Empresas

Comunicación y conectividad | Cloud | IoT | Seguridad

Conceptos básicos de Console

VMware Workspace ONE UEM sevices

vmware

Puede encontrar la documentación técnica más actualizada en el sitio web de VMware: https://docs.vmware.com/es/

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

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

Contenido

Cómo trabajar en UEM Console 9

- Navegadores compatibles 9
- Menú de encabezado 10
- Búsqueda global 11
- Búsqueda de un grupo organizativo 12
- Buscar ajustes 12
- Cómo contraer y expandir el submenú 12
- Cómo adaptar la interfaz de usuario con la personalización de marca 13
- Cómo unirse o abandonar el Programa de mejora de la experiencia del cliente 14

Inicio de sesión en la Console 15

- Caducidad de la contraseña 17
- Tiempos de espera y cierres de sesión 17
- Bloqueos de inicio de sesión 17
- Cómo consultar eventos de la consola de bloqueo de cuenta 18
- Administrar ajustes de cuenta 18
- Administrar ajustes de cuenta: Usuario 18
- Administrar ajustes de cuenta: Notificaciones 19
- Administrar ajustes de cuenta: Inicios de sesión 19
- Administrar ajustes de cuenta: Seguridad 19
- Administrar ajustes de cuenta: Contraseña 19
- Administrar ajustes de cuenta: Preguntas de recuperación de contraseña 19
- Administrar ajustes de cuenta: PIN de seguridad 20
- Uso de cookies (solo visible para administradores de VMware Cloud Services) 20
- Cómo restringir acciones de UEM Console 20
- Cómo seleccionar acciones para proteger la contraseña 23
- Cómo configurar notas requeridas para las acciones 25

Uso del asistente de introducción 27

- Cómo acceder al asistente de introducción 27
- Cómo acceder a los asistentes de Workspace ONE, Dispositivo, Contenido y Aplicación 28
- Cómo habilitar el asistente de introducción de forma manual 28

Menú principal 30

Certificados de APN 32
Caducidad de los certificados de APN 32
Cómo generar un certificado de APN 32
Renovar certificados de APN existentes 33
Revisar la conectividad de APN a través de HTTP/2 34

Grupos de asignación 35
Vista de lista de los grupos de asignación 35
Vista de lista del grupo de asignación: Cómo ordenar por columnas 35
Vista de lista del grupo de asignación: Cómo filtrar los grupos 36
Vista de lista del grupo de asignación: Cómo seleccionar vínculos 36
Cómo asignar uno más grupos de asignación 36
Cómo eliminar grupos 37

Grupos organizativos 38
Características de los grupos organizativos 38
Consideraciones para la configuración de los grupos organizativos 40
Cambiar grupos organizativos 41
Cómo comparar los grupos organizativos 41
Cómo crear grupos organizativos 42
Eliminar un grupo organizativo 43
Identificar el ID de grupo de cualquier grupo organizativo 43
Herencia, multiempresa y autenticación 44
Restricciones del grupo organizativo 46
Funciones y personalizaciones del tipo de grupo organizativo 46
Razones por las que no debería inscribir dispositivos en Global 47
Reemplazar frente a Heredar para los grupos organizativos 48

Grupos inteligentes 49
Vista de lista de grupos inteligentes 50
Migración de grupos inteligentes 51
Cómo migrar los grupos inteligentes 51
Grupos inteligentes en el GO global 52
Grupos inteligentes en el GO de tipo socio 53
Grupos inteligentes en el GO global con un GO de tipo socio 54
Cómo anular la asignación de un grupo inteligente 54
Cómo eliminar un grupo inteligente 55
Cómo editar un grupo inteligente 55
Cómo examinar los eventos del grupo inteligente con el registrador de eventos de la consola 56

Cómo crear un grupo inteligente 56
Crear y asignar un grupo inteligente 58
Cómo asignar un grupo inteligente al crear un producto de dispositivo 59
Cómo asignar el grupo inteligente mientras lo administra 59
Cómo excluir grupos en los perfiles y políticas de conformidad 59
Cómo crear un grupo inteligente de forma inteligente, tarea complementaria del vídeo 60

Grupos de usuarios 63
Vista de lista de los grupos de usuarios 63
Más acciones para grupos de usuarios 64
Cómo agregar usuarios a grupos de usuarios 65
Cómo agregar grupos de usuarios sin la integración del directorio (Personalizado) 66
Cómo agregar grupos de usuarios con integración del directorio 66
Editar los permisos de los grupos de usuarios 70
Acceso a los detalles de usuarios 71
Cómo cifrar datos personales 72

Grupos administrativos 72
Vista de lista de los grupos administrativos 72
Cómo agregar grupos administrativos 73

Cómo ver asignaciones 76

Configuraciones 77
Permite búsquedas 77
Clasificadas 77
Categorías portátiles 77

Monitor de Console 79
Intelligence 81
Tablero del panel administrativo 81
Monitor de aplicación y perfil 81
Plantillas del sector para iOS 82
Informes y análisis 82

Notificaciones de la consola 83
Cómo administrar las notificaciones de la consola 85
Cómo configurar ajustes de notificaciones 85

Registros de eventos 87
Eventos de la consola 87

Eventos del dispositivo 88
Cambiar ajustes de Syslog 88
Cambiar ajustes de eventos 89

Freestyle Orchestrator 90
Flujos de trabajo personalizados simplificados 90
Recursos como bloques de creación 90

Otros sistemas empresariales para la integración 91

Acceso basado en funciones 93
Roles predeterminados y roles personalizados 93
Roles de usuarios finales predeterminados 94
Cómo editar un rol predeterminado de usuario final para crear un rol de usuario personalizado 94
Roles administrativos predeterminados 94
Cómo editar un rol predeterminado para crear un rol administrativo personalizado 96
Roles administrativos 96
Hacer que los cambios del rol administrativo sean efectivos 97
Vista de lista de funciones de administrador 97
Cómo crear roles administrativos 97
Cómo exportar roles administrativos 98
Cómo importar roles administrativos 99
Problemas relacionados con las versiones al importar y exportar roles administrativos 100
Copiar rol 100
Cómo cambiar el nombre de un rol administrativo 100
Indicador Solo lectura/Editar en categorías para los roles administrativos 100
Asignar una función o editar la carga de la función de un administrador 101
Cómo ver los recursos de un rol administrativo 101
Comparar dos roles 103
Roles de usuario 105
Cómo crear un nuevo rol de usuario 105
Cómo configurar un rol predeterminado 105
Cómo asignar o editar el rol de un usuario 106

Cómo se crea un administrador del servicio de asistencia restrictivo y se agrega un rol que le otorgue permisos específicos 106

Portal de autoservicio en Workspace ONE UEM 110
Cómo configurar la página predeterminada de inicio de sesión para SSP 110
Inicie sesión en el SSP 110

Seleccione un idioma para el SSP 110
Cambie su contraseña para el SSP 110
Cómo acceder al Portal de autoservicio en los dispositivos 111
Personalizaciones del portal de autoservicio (SSP) 111
Matriz de acciones del portal de autoservicio 111
Cómo realizar acciones en el SSP 112
Seleccione un dispositivo en el SSP 115
Cómo agregar un dispositivo en el SSP 115
Información del dispositivo en el SSP 115
Medidas de seguridad basadas en token 116
Configuración del programa de mejora del producto 116

Términos de uso 117
Cómo ver la aceptación de los Términos de uso 117
Cómo hacer un seguimiento de los Términos de uso con informes 117
Cómo crear Términos de uso para la inscripción 118
Cómo crear Términos de uso para las aplicaciones o la consola 119

Cuentas administrativas y de usuarios 121
Vista de lista de cuentas de usuario 121
Cómo personalizar la Vista de lista 121
Cómo interactuar con cuentas de usuario 122
Migrar usuarios con la herramienta de migración 123

Tipos de autenticación de usuario 126
Proxy de autenticación 126
Autenticación de Active Directory con LDAP y VMware Enterprise Systems Connector 127
Autenticación SAML 2.0 128
Funcionalidad de la aplicación SaaS para administradores de SAML 129
Autenticación basada en tokens 129
Cómo habilitar los tipos de seguridad para la inscripción 131
Autenticación de usuario básica 132
Autenticación de Active Directory con LDAP 133

Cuentas de usuario básicas 134
Ventajas 134
Desventajas 134
Cómo crear cuentas de usuario básicas 135

Cuentas de usuario basadas en el directorio 137

Ventajas 138
Desventajas 138
Sincronización del estado de usuarios del directorio 138
Cómo crear cuentas de usuario basadas en el directorio 139

Función Importar por lotes 141
Cómo realizar cambios en los directorios externos de usuarios LDAP y AD 142
Importación por lotes de usuarios y dispositivos 142
Cómo importar grupos de usuarios por lotes 143
Cómo editar usuarios básicos con la importación por lotes 144
Trasladar usuarios entre grupos organizativos mediante la importación por lotes 144

Cuentas administrativas 145
Vista de lista de cuentas de administrador 145
Cómo crear una cuenta administrativa 146
Cómo crear una cuenta administrativa temporal 147
Sincronización del estado de usuarios del directorio 148
Historial de inicios de sesión 148

Usar la funcionalidad de UEM con una REST API 149
Primeros pasos con las REST API 149
Acceder a la documentación de la API 149
URL para centro de datos y token para la compatibilidad con OAuth 2.0 149
Crear un cliente de OAuth para usarlo con comandos de API (SaaS) 150
Crear una función que pueda utilizar REST API 151

Cómo trabajar en UEM Console

Puede ver y administrar todos los aspectos de la implementación de su dispositivo móvil. Este recurso centralizado en la web permite agregar nuevos dispositivos y usuarios a la flota, administrar perfiles y configurar los ajustes del sistema de manera fácil y rápida.

Familiarícese con los ajustes de seguridad y las funciones de interfaz, tales como el Asistente de introducción, los iconos de menú, el envío de comentarios y la búsqueda global.

Para obtener más información sobre cómo gestiona VMware la información recopilada mediante Workspace ONE UEM, por ejemplo, los análisis, consulte la Política de privacidad de VMware en https://www.vmware.com/help/privacy.html.

Navegadores compatibles

La consola de administración de extremos unificada (Unified Endpoint Management, UEM) de Workspace ONE es compatible con las últimas compilaciones estables de los siguientes navegadores web.

- Chrome
- Firefox
- Safari
- Microsoft Edge

Se han realizado pruebas integrales de las plataformas para garantizar la funcionalidad de estos navegadores web. Si ejecuta la consola de UEM con una versión anterior del explorador o en un explorador no certificado, es posible que tenga algunos problemas menores.

Aviso: Si utiliza Internet Explorer para acceder a UEM Console, vaya a Panel de control > Ajustes > Opciones de Internet > Seguridad y asegúrese de contar con un nivel de seguridad o un nivel de seguridad personalizado que incluya la opción Descarga de fuentes configurada como Habilitada.

- Android 5.0 o superior
- QNX 6.5 o superior
- Apple iOS 11.0 o superior
- Escritorio de Windows (8/8.1/RT/10)
- Apple macOS 10.9 o superior
- Windows Rugged (Mobile 5/6 y Windows CE 4/5/6)
- Chrome OS (última versión)

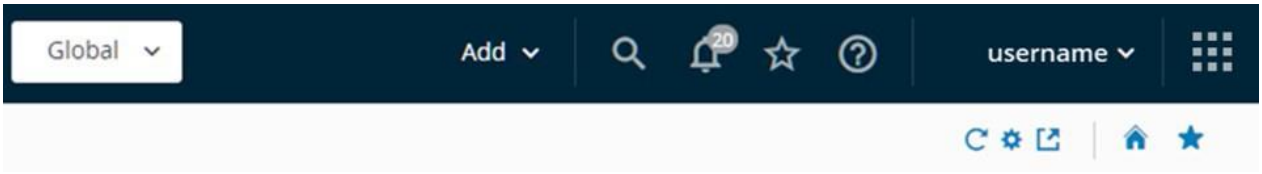
Es posible que exista soporte limitado para otros dispositivos o sistemas operativos. La inscripción directa de Workspace ONE solo es compatible con dispositivos iOS y Android. Para obtener más

información, consulte el tema Inscripción directa de Workspace ONE en la documentación sobre Administrar dispositivos Workspace ONE UEM.

Consulte la guía de cada plataforma en la sección de ayuda en línea, visite docs.vmware.com o póngase en contacto con el equipo de soporte de VMware para obtener más información.

Menú de encabezado

El Menú de encabezado aparece en la parte superior de prácticamente todas las páginas de Workspace ONE UEM basado en AirWatch y le permite acceder a las siguientes funciones y características.



- Grupo organizativo: seleccione el Grupo organizativo (la pestaña denominada Global) al que desee aplicar los cambios.
- Agregar: cree de forma rápida un administrador, dispositivo, usuario, política, contenido, perfil, aplicación interna o aplicación pública.
- Búsqueda global ( ): busque todos los aspectos de la implementación dentro de la consola de UEM, como dispositivos, usuarios, contenido, aplicaciones, ajustes de configuración, administradores, páginas, etc.
- Notificaciones: ( ) le permitirá mantenerse informado sobre eventos importantes de la consola mediante Notificaciones. El distintivo numérico que aparece en el icono de la campana de notificaciones indica la cantidad de alertas que requieren su atención.
- Guardado ( ): acceda a las páginas favoritas y más utilizadas de la consola de UEM.
- Ayuda ( ): busque la documentación de la consola de UEM y las guías disponibles.
- Selector de Mis servicios ( ): utilice este botón de menú para seleccionar entre todos los servicios de Workspace ONE a su disposición.
- Cuenta: permite consultar información sobre su cuenta. Además, puede cambiar el Rol de cuenta que se le ha asignado en el entorno actual y personalizar los ajustes de información de contacto, idioma, notificaciones, visualización del historial de inicios de sesión y seguridad, incluido el restablecimiento del PIN. También puede seleccionar la opción Cerrar sesión en la consola de UEM y volver a la pantalla de inicio de sesión.
- Actualizar: ( ) le permite ver la información y las estadísticas actualizadas sin salir de la vista actual con solo actualizar la pantalla.
- Secciones disponibles: ( ) permite personalizar la vista de Información general del Monitor mediante la selección de las secciones que se desea ver. Disponible solo en la pantalla del Monitor.
- Exportar ( ): genera un listado completo (o filtrado, si se usan filtros) de los usuarios, los

dispositivos, los perfiles, las aplicaciones, los libros o las directivas en un archivo XLSX o CSV (valores separados por comas). Puede ver y analizar estos archivos con Microsoft Excel.

- Inicio ( ): utilice este icono para asignar cualquier pantalla de la consola de UEM como página de inicio. La próxima vez que abra la consola de UEM, la pantalla seleccionada se mostrará como página de inicio.
- Guardar ( ): agregue la página actual a la lista de páginas guardadas para acceder rápidamente a sus páginas favoritas de la consola de UEM.

Búsqueda global

Al utilizar un diseño modular con una interfaz con pestañas, la búsqueda global ejecuta búsquedas por toda la implementación. La búsqueda global aplica la cadena de búsqueda a las pestañas una por una, lo que agiliza los resultados. Seleccione otra pestaña para aplicar la misma cadena a otra área de Workspace ONE UEM.

Tras ejecutar una búsqueda global, seleccione las siguientes pestañas para ver los resultados.

- Dispositivos: muestra resultados que coinciden con el nombre común del dispositivo y el nombre de perfil del dispositivo. Los resultados de la búsqueda incluyen el grupo organizativo para proporcionar contexto en entornos grandes.
- Cuentas: muestra resultados que coinciden con los nombres de usuario y nombres de administradores.
- Aplicaciones: muestra resultados que coinciden con las aplicaciones internas, públicas, compradas y web.
- Contenido: muestra resultados que coinciden con cualquier contenido que aparece en los dispositivos.

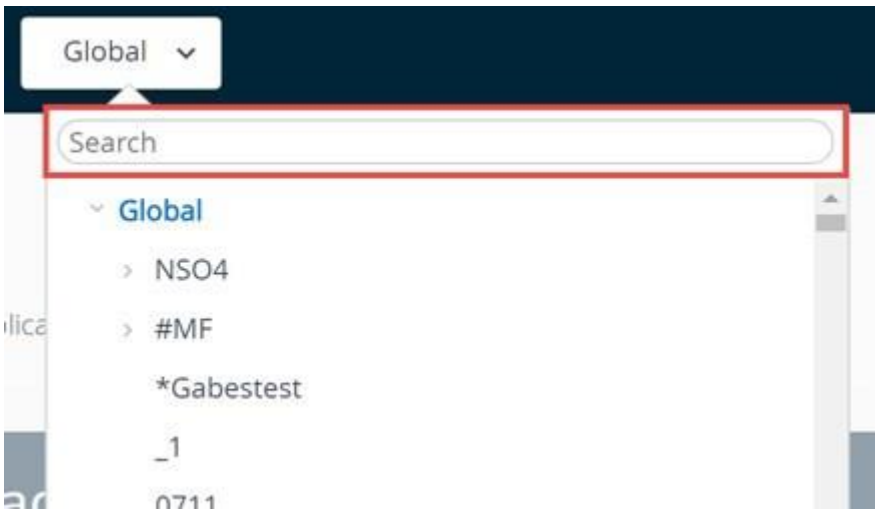
Puede utilizar el asterisco * como comodín en los parámetros de búsqueda de las siguientes maneras.

- Al introducir *device devolverá ruggeddevice, appledevice, mobiledevice
- Al introducir m*e devolverá manufacture, Maine, merge
- Al introducir admin* devolverá administrator, administration, admins
- "Con la introducción de comodines, la búsqueda global solo devuelve coincidencias exactas, a menos que se utilicen comodines antes y después del parámetro de búsqueda.
    - Por ejemplo, al introducir *desktop* se devuelven todos los dispositivos que incluyan la cadena "desktop" en cualquier lugar de la lista de dispositivos.
    - Una forma alternativa de buscar escritorios es usar filtros en la vista de lista de dispositivos. El uso de filtros significa que puede producir no solo una lista única de escritorios de Windows, sino también macOS, más una matriz grande de otras variables. Para obtener más información, consulte Filtrar dispositivos en la vista de lista.
- Para incluir un asterisco como parte del parámetro de búsqueda, escríbalo entre comillas dobles o coloque delante una barra invertida.
    - Al introducir micro"*" devolverá micro*

- Al introducir valueable* devolverá valueable*

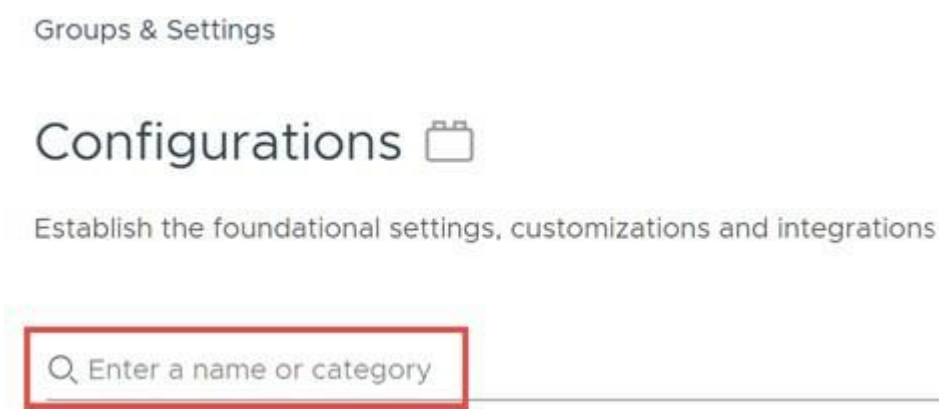
Búsqueda de un grupo organizativo

También puede llevar a cabo la búsqueda de un grupo organizativo mediante la selección del menú desplegable de este. La barra de búsqueda está en la parte superior de la lista.



Buscar ajustes

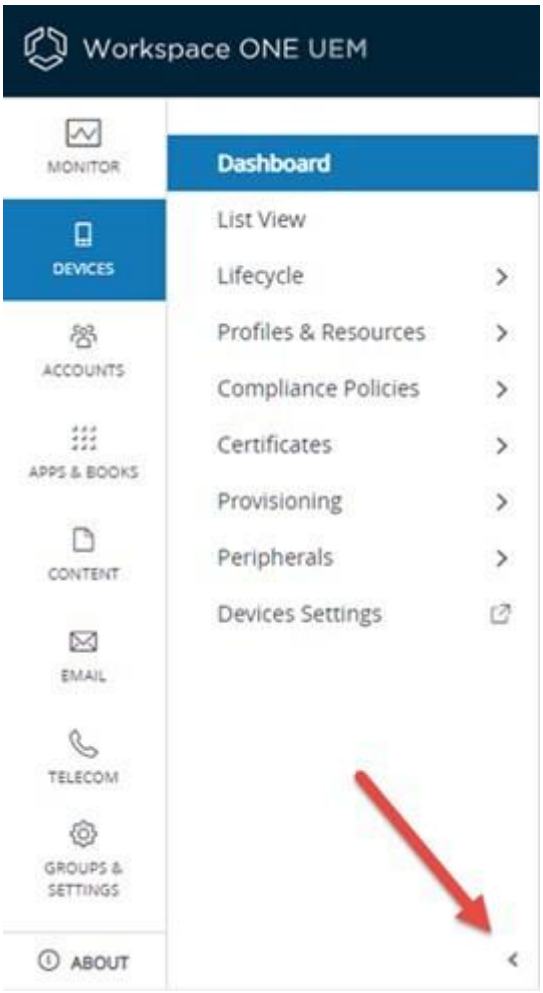
Puede buscar los ajustes mediante una búsqueda desde la página Configuraciones. Vaya a Grupos y ajustes > Configuraciones e introduzca su palabra clave en el cuadro de texto de búsqueda.



Cómo contraer y expandir el submenú

Puede contraer el submenú del panel izquierdo de Workspace ONE UEM a fin de crear más espacio en pantalla para la información del dispositivo. También puede expandir o volver a abrir un submenú contraído.

1. Para contraer el submenú temporalmente seleccione la flecha que apunta hacia la izquierda que se muestra aquí.



2. Para expandir o volver a abrir el submenú contraído, seleccione la flecha que apunta hacia la derecha en la parte inferior izquierda de la pantalla.

Cómo adaptar la interfaz de usuario con la personalización de marca

Workspace ONE UEM permite numerosas opciones de personalización. Esas opciones permiten cambiar la marca de las herramientas y los recursos para que coincida con la combinación de colores, el logotipo y la estética general de la organización.

La personalización de marca se puede configurar para respaldar la estructura jerárquica, de forma que cada división de la empresa pueda tener un diseño único en su grupo organizativo. Para obtener más información, consulte Grupos organizativos.

1. Seleccione el grupo organizativo que desea personalizar y luego acceda a Grupos y ajustes > Todos los ajustes > Sistema > Personalización de marca.
2. Configure los ajustes de logotipo y fondo en la pestaña Personalización de marca.
3. Cargue un logotipo de la empresa. Para ello, debe cargar un archivo guardado en el ordenador. La resolución recomendada de la imagen cargada es de 800 x 300.
4. Cargue un fondo para la página de inicio de sesión. Para ello, cargue un archivo guardado en el ordenador. La resolución recomendada de la imagen cargada es de 1024 x 768.
5. Cargue un fondo para la página de inicio de sesión del Portal de autoservicio (SSP). Para

ello, cargue un archivo guardado en el ordenador. La resolución recomendada de la imagen cargada es de 1024 x 768.

6. Configure personalizaciones en la sección Colores de la pestaña Personalización de marca.
7. Configure los ajustes en la pestaña CSS personalizado. Introduzca un código de CSS personalizado para la personalización de marca avanzada.
8. Seleccione Guardar.

Cómo unirse o abandonar el Programa de mejora de la experiencia del cliente

El programa de mejora de la experiencia de cliente (Customer Experience Improvement Program, "CEIP") de VMware proporciona información que VMware utiliza para mejorar sus productos y servicios, solucionar problemas y ofrecer consejos relacionados con la mejor forma de implementar y utilizar los productos de VMware. Este programa solo está disponible para implementaciones locales de Workspace ONE UEM.

Antes de comenzar: Workspace ONE UEM participa en el Programa de mejora de la experiencia de cliente ("CEIP") de VMware. El Centro de "Confianza y Garantía" https://www.vmware.com/es/solutions/trustvmware/ceip.html contiene información adicional relacionada con los datos recopilados mediante el CEIP, así como los fines para los que VMware los utiliza.

Para obtener más información sobre cómo gestiona VMware la información recopilada mediante Workspace ONE UEM, por ejemplo, los análisis, consulte la Política de privacidad de VMware en https://www.vmware.com/help/privacy.html.

Acerca de esta tarea: El aviso del CEIP aparece al instalar o actualizar Workspace ONE UEM. Debe hacer una selección. Puede cambiar la selección en cualquier momento desde la consola de UEM mediante los siguientes pasos.

1. Vaya a Grupos y ajustes > Todos los ajustes > Administrador > Programas de mejora del producto.
2. Si desea participar en el CEIP, habilite la casilla de verificación junto a Unirse al Programa de mejora de la experiencia del cliente de VMware.
    1. Si no desea participar en el CEIP, desactive (borre) esta casilla de verificación.
3. Seleccione Guardar

Inicio de sesión en la Console

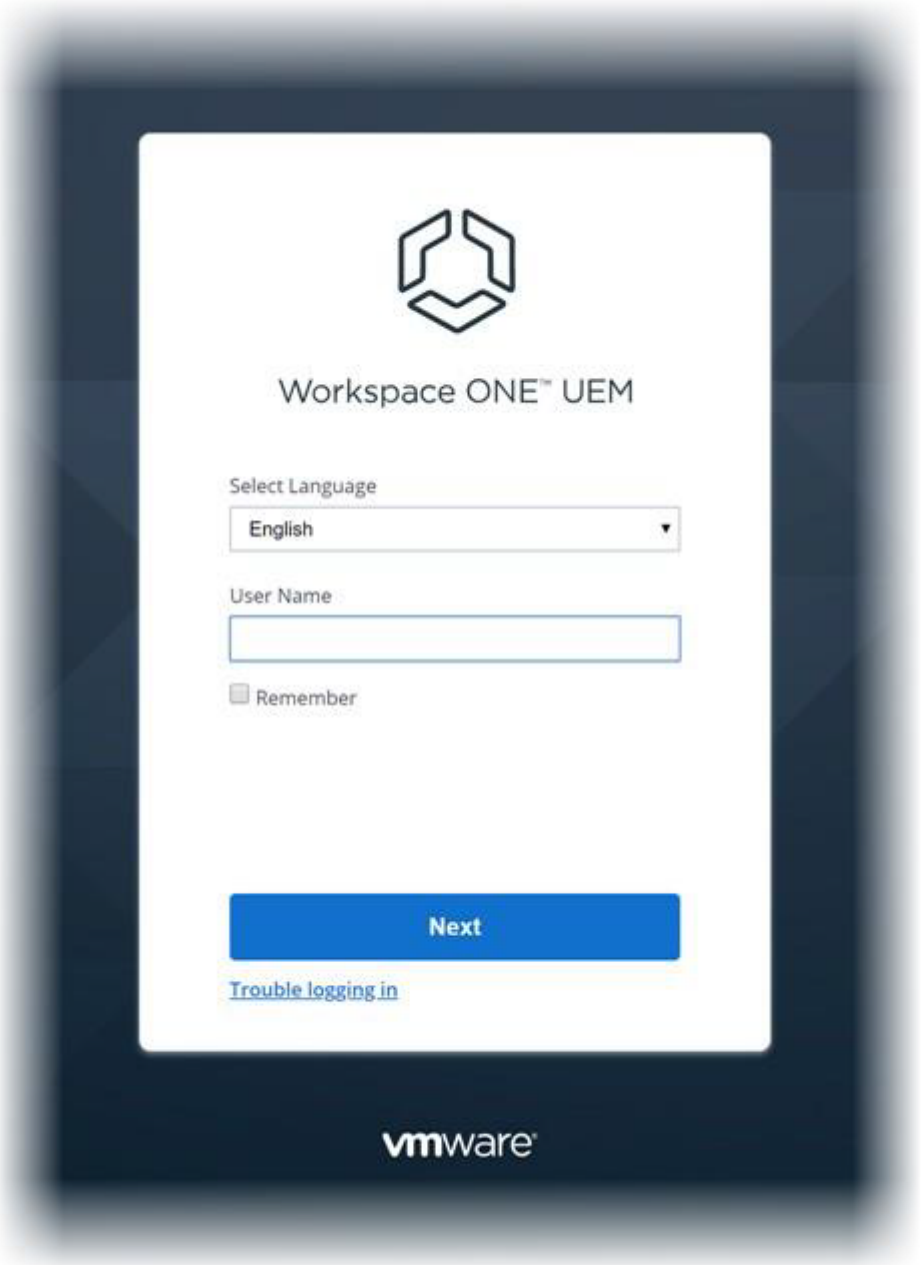
Para poder realizar cualquier acción en Workspace ONE UEM, primero debe iniciar sesión en Console.

Para iniciar sesión en Workspace ONE UEM Console, necesita tener la Dirección URL del entorno y las Credenciales de inicio de sesión. El tipo de implementación determinará dónde cómo se obtiene la información.

- Implementación de SaaS: el Administrador de la cuenta proporciona la dirección URL del entorno y el nombre del usuario/contraseña. La dirección URL no se puede personalizar y generalmente está en el formato awmdm.com.
- Local: la dirección URL local se puede personalizar y sigue el formato awmdm.<SuCompañía>.com.

El administrador de cuenta le proporcionará las credenciales iniciales para su entorno. Los administradores que crean más cuentas para delegar las responsabilidades administrativas también pueden distribuir las credenciales en el entorno.

Una vez que el navegador cargue la Dirección URL del entorno de Console, podrá iniciar sesión con el Nombre de usuario y la Contraseña suministrados por el administrador de Workspace ONE UEM.



1. Introduzca su Nombre de usuario.
    - Workspace ONE UEM Console guarda el nombre de usuario y el tipo de usuario (SAML o no SAML) en la caché del navegador.
        - Si es usuario de SAML, el administrador se dirige al inicio de sesión de SAML.
        - Si no usuario de SAML, el administrador debe introducir una contraseña.
    - Si la casilla de verificación Recordar está habilitada, el cuadro de texto Nombre de usuario se rellena automáticamente con el último usuario que inició la sesión la próxima vez que visite la dirección URL del entorno.
2. Introduzca su contraseña.
    - Si va a iniciar sesión por primera vez, se le pedirá que introduzca la contraseña de inicio de sesión. Escríbala para continuar.
    - Si inició sesión antes y permite que el navegador predeterminado recuerde los nombres de usuario y las contraseñas, el cuadro de texto Contraseña se rellena

automáticamente con la contraseña guardada en la memoria caché del navegador.

3. Seleccione el botón Iniciar sesión.
    - La pantalla de inicio predeterminada (que se puede personalizar) se abre al iniciar sesión. Para obtener información sobre cómo personalizar la pantalla de inicio, visite la sección titulada Menú de encabezado en la Consola administrativa.

Caducidad de la contraseña

Los administradores básicos reciben notificación por correo electrónico 5 días antes de que la contraseña caduque y otra notificación por correo electrónico el día antes. Los administradores locales pueden cambiar este período predeterminado de 5 días en Grupos y ajustes > Todos los ajustes > Administrador > Seguridad de Console > Contraseñas en el grupo organizativo Global. Los administradores de SaaS dedicados deben ponerse en contacto con el soporte técnico para realizar cambios en este ajuste.

Puede crear una notificación de caducidad de contraseña personalizada para los administradores. Para ello, vaya a Grupos y ajustes > Todos los ajustes > Dispositivos y usuarios > General > Plantilla de mensaje y seleccione "Administrador" como valor de Categoría y "Notificación de caducidad de contraseña de administrador" como valor de Tipo.

Para obtener más información sobre los ajustes de contraseñas de usuario de inscripción, que se administran por separado de las contraseñas de administrador de Console, consulte la página de ajustes del sistema en Grupos y ajustes > Todos los ajustes > Dispositivos y usuarios > General > Contraseñas .

Tiempos de espera y cierres de sesión

Workspace ONE UEM Console cierra la sesión en dos escenarios básicos.

1. Cierre de sesión explícito (incluye cerrar el navegador y la inactividad).
    - Si ha configurado el navegador predeterminado para que recuerde su nombre de usuario y contraseña, en el siguiente inicio de sesión, el navegador rellenará el cuadro de texto de nombre de usuario con el último usuario para iniciar sesión correctamente.
    - Si ha configurado el navegador para olvidar los nombres de usuario y las contraseñas, el nombre de usuario y el tipo de usuario (SAML/no SAML) se eliminarán de la memoria caché del navegador.
2. Invalidación de sesión (incluye los problemas del equilibrador de cargas y los tiempos de espera de las sesiones debido a la configuración del administrador).
    - Los usuarios que no sean SAML vuelven a iniciar sesión con un nombre de usuario guardado y mediante el botón Iniciar sesión.
    - Los usuarios de SAML pueden volver a iniciar sesión en la consola sin hacer clic.

Bloqueos de inicio de sesión

Los administradores del sistema y los administradores de AirWatch pueden configurar el valor de Cantidad máxima de intentos de inicio de sesión fallidos antes de que se bloquee el acceso de los administradores a Console en Grupos y ajustes > Todos los ajustes > Administrador > Seguridad

de Console > Contraseñas.

Su acceso a UEM Console se bloqueará en dos escenarios: 1) cuando realiza un número de intentos de inicio de sesión fallidos superior al número máximo configurado y 2) cuando, al intentar restablecer la contraseña, responde incorrectamente a la pregunta de recuperación de contraseña tres veces.

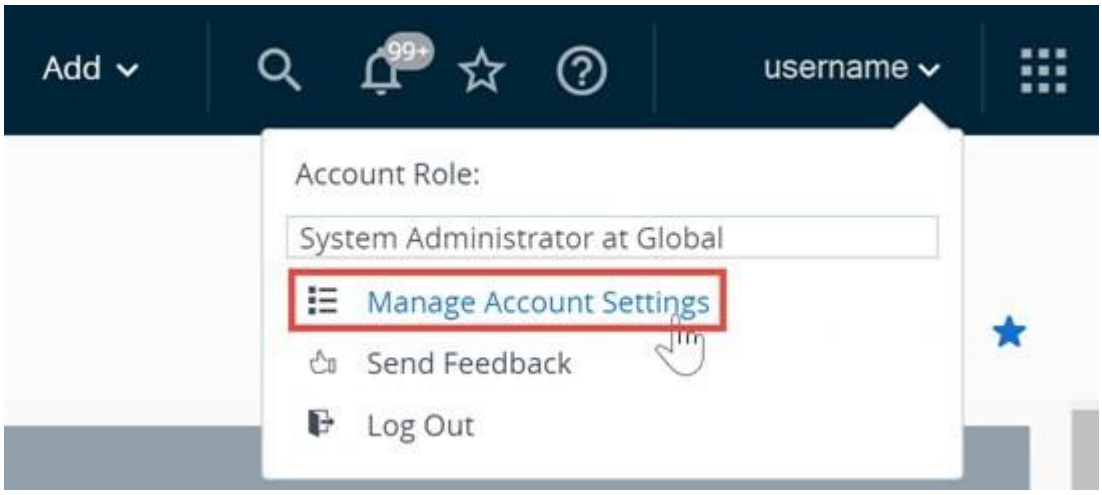
Si esto ocurre, debe restablecer la contraseña siguiendo el vínculo de solución de problemas de la página de inicio de sesión, o pedir a otro administrador que desbloquee su cuenta mediante la vista de lista del administrador. Recibirá una notificación por correo electrónico cuando su cuenta se bloquee y, de nuevo, cuando se desbloquee.

Cómo consultar eventos de la consola de bloqueo de cuenta

Al bloquear y desbloquear cuentas administrativas básicas en Workspace ONE UEM, se genera un evento de Console. Ambos eventos generan un evento de nivel de registro 5 (advertencia). Además de revisar el historial de inicio de sesión básico directamente en Ajustes de la cuenta, puede realizar los siguientes pasos para consultar los eventos de la consola de bloqueo o desbloqueo de la cuenta de administrador.

1. Vaya a Monitor > Informes y análisis > Eventos > Eventos de Console.
2. Seleccione "A partir de advertencia" en el filtro desplegable Gravedad de la parte superior de la lista Eventos de Console.
3. Seleccione "Inicio de sesión" en el filtro desplegable Categoría.
4. Seleccione "Administración" en el filtro desplegable Módulo.
5. De ser necesario, puede aplicar más filtros, incluido Intervalo de fechas.

Administrar ajustes de cuenta



Los administradores de Workspace ONE UEM tienen ajustes de cuenta específicos de Console que permiten configurar la información de contacto del usuario, las preferencias de notificación, el historial de inicios de sesión y la configuración de seguridad, incluida la recuperación de contraseña.

Administrar ajustes de cuenta: Usuario

Asegúrese de que se puede contactar con usted introduciendo su información personal en la pestaña Usuario, incluyendo el correo electrónico, hasta cuatro números de teléfono diferentes, la zona horaria y la configuración regional.

Administrar ajustes de cuenta: Notificaciones

Utilice los ajustes de Notificaciones en la página de Ajustes de cuentapara habilitar o desactivar alertas de fecha de caducidad de nombres de punto de acceso (APN), seleccione cómo recibir las alertas y cambie el correo electrónico al que las envía. Para obtener más información, consulte la sección titulada Cómo configurar ajustes de notificaciones en Notificaciones de Console.

Administrar ajustes de cuenta: Inicios de sesión

Revise el historial de inicios de sesión completo, incluida la fecha y hora de inicio de sesión, la dirección IP de origen, el tipo de inicio de sesión, las aplicaciones de origen, la marca y la versión del navegador, la plataforma de SO y el estado de inicio de sesión.

Administrar ajustes de cuenta: Seguridad

Puede restablecer su contraseña de inicio de sesión, restablecer las preguntas de recuperación de contraseña y restablecer el PIN de seguridad de cuatro dígitos.

Administrar ajustes de cuenta: Contraseña

La Contraseña acompaña al nombre de usuario de la cuenta cuando inicia sesión en la consola de UEM. Puede Restablecer esta contraseña en cualquier momento. Para obtener más información sobre los valores mínimos y máximos de contraseñas, consulte Ajustes de contraseñas.

Administrar ajustes de cuenta: Preguntas de recuperación de contraseña

Las Preguntas de recuperación de contraseña son el método por el cual restablece su contraseña. Debe definir esta pregunta junto con su respuesta cuando inicie sesión en la consola de UEM por primera vez. Puede seleccionar una nueva pregunta de recuperación de contraseña seleccionando el botón Restablecer. Esta acción cierra la sesión del usuario automáticamente. Al volver a iniciar sesión, se les presenta la pantalla Ajustes de seguridad, donde se les solicita que seleccionen de la lista de preguntas de recuperación de contraseña y proporcionen la respuesta.

Los administradores que nunca seleccionaron una pregunta de recuperación de contraseña y no tienen un botón de Restablecer para las preguntas de recuperación de contraseña deben eliminar y volver a crear sus cuentas. Al iniciar sesión por primera vez después de que se vuelva a crear su cuenta, se les requiere que definan una pregunta y respuesta de recuperación de contraseña.

No puede acceder a la página de inicio de sesión cuando responde una pregunta de recuperación de contraseña incorrectamente más de tres veces. Cuando esto ocurre, debe restablecer la contraseña utilizando el enlace de la solución de problemas en la página de inicio de sesión. Si lo prefiere, puede obtener ayuda de un administrador que desbloquee la cuenta utilizando la vista de lista de administración. Recibirá una notificación por correo electrónico cuando su cuenta se bloquee y, de nuevo, cuando se desbloquee.

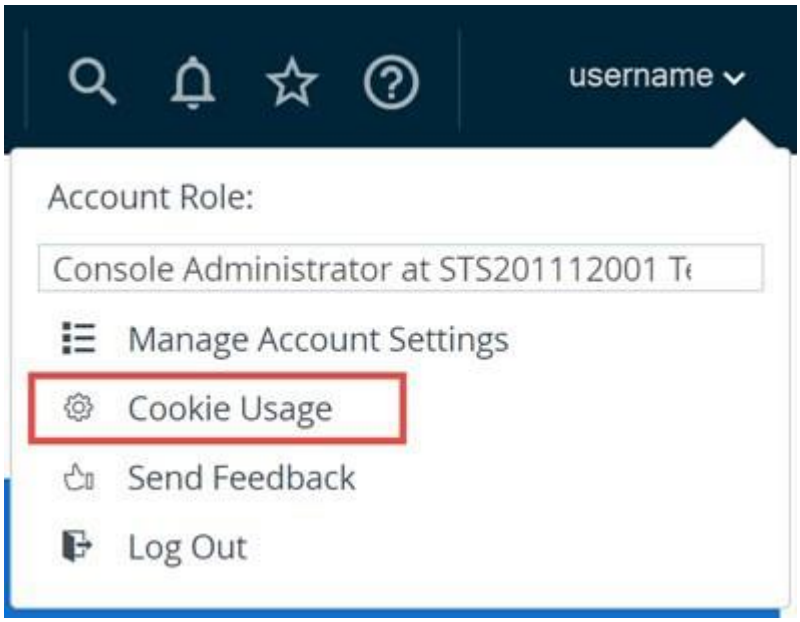
Administrar ajustes de cuenta: PIN de seguridad

Proteja la consola de UEM creando un PIN de seguridad. El PIN sirve como protección contra eliminaciones accidentales de dispositivos o de partes importantes del entorno, como usuarios y grupos organizativos. El PIN de seguridad también funciona como una segunda capa de seguridad. Representa un punto adicional de autenticación, ya que bloquea acciones de usuarios no aprobados.

Cuando inicie sesión en la consola de UEM por primera vez, se le requerirá que establezca un PIN de seguridad.

Restablezca su PIN de seguridad de vez en cuando para minimizar los riesgos relacionados con la seguridad.

Uso de cookies (solo visible para administradores de VMware Cloud Services)



Puede participar en el proceso de mejora de nuestros servicios, incluidos el soporte, las recomendaciones y la experiencia de usuario, habilitando el acceso a las guías de producto basadas en cookies del navegador y a los análisis. Para no participar, seleccione Uso de cookies y desactive los controles deslizantes de Habilitar análisis y Habilitar guías de producto en la tarjeta de información Pendo.

Cómo restringir acciones de UEM Console

Si se diera el caso de que Workspace ONE UEM Console quedase desbloqueado y desatendido, se proporcionaría protección adicional contra acciones malintencionadas potencialmente destructivas. En dicho escenario, puede protegerse contra tales acciones manteniendo a raya a los usuarios no autorizados.

1. Acceda a Grupos y ajustes > Todos los ajustes > Sistema > Seguridad > Acciones restringidas.
2. Configure el ajuste Enviar mensaje a todos. Habilite este ajuste para permitir que el

administrador del sistema envíe un mensaje a todos los dispositivos de la implementación desde la Vista de lista de dispositivos. También puede utilizarse para enviar un mensaje a un grupo específico.

3. Puede exigir que se pida a los administradores que introduzcan un PIN para realizar ciertas acciones de UEM Console. Configure Requerir contraseña para las acciones mediante la habilitación o deshabilitación de las siguientes acciones.

   Aviso: Indicadas con un * a continuación, algunas de las acciones siempre requerirán un PIN y, como resultado, no podrá desactivarlas.

Ajustes	Descripción
Eliminar cuenta administrativa	Evita que se elimine una cuenta administrativa de usuario en Cuentas > Administradores > Vista de lista.
*Volver a generar el certificado de VMware Enterprise Systems Connector	Evita que se vuelva a generar el certificado de VMware Enterprise Systems Connector en Grupos y ajustes > Todos los ajustes > Sistema > Integración empresarial > VMware Enterprise Systems Connector.
*Cambio de certificado APNs	Evita que los APNs para MDM sean inhabilitados en Grupos y ajustes > Todos los ajustes > Dispositivos y usuarios > Apple > APNs para MDM.
Eliminar/Desactivar/Retirar la aplicación	Impide la eliminación, desactivación o retirada de una aplicación en Aplicaciones y libros > Aplicaciones > Vista de lista.
Eliminar/Desactivar contenido	Protege el archivo de contenido contra la eliminación o desactivación en Contenido > Vista de lista.
*Alternar el cifrado de datos	Impide los ajustes de cifrado de información del usuario en Grupos y ajustes > Todos los ajustes > Sistema > Seguridad > Seguridad de datos.
Eliminar dispositivo	Impide la eliminación de un dispositivo en Dispositivos > Vista de lista. Se seguirá requiriendo un PIN de seguridad de administración para las acciones en masa aunque se haya desactivado este ajuste.
*Eliminación total	Protege el dispositivo contra cualquier intento de eliminación total en las pantallas Vista de lista de dispositivos o Detalles del dispositivo.
Restablecimiento empresarial	Protege el dispositivo contra cualquier intento de restablecimiento empresarial desde la página Detalles de dispositivos de un dispositivo robusto de Windows, Android o QNX.
Eliminación empresarial	Protege el dispositivo contra cualquier intento de eliminación empresarial desde la página Detalles de dispositivos de un dispositivo.

Ajustes	Descripción
Eliminación empresarial (basada en la membresía al grupo de usuarios)	Protege el dispositivo contra cualquier intento de eliminación empresarial cuando se retira de un grupo de usuarios. Este ajuste es opcional y puede configurarlo en Grupos y ajustes > Todos los ajustes > Dispositivos y usuarios > General > Inscripción en la pestaña Restricciones. Si ha elegido Restringir la inscripción a los grupos configurados en esta pestaña, tendrá la opción extra de realizar una eliminación empresarial cuando se elimine el dispositivo del grupo.
*Eliminar grupo organizativo	Protege al grupo organizativo actual contra cualquier intento de eliminación desde Grupos y ajustes > Grupos > Grupos organizativos > Detalles del grupo organizativo.
Eliminar/Desactivar perfil	Protege el perfil contra cualquier intento de eliminación o desactivación desde Dispositivos > Perfiles y recursos > Recursos.
Eliminar producto de aprovisionamiento	Protege al producto de aprovisionamiento contra cualquier intento de eliminación en Dispositivos > Aprovisionamiento > Vista de lista de productos.
Revocar certificados	Protege al certificado contra cualquier intento de revocación desde Dispositivos > Certificados > Vista de lista.
*Borrar certificado del canal seguro	Protege al certificado de canal seguro contra cualquier intento de eliminación desde Grupos y ajustes > Todos los ajustes > Sistema > Avanzado > Certificado de canal seguro.
Eliminar cuenta de usuario	Protege a la cuenta de usuario contra cualquier intento de eliminación desde Cuentas > Usuarios > Vista de lista.
Cambiar en los ajustes de privacidad	Protege contra cualquier intento de modificar la configuración de privacidad en Grupos y ajustes > Todos los ajustes > Dispositivos y usuarios > General > Privacidad.
Eliminar plan de Telecom	Protege contra la eliminación de un plan de telecomunicaciones en Telecom > Lista de planes.
Reemplazar nivel de registro del trabajo	Protege contra los intentos de reemplazar el nivel de registro de trabajo seleccionado actualmente en Grupos y ajustes > Administrador > Diagnósticos > Registro. Reemplazar el nivel de registro de trabajos es útil cuando un dispositivo o grupo de dispositivos tiene problemas. En ese caso, el administrador puede reemplazar los ajustes de esos dispositivos cambiando un nivel de registro elevado a Detallado, lo que registra el nivel máximo de actividad de la consola para facilitar la solución de problemas.
*Restablecer/alternar el proveedor de análisis de aplicaciones	Impide que los ajustes de integración del escaneo de aplicaciones se restablezcan (y se eliminen después). Esta acción se realiza desde Grupos y ajustes > Todos los ajustes > Aplicaciones > Análisis de aplicaciones.

Ajustes	Descripción
Apagar	Protege contra cualquier intento de apagar el dispositivo en Dispositivos > Vista de lista > Detalles de dispositivos.
Cantidad máxima de intentos no válidos para introducir la clave (PIN)	Define el número máximo de intentos no válidos de introducir un PIN antes de que se bloquee la consola. Este ajuste debe estar comprendido entre 1 y 5.

Cómo seleccionar acciones para proteger la contraseña

Las acciones restringidas de Console ofrecen una capa adicional de protección contra acciones malintencionadas que pueden ser destructivas para Workspace ONE UEM Console.

1. Para configurar los ajustes de las acciones restringidas, acceda a Grupos y ajustes > Todos los ajustes > Sistema > Seguridad > Acciones restringidas.
2. Para cada acción que proteja solicitando a los administradores que introduzcan un PIN, seleccione el botón Requerir contraseña para las acciones adecuado como Habilitado o Desactivado, como corresponda.

   Este requisito le proporciona un control detallado sobre las acciones que desea proteger en mayor medida.

   Aviso: Algunas de las acciones siempre requerirán un PIN y, como resultado, no podrá desactivarlas. Se indican mediante los * siguientes.
3. Establezca el número máximo de intentos fallidos que el sistema acepta antes de cerrar la sesión automáticamente. Si alcanza el número máximo de intentos, tendrá que iniciar sesión en la consola de Workspace ONE UEM y establecer un nuevo PIN de seguridad.

Ajustes	Descripción
Eliminar cuenta administrativa	Evita que se elimine una cuenta administrativa de usuario en Cuentas > Administradores > Vista de lista.
Volver a generar el certificado de VMware Enterprise Systems Connector	Evita que se vuelva a generar el certificado de VMware Enterprise Systems Connector en Grupos y ajustes > Todos los ajustes > Sistema > Integración empresarial > VMware Enterprise Systems Connector.
*Cambio de certificado APNs	Evita que los APNs para MDM sean inhabilitados en Grupos y ajustes > Todos los ajustes > Dispositivos y usuarios > Apple > APNs para MDM.

Ajustes	Descripción
Eliminar/Desactivar/Retirar la aplicación	Impide la eliminación, desactivación o retirada de una aplicación en Aplicaciones y libros > Aplicaciones > Vista de lista.
Eliminar/Desactivar contenido	Protege el archivo de contenido contra la eliminación o desactivación en Contenido > Vista de lista.
*Alternar el cifrado de datos	Impide los ajustes de cifrado de información del usuario en Grupos y ajustes > Todos los ajustes > Sistema > Seguridad > Seguridad de datos.
Eliminar dispositivo	Impide la eliminación de un dispositivo en Dispositivos > Vista de lista. Se seguirá requiriendo un PIN de seguridad de administración para las acciones en masa aunque se haya desactivado este ajuste.
*Eliminación total	Protege el dispositivo contra cualquier intento de eliminación total en las pantallas Vista de lista de dispositivos o Detalles del dispositivo.
Restablecimiento empresarial	Protege el dispositivo contra cualquier intento de restablecimiento empresarial desde la página Detalles de dispositivos de un dispositivo robusto de Windows, Android o QNX.
>Eliminación empresarial	Protege el dispositivo contra cualquier intento de eliminación empresarial desde la página Detalles de dispositivos de un dispositivo.
Eliminación empresarial (basada en la membresía al grupo de usuarios)	Protege el dispositivo contra cualquier intento de eliminación empresarial cuando se retira de un grupo de usuarios. Este ajuste es opcional y puede configurarlo en Grupos y ajustes > Todos los ajustes > Dispositivos y usuarios > General > Inscripción en la pestaña Restricciones. Si ha elegido Restringir la inscripción a los grupos configurados en esta pestaña, tendrá la opción extra de realizar una eliminación empresarial cuando se elimine el dispositivo del grupo.
*Eliminar grupo organizativo	Protege al grupo organizativo actual contra cualquier intento de eliminación desde Grupos y ajustes > Grupos > Grupos organizativos > Detalles del grupo organizativo.
Eliminar/Desactivar perfil	Protege el perfil contra cualquier intento de eliminación o desactivación desde Dispositivos > Perfiles y recursos > Recursos.
Eliminar producto de aprovisionamiento	Protege al producto de aprovisionamiento contra cualquier intento de eliminación en Dispositivos > Aprovisionamiento > Vista de lista de productos.
Revocar certificados	Protege al certificado contra cualquier intento de revocación desde Dispositivos > Certificados > Vista de lista.
*Borrar certificado del canal seguro	Protege al certificado de canal seguro contra cualquier intento de eliminación desde Grupos y ajustes > Todos los ajustes > Sistema > Avanzado > Certificado de canal seguro.

Ajustes	Descripción
Eliminar cuenta de usuario	Protege a la cuenta de usuario contra cualquier intento de eliminación desde Cuentas > Usuarios > Vista de lista.
Cambiar en los ajustes de privacidad	Protege contra cualquier intento de modificar la configuración de privacidad en Grupos y ajustes > Todos los ajustes > Dispositivos y usuarios > General > Privacidad.
Eliminar plan de Telecom	Protege contra la eliminación de un plan de telecomunicaciones en Telecom > Lista de planes.
Reemplazar nivel de registro del trabajo	Protege contra los intentos de reemplazar el nivel de registro de trabajo seleccionado actualmente en Grupos y ajustes > Administrador > Diagnósticos > Registro. Reemplazar el nivel de registro de trabajos es útil cuando un dispositivo o grupo de dispositivos tiene problemas. En ese caso, el administrador puede reemplazar los ajustes de esos dispositivos cambiando un nivel de registro elevado a Detallado, lo que registra el nivel máximo de actividad de la consola para facilitar la solución de problemas.
*Restablecer/alternar el proveedor de análisis de aplicaciones	Impide que los ajustes de integración del escaneo de aplicaciones se restablezcan (y se eliminen después). Esta acción se realiza desde Grupos y ajustes > Todos los ajustes > Aplicaciones > Análisis de aplicaciones.
Apagar	Protege contra cualquier intento de apagar el dispositivo en Dispositivos > Vista de lista > Detalles de dispositivos.
Cantidad máxima de intentos no válidos para introducir la clave (PIN)	Define el número máximo de intentos no válidos de introducir un PIN antes de que se bloquee la consola. Este ajuste debe estar comprendido entre 1 y 5.

Cómo configurar notas requeridas para las acciones

Puede exigir que los administradores introduzcan notas a través de la casilla Requerir notas para explicar su razonamiento al realizar algunas acciones de Workspace ONE UEM Console.

1. Acceda a Grupos y ajustes > Todos los ajustes > Sistema > Seguridad > Acciones restringidas.
2. Si requiere que los administradores introduzcan una nota antes de realizar alguna de estas acciones, asegúrese de que se modifique el rol con el recurso de Agregar nota (permiso).

   Para obtener más información, consulte la sección titulada Cómo crear funciones administrativas en Acceso basado en funciones.

Ajustes	Descripción

Bloquear dispositivo	Requiere una nota antes de realizar cualquier intento de bloqueo de un dispositivo en Vista de lista de dispositivos o Detalles de dispositivos.
Bloquear sesión de SSO	Requiere una nota para cualquier intento de bloqueo de una sesión de SSO en Vista de lista de dispositivos o Detalles de dispositivos.
Borrar todo	Requiere una nota para cualquier intento de eliminación total de un dispositivo en Vista de lista de dispositivos o Detalles de dispositivos.
Restablecimiento empresarial	Requiere una nota para cualquier intento de restablecimiento empresarial de un dispositivo en la página Detalles del dispositivo de un dispositivo robusto de Windows o Android.
Eliminación empresarial	Requiere una nota para cualquier intento de eliminación empresarial en Detalles de dispositivos.
Reemplazar nivel de registro del trabajo	Requiere una nota antes de intentar reemplazar el nivel predeterminado de registro de trabajos en Grupos y ajustes > Administrador > Diagnóstico > Registro.
Reiniciar el dispositivo	Requiere una nota antes de intentar reiniciar en Dispositivos > Vista de lista > Detalles de dispositivos.
Apagar	Requiere una nota antes de intentar apagar en Dispositivos > Vista de lista > Detalles de dispositivos.

Uso del asistente de introducción

El asistente de introducción sirve como una lista de comprobación que le guía paso a paso por los ajustes de Workspace ONE UEM basado en AirWatch. Presenta solo esos módulos dentro de su implementación específica y genera una experiencia de configuración adaptada a su entorno.

Cómo acceder al asistente de introducción

El menú principal del asistente de introducción funciona de una forma muy práctica. No solo realiza un seguimiento de cuánto le queda en el proceso de configuración, sino que puede iniciar, pausar, reiniciar más tarde, rebobinar, revisar e incluso cambiar las respuestas anteriores.

- Inicie el primer paso en un submódulo seleccionando Iniciar asistente. También puede configurar los ajustes de cada función respondiendo preguntas y accediendo a las páginas exactas dentro de la consola de UEM. Cada vez que realice un submódulo, el contador de porcentaje situado en la esquina superior derecha avanza y muestra su progreso.
- Si detiene el submódulo antes de completarlo, puede volver al mismo lugar donde lo dejó al seleccionar Seguir.
- Además, puede omitir cualquier submódulo al seleccionar la opción de Omitir sección, la cual desactiva temporalmente el botón de "Seguir" e introduce un enlace a la opción de Reanudar sección. Seleccione este enlace de Reanudar sección para habilitar una vez más el botón Seguir.

La página de introducción se divide en cuatro submódulos: Workspace ONE, Dispositivo, Contenido y Aplicación. Cada uno incluye su propio conjunto de pasos. El asistente de introducción realiza un seguimiento de los pasos compartidos entre todos los submódulos para que no tenga que completar el mismo paso dos veces.

- Workspace ONE: representa el acceso sin interrupciones desde el dispositivo de cualquier empleado o de propiedad corporativa. Ofrece conexión segura a las aplicaciones de productividad empresariales, como el correo electrónico, el calendario, los contactos, los documentos y mucho más, así como acceso instantáneo mediante inicio de sesión único (SSO) a las aplicaciones móviles, de nube y Windows. Proporciona seguridad de datos robusta que protege a la empresa y a los empleados contra dispositivos comprometidos.

  Para obtener más información acerca de Workspace ONE, consulte la Guía de configuración rápida de VMware Workspace ONE.

- Dispositivo: realice acciones en dispositivos inscritos en MDM, como bloqueos, notificaciones o eliminación empresarial. Puede configurar el correo electrónico, las restricciones, los ajustes y mucho más mediante la implementación de perfiles de dispositivos. Puede asegurarse de que cumple con las directivas de seguridad de su flota de dispositivos mediante la configuración de directivas de conformidad. Administre sus

dispositivos con la mejor información obtenida del panel de control y monitor.

- Contenido: implemente contenido y acceda a él dentro de la aplicación de Content Locker. Vea y administre su contenido con los Tableros de contenido, Informes y Registros. Comparta y colabore con otros usuarios utilizando el contenido personal. Intégrese con repositorios existentes e implemente su contenido en dispositivos móviles.
- Aplicación: implemente aplicaciones desarrolladas de forma interna, o aplicaciones gratis o compradas que están disponibles al público. Los usuarios pueden buscar, descargar e instalar aplicaciones al implementar un catálogo de aplicaciones personalizado. Cree una lista de permitidos y una lista de no permitidos de aplicaciones para integrarlas con los perfiles de directivas de conformidad o de control de aplicaciones. Configure opciones de administración de aplicaciones avanzada, como el análisis de aplicaciones.

Cómo acceder a los asistentes de Workspace ONE, Dispositivo, Contenido y Aplicación

Cada uno de los cuatro submódulos muestra una lista de secciones que representan funciones que puede configurar o ignorar, en función de las necesidades de su organización. Las funciones no configuradas muestran la casilla Incompleta vacía, mientras que las que sí lo están muestran la casilla Completa en verde.

- Para definir los ajustes de la función que le interesa, seleccione el botón Configurar.
- Para revisar o modificar los ajustes de una función completa, seleccione el botón Editar.
- La barra de progreso de porcentaje completado avanza a medida que configura la función.
- La mayoría de funciones cuentan con el botón Vídeo junto al botón Configurar o Editar. Este vídeo le permite ver la función en acción y le ayuda a comprender su utilidad para la organización.
- Puede omitir algunas funciones del submódulo sin penalización en la barra de progreso del porcentaje completado. Para eliminar la función de la lista, seleccione el botón Omitir este paso si está disponible. Para eliminar la función de nuevo, seleccione el botón Reactivar.

Algunas funciones cuentan con prerrequisitos. Por ejemplo, para el inicio de sesión único móvil, debe tener configurados Enterprise Connector, Active Directory y Workspace ONE Access. Se puede iniciar la configuración de estas funciones obligatorias seleccionando el botón proporcionado.

Cómo habilitar el asistente de introducción de forma manual

Para una nueva implementación de Workspace ONE UEM, acceda a la página Introducción desde el menú principal. Ahora bien, también es posible habilitar manualmente el Asistente de introducción en cualquier momento. Al habilitar el asistente de introducción de forma manual, se reinicia la revisión.

1. Seleccione un grupo organizativo distinto del grupo de nivel superior.
2. Vaya a Grupos y ajustes > Grupos > Grupos organizativos > Detalles del grupo organizativo. Asegúrese de encontrarse actualmente en un grupo organizativo de nivel de cliente y seleccione Guardar para guardar los cambios.
3. Vaya a Grupos y ajustes > Todos los ajustes > Sistema > Introducción.

4. Puede activar cada una de las secciones Introducción que desee seleccionando Habilitar.
    - Introducción al Estado de Workspace ONE
    - Introducción - Estado del dispositivo
    - Introducción - Estado del contenido
    - Introducción - Estado de la aplicación
5. Seleccione Guardar los cambios realizados en esta página.

Menú principal

Puede acceder a todas las funciones habilitadas para cada función y la implementación de MDM en Workspace ONE UEM basado en AirWatch.

Introducción: asegúrese de que todos los aspectos básicos de la implementación básica se hayan establecido. En la sección Introducción se mostrarán únicamente aquellos módulos que le interesen dentro de una implementación de Workspace ONE UEM Console. De este modo, Introducción ofrece un proceso de incorporación que se ajustará mejor a su configuración real.

Monitor: permite ver y administrar información sobre MDM que le ayude a tomar las decisiones necesarias y acceder a un breve resumen de su flota de dispositivos. Además, verá información como las aplicaciones que se encuentran más comúnmente en la lista de no permitidos y que no cumplen con las reglas de conformidad. Podrá realizar un seguimiento de las licencias de los módulos mediante el tablero del panel administrativo y supervisar todos los dispositivos que no cumplan actualmente con las reglas de conformidad. Seleccione y ejecute plantillas del sector para simplificar el proceso de incorporación con las políticas y aplicaciones específicas del sector para sus dispositivos iOS.

Dispositivos: permite acceder a un resumen de los aspectos en común de los dispositivos de su flota, tales como directivas de conformidad y estado, análisis del tipo de propiedad, la última vez que se detectaron, el tipo de plataforma y el tipo de inscripción. Podrá intercambiar las vistas según sus preferencias, como las opciones de tablero completo, la vista de lista o la vista de detalles. También accederá a pestañas, como todos los perfiles actuales, el estado de inscripción, notificaciones, ajustes de protección contra eliminaciones, políticas de conformidad, certificados, aprovisionamiento de productos y administración de impresoras.

Recursos: permite acceder a los elementos de recursos que instala en los dispositivos, tales como aplicaciones, libros, sensores, perfiles de dispositivos, actualizaciones de dispositivos, scripts y pedidos de instalación, así como administrarlos. También puede ver los registros y los análisis de aplicaciones con los ajustes de la aplicación, horarios y geolocalización.

Cuentas: permite inspeccionar y administrar los usuarios y administradores relacionados con la implementación de MDM. Accederá a grupos de usuarios, roles, estados de lote y ajustes asociados a sus usuarios, y podrá administrarlos. También podrá acceder a grupos administrativos, roles, actividad del sistema y ajustes asociados con sus administradores, además de administrarlos.

Content: permite acceder a un resumen detallado del uso de contenido, como las tendencias del historial de almacenamiento, el estado del usuario y el estado del contenido, la interacción y el análisis de usuarios. Podrá administrar y cargar contenido disponible para los usuarios y dispositivos. Además, accederá al estado de importación por lotes, las categorías de contenido, los repositorios de contenido, el almacenamiento del usuario, la configuración de la página de inicio de VMware AirWatch® Content Locker™ y todos los ajustes relacionados con contenido.

Correo electrónico: permite acceder a un resumen sobre la información de correo electrónico

relacionada con la implementación. Dicha información incluye el estado de la administración de correo electrónico, los dispositivos administrados, las infracciones de políticas de correo electrónico, el tipo de implementación y la última detección.

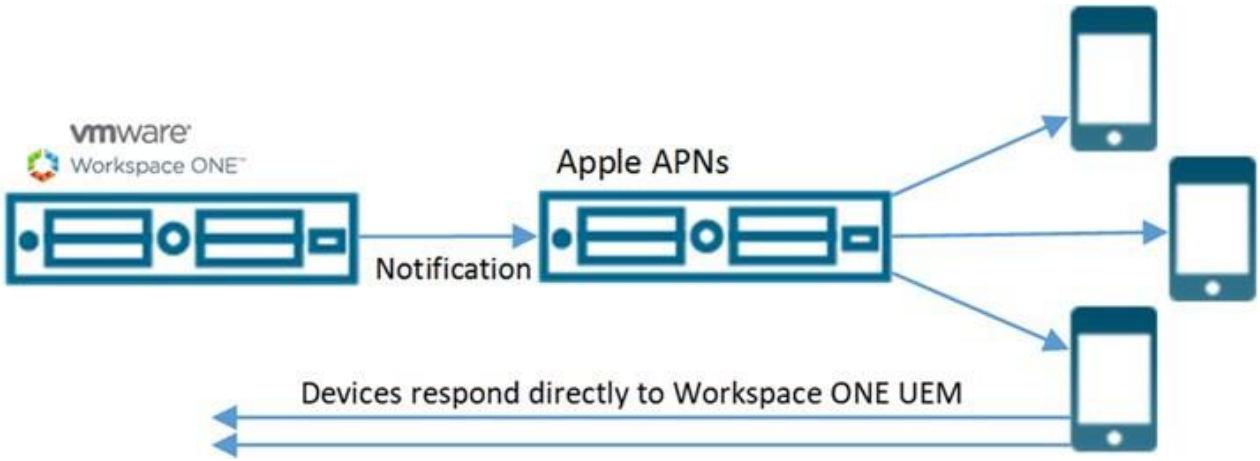
Telecom: permite acceder a un resumen detallado de los dispositivos habilitados para Telecom, con información como el historial de uso, el uso del plan y los datos de roaming. Verá y administrará el uso de telecomunicaciones y el seguimiento de datos de roaming, lo que incluye llamadas, mensajes SMS y ajustes de contenido.

Grupos y ajustes: permite administrar las estructuras, los tipos y los estados relacionados con los grupos organizativos, grupos inteligentes, grupos de aplicaciones, grupos de usuarios y grupos administrativos. Acceda a Configuraciones, que es una lista clasificada y elaborada de vínculos que conducen directamente a las páginas de ajustes que necesita.

Certificados de APN

Para administrar dispositivos iOS, primero debe obtener un certificado de servicio de notificaciones push de Apple (APN). Workspace ONE UEM se comunica con los dispositivos Apple de forma segura y transmite la información a UEM Console mediante certificados de APN.

En el programa Apple Enterprise Developer, un certificado de APN es válido durante un año y, a continuación, requiere renovación. La consola de UEM envía recordatorios a través de Notificaciones a medida que la fecha de caducidad se aproxima. El certificado actual se revoca en cuanto lo renueve desde el portal Apple Development Portal. Esto impide que pueda administrar dispositivos hasta que no cargue el nuevo certificado. Cargue el certificado inmediatamente después de renovarlo. Se recomienda utilizar un certificado para el entorno de producción y otro certificado para el entorno de prueba.



Caducidad de los certificados de APN

El botón Notificaciones de la barra superior de la consola le enviará una alerta cuando los certificados de APN para MDM estén a punto de caducar, lo que le permitirá actuar.

Para obtener más información, consulte la sección Notificaciones de la consola.

Cómo generar un certificado de APN

Para poder administrar los dispositivos iOS con Workspace ONE UEM, primero debe generar un certificado de APN para habilitar y mantener comunicaciones seguras entre los dispositivos iOS y Workspace ONE UEM Console.

Puede seguir los pasos descritos en Uso del asistente de introducción, o bien generar un nuevo certificado de APN manualmente realizando los siguientes pasos.

1. Acceda a Grupos y ajustes > Todos los ajustes > Dispositivos y usuarios > Apple > APNs para MDM.

2. Seleccione el botón Generar nuevo certificado. Se muestra el paso 1 Firmar solicitud.
3. Seleccione el vínculo "MDM_APNsRequest.plist" y seleccione una ubicación para guardar. Cargue este archivo en Apple en el siguiente paso.
4. Puede obtener información sobre cómo cargar un certificado desde Apple Push Certificates Portal seleccionando el vínculo de instrucciones. En esta página se ofrece el botón Ir a Apple, que le resultará práctico al abrir el portal de certificados push de Apple en una pestaña nueva del navegador.
5. Necesita dos elementos para continuar:
    - La solicitud de certificado de Workspace ONE UEM, que es el archivo PLIST que guardó en el dispositivo.
    - Un ID de Apple corporativo que está dedicado a la MDM de la empresa. Seleccione el vínculo proporcionado ("Haga clic aquí") para continuar con la creación del ID de Apple. A continuación, se abrirá una nueva pestaña en el navegador.
6. Haga clic en Siguiente para avanzar a la siguiente página, donde deberá introducir su ID de Apple y cargar el certificado de MDM de Workspace ONE UEM emitido por Apple (archivo PEM).
7. Seleccione Guardar.

Resultados: Se genera el certificado de APN.

Pasos siguientes: Compruebe la conectividad del certificado de APN a través del protocolo HTTP/2. Consulte la sección con el título Revisar la conectividad de APN a través de HTTP/2.

Renovar certificados de APN existentes

Para habilitar y mantener comunicaciones seguras entre los dispositivos iOS y Workspace ONE UEM, en ocasiones debe renovar los certificados de APN.

Puede seguir los pasos descritos en Uso del asistente de introducción, o bien renovar los certificados de APN caducados manualmente realizando los siguientes pasos.

1. Acceda a Grupos y ajustes > Todos los ajustes > Dispositivos y usuarios > Apple > APNs para MDM.
2. Seleccione el botón Renovar y siga las instrucciones.
3. Seleccione el vínculo "MDM_APNsRequest.plist" y seleccione una ubicación para guardar. Debe cargar este archivo en Apple en el siguiente paso.
4. Puede obtener información sobre cómo cargar un certificado desde Apple Push Certificates Portal seleccionando el vínculo de instrucciones. En esta página se ofrece el botón Ir a Apple, que le resultará práctico al abrir el portal de certificados push de Apple en una pestaña nueva del navegador.
5. Necesita dos elementos para continuar:
    - La solicitud de certificado de Workspace ONE UEM, que es el archivo PLIST que guardó en el dispositivo.
    - El ID de Apple que se usó originalmente para crear el certificado, que se muestra en el elemento 2 del paso 1: Firmar solicitud. Consulte la sección con el título Generar

un nuevo certificado de APN.

6. Haga clic en Siguiente para avanzar a la siguiente página, donde deberá introducir su ID de Apple y cargar el certificado de MDM de Workspace ONE UEM emitido por Apple (archivo PEM).
7. Seleccione Guardar.

Resultados: El certificado de APN existente se renueva.

Seleccione la conectividad del certificado de APN a través del protocolo HTTP/2. Consulte la siguiente sección con el título Revisar la conectividad de APN a través de HTTP/2.

Revisar la conectividad de APN a través de HTTP/2

Puede revisar la conectividad entre Workspace ONE UEM y el endpoint de la API HTTP/2 de Apple, api.push.apple.com:443. Esta revisión le garantiza la funcionalidad de APN a través de una conexión HTTP/2 después de generar un nuevo certificado o después de la renovación de un certificado.

Esta prueba de conectividad solo sirve para probar APN a través de la conexión HTTP/2 predeterminada. Los errores de conectividad de esta prueba no afectan a la funcionalidad de APN en una conexión heredada.

1. Acceda a Grupos y ajustes > Todos los ajustes > Dispositivos y usuarios > Apple > APNs para MDM.
2. Seleccione el botón Probar conexión. Workspace ONE UEM Console realiza una prueba interna para determinar si la conectividad a través del nuevo protocolo HTTP/2 funciona.

Resultados: Debido a que esta prueba solo se centra en el protocolo HTTP/2, los errores de esta prueba no afectan a la comunicación de APN actual. Si se produce un error en la prueba de conectividad HTTP/2, los pasos que realice dependerán de la causa del error.

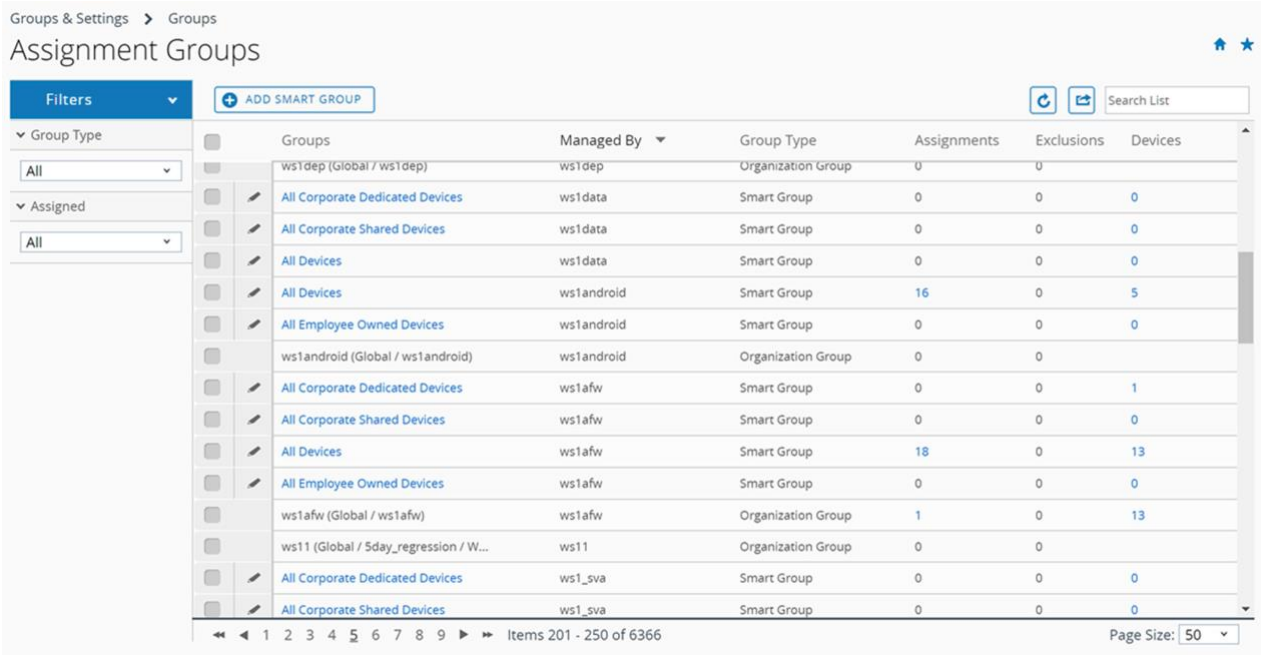
1. Certificado caducado: el certificado que está usando para la prueba ha caducado. Solicite una renovación siguiendo las instrucciones sobre renovación de un certificado de APN existente en esta página.
2. Certificado no válido: el certificado que está usando para la prueba, aunque no ha caducado, no es válido por otros motivos. Puede solicitar la renovación del certificado o esperar unos minutos y volver a probar la conexión.
3. Error desconocido: suele producirse durante una pérdida temporal de acceso a Internet. Espere unos minutos y vuelva a probar la conexión.
4. Cliente de APN desactivado: aunque es raro, esto significa que Apple ha devuelto un error interno o que el servicio de APN no está disponible. Espere unos minutos y vuelva a probar la conexión.

Grupos de asignación

El término general "grupos de asignación" se utiliza para categorizar ciertas estructuras de agrupación administrativas dentro de Workspace ONE UEM basado en AirWatch. Los grupos organizativos, grupos inteligentes y grupos de usuarios tienen su propio conjunto de funciones y cada uno es distinto.

Una función que estos grupos tienen en común es asignar contenido a los dispositivos de los usuarios fácilmente. Cada administrador puede administrar estas tres estructuras de agrupamiento desde una sola ubicación.

Acceda a Grupos y ajustes > Grupos > Grupos de asignación.



Puede asignar varios grupos organizativos, grupos inteligentes y grupos de usuarios a uno o varios perfiles, aplicaciones públicas y políticas desde la vista de lista Grupos de asignación.

Vista de lista de los grupos de asignación

La Vista de lista de los grupos de asignación organiza tres tipos de grupos que tienen la capacidad de asignar contenido a los dispositivos: grupos organizativos, grupos inteligentes y grupos de usuarios. Puede crear una lista solo con los grupos que le interese ver.

Vaya a Grupos y ajustes > Grupos > Grupos de asignación, y se mostrará la Vista de lista de los grupos de asignación. Los únicos grupos de asignación que se muestran son aquellos administrados por el grupo organizativo en el que se encuentra actualmente el administrador.

Vista de lista del grupo de asignación: Cómo ordenar por

columnas

Puede ordenar las listas de grupos por columnas individuales mediante la selección del encabezado de columna.

Vista de lista del grupo de asignación: Cómo filtrar los grupos

Puede filtrar los grupos por Tipo de grupo (Grupos inteligentes, Grupos organizativos y Grupos de usuarios). También puede filtrar por cómo se han asignado o si tienen el estado Asignado(s) (Asignaciones, Exclusiones, Todo y Ninguno).

Vista de lista del grupo de asignación: Cómo seleccionar vínculos

Las cuatro columnas de la página de lista Grupos de asignación tienen una función específica y requieren una mención especial.

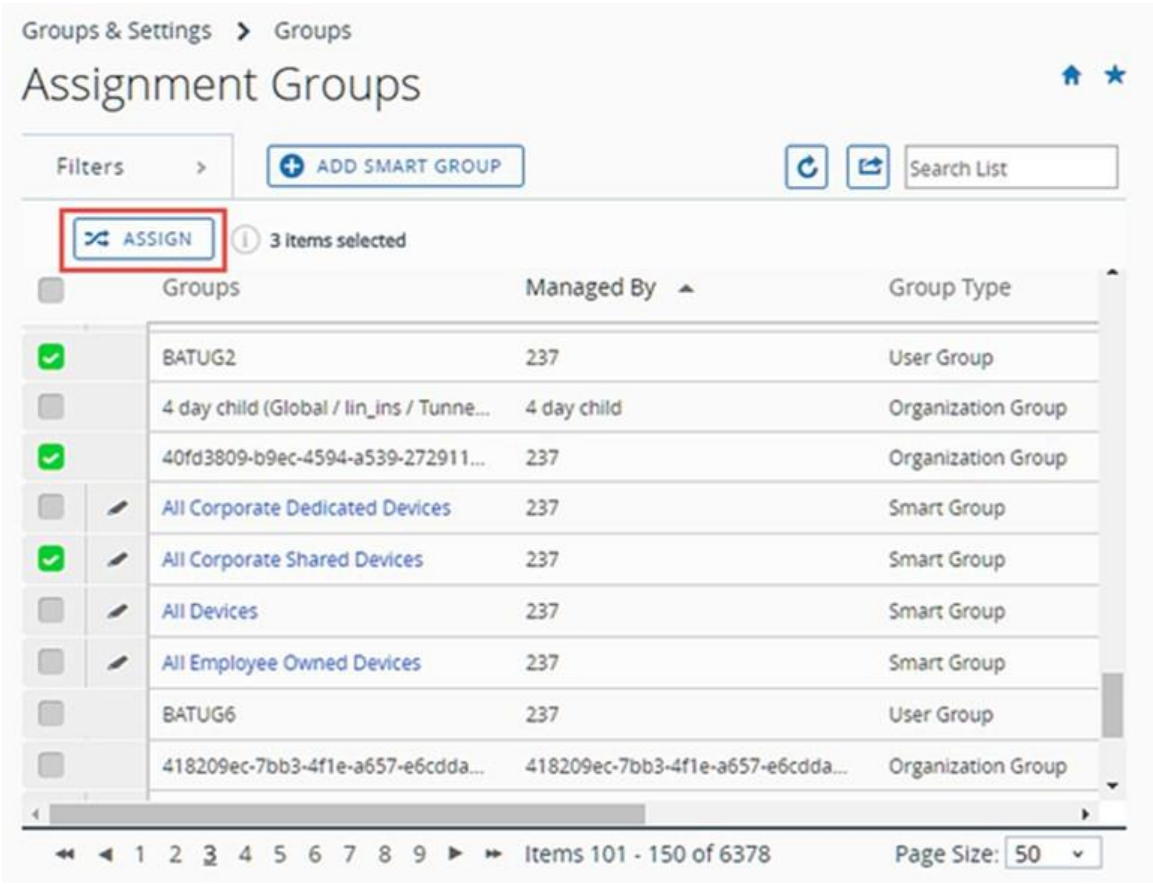
- La columna Grupos tiene un enlace para cada Grupo inteligente. Puede editar el grupo inteligente al seleccionar este enlace.
- Si selecciona valores que no sean cero en la columna Asignaciones, aparecerá la página Ver asignaciones, incluso para los grupos de usuarios y grupos organizativos asignados. Puede ver y confirmar asignaciones a perfiles, aplicaciones públicas y políticas de conformidad. Para obtener más información, consulte Ver asignaciones.
- Si selecciona valores que no sean cero en la columna Exclusiones, aparecerá la página Ver asignaciones, incluso para los grupos de usuarios y grupos organizativos excluidos. Puede ver y confirmar exclusiones de perfiles, aplicaciones públicas y políticas de conformidad.
- Si selecciona el número de la columna Dispositivos, aparecerá la Vista de lista de la lista de dispositivos. La Vista de lista de dispositivos contiene la lista de todos los dispositivos del grupo organizativo, el grupo inteligente o el grupo de usuarios seleccionado.

Cómo asignar uno más grupos de asignación

Puede asignar grupos a los perfiles de dispositivos, aplicaciones públicas y políticas de conformidad. También puede asignar varios grupos de cada tipo individual (organizativo, inteligente o de usuarios) de una sola vez.

Para asignar aplicaciones públicas, puede configurar diferentes directivas de aplicaciones para diferentes grupos de usuarios. Para obtener más información, consulte Usar implementación flexible para asignar aplicaciones en la Guía de VMware Workspace One UEM para la administración de aplicaciones móviles, que puede encontrar en docs.vmware.com.

1. Acceda a Grupos y ajustes > Grupos > Grupos de asignación.
2. Seleccione uno o más grupos de la lista y luego el botón de Asignar.



3. La página Asignación mostrará los Grupos organizativos, Grupos de asignación y Grupos de usuarios que ha seleccionado.
4. Para asignarlos, busque Perfil, Aplicación pública y Directiva de conformidad. Puede seleccionar hasta 10 perfiles, hasta 10 aplicaciones públicas y una política de conformidad única.

   Solo puede seleccionar varias entidades de un solo tipo por sesión. Por ejemplo, puede asignar varios grupos a hasta 10 perfiles diferentes en un solo comando. Sin embargo, es posible que, en un único comando, no pueda asignar varios grupos a 10 perfiles, 10 aplicaciones y una política de conformidad. Si tiene entidades de varios tipos, tiene que realizar sesiones de asignación independientes para cada tipo (perfiles, aplicaciones y políticas).
5. Seleccione Siguiente para mostrar la página Ver la asignación de dispositivos, donde puede confirmar la asignación de los grupos.
6. Seleccione Guardar y publicar para finalizar la asignación.

Cómo eliminar grupos

Puede eliminar un grupo de asignación, ya sea un grupo organizativo, un grupo inteligente, un grupo de usuarios o un grupo de administradores, siempre y cuando elimine primero todas las asignaciones y vacíe el grupo. Para obtener más información sobre cómo eliminar cada tipo de grupo, consulte los siguientes temas.

- Grupo organizativo: consulte la sección Eliminar un grupo organizativo en Grupos organizativos

- Grupo inteligente: consulte la sección Cómo anular la asignación de un grupo inteligente en Grupos inteligentes
- Grupo de usuarios: consulte la sección Vista de lista de los grupos de usuarios en Grupos de usuarios
- Grupo administrativo: consulte la sección Vista de lista de los grupos administrativos en Grupos administrativos

Grupos organizativos

Entienda los grupos organizativos como ramas individuales de un árbol genealógico, en el que cada hoja es un usuario de dispositivo. Workspace ONE UEM basado en AirWatch identifica cada hoja y establece su posición en el árbol genealógico mediante grupos organizativos (GO). La mayoría de los clientes hacen que los árboles de GO reflejen la jerarquía corporativa: Ejecutivos, Administración, Operaciones, Ventas, etc.

También puede establecer GO basados en funciones y contenido de Workspace ONE UEM.

Puede acceder a los grupos organizativos si accede a Grupos y ajustes > Grupos > Grupos organizativos > Vista de lista o a través del menú desplegable del grupo organizativo.

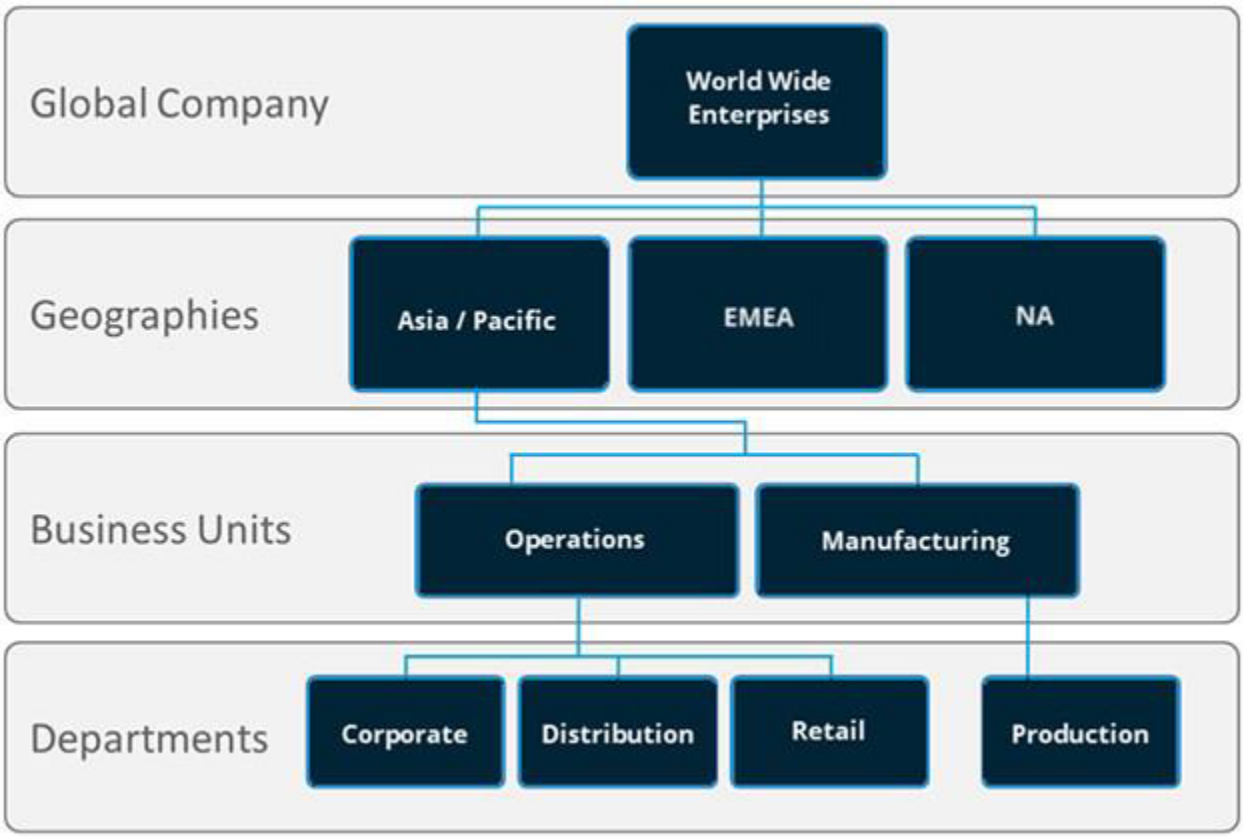
- Cree grupos para las entidades de su organización (Administración, Asalariados, Por horas, Ventas, Minoristas, Recursos humanos, Ejecutivos, etc.).
- Personalice las jerarquías con niveles principales y secundarios (por ejemplo, "Asalariados" y "Por horas" como elementos secundarios de "Administración").
- Integre con varias infraestructuras internas en cada nivel.
- Delegue el acceso basado en roles y la administración basada en una estructura jerárquica.

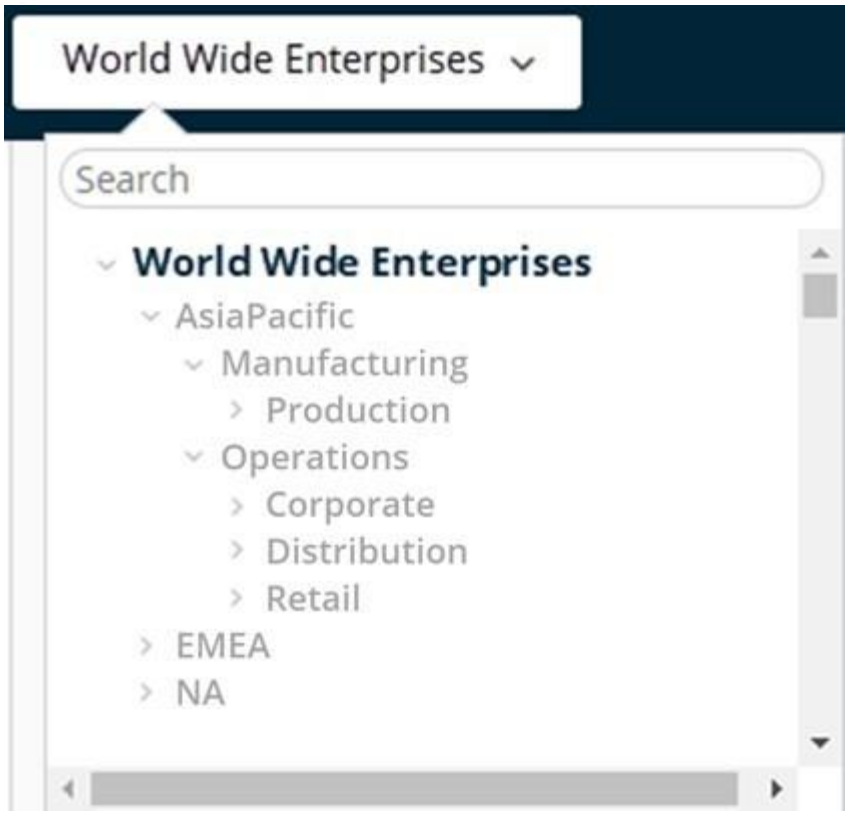
Aviso: La Vista de lista de los grupos organizativos define como "Dispositivos activos" solo aquellos dispositivos que se han notificado a Workspace ONE UEM Console dentro del período de 8 horas anterior.

Características de los grupos organizativos

Los grupos organizativos tienen capacidad para admitir entidades funcionales, geográficas y organizacionales, además de permitir una solución de estructura jerárquica.

- Escalabilidad: soporte flexible para el crecimiento exponencial.
- Multiempresa: creación de grupos que funcionan como entornos independientes.
- Herencia: simplificación del proceso de configuración al asignar que los grupos secundarios hereden las configuraciones de los grupos primarios.





Como se ve en el ejemplo del menú desplegable de grupo organizativo, se pueden configurar perfiles, funciones y aplicaciones y otros ajustes de MDM en el nivel Empresas globales.

Los ajustes se heredan a los grupos organizativos secundarios, tales como Asia Pacífico y EMEA, o incluso en niveles inferiores de la jerarquía, como Asia Pacífico > División de fabricación o Asia Pacífico > División de operaciones > Corporativo.

Los ajustes entre grupos organizativos del mismo nivel como Asia Pacífico y EMEA aprovechan la naturaleza de estructura jerárquica de estos grupos, todo ello manteniendo los ajustes independientes los unos de los otros. Sin embargo, estos dos grupos organizativos del mismo nivel heredan los ajustes de los grupos primarios, Empresas Exportaciones Iberoamérica.

También puede reemplazar los ajustes en un nivel inferior y modificar solo aquellos que desee cambiar o mantener. Puede cambiar esos ajustes o transferirlos a cualquier nivel inferior.

Consideraciones para la configuración de los grupos organizativos

Antes de configurar la jerarquía de grupos organizativos (GO) en Workspace ONE UEM Console, debe diseñar la estructura de los grupos. La estructura de los grupos le permite aprovechar al máximo los ajustes, aplicaciones y recursos.

- Administración delegada: puede delegar la administración de grupos secundarios a los administradores de un nivel inferior mediante la restricción de su visibilidad a un grupo organizativo inferior.

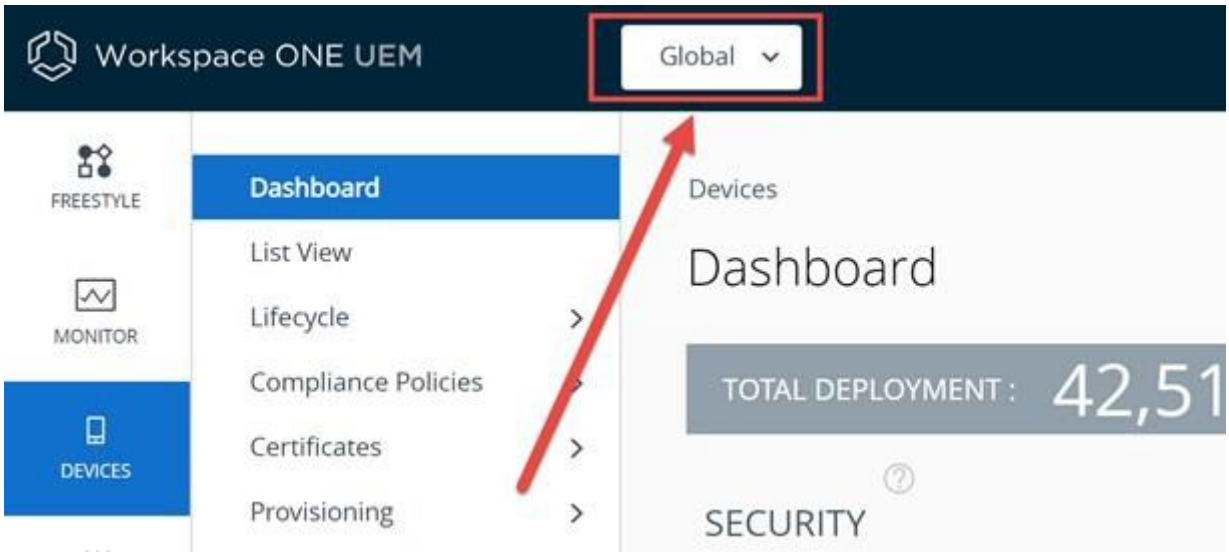
- Los administradores corporativos pueden acceder y ver todo el entorno.
- El administrador de Los Ángeles tiene acceso al grupo organizativo de Los Ángeles y solo puede administrar estos dispositivos.
- El administrador de Nueva York tiene acceso al GO de Nueva York y solo puede administrar estos dispositivos.
- Ajustes del sistema: los ajustes se aplican a niveles diferentes en el árbol de grupos organizativos y heredarse en los niveles inferiores. También pueden remplazarse en cualquier nivel. Los ajustes incluyen opciones de inscripción de dispositivos, métodos de autenticación, configuración de privacidad y personalización de marca.

- La compañía en general establece la inscripción con el servidor de Active Directory de la compañía.
- Los controladores de dispositivos anulan la autenticación primaria y permiten el uso de inscripción basada en token.
- Los dispositivos de almacén heredan los ajustes de AD desde el grupo principal.
- Escenario de uso del dispositivo: un perfil puede asignarse a uno o varios grupos organizativos. Los dispositivos de esos grupos podrán recibir ese perfil. Consulte la sección Perfiles para obtener más información. Contemple la posibilidad de configurar los dispositivos usando los ajustes de perfil, aplicación y contenido de acuerdo con atributos tales como la marca del dispositivo, el modelo, el tipo de propiedad o los grupos de usuarios antes de crear los grupos organizativos.

- Los dispositivos ejecutivos no pueden instalar aplicaciones ni tener acceso a la red Wi-Fi del equipo de ventas.
- Los dispositivos de ventas pueden instalar aplicaciones y tener acceso a la VPN.

Cambiar grupos organizativos

Puede cambiar los grupos organizativos seleccionando el indicador de grupo organizativo en la parte superior derecha de la pantalla.



Cuando se selecciona, un menú desplegable muestra la jerarquía del grupo organizativo, lo que le permite cambiar a otro grupo organizativo.

Cómo comparar los grupos organizativos

Puede comparar los ajustes de un grupo organizativo con los de otro para mitigar los problemas relacionados con la migración de la versión. La función de comparación de grupos organizativos solo está disponible para los clientes en la sede.

Puede realizar las siguientes tareas cuando compare los ajustes de GO.

- Cargar archivos XML que contengan los ajustes del GO de diferentes versiones del software de Workspace ONE UEM.
- Eliminar la posibilidad de que una diferencia en la configuración cause problemas durante la migración de una versión.
- Filtrar los resultados de la comparación para mostrar solo los ajustes que desea comparar.
- Buscar un ajuste concreto por su nombre con la función de búsqueda.

Un ejemplo de un escenario de migración de la versión es que cuando un servidor de pruebas de aceptación de usuario (UAT) se ha actualizado, configurado y probado, puede comparar directamente los ajustes de UAT con los ajustes de producción.

1. Vaya a Grupos y ajustes > Todos los ajustes > Administrador > Administración de ajustes > Comparación de ajustes.
2. Seleccione un GO del entorno en el menú desplegable que está a la izquierda (que está marcado con un 1). O bien cargue el archivo de ajustes XML mediante la selección del botón Cargar y elija un archivo XML de ajustes de GO que se haya exportado.
3. Seleccione el GO con el que desea realizar la comparación en el menú desplegable de la derecha (que está marcado con un 2).
4. Visualice una lista con todos los ajustes de ambos grupos organizativos seleccionados. Para ello, seleccione el botón Actualizar.
    - Las diferencias entre los dos conjuntos de ajustes del GO se marcan.
    - También tiene la opción de marcar la casilla de verificación Mostrar solo las diferencias. La casilla solo muestra los ajustes que se aplican a un GO, no al otro.
    - Los ajustes individuales que estén en blanco (o sin especificar) se muestran en la lista comparativa como "NULL".

Cómo crear grupos organizativos

Deberá crear un grupo organizativo (GO) para cada entidad de la empresa en la que haya dispositivos implementados. Debe saber que el GO en el que se encuentra actualmente será el GO principal del GO secundario que está a punto de crear.

1. Vaya a Grupos y ajustes > Grupos > Grupos organizativos > Detalles.
2. Seleccione la pestaña Agregar grupo organizativo secundario y realice los siguientes ajustes.

Ajustes	Descripción
Nombre	Introduzca el nombre del grupo organizativo (GO) secundario que se mostrará. Utilice únicamente caracteres alfanuméricos. No utilice caracteres especiales.
ID del grupo	Los usuarios finales utilizan este identificador de GO obligatorio durante el inicio de sesión del dispositivo y durante la inscripción de dispositivos de grupo en el GO pertinente. Asegúrese de que los usuarios que comparten dispositivos reciban el ID de grupo, ya que es posible que lo necesiten para iniciar sesión en función de la configuración del dispositivo compartido. Si no está en un entorno local, el ID de grupo identifica el grupo organizativo en todo el entorno de SaaS compartido. Por este motivo, todos los ID de grupo deben ser exclusivos.
Tipo	Seleccione el tipo de grupo organizativo preconfigurado que refleje la categoría del grupo organizativo secundario.
País	Seleccione el país del GO.
Región	Seleccione la clasificación del idioma del país seleccionado.
Industria del cliente	Este ajuste solo está disponible cuando en Tipo se ha especificado como Cliente. Selecciónelo en la lista de industrias de clientes.

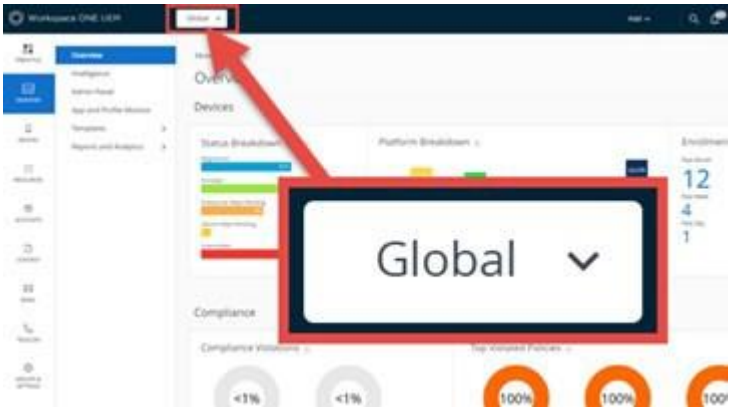
Ajustes	Descripción
Zona horaria	Seleccione la zona horaria para la ubicación del GO.

3. Seleccione Guardar.

Eliminar un grupo organizativo

Puede eliminar un grupo organizativo (GO) siempre que no contenga grupos secundarios del grupo organizativo, ni dispositivos en ninguna sección de su línea descendente.

1. Desplácese hasta el grupo organizativo que desea eliminar y selecciónelo en el menú desplegable del grupo organizativo.



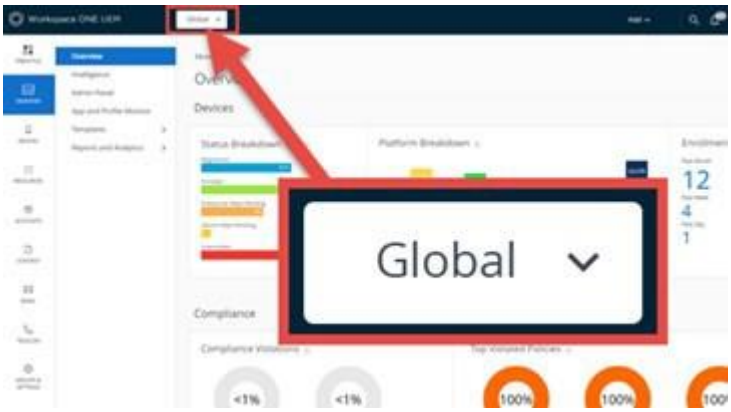
2. Vaya a Grupos y ajustes > Grupos > Grupos organizativos > Detalles.
3. En la parte inferior de la pantalla Detalles, revise los recuentos de Dispositivos en el grupo organizativo y de Grupos organizativos secundarios. Si alguna de las entradas no es cero, no podrá eliminar el grupo organizativo y el botón Eliminar no estará disponible.

   Debe mover todos los dispositivos de este grupo organizativo a otro grupo organizativo. Cualquier grupo organizativo secundario que desee eliminar tampoco debe contener ningún dispositivo antes de poder eliminarlo.
4. Una vez que los recuentos de Dispositivos en el grupo organizativo y Grupos organizativos secundarios sean ambos cero, puede continuar con la eliminación del grupo organizativo.
5. Seleccione el botón Eliminar.
6. La pantalla Acción restringida: eliminar grupo organizativo muestra y proporciona advertencias sobre los preparativos que debe realizar antes de eliminar el grupo organizativo.
7. Antes de poder continuar con la eliminación, debe introducir el PIN de seguridad de cuatro dígitos que seleccionó al inscribirse como administrador de UEM. Restablezca este PIN seleccionando el vínculo *¿Ha olvidado el PIN de seguridad?*.

Identificar el ID de grupo de cualquier grupo organizativo

Puede realizar los siguientes pasos para identificar el ID de grupo de cualquier grupo organizativo (GO).

1. Desplácese hasta el grupo organizativo que desea identificar y selecciónelo en el menú desplegable del grupo organizativo.

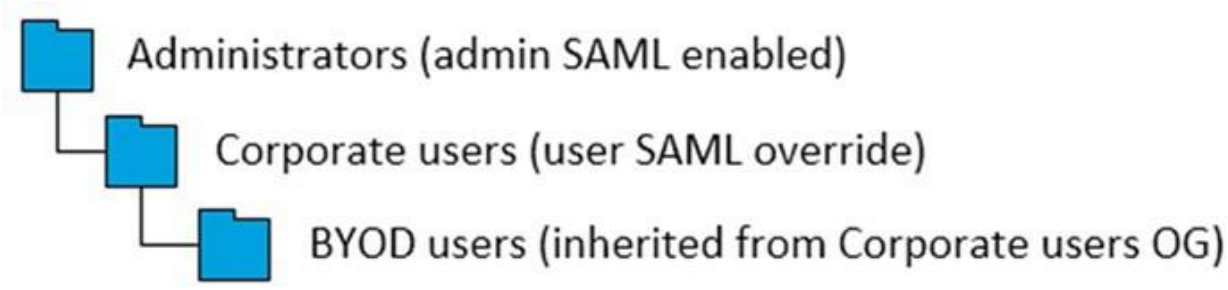


2. Coloque el puntero sobre la etiqueta del GO. Un menú emergente muestra el nombre y el ID de grupo del grupo organizativo seleccionado actualmente.

Herencia, multiempresa y autenticación

El concepto de la anulación de ajustes en un grupo organizativo, cuando se combina con características de grupo organizativo (GO) como la herencia y la multiempresa, puede combinarse además con la autenticación. Esta combinación proporciona una configuración flexible.

El siguiente modelo de grupo organizativo demuestra dicha flexibilidad.



En este modelo, los Administradores, normalmente en posesión de permisos y funcionalidad superiores, se sitúan en la parte superior de esta rama de GO. Estos administradores inician sesión en su GO mediante SAML, que es de uso exclusivo para los administradores.

Los Usuarios corporativos están subordinados a los administradores, de modo que su grupo organizativo queda organizado como su elemento secundario. Dado que son usuarios y no administradores, la configuración de SAML para el inicio de sesión no puede heredar la

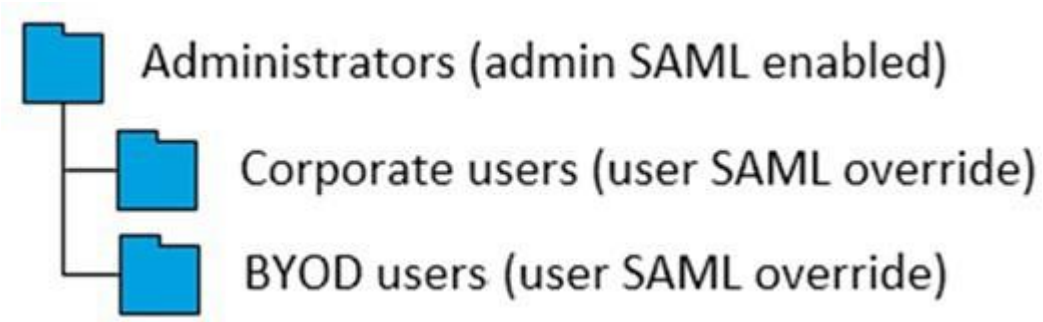
configuración de administrador. Por lo tanto, se anula el ajuste de SAML de los usuarios corporativos.

Los usuarios de BYOD son diferentes de los usuarios corporativos. Los dispositivos que utilizan los usuarios de BYOD pertenecen a los propios usuarios y es probable que contengan más información personal. Por lo tanto, estos perfiles de dispositivo pueden requerir una configuración ligeramente distinta. Los usuarios de BYOD pueden contar con un acuerdo de términos de uso diferente. Es posible que los dispositivos de BYOD necesiten parámetros de eliminación empresarial diferentes. Por estas y otras razones, es lógico que los usuarios de BYOD inicien sesión en un GO distinto.

Considerar a los usuarios de BYOD como elemento secundario de los usuarios corporativos conlleva una serie de ventajas, aunque los primeros no estén subordinados a los usuarios corporativos en un sentido jerárquico dentro de la empresa. Esta organización significa que los usuarios de BYOD heredan configuraciones aplicables a TODOS los dispositivos de usuario corporativos asignándolos al GO de usuarios de la empresa.

La herencia también afecta a los ajustes de autenticación mediante SAML. Dado que los usuarios de BYOD son un elemento secundario de los usuarios corporativos, los usuarios de BYOD heredan su SAML para los ajustes de autenticación.

Otro modelo es convertir a los usuarios de BYOD en elemento del mismo nivel que los usuarios corporativos.



Con este modelo alternativo, se cumpliría lo siguiente.

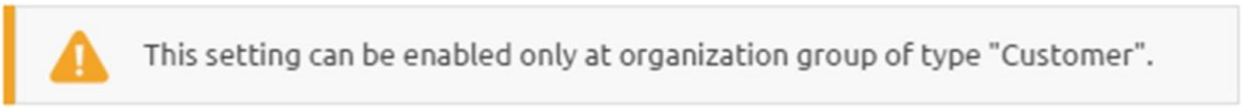
- Todos los perfiles de dispositivo creados para aplicarse globalmente en TODOS los dispositivos, incluidas las políticas de conformidad y otros ajustes de dispositivo globalmente aplicables, se aplican a dos grupos organizativos en lugar de uno. El motivo de esta duplicación se debe a que la herencia de los usuarios corporativos a los usuarios de BYOD ya no es un factor en este modelo. Los usuarios corporativos y los usuarios de BYOD son *elementos del mismo nivel* y, por lo tanto, no existe herencia.
- Se debe aplicar otra anulación SAML a los usuarios de BYOD. Esta anulación es necesaria porque el sistema supone que hereda configuraciones de SAML de su elemento principal: los administradores. Esta suposición es un error, ya que los usuarios de BYOD no son administradores y no tienen los mismos derechos de acceso y permisos.
- Los usuarios de BYOD siguen considerándose distintos de los usuarios corporativos. Este modelo alternativo significa que siguen contando con su propia configuración de perfil de dispositivo.

¿Cómo saber qué modelo es el mejor? Compare la cantidad de configuraciones de dispositivo globalmente aplicables con la cantidad de configuraciones de dispositivo para los grupos. Básicamente, si, en general, desea considerar todos los dispositivos por igual, evalúe la opción de convertir a los usuarios de BYOD en elemento secundario de los usuarios corporativos. Si le interesa

más contar con configuraciones independientes, evalúe la opción de convertir a los usuarios de BYOD en elemento del mismo nivel que los usuarios corporativos.

Restricciones del grupo organizativo

Si trata de configurar un ajuste limitado para el grupo organizativo (GO), las páginas de ajustes disponibles en Grupos y ajustes > Todos los ajustes le informarán acerca del límite.



Las siguientes restricciones aplican a la creación de grupos organizativos de tipo cliente.

- Tanto si se trata de un entorno de software como servicio (SaaS) o local, no se pueden crear GO de cliente anidados.

Funciones y personalizaciones del tipo de grupo organizativo

El tipo de grupo organizativo puede afectar los ajustes que los administradores podrán configurar.

- Global: el grupo organizativo de nivel más elevado. Normalmente, este grupo se denomina Global y es de tipo global.
    - En entornos alojados de SaaS, no es posible acceder a este grupo.
    - En las instalaciones, los clientes pueden activar un nivel de registro Detallado.
- Cliente – el grupo organizativo de nivel superior para cada cliente.
    - Un grupo organizativo de clientes no puede tener grupos organizativos primarios y secundarios de tipo cliente.
    - Los flujos de trabajo esenciales solo pueden producirse dentro de un GO de tipo Cliente o dentro de su jerarquía. Estos flujos de trabajo incluyen agregar un dispositivo, registrar e inscribir un dispositivo, asignar grupos de usuarios, crear y asignar grupos inteligentes, cambiar el GO de un dispositivo (o mover un dispositivo de un GO a otro) y retirar el dispositivo.
    - Algunos ajustes solo pueden configurarse en un grupo de clientes. Estos ajustes se filtran a los GO de tipo contenedor inferiores.
        - Dominios de correo electrónico de detección automática
        - Ajustes del programa de inscripción de dispositivos (antes de AirWatch 8.0)
        - Contenido personal
        - El VPP (programa de compras por volumen) de Apple debe estar habilitado en el GO principal del cliente para que la funcionalidad del VPP funcione en los GO de tipo contenedor secundarios.
        - Samsung Enterprise FOTA
        - Paquetes de Hub
        - Atributos personalizados
        - Servidor de retransmisión

    - Intelligence
    - Sensores
    - Protección contra el análisis y la eliminación de aplicaciones
    - CDN (Content Delivery Network) para la entrega de aplicaciones
    - El almacenamiento NFS para la administración de contenido se podrá configurar
    - Servicios de Workspace One Hub
    - Acceso condicional
    - MAG (Mobile Access Gateway)
    - LBUS (Local Basic User Sync)
    - Dynamic Environment Manager
    - Flujos de trabajo móviles
- Contenedor: el tipo predeterminado de grupo organizativo.
    - Todos los grupos organizativos por debajo de un grupo organizativo de clientes deben ser de tipo contenedor. Puede tener contenedores entre los grupos de socios y clientes.
- Socio: grupo organizativo de nivel superior para los socios (distribuidores externos de Workspace ONE UEM).
- Cliente potencial: los clientes potenciales. Similar a un grupo organizativo de clientes y puede tener menos funcionalidad que un verdadero grupo de clientes.

Hay otros tipos de grupos organizativos, por ejemplo, de división y región, y dispone de la capacidad de definir su propio tipo de grupo organizativo.

Agregar tipo de grupo organizativo

Puede agregar tipos de grupos organizativos personalizados. Estos tipos no tienen ninguna característica especial y funcionan de forma idéntica al grupo organizativo de tipo contenedor.

Para crear su propio tipo de GO…

1. Vaya a Grupos y ajustes > Grupos > Grupos organizativos > Tipos y, a continuación, seleccione el botón Agregar tipo de grupo organizativo.
2. Introduzca el Nombre que desee para el tipo de grupo organizativo y su Descripción.
3. Seleccione Guardar.

Razones por las que no debería inscribir dispositivos en Global

Existen varias razones por las que no es buena idea inscribir dispositivos directamente en el grupo organizativo (GO) de nivel superior, comúnmente conocido como Global. Estas razones son la arquitectura multiempresa, la herencia y la funcionalidad.

Arquitectura multiempresa

Puede crear todos los grupos organizativos que necesite y configurar cada uno de ellos de forma

independiente con respecto al resto. Los ajustes que aplique a un GO secundario no afectarán a otros elementos del mismo nivel.

Herencia

Los cambios realizados en un GO primario se aplican a los elementos secundarios. A la inversa, los cambios realizados en un GO secundario no se aplican a los elementos primarios ni del mismo nivel.

Funcionalidad

Existen ajustes y funcionalidades que solo pueden configurarse en grupos organizativos de tipo Cliente. Entre ellos se incluyen protección contra eliminaciones, Telecom y contenido personal. Los dispositivos añadidos directamente al grupo organizativo global del nivel más alto se excluyen de estos ajustes y esta funcionalidad.

El grupo organizativo (GO) Global está diseñado para albergar a Cliente y otros tipos de GO. Dada la forma en la que funciona la herencia, si agrega servicios a Global y configura Global con ajustes que afectarán a estos dispositivos, también resultarán afectados todos los GO de Cliente inferiores. Esto reduce las ventajas de la estructura jerárquica y la herencia.

Reemplazar frente a Heredar para los grupos organizativos

La jerarquía de la estructura del grupo organizativo (GO) que cree determina qué grupos organizativos son elementos secundarios y cuáles son principales. Los GO secundarios heredan la configuración del grupo primario, pero pueden optar por reemplazar esta herencia.

Cada página de ajustes del sistema aplica sus ajustes según dos tipos de opciones de herencia o reemplazo en lo que concierne a la jerarquía de grupos organizativos: 1) Ajuste actual y 2) Permiso del grupo secundario. El GO al que aplica la configuración es el GO en el que se encuentra actualmente.

En otras palabras, si se encuentran en GO Empleados\Almacén, los cambios que realice en la configuración se aplicarán a ese GO y a todos los GO que sean secundarios del GO Almacén.

Por ejemplo, la página de ajustes Marca a la que se llega al navegar a Grupos y ajustes > Todos los ajustes > Sistema > Marca controla todas las imágenes de fondo, los logotipos y las combinaciones de colores personalizados del GO que aparecen en el menú desplegable visible del grupo organizativo.

Al aplicar nuestro ejemplo anterior, puede importar una nueva imagen de fondo, un nuevo logotipo o una combinación de colores diferente, específicamente para el GO Empleados/Almacén. También puede configurar los ajustes para que se apliquen al GO Almacén únicamente. Esta opción se habilita si se cambia la herencia de los GO en la página Ajustes.

Permiso del grupo secundario

Considere el ajuste Permiso del grupo secundario como la actitud del GO principal respecto al GO secundario. Existen tres ajustes diferentes para Permiso del grupo secundario: Heredar o reemplazar, Solo heredar y Solo reemplazar.

El ajuste Heredar o reemplazar simplemente significa que el elemento principal no tiene preferencia respecto a los permisos del elemento secundario. Cuando el valor del ajuste Permiso del grupo secundario de un elemento principal es Heredar o reemplazar, el Ajuste actual del GO secundario determina si el ajuste se reemplaza o hereda. Los permisos secundarios se establecen en Heredar o

reemplazar de forma predeterminada.

Un ajuste de permiso secundario Heredar solamente en el elemento principal fuerza la herencia en todos los elementos secundarios. Este ajuste significa que todos los objetos secundarios tienen la misma configuración que el elemento principal. La configuración de Permiso secundario Reemplazar solamente elimina el efecto de herencia en todos los grupos organizativos secundarios, lo que requiere que configure los ajustes específicos de ese grupo organizativo secundario.

La configuración de permisos secundarios solo afecta a los secundarios de un nivel inferior. Este ajuste no tiene ningún impacto en los grupos secundarios de segundo nivel o inferiores.

Configuración actual

El permiso secundario es la posición del elemento principal respecto al secundario, el ajuste actual de un GO es la conducta del elemento secundario con respecto al principal. Una configuración actual puede ser solo Heredar o Reemplazar.

Una configuración actual Heredar significa que el GO secundario acepta toda la configuración del GO principal. Seleccione una configuración actual Reemplazar para que el secundario rechace al principal y se quede solo. La selección de reemplazo significa que puede crear una nueva configuración para el elemento secundario.

Solo puede cambiar el Ajuste actual del GO si el valor de Permiso del grupo secundario del GO principal es Heredar o reemplazar.

Siguiendo con el ejemplo anterior, si desea modificar los ajustes de Marca del GO Almacén *únicamente*, puede cambiar el Ajuste actual de cada GO secundario de Almacén a Reemplazar, siempre y cuando el valor de Permiso del grupo secundario para Almacén sea Heredar o reemplazar (predeterminado). A continuación, puede configurar los ajustes Personalización de marca de los elementos secundarios del almacén, de forma distinta o igual al almacén.

Cómo cambiar los ajustes de permisos

No puede cambiar el Ajuste actual de un elemento secundario si el valor de Permiso del grupo secundario de su elemento principal no lo permite. Por ejemplo, si el ajuste de Permiso del grupo secundario de MomandDadOG es Reemplazar solamente, no puede cambiar el Ajuste actual de JuniorOG a Heredar. En resumen, el ajuste Permiso del grupo secundario del GO principal tiene prioridad sobre el Ajuste actual del GO secundario.

Al cambiar el Ajuste actual de un elemento secundario de Reemplazar a Heredar, el cambio del ajuste Permiso del grupo secundario de su principal a Heredar solamente bloquea el ajuste Permiso del grupo secundario del GO secundario. No puede cambiar la configuración de los permisos secundarios en esta situación. Este comportamiento no se aplica si el ajuste de GO secundario nunca se reemplaza.

La solución a este comportamiento es que cambie la configuración de Permiso secundario del GO principal de nuevo a Heredar o reemplazar, con lo que se desbloquea el ajuste Permiso secundario del GO secundario.

La mejor estrategia es planificar por adelantado y configurar los ajustes de herencia y reemplazo a los niveles de GO que tengan sentido según la estructura de jerarquía que desee.

Grupos inteligentes

Los grupos inteligentes son grupos personalizables de Workspace ONE UEM basado en AirWatch

que determinan qué plataformas, dispositivos y usuarios recibirán una aplicación, libro, directiva de conformidad, perfil de dispositivo o provisión.

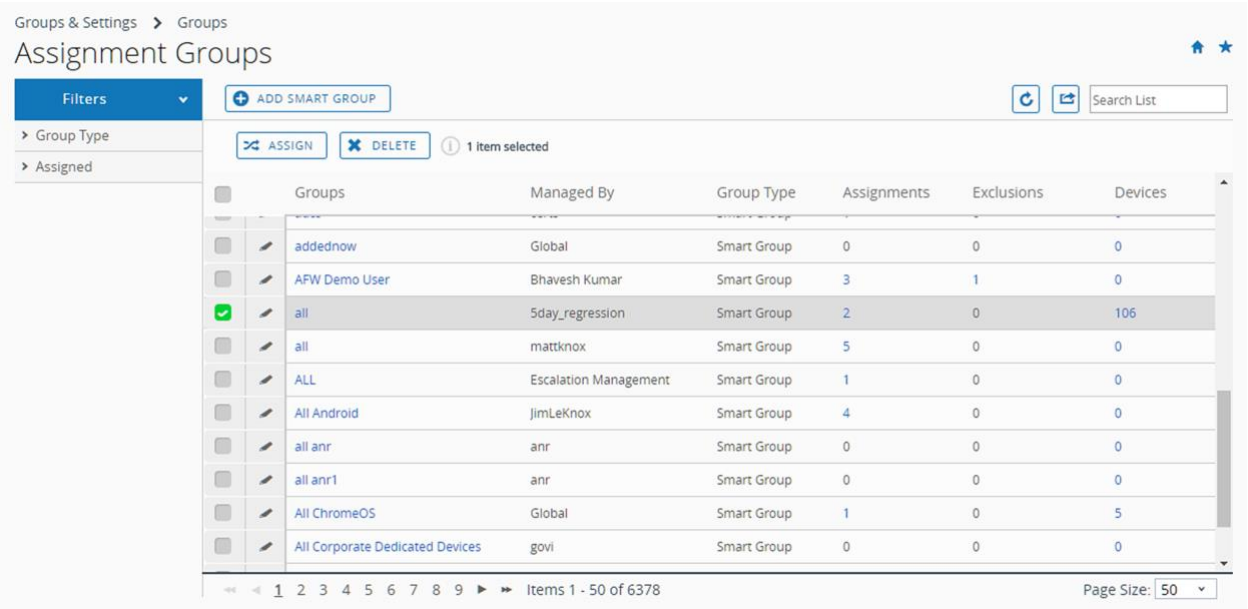
Cuando crea grupos organizativos, suele basarlos en la estructura corporativa interna: ubicación geográfica, unidad de negocio y departamento. Por ejemplo, "Ventas corporativas", "Asia" con los grupos inteligentes, puede distribuir contenido y ajustes por plataforma del dispositivo, modelo, sistema operativo, etiqueta de dispositivo o grupo de usuarios. Puede enviar contenido a usuarios individuales de todos los grupos organizativos.

Puede crear grupos inteligentes cuando cargue contenido y defina ajustes. Sin embargo, puede crearlos en cualquier momento y asignarlos más adelante.

La ventaja principal de los grupos inteligentes es que se pueden reutilizar. Crear una nueva asignación cada vez que agrega contenido o define un perfil o política puede ser intuitivo. Sin embargo, si en su lugar define a los usuarios asignados a los grupos inteligentes solo una vez, puede incluir esos grupos inteligentes en su definición de contenido.

Vista de lista de grupos inteligentes

Vea la lista completa de grupos inteligentes en Grupos y ajustes > Grupos > Grupos de asignación. Los administradores verán solo los grupos que puedan administrar según los permisos que tengan configurados.



Para ver información detallada, seleccione los vínculos de las columnas Grupos, Asignaciones, Exclusiones y Dispositivos.

- Al seleccionar los enlaces de las columnas Asignaciones o Exclusiones, aparece la pantalla Cómo ver las asignaciones de los grupos inteligentes.
- Al seleccionar un enlace en la columna Dispositivos, se mostrará la ruta Dispositivos > Vista de lista con los dispositivos incluidos en el grupo inteligente únicamente.
- Puede aplicar un Filtro a los grupos según el Tipo de grupo (Inteligente, Organizativo, Usuarios o Todo) o según el estado Asignado. El estado asignado muestra si el grupo está asignado, excluido, ambos o ninguno.
- Puede Asignar un grupo inteligente directamente desde la lista.

Migración de grupos inteligentes

Para prepararse para las nuevas reglas de tenant relacionadas con los grupos inteligentes, debe migrar todos los grupos inteligentes afectados en su entorno. La nueva regla establece que los grupos inteligentes solo se pueden administrar desde grupos organizativos de tipo "cliente" o que debe existir un GO de tipo cliente por encima del grupo inteligente en el mismo árbol. Por lo tanto, si su entorno tiene grupos inteligentes en el grupo organizativo global o en cualquier otro grupo organizativo (GO) que no tenga un GO de tipo "cliente" por encima, deberá migrar dichos grupos inteligentes.

Si bien el proceso de migración se basa completamente en el cliente, este proceso de migración no es opcional. Si tiene grupos inteligentes en GO que no son de tipo cliente o un grupo inteligente en una posición que no tenga ningún GO de tipo cliente por encima, debe realizar el proceso de migración.

Es importante tener en cuenta que el objeto que se va a migrar es el grupo inteligente en sí, no los dispositivos a los que está asignado. Solo se migra el grupo inteligente. Los dispositivos individuales conservan el mismo GO "administrado por" que tenían antes de la migración.

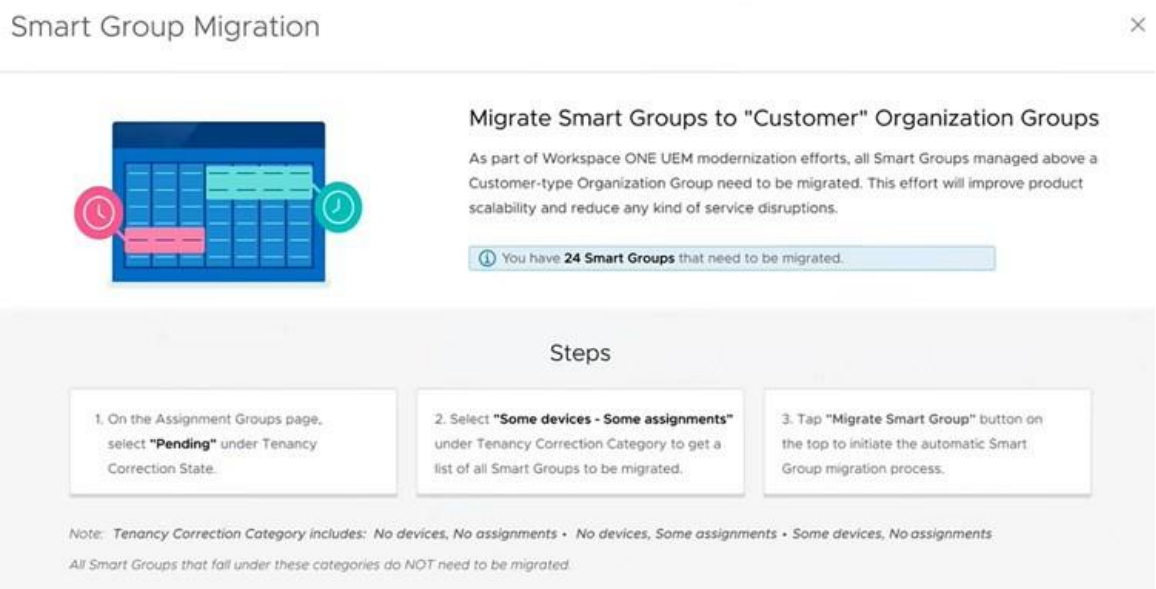
Cómo migrar los grupos inteligentes

Realice los siguientes pasos para migrar los grupos inteligentes. Este es un procedimiento único.

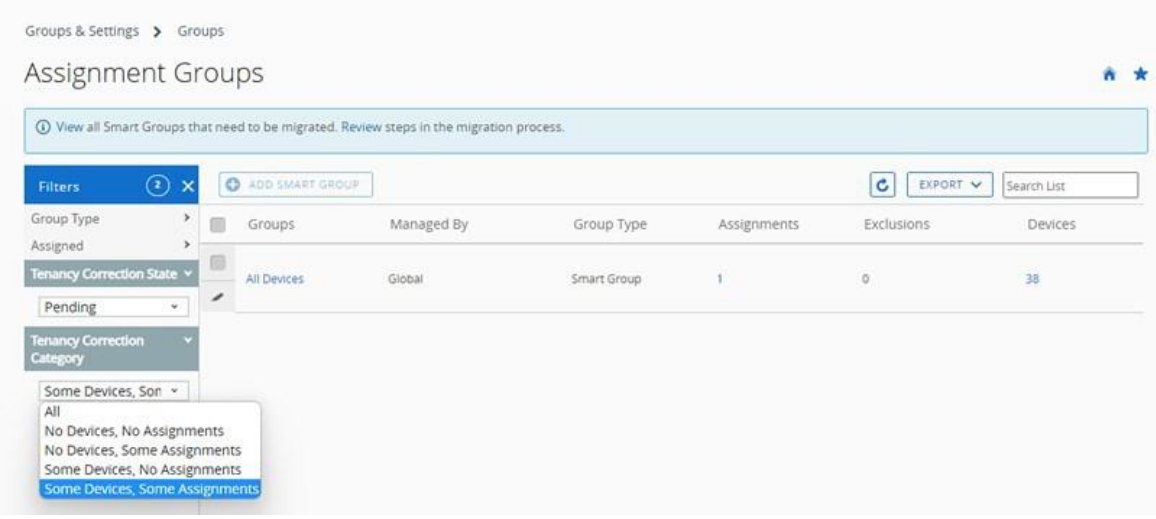
1. Vaya a Dispositivos > Vista de lista. Si ve este banner, seleccione Más información para continuar con la migración.

   Al seleccionar "Más información", verá la pantalla de Migración de grupos inteligentes.

2. Cierre la pantalla Migración de grupos inteligentes. Se muestra la página Grupos de asignación.



3. En Categoría de corrección de tenants, seleccione "Algunos dispositivos, algunas asignaciones".

   Solo se deben migrar los grupos inteligentes que tienen dispositivos y asignaciones.

   No es necesario migrar los grupos inteligentes que no tienen dispositivos O asignaciones. Los grupos inteligentes de este tipo migrados no tienen ningún impacto en las asignaciones de recursos y deben eliminarse. Para eliminar estos grupos inteligentes migrados, seleccione cada grupo inteligente de esta categoría y, a continuación, seleccione el botón Eliminar.

4. Seleccione el grupo inteligente que desea migrar haciendo clic en la casilla de verificación a la izquierda de la lista.

5. Seleccione el botón Migrar grupo inteligente. Se muestra una ventana emergente de confirmación Migrar grupo inteligente, que muestra cuántos grupos nuevos se deben crear para poder migrar el grupo inteligente por completo.

   Solo puede migrar un grupo inteligente a la vez.

6. Seleccione Continuar para proceder. El proceso de migración se ejecuta. Si se produce un error durante la migración, la confirmación muestra el error y proporciona la opción Reintentar. De lo contrario, la confirmación muestra los resultados de una migración correcta y que el grupo inteligente original está marcado para su eliminación en 24 horas.

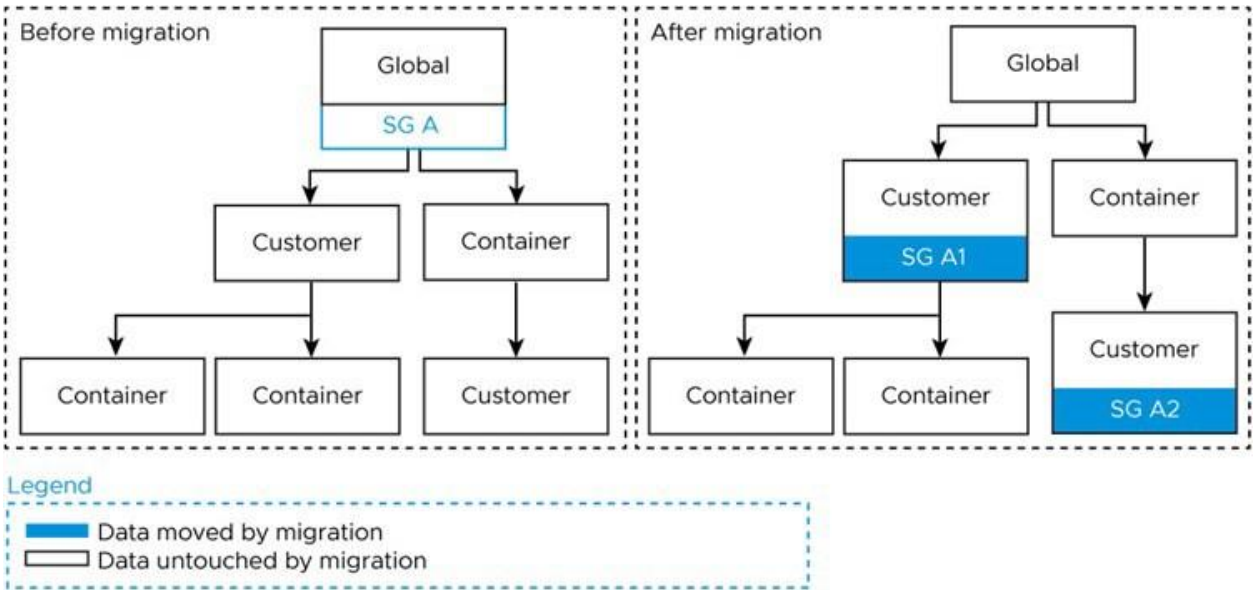
7. Seleccione el botón Hecho para cerrar la confirmación.

8. Repita los pasos del 4 al 7 hasta que se migren todos los grupos inteligentes pendientes que tienen dispositivos y asignaciones.

Revise los siguientes escenarios para ver cómo el proceso de migración repercute exactamente sobre los grupos inteligentes afectados.

Grupos inteligentes en el GO global

Si tiene grupos inteligentes en el GO global, el proceso de migración tendrá en cuenta cada dispositivo al que está asignado el grupo inteligente. A continuación, busca el GO secundario de tipo cliente más cercano al global (que al mismo tiempo es un GO principal situado por encima de estos dispositivos), crea un grupo inteligente en ese GO y convierte los dispositivos en parte del nuevo grupo inteligente. El grupo inteligente original se marca para su eliminación y se eliminará automáticamente en 24 horas.

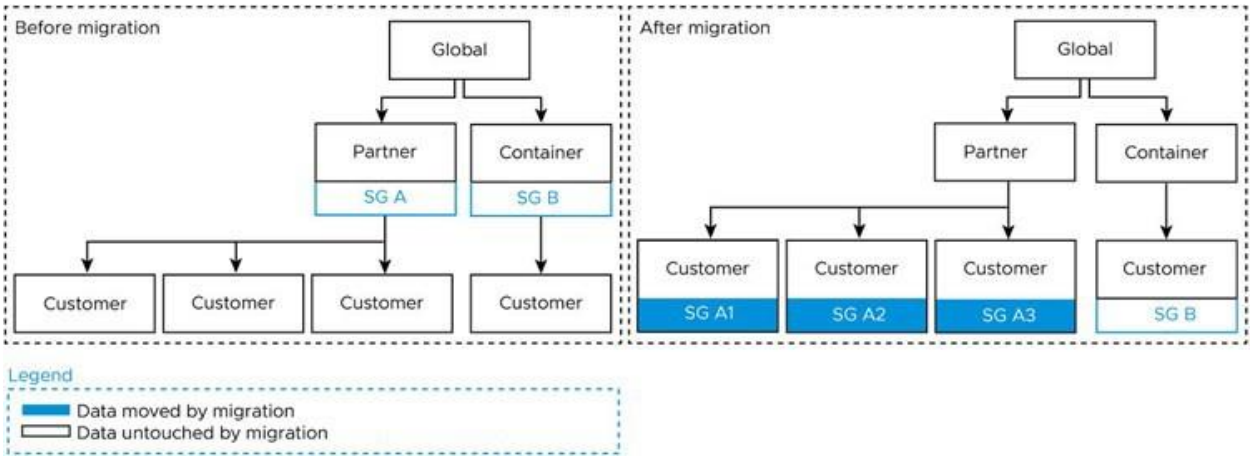


Para todos los dispositivos a los que esté asignado el grupo inteligente que estén administrados por un GO en otra rama de árbol, se creará un segundo grupo inteligente administrado por el GO de tipo de cliente superior más cercano al global, pero que esté situado por encima de estos dispositivos restantes.

Este proceso se repite tantas veces y crea tantos grupos inteligentes como sea necesario para garantizar que cada dispositivo del grupo inteligente original esté representado y conserve las mismas asignaciones de contenido que antes de la migración. Esto puede implicar la división del grupo inteligente original en una doce grupos o más con el fin de garantizar 1) que el mismo contenido se entregue a los dispositivos y 2) que los grupos inteligentes estén dentro o bajo grupos organizativos de tipo "cliente".

Grupos inteligentes en el GO de tipo socio

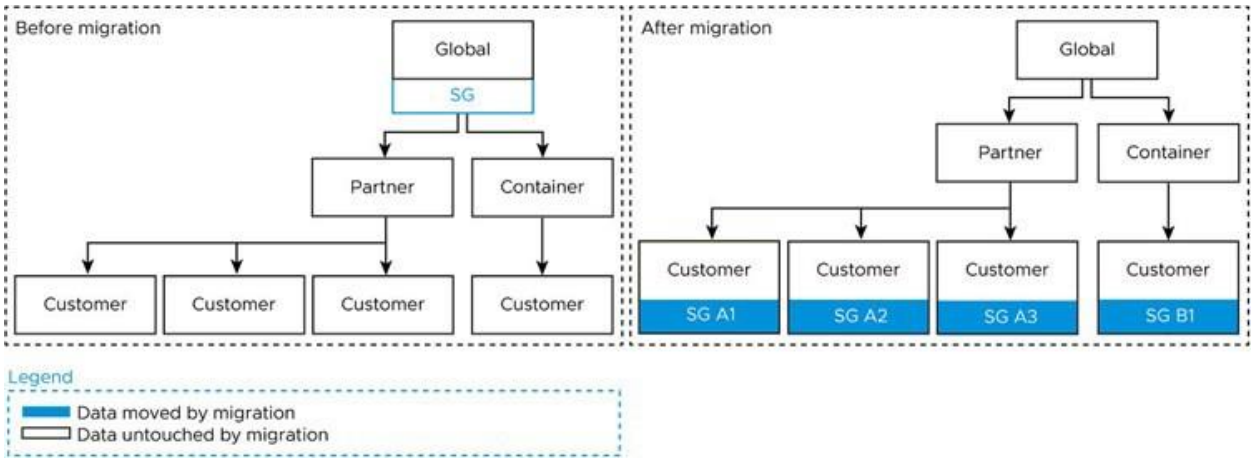
En este escenario, los grupos inteligentes de GO de tipo socio se dividen de forma similar entre varios GO de tipo cliente siguiendo la misma lógica que antes. Solo se crea un nuevo grupo inteligente cuando el GO situado por encima de los dispositivos a los que el grupo inteligente está asignado es de tipo cliente. Si uno o más dispositivos que forman parte del grupo inteligente se encuentran en otra rama de árbol, se creará un grupo inteligente y se situará en el GO de cliente por encima de esos dispositivos. El grupo inteligente original se marca para su eliminación y se eliminará automáticamente en 24 horas.



Tenga en cuenta que en este escenario, "SG B", que antes de la migración se administraba mediante un GO de contenedor con un único GO de cliente secundario, se mueve al GO de cliente secundario después de la migración, pero sus datos permanecen intactos. La migración no modifica estos datos porque los dispositivos y las asignaciones de SG B son idénticos antes y después de la migración, ya que solo había un elemento secundario de cliente en su posición original.

Grupos inteligentes en el GO global con un GO de tipo socio

En este escenario, un único grupo inteligente en el GO global se divide en varios árboles porque un GO de socio y un GO de contenedor se encuentran entre el GO global y otro GO de cliente. El grupo inteligente original se marca para su eliminación y se eliminará automáticamente en 24 horas.



Cómo anular la asignación de un grupo inteligente

Puede anular la asignación de un grupo inteligente a una aplicación, libro, política, perfil o producto. Esta acción elimina el contenido asociado de todos los dispositivos pertenecientes al grupo inteligente.

1. Tiene la opción de anular la asignación de los grupos inteligentes de aplicaciones, libros, políticas de conformidad, perfiles de dispositivos o aprovisionamientos de productos. Siga las rutas de navegación mostradas.
    - Aplicaciones nativas: navegue a Recursos > Aplicaciones > Nativas y seleccione la pestaña Internas, Públicas o Compradas.
    - Libros: navegue a Recursos > Libros > Vista de lista y seleccione la pestaña Internos, Públicos o Comprados.
    - Política de conformidad – Navegue a Dispositivos > Políticas de conformidad > Vista en lista.
    - Perfil de dispositivo: navegue a Recursos > Perfiles y líneas de base > Perfiles.
    - Aprovisionamiento de productos: navegue a Dispositivos > Aprovisionamiento > Vista de lista de productos.
    - Scripts: navegue a Recursos > Scripts.
    - Sensores: navegue a Recursos > Sensores.
    - Ventanas de tiempo: navegue a Recursos > Ventanas de tiempo.
2. Busque el contenido o ajuste en la lista y seleccione el icono Editar en el menú de

acciones. También puede seleccionar una casilla de verificación o un botón de opción a la izquierda de la lista.

3. Seleccione la pestaña Asignación o busque el cuadro de texto Grupos inteligentes.
4. Seleccione Eliminar (X) ubicada junto al grupo inteligente cuya asignación desea anular. Esta acción no elimina el grupo inteligente. Solo elimina la asignación del grupo de los ajustes guardados.
5. Siga los pasos necesarios para Guardar los cambios.

Cómo eliminar un grupo inteligente

Cuando ya no necesite un grupo inteligente, puede eliminarlo. Solo puede eliminar un grupo inteligente a la vez. Si selecciona más de un grupo inteligente, el botón Eliminar no estará disponible.

Antes de poder eliminar un grupo inteligente, no se podrá asignar a ningún producto del dispositivo. Si está seguro de que el grupo inteligente que desea eliminar está sin asignar, deberá llevar a cabo los siguientes pasos.

1. Acceda a Grupos y ajustes > Grupos > Grupos de asignación y busque el grupo inteligente que desea eliminar de la lista.
2. Seleccione la casilla de verificación situada a la izquierda del grupo inteligente que desea eliminar.
3. Seleccione Eliminar en el menú acciones que se muestra.

Resultados: El grupo inteligente sin asignar se eliminó.

Cómo editar un grupo inteligente

Puede editar un grupo inteligente establecido. Cualquier modificación que se aplique a un grupo inteligente afectará a todas las políticas y perfiles a los que este se encuentre asignado.

A continuación se muestra un ejemplo típico de la necesidad de editar un grupo inteligente. Imagine que se asigna un grupo inteligente para ejecutivos a una política de conformidad, un perfil de dispositivo y dos aplicaciones internas. Si desea excluir a algunos de los ejecutivos de uno o más de los elementos de contenido asignado, solo tiene que editar el grupo inteligente especificando las Exclusiones. Esta acción evita que tanto las dos aplicaciones internas como la directiva de conformidad y el perfil de dispositivo se instalen en los dispositivos de los ejecutivos excluidos.

1. Acceda a Grupos y ajustes > Grupos > Grupos de asignación.
2. Seleccione el icono Editar (), situado a la izquierda del grupo inteligente que desea editar. También puede seleccionar el nombre del grupo inteligente en la columna Grupo. Se mostrará la página Editar grupo inteligente con los ajustes existentes.
3. En la página Editar grupo inteligente, cambie los Criterios o los Dispositivos y usuarios (según el tipo con el que se haya guardado el grupo inteligente) y seleccione Siguiente.
4. En la página Ver asignaciones, puede ver qué perfiles, aplicaciones, libros, provisiones y políticas pueden agregarse o eliminarse del dispositivo como resultado

5. Seleccione Publicar para guardar las ediciones realizadas en el grupo inteligente. Todos los perfiles, aplicaciones, libros, provisiones y políticas ligados a este grupo inteligente cambiarán las asignaciones de dispositivos de acuerdo con esta modificación.

Resultados: El registrador de Eventos de la consola controla los cambios realizados en los grupos inteligentes, incluidos el autor de los cambios, los dispositivos agregados y los dispositivos eliminados.

Cómo examinar los eventos del grupo inteligente con el registrador de eventos de la consola

Puede realizar un seguimiento de los cambios realizados en los grupos inteligentes, además de cuándo y quién los realizó, mediante el registrador de Eventos de la consola. Esta información puede ser útil al tratar de solucionar problemas de los dispositivos.

1. Vaya a Monitor > Informes y análisis > Eventos > Eventos de la consola.
2. Seleccione Grupos inteligentes desde el filtro despegable Módulos, en la parte superior de la lista de Eventos de la consola.
3. De ser necesario, puede aplicar más filtros, incluyendo Intervalo de fechas, Gravedad y Categoría.
4. Cuando corresponda, seleccione el enlace de hipertexto en la columna Datos del evento, que contiene detalles adicionales que pueden ayudarle con las actividades de investigación.

Cómo crear un grupo inteligente

Antes de poder asignar un grupo inteligente a una aplicación, libro, política de conformidad, perfil de dispositivo o aprovisionamiento de producto, primero deberá crearlo.

Haga clic en este vínculo para ver un vídeo sobre cinco consejos de prácticas recomendadas para crear grupos inteligentes.

Cómo crear un grupo inteligente de forma inteligente (haga clic con el botón derecho y seleccione Abrir enlace en nueva pestaña)

- Simultáneamente, puede revisar la tarea complementaria prescriptiva Cómo crear un grupo inteligente de forma inteligente, tarea complementaria del vídeo mientras ve el vídeo. Esta tarea complementaria se puede encontrar en una sección posterior de este tema.
- Elija 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.
- Acceda a Grupos y ajustes > Grupos > Grupos de asignación y, luego, seleccione Agregar grupo inteligente.
- Introduzca el Nombre del grupo inteligente.
- También puede habilitar Vista previa del dispositivo para ver qué dispositivos se incluyen en el grupo inteligente que ha diseñado. Esta vista previa del dispositivo está desactivada de forma predeterminada para mejorar el rendimiento.
- Configure el tipo de grupo inteligente.

  Puede elegir:

- Criterios: la opción Criterios funciona mejor con los grupos grandes (más de 500 dispositivos) 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: la opción Dispositivos o usuarios funciona mejor para los grupos más pequeños (500 dispositivos 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 las opciones Criterios y Dispositivos o usuarios, se borra cualquier entrada y selección que haya realizado anteriormente.
- En el tipo Criterios, seleccione los parámetros calificados para agregar en el grupo inteligente. Si no se realiza ninguna selección en ningún ajuste, ese filtro no se aplicará a los criterios.

Ajustes	Descripción
Grupo organizativo	Esta opción de criterios filtra los dispositivos por grupo organizativo seleccionado. Puede seleccionar más de un GO. Debe seleccionar un GO de tipo Cliente o un GO secundario con un GO principal de tipo Cliente. No se permite asignar el grupo inteligente a un GO que no sea de tipo Cliente. Para obtener más información, consulte las secciones Cambiar grupos organizativos y Cómo crear grupos organizativos en Grupos organizativos
Grupo de usuarios	Esta opción de criterios filtra los dispositivos por grupos de usuarios seleccionados. Puede seleccionar más de un grupo de usuarios.
Propiedad	Esta opción de criterios filtra los dispositivos según el tipo de propiedad seleccionado.
Etiquetas	Esta opción de criterios filtra los dispositivos según las etiquetas de dispositivo. Puede seleccionar más de una etiqueta.
Plataforma y sistema operativo	Esta opción de criterios filtra los dispositivos según la plataforma y el SO seleccionado. Puede seleccionar varias combinaciones de cada uno. Aunque la plataforma es un criterio dentro de un grupo inteligente, la plataforma configurada en el perfil del dispositivo o la directiva de conformidad siempre prevalece sobre la plataforma del grupo inteligente. Por ejemplo, si crea un perfil de dispositivo iOS y lo asigna a un grupo inteligente, el perfil solo se asigna a dispositivos iOS, incluso si el grupo inteligente incluye dispositivos Android.
OEM y modelo	Esta opción de criterios se aplica solo a las selecciones de plataformas de escritorios Windows y Android realizadas en Plataforma y sistema operativo. Puede seleccionar uno o varios fabricantes de equipos originales y varios modelos por OEM. Los nuevos OEM y modelos de Android se añaden al menú desplegable cuando los dispositivos se inscriben o se sincronizan.
Modelo (heredado)	Esta opción de criterios filtra los dispositivos que no son de escritorios Windows ni Android por modelo. Los modelos individuales mostrados se basan en las selecciones realizadas en Plataforma y sistema operativo. Selecciónelos de la lista de modelos presentados para incluirlos en su grupo inteligente.

Ajustes	Descripción
Versión OEM empresarial	Esta opción de criterios filtra los dispositivos según la versión del fabricante del equipo original empresarial. Puede seleccionar más de un OEM empresarial. Una versión de OEM empresarial es una clasificación basada en software aplicable a modelos de dispositivos OEM. Por ejemplo, una versión de OEM empresarial puede ser asistencia adicional de software para dispositivos como Mobility Extensions (MX) de Motorola o Samsung SAFE. Una versión de OEM empresarial también puede ser un tipo específico del sistema operativo Android del OEM, como los ofrecidos por Honeywell, LG y Sony, entre otros.
Tipo de administración	Filtre los dispositivos según la forma en que se administre el dispositivo.
Categoría de inscripción	Filtre los dispositivos según la forma en que se inscriba el dispositivo.
Adiciones	Esta opción de criterios agrega dispositivos individuales y usuarios no incluidos en los criterios de filtrado. Puede seleccionar más de un dispositivo y más de un usuario.
Exclusiones	Esta opción de criterios excluye dispositivos individuales, usuarios individuales y grupos de usuarios incluidos en los criterios de filtrado. Puede excluir más de un dispositivo, más de un usuario y más de un grupo de usuarios.

1. Use el tipo Dispositivos o usuarios para asignar contenido y ajustes a casos especiales distintos de los criterios generales de movilidad empresarial. Introduzca el nombre descriptivo del dispositivo en Dispositivos y el nombre de usuario (nombre o apellido) en Usuarios. Debe Agregar al menos un dispositivo o usuario o no podrá guardar el grupo inteligente.

Ajustes	Descripción
Dispositivos	Agregue un dispositivo a este grupo inteligente especificando el nombre descriptivo del dispositivo. Puede agregar más de un dispositivo con este método.
Usuarios	Agregue usuarios a este grupo inteligente especificando el nombre de usuario, nombre o apellido. Puede agregar más de un usuario con este método.

Crear y asignar un grupo inteligente

Puede crear un grupo inteligente clasificado por plataforma, propiedad, grupo de usuarios, versión del sistema operativo, modelo, etiqueta de dispositivo, OEM empresarial y los dispositivos individuales incluso por su nombre descriptivo.

Por ejemplo, puede crear un grupo inteligente que contenga todos los dispositivos iPhone Touch propiedad de los empleados con una versión de iOS anterior a la 9.0.2. Agregue a este mismo grupo inteligente todos los dispositivos Android de la versión 2.0 de HTC con sistema operativo versión 4.1 o posterior. Fuera de este grupo, puede excluir los dispositivos del grupo de usuarios "A tiempo completo". A este grupo altamente personalizado de *dispositivos, puede asignar 10 perfiles de dispositivos, 10 aplicaciones o una política de conformidad.

*Debido a la naturaleza multiplataforma de este grupo de dispositivos personalizados, pueden darse

algunas restricciones. Por ejemplo, puede que desee asignar aplicaciones que no ofrezcan una versión de Android.

Puede asignar a un grupo inteligente de dos formas.

Cómo asignar un grupo inteligente al crear un producto de dispositivo

Puede asignar un grupo inteligente cuando agregue o cree una aplicación, libro, política de conformidad, perfil de dispositivo o provisión de producto.

1. Complete el menú desplegable Grupos asignados.
2. Seleccione un grupo inteligente del menú desplegable. Los grupos inteligentes disponibles se administran únicamente dentro del grupo organizativo (GO) al cual se está agregando el recurso o al grupo secundario situado debajo de tal GO.
3. Si ningún grupo inteligente coincide con los criterios de asignación deseados, seleccione la opción Crear un grupo inteligente. Puede asignar más de un grupo inteligente a cada aplicación, libro, política de conformidad, perfil de dispositivo o provisión de producto.
4. Seleccione Guardar para incluir la asignación.

Cómo asignar el grupo inteligente mientras lo administra

También puede asignar un grupo inteligente durante el propio proceso de administración de grupo inteligente.

1. Vea la lista completa de grupos inteligentes en Grupos y ajustes > Grupos > Grupos de asignación.
2. Seleccione los grupos inteligentes que desea asignar y seleccione Asignar. Aparecerá la página Asignar. Seleccione el enlace de los grupos en la parte superior de la página Asignar para ver la página Grupos. En esta página, verá los grupos organizativos que administran los grupos inteligentes. Seleccione el botón Cerrar para regresar a la página Asignar.
3. En la pantalla Asignar, utilice la barra de búsqueda para ver una lista de los productos elegibles y asígnelos a los grupos inteligentes seleccionados.
4. Seleccione Siguiente para que aparezca la página Ver la asignación de dispositivos y confirme el estado de la asignación.
5. Seleccione Guardar y publicar.

Cómo excluir grupos en los perfiles y políticas de conformidad

Puede excluir grupos de la asignación de perfiles de dispositivos y políticas de conformidad con la misma facilidad con la que asigna grupos a estos productos de dispositivos.

Antes de iniciar esta tarea, debe tener los grupos definidos. Como mínimo, debe poder hacer un grupo inteligente formado por los usuarios que desea excluir. Esta tarea le permite crear un nuevo grupo inteligente sobre la marcha, pero si prefiere excluir un grupo organizativo o un grupo de usuarios, consulte la sección titulada Cómo crear grupos organizativos en Grupos organizativos y

Grupos de usuarios respectivamente.

1. Cuando agregue un perfil o política de conformidad a un dispositivo, seleccione la opción Sí, situada junto al ajuste Exclusiones, para mostrar la opción Grupos excluidos.
2. En el ajuste Grupos excluidos, seleccione los grupos inteligentes que desee excluir de la asignación del perfil o política.
    - Puede introducir las primeras letras del nombre del grupo, y la función de búsqueda automática muestra todos los grupos cuyo nombre coincida con la cadena introducida.
    - Puede seleccionar uno o varios grupos organizativos, grupos de usuarios o grupos inteligentes.
    - Puede crear un nuevo grupo inteligente con el botón Crear grupo inteligente.
3. Seleccione Guardar y publicar (para perfiles de dispositivos) o Siguiente (para políticas de conformidad) y continúe el proceso para esas tareas.

    Si selecciona el mismo grupo para ambos ajustes, Grupos asignados y Grupos excluidos, no se podrá guardar el perfil o política.

Pasos siguientes: Si desea obtener una vista previa de los dispositivos afectados, seleccione Ver la asignación de dispositivos.

Cómo crear un grupo inteligente de forma inteligente, tarea complementaria del vídeo

Esta es una tarea complementaria del vídeo con el mismo nombre.

Cómo crear un grupo inteligente de forma inteligente (haga clic con el botón derecho y seleccione Abrir enlace en nueva pestaña)

En una pestaña de su navegador, puede reproducir el vídeo y pausarlo según sea necesario y, en otra, desplazarse por esta tarea, que incluye todos los detalles que no se mencionan en el vídeo.

1. Mover al grupo organizativo desde el que desea administrar el grupo inteligente

Los paquetes de contenido, como los perfiles de dispositivo, las directivas de conformidad, las aplicaciones, los libros, etc., se crean y administran desde un grupo organizativo (GO) específico, al igual que los dispositivos. Estos paquetes de contenido solo se pueden incluir en un grupo inteligente si crea el grupo inteligente desde el mismo GO desde el que se crearon los paquetes de contenido.

Utilice el selector de GO para pasar al GO secundario que contiene los paquetes de contenido (aplicaciones, libros, perfiles de dispositivo, directivas de conformidad, etc.) que desea incluir en el grupo inteligente. Puede identificar el GO administrado de cualquier paquete de contenido. Seleccione el paquete de contenido en su Vista de lista y revise la opción Administrado por seleccionada.

Por ejemplo, si desea asignar un perfil de dispositivo a su grupo inteligente, navegue a Recursos > Perfiles y líneas base > Perfiles, busque el nombre del perfil de dispositivo que desea asignar a su grupo inteligente en la lista y consulte la columna Administrado por para ese perfil. Este es el GO al que se mueve antes de crear el grupo inteligente.

Tenga en cuenta que sigue teniendo acceso al contenido creado en todos los GO principales por

encima del GO al que se ha movido. Esto significa que puede asignar contenido al grupo inteligente desde el GO en el que se encuentra y también desde todos los GO principales superiores.

2. Crear el grupo inteligente

Una vez que esté en el grupo organizativo que contiene los paquetes de contenido objetivo, continúe con la creación del grupo inteligente.

1. Acceda a Grupos y ajustes > Grupos > Grupos de asignación.
2. Seleccione el botón Agregar grupo inteligente. Se mostrará la pantalla Crear nuevo grupo inteligente.
3. Asigne un Nombre al grupo inteligente como si fuera un titular de periódico, un resumen de su contenido. Al asignar al grupo inteligente un nombre que describa los dispositivos, podrá asignar contenido al mismo grupo inteligente en cualquier momento en el futuro.
    - Tenga en cuenta que si asigna un nombre funcional al grupo inteligente en lugar de un nombre que represente los dispositivos, es más probable que cree grupos inteligentes adicionales en el futuro que representen el mismo conjunto de dispositivos para cada nueva función. Esto supone un gran desperdicio y una sobrecarga para Workspace ONE UEM Console.
        - Por ejemplo…
        - …si mantiene un solo grupo inteligente para "Personal no exento" que contiene 2500 dispositivos, puede simplemente asignar y anular la asignación de paquetes de contenido según sea necesario durante toda la vida útil de la flota. Esos 2500 dispositivos pueden recibir servicio desde el mismo grupo inteligente de forma indefinida.
        - Compare esta práctica optimizada con tener varios grupos inteligentes con nombres funcionales, cada uno con los mismos 2500 dispositivos, cada uno con un contenido diferente asignado. Workspace ONE UEM Console debe dedicar una cantidad excesiva de ciclos de CPU para realizar un seguimiento de todos esos grupos inteligentes y todo el contenido asignado a cada uno de ellos, lo que ralentiza todo lo demás.
        - El momento para crear un nuevo grupo inteligente es cuando identifica un subconjunto dentro de esos 2500 dispositivos que debe tratarse de manera diferente a los demás, por ejemplo, diferentes aplicaciones, diferentes directivas o diferentes perfiles. Pero incluso entonces, asigne un nombre al nuevo grupo inteligente que represente los dispositivos en sí, en lugar de asignarle un nombre que describa lo que planea hacer con ellos.
4. Seleccione el Tipo correcto de grupo inteligente. La mayoría de las veces, el tipo que desea es Criterios, que ofrece la mayor flexibilidad y personalización. En escenarios específicos, como el escenario de formación mencionado en el vídeo, tiene más sentido Dispositivos y usuarios.
5. Seleccione los mejores Criterios. Pase el puntero del mouse sobre la etiqueta de información de cada categoría de criterios y verá una ventana emergente que describe cómo la categoría filtra la flota de dispositivos.
6. Seleccione Adiciones y Exclusiones. Como se indica en el vídeo, estas dos categorías de criterios ofrecen la mayor libertad, incluso si el dispositivo agregado o excluido va en contra

de todas las demás categorías que definió anteriormente.

- Por ejemplo, si solo desea incluir dispositivos iPhone de Apple en el grupo inteligente, incluso especificando un número de versión de iOS, puede desafiar esta regla en la categoría Adiciones agregando usuarios de iPad e incluso dispositivos macOS, siempre que el contenido asignado sea compatible con iOS y macOS.
- Otro ejemplo: si crea un grupo inteligente que contiene los dispositivos para todos los administradores y les asigna todos los perfiles, directivas y aplicaciones solo para administradores, tiene la libertad de incluir un dispositivo utilizado por un administrador en prácticas, por ejemplo, con el objetivo de prepararlo para su nueva función. A la inversa, puede realizar una Exclusión de un dispositivo en el grupo de administradores, lo que hace que los perfiles, directivas y aplicaciones de administrador no estén disponibles para ese dispositivo. Las posibilidades son numerosas.

3. Asignar el grupo inteligente

Existen 2 escenarios diferentes para el momento en el que se asignan los grupos inteligentes.

1. Asigne el grupo inteligente directamente después de crearlo.
    1. Navegue a Grupos y ajustes > Grupos > Grupos de asignación
    2. Busque el grupo inteligente que acaba de crear y selecciónelo insertando una marca de verificación en la casilla a la izquierda de la lista.
    3. Seleccione el botón Asignar. Se mostrará la pantalla Asignar.
    4. Seleccione perfiles y directivas de la lista disponible, que se basa en el grupo organizativo en el que se encuentra actualmente. Los únicos perfiles de dispositivos y directivas de conformidad disponibles para seleccionar son 1) los creados en el grupo organizativo en el que se encuentra actualmente y 2) los creados en el mismo GO que el grupo inteligente que seleccionó.
2. Asigne el grupo inteligente directamente después de crear el paquete de contenido. Esto incluye no solo los perfiles de dispositivo y las directivas de conformidad, sino también las aplicaciones, los libros, los productos, los scripts, los sensores y las ventanas de tiempo.
    1. Desplácese hasta la vista de lista del tipo de contenido al que desea asignar el grupo inteligente.
        - Aplicaciones nativas: navegue a Recursos > Aplicaciones > Nativas y seleccione la pestaña Públicas o Internas.
        - Libros: navegue a Recursos > Libros > Vista de lista y seleccione la pestaña Internos, Públicos o Comprados.
        - Política de conformidad – Navegue a Dispositivos > Políticas de conformidad > Vista en lista.
        - Perfil de dispositivo: navegue a Recursos > Perfiles y líneas de base > Perfiles.
        - Aprovisionamiento de productos: navegue a Dispositivos > Aprovisionamiento > Vista de lista de productos.
        - Scripts: navegue a Recursos > Scripts.

- Sensores: navegue a Recursos > Sensores.
- Ventanas de tiempo: navegue a Recursos > Ventanas de tiempo.

2. Busque el contenido o ajuste en la lista y seleccione el icono Editar en el menú de acciones. También puede seleccionar una casilla de verificación o un botón de opción a la izquierda de la lista.
3. Seleccione el botón Asignar o la pestaña Asignación, según el diseño de la pantalla. Busque y haga clic en el cuadro de texto Grupos inteligentes, y seleccione el grupo inteligente en el menú desplegable que aparece.

Grupos de usuarios

Puede agrupar conjuntos de usuarios en grupos de usuarios que, al igual que los grupos organizativos, actúan como filtros para asignar perfiles y aplicaciones. Cuando configure el entorno en Workspace ONE UEM, alinee los grupos de usuarios con los grupos de seguridad y las funciones empresariales de su organización.

Puede asignar perfiles, políticas de conformidad, contenido y aplicaciones a los usuarios y a los dispositivos con grupos de usuarios. Puede agregar los grupos de su servicio de directorio a Workspace ONE UEM o crear grupos de usuarios completamente nuevos.

En vez de utilizar grupos de usuarios, también se pueden asignar los dispositivos de acuerdo con un intervalo preconfigurado de direcciones IP de red o atributos personalizados.

Vista de lista de los grupos de usuarios

La página Vista de lista de los grupos de usuarios ofrece herramientas útiles para el mantenimiento regular de los grupos de usuarios, como las funciones de vista, combinación y eliminación de grupos de usuarios, la adición de los usuarios que faltan y la sincronización de grupos de usuarios.

Puede utilizar la vista de lista de grupos de usuarios para crear listas de grupos de usuarios inmediatamente, según el criterio que juzgue más relevante. También puede agregar grupos de usuarios nuevos de forma individual o en masa.

Vaya a Cuentas > Grupos de usuarios > Vista de lista.

Acción	Descripción
Filtros	Para ver solo los grupos de usuarios deseados, utilice los siguientes filtros. * Tipo de grupo de usuarios * Estado de sincronización * Estado de combinación
Agregar	
Agregar grupo de usuarios.	Permite agregar un único grupo de usuarios basados en directorio o un grupo de usuarios personalizado.
Importar por lotes	Permite importar grupos de usuarios nuevos en masa a través de un archivo de valores separados por comas (CSV). Puede organizar varios grupos de usuarios a la vez introduciendo un nombre y una descripción únicos.

Acción	Descripción
Cómo ordenar y ajustar el tamaño de columnas	Las columnas de la Vista de lista que se pueden ordenar son Nombre de grupo, Última sincronización el, Usuarios y Estado de combinación. Las columnas cuyo tamaño se puede ajustar son Nombre de grupo y Última sincronización el.
Vista de detalles	Para ver información básica sobre el grupo de usuarios en la Vista de detalles, seleccione el enlace de la columna Nombre de grupo. La información incluye el nombre de grupo, el tipo de grupo, el tipo externo, el administrador y el número de usuarios. La Vista de detalles también incluye un vínculo a los ajustes de asignación de grupos en Todos los ajustes > Dispositivos y usuarios > General > Inscripción en la pestaña Agrupación.
Exportar ( )	Guarde un archivo XLSX o CSV (valores separados por comas) de toda la vista de lista no filtrada o filtrada. Ambos formatos de archivo se pueden ver y analizar con MS Excel.

La Vista de lista de los grupos de usuarios también presenta una casilla y el icono Editar a la izquierda del usuario. Si selecciona el icono Editar ( ), puede realizar cambios básicos en el grupo de usuarios. Para realizar acciones en masa en grupos de usuarios, marque una o varios de los grupos que muestran botones de acción para la lista.

Más acciones para grupos de usuarios

Puede seleccionar más de un grupo de usuarios mediante la selección de todas las casillas que desee. Al hacerlo, se modificarán los botones de acción y las acciones se aplicarán a varios grupos y a sus respectivos usuarios.

Acción	Descripción
Sincronizar	Permite copiar los usuarios del grupo de usuarios que se agregaron recientemente a la tabla temporal de forma manual antes de que Workspace ONE UEM y Workspace ONE Express realicen la sincronización automatizada programada de Active Directory. Aviso: El proceso de sincronización de atributos de usuarios continúa incluso aunque se detecte un usuario duplicado. Cuando se produce un error de sincronización de este tipo, se crea una entrada en el registro de eventos de la consola para fines de solución de problemas, denominada DuplicateUserSyncFailure. Para revisar esta y otras entradas del registro de eventos de Console, vaya a Monitor > Informes y análisis > Eventos > Eventos de Console.
Ver los usuarios	Muestra la pantalla Miembros del grupo de usuarios, que le permitirá revisar los nombres de usuario de todos los miembros del grupo de usuarios seleccionado.
Más acciones	
Ver y combinar	Permite ver, agregar o eliminar usuarios agregados recientemente a la tabla temporal del grupo de usuarios. Los usuarios del grupo de usuarios que aparecen en esta tabla esperan la sincronización automatizada del grupo de usuarios en Workspace ONE UEM y Workspace ONE Express.

Acción	Descripción
Agregar usuarios faltantes	Permite combinar la tabla temporal del grupo de usuarios con la tabla de Active Directory para agregar los nuevos usuarios al grupo de usuarios oficial.
Eliminar	Permite eliminar un grupo de usuarios.

Cómo agregar usuarios a grupos de usuarios

Puede agregar usuarios a grupos de usuarios según sea necesario. Si no desea esperar a que se realice la sincronización de Active Directory de los grupos de usuarios, que es un evento programado y automático, puede sincronizar manualmente los grupos de usuarios.

Sigas estos pasos cuando desee agregar un nuevo usuario a uno o varios grupos de usuarios.

1. Vaya a Cuentas > Usuarios > Vista de lista.
2. Seleccione uno o varios usuarios de la lista marcando la casilla de la izquierda.
3. Seleccione el botón Más acciones y, a continuación, seleccione Agregar a grupo de usuarios. Aparecerá la página Agregar los usuarios seleccionados al grupo de usuario personalizado.
4. Puede agregar usuarios a un Grupo de usuarios existente o crear un Grupo de usuarios nuevo.
5. Elija el Nombre de grupo.
6. Seleccione Guardar.
7. Vaya a Cuentas > Grupos de usuarios > Vista de lista.
    1. La sincronización de Active Directory (AD), que consiste en un proceso programado y automatizado, copia estos usuarios del grupo de usuarios pendientes a una tabla temporal. A continuación, estos usuarios se revisan, se agregan o se eliminan.
    2. Si no desea esperar a que se realice la sincronización automatizada de AD, puede llevarla a cabo de forma manual. Para iniciar una sincronización manual, seleccione el grupo de usuarios al que agregó usuarios y, a continuación, seleccione el botón Sincronizar.

       Aviso: El proceso de sincronización de atributos de usuarios continúa incluso aunque se detecte un usuario duplicado. Cuando se produce un error de sincronización de este tipo, se crea una entrada en el registro de eventos de la consola para fines de solución de problemas, denominada DuplicateUserSyncFailure. Para revisar esta y otras entradas del registro de eventos de Console, vaya a Monitor > Informes y análisis > Eventos > Eventos de Console.
8. También puede seleccionar Más > Ver y combinar para realizar tareas de mantenimiento como consultar, agregar y eliminar usuarios del grupo de usuarios pendientes.
9. Seleccione Más > Agregar usuarios faltantes para combinar la tabla temporal de usuarios del

grupo de usuarios pendientes con los usuarios del grupo de usuarios de Active Directory.

Cómo agregar grupos de usuarios sin la integración del directorio (Personalizado)

La creación de un grupo de usuarios fuera de la estructura existente en Active Directory permite crear grupos especializados en cualquier momento. Personalice grupos de usuarios según la implementación estableciendo acceso específicamente a las funciones y al contenido que puede convertirse en la opción de preferencia en función de la clase de grupo de usuarios que necesite.

Por ejemplo, puede crear un grupo de usuarios temporal para un proyecto específico que requiera aplicaciones, perfiles de dispositivos y políticas de conformidad especializados.

Para obtener más información sobre cómo agregar grupos de usuarios en masa, consulte la sección titulada Cómo importar grupos de usuarios por lotes en Función Importar por lotes.

Los grupos organizativos personalizados solo se pueden agregar un grupo organizativo en el ámbito del cliente.

1. Navegue a Cuentas > Grupos de usuarios > Vista en lista, seleccione Agregar y luego Agregar grupo de usuarios.
2. Cambie la opción Tipo de grupos de usuarios a Personalizado.
3. Introduzca el Nombre de grupo y la Descripción para identificar el grupo de usuarios en Workspace ONE UEM Console.
4. Confirme el grupo organizativo que administra el grupo de usuarios y seleccione Guardar.
5. A continuación, podrá agregar usuarios a este nuevo grupo de usuarios en Cuentas > Usuarios > Vista de lista.

Para agregar varios usuarios, marque las casillas situadas en el extremo izquierdo de cada nombre de usuario mostrado. A continuación, seleccione el botón Administración situado sobre los encabezados de columna y seleccione Agregar a grupo de usuarios.

Cómo agregar grupos de usuarios con integración del directorio

Una alternativa a los grupos de usuarios personalizados sin integración con Active Directory es a través de la integración de grupos de usuarios que aplica la estructura actual de Active Directory, lo que supone numerosos beneficios.

Al importar los grupos de usuarios del servicio de directorio existentes como grupos de usuarios de Workspace ONE UEM, podrá realizar los siguientes tipos de tareas:

- Administración de usuarios: consulte los grupos del servicio de directorio (tales como los grupos de seguridad o las listas de distribución) y alinee la administración de usuarios en Workspace ONE UEM con los sistemas organizativos existentes.
- Perfiles y políticas: asigne perfiles, aplicaciones y políticas mediante la implementación de Workspace ONE UEM en los grupos de usuarios.
- Actualizaciones integradas: permite actualizar automáticamente las asignaciones del grupo de usuarios según los cambios en la inscripción del grupo.

- Permisos de administración: establezca los permisos de administración para que solo los administradores aprobados puedan cambiar las asignaciones de políticas y perfiles para grupos de usuarios específicos.
- Inscripción: sirve para permitir que los usuarios se inscriban en AirWatch con sus credenciales existentes y asignarlos automáticamente al grupo organizativo adecuado.

El administrador debe designar un grupo organizativo existente como ubicación principal desde la cual puede administrar dispositivos y usuarios. Los servicios de directorio deben estar habilitados en este grupo organizativo raíz.

Puede agregar los grupos de su servicio de directorio a Workspace ONE UEM. Aunque la integración no crea cuentas de usuario automáticamente para cada una de las cuentas del servicio de directorio, garantiza que Workspace ONE UEM los reconozca como grupos de usuarios. Puede utilizar ese grupo para restringir la inscripción de usuarios.

Para obtener más información sobre cómo agregar grupos de usuarios de directorio en masa, consulte la sección titulada Cómo importar grupos de usuarios por lotes en Función Importar por lotes.

La creación de grupos de usuarios mediante la integración del directorio fomenta un enfoque alineado con la administración de dispositivos: la inscripción de dispositivos, las actualizaciones posteriores, el resumen administrativo y la administración de usuarios están todos en sintonía con su estructura de servicio de directorio existente.

Antes de comenzar: Asegúrese de que el Tipo de grupo de usuarios sea Directorio.

1. Acceda a Cuentas > Grupos de usuarios > Vista de lista, seleccione Agregar y, a continuación, Agregar grupo de usuarios.

Ajustes	Descripción
Tipo	Seleccione el tipo de Grupo de usuarios. * Directorio: cree un grupo de usuarios que esté alineado con su estructura actual de Active Directory. * Personalizado: cree un grupo de usuarios fuera de la estructura actual de Active Directory de su organización. Este grupo de usuarios otorga acceso a determinadas funciones y contenidos a usuarios básicos y de directorios para personalizar los grupos de usuarios según su implementación. Los grupos organizativos personalizados solo se pueden agregar un grupo organizativo en el ámbito del cliente.
Tipo externo	Seleccione el tipo externo de grupo que está agregando. * Grupo: se refiere a la clase de objeto de grupo en la que se basa su grupo de usuarios. Vaya a Grupos y ajustes > Todos los ajustes > Sistema > Integración empresarial > Servicios de directorio > Grupo para personalizar esta clase. * Unidad organizativa: se refiere a la clase del objeto de la unidad organizativa en la que se basa su grupo de usuarios. Vaya a Grupos y ajustes > Todos los ajustes > Sistema > Integración empresarial > Servicios de directorio > Grupo para personalizar esta clase. * Consulta personalizada: también puede crear un grupo de usuarios que contenga usuarios localizados mediante la ejecución de una consulta personalizada. Si selecciona este tipo externo, se reemplazará la función Texto de búsqueda y se mostrará la sección Consulta personalizada.

Ajustes	Descripción
Texto de búsqueda	Introduzca los criterios de búsqueda para identificar el nombre de un grupo de usuarios de su directorio y seleccione la opción Buscar para encontrarlo. Si el grupo de directorio contiene el texto de búsqueda, se mostrará una lista de nombres de grupos. Esta opción no está disponible si la opción Tipo externo está configurada en Consulta personalizada.
Nombre de directorio	Ajuste de solo lectura que muestra la dirección de su servidor de servicio de directorio.
Dominio y DN base del grupo	Esta información se rellena automáticamente según la información del servidor de servicios de directorio introducido en la página Servicios de directorio (Grupos y ajustes > Sistema > Integración empresarial > Servicios de directorio). Seleccione el signo más (+) de Capturar DN, situado junto al ajuste DN base del grupo, que mostrará una lista de elementos de nombre distintivo entre los que podrá elegir.
Clase de objetos personalizados	Identifica la clase de objeto bajo la cual se ejecuta la consulta. La clase de objeto predeterminada es "persona", pero puede personalizar esta clase de objeto para identificar a los usuarios con mayor éxito y precisión. Esta opción solo está disponible cuando se selecciona Consulta personalizada como Tipo externo.
Nombre de grupo	Seleccione un a Nombre de grupo de la lista de resultados Texto de búsqueda. Si selecciona un nombre de grupo, se modificará automáticamente el valor del ajuste Nombre distintivo. Esta opción solo está disponible después de haber realizado una búsqueda fructuosa con el ajuste Texto de búsqueda.
Nombre distintivo	Este ajuste de solo lectura muestra el nombre distintivo completo del grupo que está creando. Esta opción solo está disponible cuando se selecciona Grupo o Unidad organizativa como Tipo externo.
DN base personalizado	Identifica el nombre distinguido base que sirve como punto de partida de su consulta. El nombre distintivo base predeterminado es "AirWatch" y "sso". Sin embargo, si desea ejecutar la consulta con un punto de partida diferente, puede indicar un nombre distintivo base personalizado. Esta opción solo está disponible cuando se selecciona Consulta personalizada como Tipo externo.
Asignación de grupo organizativo	Este ajuste opcional le permite asignar el grupo de usuarios que está creando a un grupo organizativo (GO) específico. * Esta opción solo está disponible cuando se selecciona Grupo o Unidad organizativa como Tipo externo. * Debe seleccionar un GO de tipo Cliente. No se permite asignar el grupo de usuarios a un GO que no sea de tipo Cliente.

Ajustes	Descripción
Ajustes de grupo de usuarios	Seleccione entre Aplicar los ajustes predeterminados y Utilizar los ajustes personalizados para este grupo de usuarios. Consulte la fila Ajustes personalizados de esta tabla para obtener descripciones adicionales de los ajustes. Puede configurar esta opción en los ajustes de los permisos después de crear el grupo. Esta opción solo está disponible cuando se selecciona Grupo o Unidad organizativa como Tipo externo.
Consulta personalizada: consulta	Este ajuste muestra la consulta que está cargada actualmente y que se ejecuta mediante la selección del botón Probar la consulta y el botón Continuar. Aquí se reflejarán los cambios realizados en el ajuste Lógica personalizada o en el ajuste Clase de objetos personalizados.
Lógica personalizada	Agregue aquí su lógica de consulta personalizada, como el nombre de usuario o el nombre de administrador. Por ejemplo, "cn=jperez". El nombre distintivo puede ser corto o largo, según lo desee. El botón Probar la consulta permite verificar si la sintaxis de su consulta es correcta antes de seleccionar el botón Continuar.
Ajustes personalizados: permisos de administración	Tiene la opción de permitir o no permitir a todos los administradores que administren el grupo de usuarios que está creando.
Rol predeterminado	Seleccione el rol predeterminado para el grupo de usuarios del menú desplegable.
Política predeterminada de inscripción	Seleccione una política predeterminada de inscripción del menú desplegable.
Sincronización automática con el directorio	Esta opción habilita la sincronización del directorio, lo que detecta la membresía del usuario en el servidor de directorio y la almacenará en una tabla temporal. Los administradores aprobarán los cambios de la consola a menos que la opción Combinación automática esté seleccionada. Si desea evitar que los grupos de usuarios se sincronicen automáticamente durante una sincronización programada, deberá desactivar este ajuste.
Combinar todos los cambios automáticamente	Habilite esta opción para aplicar automáticamente los cambios de sincronización de la base de datos sin necesidad de contar con la aprobación administrativa.
Cantidad máxima de cambios permitidos	Utilice este ajuste para establecer un umbral para la cantidad de cambios de sincronización de grupo de usuarios automáticos que podrán realizarse antes de requerir aprobación. Los cambios que superen el umbral necesitarán aprobación administrativa y se enviará una notificación con este fin. Esta opción solo está disponible cuando está habilitada la opción Combinar todos los cambios automáticamente.

Ajustes	Descripción
Agregar miembros al grupo automática mente	Habilite este ajuste para agregar usuarios automáticamente al grupo de usuarios. Si desea evitar que los grupos de usuarios se sincronicen automáticamente durante una sincronización programada, deberá desactivar este ajuste.
Enviar correo electrónico al usuario si se agregan usuarios faltantes	Habilite esta opción para enviar un correo electrónico a los usuarios cuando se añadan usuarios faltantes al grupo de usuarios. Combine la tabla temporal del grupo de usuarios con la tabla de Active Directory para agregar a los usuarios faltantes.
Plantilla de mensaje	Esta opción solo está disponible cuando se ha habilitado la opción Enviar correo electrónico al usuario si se agregan usuarios faltantes. Seleccione una plantilla de mensaje para utilizarla cuando envíe notificaciones de correo electrónico durante el proceso de adición de usuarios faltantes al grupo de usuarios. Al agregar usuarios de Active Directory que son nuevos para Workspace ONE UEM Console, la disponibilidad de la plantilla de mensaje depende del modo de inscripción configurado en Grupos y ajustes > Todos los ajustes > Dispositivos y usuarios > General > Inscripción al seleccionar Autenticación y efectuar una selección en la opción Modo de inscripción de dispositivos. Si Inscripción abierta está seleccionada como el Modo de inscripción de dispositivos, estará disponible una plantilla de correo electrónico de activación del usuario en el menú desplegable Plantilla de mensaje. Este mensaje de correo electrónico permite inscribir al nuevo usuario de AD. Si Dispositivos registrados solamente está seleccionada como el Modo de inscripción de dispositivos, estará disponible una plantilla de correo electrónico de activación del dispositivo en el menú desplegable Plantilla de mensaje. Este mensaje de correo electrónico permite al nuevo usuario de AD inscribir sus dispositivos. Si Requerir token de registro está habilitada, el dispositivo se puede registrar con el token incluido en el mensaje.

Para obtener más información sobre el nombre distintivo, busque el artículo titulado "Object Naming" en el sitio TechNet de Microsoft: https://technet.microsoft.com/.

2. Seleccione Guardar.

Editar los permisos de los grupos de usuarios

El reajuste de los permisos de los grupos de usuarios permite reconsiderar quién puede editar ciertos grupos de la organización. Por ejemplo, si la organización tiene un grupo de usuarios para los ejecutivos de la empresa, no se recomienda que los administradores de niveles secundarios tengan permisos administrativos para ese grupo de usuarios.

Utilice la página Permisos para controlar quién puede administrar ciertos grupos de usuarios y quién puede asignar perfiles, políticas de conformidad y aplicaciones a los grupos de usuarios.

1. Vaya a Cuentas > Grupos de usuarios > Vista de lista.
2. Seleccione el icono Editar de una fila de grupo de usuario.

3. Seleccione la pestaña Permisos y luego seleccione Agregar.
4. Seleccione el Grupo organizativo en el que desea definir los permisos. Debe seleccionar un grupo organizativo (GO) que esté dentro de la jerarquía de GO raíz del grupo de usuarios. El GO que seleccione también debe ser de tipo Cliente. Para obtener más información, consulte la sección titulada Funciones y personalizaciones del tipo de grupo organizativo en Grupos organizativos.
5. Seleccione los Permisos que desea habilitar.
    - Administrar grupo (Editar/Eliminar): permite activar la capacidad de editar y eliminar grupos de usuarios.
    - Administrar usuarios dentro del grupo y permitir la inscripción: permite administrar usuarios del grupo de usuarios y autorizar la inscripción de dispositivos en el GO. Este ajuste solo puede habilitarse si también está activada la opción Administrar grupo (Editar/Eliminar). Si la opción Administrar grupo (Editar/Eliminar) está desactivada, este ajuste también se desactivará.
    - Utilizar grupo para asignación: permite utilizar el grupo para asignar políticas de seguridad y recursos empresariales a dispositivos. Este ajuste solo puede modificarse si está desactivada la opción Administrar grupo (Editar/Eliminar). Si la opción Administrar grupo (Editar/Eliminar) está habilitada, este ajuste se bloqueará y no podrá editarse.
        - Este ajuste se desactiva cuando el grupo de usuarios lo administra un grupo organizativo principal y usted desea asignar el grupo desde uno de sus grupos organizativos secundarios.
6. Seleccione el Ámbito para estos permisos, es decir, qué grupos de administradores pueden administrar o utilizar este grupo de usuarios. Solo una de las siguientes opciones puede estar activa.
    - Solo el administrador: los permisos solo afectan a los administradores del GO principal.
    - Todos los administradores en este grupo organizativo o más abajo en la jerarquía: los permisos afectan a los administradores del GO y a todos los administradores de los GO secundarios inferiores.

Acceso a los detalles de usuarios

Cuando los usuarios y los grupos de usuarios estén configurados, puede ver toda la información acerca de los detalles de usuarios, los dispositivos asociados y las interacciones.

Acceda a la información del usuario desde cualquier parte de Workspace ONE UEM console donde aparezca el nombre de usuario y en las siguientes páginas de la consola:

- Miembros del grupo de usuarios (Cuentas > Grupos de usuarios > Vista de detalles > Más > Ver los usuarios)
- Vista de lista de usuarios (Cuentas > Usuarios > Vista de lista)
- Vista de lista de administradores (Cuentas > Administradores > Vista de lista).

La página Detalles del usuario es una vista de una sola página.

- Todos los grupos de usuarios asociados.
- Todos los dispositivos asociados con el usuario a lo largo del tiempo y un enlace con todos los dispositivos inscritos.
- Todos los dispositivos retirados por el usuario en un entorno de dispositivos compartidos y un enlace al historial completo de las devoluciones/retiros.
- Todos los registros relacionados con el dispositivo o el usuario.
- Todos los Términos de uso asignados, aceptados y rechazados.

Cómo cifrar datos personales

Es posible cifrar información de identificación personal, como nombres, apellidos, direcciones de correo electrónico y números de teléfono.

1. Acceda a Grupos y ajustes > Todos los ajustes > Sistema > Seguridad > Seguridad de datos desde el grupo organizativo de nivel global o de cliente para el que desea configurar el cifrado.
2. Habilite el ajuste Cifrar la información del usuario y, a continuación, seleccione los ajustes de datos de usuario concretos para activar el cifrado. De este modo, se desactiva la funcionalidad desactivar buscar, clasificar y filtrar.
3. Haga clic en Guardar para cifrar los datos del usuario para que no resulten accesibles en la base de datos. Si realiza el cifrado, algunas de las funciones en Workspace ONE UEM Console, tales como la búsqueda, la ordenación y el filtrado, estarán limitadas.

Grupos administrativos

Los grupos administrativos permiten formar subgrupos de cuentas administrativas para asignar funciones y permisos adicionales a los que ya se incluyen en una cuenta administrativa de Workspace ONE UEM basado en AirWatch.

Los grupos administrativos pueden utilizarse para asignar roles y permisos que concedan acceso a la consola que esté específicamente relacionada con un proyecto especial. Puede agregar a los administradores del servicio de directorio ya existentes a grupos administrativos o crear grupos administrativos de cero utilizando consultas personalizadas.

Por ejemplo, si tiene una nueva directiva empresarial, es posible que tenga que asignar acceso administrativo especial a un grupo de facilitadores de formación. Es posible que tenga que crear un grupo administrativo, ejecutar una consulta personalizada para los facilitadores de formación y asignar un rol específico para el nuevo proyecto empresarial. Para obtener más información, consulte Cuentas administrativas.

Vista de lista de los grupos administrativos

La página Vista de lista de los grupos administrativos ofrece herramientas útiles para las tareas de mantenimiento de los grupos de usuarios comunes. En este proceso de mantenimiento se incluyen las tareas de agregar, ver, combinar y eliminar grupos de usuarios y usuarios que faltan.

Navegue a Cuentas > Administradores > Grupos administrativos para ver esta página.

Vaya a la página Editar grupo administrativo; para ello, seleccione el nombre del hipertexto en la columna Nombre de grupo de la vista de lista. Utilice esta página para cambiar el nombre del grupo administrativo. Asimismo, puede agregar y eliminar roles que se aplican a miembros del grupo. Para obtener más información, consulte la sección Funciones administrativas en Acceso basado en funciones.

Vaya a la lista Miembros del grupo de administradores; para ello, seleccione el número del enlace de hipertexto en la columna Administrador. Esta lista muestra los nombres de todos los administradores del grupo administrativo.

También puede descargar un archivo XLSX o CSV (valores separados por comas) de la Vista de lista de los grupos administrativos. A continuación, puede ver y analizar este archivo con MS Excel. Seleccione el botón Exportar y elija una ubicación de descarga.

Seleccione el botón de radio situado junto al nombre del grupo para acceder a las siguientes acciones y funciones de mantenimiento.

Acción	Descripción
Sincronizar	Permite copiar los usuarios del grupo administrativo que se han agregado recientemente a la tabla temporal de forma manual antes de que Workspace ONE UEM realice la sincronización automatizada programada de Active Directory.
Más acciones	
Ver y combinar	Permite ver, agregar o eliminar usuarios que se han agregado recientemente a la tabla temporal del grupo administrativo. Los administradores del grupo administrativo que aparecen en esta tabla se encuentran a la espera de una sincronización automatizada del grupo administrativo de Workspace ONE UEM.
Eliminar	Permite eliminar un grupo administrativo.
Inicio, Activo, Inactivo, Abajo	Puede editar la categoría de cada grupo administrativo según aparece en la lista. Resulta útil mover los grupos de esta forma cuando todos los grupos administrativos no se pueden mostrar en una sola página.
Agregar usuarios faltantes.	Permite combinar la tabla temporal del grupo administrativo con la tabla de Active Directory para agregar los nuevos administradores al grupo oficial.

Cómo agregar grupos administrativos

Mediante los siguientes pasos, puede agregar grupos administrativos en Workspace ONE UEM basado en AirWatch para asignar funciones y permisos adicionales a sus administradores para proyectos especiales.

1. Acceda a Cuentas > Administradores > Grupos administrativos y seleccione Agregar. Complete los ajustes correspondientes.

Ajustes	Descripción

Tipo externo	Seleccione el tipo externo del grupo administrativo que vaya a agregar. * Grupo: se refiere a la clase de objeto de grupo en la que se basa su grupo administrativo. Vaya a Grupos y ajustes > Todos los ajustes > Sistema > Integración empresarial > Servicios de directorio > Grupo para personalizar esta clase. * Unidad organizativa: se refiere a la clase del objeto de unidad organizativa en la que se basa su grupo administrativo. Vaya a Grupos y ajustes > Todos los ajustes > Sistema > Integración empresarial > Servicios de directorio > Grupo para personalizar esta clase de objeto. * Consulta personalizada: también puede crear un grupo administrativo que contenga administradores que se localizan al ejecutar una consulta personalizada. Si selecciona este tipo externo, se reemplazará la función Texto de búsqueda y se mostrará la sección Consulta personalizada.
Nombre de directorio	Ajuste de solo lectura que muestra la dirección de su servidor de servicio de directorio.
Dominio y DN base del grupo	Esta información se rellena automáticamente según la información del servidor de servicio de directorio que introdujo en la página Servicios de directorio (Cuentas > Grupos de usuarios > Ajustes > Servicios de directorio). Seleccione el signo más (+) de Capturar DN, situado junto al ajuste DN base del grupo, que mostrará una lista de Nombre de dominio base entre los que podrá elegir.
Texto de búsqueda	Introduzca los criterios de búsqueda para identificar el nombre de un grupo administrativo en su directorio y seleccione Buscar para encontrarlo. Si el grupo de directorio contiene el texto de búsqueda, se mostrará una lista de nombres de grupos. Además, puede aplicar roles predeterminados al grupo administrativo que esté creando. Después de realizar una búsqueda fructuosa, seleccione la pestaña Roles y, luego, seleccione el botón Agregar para añadir un nuevo rol. También puede editar un rol existente. Para ello, cambie la selección Grupo organizativo y Rol. Este ajuste solo está disponible cuando se selecciona Grupo o Unidad organizativa como Tipo externo.
Clase de objetos personalizados	Identifica la clase de objeto bajo la cual se ejecuta la consulta. La clase de objeto predeterminada es "persona", pero puede proporcionar una clase de objeto personalizada para identificar a los administradores con mayor precisión. Este ajuste solo está disponible cuando se selecciona Consulta personalizada como Tipo externo.
DN base personalizado	Identifica el nombre distinguido base que sirve como punto de partida de su consulta. La opción predeterminada es "airwatch" y "sso", pero se puede introducir un nombre distintivo base personalizado si se desea ejecutar la consulta desde un punto de partida diferente. Este ajuste solo está disponible cuando se selecciona Consulta personalizada como Tipo externo.
Nombre de grupo	Seleccione un a Nombre de grupo de la lista de resultados Texto de búsqueda. Si selecciona un nombre de grupo, se modificará automáticamente el valor del ajuste Nombre distintivo. Este ajuste solo está disponible después de haber realizado una búsqueda fructuosa con el ajuste Texto de búsqueda.

Ajustes	Descripción
Nombre distintivo	Ajuste de solo lectura que muestra el nombre distintivo completo del grupo administrativo que está creando. Este ajuste solo está disponible después de haber realizado una búsqueda fructuosa con el ajuste Texto de búsqueda.
Rango	Ajuste de solo lectura que muestra el rango del grupo administrativo una vez que se ha creado. Puede cambiar el rango del grupo administrativo en Grupos y ajustes > Grupos > Grupos administrativos y mover su posición relativa con el botón de acción Más ubicado a la derecha de la lista de grupos administrativos.
Sincronización automática	Esta opción habilita la sincronización del directorio, lo que detecta la membresía del usuario en el servidor de directorio y la almacenará en una tabla temporal. Un administrador aprobará todos los cambios de la consola a menos que la opción Combinación automática esté habilitada.
Combinación automática	Habilite esta opción para aplicar automáticamente los cambios de sincronización de la base de datos sin necesidad de contar con la aprobación administrativa.
Cantidad máxima de cambios permitidos	Utilice este ajuste para establecer un umbral para la cantidad de cambios de sincronización de grupos administrativos automáticos que podrán realizarse antes de requerir aprobación. Esta opción solo está disponible cuando está habilitada la opción Combinación automática.
Agregar miembros al grupo automáticamente	Habilite esta opción para agregar administradores automáticamente al grupo administrativo.
Zona horaria	Introduzca la zona horaria asociada al grupo administrativo. Este ajuste obligatorio actúa cuando se ejecuta la sincronización programada y automatizada de Active Directory.
Región	Seleccione los ajustes de región (idioma) asociados con el grupo administrativo. Este ajuste es obligatorio.
Página de destino inicial	Introduzca la página de destino inicial para los administradores del grupo administrativo. El ajuste predeterminado de este ajuste obligatorio es Tablero de dispositivos, pero puede cambiarlo a la página que desee.
Consulta personalizada	
Consulta	Este ajuste muestra la consulta que está cargada actualmente y que se ejecuta mediante la selección del botón Probar la consulta y el botón Continuar. Aquí se reflejarán los cambios realizados en la opción Lógica personalizada o en el ajuste Clase de objetos personalizados.
Lógica personalizada	Agregue aquí su lógica de consulta personalizada, como el nombre de administrador. Por ejemplo, "cn=jperez". El nombre distintivo puede ser corto o largo, según lo desee. El botón Probar la consulta permite verificar si la sintaxis de los resultados de su consulta es correcta antes de seleccionar el botón Continuar.

Para obtener más información sobre el nombre distintivo, busque el artículo titulado "Object Naming" en el sitio TechNet de Microsoft: https://technet.microsoft.com/.

2. Seleccione Guardar.

Cómo ver asignaciones

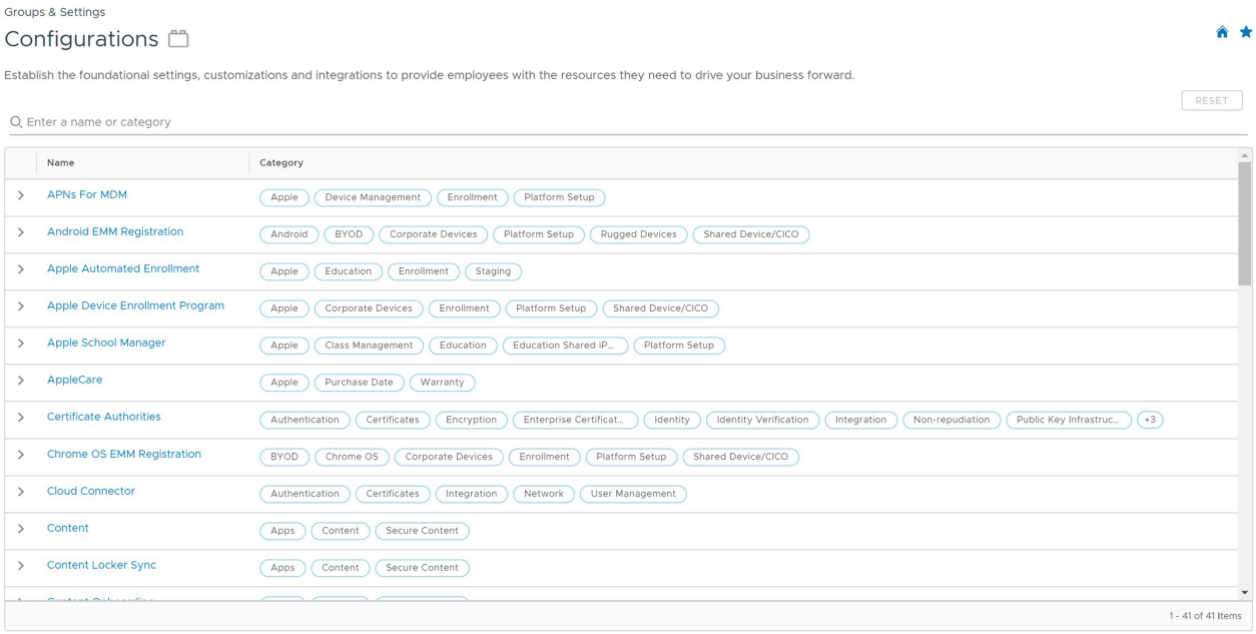
Para su comodidad, puede ver la vista previa de los perfiles del dispositivo, aplicaciones, libros, canales y directivas de conformidad incluidos en los grupos asignados de Workspace ONE UEM basado en AirWatch (y también excluidos de ellos), así como confirmarlos.

1. Acceda al listado de grupos en Grupos y ajustes > Grupos > Grupos de asignación y busque un grupo que se haya asignado por lo menos a una entidad.
2. En la columna Asignaciones, seleccione el número con el enlace de hipertexto para abrir la página Ver asignaciones. Esta página solo muestra las categorías que contienen Asignaciones o Exclusiones en el grupo.

Justo encima de la fila de encabezado de la pantalla Ver asignaciones, puede utilizar el botón Actualizar, el botón Exportar y el cuadro de texto Buscar en lista para localizar y confirmar que el perfil, la aplicación, el libro, el canal y la política de conformidad específicos se han asignado.

Configuraciones

Las configuraciones son una lista elaborada de páginas de configuración categorizadas que se pueden buscar y se organizan lógicamente. Puede identificar y acceder directamente a las páginas de configuración esenciales de Workspace ONE UEM basado en AirWatch y Workspace ONE Express. Para comenzar, vaya a Grupos y ajustes > Configuraciones.



Para inspeccionar cada una de las configuraciones, seleccione la flecha izquierda "mayor que" para expandir la fila y leer la descripción. Una vez expandida, también puede leer la documentación oficial de la configuración si selecciona el botón Más información.

Permite búsquedas

Para buscar configuraciones y categorías, introduzca contenido en la barra de búsqueda situada encima de la lista.

Clasificadas

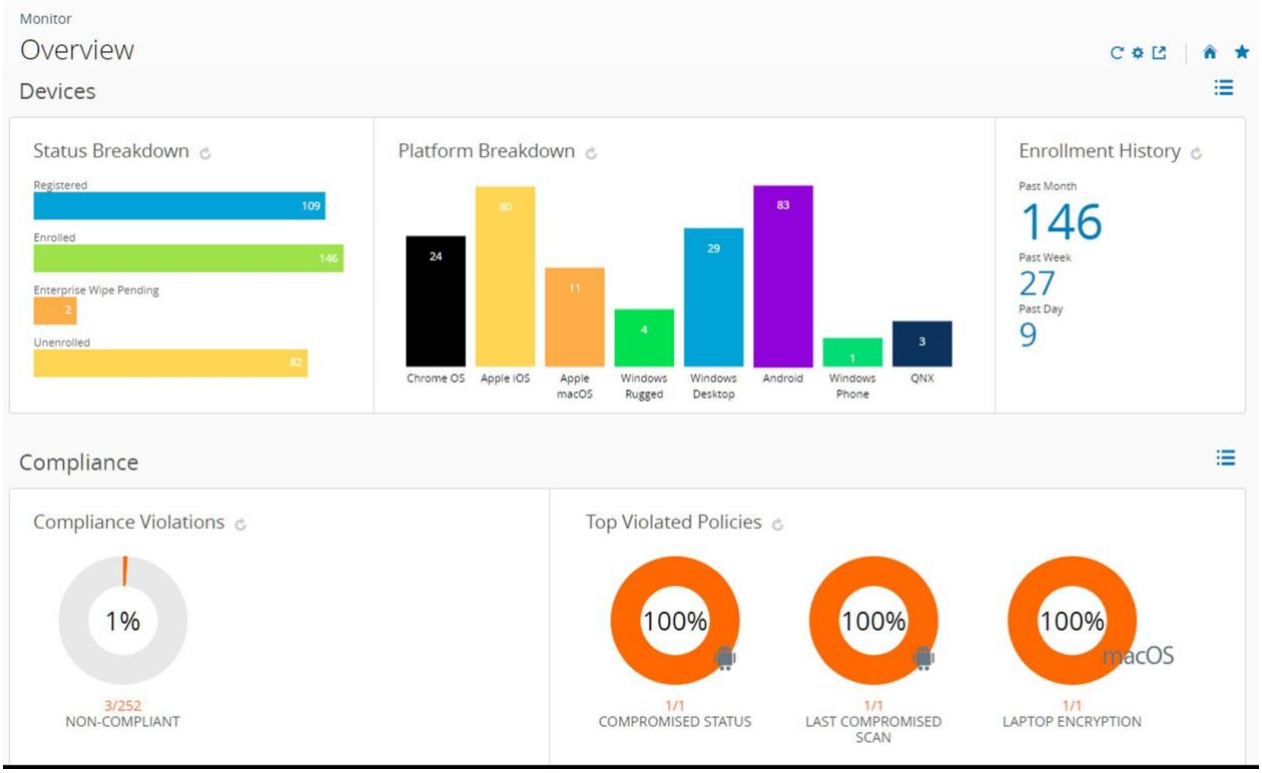
Todas las configuraciones se clasifican en función de los atributos y los casos de uso para que pueda localizar rápidamente las que más necesite. Hacer clic en las categorías equivale a aplicar un filtro, con lo que se eliminan las configuraciones de la vista que no formen parte de la categoría seleccionada. Para borrar las categorías seleccionadas y restablecer la vista, haga clic en la "x" que aparece junto al nombre de la categoría o seleccione el botón Restablecer encima de la barra de búsqueda.

Categorías portátiles

Puede compartir categorías de configuración con otros administradores que incluyan combinaciones de categorías. Por ejemplo, si selecciona Configuración de la plataforma, Apple e Inscripción, puede compartir esta combinación de categorías copiando la URL en la barra de direcciones del navegador.

Monitor de Console

El monitor de Console de Workspace ONE UEM es el portal central para obtener acceso rápido a información importante. Gracias a sus coloridos gráficos de barras y circulares, puede identificar rápidamente problemas importantes y actuar desde una única ubicación.



Si selecciona cualquier gráfico de barras o circular de la página, aparecerá Vista de lista de dispositivos. Esta vista de lista contiene todos los dispositivos específicos de la métrica seleccionada. A continuación, podrá realizar acciones como enviar un mensaje a dichos dispositivos.

Por ejemplo, seleccione el gráfico circular Estado del antivirus. En segundos, la Vista de lista de dispositivos mostrará una lista de los dispositivos cuya falta de software antivirus ha activado una infracción de política. Para seleccionar todos los dispositivos de esta lista, marque las casillas situadas más a la izquierda de cada dispositivo. También puede seleccionar la casilla "Seleccionar todo" debajo del botón Agregar dispositivo. La agrupación de botones de acción aparece encima de la lista. Seleccione el botón Enviar para enviar un mensaje a los usuarios de los dispositivos seleccionados. Puede seleccionar un correo electrónico, una notificación push o un mensaje de texto SMS.

La página Monitor > Información general proporciona gráficas de resumen y vistas detalladas.

- Dispositivos: permite ver la cantidad exacta de dispositivos.
    - Resumen del estado de todos los dispositivos registrados, inscritos, con una eliminación empresarial pendiente y los dispositivos con una inscripción anulada o

eliminación pendiente.

- Desglose de plataformas de los dispositivos inscritos en Workspace ONE UEM.
- Historial de la inscripción en el último día, la última semana o el último mes.

- Conformidad: permite ver qué dispositivos no cumplen con las políticas de conformidad.
  - Todas las políticas de conformidad que los dispositivos no están cumpliendo actualmente, como aquellas relacionadas con aplicaciones, ajustes de seguridad, geolocalización, entre otras.
  - Las políticas más infringidas, las cuales cubren todos los tipos de políticas de conformidad establecidas.
  - Aplicaciones en la lista de no permitidos, incluyendo aquellas instaladas en los dispositivos, organizadas por las instancias de infracción.
  - Los dispositivos que no tienen las aplicaciones que desea instalar y tener listas para los usuarios.
- Perfiles: permite ver qué perfiles han vencido.
  - La última versión del perfil, lo que incluye dispositivos con versiones anteriores de cada perfil.
- Aplicaciones: permite ver qué aplicaciones están asociadas con los dispositivos.
  - La última versión de la aplicación, lo que incluye dispositivos con versiones anteriores de cada aplicación.
  - Las aplicaciones más instaladas, organizadas por los dispositivos que tienen esa aplicación actualmente instalada.

  Para obtener más información, consulte Seguimiento y supervisión de la implementación de aplicaciones.
- Contenido: permite ver los dispositivos que tienen contenido vencido.
  - La última versión del contenido, que incluye cada archivo vencido clasificado por orden de instancia.
- Correo electrónico: permite ver los dispositivos que actualmente no pueden recibir correo electrónico.
  - Los dispositivos bloqueados que no pueden recibir correo electrónico, incluidos aquellos bloqueados de forma predeterminada, que están en la lista de no permitidos o cuya inscripción se ha anulado.
- Certificados: permite ver qué certificados están configurados para caducar.
  - Se muestran certificados que van a caducar dentro de un mes, de uno a tres meses, de tres a seis meses, de seis a 12 meses o más de 12 meses. Además, podrá ver los certificados que ya han caducado.

El conjunto de dispositivos que se muestra varía según el grupo organizativo actual, incluidos todos los dispositivos de los grupos secundarios. Podrá acceder a un grupo organizativo inferior y actualizar automáticamente los resultados de dispositivos mediante el menú desplegable del grupo organizativo.

Podrá alternar entre las vistas seleccionando los iconos Vista de lista () y Vista de diagrama (

). Seleccione cualquier métrica para abrir la Vista de lista de dispositivos para dicho conjunto específico de dispositivos. A continuación, podrá realizar acciones como enviar un mensaje a dichos dispositivos.

Personalice el Monitor seleccionando el icono Secciones disponibles (). Marque o desmarque las casillas que representan las secciones disponibles (Dispositivos, Conformidad, Perfiles, etc.) y seleccione Guardar para diseñar la Información general del Monitor.

Intelligence

Aviso: Debe tener una cuenta de Cloud Services para acceder a Workspace ONE Intelligence.

Los informes personalizados y los análisis avanzados de Workspace ONE Intelligence pueden proporcionarle información más detallada sobre su flota de dispositivos. Este tipo información incluye una mejor visibilidad sobre los problemas de rendimiento, herramientas de planificación muy efectivas y tiempos de implementación más rápidos.

Asegúrese de que se encuentra en un grupo organizativo de tipo cliente y, a continuación, vaya a Monitor > Intelligence, seleccione el botón Siguiente para ver cómo funciona Intelligence y participe para aprovechar el servicio.

Puede abandonar la creación de informes personalizada de Intelligence en cualquier momento.

Para obtener más información, consulte la guía Productos de VMware Workspace ONE Intelligence.

Tablero del panel administrativo

El Panel administrativo proporciona una descripción general de la información de licencias del módulo y los componentes de Workspace ONE™ UEM implementados divididos en dos secciones independientes: Productos activos y Componentes implementados.

Acceda al Panel administrativo a través de Monitor > Panel administrativo. Solo puede acceder al panel administrativo desde un grupo organizativo de tipo cliente.

La sección Productos activos identifica los productos activos y muestra información resumida de las licencias, incluidos el modelo de licencia y el tipo de licencia.

La sección Componentes implementados presenta un panel para cada componente habilitado en el grupo organizativo de cliente que muestra el estado de conexión de los siguientes componentes.

Monitor de aplicación y perfil

Realice un seguimiento de la implementación de aplicación o perfil en los dispositivos de los usuarios finales con el Monitor de aplicación y perfil. Esta herramienta proporciona información de un vistazo sobre el estado de las implementaciones.

1. Vaya a Monitor > Monitor de aplicación y perfil.
2. En el campo de búsqueda, introduzca el nombre de la aplicación o el perfil. Presione la tecla Intro del teclado para iniciar la búsqueda.
3. Seleccione la aplicación o el perfil en el menú desplegable y seleccione el botón Agregar.

Los datos de aplicación o perfil se muestran en una tarjeta. Solo puede tener cinco tarjetas agregadas a la vez.

El Monitor de aplicación y perfil muestra el estado actual de los dispositivos durante una implementación. El estado combina diferentes estados de instalación de aplicaciones y perfiles, como Listo, Pendiente o Incompleto.

Plantillas del sector para iOS

Una plantilla del sector es un conjunto de aplicaciones móviles y perfiles de dispositivos que puede enviar a los dispositivos para acelerar el proceso de implementación.

Puede seleccionar plantillas útiles para los sectores de la salud y ventas minoristas. Además, se pueden editar para ajustarlas a sus necesidades. Para obtener más información, consulte Plantillas del sector de Apple.

Informes y análisis

Workspace ONE UEM le permite acceder a información detallada sobre los dispositivos, los usuarios y las aplicaciones en el formulario de informe que puede analizar con Excel. Para obtener más información, consulte Informes y análisis.

Notificaciones de la consola

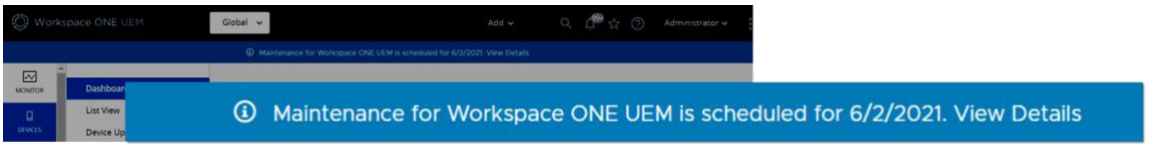
Las notificaciones son una herramienta de comunicación diseñada para que pueda mantenerse informado sobre eventos que pueden afectar al uso de Workspace ONE UEM. El botón Notificaciones está ubicado al lado del botón de lupa de búsqueda global.

Existen diferentes tipos de notificaciones.

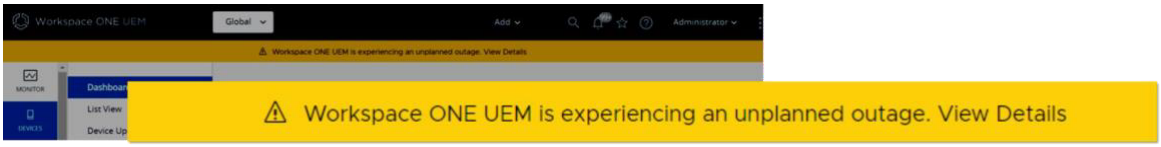
- Caducidad del certificado de las APN de la aplicación: se le avisará 30 días antes de que caduquen las APN para las aplicaciones, por lo que se trata de una alerta de prioridad crítica. Esta notificación ayuda a evitar los problemas que se producen cuando los certificados caducan y mantiene la funcionalidad de las aplicaciones en los dispositivos.
- Protección contra eliminación de aplicaciones: esta alerta de alta prioridad aparece cuando se cruza el umbral de eliminación de aplicaciones. Puede seleccionar el enlace Revisar la eliminación de aplicaciones en la ventana emergente Notificaciones.
- Alerta de almacenamiento de registros de aplicaciones del dispositivo: se trata de una alerta de prioridad alta que aparece cuando el registro de almacenamiento supera el 75 % de su capacidad. Purgue los registros o aumente el límite poniéndose en contacto con su representante de soporte. Esta alerta se puede descartar.
- Actualizaciones del repositorio de aplicaciones de empresa: esta notificación es una alerta informativa que se muestra cuando hay una actualización de la aplicación disponible del catálogo seleccionado de aplicaciones de empresa que se puede aplicar a los dispositivos de su flota.
- Exportación de la vista de lista: esta notificación aparece cuando la exportación de la vista de lista de dispositivos o usuarios solicitada se ha completado y está lista para examinarse. Esta notificación tiene nivel de prioridad informativo y se puede descartar.
- Notificaciones de mantenimiento y actualización: estas notificaciones de icono de timbre son alertas informativas que le permiten saber cuándo hay disponible una revisión de actualización o de mantenimiento. Incluye notificaciones para Workspace ONE UEM y Workspace ONE Assist.

  Las notificaciones de banner de Console son alertas informativas que le permiten saber cuándo está disponible una revisión de actualización o cuándo un evento de mantenimiento está planificado o no. Las notificaciones de banner de Console que se muestran son visibles para todos los administradores de SaaS e incluyen las siguientes subcategorías.

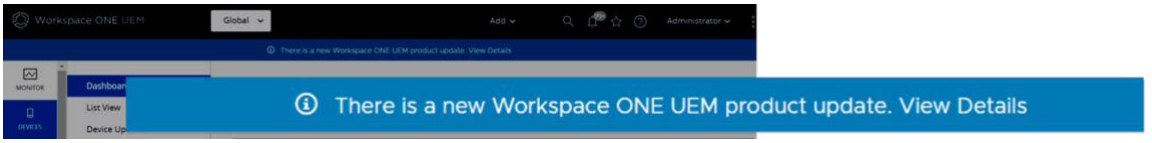
  - Mantenimiento



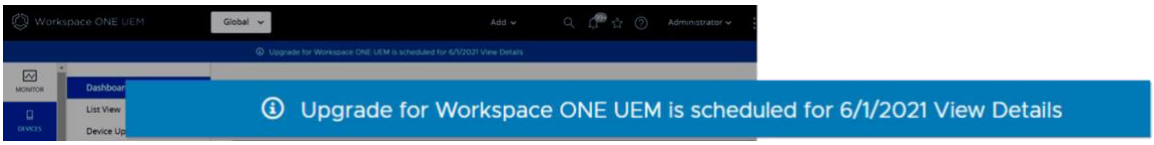
- Interrupciones



- Avisos de productos de SaaS



- Actualización



- Caducidad de las APN para MDM: recibirá una notificación 30 días antes de que caduquen los certificados de APN para MDM, lo que constituye una alerta de prioridad crítica. Cuando caduque el certificado de APN, la alerta de prioridad crítica se recudirá a una alerta de prioridad alta. Esta notificación ayuda a evitar los problemas que se producen cuando los certificados caducan y permite que los dispositivos mantengan la comunicación con Workspace ONE UEM.
- Actualización del servidor igual a igual requerida: recibirá una notificación cuando haya disponible una versión nueva del servidor igual a igual. Además, se le informará de que debe actualizar el servidor para evitar interrupciones del servicio.
- Caducidad del perfil de aprovisionamiento: se le avisará cuando caduque un perfil de aprovisionamiento que contenga aplicaciones, por lo que tendrá que volver a generar y actualizar el perfil aprovisionamiento. Esta notificación tiene nivel de prioridad crítico y no se puede descartar.
- Errores de token (DEP): recibirá una notificación cuando se produzca un error en la sincronización de DEP debido a un token DEP caducado.
- Caducidad del token (VPP y DEP): recibirá una notificación cuando un token vaya a caducar, de modo que pueda renovarlo y evitar la interrupción del servicio.
- Combinación de grupo de usuarios pendiente: esta notificación le permite saber que el proceso de combinación de grupo de usuarios está pendiente y necesita aprobación administrativa. Dicha notificación se produce en dos escenarios:
  - Tiene el ajuste Combinar todos los cambios automáticamente desactivado en el grupo de usuarios basado en el directorio, lo que significa que todos los cambios deben aprobarse.
  - Tiene el ajuste Combinar todos los cambios automáticamente habilitado y el número de cambios supera el umbral de Cantidad máxima de cambios permitidos. La parte

de la información del grupo de usuarios modificado más allá del máximo requiere la aprobación del administrador.

- Actualización automática de la aplicación VPP: alertas de alta prioridad que le indican que una aplicación instalada con el Programa de compra por volumen de Apple tiene una versión actualizada que puede instalar.

Cómo administrar las notificaciones de la consola

Cuando existan notificaciones activas que requieran de su atención, aparecerá un distintivo numérico en el icono de notificaciones que le indicará la cantidad de alertas activas. Seleccione el icono Notificaciones en forma de campana para ver la ventana emergente.

Puede administrar las notificaciones que reciba. Esta administración incluye la visualización de la lista de alertas activas, la renovación de sus APNs, el descarte de las alertas caducadas, la visualización de la lista de alertas descartadas y la configuración de los ajustes de notificaciones.

Cada alerta muestra el grupo organizativo en el cual se encuentran los APN de un certificado de MDM. La alerta también muestra la fecha de caducidad del certificado y un enlace a la opción Renueve sus APNs.

- Ver alertas activas: la vista predeterminada muestra la lista de alertas activas.
- Renueve sus APNs: muestra la pantalla Cambiar grupo organizativo. Esta pantalla aparece cuando el GO que administra el dispositivo con la fecha de caducidad de la licencia inminente es diferente al GO en el que se encuentra actualmente. Para renovar esta licencia de APNs y cambiar el GO automáticamente, seleccione Sí.

  Siga las instrucciones detalladas en la página de ajustes APNs para MDM para renovar la licencia y mantener el dispositivo en contacto con Workspace ONE UEM.
- Descartar alerta: seleccione el botón X para cerrar la alerta caducada y enviarla a la lista de alertas descartadas. No es posible cerrar notificaciones cuya prioridad sea crítica.
- Descartar todas: permite cerrar todas las alertas activas y enviarlas a la lista de alertas descartadas.
- Ver alertas descartadas: seleccione la pestaña Descartados en la parte superior de la ventana emergente Notificaciones para ver la lista de alertas descartadas.

Cómo configurar ajustes de notificaciones

Utilice los ajustes de Notificaciones en la página de Ajustes de cuentapara habilitar o desactivar alertas de fecha de caducidad de nombres de punto de acceso (APN), seleccione cómo recibir las alertas y cambie el correo electrónico al que las envía.

1. Seleccione la opción desplegable Cuenta, a la que se puede acceder desde prácticamente cualquier página de Workspace ONE UEM Console y, a continuación, seleccione Administrar ajustes de cuenta y la pestaña Notificaciones.

   También puede acceder a la página de ajustes de notificaciones mediante la selección del

icono del engranaje de la esquina inferior derecha de la pantalla emergente Notificaciones.

2. Seleccione el método de notificación cuando se produzca cada uno de los siguientes eventos.

Ajustes	Descripción
Fecha de caducidad de APNs	Esta notificación ayuda a evitar los problemas que se producen cuando los certificados caducan y permite que los dispositivos mantengan la comunicación con Workspace ONE UEM.
Exportación de la vista de lista	Puede activar una alerta para cuando finalice la exportación de una Vista de lista de usuarios o una Vista de lista de dispositivos.
Combinar grupos de usuarios	Puede activar una alerta para cuando la base de datos de Active Directory cambie la sincronización con Workspace ONE UEM y la opción Combinar todos los cambios automáticamente esté desactivada.
Actualización automática de PCV	Puede activar una alerta para cuando una aplicación instalada con el Programa de compra por volumen de Apple tenga una versión actualizada que puede instalar.
Caducidad del certificado de las APN de la aplicación	Esta notificación ayuda a evitar los problemas que se producen cuando los certificados caducan y mantiene la funcionalidad de las aplicaciones en los dispositivos.
Caducidad del perfil de aprovisionamiento	Recibirá un aviso cuando caduque un perfil de aprovisionamiento que contenga aplicaciones. Además, se le pedirá que regenere el perfil de aprovisionamiento y que lo actualice.
Token de dispositivo de Apple Business Manager a punto de caducar	Recibirá una notificación cuando un token DEP vaya a caducar, de modo que pueda renovarlo para evitar interrupciones.
Token de ubicación de Apple Business Manager a punto de caducar	Recibirá una notificación cuando un token de ubicación vaya a caducar, de modo que pueda renovarlo para evitar interrupciones.
Error de token de dispositivo de Apple Business Manager	Recibirá una notificación cuando se produzca un error en la sincronización de DEP debido a un token DEP caducado.
Uso de API	Recibirá un aviso cuando la cantidad de llamadas API (interfaz de programación de aplicaciones) alcance el 50 %, 75 %, 90 % y 100 % del límite API diario.
Actualizaciones del repositorio de aplicaciones empresariales	Se le notificará cuando una aplicación del catálogo de aplicaciones de empresa seleccionadas tenga una actualización que se pueda aplicar a los dispositivos.

3. En cada evento, seleccione entre Ninguno, Console, Correo electrónico y Console y correo electrónico, a menos que se especifique lo contrario.

   Las opciones Correo electrónico y Consola y correo electrónico requieren especificar al menos un correo electrónico en el cuadro de texto Enviar correos electrónicos a:. Puede introducir varias direcciones de correo electrónico separadas por comas.

4. Seleccione Guardar o Cancelar los cambios.

Registros de eventos

Los eventos son registros de acciones administrativas y de dispositivos que Workspace ONE UEM Console almacena en los registros. Exporte los registros de eventos como archivos CSV. También puede configurar Workspace ONE UEM Console para enviar los registros de eventos a las herramientas de información de seguridad y administración de eventos, o a los sistemas de inteligencia empresarial.

Los registros de eventos muestran los eventos del dispositivo y los eventos de Workspace ONE UEM Console. Los eventos del dispositivo muestran los comandos enviados desde la consola a los dispositivos, las respuestas de los dispositivos y las acciones del usuario del dispositivo. Los eventos de Console muestran las acciones realizadas desde Workspace ONE UEM Console, incluidas las sesiones de inicio de sesión, los intentos de inicio de sesión fallidos, las acciones administrativas, los cambios de ajustes del sistema y las preferencias de usuario.

Puede filtrar por rango de fechas, nivel de gravedad, categoría o módulo.

Los niveles de gravedad incluyen las siguientes descripciones.

- Crítico: indica un error en un sistema principal de Workspace ONE UEM Console.
- Error: indica un error en un sistema no principal de Workspace ONE UEM Console.
- Advertencia: indica un problema en el futuro si no se lleva a cabo la acción.
- Aviso: indica condiciones inusuales.
- Información: indica datos operativos normales.
- Depuración: indica información útil para la solución de problemas.

Aviso: Si la opción Fecha y hora seleccionada devuelve más de 10 000 eventos, aparecerá un mensaje de banner donde se le recomendará que seleccione un rango de fechas menor. Si prefiere un rango de fechas más amplio, ejecute un informe de eventos para cada grupo secundario en lugar de un único informe de eventos en un único GO principal.

Eventos de la consola

Los eventos de Console muestran acciones de MDM desde Workspace ONE UEM Console, que incluyen los siguientes ejemplos: Sesiones de inicio de sesión, intentos de inicio de sesión fallidos, acciones administrativas, cambios de ajustes del sistema y preferencias de usuario.

1. Vaya a Monitor > Informes y análisis > Eventos > Eventos de Console.
2. Aplique un filtro () a la lista de eventos de Console.

   Puede elegir:

- Fecha y hora (ver Nota anterior)
- Gravedad
- Categoría
- Módulo

3. Para ver los detalles de un evento específico de la consola, seleccione la opción Evento.

Eventos del dispositivo

Eventos del dispositivo proporciona una lista de varios tipos diferentes de eventos registrados por el sistema. Enumera los comandos de administración de dispositivos móviles (MDM) para dispositivos, respuestas de dispositivos y acciones de usuario del dispositivo. Puede filtrar el registro por intervalo de fechas, nivel de gravedad, categoría o módulo.

Los niveles de gravedad de los eventos del dispositivo incluyen las siguientes descripciones.

- Urgente: indica un error grave de MDM que requiere atención inmediata.
- Alerta: indica un error en un sistema básico de MDM que requiere atención.
- Crítico: indica un error en un sistema primario de MDM.
- Error: indica un error en un sistema no primario de MDM.
- Advertencia: indica un problema en el futuro si no se lleva a cabo la acción.
- Aviso: indica condiciones inusuales.
- Información: indica datos operativos normales.
- Depuración: indica información útil para la solución de problemas.

Examine los registros de eventos del dispositivo siguiendo estos pasos.

1. Vaya a Monitor > Informes y análisis > Eventos > Eventos del dispositivo.
2. Aplique un filtro () a la lista de eventos del dispositivo.

   Puede elegir:

   - Fecha y hora (ver Nota anterior)
   - Gravedad
   - Categoría
   - Módulo
3. Para ver los detalles de un evento específico del dispositivo, seleccione la opción Evento.
4. Para ver los detalles de un dispositivo específico, seleccione la opción Nombre común del dispositivo.
5. Puede Agregar dispositivo, Editar y Cambiar grupo organizativo seleccionando la opción Nombre de usuario de inscripción.

Cambiar ajustes de Syslog

Puede realizar cambios en los ajustes de Syslog. Acceda a la página de ajustes en Grupos y ajustes > Todos los ajustes > Sistema > Integración empresarial > Syslog.

También puede seleccionar el elemento de menú Syslog en Monitor > Informes y análisis > Eventos > Syslog.

Para obtener más información, consulte Integración de Syslog.

Cambiar ajustes de eventos

Puede cambiar el nivel de registro mínimo para los eventos. Vaya a Grupos y ajustes > Todos los ajustes > Administrador > Eventos y seleccione el botón Ajustes de eventos.

Establezca el nivel de registro mínimo para los eventos de Dispositivo y Console. Los eventos que satisfacen los niveles seleccionados y niveles superiores tanto para Dispositivo como para Console se capturan y guardan en la base de datos de Workspace ONE UEM, y se muestran en Workspace ONE UEM Console, en Monitor > Informes y análisis > Eventos > Eventos del dispositivo/Eventos de Console.

Freestyle Orchestrator

Realice un objetivo específico en relación con su dispositivo mediante la creación de un flujo de trabajo personalizado con Freestyle Orchestrator. Puede instalar recursos (tales como aplicaciones, scripts y perfiles) en función de las condiciones que defina.

Aviso: Freestyle Orchestrator solamente está disponible para dispositivos macOS y Windows.

Flujos de trabajo personalizados simplificados

Freestyle Orchestrator es una plataforma de orquestación de TI sin código que le permite arrastrar y soltar con la mayor la facilidad y que le proporciona la flexibilidad necesaria para crear flujos de trabajo con las funciones de recursos, condiciones y grupos.

Recursos como bloques de creación

Los recursos se pueden instalar en un dispositivo en forma de aplicación, un perfil de dispositivo o un script (Windows PowerShell o script de shell de macOS). Los recursos también pueden ser un mecanismo nativo para el dispositivo, como un sensor. Al crear un flujo de trabajo de Freestyle, se obtiene la capacidad para aprovechar todos estos recursos para realizar una tarea que se defina.

Acceda a recursos y configure aplicaciones, perfiles, scripts y sensores para utilizarlos dentro de un flujo de trabajo y aplicarlos a los dispositivos según criterios detallados.

Para obtener más información, consulte la Guía de Freestyle Orchestrator.

Otros sistemas empresariales para la integración

Aproveche la funcionalidad avanzada de MDM al integrar su entorno de Workspace ONE UEM basado en AirWatch con las infraestructuras empresariales existentes, tales como los servicios de directorio, la administración de correo electrónico con SMTP y los repositorios de administración de contenido.

- Retransmisión de correo electrónico (SMTP): permite proporcionar seguridad, visibilidad y control para el correo electrónico móvil.
- Servicios de directorio (LDAP/AD): permite aprovechar los grupos corporativos existentes para administrar los usuarios y los dispositivos.
- Servicios de certificados de Microsoft: permite utilizar la infraestructura de certificados de Microsoft existente para la implementación de Workspace ONE UEM.
- Protocolo de inscripción de certificados simple (SCEP PKI): permite configurar certificados para Wi-Fi, VPN, Microsoft EAS y más.
- Administración de correo electrónico con Exchange 2010 (PowerShell): permite conectarse a Workspace ONE UEM de forma segura para garantizar el cumplimiento de las políticas con servidores empresariales de correo electrónico.
- Servidor empresarial de BlackBerry (BES): permite integrar con BES para disfrutar de una administración optimizada de BlackBerry.
- Servicios de certificados de terceros: permite importar sistemas de administración de certificados para que se administren en la consola.
- Servicio web de Lotus Domino (HTTPS): permite acceder al contenido y a las funciones de Lotus Domino a través de la implementación de AirWatch.
- Repositorios de contenido: permite integrar con SharePoint, Google Drive, SkyDrive, servidores de archivos y recursos compartidos de archivos de red.
- Syslog (datos del registro de eventos): permite exportar los datos del registro de eventos para que se puedan ver en todos los servidores y sistemas integrados.
- Redes corporativas: permite configurar los ajustes de VPN y Wi-Fi, así como perfiles de provisión de dispositivos que contengan las credenciales requeridas para obtener acceso.
- Administración de la información y los eventos del sistema (SIEM): permite guardar y compilar los datos de los dispositivos y de la consola para garantizar la seguridad y conformidad con las reglas y las políticas corporativas.

Para obtener más información sobre cómo integrar Workspace ONE UEM con estas infraestructuras, consulte la documentación de Workspace ONE Access.

Consulte también la Introducción a VMware Tunnel, la Guía de solución de problemas y registro de Workspace ONE UEM y la Guía de instalación de Workspace ONE UEM, disponibles en docs.vmware.com. También puede buscar estos temas en docs.vmware.com.

Acceso basado en funciones

Puede hacer que las funciones otorguen tipos de acceso específicos a Workspace ONE UEM basado en AirWatch. Defina roles para usuarios y grupos individuales en función de los niveles de acceso de la consola de UEM que encuentre útiles.

Por ejemplo, los administradores del servicio de asistencia de la empresa pueden tener acceso limitado dentro de la consola, mientras que el administrador de TI tiene acceso a más permisos. Para obtener más información sobre este ejemplo, consulte el caso práctico Cómo se crea un administrador del servicio de asistencia restrictivo y se agrega una función que le otorgue permisos específicos.

Para habilitar el control de acceso basado en funciones, primero tiene que configurar las funciones de administradores y usuarios en la consola de UEM. Los recursos específicos, también conocidos como permisos, definen estos roles, que habilitan y desactivan el acceso a varias funciones dentro de la consola de UEM. Puede crear funciones de usuario que concedan acceso al portal de autoservicio.

Ya que las funciones (y específicamente los recursos o los permisos) determinan qué pueden y no pueden hacer los usuarios y administradores en la consola de UEM, se debe tener cuidado a la hora de otorgar los permisos o recursos correctos. Por ejemplo, si necesita que los administradores introduzcan una nota antes de que se pueda realizar una eliminación empresarial en un dispositivo, el rol no solo debe tener los permisos para realizar la eliminación empresarial en el dispositivo, también debe tener los permisos para agregar una nota.

Las funciones son importantes para mantener la seguridad de su flota de dispositivos, por ejemplo, la creación de usuarios provisionales, que es un privilegio de administrador de nivel elevado. Deberá tratar las credenciales de usuarios provisionales como privilegios de administrador y no divulgar las credenciales de usuario.

Roles predeterminados y roles personalizados

Workspace ONE UEM basado en AirWatch ofrece varias funciones predeterminadas que puede seleccionar. Estos roles predeterminados están disponibles con cada actualización y permiten asignar roles de manera rápida a los usuarios nuevos. Puede personalizar aún más los privilegios y los permisos de usuario si necesita más personalización.

A diferencia de los roles predeterminados, los roles personalizados requieren actualizaciones manuales con cada actualización de la versión de Workspace ONE UEM.

Todos los tipos de rol tienen ventajas y desventajas inherentes. Los Roles predeterminados ahorran tiempo en la configuración de un rol completamente nuevo, se adaptan lógicamente a varios privilegios administrativos y se actualizan automáticamente con nuevas funciones y ajustes. Sin embargo, es posible que las funciones predeterminadas no sean adecuadas para su organización o implementación de MDM, razón por la cual las funciones personalizadas están disponibles.

Roles de usuarios finales predeterminados

Las funciones están disponibles de forma predeterminada para los usuarios de dispositivos en la consola de administración de extremos unificada.

- Función de acceso completo: proporciona acceso completo al portal de autoservicio.
- Rol de acceso básico: otorgue permisos completos, excepto los comandos de MDM, desde el portal de autoservicio.

Los Roles personalizados permiten personalizar todos los roles únicos que se desee y ajustar cambios grandes o pequeños para los diferentes usuarios y administradores. Sin embargo, debe mantener manualmente las funciones personalizadas a lo largo del tiempo y actualizarlas con nuevas funciones.

Cómo editar un rol predeterminado de usuario final para crear un rol de usuario personalizado

Si ninguno de los roles predeterminados disponibles cumplen con los requisitos para su organización, considere modificar un rol predeterminado que ya exista y crear un rol personalizado.

Cree un rol de usuario final personalizado editando un rol predeterminado incluido en la consola de UEM.

1. Asegúrese de estar en el grupo organizativo que se asociará con el nuevo rol.
2. Acceda a Cuentas > Usuarios > Roles.
3. Determine qué rol de la lista se adapta mejor al que desea crear. A continuación, editar ese rol seleccionando el icono para editar ( ) en el extremo derecho. Aparecerá la página Agregar/Editar el rol.
4. Edite los cuadros de texto Nombre, Descripción y Página de destino inicial según sea necesario. Revise todas las casillas, que representan los distintos permisos. Seleccione o no las opciones según sea necesario.
5. Seleccione Guardar.

Roles administrativos predeterminados

Los siguientes roles están disponibles de forma predeterminada para los administradores en Workspace ONE UEM Console.

Utilice la herramienta para comparar roles administrativos para comparar los permisos específicos de dos roles administrativos. Para obtener más información, consulte la sección de esta página titulada Cómo crear una función de administrador.

Rol	Descripción

Administrador del sistema	El rol de administrador del sistema proporciona acceso completo a un entorno de Workspace ONE UEM. También incluye acceso a los ajustes de contraseña y seguridad, a la administración de sesiones y a información de auditoría de la consola de UEM que se encuentra en la pestaña Administración, en Configuración del sistema. Este rol está limitado a administradores de entorno, por ejemplo, equipos de operaciones de SaaS para todos los entornos de SaaS alojados por VMware.
Administrador de AirWatch	El rol de administrador de AirWatch ofrece acceso completo al entorno de Workspace ONE UEM. Sin embargo, el acceso excluye la pestaña Administración en la Configuración del sistema, ya que esta pestaña administra los ajustes de nivel superior en la consola de UEM. Este rol se limita a los empleados de VMware con acceso a los entornos con fines de solución de problemas, instalación y configuración.
Administrador de la consola	El rol de administrador de la consola es el rol administrativo predeterminado para los entornos de SaaS compartidos. El rol cuenta con una funcionalidad limitada en cuanto a atributos de política de conformidad, creación de informes y selección de grupos organizativos.
Administrador del dispositivo	El rol de administrador de dispositivos brinda a los usuarios acceso significativo a la consola de UEM. Sin embargo, este rol no está diseñado para configurar la mayoría de las Configuraciones del sistema. Estas configuraciones incluyen Active Directory (AD)/Protocolo ligero de acceso a directorios (LDAP), Protocolo simple de transferencia de correo (SMTP), hubs de interfaz de dispositivo-UEM, como Intelligent Hub, etc. Para esas tareas importantes es más apropiado utilizar un rol de alto nivel como Administrador de AirWatch o Administrador del sistema.
Visor de reportes	El rol del visor de reportes permite ver los datos recopilados a través de la administración de dispositivos móviles (MDM). Este rol solo otorga acceso a los usuarios para generar, ver y exportar informes de la consola de UEM, así como para suscribirse a ellos.
Administración de contenido	El rol de administración de contenido solo otorga acceso a la administración de VMware AirWatch Content Locker. Utilice este rol para los administradores especializados encargados de cargar y administrar el contenido de la flota de dispositivos.
Administración de aplicaciones	La función Administración de aplicaciones permite que los administradores que tengan este nivel de permisos implementen y administren las aplicaciones internas y públicas de la flota de dispositivos. Utilice este rol para los administradores de aplicaciones.
Servicio de asistencia	El rol de servicio de asistencia proporciona las herramientas necesarias para la mayoría de las funciones del servicio de asistencia de TI del nivel 1. La utilidad principal de este rol es permitir a los administradores de AirWatch ver la información de los dispositivos y responder a través de acciones remotas. Sin embargo, este rol también permite las acciones de ver informes y buscar dispositivos.
Administrador del catálogo de aplicaciones solamente	El rol administrativo Solo catálogo de aplicaciones tiene prácticamente los mismos permisos que Administración de aplicaciones. Además de estos permisos encontramos la capacidad de agregar y mantener cuentas de usuario y administrador, grupos de usuarios y administradores, detalles de dispositivos y etiquetas.

Rol	Descripción
Sólo lectura	El rol de solo lectura ofrece acceso a la mayor parte de la consola de UEM, pero limita el acceso al estado de solo lectura. Utilice este rol para auditar o registrar la configuración en un entorno de Workspace ONE UEM. Este rol no es útil para los administradores o los operadores del sistema.
Administrador de Horizon	El rol Administrador de Horizon es un conjunto de permisos especialmente diseñado para complementar una configuración de Workspace ONE UEM integrada en la vista de VMware Horizon View.
Administrador de NSX	El rol Administrador de NSX es un conjunto de permisos especialmente diseñado para complementar VMware NSX integrado en Workspace ONE UEM. Este rol ofrece el complemento completo de permisos de administración de certificados y sistema, lo que permite a los administradores complementar la seguridad de los extremos con la seguridad del centro de datos.
Oficial de privacidad	El rol Oficial de privacidad ofrece acceso de lectura a Información general del Monitor, la Vista de lista de dispositivos, la opción Ver ajustes del sistema y permisos de edición completos para los ajustes de privacidad.

Cómo editar un rol predeterminado para crear un rol administrativo personalizado

Si los roles predeterminados disponibles no cumplen con los requisitos organizativos para los recursos administrativos, considere modificar un rol predeterminado que ya exista y utilícelo para crear un rol administrativo personalizado.

Cree un rol administrativo personalizado editando un rol predeterminado incluido en la consola de UEM.

1. Asegúrese de que esté en el grupo organizativo que se asociará con el nuevo rol.
2. Acceda a Cuentas > Administradores > Roles.
3. Determine qué rol de la lista se adapta mejor al que desea crear. Marque la casilla de ese rol.
4. Seleccione Copiar en el menú de acciones. La página Copiar rol aparecerá.
5. Edite los ajustes necesarios de la copia que aparece en la página Copiar rol. Cree un Nombre y Descripción únicos para el rol personalizado.
6. Seleccione Guardar.

Pasos siguientes: Para obtener más información, consulte la sección de esta página titulada Cómo crear una función de administrador.

Roles administrativos

Puede habilitar o desactivar los permisos para todos los ajustes y recursos disponibles en Workspace ONE UEM basado en AirWatch. Estos ajustes conceden o restringen capacidades de la consola para cada miembro del equipo administrativo, lo que permite crear una jerarquía de administradores que se adapte específicamente a sus necesidades.

La creación de múltiples roles administrativos es una medida que ahorra tiempo. Realizar configuraciones completas en diferentes grupos organizativos significa que puede cambiar los permisos para un administrador específico en cualquier momento.

Hacer que los cambios del rol administrativo sean efectivos

Si edita una función que está utilizando un administrador, los cambios no se aplicarán hasta que el administrador cierre sesión y vuelva a iniciarla.

Vista de lista de funciones de administrador

Acceda a Cuentas > Administradores > Roles.

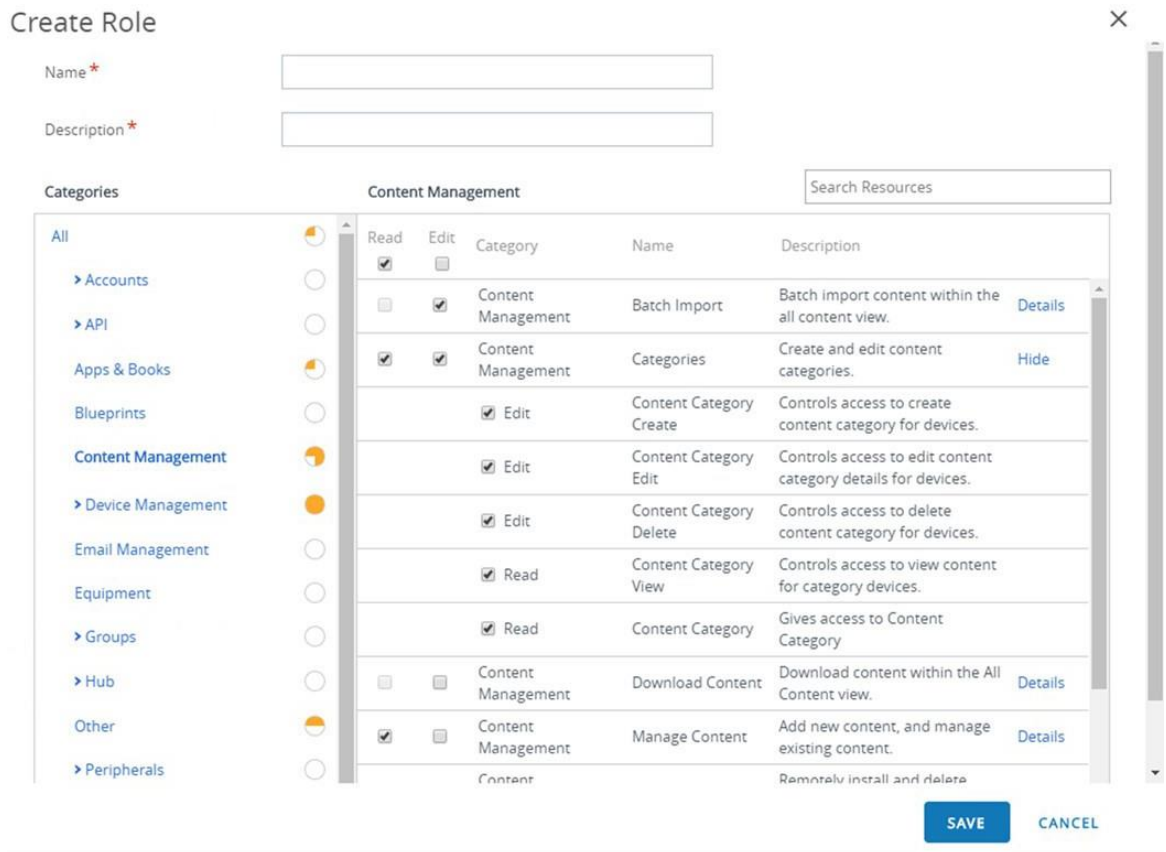
Puede eliminar un rol no utilizado de la biblioteca de roles administrativos. No puede eliminar una función asignada. Seleccione una función sin asignar y seleccione el botón Eliminar.

Puede editar el nombre, la descripción y los permisos específicos de una función. Seleccione el icono del lápiz a la izquierda del nombre de la función de la lista y aparece la pantalla Editar función.

También puede descargar un archivo XLSX o CSV (valores separados por comas) que contenga toda la vista de lista de funciones de administradores. A continuación, puede ver y analizar este archivo con MS Excel. Seleccione el botón Exportar y elija una ubicación de descarga. Para obtener información sobre cómo exportar funciones e importarlas posteriormente, consulte la sección de esta página denominada Exportar funciones administrativas.

Cómo crear roles administrativos

1. Acceda a Cuentas > Administradores > Roles y seleccione Agregar rol en la consola de UEM.



2. En el campo Crear rol, introduzca el Nombre y la Descripción del rol.

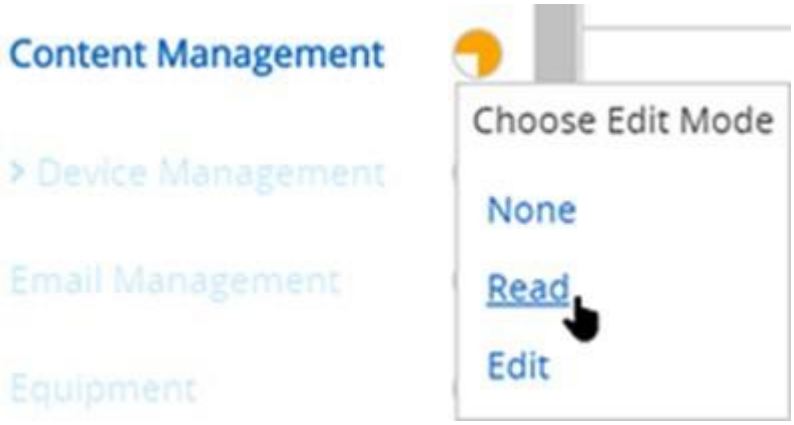
3. Realice una selección en la lista de Categorías.

   La sección Categorías organiza categorías de alto nivel, como Administración de dispositivos, que contiene las subcategorías Aplicaciones, Navegador y Administración en masa, entre otras. La subdivisión de esta categoría facilita un proceso de creación de roles sencillo y rápido. Los ajustes de cada subcategoría en el panel derecho tienen una casilla para Leer y Editar.

   Cuando realiza una selección en la sección Categorías, el contenido de esa subcategoría (ajustes individuales) se rellenarán en el panel derecho. Cada ajuste individual tienen sus propias casillas Leer y Editar, aparte de las casillas con la opción "Seleccionar todo" para Leer y Editar, que puede elegir en cada encabezado de columna. Esas casillas le proporcionan un nivel de control y personalización flexibles a la hora de crear un rol.

   Utilice el cuadro de texto Buscar recursos para reducir el número de recursos del cual puede seleccionar. Por lo general, los recursos están etiquetados del mismo modo en el que se hace referencia a ellos en la consola de UEM. Por ejemplo, si desea limitar una función administrativa para editar los registros de aplicaciones, introduzca "Registros de aplicaciones" en el cuadro Buscar recursos y aparecerá una lista de todos los recursos que contienen la cadena "Registros de aplicaciones".

4. Seleccione la casilla apropiada para Leer y Editar en las opciones de recursos correspondientes. También puede borrar cualquier recurso seleccionado.



5. Para realizar selecciones globales en las categorías, seleccione la opción Ninguno, Leer o Editar directamente desde la sección Categorías, sin necesidad de rellenar el panel derecho. Seleccione el icono circular a la derecha de la etiqueta Categoría, que es un menú desplegable. Utilice este método de selección cuando esté completamente seguro de que desea seleccionar Ninguno, Solo lectura o Editar para las capacidades de los ajustes de toda la categoría.

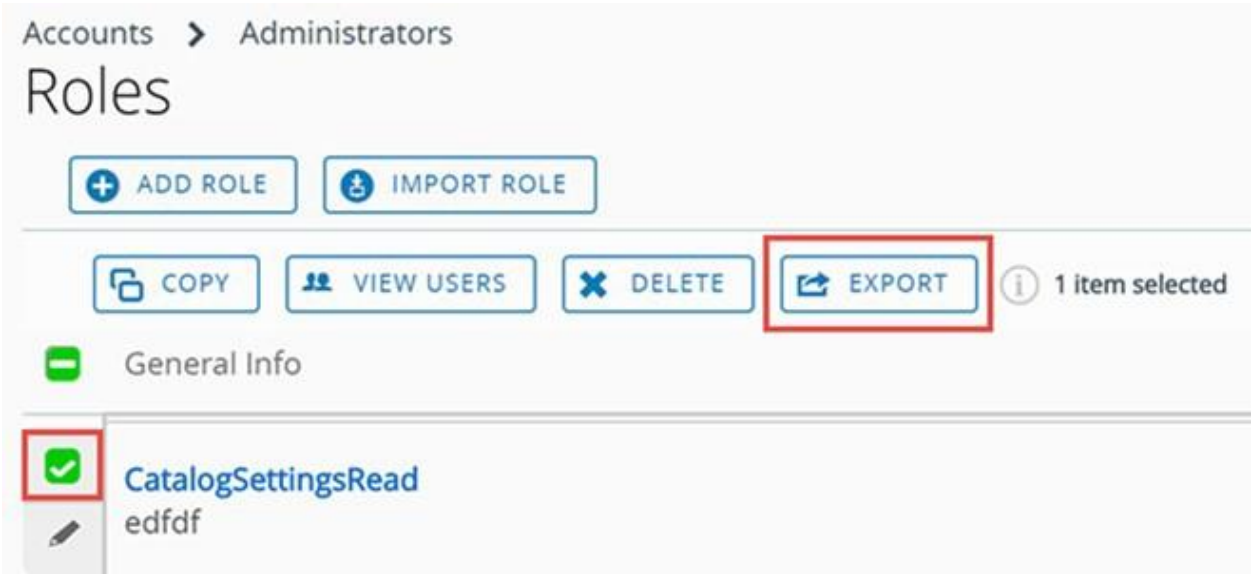
6. Seleccione Guardar para terminar de crear el rol personalizado. Ahora podrá ver el rol agregado en la lista de la página Roles. Desde aquí, también puede editar los detalles del rol o eliminarlo.

Pasos siguientes: Debe actualizar el rol personalizado después de cada actualización de Workspace ONE UEM para tener en cuenta todas las nuevas funcionalidades en la última versión.

Cómo exportar roles administrativos

Las funciones de administrador constituyen un recurso portátil. Esta portabilidad puede ahorrar

tiempo si se gestionan varios entornos de Workspace ONE UEM. Puede exportar los ajustes desde un entorno como un archivo XML y, a continuación, importar ese archivo XML a otro entorno. Esta actividad puede causar problemas de control de versiones.



1. Acceda a Cuentas > Administradores > Roles.
2. Exporte una función seleccionando la casilla de verificación junto a la función de administrador. Si seleccione más de un rol administrativo, la acción Exportar no se encontrará disponible.
3. Seleccione el botón Exportar y guarde el archivo XML en una ubicación del dispositivo.

Cómo importar roles administrativos

1. Acceda a Cuentas > Administradores > Roles y seleccione Importar rol.
2. En la página Importar rol, seleccione Examinar y busque el archivo XML que haya guardado. Cargue la función de administrador en la lista de categorías para su validación seleccionando Cargar.
3. Workspace ONE UEM realiza una serie de comprobaciones de validación, como la comprobación del archivo XML, la de la importación de permisos de roles, la de nombres de roles duplicados y la de nombres y descripciones vacíos.
4. Compruebe los ajustes del recurso y verifique las especificaciones del rol importado. Para ello, seleccione las categorías específicas en el panel de la izquierda.
5. También puede editar los recursos y el Nombre y la Descripción del rol importado según sus necesidades. Si desea mantener el rol existente y el importado, cambie el nombre del rol administrativo existente antes de importar el nuevo.
    1. Si el rol que va a importar tiene el mismo nombre que otro rol de su entorno, aparecerá el mensaje “Existe una función con este nombre en este entorno. ¿Desea reemplazar la función existente?”
    2. Si selecciona "No", entonces el rol existente en su entorno permanece sin cambios y se cancela la importación del otro rol.
    3. Si selecciona "Sí", se le pedirá el PIN de seguridad. Si es correcto, se sustituirá el rol

existente por el importado.

6. Seleccione Guardar para aplicar el rol importado al nuevo entorno.

Problemas relacionados con las versiones al importar y exportar roles administrativos

Puede haber casos en que una función exportada se importe a un entorno que ejecute una versión anterior de Workspace ONE UEM. La versión anterior no tiene necesariamente los mismos recursos y permisos que componen el rol importado.

En estos casos, Workspace ONE UEM notifica el siguiente mensaje:

No se encuentran ciertos permisos de este entorno en el archivo importado. Revise y corrija los permisos resaltados antes de guardar.

Utilice la página de lista de categorías para anular la selección de los permisos resaltados. Esta acción permite guardar el rol en el nuevo entorno.

Copiar rol

Puede crear una copia de un rol existente para ahorrar tiempo. También puede cambiar los permisos de la copia y guardarla con un nombre diferente.

1. Marque la casilla que aparece junto al rol que desea copiar.
2. Seleccione el botón Copiar. La página Copiar rol aparecerá.
3. Realice los cambios en Categorías, Nombre y Descripción.
4. Cuando finalice, seleccione Guardar.

Cómo cambiar el nombre de un rol administrativo

Si va a importar un rol administrativo con el mismo nombre que otro rol administrativo ya existente, es posible que le resulte útil cambiar primero el nombre de este último. Al cambia el nombre de un rol, podrá mantener tanto el rol nuevo como el antiguo dentro del mismo entorno.

1. Acceda a Cuentas > Administradores > Roles y seleccione el icono Editar () del rol cuyo nombre desea cambiar. Aparecerá la página Editar rol.
2. Edite el Nombre del rol y, si lo desea, la Descripción.
3. Seleccione Guardar.

Indicador Solo lectura/Editar en categorías para los roles administrativos

En la sección Categorías, existe un indicador visual que refleja la selección actual de Solo lectura, Editar o una combinación de ambas. Este indicador indica cuál es el ajuste sin que tenga que abrir y examinar los ajustes de cada subcategoría.

El indicador tiene un icono circular ubicado a la derecha de la lista de categorías que proporciona información sobre lo siguiente.

Icono	Descripción
	Todas las opciones de esta categoría cuentan con capacidad de edición (lo que significa que también cuentan con la capacidad de solo lectura).
	La mayoría de los ajustes de categoría tienen la capacidad de edición habilitada, pero hay al menos una subcategoría que la tiene desactivada.
	Todos los ajustes de la categoría tienen la capacidad de solo lectura (la edición está desactivada).
	La mayoría de los ajustes de categoría son de solo lectura, pero hay al menos una subcategoría que tiene la función de editar habilitada.

Asignar una función o editar la carga de la función de un administrador

Puede asignarle funciones a un administrador para ampliar sus capacidades en Workspace ONE UEM Console. También puede editar la carga existente de la función, lo que puede limitar o ampliar las capacidades de un administrador.

Si edita una carga de una función que está utilizando un administrador, los cambios no tendrán efecto hasta que el administrador cierre sesión y vuelva a iniciarla.

1. Vaya a Cuentas > Administradores > Vista de lista, localice la cuenta de administrador cuya carga de función desea modificar y seleccione el icono Editar () a la izquierda del nombre de usuario de la cuenta administrativa. Aparecerá la página Agregar/Editar administrador.
2. Seleccione la pestaña Funciones y, a continuación, elija entre las siguientes, a, b o una combinación de ambas:
    1. Si desea agregar una nueva función a la cuenta de administrador, seleccione el botón Agregar función y, a continuación, introduzca los detalles de Grupo organizativo y Función de cada función que agregue.
    2. Si desea eliminar una función existente de la cuenta de administrador, seleccione la función y, a continuación, haga clic en el botón Eliminar.
3. Seleccione Guardar.

Cómo ver los recursos de un rol administrativo

Puede ver todos los recursos o permisos de cualquier rol administrativo, incluidos los roles personalizados o predeterminados. Esta vista puede ayudarle a determinar qué puede, y no puede, hacer un administrador en la consola de UEM.

Las funciones están formadas por cientos de recursos, o permisos, que sirven de acceso (de solo lectura o edición) a una función específica dentro de UEM Console.

Las pantalla Ver función y Editar función son las mismas, con la excepción de que la pantalla Editar función le permite realizar y guardar cambios con el botón Guardar.

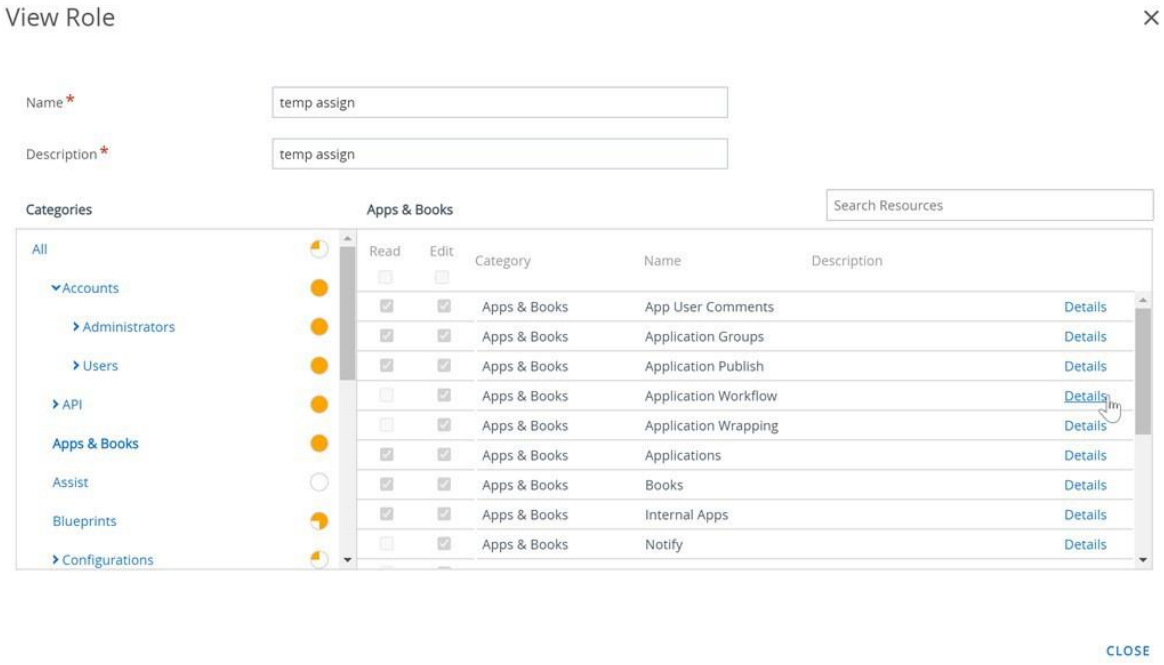
Para ver o editar los recursos de una función administrativa, realice los siguientes pasos.

1. Acceda a Cuentas > Administradores > Roles.
2. Busque la función de administrador para la que desea ver los permisos. Si tiene una

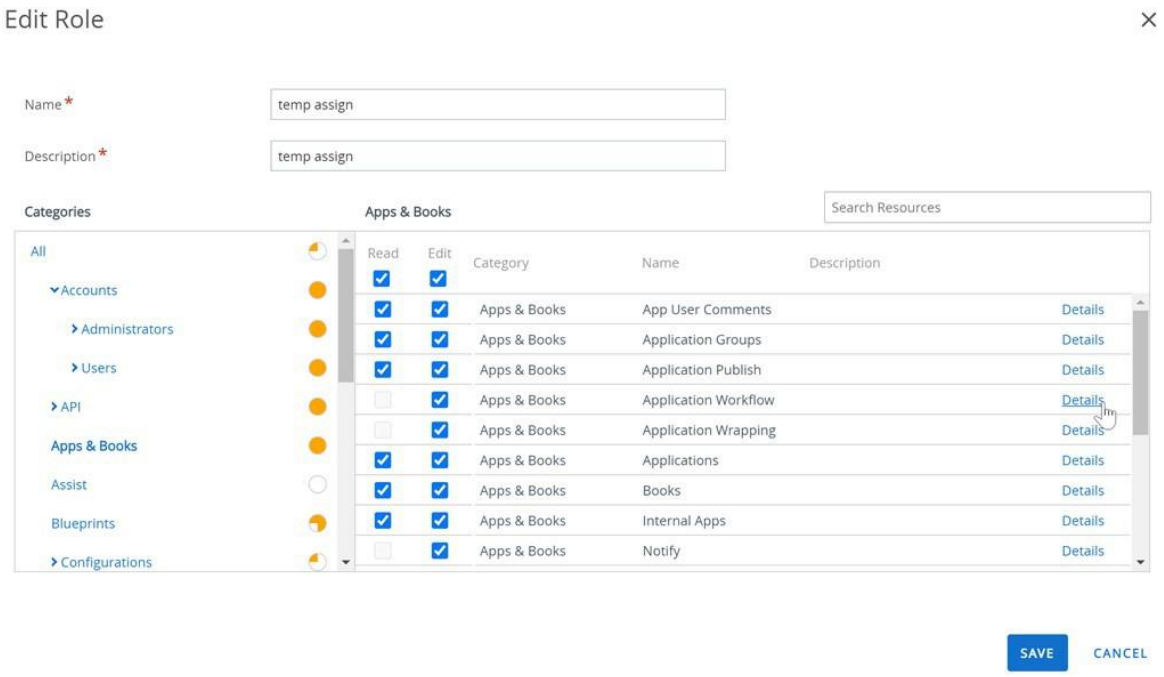
biblioteca grande de roles administrativos, utilice la barra Buscar en lista en la esquina superior derecha para reducir la lista.

3. Seleccione entre las siguientes opciones, a o b:

    1. Para ver la función, seleccione el nombre de la función, que es un enlace, y la pantalla Ver función muestra todos los permisos asociados con la función. Cuando finalice la auditoría de los roles administrativos, seleccione Cerrar.



    1. Para editar la función, seleccione el icono Editar ( ) a la izquierda del nombre de la función y aparecerá la pantalla Editar función. Edite la función agregando o eliminando las marcas de verificación Lectura y Editar. Cuando termine de editar la función, seleccione Guardar.



Algunos aspectos sobre la lista, si selecciona Ver o Editar.

- Las categorías de función se enumeran en el panel izquierdo. Seleccione el indicador ">"

para expandir la categoría y ver las subcategorías de las funciones.

- Para obtener más información acerca de los indicadores visuales de lectura o edición de color naranja que se ven en esta pantalla, consulte la sección de esta página con el título Indicador de lectura o edición en categorías para las funciones administrativas.
- Seleccione una categoría específica en el panel izquierdo, y la categoría, nombre y descripción de cada recurso se muestra en el panel derecho.
    - El enlace Detalles en el extremo derecho revela cada función de solo lectura y edición específica dentro de la consola de UEM.
- Puede utilizar el cuadro de texto Buscar recursos para localizar una función específica por su nombre. Esta función de búsqueda facilita la tarea de localizar la función relacionada con la etiqueta específica y asignarla a una función.
    - Por ejemplo, si desea que una función administrativa solo pueda agregar una etiqueta a un dispositivo, escriba la palabra "etiqueta" en el cuadro de texto Buscar recursos y pulse la tecla Intro. Todos los recursos que contengan la cadena "etiqueta" en la categoría, el nombre, la descripción o los detalles de la descripción aparecen en el panel derecho.

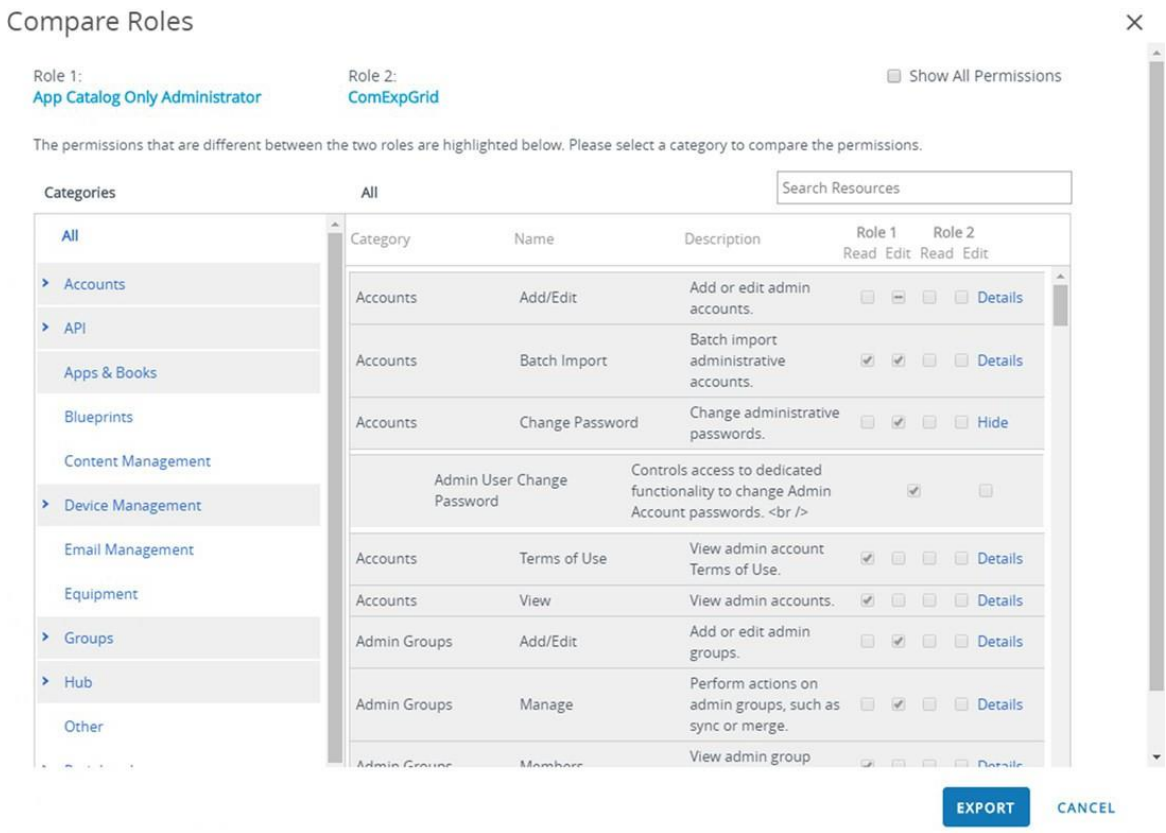
      Aviso: Tenga en cuenta que "provisional" (como en los dispositivos provisionales) también incluye la cadena "etiqueta".

Pasos siguientes: Puede aplicar estos pasos para crear sus propias funciones; para ello, visite la sección de esta página con el título Cómo crear una función de administrador.

Comparar dos roles

A la hora de crear una función administrativa, a menudo es más sencillo modificar una función rol existente que crear una desde cero. La herramienta Comparar funciones le permite comparar los ajustes de permisos de dos funciones administrativas para garantizar su precisión o confirmar las diferencias de los ajustes que estableció de forma deliberada.

1. Acceda a Cuentas > Administradores > Roles.
2. Elija dos roles en la lista, aunque estén en páginas distintas, y selecciónelos.
3. Seleccione Comparar. La página Comparar roles muestra una lista de categorías. Al seleccionar una categoría específica a la izquierda, todos los detalles de esa categoría se rellenarán.



- Si tiene menos de dos o más de dos roles seleccionados, no se muestra el botón Comparar.
- Seleccione el enlace Detalles en el lado derecho para ver las subcategorías de funciones. Contraiga la subcategoría del rol mediante la selección del enlace Ocultar.
- En el panel izquierdo, hay una categoría Todos que cuando se selecciona muestra todas las categorías principales en la página Comparar roles. Cuando introduce un parámetro de búsqueda en la barra Buscar recursos, el panel derecho mostrará solamente las listas de categorías y recursos (también conocidos como permisos) correspondientes.
- La función de búsqueda es persistente. Esto significa que, si tiene un parámetro en la barra de Buscar recursos, al seleccionar la categoría Todos, solo aparecerán las categorías y recursos que coincidan. La función de búsqueda es persistente incluso después de que se seleccionan recursos específicos y las opciones Leer y Editar.
- De forma predeterminada, solo se muestran las categorías y subcategorías cuyos ajustes son diferentes. Para mostrar todos los permisos, incluso aquellos ajustes que sean idénticos en ambos roles seleccionados, seleccione la casilla Mostrar todos los permisos.
- Si selecciona dos roles que tienen permisos idénticos, la consola muestra este mensaje en la parte superior de la página Comparar roles.

"No hay diferencias entre los permisos de estas dos funciones."

Pasos siguientes: También puede seleccionar Exportar para crear un archivo XLSX o CSV (valores separados por comas) que puede verse en Excel. El archivo de exportación contiene todos los ajustes del Rol 1 y el Rol 2 para que pueda analizar las diferencias entre ellos.

Roles de usuario

Las funciones de usuario en Workspace ONE UEM basado en AirWatch permiten habilitar o desactivar las acciones específicas que los usuarios pueden realizar. Entre estas acciones se incluye controlar el acceso a una eliminación total, consultar dispositivos y administrar contenido personal. Las funciones de usuario también pueden personalizar las páginas de destino iniciales y restringir el acceso al portal de autoservicio.

La creación de múltiples roles de usuario es una medida que ahorra tiempo. Puede realizar configuraciones completas en diferentes grupos organizativos o cambiar el rol del usuario para un usuario específico en cualquier momento.

Cómo crear un nuevo rol de usuario

Además de los roles de acceso básico y de acceso completo predeterminados, también puede crear roles personalizados. Tener varios roles disponibles fomenta la flexibilidad y puede ahorrar tiempo a la hora de asignar roles a usuarios nuevos.

1. Acceda a Cuentas > Usuarios > Roles y seleccione Agregar rol. Aparecerá la página Agregar/Editar el rol.
2. Introduzca el Nombre y la Descripción y seleccione la Página de destino inicial del SSP para los usuarios que tengan este nuevo rol.

   Para los roles de usuario existentes, la Página de destino inicial predeterminada es la página Mis dispositivos.
3. Seleccione, en la lista de opciones, el nivel de acceso y control que los usuarios finales de este rol asignado tienen en el SSP.
   - Haga clic en No seleccionar nada para borrar las casillas de la página.
   - Elija Seleccionar todo para marcar todas las casillas de la página.
4. Seleccione Guardar para guardar los cambios en el rol. El nuevo rol de usuario aparecerá en la lista de la página Roles.

Pasos siguientes: En la página de roles puede ver, editar o eliminar roles.

Cómo configurar un rol predeterminado

Un rol predeterminado es un valor de referencia para todos los roles de usuario. Si configura un rol predeterminado, podrá establecer los permisos y privilegios que los usuarios reciben automáticamente durante la inscripción.

1. Acceda a Dispositivos > Configuraciones de dispositivos > Dispositivos y usuarios > General > Inscripción y seleccione la pestaña Agrupación.
2. Configure un nivel de acceso predeterminado para los usuarios finales en el portal de autoservicio (SSP) mediante la selección de un rol predeterminado.

   Estas configuraciones de los roles se pueden personalizar por grupo organizativo. Escoja una de las siguientes opciones.
   - Acceso completo: concede a los usuarios acceso a las funciones superiores de SSP

como instalar o eliminar perfiles y aplicaciones, restablecer los códigos de acceso, enviar mensajes de dispositivos y acceso de escritura al contenido.

- Acceso básico: concede a los usuarios acceso de un impacto bajo. Pueden registrar su propio dispositivo, tener (pero no instalar) perfiles solo de consulta y aplicaciones, ver su propia cuenta y consultar y buscar su dispositivo.
- Acceso externo: los usuarios con acceso externo cuentan con todas las habilidades como usuarios de acceso básico, pero también tienen acceso de solo lectura al contenido en el SSP que ha sido explícitamente compartido con ellos.

3. Seleccione Guardar.

Cómo asignar o editar el rol de un usuario

Puede editar el rol de un usuario específico para, por ejemplo, otorgarle o restringirle el acceso a funciones de Workspace ONE UEM.

Si edita una función que está utilizando un usuario, los cambios no tendrán efecto hasta que el usuario cierre sesión y vuelva a iniciarla.

1. Seleccione el grupo organizativo correspondiente.
2. Vaya a Cuentas > Usuarios > Vista de lista.
3. Busque un usuario específico que desee editar en la lista. Una vez que haya identificado el usuario, seleccione el icono de edición que hay bajo la casilla. Aparecerá la pantalla Agregar/Editar usuario.
4. En la pestaña General, vaya a la sección Inscripción y seleccione el Rol de usuario del menú desplegable para cambiar el rol del usuario específico.
5. Seleccione Guardar.
6. Cómo se crea un administrador del servicio de asistencia restrictivo y se agrega una función que le otorgue permisos específicos
   Puede crear una función personalizada que permita a un administrador del servicio de asistencia realizar aquellas tareas que usted le permita en Workspace ONE UEM basado en AirWatch. Descubra cómo las cuentas, las funciones y los permisos programables funcionan juntos para que pueda conseguir sus objetivos.

Cómo se crea un administrador del servicio de asistencia restrictivo y se agrega un rol que le otorgue permisos específicos

Puede crear una función personalizada que permita a un administrador del departamento de servicio de asistencia realizar solo aquellas acciones que usted le permita en Workspace ONE UEM basado en AirWatch. Descubra cómo las cuentas, las funciones y los permisos programables funcionan juntos para que pueda conseguir sus objetivos.

Debe tener una cuenta de administrador existente. En este caso práctico se crea una función personalizada basada en la función "Servicio de asistencia", incluida en Workspace ONE UEM basado en AirWatch, y la asigna a su cuenta de administrador.

Caso práctico: necesita que los recursos dedicados del servicio de asistencia asuman la tarea de agregar usuarios y dispositivos, pero sin que esto afecte a los demás administradores. Estos administradores también deben incluir los dispositivos de la lista de permitidos y de la lista de no permitidos. Al mismo tiempo, es esencial limitar los puntos de acceso a las capacidades de la consola de más alto nivel. Desea agregar una serie de cuentas de administrador y permitirles la adición de usuarios y dispositivos, la inclusión de dispositivos en las listas de permitidos y de no permitidos, pero nada más.

A la función que se crea en este caso práctico se le otorga un conjunto reducido de funciones de Console: agregar usuarios y dispositivos, e incluirlos en las listas de permitidos y de no permitidos. Esta función prohíbe todas las demás funciones en Workspace ONE UEM.

1. Acceda a Cuentas > Administradores > Roles.

   Se mostrará la lista completa de roles de administrador.

2. Introduzca la palabra clave "ayuda" en el cuadro de texto de búsqueda en la esquina superior derecha de la pantalla.

   Todas las funciones que contengan la cadena de texto "ayuda" se mostrarán en la lista.

3. Seleccione el rol Servicio de asistencia marcando la casilla de verificación a la izquierda del nombre del rol.

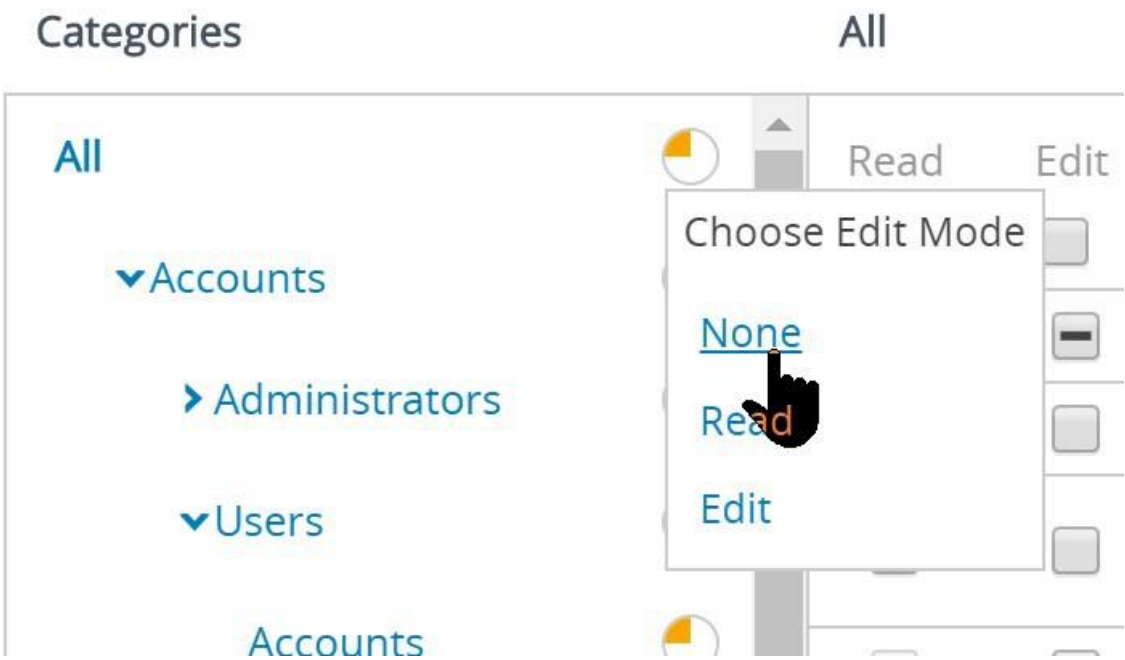
   Aparece una nueva agrupación de botones en el grupo de botones principal.

4. Seleccione el botón Copiar.

   Aparecerá la página Copiar rol.

5. Introduzca valores en Nombre y Descripción para el rol personalizado del servicio de asistencia.

6. Seleccione el gráfico circular de color naranja a la derecha de la categoría Todo en la parte izquierda de la pantalla Copiar rol. Seleccione Ninguno en la lista emergente Elegir modo de edición que se muestra.



Con esta acción se eliminan todos los permisos de este rol personalizado del servicio de asistencia, lo que le permite empezar de cero. Por lo tanto, los únicos permisos que tienen estos administradores serán los que se otorguen aquí.

7. Habilite los ocho permisos siguientes. Puede encontrar la ubicación de cada casilla de verificación de permiso con los nombres de categoría, subcategoría y permiso en la tabla.

   Recuerde que puede escribir el nombre del permiso en el cuadro de texto Buscar recursos para acceder directamente a su ubicación.

Categoría > Subcategorías	Nombre de permiso (casilla de verificación)
Cuentas > Usuarios > Cuentas	Cuentas de los usuarios/Agregar (Editar)
Cuentas > Usuarios > Cuentas	Cuentas de usuario/Editar (Editar)
Cuentas > Usuarios > Cuentas	Editar la inscripción del usuario (Editar)
Cuentas > Usuarios > Cuentas	Inscripción del usuario (Leer)
Administración de dispositivos > Vista de lista de dispositivos	Acceso a la vista de lista de dispositivos (Leer)
Administración de dispositivos > Vista de lista de dispositivos	Dispositivos (Leer)
Ajustes > Dispositivos y usuarios > General	Agregar dispositivo en lista de no permitidos (Editar)
Ajustes > Dispositivos y usuarios > General	Agregar dispositivo en lista de permitidos (Editar)

Empezando por la parte superior de la tabla, revisaremos los primeros cuatro permisos como ejemplo. El nombre del primer permiso que necesitamos (denominado "Cuentas de usuario/Agregar") se puede encontrar en la pantalla Copiar función si se selecciona la categoría "Cuenta" en el panel izquierdo.

En el mismo panel de la izquierda, seleccione la subcategoría "Usuarios" y, por último, seleccione "Cuentas", que se encuentra bajo Usuarios. Ahora puede ver todos los permisos en el panel derecho de la pantalla Copiar rol.

En esta subcategoría "Cuentas > Usuarios > Cuentas", hay cuatro casillas de verificación que nos interesan.

1 y 2. Seleccione el vínculo Detalles en "Agregar/Editar" para revelar dos permisos de la lista. Habilítelas como se indica en la tabla. "Cuentas de usuario/Agregar" tiene la casilla Editar y "Cuentas de usuario/Editar" también tiene la casilla Editar.

3. A continuación, seleccione el vínculo Detalles para "Agregar dispositivo". Debería ver el siguiente permiso en nuestra lista: "Editar la inscripción del usuario", que también tiene la casilla Editar.

4. Se mantiene un permiso de esta subcategoría, denominado "Inscripción del usuario", que se encuentra al seleccionar el vínculo Detalles de "Ver". Obtiene la casilla de verificación Lectura.

Siga el mismo proceso para los cuatro permisos restantes de la tabla, comenzando por "Acceso a la vista de lista de dispositivos".

8. Seleccione Guardar para finalizar la definición del rol personalizado del servicio de asistencia.
9. Asigna esta función personalizada a su cuenta administrativa existente. Para ello, vaya a Cuentas > Administradores > Vista de lista y busque la cuenta de administrador en la lista.
10. Selecciona el icono Editar () a la izquierda de su cuenta de administrador.

    Aparecerá la pantalla Agregar/Editar administrador.
11. Seleccione la pestaña Roles.
12. Asigne el rol personalizado del servicio de asistencia a la cuenta de administrador.

    Este caso de uso determina que solo se asignan nueve funciones de la consola de UEM al rol de administrador. Aun así, puede agregar este rol de soporte técnico personalizado y otros roles a su cuenta de administrador, incluso si su cuenta de administrador ya tiene uno o varios roles asignados.
13. Seleccione Guardar para finalizar la asignación de roles.

Cuando los administradores que tengan solo esta función personalizada del servicio de asistencia inicien sesión en el entorno de Workspace ONE UEM, la única función a la que tienen acceso es el botón Agregar, en el que solo pueden seleccionar dos opciones: Dispositivo y Usuario. También tienen acceso al botón del menú principal Dispositivos, que incluye Vista de lista y Ciclo de vida > Estado de inscripción, que es donde se agregan los dispositivos de las listas de permitidos y de no permitidos.

Portal de autoservicio en Workspace ONE UEM

Introduzca los usuarios finales del dispositivo en el Portal de autoservicio (SSP) y permítales realizar tareas de administración del dispositivo básicas, investigar problemas y solucionarlos, lo que reducirá el número de problemas de soporte técnico. Por lo tanto, mientras los administradores tengan acceso a Workspace ONE UEM, los usuarios finales del dispositivo tendrán el SSP.

Cómo configurar la página predeterminada de inicio de sesión para SSP

Puede establecer el método de autenticación predeterminado que se muestra en el Portal de autoservicio de Workspace ONE UEM según las necesidades de su organización y las necesidades de sus usuarios.

Aviso: Los clientes en la sede solo pueden acceder a este ajuste en el nivel global.

Configure este ajuste desde Grupos y ajustes > Todos los ajustes > Instalación > Avanzado > Otro y establezca el Tipo de autenticación SSP en:

- Correo electrónico: si configura el servicio de detección automática, los usuarios recibirán una solicitud para introducir la dirección de correo electrónico.
- Heredado: los usuarios reciben una solicitud para introducir el ID de grupo y credenciales (nombre de usuario/contraseña).
- Dedicado: los usuarios reciben una solicitud para introducir las credenciales (nombre de usuario/contraseña) solamente. Esta opción crea un solo ID de grupo predeterminado para los entornos de cliente único.

Inicie sesión en el SSP

Inicie sesión con las mismas credenciales (ID de grupo, Nombre de usuario y Contraseña) que utilizó para inscribirse en Workspace ONE UEM.

Seleccione un idioma para el SSP

El Portal de autoservicio se muestra automáticamente en el idioma predeterminado del navegador. Sin embargo, puede reemplazar este ajuste predeterminado mediante la elección de Seleccionar idioma en el campo desplegable que está en la página de inicio de sesión.

Cambie su contraseña para el SSP

Para cambiar la contraseña, haga clic en el botón Cuenta, en la parte superior derecha de la pantalla Portal de autoservicio. Seleccione el botón Cambiar situado junto al campo Contraseña actual en la página Cuenta de usuario.

Aviso: Si un usuario final del dispositivo inicia sesión en SSP para cambiar el código de acceso compartido del dispositivo antes de que caduque, este nuevo código de acceso indicará la fecha de caducidad del GO asociado con el dispositivo compartido y no el GO desde el cual se administra el usuario final.

Por ejemplo, supongamos que cuenta con una estructura de GO con un elemento "Principal" en el nivel superior y un elemento "Secundario" que depende de él. Supongamos que la cuenta de usuario final está administrada por el "Principal" con una caducidad de código de acceso de 90 días. Supongamos también que el dispositivo compartido está administrado por el "Secundario" con una caducidad de código de acceso de 30 días. En este escenario, cuando el usuario final inicia sesión en el portal de autoservicio y cambia el código de acceso compartido del dispositivo antes de que caduque, la caducidad del nuevo código de acceso pasa de 90 días (Principal) a 30 días (Secundario).

La solución alternativa consiste en garantizar la configuración del código de acceso del dispositivo compartido en el GO desde el cual se administran los usuarios.

Como administrador, si cambia el código de acceso del dispositivo compartido del usuario final en la pantalla Agregar/Editar usuario de Workspace ONE UEM Console, adoptará correctamente la fecha de caducidad del GO desde el que se administra el usuario final.

Cómo acceder al Portal de autoservicio en los dispositivos

Acceda al Portal de autoservicio (SSP) desde una estación de trabajo o un dispositivo desde https://<AirWatchEnvironment>/MyDevice. Si tiene un dispositivo que es compatible con Web clips o Marcadores, su administrador puede suministrar estos accesos directos, lo que, a la vez, permite tener acceso directo al SSP.

Personalizaciones del portal de autoservicio (SSP)

Es posible modificar el fondo predeterminado de la página de inicio de sesión mediante la configuración de la personalización de marca.

Navegue a Grupos y ajustes > Todos los ajustes > Sistema > Personalización de marca y seleccione el botón Cargar en el ajuste Fondo de pantalla de la página de inicio de sesión del Portal de autoservicio. Seleccione una imagen de fondo personalizada con un tamaño recomendado de 1024 x 768 píxeles.

Matriz de acciones del portal de autoservicio

Cada una de las principales plataformas de dispositivos es compatible con varias acciones de SSP básicas y avanzadas en Workspace ONE UEM.

Acción	Android	iOS	macOS	Windows Mobile	Win 7	Escritorio de Windows
Acciones básicas						
Cambiar código de acceso.	✓					

Acción	Android	iOS	macOS	Windows Mobile	Win 7	Escritorio de Windows
Borrar código de acceso (SSO).	✓	✓				✓
Eliminar dispositivo.	✓	✓	✓	✓	✓	✓
Eliminar registro.	✓	✓		✓	✓	✓
Consultar dispositivo	✓	✓	✓		✓	✓
Borrar todo	✓	✓	✓	✓		
Descargar Hub.			✓		✓	
Eliminación empresarial	✓	✓	✓	✓	✓	✓
Ubicar dispositivo.	✓	✓		✓		✓
Bloquear dispositivo/pantalla.	✓	✓	✓	✓	✓	
Bloquear SSO.		✓				
Hacer ruido.	✓					
Reenviar mensaje de inscripción.	✓	✓		✓	✓	✓
Enviar mensaje.	✓	✓	✓	✓	✓	✓
Establecer roaming.		✓				
Sincronizar dispositivo.	✓	✓				
Ver mensaje de inscripción.*	✓	✓		✓	✓	✓
Acciones avanzadas						
Generar token de la aplicación.	✓	✓	✓	✓	✓	✓
Administrar correo electrónico.				✓	✓	✓
Revisar los Términos de uso.	✓	✓	✓	✓	✓	✓
Revocar token.	✓	✓	✓	✓	✓	✓
Cargar certificado S/MIME.	✓	✓	✓	✓	✓	✓

* A modo de función de seguridad, esta acción no está disponible para las cuentas que se inscribieron con un token.

Cómo realizar acciones en el SSP

Los usuarios finales pueden realizar acciones remotas de forma inalámbrica en el dispositivo seleccionado desde el Portal de autoservicio. El administrador determina los permisos de acción y las acciones disponibles en el SSP, que varían según la plataforma. Las acciones permitidas se dividen en Acciones básicas y Acciones avanzadas en la página de acceso principal.

Los administradores disponen de varias acciones y opciones remotas para los dispositivos administrados. Sin embargo, cuando los dispositivos son propiedad de los empleados, seguramente deseen tener acceso a herramientas de administración similares. El portal de autoservicio (SSP) ofrece a los empleados una manera de utilizar herramientas clave de MDM sin necesitar la ayuda del

equipo de TI. Si lo habilita, los usuarios finales podrán ejecutar el SSP en un navegador web y acceder a las herramientas de ayuda clave de MDM. También puede habilitar o desactivar la muestra de información y la habilidad de llevar a cabo acciones remotas desde el SSP.

El administrador determina los permisos de acción, por lo que los usuarios de los dispositivos podrían tener limitadas las acciones disponibles. Consulte la guía de la plataforma correspondiente, disponible en docs.vmware.com. También puede buscar opciones de una determinada plataforma en la sección de ayuda en línea.

Acciones remotas básicas

Las acciones remotas básicas aparecen en la pestaña Acciones básicas del dispositivo seleccionado en el portal de autoservicio. Las acciones disponibles dependen del estado de inscripción, plataforma de dispositivo y permisos de acciones.

Acción	Descripción
Cambiar código de acceso	Permite configurar un código de acceso nuevo para el dispositivo seleccionado. Si un usuario final del dispositivo inicia sesión en SSP para cambiar el código de acceso compartido del dispositivo antes de que caduque, este nuevo código de acceso indicará la fecha de caducidad del GO asociado con el dispositivo compartido y no el GO desde el cual se administra el usuario final. Por ejemplo, supongamos que cuenta con una estructura de GO con un elemento "Principal" en el nivel superior y un elemento "Secundario" que depende de él. Supongamos que la cuenta de usuario final está administrada por el "Principal" con una caducidad de código de acceso de 90 días. Supongamos también que el dispositivo compartido está administrado por el "Secundario" con una caducidad de código de acceso de 30 días. En este escenario, cuando el usuario final inicia sesión en el portal de autoservicio y cambia el código de acceso compartido del dispositivo antes de que caduque, la caducidad del nuevo código de acceso pasa de 90 días (Principal) a 30 días (Secundario). La solución alternativa consiste en garantizar la configuración del código de acceso del dispositivo compartido en el GO desde el cual se administran los usuarios. Como administrador, si cambia el código de acceso del dispositivo compartido del usuario final en la pantalla Agregar/Editar usuario de Workspace ONE UEM Console, adoptará correctamente la fecha de caducidad del GO desde el que se administra el usuario final.
Borrar código de acceso	Permite borrar el código de acceso del dispositivo seleccionado. Se solicita un nuevo código de acceso. Esta acción es útil si los usuarios olvidan el código de acceso para el dispositivo y no pueden acceder a sus dispositivos.
Eliminar dispositivo	Permite eliminar el dispositivo del portal de autoservicio.
Eliminar registro	Permite eliminar cualquier informe de inscripción pendiente del portal de autoservicio.
Consultar dispositivo	Permite solicitar que el dispositivo envíe un conjunto completo de información de MDM al servidor de Workspace ONE UEM.

Acción	Descripción
Borrar todo	Permite eliminar todos los datos del dispositivo seleccionado: todos los datos, correos electrónicos, perfiles y capacidades de MDM. El dispositivo se restablece a la configuración predeterminada de fábrica.
Descargar el Hub	Permite descargar e instalar Workspace ONE Intelligent Hub en el dispositivo en el que está viendo el SSP.
Eliminación empresarial	Permite eliminar todos los datos empresariales del dispositivo seleccionado. También se elimina el dispositivo de Workspace ONE UEM. Se eliminarán todos los datos empresariales del dispositivo: los perfiles, las políticas y las aplicaciones internas de MDM. El dispositivo vuelve al estado en el que estaba antes de la instalación de Workspace ONE UEM.
Ubicar dispositivo	Activa la función de GPS para ubicar un dispositivo robado o perdido. Esta acción queda oculta cuando los ajustes de seguridad son restrictivos.
Bloquear dispositivo/pantalla	Permite bloquear el dispositivo seleccionado para que usuarios no autorizados no puedan acceder a él. Esta función es útil en caso de que el dispositivo se pierda o sustraiga. Los usuarios finales también pueden utilizar la función de GPS para localizar el dispositivo.
Bloquear sesión de SSO	Permite bloquear el código de acceso del inicio de sesión único para las aplicaciones que están en el dispositivo. La siguiente aplicación de SSO que se abra solicita un código de acceso.
Hacer ruido	Permite encontrar un dispositivo al hacer que suene de forma remota.
Reenviar mensaje de inscripción	Permite enviar otra copia del correo electrónico, SMS o código QR de la inscripción inicial al dispositivo que se va a registrar. A modo de función de seguridad, la dirección de correo electrónico que aparece en el formulario para volver a enviar el mensaje de inscripción es de solo lectura para las cuentas que se inscribieron con un token.
Enviar mensaje	Permite enviar un mensaje por correo electrónico, notificación telefónica o SMS al dispositivo.
Establecer roaming	Permite determinar si el roaming estará o no habilitado en el dispositivo.
Sincronizar dispositivo	Permite proporcionar a los dispositivos las políticas, contenido y aplicaciones más recientes de la empresa.
Ver mensaje de inscripción	Permite ver el correo electrónico, SMS o código QR concreto que se recibió en el mensaje de inscripción inicial. A modo de función de seguridad, esta acción no está disponible para las cuentas que se inscribieron con un token.

Aviso: Las acciones de registro e inscripción solo se muestran en el SSP cuando la inscripción del

dispositivo está pendiente.

Acciones remotas avanzadas

Las acciones remotas avanzadas aparecen en la pestaña Acciones avanzadas del dispositivo seleccionado en el portal de autoservicio. Las acciones disponibles dependen del estado de inscripción, plataforma de dispositivo y permisos de acciones.

Acción	Descripción
Generar token de la aplicación	Permite generar un token que el dispositivo puede utilizar para acceder a las aplicaciones seguras.
Administrar correo electrónico	Permite administrar dispositivos conectados a una cuenta de correo electrónico.
Revisar los Términos de uso	Permite revisar los términos de uso anteriores de esta cuenta.
Revocar token	Revoca el token para una aplicación seleccionada.
Cargar certificado S/MIME	Permite cargar un certificado S/MIME para una cuenta de correo electrónico corporativa.

Seleccione un dispositivo en el SSP

Después de iniciar sesión en el SSP, la página Mis dispositivos mostrará todos los dispositivos asociados a la cuenta. Cada dispositivo inscrito aparece en su propia pestaña en la parte superior de la página Portal de autoservicio. Seleccione la pestaña que represente el dispositivo que desea ver y administrar.

El estado del dispositivo se muestra debajo del nombre del dispositivo en la pestaña. Los estados pueden ser: Descubierto, Inscrito, Inscripción pendienteNo está inscrito y Eliminación empresarial pendiente.

Cómo agregar un dispositivo en el SSP

Puede agregar un dispositivo directamente desde el portal de autoservicio.

1. Seleccione Agregar dispositivo en la página Mis dispositivos.
2. Complete los cuadros de texto requeridos: Nombre descriptivo, Plataforma, Propiedad del dispositivo y Tipo de mensaje, según corresponda.
3. Seleccione Guardar para agregar el nuevo dispositivo a la cuenta de SSP.

   Aviso: El estado de un dispositivo recién agregado es "Inscripción pendiente" hasta que la inscripción finalice.

Información del dispositivo en el SSP

Cuando el usuario inicia sesión en el SSP, el dispositivo primario aparece en la vista principal. La página principal muestra información básica como la Fecha de inscripción, la Fecha de la última detección y el Estado del dispositivo.

El botón Ir a "Detalles" muestra las pestañas que contienen información sobre el dispositivo que

seleccione de la cuenta del usuario seleccionado.

- Resumen: presenta información resumida sobre Conformidad, Perfiles, Aplicaciones, Contenido, Nombre común, Número de recurso, Número de UDID y dirección MAC de Wi-Fi.
    - El nombre común de un dispositivo puede ser editado directamente desde la pestaña de Resumen al seleccionar el icono de edición a la derecha del cuadro de texto de Nombre común. Aviso: El recurso de Resumen del dispositivo del rol del usuario controla la visibilidad en la pestaña de Resumen del SSP. Si partes específicas de la información están restringidas en la vista del usuario final porque algún recurso esté desactivado (Aplicaciones de dispositivos, Conformidad del dispositivo o Perfiles del dispositivo), la información correspondiente que usualmente aparece en la pestaña Resumen también estará oculta. Para obtener instrucciones detalladas sobre cómo limitar los recursos de las funciones de usuario y administrador, consulte las secciones Cómo crear una nueva función de usuario y Cómo crear una nueva función de administrador en el tema Acceso basado en funciones.
- Conformidad: muestra el estado de conformidad del dispositivo, incluidos el nombre y nivel de todas las políticas de conformidad asignadas al dispositivo.
- Perfiles: muestra todos los perfiles de MDM (incluye los perfiles automáticos) enviados a los dispositivos inscritos en la cuenta de usuario. Esta pestaña también muestra el estado de cada perfil.
- Aplicaciones: muestra todas las aplicaciones instaladas en el dispositivo seleccionado y proporciona información básica de la aplicación.
- Seguridad: muestra información de seguridad general sobre un determinado dispositivo inscrito en su cuenta de usuario.

Medidas de seguridad basadas en token

Como función de seguridad, los siguientes cambios se aplican a las cuentas que se inscriben con un token.

- Tanto la dirección de correo electrónico como el número de teléfono en las pantallas Agregar dispositivo y Cuenta se han convertido a solo lectura.
- La acción Ver mensaje de inscripción no está disponible.

Configuración del programa de mejora del producto

El portal de autoservicio se incluye en el programa de mejora de productos de VMware, que le permite influir en la calidad y eficacia de nuestros productos. Cuando se habilita, este programa comprueba únicamente los datos de facilidad de uso, los cuales son esenciales para garantizar que se satisfacen las necesidades reales de nuestros clientes.

Puede participar en el programa de mejora del producto o abandonarlo en cualquier momento en Grupos y ajustes > Todos los ajustes > Administrador > Programas de mejora de producto.

Para obtener más información sobre este programa, consulte https://resources.workspaceone.com/view/9yfkbk6r2pzldhjlhrz9.

Términos de uso

Puede aplicar los Términos de uso (TOU) en todos los dispositivos administrados dentro de Workspace ONE UEM basado en AirWatch.

Defina y aplique Términos de uso (TOU) para asegurarse de que todos los usuarios con dispositivos administrados están de acuerdo con la política. Si es preciso, los usuarios deben aceptar los TOU antes de continuar con la inscripción, la instalación de aplicaciones o el acceso a la consola de UEM. UEM console permite personalizar totalmente los TOU y asignarlos a cada grupo organizativo y grupo organizativo secundario.

Los términos de uso se muestran durante la inscripción de cada dispositivo. Puede acceder a las siguientes funciones.

- Definir el número de versión.
- Establecer las plataformas que recibirán los términos de uso.
- Notificar a los usuarios por correo electrónico acerca de las actualizaciones de los términos de uso.
- Crear copias de los términos de uso específicas para cada idioma.
- Crear varios términos de uso y asignarlos a los grupos organizativos según la plataforma o el tipo de propiedad.
- Cumplir con las obligaciones legales de distintos grupos personalizando los términos de uso.

Cómo ver la aceptación de los Términos de uso

Puede exigir la aceptación de los Términos de uso si realiza una directiva de conformidad. También puede ver quién aceptó el acuerdo y quién no. De ser necesario, puede ponerse en contacto con esos usuarios de forma directa.

1. Acceda a Grupos y ajustes > Todos los ajustes > Sistema > Términos de uso.
2. Utilice el menú desplegable Tipo para filtrar según el tipo de acuerdo, como, por ejemplo, Inscripción. La columna Usuarios/Dispositivos muestra los dispositivos que han aceptado/no han aceptado/tienen asignados los Términos de uso.
3. Seleccione el número apropiado en la columna Dispositivos para la fila de Términos de uso aplicable y así ver la información del dispositivo que pertenece a ese acuerdo. También puede acceder al menú desplegable para la fila y seleccionar una de las siguientes opciones.

   Ver dispositivos o usuarios: muestra todos los dispositivos y sus estados de aceptación. Puede filtrar por grupo organizativo. Ver las versiones anteriores: permite ver iteraciones anteriores del acuerdo. Ver Términos de uso: permite ver los Términos de uso.

Cómo hacer un seguimiento de los Términos de uso con informes

Puede realizar un seguimiento de la aceptación de los términos de uso por parte de los usuarios.

Puede ver los detalles de grupos organizativos específicos, aceptaciones de la consola y aceptaciones de inscripción de dispositivos. Puede ver las aceptaciones directamente en Workspace ONE UEM Console, o bien exportar el informe en formato XLSX o CSV, ambos visibles en MS Excel.

1. Vaya a Monitor > Informes y análisis > Informes > Vista de lista.
2. Busque y genere el informe de Detalles de la aceptación de los Términos de uso mediante la selección del título del informe.
3. Seleccione los Grupos organizativos.
4. Seleccione el Tipo de Términos de uso.
5. Seleccione el Formato de informe.
6. Seleccione Descargar para guardar el informe.

   VMware Workspace ONE UEM no proporciona texto de ejemplo vinculante jurídicamente. El equipo legal de su empresa debe revisar cualquier ejemplo de texto proporcionado.

Cómo crear Términos de uso para la inscripción

Puede crear un acuerdo sobre los Términos de uso (TOU) específicos de los objetivos de inscripción. Asimismo, puede limitar la distribución de TOU según la plataforma del dispositivo, el tipo de propiedad y el tipo de inscripción.

Puede establecer acuerdos de términos de uso (TOU) específicos para un grupo organizativo. Asegúrese de que esté creando los TOU para el grupo organizativo activo correcto.

1. Acceda a Dispositivos > Configuración del dispositivo > Dispositivos y usuarios > General > Inscripción y seleccione la pestaña Términos de uso.
2. Seleccione el botón Agregar nuevos términos de uso de inscripción y complete las siguientes opciones.

Ajustes	Descripción
Nombre	Introduzca un nombre único para los nuevos TOU.
Tipo	Esta opción se rellena como Inscripción.
Versión	Esta opción se rellena, y se realiza un seguimiento automático de ella, según corresponda.
Plataformas, Propiedad del dispositivo y Tipo de inscripción	Si no desea aplicar un TOU a categorías específicas de dispositivo, no cambie la selección predeterminada Ninguno en estas opciones. Si prefiere especificar una plataforma, la propiedad y la inscripción, puede seleccionar una o varias de estas categorías y definir los límites específicos de sus TOU.

Ajustes	Descripción
	Si elige la opción Plataformas seleccionadas, elija las plataformas que desee cuando aparezca la lista. Sus TOU se aplicarán a las plataformas de dispositivo seleccionadas, excluyendo el resto.
	Si elige la opción Tipos de propiedad seleccionados, deberá seleccionar los tipos de propiedad que desee cuando aparezca la lista. Sus TOU se aplicarán a los tipos de propiedad seleccionados, excluyendo el resto.
	Si elige la opción Tipos de inscripción seleccionados, deberá seleccionar los tipos de inscripción que desee cuando aparezca la lista. Los Términos de uso se aplican a los tipos de inscripción seleccionados, y el resto quedan excluidos.
Notificación	Seleccione esta casilla para enviar un correo electrónico a los usuarios cuando se actualicen los TOU. El correo electrónico de notificación se envía al seleccionar Guardar en el paso 4.
Seleccionar idioma	Con fines de localización, puede agregar términos de uso para cada idioma que necesite seleccionando una opción en el menú desplegable Seleccionar idioma.

3. En el cuadro de texto que aparece, introduzca los TOU personalizados. El editor le proporciona una herramienta básica para escribir con el fin de crear TOU o pegar TOU ya existentes. Para pegar contenido externo, haga clic con el botón derecho del ratón en el cuadro de texto y seleccione Pegar como texto sin formato para evitar errores de formato o HTML.
4. Seleccione Guardar.

Resultados: Puede exigir que se acepten los Términos de uso de MDM creando una política de conformidad para la Aceptación de los Términos de uso de MDM.

Cómo crear Términos de uso para las aplicaciones o la consola

Puede crear Términos de uso (TOU) basados en las aplicaciones para notificar a los usuarios cuándo una aplicación específica recopila datos o cuándo impone restricciones.

Cuando los usuarios ejecutan estas aplicaciones desde el catálogo de aplicaciones empresariales, deben aceptar el acuerdo para poder acceder a la aplicación. Puede configurar TOU para versiones de aplicaciones, crear TOU específicos de un idioma y eliminar aplicaciones si no se aceptan los TOU.

Los TOU para la consola se muestran cuando un administrador inicia sesión en Workspace ONE UEM Console por primera vez. Puede establecer números de versiones de los TOU y crear copias de ellos en idiomas específicos para la consola de UEM. En el caso de las aplicaciones, asigne los TOU cuando esté agregando o editando una aplicación con la pestaña Términos de uso.

1. Acceda a Grupos y ajustes > Todos los ajustes > Sistema > Términos de uso.
2. Seleccione Agregar Términos de uso.
3. Introduzca un Nombre para los Términos de uso y seleccione el Tipo, el cual puede ser Consola o Aplicación.
4. Configure los ajustes del número de Versión y Periodo de gracia, según el Tipo que haya

seleccionado.

5. Introduzca los TOU en el cuadro de texto indicado. El editor le proporciona una herramienta básica para escribir con el fin de crear TOU o pegar TOU ya existentes. Si va a pegar texto de una fuente externa, haga clic con el botón derecho del ratón en el cuadro de texto y seleccione Pegar como texto sin formato para evitar errores de formato o HTML.
6. Seleccione Guardar.

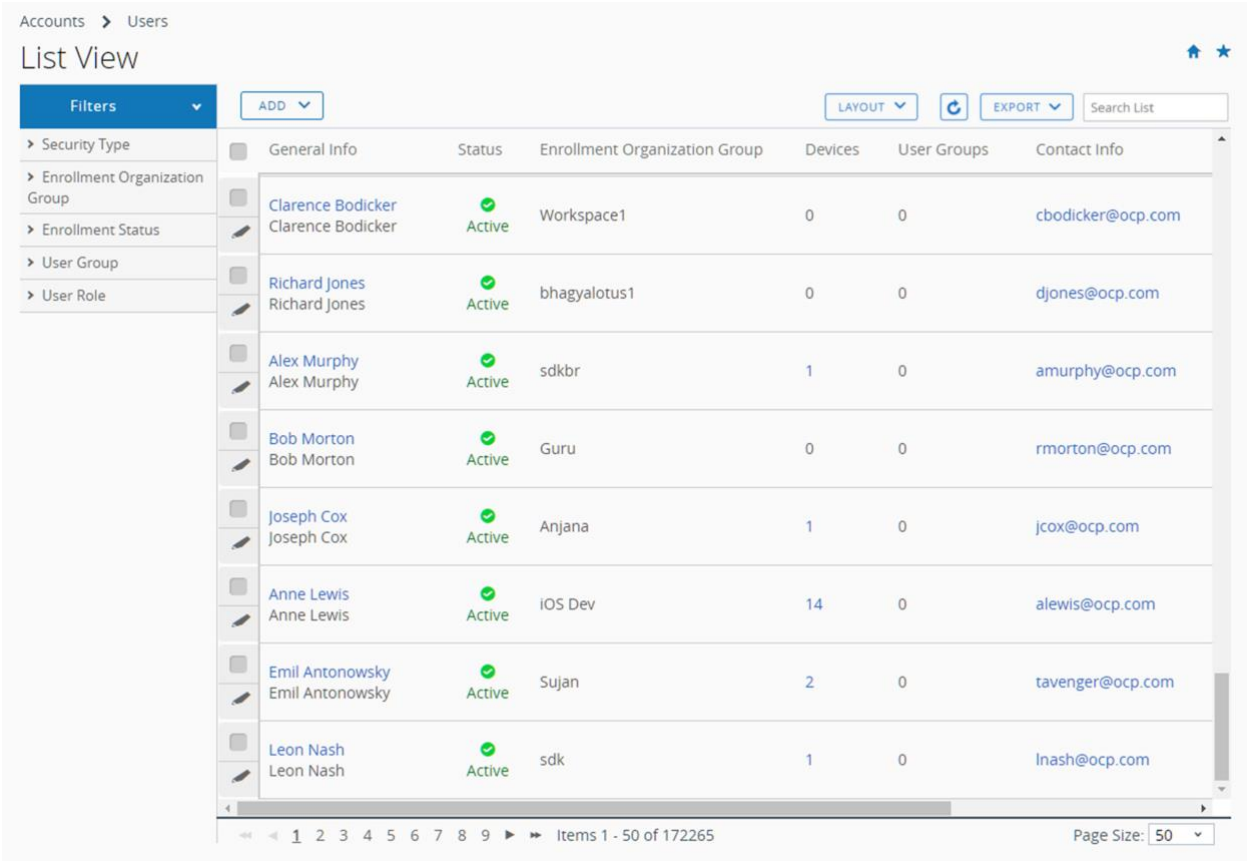
Cuentas administrativas y de usuarios

Para inscribir dispositivos en Workspace ONE Express y Workspace ONE UEM, debe crear e integrar cuentas de usuario. Del mismo modo, también debe crear cuentas administrativas para que los administradores puedan administrar usuarios y dispositivos fácilmente.

Vista de lista de cuentas de usuario

La consola permite establecer una infraestructura administrativa y de usuario completa. Ofrece opciones de configuración para disponer de autenticación, integración empresarial y mantenimiento constante.

La página Vista de lista, que puede ver si accede a Cuentas > Usuarios > Vista de lista, ofrece herramientas útiles para el mantenimiento regular de la cuenta de usuario de Workspace ONE UEM.



Cómo personalizar la Vista de lista

Puede utilizar la Vista de lista de las cuentas de usuario para crear listas personalizadas de los usuarios de forma inmediata. También puede personalizar el diseño de la pantalla según los criterios que considere más importantes. Podrá exportar esta lista personalizada para realizar un análisis más

adelante y agregar nuevos usuarios de forma individual o en masa.

Acción	Descripción
Filtros	Para ver solo los usuarios deseados, utilice los siguientes filtros. Tipo de seguridad Grupo organizativo de inscripción Estado de inscripción Grupo de usuarios Función de usuario Estado
Botón Agregar	Agregar usuario: permite agregar una única cuenta de usuario básica. Agregue un empleado o un empleado recién ascendido que necesite acceso a las capacidades de MDM. Importar por lotes: agregue varios usuarios a Workspace ONE mediante la importación de un archivo de valores separados por comas (CSV). Escriba un nombre y una descripción únicos para agrupar y organizar varios usuarios a la vez. Para obtener más información, consulte la sección Importación por lotes de usuarios y dispositivos en la Función Importar por lotes.
Botón Diseño	Permite personalizar todo el diseño de las columnas. Resumen: puede consultar la Vista de lista con columnas y los ajustes de vista predeterminados. Personalizado: permite seleccionar solamente las columnas de la Vista de lista que se deseen ver. También puede aplicar las columnas seleccionadas a todos los administradores que se encuentren en el grupo organizativo actual o por debajo de este.
Ordenar	La mayoría de las columnas de la Vista de lista (en el diseño de Resumen y Personalizado) pueden ordenarse por temas como Dispositivos, Grupos de usuarios y Grupo organizativo para la inscripción.
Botón Exportar	Permite guardar un archivo XLSX o CSV (valores separados por comas) de toda la Vista de lista de usuarios para poder verlo y analizarlo con Microsoft Excel. Si ha aplicado un filtro a la Vista de lista de usuarios, la lista exportada reflejará los resultados del filtro. Seleccione el botón Exportar, seleccione el formato (XLSX o CSV) y, a continuación, navegue a Supervisión > Informes y análisis > Exportaciones para ver y descargar el informe resultante.

Cómo interactuar con cuentas de usuario

La vista de lista también tiene una casilla a la izquierda de cada cuenta de usuario. Para ver los detalles de los usuarios, seleccione el nombre de usuario del hipertexto de la columna Información general.

El icono Editar  permite realizar cambios básicos en la cuenta de usuario. Al seleccionar una sola casilla, aparecerán tres botones de acción: Enviar mensaje, Agregar dispositivo y Más acciones.

Puede seleccionar varias cuentas de usuario mediante esta casilla, lo que a su vez modifica las acciones disponibles.

Acción	Descripción
Enviar mensaje	Permite proporcionar ayuda inmediata a un dispositivo único o a un grupo de usuarios. Envíe un correo electrónico para la activación del usuario (a través de la plantilla de usuarios) para notificar al usuario sus credenciales de inscripción.

Acción	Descripción
Agregar dispositivo	Agregue un dispositivo para el usuario seleccionado. Disponible solamente para las selecciones de usuarios únicos.
Más acciones	Visualice las siguientes acciones.
Agregar a grupo de usuarios	Permite agregar los usuarios seleccionados a un grupo de usuarios nuevo o existente para simplificar la administración. Para obtener más información, consulte las secciones tituladas Vista de lista de los grupos de usuarios y Editar los permisos de los grupos de usuarios en Grupos de usuarios.
Eliminar del grupo de usuarios	Permite eliminar a los usuarios seleccionados del grupo de usuarios existente.
Cambiar grupo organizativo	Traslade los usuarios de forma manual a un grupo organizativo diferente. Además, permite actualizar el contenido disponible, al igual que los permisos y las restricciones de los usuarios si estos cambian de puesto, reciben un ascenso o se mudan a otra ubicación.
Eliminar	Si un miembro de la organización es despedido de forma permanente, puede eliminar su cuenta de usuario rápidamente. Eliminar la información de la cuenta es igual que si la cuenta nunca hubiera existido. No se puede reactivar una cuenta eliminada. Si el propietario de una cuenta eliminada vuelve, hay que crearle una cuenta nueva.
Activación	Permite activar una cuenta previamente desactivada si el usuario regresa a la organización o necesita volver a la empresa.
Desactivar	La desactivación es una medida de seguridad. La desactivación se utiliza cuando un usuario está desaparecido en combate, su dispositivo no cumple las normas, se ha perdido o ha sido robado. Workspace ONE UEM retiene toda la información de una cuenta desactivada, como el nombre, la dirección de correo electrónico, la contraseña, el grupo organizativo de inscripción, etc. Una cuenta desactivada significa que los usuarios con credenciales de cuenta desactivada no puede iniciar sesión. Podrá activar la cuenta una vez que se resuelva el problema de seguridad (se encuentre el usuario, el dispositivo se vuelva conforme, el dispositivo se recupere).

Migrar usuarios con la herramienta de migración

La herramienta de migración de usuarios corrige los errores en el proceso de sincronización del grupo de usuarios, así como los flujos de trabajo no controlados y los errores de migración de la base de datos.

Solo puede ejecutar la herramienta de migración de usuarios en grupos organizativos (GO) que estén configurados con el protocolo ligero de acceso a directorios (Lightweight Directory Access Protocol, LDAP). Debe cambiar a un GO que esté sincronizado con LDAP o configurar el GO sin LDAP. Seleccione el vínculo Configurar en el GO configurado sin LDAP para abrir la página

Configuración del sistema de servicios de directorio.

Para obtener más información sobre cómo configurar los servicios de directorio, incluido LDAP, ya sea a través del asistente o manualmente, consulte Configuración de servicios de directorio.

Aviso: Debe utilizar la consola de Active Directory para migrar usuarios de un dominio secundario a otro. Esta migración no solo cambia el dominio del usuario, sino también el *nombre distintivo* del usuario. Al completar las opciones de migración en la consola de Active Directory, debe habilitar la casilla Migrar grupos de usuarios asociados. Debe realizar estos pasos antes de utilizar la herramienta de migración de usuarios.

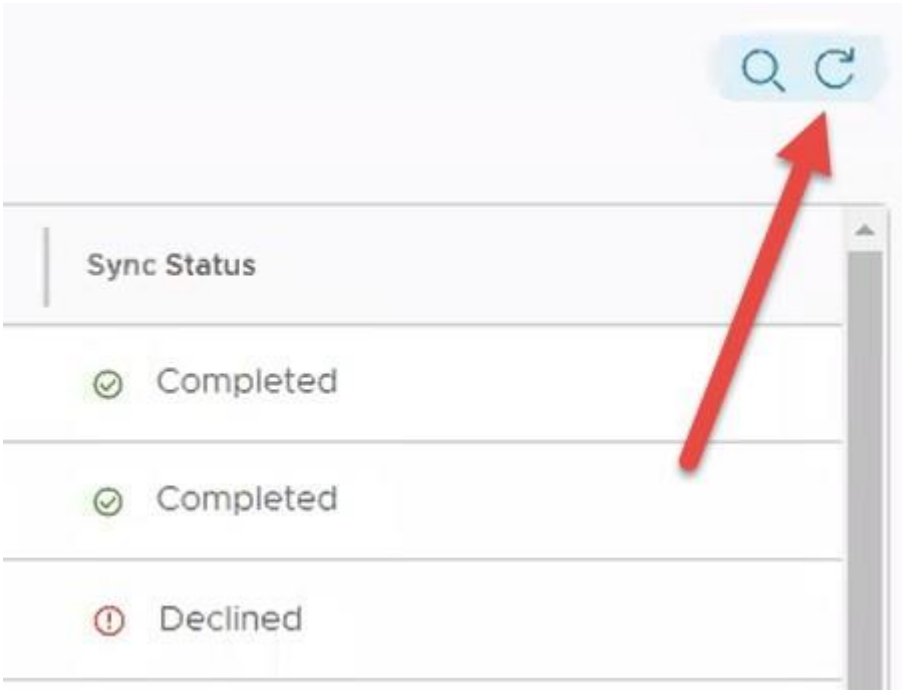
Realice los siguientes pasos para utilizar la herramienta de migración de usuarios.

1. Asegúrese de estar en un GO que esté configurado con LDAP y de haber seguido la nota anterior; a continuación, vaya a Cuentas > Sincronización de LDAP.
2. Seleccione el botón Agregar sincronización de LDAP. Se mostrará la pantalla Sincronización de LDAP. Realice los siguientes ajustes.

Ajustes	Descripción
Usuarios	Seleccione una opción de migración para los usuarios en este GO: Todos o Seleccionar.
Usar ID externo	Esta opción está desactivada de forma predeterminada, lo que significa que los usuarios se sincronizan con LDAP en función de su UserDN (nombre de dominio). Si habilita esta opción, los usuarios se sincronizarán con LDAP en función del ID externo, en lugar del nombre de dominio.
Usuario de inscripción	Esta opción solo está visible cuando la opción Seleccionar anterior está habilitada en Usuarios. Utilice este cuadro de texto para buscar usuarios. Cuando la búsqueda devuelva una coincidencia como un elemento del menú desplegable, selecciónelo para agregar el nombre de usuario a la Vista de lista de usuarios.
Tipo de actualización	Seleccione el método de actualización de atributos. Puede seleccionar ambos. Actualice todos los atributos en función del UserDN (nombre de dominio). Seleccione esta opción si Usar ID externo está desactivado. Actualice todos los atributos en función de la GUID de objetos. Seleccione esta opción si Usar ID externo está habilitado.
Vista de lista de usuarios	Esta opción solo está visible cuando la opción Seleccionar anterior está habilitada en Usuarios. A medida que agrega más usuarios de inscripción para migrar, esta vista de lista se amplía. Para eliminar usuarios de esta lista, selecciónelos en la lista y seleccione el botón Eliminar.

3. Seleccione el botón Iniciar para finalizar el trabajo de sincronización y agregar el trabajo a la vista de lista.
4. Cada trabajo que se agrega a la lista Sincronización de LDAP aparece en la lista con el Estado de sincronización como Aprobación pendiente. Debe aprobar, aprobar parcialmente o rechazar el trabajo.

5. Seleccione los "puntos suspensivos verticales" que aparecen a la izquierda de cada lista de trabajo y seleccione una de las siguientes opciones.
    1. Aprobar: permite aprobar y procesar el trabajo de migración de usuarios. Debe confirmar la aprobación.
    2. Aprobar parcialmente: al seleccionar esta opción, se muestra el trabajo de aprobación pendiente en una pantalla emergente en la que puede seleccionar usuarios individuales para su aprobación. Esta opción puede ser útil cuando quiere excluir algunos usuarios del GO de la aprobación para la migración. Para ello, seleccione la casilla Todos los usuarios a la izquierda del encabezado Nombre de usuario. Al seleccionar esta casilla de verificación, se seleccionan todos los usuarios de todo el trabajo. A continuación, desplácese por la lista y anule la selección de los usuarios individuales que desea *excluir* de la migración. Seleccione el botón Aprobar. A continuación, debe confirmar la aprobación.
    3. Rechazar: rechaza el trabajo de migración del usuario. Debe confirmar el rechazo el trabajo de sincronización.
6. La lista Sincronización de LDAP actualiza la columna Estado de sincronización con cada opción de aprobación que seleccione. Puede actualizar manualmente la lista seleccionando el icono Actualizar.



Tipos de autenticación de usuario

Antes de inscribir dispositivos, cada usuario de dispositivo debe tener una cuenta de usuario autenticada reconocida por Workspace ONE UEM. El tipo de autenticación de usuario que elija dependerá de las necesidades de su organización.

Proxy de autenticación

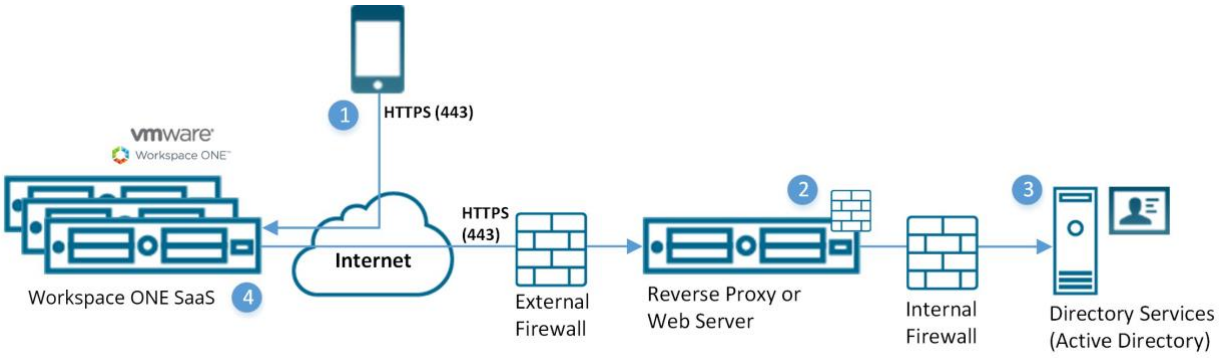
El proxy de autenticación permite integrar los servicios de directorio en la nube o en redes internas protegidas. En este modelo, el servidor de Workspace ONE UEM se comunica con un servidor web accesible al público o con un servidor de Exchange ActiveSync. Este proceso autentica a los usuarios ante el controlador de dominio.

VENTAJAS

- Método seguro para la integración de proxy con AD/LDAP en la nube.
- Los usuarios finales se autentican con las credenciales corporativas existentes.
- El módulo ligero requiere una configuración mínima.

DESVENTAJAS

- Requiere un servidor web público o un servidor de Exchange ActiveSync ligado un servidor de AD/LDAP.
- Solo es factible para ciertos diseños de arquitectura.
- Es una solución menos robusta que VMware Enterprise Systems Connector.
- No puede utilizarse para la inscripción directa de Workspace ONE.



1. El dispositivo se conecta a Workspace ONE UEM para inscribir el dispositivo. El usuario introduce su nombre de usuario y contraseña de los servicios de directorio.
    - Nombre de usuario y contraseña cifrados durante el transporte.
    - Workspace ONE UEM no almacena la contraseña de los servicios de directorio del usuario.
2. Workspace ONE UEM retransmite el nombre de usuario y la contraseña a un extremo de proxy de autenticación configurado que requiere autenticación (por ejemplo, autenticación básica).
3. Las credenciales del usuario se validan con los servicios de directorio corporativos.
4. Si las credenciales del usuario son válidas, el servidor de Workspace ONE UEM inscribe el dispositivo.

Autenticación de Active Directory con LDAP y VMware Enterprise Systems Connector

La autenticación de Active Directory con LDAP y VMware Enterprise Systems Connector ofrece la misma funcionalidad que la autenticación de AD y LDAP tradicional. Este modelo funciona en toda la nube para las implementaciones de software como servicio (SaaS).

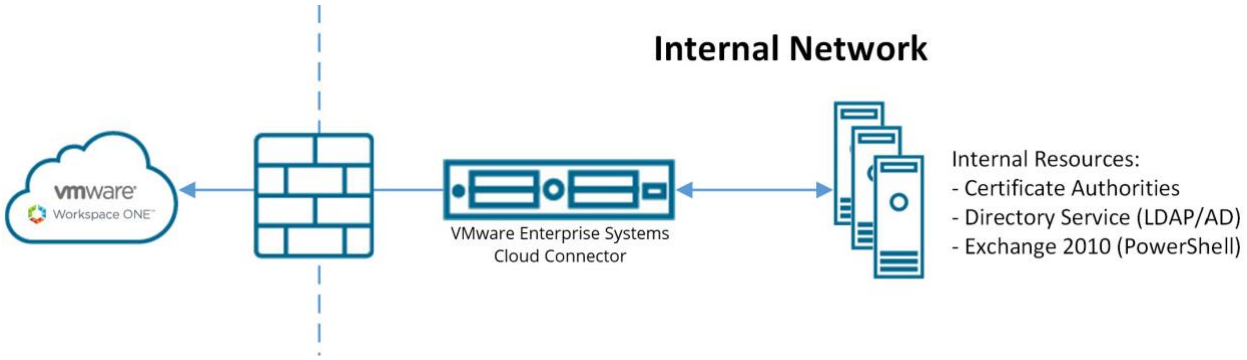
VENTAJAS

- Los usuarios finales pueden autenticarse con credenciales corporativas existentes.
- No es necesario realizar cambios de firewall, ya que la comunicación se inicia desde VMware Enterprise Systems Connector dentro de su red.
- La transmisión de credenciales se cifra de forma segura.
- Ofrece una configuración segura para otras infraestructuras, como los servidores de BES, Microsoft ADCS, SCEP y SMTP.
- Compatible con la inscripción directa de Workspace ONE™.

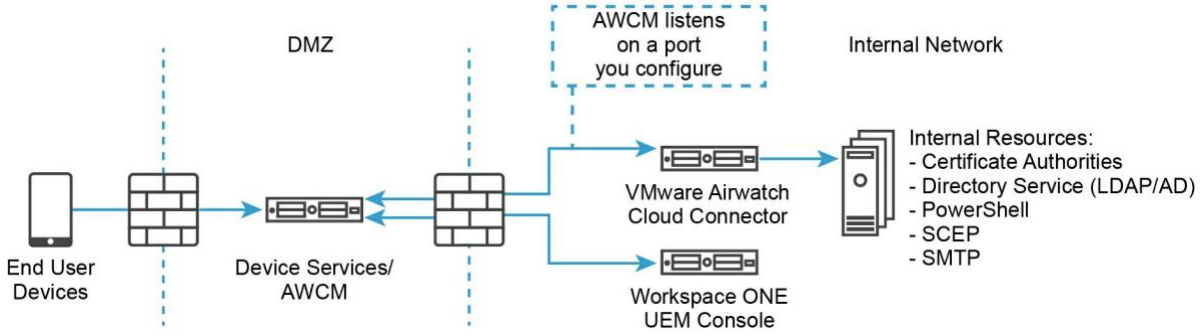
DESVENTAJAS

- Requiere la instalación de VMware Enterprise Systems Connector detrás del firewall o en un DMZ.
- Se requiere una configuración adicional.

Modelo de implementación de SaaS



Modelo de implementación en la sede



Autenticación SAML 2.0

La autenticación de lenguaje de marcado de aserción de seguridad (SAML) 2.0 ofrece soporte para el inicio de sesión único y la autenticación federada. Workspace ONE UEM nunca recibe credenciales corporativas.

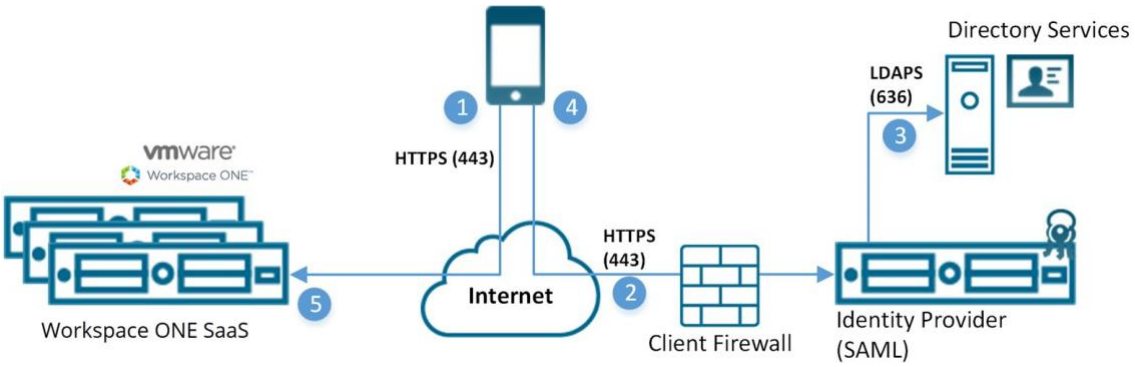
Si una organización tiene un servidor de proveedor de identidad de SAML, utilice la integración con SAML 2.0. Asegúrese de que el proveedor de identidad devuelve el atributo `objectGUID` como parte de la respuesta SAML.

VENTAJAS

- Ofrece capacidades de inicio de sesión único.
- Autenticación con las credenciales corporativas existentes.
- Workspace ONE UEM nunca recibe credenciales corporativas en texto sin formato.
- Compatible con la inscripción directa de Workspace ONE cuando se empareja con un usuario de directorio SAML.
- Solo los administradores pueden utilizar entornos de varios dominios.

DESVENTAJAS

- Requiere una infraestructura de proveedor de identidad de SAML.
- Incompatible con la inscripción directa de Workspace ONE cuando se empareja con un usuario básico de SAML.
- La configuración de SAML con Workspace ONE Access como IDP con la función Usuario básico local habilitada no admite la autenticación de usuarios básicos.



1. El dispositivo se conecta a Workspace ONE UEM para la inscripción. El servidor de UEM, a continuación, dirige el dispositivo al proveedor de identidad especificado por el cliente.
2. El dispositivo se conecta de forma segura a través de HTTPS al proveedor de identidad cliente especificado y el usuario introduce sus credenciales.
    - Credenciales cifradas durante el transporte directamente entre el dispositivo y el endpoint de SAML.
3. Las credenciales se validan con los servicios de directorio.
4. El proveedor de identidad devuelve una respuesta SAML firmada con el nombre de usuario autenticado.
5. El dispositivo vuelve a responder al servidor de Workspace ONE UEM y presenta el mensaje SAML firmado. El usuario se autentica. Para obtener más información, consulte Configurar servicios de directorio manualmente y desplácese hasta la sección SAML.

- Las aplicaciones SaaS no están disponibles para los administradores de SAML que se autentican mediante Workspace ONE Access.

Funcionalidad de la aplicación SaaS para administradores de SAML

Las aplicaciones SaaS, así como otras funciones y políticas de Workspace ONE Access, no están disponibles si se trata de un administrador de SAML que se autentica mediante Workspace ONE Access. Observará el siguiente mensaje de error cuando se desplace hasta la página de las aplicaciones SaaS.

Compruebe que su cuenta de administrador existe en los sistemas UEM e IDM y que el dominio de Workspace ONE UEM coincide exactamente con el dominio de la misma cuenta en VMware Identity Manager.

Para restaurar la accesibilidad de la aplicación SaaS, debe iniciar sesión en Workspace ONE UEM mediante una autenticación básica y también debe habilitar Workspace ONE Access en el grupo organizativo.

Autenticación basada en tokens

La autenticación basada en tokens es la manera más fácil para que el usuario inscriba el dispositivo. Con esta configuración de inscripción, Workspace ONE UEM genera un token, que se coloca en la

dirección URL de inscripción.

Para una autenticación de token único, el usuario accede al enlace desde el dispositivo para completar la inscripción y el servidor de Workspace ONE UEM hace referencia al token proporcionado al usuario.

Para aumentar la seguridad, configure una hora de caducidad (en horas) para cada token. De este modo se minimizará el riesgo de que otro usuario obtenga acceso a cualquier información o funciones disponibles en dicho dispositivo.

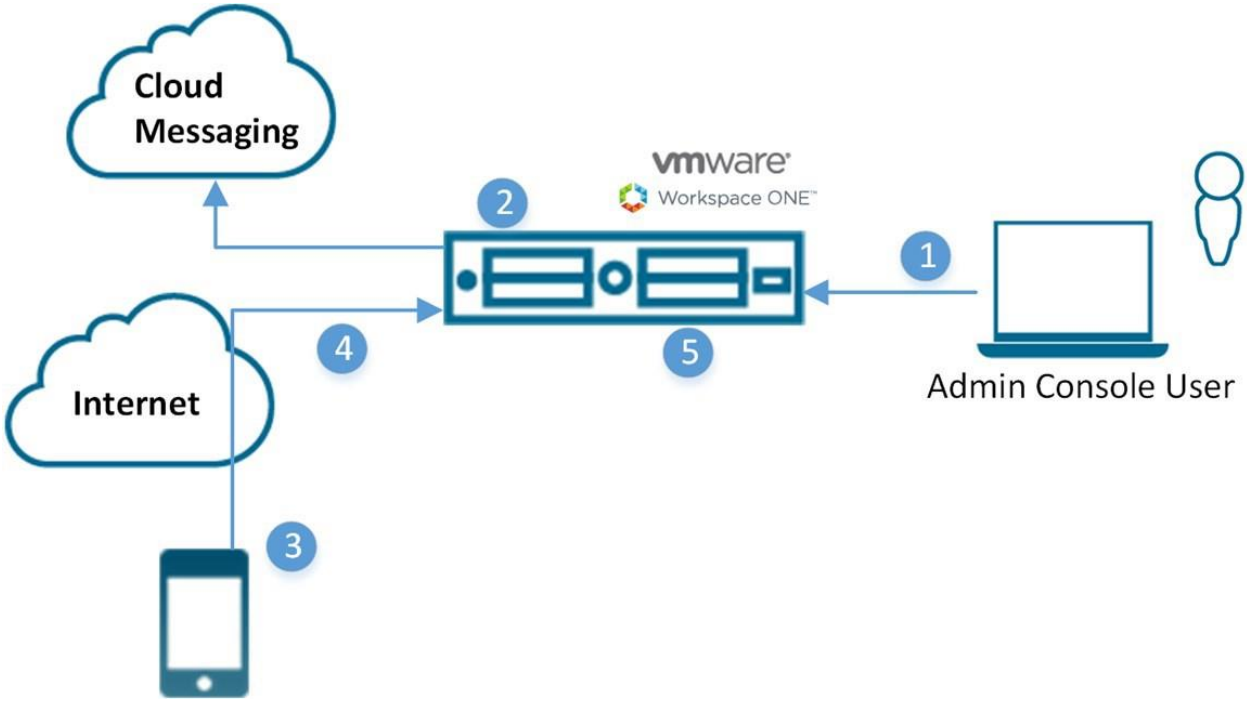
También puede decidir implementar una autorización de dos factores para ir un poco más allá en la verificación de identidad de usuario final. Con este ajuste de autenticación, el usuario debe introducir su nombre de usuario y contraseña tras acceder al enlace de la inscripción, que contiene el token de autorización.

VENTAJAS

- Requiere poco esfuerzo por parte del usuario final a la hora de inscribir y autenticar el dispositivo.
- Protege el uso del token al establecer una hora de caducidad.
- El usuario no necesita credenciales para la autenticación de token único.

DESVENTAJAS

- Se requiere una integración de protocolo simple de transferencia de correo (SMTP) o de servicio de mensajes cortos (SMS) para enviar tokens al dispositivo.



1. El administrador autoriza el registro de dispositivos de usuario.
2. Se genera un token de un solo uso, que se envía al usuario desde Workspace ONE UEM.
3. El usuario recibe el token y accede a la dirección URL de inscripción. Se solicita al usuario que indique el token y, opcionalmente, una autenticación de dos factores.
4. Proceso de inscripción de dispositivos.

5. Workspace ONE UEM marca el token como caducado.

Aviso: Las implementaciones SaaS incluyen SMTP.

Cómo habilitar los tipos de seguridad para la inscripción

Una vez que Workspace ONE UEM se integra con un tipo de seguridad de usuario seleccionado y antes de la inscripción, habilite cada modo de autenticación que tenga previsto permitir.

1. Vaya a Dispositivos > Ajustes de dispositivos > Dispositivos y usuarios > General > Inscripción en la pestaña Autenticación.
2. Seleccione las casillas de verificación correspondientes para el ajuste Modo de autenticación.

Ajustes	Descripción
Agregar dominio de correo electrónico	Este botón se usa para configurar el servicio de detección automática y registrar los dominios de correo electrónico en su entorno.
Modo(s) de autenticación	Seleccione los tipos de autenticación permitidos: * Básica: se pueden inscribir cuentas de usuario básicas (creadas manualmente en UEM Console). * Directorio: se pueden inscribir las cuentas de usuario de directorio (aquellas que se han importado o permitido mediante la integración del servicio de directorio). La inscripción directa de Workspace ONE es compatible con los usuarios de directorio con o sin SAML. * Proxy de autenticación: permite a los usuarios inscribirse utilizando las cuentas de usuario del proxy de autenticación. Los usuarios se autentican en un extremo web. Introduzca la URL del Proxy de autenticación, Copia de seguridad de la URL del Proxy de autenticación y Tipo de método de autenticación (elija entre HTTP básico y Exchange ActiveSync).
Origen de la autenticación para Intelligent Hub	Seleccione el sistema que el servicio de Intelligent Hub utiliza como origen para los usuarios y las políticas de autenticación. * Workspace ONE UEM: seleccione esta opción si desea que los servicios de Hub utilicen Workspace ONE UEM como el origen de las políticas de usuarios y de autenticación. Cuando configura la página Configuración de Hub para los servicios de Hub, introduce la dirección URL de arrendatario de servicios de Hub. * Workspace ONE Access: seleccione esta opción si desea que los servicios de Hub utilicen Workspace ONE Access como el origen de las políticas de usuarios y de autenticación. Al configurar la página Configuración de Hub para los servicios de Hub, introduzca la URL del tenant de Workspace ONE Access. Aviso: Si habilita Workspace ONE Access como origen de autenticación para Intelligent Hub y utiliza una línea de comandos para la inscripción con fines de inscripción provisional, esta configuración se omite en favor de las credenciales proporcionadas en la línea de comandos. Para obtener más información sobre Workspace ONE Intelligent Hub, consulte la documentación de servicios de Hub de VMware Workspace ONE. Para obtener más información sobre Workspace ONE Access, consulte la documentación de VMware Workspace ONE Access.

Ajustes	Descripción
Modo de inscripción de dispositivos	Seleccione el modo de inscripción de dispositivos que prefiera: * Inscripción abierta: permite la inscripción de prácticamente cualquier persona que cumpla los demás criterios de inscripción (modo de autenticación, restricciones y demás). La inscripción directa de Workspace ONE es compatible con la inscripción abierta. * Solo dispositivos registrados: solo permite la inscripción de usuarios con dispositivos registrados por ellos o por usted. El registro del dispositivo es el proceso de agregar dispositivos corporativos a la consola de UEM antes de que se inscriban. La inscripción directa de Workspace ONE es compatible únicamente con permitir la inscripción de los dispositivos registrados pero solo si no se necesitan tokens de registro.
Requerir token de registro	Solo es visible si la opción Dispositivos registrados solamente está seleccionada. Si restringe la inscripción únicamente a los dispositivos registrados, también tendrá la opción de requerir un token de registro para la inscripción. Esta opción mejora la seguridad al confirmar que un usuario concreto está autorizado para inscribirse. Puede enviar un correo electrónico o mensaje SMS con el token de inscripción adjunto a usuarios con cuentas de Workspace ONE UEM.
Requerir la inscripción del Intelligent Hub para iOS	Seleccione esta casilla de verificación para exigir que los usuarios de dispositivos iOS descarguen e instalen Workspace ONE Intelligent Hub antes de inscribirse. Si está desactivada, la inscripción en Web está disponible.
Requerir la inscripción de Intelligent Hub para macOS	Seleccione esta casilla de verificación para exigir que los usuarios de dispositivos macOS descarguen e instalen Workspace ONE Intelligent Hub antes de poder inscribirse. Si está desactivada, la inscripción en Web está disponible.

3. Seleccione Guardar.

Autenticación de usuario básica

Puede utilizar la autenticación básica para identificar a usuarios en la arquitectura de Workspace ONE UEM, pero este método no ofrece integración con las cuentas corporativas de usuarios.

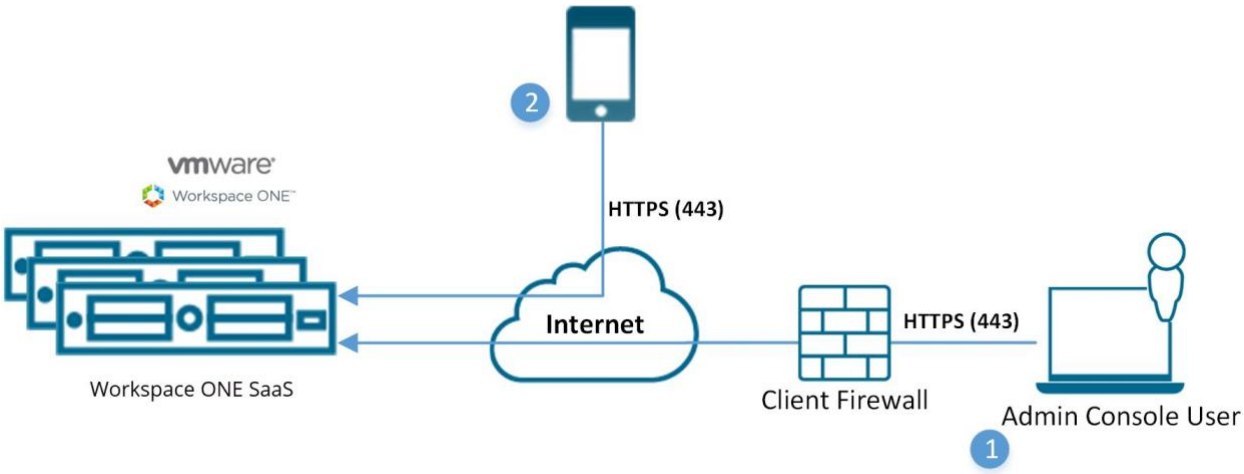
VENTAJAS

- Compatible con cualquier método de implementación.
- No requiere una integración técnica.
- No requiere una infraestructura empresarial.

DESVENTAJAS

- Compatible con la detección automática.
- Las credenciales existen solamente en Workspace ONE UEM y no coinciden necesariamente con las credenciales corporativas existentes.
- Tampoco ofrece seguridad ni inicio de sesión único federados.

- Workspace ONE UEM almacena todos los nombres de usuario y las contraseñas,
- Incompatible con la inscripción directa de Workspace ONE.



1. El usuario de la consola inicia sesión en la solución de software como servicio Workspace ONE UEM utilizando una cuenta local para la autenticación (autenticación básica).
    - Las credenciales se cifran durante el transporte.
    - (Por ejemplo, nombre de usuario: juanperez@air-watch.com, contraseña: Abcd).
2. El usuario inscribe el dispositivo utilizando las credenciales de su cuenta local de Workspace ONE UEM (autenticación básica).
    - Las credenciales se cifran durante el transporte.
    - (Por ejemplo, nombre de usuario: juanperez2, contraseña: 2557).

Autenticación de Active Directory con LDAP

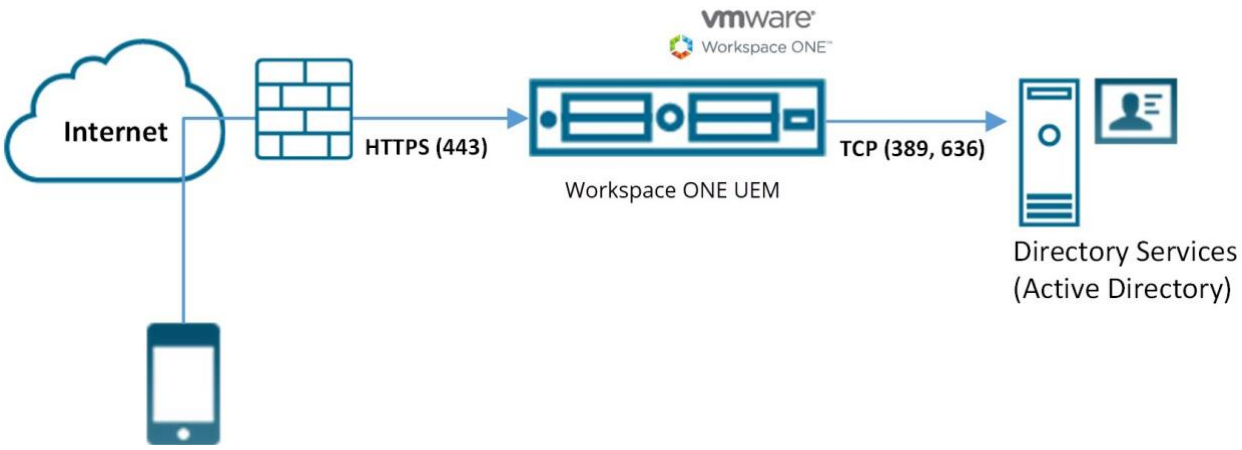
La autenticación de Active Directory (AD) con el protocolo ligero de acceso a directorios (LDAP) se utiliza para integrar cuentas de usuarios y administrativas de Workspace ONE UEM con las cuentas corporativas existentes.

VENTAJAS

- Ahora, los usuarios finales pueden autenticarse utilizando credenciales corporativas existentes.
- Es un método seguro para la integración con LDAP/AD.
- Es una práctica de integración estándar.
- Compatible con la inscripción directa de Workspace ONE.

DESVENTAJAS

- Se requiere AD u otro servidor LDAP.



1. El dispositivo se conecta a Workspace ONE UEM para inscribir el dispositivo. El usuario introduce su nombre de usuario y contraseña de los servicios de directorio.
    - El nombre de usuario y la contraseña se cifran durante el transporte.
    - Workspace ONE UEM no almacena la contraseña de los servicios de directorio del usuario.
2. Workspace ONE UEM realiza consultas a los servicios de directorio del cliente mediante un protocolo LDAP seguro a través de Internet utilizando una cuenta de servicio para la autenticación.
3. Las credenciales del usuario se validan con el servicio de directorio corporativo.
4. Si las credenciales del usuario son válidas, el servidor de Workspace ONE UEM inscribe el dispositivo.

Cuentas de usuario básicas

Cree cuentas de usuario básicas para sus usuarios finales si no está realizando la integración de un servicio de directorio con Workspace ONE UEM. Puede crear cuentas básicas rápidamente y desecharlas fácilmente, lo que las hace útiles para realizar pruebas.

Ventajas

- Puede utilizarse con cualquier método de implementación.
- No requiere una integración técnica.
- No requiere una infraestructura empresarial.
- Puede inscribirse en varios grupos organizativos.

Desventajas

- Las credenciales existen solamente en Workspace ONE UEM y no coinciden necesariamente con las credenciales corporativas existentes.
- No ofrecen seguridad federada.
- No admiten el inicio de sesión único.
- Workspace ONE UEM almacena todos los nombres de usuario y las contraseñas,

- y no puede utilizarse para la inscripción directa de Workspace ONE.

Cómo crear cuentas de usuario básicas

Puede crear cuentas de usuario básicas para que los usuarios se autentiquen e inicien sesión en el sistema de Workspace ONE UEM. A continuación, puede enviar a los usuarios básicos una notificación con las instrucciones sobre cómo activar la cuenta, incluido un enlace para restablecer la contraseña, que caduca en 24 horas.

Este tema detalla cómo crear cuentas de usuario una a una. Para crear cuentas de usuario en masa, consulte la sección titulada Importación por lotes de usuarios y dispositivos en Función Importar por lotes

1. Acceda a Cuentas > Usuarios > Vista de lista, seleccione Agregar y, a continuación, Agregar usuario. Se mostrará la página Agregar/Editar usuario.
2. En la pestaña General, realice los siguientes ajustes para agregar un usuario básico.

Ajustes	Descripción
Tipo de seguridad	Seleccione Básico para agregar un usuario básico.
Nombre de usuario	Introduzca un nombre de usuario que el usuario final del dispositivo utilizará para iniciar sesión.
Contraseña	Introduzca la contraseña que el usuario puede utilizar para iniciar sesión.
Confirmar contraseña	Confirme la contraseña.
Nombre completo	Escriba el Nombre, Segundo nombre y Apellido del usuario.
Nombre de la pantalla	Introduzca un nombre que represente al usuario en la consola de UEM.
Dirección de correo electrónico	Permite introducir o editar la dirección de correo electrónico del usuario.
Nombre de usuario de correo electrónico	Permite introducir o editar el nombre de usuario de correo electrónico del usuario.
Dominio	Permite seleccionar el dominio del correo electrónico desde el ajuste desplegable.
Número telefónico	Permite introducir el número de teléfono del usuario, incluidos el signo más, el código de país y el código de área. Esta opción es obligatoria si desea utilizar SMS para enviar notificaciones.
Inscripción	
Grupo organizativo para la inscripción	Seleccione el grupo organizativo en el que se inscribirá el usuario.
Permiso para que el usuario se inscriba en grupos organizativos adicionales	Puede permitir al usuario inscribirse en más de un grupo organizativo. Si habilita esta opción pero deja en blanco Grupos organizativos adicionales, cualquier GO secundario del Grupo organizativo de inscripción podrá utilizarse como punto de inscripción.

Ajustes	Descripción
Grupos organizativos adicionales	Este ajuste solo aparece cuando la opción para permitir que el usuario se inscriba en grupos organizativos adicionales está habilitada. Esta opción permite agregar grupos organizativos adicionales desde los que se puede inscribir su usuario básico.
Rol de usuario	En el ajuste desplegable, seleccione el rol del usuario que está agregando.
Notificación	
Tipo de mensaje	Seleccione el tipo de mensaje que desee enviar al usuario: Correo electrónico, SMS o Ninguno. Para seleccionar un SMS, se requiere una entrada válida en la opción Número de teléfono.
Plantilla de mensaje	El usuario básico activa su cuenta con esta notificación. Por motivos de seguridad, no se incluye la contraseña del usuario en esta notificación. En su lugar, la notificación incluye un vínculo para restablecer la contraseña. Este enlace para restablecer la contraseña caduca automáticamente después de 24 horas.

Seleccione la plantilla para los mensajes de correo electrónico o SMS mediante la selección de una de estas opciones en el ajuste desplegable. También puede seleccionar Vista previa del mensaje para ver una vista previa de la plantilla y, a continuación, seleccionar Configurar las plantillas de los mensajes para crear una nueva.

3. También puede seleccionar la pestaña Avanzado y realizar los siguientes ajustes.

Ajustes	Descripción
Sección de información avanzada	
Contraseña del correo electrónico	Introduzca la contraseña del correo electrónico del usuario que está agregando.
Confirmar la contraseña del correo electrónico	Confirme la contraseña del correo electrónico del usuario que está agregando.
Nombre principal de usuario	Introduzca el nombre principal del usuario básico. Este ajuste es opcional.
Categoría	Seleccione la categoría de usuario para el usuario que se está agregando.
Departamento	Introduzca el departamento del usuario para fines administrativos.
ID de empleado	Introduzca el ID de empleado del usuario para fines administrativos.
Centro de costos	Introduzca el centro de coste del usuario para fines administrativos.
Sección de certificados	

Ajustes	Descripción
Utilizar S/MIME	Habilite o desactive las extensiones seguras multipropósito al correo desactivar Internet (S/MIME). Si está habilitada esta opción, debe tener un perfil habilitado por S/MIME y, luego, cargar un certificado S/MIME mediante la selección del botón Cargar.
Certificado de cifrado separado	Habilitar o desactivar el certificado de cifrado. Si está habilitada esta opción, debe cargar un certificado de cifrado con la función Cargar. Generalmente, el mismo certificado S/MIME se utiliza para firmar y cifrar, a menos que se esté utilizando otro certificado expresamente.
Certificado de cifrado antiguo	Habilite o desactive un certificado de cifrado de versión heredada. Si está habilitada esta opción, debe Cargar un certificado cifrado.
Sección Inscripción preparada	
Habilitar la inscripción preparada	Permite habilitar o desactivar la inscripción provisional de los dispositivos.

Si está habilitada esta opción, debe seleccionar entre Dispositivos de usuario único y Dispositivos de múltiples usuarios. Si selecciona Dispositivos de usuario único, debe elegir entre Estándar (los propios usuarios inician sesión) y Avanzado (el dispositivo se inscribe en nombre de otro usuario).

Consulte la sección Inscripción preparada para más información.

4. Seleccione Guardar para guardar solamente el usuario nuevo o seleccione Guardar y agregar dispositivo para guardar el usuario nuevo y continuar a la página Agregar dispositivo.

Cuentas de usuario basadas en el directorio

Puede inscribir usuarios automáticamente integrándose con un servicio de directorio existente. Elimina la necesidad de agregar usuarios de forma manual a Workspace ONE UEM.

Cada usuario del directorio que desee administrar a través de Workspace ONE UEM debe tener una cuenta de usuario en la consola de UEM.

Puede agregar usuarios de los servicios de directorio directamente a Workspace ONE UEM aplicando uno de los siguientes métodos.

- Cargue por lotes un archivo que contenga todos los usuarios del servicio de directorio. La función de importar por lotes crea cuentas de usuarios automáticamente.
- Cree cuentas de usuario, una a una, introduciendo el nombre de usuario del directorio y seleccionando la opción de Verificar usuario para rellenar automáticamente los detalles que falten.
- No realice importaciones por lotes ni cree cuentas de usuario de forma manual. En lugar de eso, permita a todos los usuarios del directorio inscribirse ellos mismos en la etapa de

inscripción.

Ventajas

- Los usuarios finales pueden autenticarse con credenciales corporativas existentes.
- Detecta y sincroniza automáticamente los cambios del sistema de directorio en Workspace ONE UEM. Por ejemplo, cuando desactiva usuarios en AD, la cuenta de usuario correspondiente se marca como inactiva en Workspace ONE UEM Console.
- Método seguro para integrar con su servicio de directorio actual.
- Es una práctica de integración estándar.
- Puede utilizarse para la inscripción directa de Workspace ONE.
- Las implementaciones de SaaS realizadas con AirWatch Cloud Connector no requieren cambios de firewall. Además, ofrece una configuración segura para otras infraestructuras, como servidores de Microsoft ADCS, SCEP y SMTP.

Para obtener más información sobre la sincronización de los estados de las cuentas, consulte la sección documentada en esta página con el título Sincronización del estado del usuario de directorio.

Desventajas

- Se requiere disponer previamente de una infraestructura de servicio de directorio.
- Las implementaciones de SaaS requieren una mayor configuración debido a que AirWatch Cloud Connector se instala detrás del firewall o en una DMZ.

Sincronización del estado de usuarios del directorio

Cuando hace que usuarios pasen a ser inactivos en el servicio de directorio, afecta a la cuenta de Workspace ONE UEM y Workspace ONE Express correspondiente de manera similar, pero solo asume estas condiciones de requisitos previos.

- La sincronización de los usuarios eliminados solo funciona con Active Directory.
- El nombre de usuario que introdujo en la opción Nombre de usuario de enlace debe tener privilegios de administrador de Active Directory.
    - Para comprobar este nombre, vaya a Grupos y ajustes > Todos los ajustes > Sistema > Integración empresarial > Servicios de directorio, y en la pestaña Servidor, busque el cuadro de texto Vincular nombre de usuario.
    - Los clientes de Workspace ONE Express pueden encontrar el cuadro de texto Nombre de usuario de enlace en la misma pestaña Servidor navegando hasta Grupos y Ajustes y, a continuación, seleccionar Servicios de directorio en la columna Nombre.
- Puede permitir que los usuarios no administradores de Active Directory accedan al contenedor de objetos eliminados, siempre que siga los pasos descritos en el siguiente artículo de soporte técnico de Microsoft: https://support.microsoft.com/en-in/help/892806/how-to-let-non-administrators-view-the-active-directory-deleted-object.

- Además, la papelera de reciclaje debe habilitarse con el Centro de administración de Active Directory, pero solo si tiene que eliminar usuarios de AD.
    1. Abra el Centro de administración de Active Directory.
    2. Seleccione el dominio y, a continuación, haga clic con el botón secundario en el dominio.
    3. Seleccione Habilitar la papelera de reciclaje. Una vez habilitada, la papelera de reciclaje no se puede desactivar.

Cómo crear cuentas de usuario basadas en el directorio

Debe crear cuentas para cada usuario en el sistema de Workspace ONE UEM, y los usuarios de directorio se autentican utilizando las credenciales corporativas ya existentes.

Este tema detalla cómo crear cuentas de usuario una a una. Para crear cuentas de usuario en masa, consulte la sección titulada Importación por lotes de usuarios y dispositivos en Función Importar por lotes.

1. Acceda a Cuentas > Usuarios > Vista de lista, seleccione Agregar y, a continuación, Agregar usuario. Se mostrará la página Agregar/Editar usuario.
2. En la pestaña General, realice los siguientes ajustes para agregar un usuario de directorio.

Ajustes	Descripción
Tipo de seguridad	Elija Directorio como tipo de seguridad para añadir un usuario de Active Directory.
Nombre de directorio	Este ajuste, previamente rellenado, identifica el nombre del Active Directory.
Dominio	Elija el nombre de dominio desde el menú desplegable.
Nombre de usuario	Introduzca el nombre de usuario del directorio del usuario y seleccione Verificar usuario. Si el sistema encuentra una coincidencia, la información del usuario se rellena automáticamente. Los ajustes restantes de esta sección solo estarán disponibles cuando haya conseguido localizar un usuario de directorio activo con el botón Verificar usuario.
Nombre completo	Utilice Editar los atributos para poder editar cualquier opción que sincronice un valor vacío del directorio. La opción Editar los atributos también le permite introducir la información del usuario correspondiente de forma automática. Si un ajuste sincroniza un valor real del directorio, dicho ajuste deberá editarse en el mismo directorio. El cambio se implementará la próxima vez que se sincronice el directorio. Complete cualquier opción en blanco que haya devuelto el directorio en Nombre completo y seleccione Editar los atributos para guardar la adición.
Nombre de la pantalla	Permite introducir el nombre que aparece en la consola administrativa.
Dirección de correo electrónico	Permite introducir o editar la dirección de correo electrónico del usuario.

Ajustes	Descripción
Nombre de usuario de correo electrónico	Permite introducir o editar el nombre de usuario de correo electrónico del usuario.
Dominio (correo electrónico)	Permite seleccionar el dominio de correo electrónico desde el menú desplegable.
Número telefónico	Permite introducir el número de teléfono del usuario, incluidos el signo más, el código de país y el código de área. Si desea utilizar SMS para enviar notificaciones, el número de teléfono es obligatorio.
Inscripción	
Grupo organizativo para la inscripción	Seleccione el grupo organizativo en el que se inscribirá el usuario.
Permiso para que el usuario se inscriba en grupos organizativos adicionales	Elija si desea o no que el usuario se inscriba en más de un grupo organizativo. Si selecciona la opción Habilitado, complete el campo Grupos organizativos adicionales.
Rol de usuario	Seleccione el rol para el usuario que está agregando desde el menú desplegable.
Notificación	
Tipo de mensaje	Elija el tipo de mensaje que puede enviar al usuario: Correo electrónico, SMS o Ninguno. La selección de SMS requiere una entrada válida en el campo de Número de teléfono.
Plantilla de mensaje	Seleccione la plantilla para los mensajes de correo electrónico o SMS en este ajuste desplegable. También puede seleccionar Vista previa del mensaje para ver una vista previa de la plantilla y, a continuación, el enlace Configurar las plantillas de los mensajes para crear una plantilla.

3. También puede seleccionar la pestaña Avanzado y realizar los siguientes ajustes.

Ajustes	Descripción
Sección de información avanzada	
Contraseña del correo electrónico	Introduzca la contraseña del correo electrónico del usuario que está agregando.
Confirmar la contraseña del correo electrónico	Confirme la contraseña del correo electrónico del usuario que está agregando.
Nombre distintivo	Para los usuarios del directorio reconocidos por Workspace ONE UEM, este campo se rellena previamente con el nombre distinguido del usuario. Nombre distintivo es una cadena que representa el nombre de usuario y todos los códigos de autorización asociados a un usuario de Active Directory.

Ajustes	Descripción
Nombre distintivo del administrador	Introduzca el nombre distintivo del administrador del usuario. Este cuadro de texto es opcional.
Categoría	Elija la categoría de usuario para el usuario que se está agregando.
Departamento	Introduzca el departamento del usuario para fines administrativos de la empresa.
ID de empleado	Introduzca el ID de empleado del usuario para fines administrativos de la empresa.
Centro de costos	Introduzca el centro de costes del usuario para fines administrativos de la empresa.
Atributo personalizado 1–5 (solamente para usuarios de directorio)	Introduzca los atributos personalizados previamente configurados, según corresponda. Puede definir estos atributos personalizados en Grupos y ajustes > Todos los ajustes > Dispositivos y usuarios > Avanzado > Atributos personalizados. Aviso: Los atributos personalizados se pueden configurar solamente en los grupos organizativos de clientes.
Sección de certificados	
Utilizar S/MIME	Permite habilitar o desactivar el uso de las extensiones seguras multipropósito al correo de Internet (S/MIME). Si está habilitada esta opción, debe tener un perfil habilitado por S/MIME y, luego, cargar un certificado S/MIME mediante la selección del botón Cargar.
Certificado de cifrado separado	Habilite o desactive el uso de un certificado de cifrado independiente. Si está habilitada esta opción, debe cargar un certificado de cifrado con la función Cargar. Generalmente, el mismo certificado S/MIME se utiliza para firmar y cifrar, a menos que se esté utilizando otro certificado expresamente.
Certificado de cifrado antiguo	Habilite o desactive un certificado de cifrado de versión heredada. Si está habilitada esta opción, debe Cargar un certificado cifrado.
Sección Inscripción preparada	
Habilitar la inscripción preparada	Permite habilitar o desactivar la inscripción provisional de los dispositivos.

Si está habilitada esta opción, debe elegir entre Dispositivos de usuario único y Dispositivos de múltiples usuarios.

Si selecciona Dispositivos de usuario único, debe elegir entre Estándar (los propios usuarios inician sesión) y Avanzado (el dispositivo se inscribe en nombre de otro usuario).

Consulte la sección Inscripción preparada para más información.

4. Seleccione Guardar para guardar solamente el usuario nuevo o seleccione Guardar y agregar dispositivo para guardar el usuario nuevo y continuar a la página Agregar dispositivo.

Función Importar por lotes

Puede crear usuarios y grupos de usuarios por lotes o importarlos por lotes en Workspace ONE UEM desde el servicio de directorio.

Realizar una importación por lotes significa utilizar una plantilla suministrada en un formato de valores separados por comas, introducir sus propios datos y cargar la plantilla completada.

Aviso: Los archivos de plantilla descargables se proporcionan a partir de Workspace ONE UEM Console; son específicos y se encuentran dentro del tipo de importación por lotes que desee. Seleccione uno de los siguientes vínculos para ver las rutas de navegación específicas que deberá seguir dentro de Workspace ONE UEM Console para poder acceder a estas descargas.

Cómo realizar cambios en los directorios externos de usuarios LDAP y AD

Una vez que las listas de lote de usuarios y grupos de usuarios estén cargadas, los cambios realizados en los directorios externos de usuarios de LDAP/AD no se actualizarán en Workspace ONE UEM. Debe actualizar estos cambios manualmente o cargarlos como un lote nuevo.

Importación por lotes de usuarios y dispositivos

Puede importar por lotes varios usuarios y dispositivos a la consola. También puede comprobar el estado de un trabajo por lotes desplazándose a Cuentas > Usuarios > Estado del lote.

La pantalla Estado del lote muestra una lista de todos los trabajos importados por lotes que ha solicitado, incluido el estado del trabajo.

Para comenzar el proceso de importación de usuarios o dispositivos por lotes, realice los siguientes pasos.

1. Navegue a Cuentas > Usuarios > Estado del lote o Dispositivos > Ciclo de vida > Estado de inscripción > Agregar y seleccione Importar por lotes.
2. Introduzca la información básica como el Nombre del lote y la Descripción del lote.
3. Seleccione el tipo de lote adecuado en el menú desplegable Tipo de lote.
4. Seleccione y descargue la plantilla que mejor se ajuste al tipo de importación por lotes que esté realizando. Escoja de entre las siguientes opciones.
    - Dispositivos de la lista de no permitidos: importe una lista de dispositivos conocidos no conformes en función del IMEI, Número de serie o UDID. Los dispositivos de la lista de no permitidos no pueden inscribirse. Si un dispositivo de la lista de no admitidos intenta inscribirse, se bloqueará de forma automática.
    - Dispositivos de la lista de permitidos: importe dispositivos previamente aprobados en función del IMEI, Número de serie o UDID. Utilice esta plantilla para importar una lista de dispositivos conocidos de confianza. La propiedad y el ID de grupo asociados a este dispositivo se aplican de forma automática durante la inscripción.
    - Usuario o dispositivo: seleccione entre una plantilla CSV simple y una avanzada. La plantilla simple cuenta solamente con las opciones más utilizadas, mientras que la avanzada dispone de las opciones completas e íntegras.
    - Cambiar grupo organizativo: traslade usuarios a un grupo organizativo diferente.

5. Abra el archivo CSV. Confirme si los usuarios forman parte del grupo organizativo (GO) para la inscripción.

   El archivo CSV presenta varias columnas que se corresponden con las opciones de la página Agregar/Editar usuario. Al abrir la plantilla CSV, observe que existen datos de muestra en cada columna de la plantilla. Los datos de muestra se proporcionan para informarle sobre qué tipo de datos se necesitan y en qué formato deben estar. No se desvíe del formato presentado por los datos de muestra.

   Aviso: Un archivo CSV (valores separados por comas) es simplemente un archivo de texto cuya extensión se cambia de "TXT" a "CSV". Almacena datos tabulares (texto y números) en texto sin formato. Cada línea del archivo es un registro de datos. Cada registro consta de uno o más campos separados por comas. Se puede abrir y editar con cualquier editor de texto. También puede abrirse y editarse con Microsoft Excel.

6. Vaya a Grupos y ajustes > Todos los ajustes > Dispositivos y usuarios > General > Inscripción y seleccione la pestaña Agrupación.

   Para la inscripción basada en el directorio, cada usuario debe tener el Tipo de seguridad como Directorio.

   Resultado: Si está establecido el modo de asignación de ID de grupo como Predeterminado, los usuarios forman parte del grupo organizativo para la inscripción.

7. Introduzca los datos de los usuarios, incluida la información del dispositivo si es necesario, y luego guarde el archivo.

8. Vuelva a la página Importar por lotes y seleccione Elegir archivo para localizar y cargar el archivo CSV que descargó y rellenó anteriormente.

9. Seleccione Guardar.

Cómo importar grupos de usuarios por lotes

Para ahorrar tiempo puede importar varios grupos de usuarios de Protocolo ligero de acceso a directorios (LDAP)/Active Directory (AD) en Workspace ONE UEM Console. Puede importar por lotes grupos de usuarios del mismo modo que los usuarios individuales, completando la plantilla proporcionada y cargándola.

1. Vaya a Cuentas > Grupos de usuarios > Vista de lista y seleccione Agregar.

2. Seleccione Importar por lotes.

3. Introduzca la información básica como el Nombre del lote y la Descripción del lote en Workspace ONE UEM Console.

4. En Archivo por lotes (.csv), seleccione el botón Seleccionar archivo para localizar y cargar el archivo CSV completado.

5. También puede seleccionar el enlace Descargar plantilla para este tipo de lote y guardar el archivo de valores separados por comas (CSV) y utilizarlo para preparar un nuevo archivo de importación.

   - Abra el archivo CSV, que contiene varias columnas que corresponden a los ajustes que se muestran en la página Agregar grupo de usuarios. Las columnas que tienen un asterisco son obligatorias y deben contener datos. Guarde el archivo.

- El encabezado de la última columna del archivo CSV tiene la etiqueta "GroupID/Manage (Edit and Delete)/Manage(Users and Enrollment)/UG assignment/Admin Inheritance". El encabezado de esta columna corresponde a los ajustes y se atiene a la lógica de la pestaña Permisos de la página Editar grupo de usuarios. Para obtener más información, consulte la sección titulada Editar los permisos de los grupos de usuarios en Grupos de usuarios.

6. Seleccione Importar.
7. Si hay algún problema con la importación por lotes, consulte y solucione problemas mediante la selección de Cuentas > Estado del lote. Haga clic en el hipervínculo Errores para ver los errores específicos de la importación del lote.

Cómo editar usuarios básicos con la importación por lotes

La función Importar en lote permite editar y trasladar usuarios en grupos, en vez de uno cada vez. Los usuarios deben existir en Workspace ONE UEM para que funcione dicho procedimiento. Edite los siguientes ajustes en el archivo CSV y utilice la opción Importar por lotes para cargar este archivo.

Puede editar y mover usuarios en grupos en lugar de uno a uno cambiando determinadas columnas del archivo CSV que ha cargado como parte del proceso de importación por lotes. Esta manipulación de columna solo es aplicable a dos tipos de autenticación de usuario: autenticación de usuario básica y proxy de autenticación.

- Contraseña (Básico solamente)
- Nombre
- Segundo nombre
- Apellido
- Dirección de correo electrónico
- Número de teléfono
- Teléfono móvil
- Departamento
- Nombre de usuario del correo electrónico
- Contraseña del correo electrónico
- Grupos organizativos autorizados (solamente dentro del ID de grupo dado o en niveles inferiores).
- Categoría del usuario para la inscripción (esta categoría es accesible para el usuario; de no ser así, el valor predeterminado es 0).
- Rol de usuario de inscripción (este rol es accesible para el usuario, de no ser así, asumirá el rol predeterminado del grupo organizativo).

Esta edición de usuarios básicos se aplica únicamente a Autenticación de usuario básico y Proxy de autenticación. Para obtener más información sobre estos y otros tipos de autenticación, consulte Tipos de autenticación de usuario

Trasladar usuarios entre grupos organizativos mediante la importación por lotes

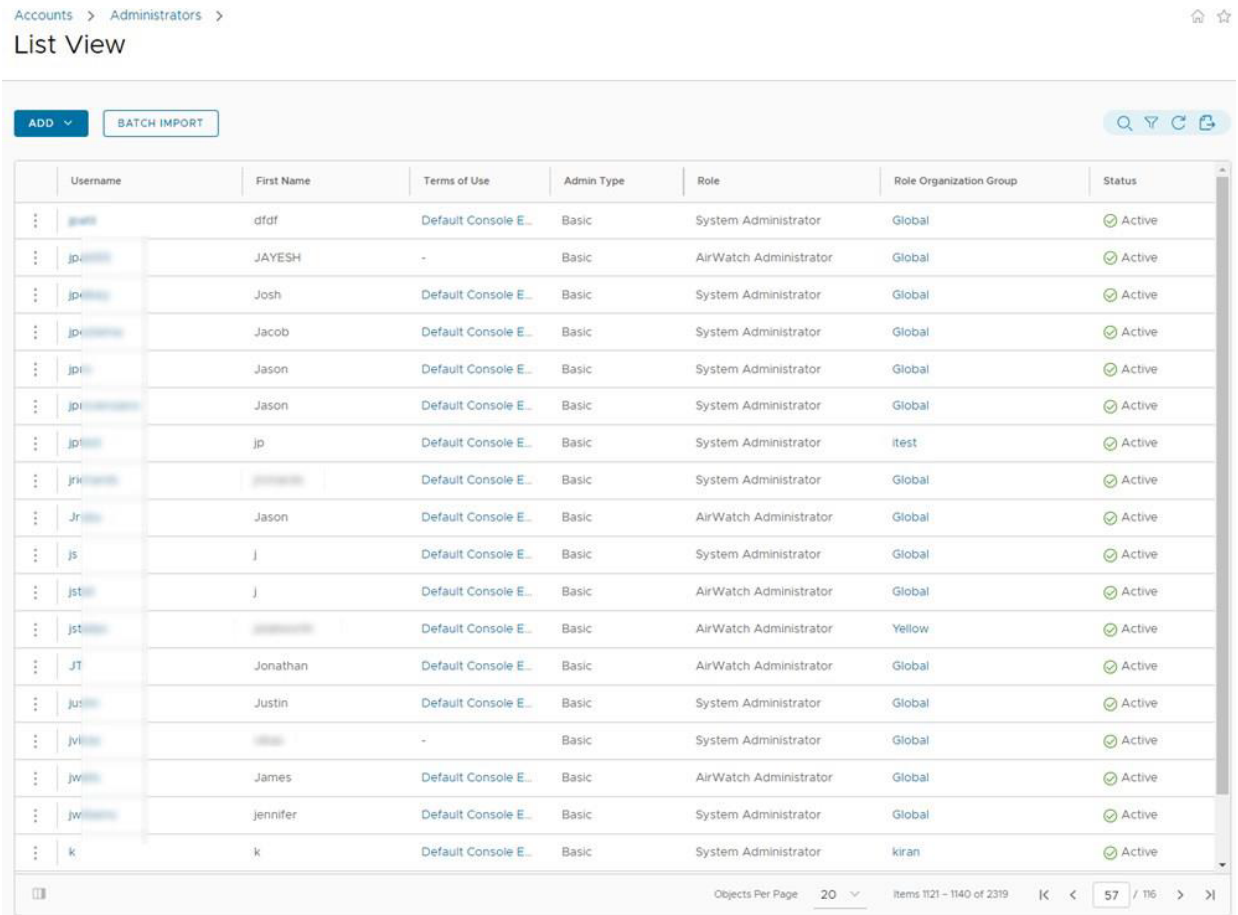
La importación por lotes se utiliza para trasladar varios usuarios a un grupo organizativo diferente.

1. Desde la pantalla Importar por lotes, introduzca la información básica, incluidos el Nombre de lote y una Descripción del lote, en Workspace ONE UEM Console.
2. Elija Cambiar grupo organizativo en la lista de plantillas y guarde el archivo CSV en algún lugar al que pueda acceder.
3. Introduzca el ID de grupo correspondiente del grupo organizativo existente del usuario, el Nombre de usuario que desea mover y el ID de grupo de destino del nuevo grupo organizativo del usuario.
4. Vuelva a la pantalla Importar por lotes, seleccione Seleccionar archivo para buscar y cargar el archivo CSV guardado y seleccione Abrir.
5. Seleccione Guardar.

Cuentas administrativas

Las cuentas administrativas en Workspace ONE Express y Workspace ONE UEM le permiten mantener la configuración, enviar o revocar funciones y contenido, y mucho más.

Vista de lista de cuentas de administrador



Puede implementar funciones de administración importantes relacionadas con el mantenimiento de cuentas administrativas en Cuentas > Administradores > Vista de lista.

Para ver la página Agregar/Editar administrador, seleccione el enlace de hipertexto de la columna del nombre de usuario. Este enlace le permite actualizar rápidamente los roles actuales asignados o cambiar rápidamente los roles de su organización para mantener los privilegios actualizados. También puede modificar la información general del administrador y restablecer la contraseña.

Puede utilizar el Filtro para filtrar la lista de administradores con el fin de incluir todos los roles o limitar la lista al rol específico que desee ver. También puede exportar un archivo XLSX o CSV (valores separados por comas) de la Vista de lista de administradores filtrada o sin filtrar. A continuación, puede ver y analizar este archivo con MS Excel. Seleccione el botón Exportar y elija una ubicación de descarga.

Para mostrar los botones de acción aplicables a ese administrador, seleccione el botón de radio situado junto al nombre de usuario del administrador.

- Ver historial: permite recopilar información sobre cuándo inician y cierran sesión los administradores en Workspace ONE UEM Console o Workspace ONE Express.
- Desactivar: permite cambiar el estado de una cuenta administrativa de activo a inactivo. Esta función le permite suspender los privilegios y las funciones de administración de forma temporal. Al mismo tiempo, esta función le permite conservar los roles definidos de la cuenta administrativa para utilizarlos más adelante.
- Activar: permite cambiar el estado de una cuenta administrativa de inactivo a activo.
- Eliminar: permite eliminar la cuenta administrativa desde la consola. Esta acción resulta útil cuando un administrador deja de trabajar en la empresa.
- Restablecer contraseña: disponible solo para administradores básicos. Envía un correo electrónico a la dirección registrada de correo electrónico del administrador básico. El correo electrónico contiene un enlace que caduca en 48 horas. Para restablecer la contraseña, el administrador básico debe seleccionar el vínculo y responder a la pregunta de recuperación de contraseña. Este enlace permite al administrador básico cambiar su propia contraseña.

  Los administradores basados en directorios deben restablecer sus contraseñas utilizando el sistema de Active Directory.

  Los administradores temporales no pueden restablecer su contraseña. Otro administrador debe eliminar y luego volver a crear la cuenta de administrador temporal.

Cómo crear una cuenta administrativa

Puede agregar cuentas administrativas desde la página Vista de lista de administradores para brindar acceso a las funciones avanzadas de Workspace ONE UEM Console o Workspace ONE Express. Todos los administradores que vayan a mantener y supervisar la consola deben tener una cuenta individual.

1. Vaya a Cuentas > Administradores > Vista de lista, seleccione Agregar y, a continuación, Agregar administrador. Aparecerá la página Agregar/Editar administrador.
2. En la pestaña Básico, para el ajuste Tipo de usuario, seleccione Básico o Directorio.
   - Si selecciona Básico, debe llenar todos los ajustes requeridos en la pestaña Básico,

incluidos el nombre de usuario, la contraseña, el nombre y el apellido.

- Puede habilitar la autenticación de dos factores seleccionando entre Correo electrónico y SMS como método de entrega y la hora de caducidad en minutos del token.
- Asimismo, puede seleccionar la opción Notificación eligiendo Ninguno, Correo electrónico y SMS. El administrador recibirá una respuesta generada automáticamente.
- Si selecciona Directorio, debe introducir el Dominio y el Nombre del usuario del usuario administrativo.

3. Seleccione la pestaña Detalles e introduzca cualquier información adicional que sea necesaria.
4. Seleccione la pestaña Roles y luego el Grupo organizativo, seguido del Rol que desea asignar a su nuevo administrador. Para agregar nuevos roles, utilice el botón Agregar rol.
5. Seleccione la pestaña API y elija el tipo de Autenticación.
6. Seleccione la pestaña Notas e introduzca Notas adicionales para el usuario administrativo.
7. Seleccione Guardar para crear la cuenta administrativa con el rol asignado.

Cómo crear una cuenta administrativa temporal

Puede otorgar acceso administrativo temporal al entorno para soporte, demostraciones y otros casos de uso de tiempo limitado.

1. Acceda a Cuentas > Administradores > Vista de lista y seleccione Agregar. Seleccione la opción Agregar administrador temporal.

   Si lo prefiere, puede seleccionar el botón Ayuda en la barra de encabezado que aparece en la esquina superior derecha de casi todas las páginas de Workspace ONE UEM y Workspace ONE Express, y seleccionar Agregar administrador temporal.

2. En la pestaña Básico, elija agregar una cuenta administrativa temporal basada en la Dirección de correo electrónico o en el Nombre de usuario y realice los siguientes ajustes.

Ajustes	Descripción
Dirección de correo electrónico	Introduzca las direcciones de correo electrónico en la que se basa la cuenta administrativa temporal. Disponible solo cuando se selecciona el botón de selección Correo electrónico.
Nombre de usuario	Introduzca el nombre del usuario en el que se basa la cuenta administrativa temporal. Disponible solo cuando se selecciona el botón de radio Nombre del usuario.
Contraseña / Confirmar contraseña	Introduzca y confirme la contraseña que corresponde a la dirección de correo electrónico o al nombre del usuario.
Periodo de caducidad	Seleccione el Periodo de caducidad, cuyo valor predeterminado es de 6 horas. También puede configurar este menú desplegable como Inactivo para crear la cuenta en el momento y activarla más adelante.
Número de vale	De manera opcional, puede agregar el número de ticket desde ZenDesk, Bugzilla, Jira u otra herramienta de soporte técnico como marcador de referencia.

3. En la pestaña Roles, puede agregar, editar y eliminar roles que se apliquen a la cuenta administrativa temporal.
    - Para agregar un rol, seleccione el botón Agregar rol y, a continuación, seleccione el grupo organizativo y el rol a los que se aplicará la cuenta administrativa temporal.
    - Edite una función existente seleccionando el icono de edición ( ) y seleccione un grupo organizativo y una función diferentes.
    - Para borrar un rol, seleccione el icono de "Eliminar" ( ).

Sincronización del estado de usuarios del directorio

Cuando hace que usuarios pasen a ser inactivos en el servicio de directorio, afecta a la cuenta de Workspace ONE UEM y Workspace ONE Express correspondiente de manera similar, pero solo asume estas condiciones de requisitos previos.

- La sincronización de los usuarios eliminados solo funciona con Active Directory.
- El nombre de usuario que introdujo en la opción Nombre de usuario de enlace debe tener privilegios de administrador de Active Directory.
    - Para comprobar este nombre, vaya a Grupos y ajustes > Todos los ajustes > Sistema > Integración empresarial > Servicios de directorio, y en la pestaña Servidor, busque el cuadro de texto Vincular nombre de usuario.
    - Los clientes de Workspace ONE Express pueden encontrar el cuadro de texto Nombre de usuario de enlace en la misma pestaña Servidor navegando hasta Grupos y Ajustes y, a continuación, seleccionar Servicios de directorio en la columna Nombre.
- Puede permitir que los usuarios no administradores de Active Directory accedan al contenedor de objetos eliminados, siempre que siga los pasos descritos en el siguiente artículo de soporte técnico de Microsoft: https://support.microsoft.com/en-in/help/892806/how-to-let-non-administrators-view-the-active-directory-deleted-object.
- Además, la papelera de reciclaje debe habilitarse con el Centro de administración de Active Directory, pero solo si tiene que eliminar usuarios de AD.
    1. Abra el Centro de administración de Active Directory.
    2. Seleccione el dominio y, a continuación, haga clic con el botón secundario en el dominio.
    3. Seleccione Habilitar la papelera de reciclaje. Una vez habilitada, la papelera de reciclaje no se puede desactivar.

Historial de inicios de sesión

Desplácese hasta Cuentas > Administradores > Actividad del sistema > Historial de inicios de sesión y podrá ver una lista de todos los inicios de sesión de los administradores, incluidos la fecha y la hora, su dirección IP, navegador y plataforma. Seleccione un Nombre de usuario de la lista para ver todo el historial de inicios de sesión del administrador seleccionado.

Usar la funcionalidad de UEM con una REST API

Puede configurar aplicaciones externas para que utilicen la funcionalidad de producto principal de Workspace ONE UEM mediante la integración de las REST API con la infraestructura de UEM y facilitar la conectividad. También puede seleccionar una URL de token de OAuth más cercana al centro de datos para autenticar las llamadas de API.

Primeros pasos con las REST API

Al utilizar la arquitectura de software REST simplificada, las REST API de Workspace ONE UEM actualmente son compatibles con varias funcionalidades, entre las que se incluyen grupo organizativo, administración de Console, aplicación móvil, dispositivo móvil, correo electrónico, usuario de inscripción, perfil, grupo inteligente y administración de grupo de usuarios.

El uso de las API basadas en REST ofrece varias ventajas a las empresas, entre las que destacan la eliminación de costes y de tiempo invertidos en el desarrollo de aplicaciones internas. Las REST API de Workspace ONE UEM están totalmente disponibles para integrarse con servidores, programas y procesos empresariales. Las REST API de Workspace ONE UEM son más eficientes, pueden funcionar sin problemas y se pueden personalizar fácilmente con las marcas de las empresas. Estas API son para desarrolladores de aplicaciones. Esta guía proporciona conocimientos sobre el diseño y la arquitectura de la biblioteca de API y facilita el desarrollo personalizado y la integración con Workspace ONE UEM.

Acceder a la documentación de la API

Para revisar la documentación detallada de la API, vaya a la página de ayuda de la API de Workspace ONE UEM.

En la barra de direcciones del navegador, reemplace "cn" en la URL por "as" y, a continuación, agregue `/api/help` después de .com.

Por ejemplo, la documentación de la API para la URL de un entorno SaaS de…

```
https://cn4855.awmdm.com
```

…es…

```
https://as4855.awmdm.com/api/help
```

URL para centro de datos y token para la compatibilidad con OAuth 2.0

Workspace ONE UEM es compatible con el protocolo estándar del sector OAuth 2.0 para la autenticación y la autorización seguras de llamadas REST API.

El servicio de token de Workspace ONE es el emisor de tokens para la autenticación de OAuth y solo se admite en entornos de SaaS. Las URL del token son específicas de cada región.

Región	Ubicación del centro de datos de SaaS de Workspace ONE UEM	URL de token
Ohio (Estados Unidos)	Todo el entorno de UAT	`https://uat.uemauth.vmwservices.com/connect/token`
Virginia (Estados Unidos)	Estados Unidos	`https://na.uemauth.vmwservices.com/connect/token`
Virginia (Estados Unidos)	Canadá	`https://na.uemauth.vmwservices.com/connect/token`
Frankfurt (Alemania)	Reino Unido	`https://emea.uemauth.vmwservices.com/connect/token`
Frankfurt (Alemania)	Alemania	`https://emea.uemauth.vmwservices.com/connect/token`
Tokio (Japón)	India	`https://apac.uemauth.vmwservices.com/connect/token`
Tokio (Japón)	Japón	`https://apac.uemauth.vmwservices.com/connect/token`
Tokio (Japón)	Singapur	`https://apac.uemauth.vmwservices.com/connect/token`
Tokio (Japón)	Australia	`https://apac.uemauth.vmwservices.com/connect/token`
Tokio (Japón)	Hong Kong	`https://apac.uemauth.vmwservices.com/connect/token`

Crear un cliente de OAuth para usarlo con comandos de API (SaaS)

Puede crear un cliente de OAuth para utilizarlo con comandos de API y que solo sea compatible en entornos de SaaS. Cree un cliente de OAuth para su entorno de SaaS siguiendo estos pasos.

1. Vaya a Grupos y ajustes > Configuraciones.
2. Introduzca `OAuth` en el cuadro de texto de búsqueda con la etiqueta "Introducir un nombre o una categoría".
3. Seleccione Administración de clientes OAuth en los resultados. Se mostrará la pantalla Administración de clientes OAuth.
4. Seleccione el botón de Agregar.
5. Introduzca el Nombre, la Descripción, el Grupo organizativo y la Función.

   Aviso: Para obtener más información sobre los permisos específicos de REST API para la función que seleccione, consulte la sección de este tema titulada Crear una función que

puedan utilizar las REST API.

6. Asegúrese de que el Estado se haya establecido en Habilitado.
7. Seleccione Guardar.
8. AVISO IMPORTANTE: Copie el ID de cliente y el Secreto de cliente en el portapapeles y guárdelos antes de cerrar esta pantalla. Seleccione el icono Copiar () para enviar el Secreto de cliente al portapapeles.

   No puede volver aquí para recuperar estos datos después de seleccionar Cerrar.
9. Use el ID de cliente, el secreto de cliente y la URL del token para generar el token de acceso en el siguiente formato:

   Llamada API: POST {URL de token específica según la región de la sección anterior}

Clave	Valor
grant_type	client_credentials
client_id	{ID de CLIENTE generado en UEM Console}
client_secret	{CLIENT SECRET generated on UEM console}

10. Use el token de acceso devuelto para autorizar futuras solicitudes de API a los servidores de API de Workspace ONE UEM. Debe formatear el token de acceso en los encabezados de solicitud de la siguiente manera.

    Llamada API: {API de UEM}

Clave	Valor
Autorización	{Token de acceso}

Crear una función que pueda utilizar REST API

Cada llamada a API tiene un recurso (o permiso) correspondiente que debe incluir en la función que asigne al cliente de OAuth. Por lo tanto, los permisos que se deben incluir en la función que asigne se alinean con los tipos de llamadas a API que está realizando.

Utilice la información de la siguiente tabla para seleccionar los permisos que debe incluir en la función que asigne. A continuación, visite la sección titulada Cómo crear funciones administrativas en Acceso basado en funciones para obtener instrucciones sobre cómo crear esa función.

Categoría	Nombre	Descripción	Solo lectura / Editar
REST > Administradores	Grupos de sistemas de API de REST	Acceso a la información del grupo de la organización	Editar
	Administrador del sistema de API de REST	Acceso a la información del administrador	Editar
	Usuarios del sistema API REST	Acceso a la información del usuario	Editar

Categoría	Nombre	Descripción	Solo lectura / Editar
	Escribir API de REST - Administradores	Habilita el acceso a todas las API de escritura/actualización del conjunto de usuarios administrativos	Editar
	Ejecutar API de REST - Administradores	Habilita el acceso a todas las API de ejecución del conjunto de usuarios administrativos	Editar
	Eliminar API de REST - Administradores	Habilita el acceso a todas las API de eliminación del conjunto de usuarios administrativos	Editar
	Leer API de REST - Administradores	Habilita el acceso a todas las API de solo LECTURA del conjunto de usuarios administrativos	Sólo lectura
REST > Aplicaciones	Blob MAM de API de REST	Subir contenido de descarga	Editar
	Aplicaciones MAM de API de REST	Acceso a aplicaciones administradas	Editar
	Escribir API de REST - Aplicaciones	Habilita el acceso a todas las API de escritura/actualización del conjunto de aplicaciones	Editar
	Ejecutar API de REST - Aplicaciones	Habilita el acceso a todas las API de ejecución del conjunto de aplicaciones	Editar
	Eliminar API de REST - Aplicaciones	Habilita el acceso a todas las API de eliminación del conjunto de aplicaciones	Editar
	Leer API de REST - Aplicaciones	Habilita el acceso a todas las API de solo LECTURA del conjunto de aplicaciones	Sólo lectura
REST > Directiva de conformidad	Eliminar política de conformidad de API de REST	Habilita el acceso para las API de Eliminar en el conjunto de políticas de conformidad	Editar
	Ejecutar política de conformidad de API de REST	Habilita el acceso para las API de Ejecutar en el conjunto de políticas de conformidad	Editar
	Escribir política de conformidad de API de REST	Habilita el acceso a las API de Escritura en el conjunto de políticas de conformidad	Editar
	Leer política de conformidad de API de REST	Habilita el acceso a las API de solo LECTURA en el conjunto de políticas de conformidad	Sólo lectura
REST > Atributos personalizados	Ejecutar atributos personalizados de API de REST	Habilita el acceso para todas las API de Ejecución en el conjunto de atributos personalizados	Editar
	Escribir atributos personalizados de API de REST	Habilita el acceso para todas las API de Escritura en el conjunto de atributos personalizados	Editar
	Eliminar atributos personalizados de API de REST	Habilita el acceso para todas las API de Eliminación en el conjunto de atributos personalizados	Editar
	Leer atributos personalizados API de REST	Habilita el acceso a todas las API de solo lectura en el conjunto de atributos personalizados	Sólo lectura
REST > Dispositivos	API de REST - Grupos inteligentes de MDM	Acceso a la información del grupo inteligente	Editar

Categoría	Nombre	Descripción	Solo lectura / Editar
	API de REST - Grupos de usuarios de MDM	Acceso a grupos de usuarios	Editar
	API de REST - Perfiles de MDM	Enviar comandos de bloqueo/desbloqueo	Editar
	API de REST - Dispositivos MDM	Enviar comandos de bloqueo/desbloqueo	Editar
	Escribir BLOBS de API de REST	Habilita acceso a todos los APIs de escribir/actualizar en la colección de BLOBS	Editar
	Ejecutar BLOBS de API de REST	Habilita acceso a todos los APIs de ejecución en la colección de BLOBS	Editar
	Eliminar BLOBS de API de REST	Habilita acceso a todos los APIs de eliminación en la colección de BLOBS	Editar
	Escribir API de REST - Dispositivos	Habilita el acceso a todas las API de escritura/actualización del conjunto de dispositivos	Editar
	Ejecutar API de REST - Dispositivos	Habilita el acceso a todas las API de ejecución del conjunto de dispositivos	Editar
	Eliminar API de REST - Dispositivos	Habilita el acceso a todas las API de eliminación del conjunto de dispositivos	Editar
	API de REST - Dispositivos, avanzado	Habilita el acceso a todas las API avanzadas del conjunto de dispositivos	Editar
	Leer BLOBS de API de REST	Habilita acceso a todos los APIs de solo lectura en la colección de BLOBS	Sólo lectura
	Leer API de REST - Dispositivos	Habilita el acceso a todas las API de solo LECTURA del conjunto de dispositivos	Sólo lectura
REST > Integración empresarial de REST	Lectura de integración empresarial de REST API	Habilita el acceso a todos los APIs de solo LECTURA en la integración empresarial	Sólo lectura
REST > Grupos	Escribir API de RESTT - Grupos	Habilita el acceso a todas las API de escritura/actualización de la colección de grupos de la organización	Editar
	Ejecutar API de REST - Grupos	Habilita el acceso a todas las API de ejecución de la colección de grupos de organización	Editar
	Eliminar API de REST -Grupos	Habilita el acceso a todas las API de eliminación del conjunto de grupos organizativos	Editar
	Escribir grupos inteligentes de API de REST	Habilita el acceso a todas las API de escritura del conjunto de grupos inteligentes	Editar
	Ejecutar grupos inteligentes de API de REST	Habilita el acceso a todas las API de ejecución de los conjuntos de grupos inteligentes	Editar
	Eliminar grupos inteligentes de API de REST	Habilita el acceso a todas las API de eliminación del conjunto de grupos inteligentes	Editar

Categoría	Nombre	Descripción	Solo lectura / Editar
	Escribir grupos de usuarios de API de REST	Permite el acceso a todas las API de escritura/actualización en grupos de usuarios	Editar
	Ejecutar grupos de usuarios de API de REST	Permite el acceso a todas las API de ejecución en grupos de usuarios	Editar
	Eliminar grupos de usuarios de API de REST	Habilita el acceso a todas las API de eliminación de los grupos de usuarios	Editar
	API de REST de escritura del carrito	API de REST para guardar y editar los datos del carrito	Editar
	API de REST de eliminación del carrito	API de REST para eliminar los datos del carrito	Editar
	Escritura de API de REST Apple School Manager	API de REST para iniciar la sincronización de Apple School Manager	Editar
	API de REST de asociación de Apple School Manager	API de REST para asociar un usuario de inscripción a un miembro de Apple School Manager	Editar
	Guardar asignaciones de clases de API de REST	API de REST para guardar las asignaciones de la clase	Editar
	API de REST de escritura de la clase	API de REST para guardar y editar datos de la clase	Editar
	API de REST de eliminación de la clase	API de REST para borrar datos de la clase	Editar
	Escritura de ajustes de API de REST de Education	API de REST para guardar y editar ajustes de Educación	Editar
	API de REST de lectura de los ajustes de Educación	API de REST para ver la configuración de Education	Editar
	Leer API de REST - Grupos	Habilita el acceso a todas las API de solo LECTURA del conjunto de grupos organizativos	Sólo lectura
	Leer grupos inteligentes de API de REST	Habilita el acceso a todas las API de solo LECTURA del conjunto de grupos inteligentes	Sólo lectura
	Leer grupos de usuarios de API de REST	Habilita el acceso a todas las API de solo LECTURA de los grupos de usuarios	Sólo lectura
	API de REST de lectura de la sincronización de Apple School Manager	API de REST para comprobar el estado de sincronización de Apple School Manager	Sólo lectura
	API de REST de lectura de aplicaciones para el dispositivo	API de REST para obtener una lista de aplicaciones elegibles para el dispositivo	Sólo lectura
	API de REST de lectura de la clase	API de REST para ver datos de la clase	Sólo lectura
REST > Productos	Ejecutar productos de API de REST	Habilita el acceso a todas las API de ejecución del conjunto de productos	Editar

Categoría	Nombre	Descripción	Solo lectura / Editar
	Escribir productos API de REST	Habilita el acceso a todas las API de escritura del conjunto de productos	Editar
	Eliminar productos de API de REST	Habilita el acceso a todas las API de eliminación del conjunto de productos	Editar
	Leer productos de API de REST	Habilita el acceso a todas las API de solo LECTURA del conjunto de productos	Sólo lectura
REST > Perfiles	Acceso de escritura en la política de actualizaciones	Habilita el acceso a todas las API de ESCRITURA en el conjunto de políticas de actualizaciones	Editar
	Acceso de ejecución en la política de actualizaciones	Habilita el acceso a todas las API de EXECUTE en la colección de directivas de actualizaciones	Editar
	Acceso de eliminación en la política de actualizaciones	Habilita el acceso a todas las API de ELIMINACIÓN en el conjunto de políticas de actualizaciones	Editar
	Escribir perfiles de API de REST	Habilita el acceso a todas las API de escritura del conjunto de perfiles	Editar
	Ejecutar perfiles de API de REST	Habilita el acceso a todas las API de ejecución del conjunto de perfiles	Editar
	Eliminar perfiles de API de REST	Habilita el acceso a todas las API de eliminación del conjunto de perfiles	Editar
	Acceso de lectura en la política de actualizaciones	Habilita el acceso a todas las API de LECTURA en el conjunto de políticas de actualizaciones	Sólo lectura
	Leer perfiles de API de REST	Habilita el acceso a todas las API de solo LECTURA del conjunto de perfiles	Sólo lectura
REST > Usuarios	Escribir API de REST - Usuarios	Habilita el acceso a todas las API de escritura/actualización del conjunto de usuarios de inscripción	Editar
	Ejecutar API de REST - Usuarios	Habilita el acceso a todas las API de ejecución del conjunto de usuarios de inscripción	Editar
	Eliminar AAPI de REST - Usuarios	Habilita el acceso a todas las API de eliminación del conjunto de usuarios de inscripción	Editar
	Leer tokens de usuario de API de REST	Habilita el acceso de los tokens de inscripción de usuarios para las API en la colección de usuarios de inscripción	Sólo lectura
	Leer API de REST - Usuarios	Habilita el acceso a todas las API de solo LECTURA del conjunto de usuarios de inscripción	Sólo lectura