite sincronizar el dispositivo seleccionado con UEM Console para alinear el estado de Última detección.

Administración

- Cambiar grupo organizativo: permite cambiar el grupo organizativo principal del dispositivo a otro GO existente. Incluye una opción para seleccionar un grupo organizativo estático o dinámico. Si desea cambiar el grupo organizativo de varios dispositivos a la vez, debe seleccionar dispositivos para la acción en masa mediante el método de selección en bloque (con la tecla Mayús) en lugar de la casilla de verificación Global (que está situada junto al encabezado de la columna Última detección que aparece en la vista de lista de dispositivos).
- Administrar etiquetas:
- Editar dispositivo: permite editar la información del dispositivo, como Nombre común, Número de activo, Propiedad del dispositivo, Grupo de dispositivos y Categoría del dispositivo.
- Eliminar dispositivo: permite eliminar y anular la inscripción de un dispositivo de la consola. Envía el comando de eliminación empresarial al dispositivo que se eliminará en el próximo check-in y marca el dispositivo como Eliminación en curso en la consola. Si la protección contra eliminaciones está deshabilitada en el dispositivo, el comando emitido realiza inmediatamente una eliminación empresarial y elimina la representación del dispositivo en la consola.
- Solicitar registro de dispositivo: permite solicitar el registro de depuración del dispositivo seleccionado para, a continuación, verlo seleccionado la pestaña Más y Archivos adjuntos > Documentos. No es posible ver el registro en Workspace ONE UEM Console. El registro se envía como un archivo ZIP que puede utilizarse para solucionar problemas y proporcionar soporte. Al solicitar un registro, se puede optar por recibir los registros del sistema o el de Hub. El sistema proporciona registros de nivel de sistema. Hub proporciona registros de los

diversos agentes que se ejecutan en el dispositivo.

Solo para Android: puede recuperar registros detallados desde dispositivos Android corporativos y verlos en la consola para resolver rápidamente los problemas en el dispositivo.

- Reemplazar nivel de registro del trabajo: permite reemplazar el nivel específico de un registro de evento de trabajo en el dispositivo seleccionado. Esta acción establece el nivel de detalle de los registros de los trabajos enviados a través del aprovisionamiento de productos y reemplaza el nivel de registro actual que esté configurado en los ajustes de Android Hub. El reemplazo del nivel de registro del trabajo se puede borrar mediante la selección del elemento del menú desplegable Restablecer valores predeterminados en la pantalla de la acción. También puede cambiar el nivel de registro del trabajo en la categoría Aprovisionamiento de producto en los ajustes del Hub de Android.

Avanzado

- Iniciar/Detener AWCM: permite iniciar o detener el servicio VMware AirWatch Cloud Messaging en el dispositivo seleccionado. VMware AirWatch Cloud Messaging (AWCM) simplifica la entrega de mensajes y comandos desde la consola de administración. AWCM acaba con la necesidad de que los usuarios finales accedan a la red pública de Internet o de que utilicen cuentas de consumidor como, por ejemplo, los ID de Google.
- Sincronizar dispositivo: permite sincronizar el dispositivo seleccionado con UEM Console para alinear el estado de Última detección.

Pestaña Aplicaciones de detalles

La pestaña Aplicaciones de detalles de dispositivos de Workspace ONE UEM Console contiene opciones para controlar las aplicaciones públicas en el dispositivo. Puede ver las aplicaciones que se han asignado a UEM Console, así como las aplicaciones personales basadas en el tipo de inscripción y las configuraciones de privacidad.

Los administradores pueden ver información acerca de la aplicación, como el estado de instalación, el tipo de aplicación, la versión de la aplicación y el identificador de aplicación.

La opción Instalar del menú de acciones permite seleccionar las aplicaciones asignadas de la vista de lista en insertarlas mediante push directamente en el dispositivo. La opción Eliminar del menú Acciones le permite desinstalar la aplicación del dispositivo de manera silenciosa.

Las inscripciones del perfil de trabajo solo muestran las aplicaciones asignadas por el administrador y no mostrarán las aplicaciones personales instaladas por el usuario. Las inscripciones administradas de trabajo muestran todas las aplicaciones, puesto que Workspace ONE UEM tiene el control total del dispositivo y no existe el concepto de aplicaciones personales. Para una inscripción COPE, la pestaña de aplicaciones de detalles del dispositivo muestra las aplicaciones administradas, que incluyen las aplicaciones internas que se instalan en la sección personal de forma predeterminada.

Workspace ONE UEM Console no mostrará aplicaciones que los usuarios no puedan iniciar. La consola de UEM informa del estado de las aplicaciones que tienen un icono de iniciador en el que el usuario puede hacer clic y abrir. Por lo tanto, las aplicaciones en segundo plano o las aplicaciones de servicio no se muestran en los detalles del dispositivo.

El comando Solicitar registro de dispositivo permite recuperar Workspace ONE Intelligent Hub o los registros detallados del sistema de dispositivos corporativos y visualizarlos en Console para resolver

rápidamente cualquier problema en el dispositivo. El cuadro de diálogo Solicitar registro de dispositivo permite personalizar la solicitud de registro de los dispositivos Android. Consulte más detalles a continuación.

Solicitar registro de dispositivos

El comando Solicitar registro de dispositivo permite recuperar Workspace ONE Intelligent Hub o los registros detallados del sistema de dispositivos corporativos y visualizarlos en Console para resolver rápidamente cualquier problema en el dispositivo. El cuadro de diálogo Solicitar registro de dispositivo permite personalizar la solicitud de registro de los dispositivos Android.

1. Desplácese a Grupos y ajustes > Todos los ajustes > Dispositivos y usuarios > General > Privacidad y habilite la opción Solicitar registro de dispositivos en los ajustes de privacidad.

   Los dispositivos que son propiedad de los empleados no se pueden seleccionar debido a cuestiones de privacidad

2. Desplácese a Dispositivos > Vista de lista > Seleccionar dispositivo de la lista > Más acciones > Solicitar registro de dispositivos.

3. Personalice los ajustes de registro:

Ajustes	Descripción
Fuente	Seleccione Hub para recopilar los registros generados por Workspace ONE Intelligent Hub.
	Seleccione Sistema para incluir todas las aplicaciones y los eventos en el dispositivo. El sistema está disponible en función de los ajustes de privacidad y se limita a los fabricantes de dispositivos con aplicaciones de servicios específicos de la plataforma. Aviso: Disponible en los dispositivos que ejecuten Platform OEM Service v3.3+, MSI Service v1.3+ y Honewell Service v3.0+.
	Seleccione Red para registrar las solicitudes de DNS y las conexiones de red de las aplicaciones en un archivo de registro durante el periodo especificado. Aviso: Disponible en dispositivos administrados de trabajo que ejecuten Android 8 o versiones posteriores. Aviso: La opción de recopilación de direcciones IP públicas debe estar habilitada en los ajustes de privacidad.
	Seleccione Seguridad para recopilar registros de seguridad que detallen posibles infracciones de seguridad, tales como las actividades previas y posteriores al arranque, los intentos de autenticación, la modificación del almacenamiento de credenciales, intentos de conexiones a ADB, etc. Aviso: Requiere dispositivos administrados de trabajo con Android 7.0 o versiones posteriores y Workspace ONE Intelligent Hub 21.05 for Android. La opción Seguridad aparecerá sombreada si los dispositivos no cumplen con estos requisitos.
Tipo	Seleccione Instantánea para recuperar las últimas entradas de registro disponibles en los dispositivos. Seleccione Programado para recopilar un registro gradual a lo largo de un periodo determinado. Es posible enviar varios archivos de registro a UEM Console. La opción "Nivel" no estará disponible cuando se selecciona la opción Red
Duración	Especifique el periodo de tiempo durante el cual el dispositivo recopilará e informará de los registros a Console.
Nivel	Determine el nivel de detalle que se incluye en el registro (Error, Advertencia, Información, Depuración, Detallado).

4. Seleccione Guardar.

5. Para revisar los archivos de registro, desplácese a Detalles del dispositivo > Más > Archivos adjuntos > Documentos.

6. Cancele la solicitud de registro del dispositivo una vez que se hayan recibido los registros y no haya necesidad de realizar una recopilación de registros. Desplácese hasta Dispositivos > Vista de lista > Seleccionar dispositivo de la lista > Más acciones > Cancelar registro de dispositivo para cancelar la solicitud de registro del dispositivo.

Atestación de SafetyNet

La atestación de SafetyNet es una API de Google que se usa para validar la integridad del dispositivo, lo que garantiza que no está en riesgo.

SafetyNet valida la información de software y hardware en el dispositivo y crea un perfil de ese dispositivo. Esta atestación ayuda a determinar si se ha manipulado o modificado un dispositivo en particular. Cuando Workspace ONE UEM Console ejecuta la API de atestación de SafetyNet e informa de que el dispositivo está en riesgo, en la página Detalles del dispositivo de la consola de UEM informa de que el dispositivo está en riesgo. Si la atestación de SafetyNet detecta que el dispositivo está en peligro, la única forma de revertir el estado de un dispositivo en peligro es volver a inscribir al dispositivo afectado.

Es importante tener en cuenta que la atestación de SafetyNet no vuelve a evaluar el estado comprometido una vez que se ha informado inicialmente del mismo.

La atestación de SafetyNet solo es compatible con Workspace ONE Intelligent Hub.

Habilitar la atestación de SafetyNet Habilite la API de atestación de SafetyNet en UEM Console para validar la integridad de un dispositivo y determinar si el dispositivo está en riesgo.

1. Desplácese a Grupos y ajustes > Todos los ajustes > Aplicaciones > Ajustes y políticas > Ajustes > Ajustes personalizados
2. Pegue el siguiente XML personalizado en el campo Ajustes personalizados: { “SafetyNetEnabled”:true }
3. Guarde el XML personalizado.
4. Compruebe SafetyNet en la pestaña Resumen de la página Detalles del dispositivo en UEM Console. Si no ve el estado de la atestación de SafetyNet, puede enviar un comando remoto para reiniciar el dispositivo.

Actualizaciones de sistema de Android con Workspace ONE UEM

La página de la consola de actualizaciones de Android incluye todas las actualizaciones de firmware disponibles para dispositivos Android. En esta página, puede revisar e insertar actualizaciones para dispositivos Android. Esto resulta útil para realizar pruebas a fin de resolver problemas de compatibilidad y supervisar las actualizaciones disponibles en los dispositivos antes de enviar actualizaciones de firmware a la flota de dispositivos.

Las actualizaciones se enumeran por fecha de lanzamiento e incluyen datos como la información sobre OEM, modelo y operadores específicos. Cada combinación de modelo/operador es una actualización de firmware diferente.

Por ejemplo, puede ver Samsung Galaxy S7 para T-mobile y una actualización independiente para Samsung Galaxy S7 en Sprint. La lista se puede clasificar por OEM y operador.

Publicar actualizaciones de firmware (Android)

La página de la consola de actualizaciones de Android incluye todas las actualizaciones de firmware disponibles para dispositivos Android y le permite ver versiones de firmware específicas y seleccionar la opción para indicar al usuario que instale la actualización.

1. Desplácese hasta Dispositivos Actualizaciones de dispositivos.
2. Seleccione el botón de radio junto a la actualización que desee.
3. Seleccione Administrar actualización.
4. Configure los ajustes:

Ajustes	Descripción
Método de instalación	Seleccione Instalación automática para seleccionar el período de tiempo a fin de programar las actualizaciones. Seleccione Instalación a pedidoy se solicitará a los usuarios que acepten las actualizaciones de firmware para que se instalen en el dispositivo.
Inicio de la implementación	Programe la fecha y la hora de inicio de la actualización. Las actualizaciones se pueden programar con una antelación máxima de 30 días y con un margen máximo de actualización de 7 días. Las actualizaciones que se encuentren en este margen se publicarán en los dispositivos cada 4 horas en la zona horaria del servidor.
Final de la implementación	Programe la fecha y la hora de finalización de la actualización.

Ajustes	Descripción
Zona horaria del servidor	Este campo es de solo lectura ya que se genera desde el servidor.
Red	Seleccione si desea implementar las actualizaciones cuando los dispositivos estén conectados en Solo Wi-Fi o Cualquiera (cualquier conexión de red).

5. Seleccione Publicar. La ventana Administrar actualización se cierra y UEM Console muestra la página Actualizaciones.

   Aviso: Si por alguna razón es necesario cancelar o cambiar la actualización, seleccione la actualización que desee y, a continuación, seleccione Cancelar programación en la ventana Administrar actualización.

Dado que las actualizaciones se agrupan en lote en grupos de dispositivos, no se pueden revocar los dispositivos actualizados previamente.

Actualizaciones de Samsung Enterprise Firmware Over The Air (EFOTA)

Samsung Enterprise Firmware Over the Air (EFOTA) le permite gestionar y restringir las actualizaciones de firmware en dispositivos Samsung con Android 7.0 Nougat y versiones posteriores.

En el caso de dispositivos Samsung, debe registrarse para obtener una licencia de Samsung E-FOTA con el fin de obtener actualizaciones. Las funciones no estarán disponibles hasta que se haya registrado.

El flujo de Samsung EFOTA implica registrar los ajustes de EFOTA suministrados por su distribuidor autorizado. Para ello, debe habilitar "Registrar Enterprise FOTA" en el perfil de restricciones de Android, y visualizar y seleccionar las actualizaciones aplicables para enviarlas mediante push a los dispositivos.

Samsung EFOTA solo se puede configurar en el grupo organizativo de nivel de cliente para que todos los dispositivos registrados en ese grupo de organización reciban actualizaciones. Considere la opción de crear un grupo organizativo independiente para realizar pruebas antes del envío a todos los dispositivos.

Registrar actualizaciones de Samsung Enterprise Firmware Over The Air

Utilice la página Dispositivos y usuarios > Ajustes del sistema para introducir los ajustes de EFOTA proporcionados por Samsung o por su distribuidor autorizado.

1. Desplácese a Dispositivos > Ajustes del dispositivo > Dispositivos y usuarios > Android > Samsung Enterprise FOTA.
2. Introduzca los siguientes ajustes:

Ajustes	Descripción

ID de cliente	Introduzca el ID proporcionado por su distribuidor autorizado.
Licencia	Introduzca la licencia proporcionada por su distribuidor autorizado.
ID de cliente	Introduzca el ID de cliente proporcionado por su distribuidor autorizado.
Secreto del Client	Introduzca el secreto de cliente proporcionado por su distribuidor autorizado.

3. Seleccione Guardar.

Configurar el perfil de restricciones (Samsung EFOTA)

Los perfiles de restricciones bloquean la funcionalidad nativa de los dispositivos Android y varían según el OEM. Al habilitar la restricción "Registrar Enterprise FOTA", los dispositivos asignados se bloquean a su versión actual de firmware.

Este campo en el perfil de restricciones solo está disponible cuando se selecciona Samsung en el campo Ajustes de OEM.

1. Desplácese a Dispositivos > Perfiles y recursos > Perfiles > Agregar > Agregar perfil > Android > Restricciones.
2. Seleccione Configurar
3. Habilite Registrar Enterprise FOTA.

   Permitir actualización de forma inalámbrica (OTA) debe estar habilitada o las actualizaciones de firmware se bloquean.
4. Seleccione Guardar y publicar.

Actualización del SO Android para dispositivos administrados de trabajo

Actualice los dispositivos administrados de trabajo de Android de forma remota con un archivo zip local a través de la acción Archivo de actualización del SO.

Esta tarea de actualización del SO se aplica específicamente a los dispositivos administrados de trabajo que ejecutan Android 10.0 o una versión posterior. Si desea actualizar el SO en dispositivos Zebra, consulte Crear una actualización del sistema operativo para dispositivos Zebra, Android 8.0+.

Procedimiento

1. Recuperar el paquete/archivo zip de actualización del SO desde el OEM
2. Desplácese a Archivo/Acción en Dispositivos > Aprovisionamiento > Componentes > Archivos/Acciones para cargar el archivo zip. El manifiesto de instalación debe contener la acción Actualizar el SO con el archivo zip cargado seleccionado
3. El archivo zip debe descargarse en el directorio de almacenamiento interno de Hub. Utilice el comodín $osupdate$ en la ubicación de descarga del archivo, que encontrará la ruta de archivo correcta independientemente del OEM.
4. Ejemplo: $osupdate$/update.zip
5. Agregue el Archivo/Acción a un manifiesto de producto. Configure cualquier otro criterio, como las condiciones de asignación e implementación.

6. Hub descarga un zip y llama a la API de actualización del SO
7. El dispositivo se reinicia en recuperación e instala la actualización (o en el caso de una actualización A/B, el dispositivo simplemente se reinicia en una nueva versión cuando está listo)
8. Hub realiza la validación posterior a la actualización para asegurarse de que se ha instalado la nueva compilación
9. Hub también actualizará el atributo personalizado del número de compilación que se notifica a Console

Resultados

Tras una validación correcta, el producto pasa al estado completo/conforme y el atributo personalizado del número de compilación del dispositivo se actualiza a la nueva versión.