Empresas

Comunicación y conectividad | Cloud | IoT | Seguridad

Administración de contenido móvil.

VMware Workspace ONE UEM sevices

vmware®

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

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

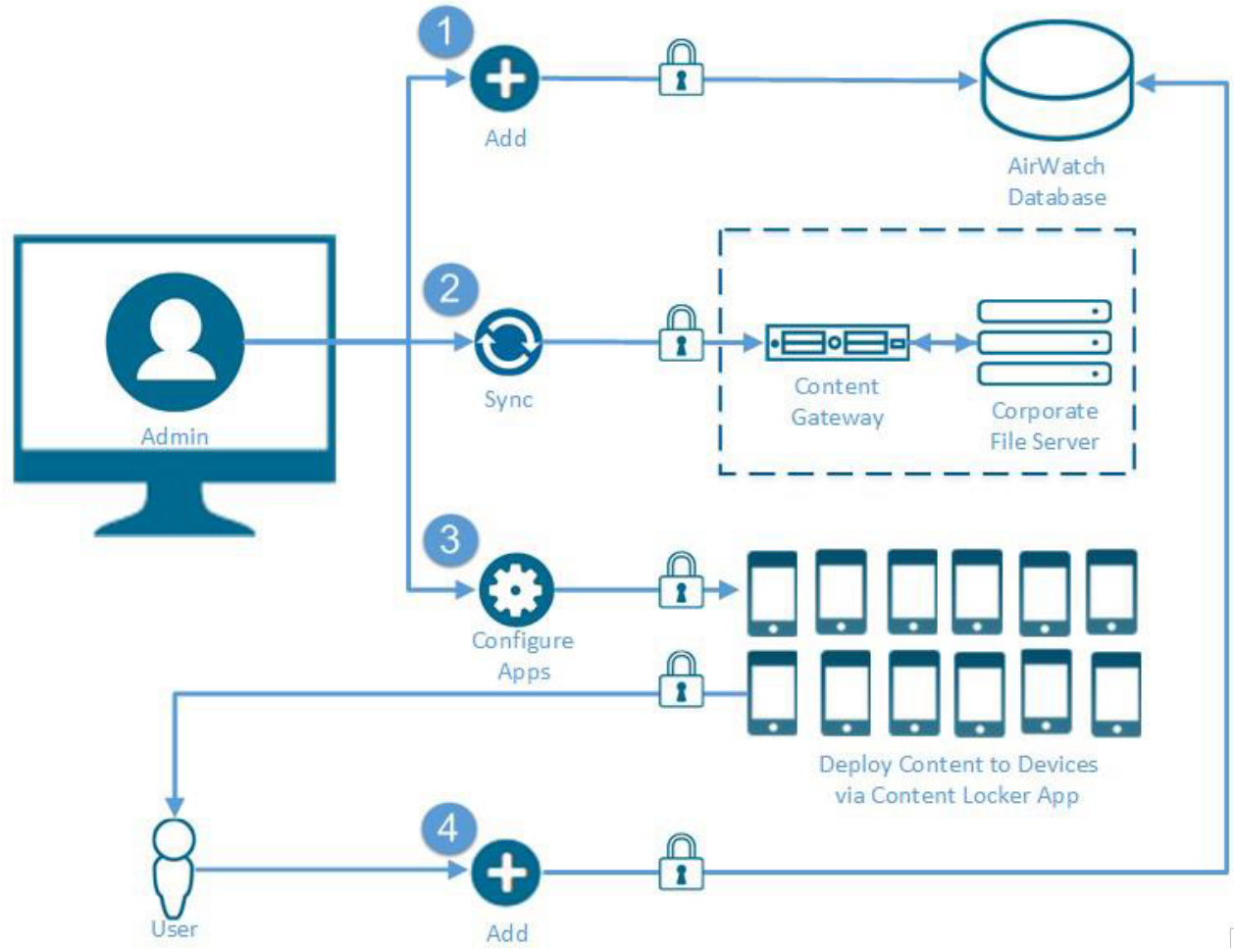
VMware Spain, S.L.
Calle Rafael Boti 26
2.ª planta
Madrid 28023
Tel.: +34 914125000
www.vmware.com/es

Contenido

Introducción a la administración de contenido móvil

Workspace ONE UEM con tecnología AirWatch proporciona la solución Mobile Content Management™ (MCM) que ayuda a su organización a abordar el desafío que presenta la implementación segura de contenido en una amplia variedad de dispositivos mediante medidas clave. Utilice Workspace ONE UEM console para crear, sincronizar o habilitar una ubicación de almacenamiento de archivos conocida como repositorio. Después de la configuración, el contenido se implementa en los dispositivos de los usuarios finales a través de la aplicación VMware Workspace ONE Content.

Para comprender cómo funciona la gestión de contenido, lea atentamente el siguiente esquema.



1. Repositorio de contenido administrado por UEM: es el repositorio en que los administradores de Workspace ONE UEM que tengan los permisos adecuados disfrutan de control completo sobre los archivos que se almacenan allí.

2. Servidor de archivos corporativos: es un repositorio existente que reside dentro de la red interna de la organización. Dependiendo de la estructura de la organización, el administrador de Workspace ONE UEM puede o no tener permisos administrativos para el servidor de archivos corporativos.
3. VMware Workspace ONE Content: es la aplicación que se implementa en los dispositivos de los usuarios finales para habilitar el acceso al contenido dentro del marco de parámetros definidos.

Requisitos de la administración de contenido móvil

La administración de contenido móvil (MCM) proporciona una flexible gama de servicios que puede implementar. Cada uno incluye su propia lista de requisitos. Antes de configurar MCM, es importante que revise los servicios que desea configurar y que confirme que cumple con los requisitos básicos.

Componente	Requisitos y descripción
Requisitos de software y hardware	
Navegadores compatibles	Workspace ONE Unified Endpoint Management (UEM) Console admite las compilaciones estables más recientes de los siguientes navegadores web: Chrome Firefox Safari Internet Explorer 11 Microsoft Edge Nota: Si utiliza IE 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 establecida como Habilitada. Si utiliza un navegador más antiguo que los mencionados, actualice el navegador para garantizar el rendimiento de la consola de UEM. Se han realizado pruebas integrales de las plataformas para garantizar la funcionalidad de estos navegadores web. Si decide utilizar un navegador no certificado, es posible que tenga algunos problemas menores con la consola de UEM.
Requisitos de plataforma	iOS 12.2 y versiones posteriores Android 8 y versiones posteriores 10.9 Mavericks y versiones posteriores
Requisitos de marco	.NET 4.0.3 y versiones posteriores .NET 4.5 y versiones posteriores Mono
Requisitos de Visual Studio	Visual Studio 2010 v10.0.50903 Visual C++ 2008
Otro	Uso compartido de vínculos habilitado Microsoft Outlook 2007 o superior (32 o 64 bits)
Requisitos de rol	

Componente	Requisitos y descripción
Roles administrativos	Seleccione una función que tenga las opciones Content, Instalar contenido en el dispositivo y Eliminar contenido del dispositivo habilitadas de forma predeterminada. Otorga acceso a la página de administración de contenido y control sobre la distribución de contenido. Para obtener más información sobre la creación de roles, consulte la guía *Roles and Added Resources Guide*.
Roles de los usuarios finales	Habilitar Administrar contenido y otorgar acceso completo Para obtener más información sobre cómo crear funciones, consulte la *Guía de funciones y recursos añadidos*.
Requisitos de repositorio	
Contenido administrado por UEM	Configure la estructura de categorías antes de cargar contenido. No puede agregar subcategorías a las categorías que ya tienen contenido.
Contenido del servidor de archivos corporativos	Instalar Content Gateway Instale Content Gateway para establecer una conexión en los casos en los que el dominio del servidor de Workspace ONE UEM no pueda acceder al servidor de archivos corporativos. Para revisar qué repositorios compatibles de Workspace ONE UEM requieren, admiten o no admiten Content Gateway, consulte Compatibilidad de los servidores de archivos corporativos. Para ver las instrucciones de instalación detalladas, consulte la guía *Content Gateway Installation Guide*.
Requisitos de almacenamiento de archivos alternativo	
Almacenamiento local de archivos	Determinar la solución adecuada para la organización Para obtener más información acerca de las opciones disponibles, consulte Almacenamiento local de archivos para el contenido administrado de AirWatch.
Requisitos de componente de seguridad opcional	
Incorporación	Cumplir con los requisitos mínimos de la aplicación y del SO iOS VMware Workspace ONE Content v2.4+ Dispositivo con iOS 7+
Requisitos de aplicación	Workspace ONE Content

Content Gateway

Workspace ONE UEM con tecnología AirWatch proporciona la solución de administración de contenido que, junto con otros componentes de integración empresarial, hace frente al reto único de proteger el contenido de los dispositivos móviles. Content Gateway es un componente de este tipo que facilita a los usuarios finales el poder acceder de forma segura al contenido.

Content Gateway, junto con la aplicación VMware Workspace ONE Content, permite a los usuarios finales acceder de forma segura a contenido desde un repositorio interno. Esto significa que los usuarios finales podrán acceder de forma remota a su documentación, documentos financieros, libros, y de una forma más directa desde repositorios de contenido o recursos compartidos de archivos internos. Dado que los archivos se agregan o actualizan dentro del repositorio de contenido existente, los cambios se reflejarán de forma inmediata en la aplicación VMware Workspace ONE Content, y los usuarios solo podrán acceder a sus archivos y carpetas aprobados según las listas de control de acceso definidas en el repositorio interno. Mediante Content Gateway, junto con la aplicación VMware Workspace ONE Content, podrá proporcionar niveles de acceso inigualables al contenido corporativo sin poner en peligro la seguridad.

Almacenamiento de archivos

En Workspace ONE UEM Console hay disponibles varios tipos de contenido para la configuración que se pueden implementar en la aplicación VMware Workspace ONE Content en los dispositivos de usuarios finales. Aunque el tipo de contenido no afecta a la ubicación de implementación, el almacenamiento back-end varía según el tipo de contenido.

Para obtener información sobre las opciones de almacenamiento disponibles para cada tipo de contenido, revise la tabla. Obtenga más información sobre los requisitos adicionales de configuración y los componentes para cada opción de almacenamiento.

agregado por el usuario	Configuraciones	Componentes	Notas
Contenido administrado por Workspace ONE UEM			
Base de datos de Workspace ONE UEM	X	X	
Almacenamiento local de archivos	√	√	Modificar en un grupo organizativo de nivel global Solo local
Servidores de archivos corporativos			
Base de datos de Workspace ONE UEM	X	X	El contenido sincronizado solo almacena metadatos en la base de datos de Workspace ONE UEM.
Repositorios de red	√	√/X	Algunos repositorios requieren Content Gateway. Los requisitos varían según el tipo de repositorio.

Servidores de archivos corporativos

La solución de administración de contenido admite la integración con sus servidores de archivos corporativos (CFS). Los servidores de archivos corporativos son repositorios existentes que residen dentro de la red interna de la organización.

Funciones

La integración del servidor de archivos corporativos admite las siguientes funciones:

- Integración segura
- Proteger el acceso a la red interna de la organización
- Opciones de integración avanzadas mediante Content Gateway

Seguridad

La solución Content Management ofrece las siguientes opciones de seguridad:

- Cifrado SSL para el tránsito de datos
- Control sobre el acceso y los derechos de descarga de los administradores de Workspace ONE UEM
- Contenido almacenado en la red de la organización
- Solo metadatos almacenados en la base de datos de Workspace ONE UEM. Soporte para revisión y administración de los metadatos almacenados.

Implementación

Dependiendo de la estructura de la organización, el administrador de Workspace ONE UEM puede o no tener permisos administrativos para un CFS. Una vez que la solución Content Management está integrada con CFS, los dispositivos de los usuarios finales pueden sincronizar el contenido desde los servidores con la ayuda de VMware Wokspace ONE Content.

Compatibilidad de los servidores de archivos corporativos

Workspace ONE UEM admite la integración con varios servidores de archivos corporativos. La compatibilidad con el método de sincronización y el requisito del componente de Content Gateway varían según el tipo de repositorio.

Métodos de sincronización disponibles

Vea los métodos de sincronización disponibles para los repositorios:

- Administrador: repositorio completamente configurado y sincronizado por un administrador en la consola de UEM. Cada usuario asignado recibe el mismo vínculo estático al repositorio de archivos.

- Automático: hace referencia a un repositorio que configura un administrador en UEM Console, pero permite que el administrador use valores de búsqueda dinámica. El repositorio lo sincronizan los usuarios finales en sus dispositivos. Cada usuario asignado recibe un vínculo único o semiúnico a un repositorio de archivos. Esta es una opción útil para vincular los directorios principales de los usuarios.
- Manual: hace referencia a un repositorio que se configura en UEM Console, pero permite al administrador establecer una parte estática y una parte variable (comodín) de un vínculo. Cada usuario final puede agregar manualmente un vínculo del repositorio con el formato establecido por el administrador y sincronizar el repositorio en sus dispositivos.

Aviso: Independientemente del número de archivos presentes en las carpetas del repositorio, solo se sincronizarán con el dispositivo 1000 archivos de cualquier carpeta que se encuentre ordenada alfabéticamente.

Matriz del servidor de archivos corporativos

Utilice la matriz para determinar los métodos de sincronización compatibles y los requisitos de Content Gateway según el tipo de repositorio:

Repositorios disponibles	Administración	Automatic	Manual
Box	✓	✓	✓
CMIS	✓	✓	✓
Google Drive	✓	–	–
Recurso compartido de red	✓	✓	✓
OneDrive	✓	–	–
OneDrive para la Empresa	✓	–	–
ADFS de OneDrive para la Empresa	✓	–	–
OneDrive para la Empresa OAuth	✓	–	–
SharePoint	✓	✓	✓
ADFS de SharePoint	✓	✓	✓
SharePoint 0365	✓	✓	✓
ADFS de SharePoint O365	✓	✓	✓
SharePoint O365 OAuth	✓	–	–
SharePoint - Personal (Mis sitios)	✓	–	–
SharePoint WebDAV	✓	–	–
Autenticación de Windows de SharePoint	✓	✓	✓
WebDAV	✓	✓	✓
Acceder mediante Content Gateway			
Box	–	–	–

Repositorios disponibles	Administración	Automatic	Manual
CMIS	✓+	✓+	✓+
Google Drive	–	–	–
Recurso compartido de red	✓+	✓+	✓+
OneDrive	–	–	–
OneDrive para la Empresa	✓	–	–
ADFS de OneDrive para la Empresa	✓	–	–
SharePoint	✓	✓	✓
ADFS de SharePoint	✓	✓	✓
SharePoint 0365	✓	✓	✓
ADFS de SharePoint O365	✓	✓	✓
SharePoint - Personal (Mis sitios)	✓	–	–
SharePoint WebDAV	✓	–	–
Autenticación de Windows en SharePoint (Content Gateway para Linux)	–	–	–
Autenticación de Windows en SharePoint (Content Gateway para Windows)	✓	✓	✓
WebDAV	✓	✓	✓
Extensiones de documentos			
Box	✓	✓	✓
CMIS	✓	✓	✓
Google Drive	✓	–	–
Recurso compartido de red	✓*	✓*	✓*
OneDrive	✓	–	–
OneDrive para la Empresa	✓	–	–
ADFS de OneDrive para la Empresa	✓	–	–
OneDrive para la Empresa OAuth	✓	–	–
SharePoint	✓ **	✓ **	✓ **
ADFS de SharePoint	✓ **	✓ **	✓ **
SharePoint 0365	✓ **	✓ **	✓ **
ADFS de SharePoint O365	✓ **	✓ **	✓ **
SharePoint O365 OAuth	✓	–	–
SharePoint - Personal (Mis sitios)	✓ **	–	–
SharePoint WebDAV	✓ **	–	–

Repositorios disponibles	Administración	Automatic	Manual
Autenticación de Windows de SharePoint	✓ **	✓ **	✓ **
WebDAV	✓*	✓*	✓*

Leyenda:

¥ = VMware Content Gateway en los servidores Linux solo admite SMB v2.0 y SMB v3.0. La versión compatible predeterminada es SMB v2.0.
✓+ = requerido
✓ = compatible
– = no compatible
✓ * = compatible, con limitaciones. Acceso limitado a los archivos de los repositorios anteriormente abiertos en VMware Workspace ONE Content.
✓ ** = Compatible, con limitaciones. Acceso limitado a los archivos anteriormente descargados en Workspace ONE Content.

Cómo habilitar el acceso de los usuarios finales a contenido del servidor de archivos corporativos

Sincronice los servidores de archivos corporativos existentes de la red con Workspace ONE UEM; para ello, configure un repositorio administrativo, un repositorio agregado por el usuario automático o un repositorio agregado por el usuario manual. Las configuraciones disponibles afectan al "desencadenador" que inicia la sincronización del contenido con los dispositivos.

Utilice este resumen sobre la configuración en el nivel de macros para obtener información sobre cómo permitir a los usuarios finales acceder al contenido del servidor de archivos corporativos.

1. Configure un repositorio en la consola de UEM.
2. Descargue y ejecute el programa de instalación de Content Gateway configurado.
3. Compruebe la conectividad entre la consola de UEM y Content Gateway.
4. Evalúe la necesidad que tiene su organización de contar con varios nodos de Content Gateway.

   Las organizaciones globales con problemas de latencia provocados por separaciones geográficas pueden utilizar esta funcionalidad.
5. Configure un repositorio administrativo o sincronice los servidores de archivos corporativos (CFS) en la consola de UEM.

   Si configura un repositorio de administrador, seleccione Probar conexión para comprobar la conectividad.
6. Configure VMware Workspace ONE Content en la consola UEM.
7. Implemente las aplicaciones de Workspace ONE UEM en la flota de dispositivos.

Cómo configurar un repositorio administrativo

Configure un repositorio administrativo para sincronizar los servidores de archivos corporativos existentes de la red con Workspace ONE UEM. Después de la sincronización, los usuarios finales pueden acceder al contenido del servidor de archivos corporativo desde sus dispositivos.

1. Desplácese a Content > Repositorios > Repositorios de administradores en UEM Console.
2. Seleccione Agregar.
3. Configure los ajustes que aparecen.

Ajustes	Descripción
Nombre	Etiquete el directorio de contenido
Tipo	Seleccione un servidor de archivos corporativos en el menú desplegable.
Enlace	Proporcione la ruta completa a la ubicación del directorio en lugar del domino raíz. Ejemplo: http://SharePoint/Corporate/DocumentsEs posible que una URL copiada directamente de un navegador web no tenga permiso para acceder a un servidor en determinados tipos de repositorios. Aviso: Si el repositorio seleccionado es un repositorio de OAuth, la URL del repositorio debe contener "/personal". Por ejemplo, si la URL del repositorio es xyz.abc.com, debe agregar la URL como xyz.abc.com/personal.
Grupo organizativo	Asigne acceso al servidor de archivos corporativos a un grupo de usuarios seleccionado.
Usar credenciales derivadas de PIV-D	Este ajuste solo está disponible cuando se selecciona SharePoint como el tipo de repositorio. Seleccione la casilla de verificación para usar la autenticación de certificados de PIV-D para autenticar a los usuarios en lugar de los nombres de usuario y contraseñas. La autenticación de certificados de PIV-D es para la autenticación de los usuarios que desean acceder a los repositorios de SharePoint locales desde sus dispositivos. Nota: Para habilitar el uso de credenciales derivadas de PIV-D se requiere la configuración de Kerberos en los ajustes de Content Gateway. Para obtener información sobre los ajustes de autenticación de certificados en Content Gateway, consulte el tema *Configurar Content Gateway en UEM Console* en la documentación de Content Gateway.
Acceder vía MAG/Content Gateway	Utilice Content Gateway si el dominio del servidor de Workspace ONE UEM no puede acceder al servidor de archivos corporativos.
Content Gateway	Identifique el nombre único del nodo de Content Gateway correspondiente en el menú desplegable.
Permitir herencia	Permita que los grupos organizativos secundarios hereden los mismos permisos de acceso del grupo organizativo primario.
Permitir la escritura	Permita que los usuarios finales creen y carguen archivos y carpetas, editen documentos y realicen retiros/devoluciones de archivos en repositorios externos desde sus dispositivos.

Ajustes	Descripción
Permitir acciones de archivos	Este ajuste solo está disponible cuando se selecciona SharePoint O365 OAuth o OneDrive para empresa Oauth como tipo de repositorio. Seleccione la casilla de verificación para permitir que los usuarios de la aplicación Workspace ONE Content cambien el nombre, muevan y eliminen archivos en los repositorios de nube.
Permitir eliminación	Permite la eliminación remota de contenido para el repositorio de recurso compartido de red. Con esta característica, el usuario final puede eliminar el contenido permanentemente del repositorio de recurso compartido de red utilizando la aplicación Workspace ONE Content.
Tipo de autenticación	Seleccione el nivel de acceso que los administradores tienen en los servidores de archivos corporativos desde la consola de UEM. Ninguno: impide que los administradores vean y descarguen contenido del servidor de archivos corporativos desde UEM Console. Usuario: permite la navegación en la estructura de archivos del repositorio dentro de UEM Console. Introduzca las credenciales en los cuadros de texto Nombre de usuario y Contraseña que aparecen. Aviso: Si se ha seleccionado la casilla de verificación Usar credenciales derivadas de PIV-D, el cuadro de texto de la contraseña no aparecerá. Proporcione el Nombre principal del usuario del usuario en el cuadro de texto Nombre de usuario.
Permitir la carga solo desde la cámara	Seleccione esta opción para permitir que los usuarios carguen imágenes solo desde la cámara del dispositivo.

4. Seleccione Probar conexión para verificar la conectividad. Un resultado positivo indica que el servidor de archivos corporativos se integró sin problemas.
5. Complete los detalles en las pestañas de seguridad, asignación e implementación.

   a. En la pestaña Seguridad, complete los cuadros de texto para controlar cómo comparten y mueven los usuarios finales documentos confidenciales fuera de los medios corporativos.

   La opción Forzar cifrado se ha eliminado de Workspace ONE UEM Console versión 9.5. La aplicación VMware Workspace ONE Content cifra todos los archivos de forma predeterminada, tanto si la opción está disponible como si no.

Ajustes	Descripción
Uso compartido de documentos	Deshabilite la configuración de uso compartido para obtener la máxima seguridad. Puede habilitarla para configurar la colaboración de usuario final.
Control de acceso	Configure esta opción como Permitir ver fuera de línea para proporcionar a los usuarios finales la máxima libertad posible para ver sus documentos. Configure la función Permitir ver solamente en línea para garantizar que todos los dispositivos que accedan al contenido cumplan con las políticas de conformidad, ya que Workspace ONE UEM no puede examinar la conformidad de los dispositivos si están fuera de línea.

Ajustes	Descripción
Permitir que se abra en correo electrónico	Permita que el contenido se abra en los correos electrónicos. Los usuarios no pueden abrir archivos de más de 10 MB. Para permitir que los usuarios abran archivos de más de 10 MB, debe editarlos en UEM Console y habilitar esta opción. Los archivos de los repositorios de usuario no se pueden editar.
Permitir que se abra en una aplicación de terceros	Otorgue permiso para abrir este contenido en otras aplicaciones. Puede configurar una lista de aplicaciones aprobadas en el perfil de SDK. Si se deshabilita esta opción, también se deshabilita el permiso del usuario final para imprimir los documentos PDF desde VMware Workspace ONE para iOS.
Permitir que se guarde en otros repositorios	Seleccione esta opción para permitir a los usuarios finales guardar el archivo en el repositorio de contenido personal.
Habilitar la marca de agua	Seleccione esta opción para agregar una superposición de marca de agua al archivo. Configure el texto superpuesto de la marca de agua como parte del perfil de SDK.
Permitir impresión	Otorgue permiso a los usuarios finales para que puedan imprimir documentos PDF desde VMware Workspace ONE Content para iOS a través del servidor de AirPrint. Una vez impreso, el contenido queda fuera del control del administrador de Workspace ONE UEM. La impresión solo es compatible si se habilita la opción Permitir que se abra en una aplicación de terceros.
Permitir modificación	Este ajuste solo se aplica a los repositorios que tienen permisos de escritura.

b. En la pestaña Asignación, configure los ajustes para controlar qué usuarios tendrán acceso al contenido. Esta función garantiza que solo los empleados autorizados tengan acceso al material confidencial o sensible y le permite configurar una jerarquía con niveles de acceso al contenido.

Ajustes	Descripción
Tipo de propiedad del dispositivo	Defínala como Cualquiera, Corporativa - Dedicada, Corporativa - Compartida, Propiedad del empleado o Sin definir.
Grupos organizativos	Para asignar el contenido a un nuevo grupo, empiece a escribir en el cuadro de texto.
Grupos de usuarios	Asigne grupos si está integrándose con los servicios de directorio o grupos de usuarios personalizados.

c. En la pestaña Implementación, configure los ajustes para controlar cómo y cuándo acceden los usuarios finales al contenido.

Ajustes	Descripción

Método de transferencia	Especifique Cualquiera o Solo Wi-Fi en el menú desplegable. Restringir las transferencias a Wi-Fi obliga a que los dispositivos se registren en Workspace ONE UEM para garantizar la conformidad.
Descargar durante roaming	Habilite esta opción para que los usuarios descarguen contenido durante roaming.
Tipo de descarga	Configure esta opción para implementar contenido de una de estas dos formas: Automáticamente: se instala en los dispositivos cuando el contenido está disponible. A pedido: se instala en los dispositivos solo cuando el usuario final lo solicita.
Prioridad de descarga	Defina esta opción para comunicar a los usuarios finales la prioridad de descarga: Normal, Alto/a o Bajo/a.
Obligatorio	Seleccione esta opción para marcar contenido como requerido en VMware Workspace ONE Content. Los usuarios finales deben descargar y revisar el contenido requerido para que sus dispositivos se mantengan conformes con Workspace ONE UEM.
Fecha de vigencia	Especifique una fecha para configurar un intervalo limitado durante el cual el contenido estará disponible.
Fecha de caducidad	Especifique una fecha para configurar un intervalo limitado durante el cual el contenido estará disponible.

6. Seleccione Guardar.

Acceda al vínculo correcto

Asegúrese de que Content Gateway esté configurado con el vínculo correcto. Esta regla en particular se aplica a SharePoint 2013, Office 365 y versiones más recientes. Algunas direcciones URL no están diseñadas para que aplicaciones y servicios accedan a ellas y solo aceptan acceso de un navegador web. Si al configurar Content Gateway se introduce una dirección URL que acepta "solo navegadores" como enlace, se producirá un error de conexión.

1. Introduzca la dirección URL en el navegador.
2. Desplácese a PÁGINA > Editar propiedades > Ver propiedades.
3. Haga clic con el botón secundario y copie la dirección del enlace.
4. Pegue la dirección en el cuadro de texto Enlace en la consola de UEM.

Cómo habilitar los usuarios para sincronizar servidores de archivos corporativos

Integre Workspace ONE UEM con los repositorios de contenido existentes mediante la configuración de una plantilla manual o automática que los usuarios finales podrán sincronizar desde sus dispositivos. Después de la sincronización, los usuarios finales pueden acceder al contenido del servidor de archivos corporativo desde sus dispositivos. El uso de Content Gateway con servidores de archivos corporativos permite a los usuarios finales agregar, editar y cargar contenido en el servidor de archivos corporativo de forma segura.

Los pasos pueden variar al configurar una plantilla manual o automática.

1. Navegue a la página correspondiente en la consola de UEM.

Tipo de servidor de archivos corporativos	Ubicación
Plantilla automática	Content > Repositorios > Plantillas > Automático
Plantilla manual	Content > Repositorios > Plantillas > Manual

2. Seleccione Agregar.
3. Complete los cuadros de texto que aparecen. Los cuadros de texto pueden cambiar al configurar un repositorio administrativo, una plantilla automática o una plantilla manual.

Ajustes	Descripción
Nombre	Introduzca el nombre del directorio de contenido.
Nombre del repositorio de usuarios (solo plantilla automática)	Utilice los valores de búsqueda para nombrar el repositorio después del usuario final en VMware Workspace ONE Content.
Tipo	Seleccione un servidor de archivos corporativos en el menú desplegable.
Enlace	Es posible que una dirección URL copiada directamente de un navegador web no tenga permiso para acceder a un servidor en determinados tipos de repositorios.
Enlace (solo plantilla automática)	Utilice los valores de búsqueda para crear un repositorio cuando el usuario final acceda a VMware Workspace ONE Content. Ejemplo: https://sharepoint.acme.com/share/{EnrollmentUser}
Enlace (solo plantilla manual)	Proporcione la ruta a la ubicación del directorio utilizando * como comodín para un vínculo de dominio. Ejemplo: http://*.sharepoint.com Puede agregar un nuevo vínculo a una plantilla manual existente, pero no puede editar ni eliminar un vínculo existente. Preste atención cuando agregue nuevos vínculos de la lista de no permitidos, ya que no puede editar ni eliminar los vínculos si hay algún error. Cualquier corrección realizada a los vínculos requiere la eliminación de toda la plantilla.
Vínculos denegados	Especifique los valores del carácter comodín (*) en las rutas de archivo. Los valores especificados para * al principio y al final de la ruta de archivo evitan que los usuarios creen repositorios y subcarpetas manuales mediante la plantilla manual.
Grupo organizativo	Asigne acceso al servidor de archivos corporativos a un grupo de usuarios específico.

Ajustes	Descripción
Utilizar credenciales derivadas	Este ajuste solo está disponible cuando se selecciona SharePoint como el tipo de repositorio. Seleccione la casilla de verificación para usar la autenticación de certificados de PIV-D para autenticar a los usuarios en lugar de los nombres de usuario y contraseñas. La autenticación de certificados de PIV-D es para la autenticación de los usuarios que desean acceder a los repositorios de SharePoint locales desde sus dispositivos. Aviso: Para habilitar el uso de credenciales derivadas de PIV-D se requiere la configuración de Kerberos en los ajustes de Content Gateway. Para obtener información sobre los ajustes de autenticación de certificados en Content Gateway, consulte el tema *Configurar Content Gateway en UEM Console* en la documentación de Content Gateway.
Acceder vía MAG/Content Gateway	Utilice Content Gateway si el dominio del servidor de Workspace ONE UEM no puede acceder al servidor de archivos corporativos.
Permitir herencia	Permita que los grupos organizativos secundarios hereden los mismos permisos de acceso del grupo organizativo primario.
Permitir la escritura	Permita que los usuarios finales creen y carguen archivos y carpetas, editen documentos y realicen retiros/devoluciones de archivos en repositorios externos desde sus dispositivos.

Compatibilidad con la autenticación de certificados de PIV-D

A los usuarios de la aplicación Workspace ONE Content se les otorga acceso a los repositorios de SharePoint y de recursos compartidos de red locales una vez que los usuarios se autentican mediante las credenciales derivadas de PIV-D. La autenticación basada en certificados acaba con el requisito del nombre de usuario y la contraseña.

Los repositorios locales, como SharePoint y de recursos compartidos de red, pueden configurarse para utilizar las credenciales derivadas de PIV-D para la autenticación. La configuración de los repositorios para usar la credencial derivada de PIV-D requiere la configuración de Kerberos en los ajustes de VMware Content Gateway.

Se deberán considerar los siguientes requisitos previos para la configuración de la autenticación de certificados de PIV-D:

- El servidor de delegación limitada de Kerberos (KCD) debe configurarse con los SPN correctos (Nombres de entidad de servicio).
- Active Directory debe sincronizarse con Workspace ONE UEM, con el Nombre principal del usuario (UPN) como atributo.
- La cuenta de servicio debe estar disponible para Workspace ONE UEM y VMware Content Gateway para usarla como parte del flujo de trabajo de autenticación de Kerberos.
- Se deberá proporcionar a Content Gateway un certificado de confianza de la entidad de certificación (CA) que emite los certificados de usuario. Estos certificados pueden ser solo certificados intermedios o bien la cadena de certificados completa en función de los requisitos de validación de la CA.

En el caso de un repositorio de recursos compartidos de red, asegúrese de que las claves de configuración se establezcan de la siguiente forma: jcifs en false y jcifsng en true.

Rendimiento de la memoria caché

Cuando se almacena en caché todo el repositorio corporativo, pueden producirse picos de memoria en el servidor de servicios de dispositivos debido a la escasez de memoria interna. La memoria caché debe deshabilitarse cada vez para soportar la carga en el servidor de servicios de dispositivos.

Aviso: El script de base de datos que se utiliza para deshabilitar la memoria caché ya no es compatible desde la versión 1904 de Workspace ONE UEM. La memoria caché se puede deshabilitar cambiando ContentCacheFeatureFlag a false en la API, https:///api/system/featureflag//<OG_GUID>/false.

La estrategia de almacenamiento en la memoria caché Just-in-Time elimina el problema de memoria insuficiente al almacenar en caché solo las carpetas y los registros de contenido a los que el usuario accede. Las carpetas y el contenido no deseados se eliminan de la memoria caché.

Las carpetas se almacenan en la memoria caché individualmente con la clave de caché `folderId`, en lugar de almacenar en caché todo el repositorio mediante la clave de caché `RepoId`.

En caso de error de la memoria caché, el servidor de servicios de dispositivos solo carga los metadatos de las carpetas actuales de la base de datos y los almacena en la memoria caché. En caso de acierto de la memoria caché, el servidor de servicios de dispositivos lee solo la estructura de carpetas del nivel raíz de la memoria caché.

Repositorio de contenido administrado por Workspace ONE UEM

El repositorio de contenido administrado por UEM se refiere a una ubicación en la que los administradores que tengan los permisos adecuados tienen control completo sobre los archivos que se almacenan allí. Mediante la aplicación VMware Workspace ONE Content, los usuarios finales pueden acceder al contenido añadido desde el repositorio etiquetado como administrado por UEM, pero no pueden editar el contenido.

Funciones

El repositorio de contenido administrado proporciona las siguientes funciones:

- Carga manual de archivos
- Opciones para configurar y otorgar permisos a archivos individuales
- Opciones de sincronización para controlar el contenido al que se accede desde los dispositivos de los usuarios finales
- Vista en lista de las opciones avanzadas de administración de archivos

Seguridad

Para proteger el contenido que se almacena y sincroniza desde el repositorio en los dispositivos de los usuarios finales, tiene a su disposición las siguientes funciones de seguridad:

- El cifrado SSL protege los datos durante el tránsito entre UEM Console y los dispositivos de usuario final.
- Funciones con PIN de seguridad para el acceso controlado al contenido.

Implementación

El contenido del repositorio administrado por UEM se almacena en la base de datos de Workspace ONE UEM. Puede elegir alojar la base de datos en la nube de Workspace ONE UEM o en la sede, según cuál sea su modelo de implementación.

Configuración de la estructura de categorías del contenido administrado por UEM

Las categorías de contenido ayudan a mantener organizado el contenido del repositorio administrado por UEM en la consola de UEM y en la aplicación Workspace ONE Content. Configure la estructura de categorías para el contenido administrado por UEM antes de cargar contenido a la consola de UEM.

1. Desplácese a Content > Categorías > Agregar categoría.
2. Configure los ajustes que aparecen y seleccione Guardar.

Ajustes	Descripción
Administrado por	Seleccione el grupo o los grupos organizativos a los que desee aplicar la categoría.
Nombre	Introduzca un nombre que sea fácil de reconocer y que sea aplicable a un conjunto claro de contenido.
Descripción	Proporcione una breve descripción de la categoría.

3. Según sea necesario, agregue una subcategoría a la estructura de categorías.

   a. Seleccione Agregar en el menú de acciones.

   b. Configure los ajustes que aparecen y seleccione Guardar.

Ajustes	Descripción
Administrado por	Revise el grupo organizativo de la categoría primaria que se llena de forma predeterminada.
Nombre	Introduzca un nombre que sea fácil de reconocer y que sea aplicable a un conjunto claro de contenido.
Descripción	Proporcione una breve descripción de la subcategoría.

Carga de contenido en el repositorio administrado por UEM

Agregue archivos al repositorio de contenido administrado por UEM cargándolos y configurándolos manualmente en la consola de UEM. El repositorio almacena el contenido en la base de datos de Workspace ONE UEM de forma predeterminada y se sincroniza con la aplicación VMware Workspace ONE Content para distribuir el contenido a los dispositivos de los usuarios finales. Sin embargo, los usuarios finales no podrán editar el contenido administrado sincronizado.

1. Desplácese a Content > Vista de lista.
2. Seleccione Agregar contenido y elija Seleccionar archivos.
3. Seleccione un archivo individual en el cuadro de diálogo de carga.
4. Configure los ajustes de Información del contenido.

Ajustes	Descripción
Nombre	Revise el nombre de archivo que se completa automáticamente en este cuadro de texto.
Grupo organizativo	Revise el grupo organizativo en el que se distribuirá el contenido.
Archivo	Revise el archivo que se completa en este cuadro de texto.
Tipo de almacenamiento	Asegúrese de que el cuadro de texto muestre Administrado por UEM.
Versión	Asegúrese de que el número de versión sea 1.0, ya que está agregando este contenido a la consola de UEM por primera vez. Puede cargar versiones nuevas en el menú de acciones de la vista en lista de contenido administrado por UEM.

Ajustes	Descripción
Descripción	Proporcione una descripción de los archivos que cargó.
Importancia	Configure la importancia del contenido como Alto, Normal o Bajo.
Categoría	Asigne contenido a una categoría configurada.

5. Proporcione metadatos adicionales sobre el contenido en los ajustes de Detalles.

Ajustes	Descripción
Autor	Provea el nombre del autor de este archivo.
Notas	Provea notas sobre el archivo.
Asunto	Provea un asunto.
Palabras clave	Enumere las palabras clave y los temas que aparecen en este archivo.

Aviso: Independientemente del número de archivos que se agreguen a UEM Console, solo se sincronizarán con el dispositivo del usuario los metadatos de los primeros 10 000 archivos que están ordenados alfabéticamente.

Cargar el contenido administrado de Workspace ONE UEM en lotes

Utilice la función de importar por lotes para omitir la integración con un recurso compartido de archivos externo en una implementación SaaS dedicada o una implementación en las sedes que tenga una red robusta.

1. Navegue a Contenido > Estado del lote.
2. Seleccione Importar por lotes.
3. Proporcione el Nombre del lote y la Descripción del lote.
4. Para descargar un archivo de plantilla .csv, seleccione el icono de información ( ).
5. Complete el archivo .csv con la ruta de archivo y demás información para el contenido que desea cargar.
6. Seleccione Elegir archivo y elija el archivo .csv que creó.
7. Seleccione Abrir para seleccionar el archivo .csv.
8. Seleccione Guardar para cargar el archivo por lotes que está completado.

Cómo definir la capacidad de almacenamiento

La capacidad de almacenamiento es la cantidad de espacio asignado a contenido administrado en un grupo organizativo y sus grupos secundarios.

Aviso: Debe asegurarse de tener los privilegios de administrador necesarios para ver y utilizar la configuración de almacenamiento.

1. Desplácese a Grupos y ajustes > Todos los ajustes > AdministradorAlmacenamiento en un nivel de grupo organizativo de cliente o global.
2. Seleccione Contenido en el menú desplegable Tipo de almacenamiento.
3. Seleccione el icono Editar para el grupo organizativo adecuado. Aparecerá la ventana Administración de almacenamiento. Complete los siguientes ajustes.

Ajustes	Descripción
Nombre del grupo organizativo	Especifique el grupo al que desea aplicarle las restricciones de almacenamiento de contenido.
Capacidad	Defina el espacio máximo de almacenamiento (en MB) asociado al contenido almacenado en la base de datos de Workspace ONE UEM. El almacenamiento predeterminado para Workspace ONE Content proporcionado por VMware Workspace ONE UEM para los clientes de SaaS es de 5 GB.
Exceso permitido	Si desea permitir una cantidad de exceso, introduzca la cantidad permitida. Para los clientes de SaaS, este valor no es configurable.
Tamaño máximo del archivo	Utilice el valor predeterminado de 200 MB como el tamaño máximo para cargas. Si no sigue la recomendación, el límite máximo es de 2 GB.
Cifrado	Cifre el contenido con el estándar AES de 256 bits en el archivo. Al habilitar el cifrado se activa el programador de “Migración de cifrado de archivos”, el cual inicia la migración de todos los datos sin cifrar que encuentra.

4. Seleccione Guardar.

Restringir extensiones de archivo

Especifique los permisos del tipo de archivo mediante la creación de una lista de permitidos o una lista de no permitidos para el contenido administrado y el servidor de archivos corporativos. Esta restricción oculta los tipos de archivo bloqueados en base a su extensión para que no se vean en UEM Console o en Workspace ONE Content y, por lo tanto, impide que se puedan descargar o actualizar en repositorios de contenido.

1. Desplácese a Content > Ajustes > Avanzado > Extensiones de archivos.
2. Configure las Extensiones de archivos permitidos.

Ajustes	Descripción
Lista de admitidos	Introduzca las extensiones de archivo que desee incluir. Separe las extensiones con una nueva línea, una coma o un espacio.
Lista de denegación	Introduzca las extensiones de archivo que desee excluir. Separe las extensiones con un salto de línea, una coma o un espacio.
Todo	Seleccione los tipos de archivos que tendrán permiso para cargar o sincronizar.

3. Seleccione Guardar para aplicar la configuración.

Una vez aplicadas las restricciones, podrá anticiparse a las siguientes respuestas.

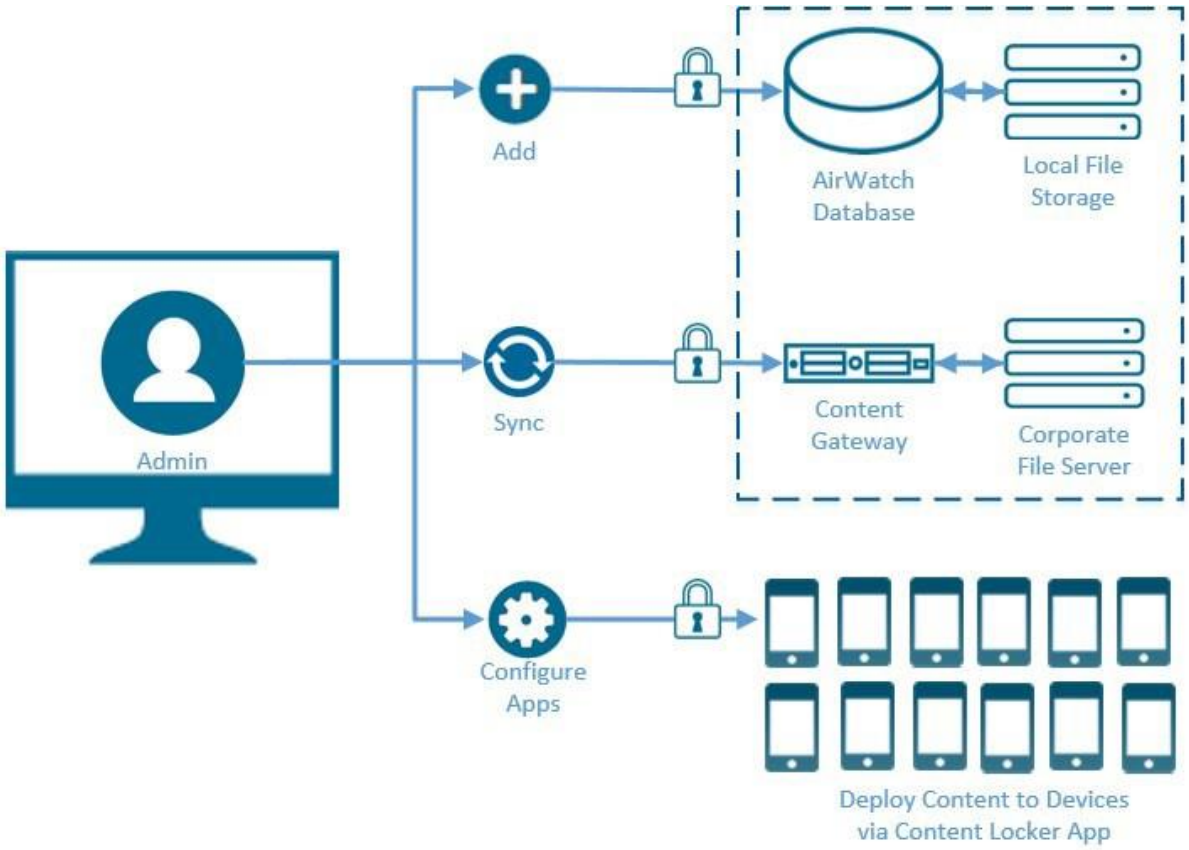
Respuesta	Quién	Qué	Dónde	agregado por el usuario
Mensaje de error	Administrator	Agrega manualmente un archivo restringido al repositorio de contenido	Console	Administrado por UEM
Interacción silenciosa	Administrator	Se sincroniza con un servidor de archivos corporativos que contiene un archivo restringido	Console	Servidor de archivos corporativos
Interacción silenciosa	Usuario final	Se sincroniza con un servidor de archivos corporativos que contiene un archivo restringido	Dispositivo (a través de la aplicación Workspace ONE Content)	Servidor de archivos corporativos

Almacenamiento local de archivos para contenido administrado de Workspace ONE UEM

El almacenamiento local de archivos separa el contenido administrado de la base de datos de Workspace ONE UEM, almacenándolo en una ubicación local dedicada con una conexión a la instancia de Workspace ONE UEM.

El contenido administrado se almacena en la base de datos de Workspace ONE UEM de forma predeterminada. Sin embargo, la carga de un gran volumen de contenido administrado puede provocar problemas de rendimiento en la base de datos. En este caso, los clientes en la sede pueden liberar espacio de la base de datos moviendo el contenido administrado a una solución de almacenamiento local de archivos integrada.

Aviso: Los clientes locales pueden configurar manualmente el almacenamiento de archivos, pero en el caso de los clientes SaaS, se configura automáticamente.



Para obtener información sobre la configuración del almacenamiento de archivos, consulte *Instalación*/*Ruta de archivo* en la documentación de *Ajustes de sistema* .

Exportación de informes de vista de lista de Content por lotes

El informe que exporta desde la página de la consola en Vista de lista de Content puede contener con frecuencia una gran cantidad de registros. A veces, la exportación de un informe en masa de este tipo puede causar problemas de tiempo de espera. Para evitar que se agote el tiempo de espera, el informe se puede dividir y exportar por lotes. De forma predeterminada, cada lote puede contener hasta 2000 registros.

De forma predeterminada, esta función está deshabilitada y, cuando se deshabilita, no se puede exportar el informe por lotes.

Informes personalizados

Mediante Workspace ONE Intelligence en Workspace ONE UEM Console, puede generar informes personalizados para recopilar y ver los detalles del contenido administrado instalado en los dispositivos de los usuarios finales. Este informe personalizado es diferente al informe de Detalles de contenido por dispositivo o al informe que exporte desde la página de la consola de Content > Vista de lista.

Para generar informes personalizados para el contenido, acceda a la interfaz de Workspace ONE Intelligence y seleccione la categoría de plantilla Contenido del dispositivo. Utilice un elemento de identificación de dispositivo, tales como un identificador de dispositivo, como parámetro de filtro.

Puede generar informes específicos de un contenido administrado o de un usuario.

Los detalles que puede ver para el contenido son:

- El número total y único de descargas del contenido en un mes para un rango de fechas específico según el repositorio.
- El número total de visualizaciones del contenido.

Los detalles que puede ver para un usuario específico son los siguientes:

- El número total de descargas del contenido por parte del usuario para un rango de fechas específico por repositorio.
- Lista de contenido que el usuario aún no ha visualizado.
- Fecha de la última descarga del contenido.
- Lista de usuarios a los que les falta una versión específica (generalmente la más reciente) de un documento.

Para obtener más información acerca de la generación de informes mediante Workspace ONE Intelligence, consulte *Informes para Workspace ONE Intelligence* en la documentación de Workspace ONE Intelligence.

Configuraciones de SDK del paquete de aplicaciones

Al configurar la aplicación debe seleccionar un perfil de aplicación predeterminado o personalizado. Esta acción aplica un perfil de SDK a la aplicación para agregar funciones adicionales a las aplicaciones de Workspace ONE UEM implementadas.

Para asegurarse de que la configuración de la aplicación funciona sin problemas, considere lo siguiente:

- Conozca la diferencia entre los perfiles de SDK predeterminados y personalizados.
- Determine qué perfil de SDK es más apropiado para la aplicación, predeterminado o personalizado.
- Asegúrese de haber configurado el tipo de perfil de SDK que desea aplicar.

Utilice el siguiente gráfico para determinar si desea aplicar un perfil de SDK Predeterminado o Personalizado a la aplicación y ver qué instrucciones de configuración debe utilizar para el perfil.

Puede definir los perfiles de SDK utilizando dos tipos diferentes de perfiles: Perfil de aplicación de SDK Predeterminado o Personalizado.

Predeterminado	Personalizado
Implementación	
Comparta ajustes de perfiles de SDK entre todas las aplicaciones configuradas en un grupo organizativo (GO) particular o uno de menor jerarquía.	Utilice los ajustes del perfil de SDK para una aplicación específica y reemplace los perfiles de SDK de ajustes predeterminados.
Ventaja	
Proporciona un punto central para la configuración de todas las aplicaciones en un determinado GO y sus grupos secundarios.	Ofrece control pormenorizado de las aplicaciones específicas y reemplaza los perfiles de SDK de ajustes predeterminados.
Configuración	
Grupos y ajustes > Todos los ajustes > Aplicaciones > Ajustes y políticas > Políticas de seguridad	Grupos y ajustes > Todos los ajustes > Aplicaciones > Ajustes y políticas > Perfiles
Leer más	
Continúe leyendo esta sección para conocer qué perfiles de SDK predeterminados corresponden a las aplicaciones implementadas.	*Obtenga más información acerca de la configuración personalizada del perfil de SDK en la Guía de administración de aplicaciones móviles de VMware Workspace ONE UEM.*

Configure los ajustes de seguridad predeterminados de SDK

Los ajustes predeterminados de SDK se aplican a todas las aplicaciones encapsuladas y de Workspace ONE UEM, y ofrecen una experiencia de usuario unificada en los dispositivos. Dado que los ajustes configurados de SDK se aplican a todas las aplicaciones encapsuladas y de Workspace ONE UEM de forma predeterminada, puede configurar el perfil de SDK predeterminado teniendo en cuenta todo el paquete de la consola Workspace ONE UEM y aplicaciones encapsuladas.

Las recomendaciones indicadas se aplican al paquete de aplicaciones que incluye:

- VMware Workspace ONE Web
- VMware Workspace ONE Content
- Dispositivos inscritos
- Aplicaciones encapsuladas o de Workspace ONE UEM
- Ajustes de SDK

No todas las plataformas o aplicaciones de Workspace ONE UEM son compatible con todos los ajustes de perfil de SDK predeterminados disponibles. Un ajuste configurado solo funciona en el dispositivo cuando se admite en la plataforma y la aplicación. También significa que un ajuste habilitado podría no funcionar de manera uniforme en una implementación multiplataforma, ni entre aplicaciones. La matriz Ajustes de SDK abarca los ajustes disponibles del perfil de SDK, así como las aplicaciones y plataformas a las que se aplican.

1. Desplácese a Grupos y ajustes > Todos los ajustes > Aplicaciones > Ajustes y políticas > Políticas de seguridad.
2. Configure las Políticas de seguridad y seleccione Guardar.

Acción	Descripción
Tipo de autenticación	
Contraseña	Solicite a los usuarios finales que se autentiquen con el código de acceso creado por ellos cuando la aplicación se inicie por primera vez y cuando se agote el tiempo de espera de la sesión. La habilitación o inhabilitación del SSO determina el número de sesiones de aplicación que pueden establecerse. Si se realiza una eliminación, es decir, cuando el usuario haya alcanzado el número máximo de intentos de código de acceso, la aplicación ya no volverá a cambiar a Hub. En su lugar, se iniciará el flujo de inicio de sesión independiente.
Nombre de usuario y contraseña	Solicite a los usuarios finales que se autentiquen volviendo a introducir las credenciales de inscripción cuando la aplicación se inicie por primera vez y cuando se agote el tiempo de espera de la sesión. La habilitación o inhabilitación del SSO determina el número de sesiones de aplicación que pueden establecerse.
Inhabilitado	Permita que los usuarios finales abran aplicaciones sin introducir credenciales.
SSO	
Habilitado	Establezca una sesión de aplicación única en todas las aplicaciones encapsuladas de Workspace ONE UEM y en la consola Workspace ONE UEM.
Inhabilitado	Establezca sesiones de aplicaciones por aplicación.
Acceso fuera de línea	

Acción	Descripción
Habilitado	Permita que los usuarios finales puedan abrir y utilizar las aplicaciones encapsuladas y de Workspace ONE UEM cuando no estén conectados a una conexión Wi-Fi. Las aplicaciones fuera de línea de Workspace ONE UEM no pueden realizar descargas. Para poder realizarlas los usuarios finales deben conectarse a Internet. Configure el Acceso fuera de línea para establecer los límites del acceso fuera de línea.
Inhabilitado	Elimine el acceso a las aplicaciones encapsuladas y de Workspace ONE UEM de los dispositivos que estén fuera de línea.
Protección contra el estado comprometido	
Habilitado	Reemplace la protección de MDM. La protección contra el estado comprometido a nivel de la aplicación bloquea los dispositivos comprometidos para que no se puedan inscribir y realiza una eliminación empresarial en los dispositivos cuyo estado esté comprometido.
Inhabilitado	Utilice solo el motor de conformidad de MDM para la protección contra dispositivos comprometidos.
Prevención de pérdida de datos	
Habilitado	Acceda a los ajustes y configúrelos para reducir las pérdidas de datos.
Habilitar copiar y pegar internamente	Permite copiar y pegar contenido de las aplicaciones externas en aplicaciones de Workspace ONE UEM cuando se configura en Sí.
Habilitar copiar y pegar externamente	Permite copiar y pegar contenido de las aplicaciones de Workspace ONE UEM en aplicaciones externas cuando se configura en Sí.Con el SDK de Swift de Workspace ONE, las restricciones se aplican en la generación de vínculos y la copia de los registros que no se vieron afectados anteriormente por las restricciones del portapapeles La acción de copiar y pegar es independiente de otras restricciones de DLP y no se ciñe a la inclusión de aplicaciones en la lista de permitidos. Por ejemplo, si se permite, la acción de copiar y pegar se puede llevar a cabo en cualquier aplicación externa y no está restringida solo a las aplicaciones de la lista de permitidos.
Habilitar la impresión	Permite que la aplicación realice impresiones desde los dispositivos cuando la opción configurada es Sí.
Habilitar la cámara	Permite que las aplicaciones accedan a la cámara del dispositivo cuando la opción configurada es Sí.
Habilitar redacción de correo electrónico	Permite que una aplicación utilice el cliente de correo nativo para enviar correos electrónicos cuando la opción configurada es Sí.
Habilitar copia de seguridad para los datos	Permite que aplicaciones encapsuladas sincronicen datos con un servicio de almacenamiento, como iCloud, cuando la opción configurada es Sí.

Acción	Descripción
Habilitar los servicios de ubicación	Permite que las aplicaciones encapsuladas reciban la latitud y longitud del dispositivo cuando la opción configurada es Sí.
Habilitar Bluetooth	Permite que las aplicaciones accedan a la funcionalidad de Bluetooth en los dispositivos cuando la opción configurada es Sí.
Habilitar captura de pantalla	Permite que las aplicaciones accedan a la funcionalidad de captura de pantalla en los dispositivos cuando la opción configurada es Sí.
Habilitar la marca de agua	Muestra el texto de la marca de agua en los documentos dentro de VMware Workspace ONE Content cuando la opción configurada es Sí. Introduzca el texto que desea mostrar en el campo Texto superpuesto o utilice valores de búsqueda. No puede cambiar el diseño de una marca de agua en la consola UEM.
Limitar que los documentos se abran solo en aplicaciones aprobadas	Introduzca las opciones para controlar las aplicaciones que se utilizan para abrir los recursos en los dispositivos. (Solo iOS) Puede utilizar los valores de configuración de Workspace ONE UEM para impedir que los usuarios importen archivos desde aplicaciones de terceros a Workspace ONE Content. Para obtener más información, consulte la sección Configurar la restricción de importación en Workspace ONE Content.
Lista de aplicaciones autorizadas	Introduzca las aplicaciones a las que les permite abrir los documentos.
Inhabilitado	Permita que los usuarios finales accedan a todas las funciones del dispositivo.

3. Desplácese a Grupos y ajustes > Todos los ajustes > Aplicaciones > Ajustes y políticas > Ajustes.
4. Configure los Ajustes y seleccione Guardar.

Acción	Descripción
Marca	
Habilitado	Aplique el logotipo y los colores de la organización al paquete de aplicaciones donde los ajustes tengan vigencia.
Inhabilitado	Mantenga la marca de Workspace ONE UEM en todo el paquete de aplicaciones.
Registro	

Acción	Descripción
Habilitado	Acceda a los ajustes y configúrelos para definir la recopilación de registros. Nivel de registro Podrá escoger entre una variedad de opciones de frecuencia de registro: Error: solo registra errores. Un error muestra lo que falló en los procesos como, por ejemplo, la imposibilidad de buscar UID o una dirección URL incompatible. Advertencia: registra solo errores y advertencias. Una advertencia muestra un posible problema en el proceso como, por ejemplo, códigos de respuesta dañados y autenticaciones de tokens no válidos. Información: registra una cantidad significativa de datos con fines informativos. El nivel de registro de información muestra los procesos generales, además de las advertencias y los mensajes de error. Depuración: registra todos los datos para ayudar en la solución de problemas. Esta opción no está disponible para todas las funciones. Enviar registros solo a través de Wi-Fi Seleccione esta opción para evitar la transferencia de datos durante la itinerancia y para limitar los cargos por datos.
Inhabilitado	No recopile registros.
Analíticas	
Habilitado	Recopile y vea estadísticas útiles sobre aplicaciones del paquete de SDK.
Inhabilitado	No recopile estadísticas útiles.
Ajustes personalizados	
Habilitado	Aplique código XML personalizado al paquete de aplicaciones.
Inhabilitado	No aplique código XML personalizado al paquete de aplicaciones.

Puede habilitar o deshabilitar ciertas funcionalidades de las aplicaciones de Workspace ONE Content y Workspace ONE Smartfolio agregando claves de configuración específicas en el perfil de SDK predeterminado o personalizado. Para obtener más información sobre cómo configurar los perfiles de SDK con las claves de configuración, consulte VMware Workspace ONE Content.

Comportamiento esperado de la autenticación de SDK

La habilitación o inhabilitación del SSO determina la cantidad de sesiones de aplicación que se establecen, lo que a su vez afecta a la cantidad de solicitudes de autenticación que los usuarios finales reciben.

Autenticación	SSO	Sesiones	Credenciales	Comportamiento esperado

Inhabilitado	Habilitado	Sencilla	Credenciales de inscripción	Abre aplicaciones sin solicitar a los usuarios finales que introduzcan credenciales.
Contraseña	Habilitado	Sencilla	Contraseña	Se solicita al iniciar la primera aplicación; establece una sola sesión de aplicación. La próxima solicitud de autenticación ocurre cuando se agota el tiempo de la sesión.
Nombre de usuario y contraseña	Habilitado	Sencilla	Credenciales de inscripción	Se solicita al iniciar la primera aplicación; establece una sola sesión de aplicación. La próxima solicitud de autenticación ocurre cuando se agota el tiempo de la sesión.
Contraseña	Inhabilitado	Por aplicación	Contraseña	Se solicita por cada aplicación; establece sesiones individuales de aplicación. Tenga en cuenta que cada aplicación puede tener un código de acceso distinto. La próxima solicitud de autenticación ocurre cuando se inicia una nueva aplicación o cuando se agota el tiempo de alguna aplicación individual.
Nombre de usuario y contraseña	Inhabilitado	Por aplicación	Credenciales de inscripción	Se solicita por cada aplicación; establece sesiones individuales de aplicación. La próxima solicitud de autenticación ocurre cuando se inicia una nueva aplicación o cuando se agota el tiempo de alguna aplicación individual.

VMware Workspace ONE Content

La solución de administración de contenido le proporciona la aplicación VMware Workspace ONE Content para habilitar el acceso de los usuarios finales al contenido administrado. La aplicación Workspace ONE Content se implementa en los dispositivos de usuario final y es posible acceder al contenido administrado en la aplicación dentro de los parámetros configurados.

Funciones

- Ajustes de contenido para definir comportamientos exclusivos de las aplicaciones.
- Utilice los ajustes predeterminados de SDK cuando se configura como parte del paquete de aplicaciones de Workspace ONE UEM.
- Tablero de administración de contenido y vistas en lista para administrar la implementación del contenido desde la consola de UEM.
- Workspace ONE Content admite la función de multitarea de iPadOS. Para mejorar la productividad, puede utilizar la aplicación Content en modo dividido mientras trabaja en otra aplicación en línea.

Seguridad

- Cifrado SSL para un tránsito de datos seguro.
- Cifrado AES de 256 bits para proteger el contenido implementado.
- VMware Workspace ONE Content v2.2 y versiones posteriores para iOS utiliza la clase NSFileProtectionComplete para almacenar el contenido.

Capacidades de contenido de VMware Workspace ONE según plataforma

La siguiente matriz se aplica a la versión de plataforma de VMware Workspace ONE Content que está disponible en la tienda de aplicaciones.

Funciones	iOS	Android
Seguridad		
Autenticación		
Básico	✓	✓
AD/LDAP	✓	✓
Token	✓	✓
Código de acceso de dos factores	✓	✓

Funciones	iOS	Android
Cifrado		
Cifrado SSL en tránsito	✓	✓
Cifrado AES de 256 bits en reposo	✓	✓
Cifrado en la memoria	✓	✓
FIPS 140-2	✓	✓
Fijación de certificados	✓	
Políticas de TI		
Detección de estado comprometido	✓	✓
Revocación fuera de línea automática cuando el dispositivo está comprometido	✓	✓
Requerir inscripción	✓	✓
Revocación fuera de línea automática cuando el documento caduca	✓	✓
Cantidad máxima de intentos de inicio de sesión sin conexión	✓	✓
Eliminación de contenido cuando se exceda el máximo de intentos de inicio de sesión fallidos	✓	✓
Impedir la eliminación de contenido obligatorio	✓	✓
DLP		
Impedir copiar y pegar	✓	✓
Habilitar/inhabilitar impresión	✓	
Habilitar/inhabilitar abrir en aplicaciones de terceros	✓	✓
Habilitar/inhabilitar uso compartido por medio de correo electrónico	✓	✓
Habilitar/inhabilitar cifrado al nivel de documentos	✓	✓
Habilitar/Deshabilitar la marca de agua en documentos* La función de marca de agua está disponible únicamente para repositorios administrativos, repositorios del usuario y el contenido administrado por Workspace ONE UEM. No está disponible para los archivos adjuntos de correo electrónico abiertos en Workspace ONE Content	✓*	✓*
Habilitar/Deshabilitar captura de pantalla ** Para Workspace ONE Content, Activar captura de pantalla tiene que estar establecido en *Sí* para permitir a los usuarios sacar capturas de pantalla de los documentos y el contenido multimedia. Además, activa la función Duplicación de pantalla utilizando aplicaciones de terceros como Vysor. Si Activar captura de pantalla se ha definido en *No*, los usuarios solo podrán sacar capturas de pantalla de la pantalla de inicio y las carpetas de Workspace ONE Content. Duplicación de pantalla también está desactivada.		✓ **
Recopilación de datos		
Instalar contenido	✓	✓
Abrir/cerrar contenido	✓	✓
Desinstalar/eliminar contenido	✓	✓

Funciones	iOS	Android
Estado de sesión	✓	✓
Experiencia móvil		
Acceso		
Mantenerme conectado	✓	✓
Autenticación con credenciales back-end (Active Directory)	✓	✓
Integrar con el inicio de sesión único de Workspace ONE UEM	✓	✓
Inicio de sesión único de Workspace ONE UEM con Hub como Broker App	✓	✓
Permitir acceso fuera de línea	✓	✓
MCM independiente	✓	✓
Términos de uso personalizados	✓	✓
Vistas de contenido		
Contenido destacado (Carpeta, Archivo, Categoría)	✓	✓
Todo el contenido (Todo/Instalado/Desinstalado)	✓	✓
Actividad reciente (Actualizado o visto recientemente)	✓	✓
Contenido nuevo	✓	✓
Contenido favorito	✓	✓
Vista de mosaico y vista de lista de contenido	✓	
Modo de pantalla completa para imágenes/PDF	✓	✓
Ver el contenido requerido	✓	
Deslizar por todas las imágenes de una carpeta o vista	✓	
Vista de cuadrícula de todas las imágenes	✓	
Administración de archivos		
Contenido por orden (alfabético, cronológico, de importancia)	✓	✓
Filtrar contenido (tipo de archivo, estado de la descarga)	✓	✓
Eliminación a pedido de documentos	✓	✓
Importar y cargar documentos nuevos o versiones nuevas	✓	✓
Sincronización bidireccional para WebDAV, recurso compartido de red	✓	✓
Sincronización bidireccional para Google Drive, One Drive	✓	✓
Retiro/Devolución a SharePoint	✓	✓
Agregar comentarios a los archivos al devolverlos a SharePoint		✓
Contenido creado por usuario: captura de fotos o vídeo en VMware Workspace ONE Content	✓	✓

Funciones	iOS	Android
Agregar, copiar, seleccionar múltiples archivos o carpetas	✓	✓
Contenido creado por usuario: agregar archivos de audio	✓	
Contenido creado por usuario: agregar archivos de Office	✓	✓
Contenido creado por usuario: agregar archivos de texto	✓	✓
Colocar en fila múltiples descargas de documentos simultáneamente	✓	✓
Administrar descargas (Pausar/Reanudar/Cancelar/Volver a solicitar)	✓	
Administrar cargas (Pausar/Reanudar/Cancelar/Volver a solicitar)	✓	
Facilidad de uso		
Buscar cadenas dentro de documentos (PDF solamente)	✓	✓
Navegación mediante miniaturas o barra de reproducción	✓	
Ver contenido	✓	✓
Múltiples pestañas para ver documentos (se aplican ciertas restricciones de tipo de archivo)	✓	
Marcación (PDF solamente)	✓	✓
Editar marcadores	✓	
Modo nocturno (PDF)	✓	
Modo de presentación (puntero nativo para presentar contenido)	✓	
Compatibilidad con enlaces en PDF	✓	✓
Ver actualizaciones	✓	✓
Buscar documentos mediante palabras clave	✓	✓
Destacar resultados de búsqueda	✓	✓
Ver última sincronización (estado de sincronización)	✓	✓
Contenido administrado por el usuario (almacenamiento local)		
Administración de archivos		
Agregar/Eliminar archivos	✓	✓
Agregar nueva versión	✓	✓
Mover archivos o carpetas	✓	✓
Agregar/Eliminar carpetas	✓	✓
Los archivos eliminados se envían a la Papelera	✓	✓
Cargar documento automáticamente al abrir en VMware Workspace ONE Content	✓	✓
Collaboration		
Agregar y guardar anotaciones de PDF	✓	✓

Funciones	iOS	Android
Acoplar anotaciones en PDF	✓	✓
Editar y guardar documentos de Office (Word, Excel, PPT)	✓	✓
Ver carpetas compartidas con archivos (Copropietario, Editor, Lector)	✓	✓
Mostrar colaboradores y roles por cada carpeta compartida	✓	✓
Agregar comentarios a las versiones de archivos	✓	
Ver fuente de actividad de comentarios e historial de revisión por documento	✓	
Guardar borradores localmente	✓	
Notificar al usuario cuando haya una actualización disponible para el documento	✓	✓
Personalización e integración		
Integración de repositorios externos de archivos		
Share Point 2007	✓	✓
Share Point 2010	✓	✓
Share Point 2013	✓	✓
Share Point Online (Office 365)	✓	✓
Recurso compartido de archivos de red	✓	✓
WebDAV	✓	✓
FileServer (HTTP)	✓	✓
Google Drive	✓	✓
OneDrive	✓	✓
CMIS	✓	✓
Compatibilidad con repositorios agregados por el usuario	✓	✓
OneDrive para la Empresa	✓	✓
Box	✓	✓
Acciones de la carpeta del repositorio de archivos externos		
Permitir el uso compartido de carpetas de Google Drive a través del correo electrónico	✓	
Permitir el uso compartido de carpetas de OneDrive a través del correo electrónico	✓	
Permitir el marcado de una carpeta como favorita	✓	
No se pueden eliminar las carpetas de Google Drive y OneDrive, ya que estos repositorios no tienen permisos de eliminación		
Localización		
Árabe	✓	✓
Chino simplificado	✓	✓

Funciones	iOS	Android
Chino tradicional	✓	✓
Checo	✓	✓
Danés	✓	✓
Holandés	✓	✓
Inglés	✓	✓
Francés	✓	✓
Hebreo	✓	✓
Alemán	✓	✓
Italiano	✓	✓
Japonés	✓	✓
Coreano	✓	✓
Polaco	✓	✓
Portugués - Brasil	✓	✓
Ruso	✓	✓
Español	✓	✓
Sueco	✓	✓
Turco	✓	✓
Archivos adjuntos de correo electrónico e integración		
Permitir ver archivos adjuntos y guardarlos en VMware Workspace ONE Content	✓	✓
Permitir ver, descomprimir y guardar archivos adjuntos comprimidos en VMware Workspace ONE Content	✓	✓
Permitir la edición de archivos adjuntos de correo electrónico	✓	✓
Permitir volver a compartir archivos adjuntos de correo electrónico	✓	✓
Múltiple selección de contenido y envío como archivos adjuntos de correo electrónico (archivos adjuntos individuales)	✓	
Seleccionar carpetas y enviar como archivos adjuntos de correo electrónico (carpeta comprimida)	✓	
Integración de VMware Browser		
Permitir ver y guardar descargas de VMware Browser	✓	✓
*Tipo de archivo compatible con la edición.		

Matriz de tipos de archivos compatibles según la plataforma

Los tipos de archivo compatibles con la aplicación Workspace ONE Content en diferentes

plataformas se indican en la matriz.

La siguiente matriz se aplica a la versión de VMware Workspace ONE Content que está disponible en la tienda de aplicaciones.

Tipos de archivos compatibles	iOS		Android		Notas
	Editar	Ver	Editar	Ver	
AD/Azure RMS	✓	✓	✓ Aplicación Content v3.5+	✓ Aplicación Content v3.5+	
AAC (audio/aac)		✓		✓	No puede editar los archivos de audio y vídeo. Solo puede agregar los archivos desde la aplicación Content en iOS y Android. Entre los archivos de audio, solo puede agregar los archivos .m4a.
ALAC (audio/m4a)		✓		✓	
WAV (audio/wav)		✓		✓	
MP3 (audio/mpeg)		✓		✓	
MOV (vídeo/Quicktime)		✓		✓	Los dispositivos Android no admiten archivos MOV de forma predeterminada. No obstante, algunos OEM sí proporcionan compatibilidad. Los dispositivos Samsung no admiten archivos MOV.
MP4 (vídeo/mp4)		✓		✓	
M4B, M4R,		✓			
M4V		✓		✓	
CSV (.csv)		✓		✓	
ePub (.epub)		✓			
iBooks					
iWorks: aplicación Keynote (.key)/vnd.apple.keynote		✓			
iWorks: aplicación Numbers (.numbers)/vnd.apple.numbers		✓			

(.pages)/vnd.apple.pages

Tipos de archivos compatibles	iOS		Android		Notas
MS Office: aplicación Excel (.xls/.xlsx)/vnd.ms-excel	✓		✓	✓	
XLSM		✓		✓	
MS Office: aplicación PowerPoint (.ppt/.pptx)/vnd.ms-powerpoint	✓		✓	✓	
PPTM		✓		✓	
MS Office: aplicación Word (.docx)/msword	✓	✓	✓	✓	No se admite la edición de archivos .doc
DOCM		✓		✓	
MS Office: protegido con contraseña (.docx, .pptx, .xlsx MS Office 2007 o posterior)	✓	✓	✓	✓	No se admite la edición de archivos .doc
MS Office: documentos con tablas dinámicas		✓		✓	
Texto HTML (.html)/html		✓		✓	El visor de HTML no admite JavaScript
Aplicación PDF (.pdf)/pdf	✓	✓	✓	✓	
Aplicación de Formato de texto enriquecido (.rtf)/rtf		✓		✓	
Aplicación de Directorio de formato de texto enriquecido (.rtfd)/octet-stream		✓		✓	
Aplicación XML (.xml)/xml		✓		✓	
Imagen PNG (.png)/png		✓		✓	Puede agregar las imágenes, pero no puede editar los archivos.
Imagen JPG (.jpg)/jpeg		✓		✓	
Imagen TIF (.tif, .tiff)/tif		✓		✓	
Imagen de Mapa de bits (.bmp)/bmp		✓		✓	
Imagen GIF (.gif)/gif		✓		✓	
Aplicación Zip (.zip)/zip	✓	✓	✓	✓	
Zip protegido por ntraseña	✓	✓	✓	✓	

Aplicación RAR (.rar)/rar	✓	✓

Tipos de archivos compatibles	iOS	Android	Notas
RAR protegido por contraseña			
Aplicación GZIP (.gzip)/zip			
Aplicación BZIP (.bzip)/zip			
Aplicación BZIP2 (.bzip2)/zip			
Aplicación TAR (.tar)/zip			
TXT	✓	✓ ✓ ✓	
MSG		✓	
Zip/Aplicación 7Zip (.7z)		✓ ✓	

Configure VMware Workspace ONE Content

Proporcione a los usuarios finales el acceso lateral del dispositivo al contenido corporativo utilizando la aplicación Workspace ONE Content. Las configuraciones establecidas en la consola de UEM determinan el grado de libertad que tendrán los usuarios finales para acceder al contenido corporativo desde sus dispositivos.

1. Desplácese a Grupos y ajustes > Todos los ajustes > Content > Aplicaciones > Aplicación Workspace ONE Content.
2. Configure los ajustes de la sección Ajustes y políticas.

Ajustes	Descripción
Perfil de aplicación	Configure esta opción para definir las políticas de seguridad y los ajustes que utiliza la aplicación. Deje la opción Predeterminado y configure los ajustes predeterminados de SDK que se recomiendan para definir el comportamiento de las aplicaciones con las recomendaciones de Workspace ONE UEM. También puede seleccionar el ajuste Personalizado de la aplicación para reemplazar los ajustes de SDK predeterminados y configurar un conjunto de comportamientos exclusivos para la aplicación.
Perfil de iOS	Seleccione un perfil de SDK personalizado en la lista desplegable.
Perfil de Android	Seleccione un perfil de SDK personalizado en la lista desplegable.

3. Configure los ajustes de la sección General.

Ajustes	Descripción

Cantidad de días para mantener contenido como nuevo	Seleccione el número de días en que los documentos agregados recientemente estarán marcados como “nuevo” en Workspace ONE Content.
Límite de carga de archivos	Establezca el número máximo de archivos que los usuarios pueden cargar en la aplicación de contenido. Puede permitir que los usuarios carguen hasta 40 archivos a la vez.
Bloquear la inscripción a través de Content, Boxer y Web	Habilite esta opción para impedir la inscripción a través de Workspace ONE Content, VMware Workspace ONE Boxer y VMware Workspace ONE Web. Si Workspace ONE Content usa VMware Workspace ONE SDK para iOS en Objective-C, entonces se requiere la inscripción de MDM para que la configuración SDK de inicio de sesión único funcione correctamente.
Cambiar nombre de repositorio para el contenido administrado	Habilite esta opción para cambiar el nombre del repositorio en el campo Nombre del repositorio principal que aparece.
Nombre del repositorio principal	Introduzca el nuevo nombre que desea utilizar para el repositorio.
Permitir hipervínculo	Habilite esta opción para permitir que los usuarios finales abran hipervínculos de documentos en el campo Abrir enlaces al Internet con que aparece.
Abrir enlaces al Internet con	Seleccione la aplicación en la que desea que se abran los hipervínculos.
Almacenamiento local	Habilite esta opción para proporcionar una alternativa de almacenamiento para el contenido de los usuarios.
Cargar solamente en Wi-Fi	Habilite esta opción para restringir las cargas de Workspace ONE Content a conexiones de Wi-Fi.

4. Implemente un acuerdo de Términos de uso para la aplicación.
5. Asígnele una Notificación a las aplicaciones de Workspace ONE Content para la plataforma especificada.

Ajustes	Descripción
Tipo de aplicación	Indique si el tipo de aplicación es Sistema o Interno/a(s).
Nombre de la aplicación	Asígneselo a la aplicación.
ID de paquete	Asígneselo a la aplicación.

Ajustes	Descripción
Número de insignias	Configure esta opción como Requerido o Solo actualizaciones o Ninguno. Obligatorio: El número de insignias representa la cantidad de documentos requeridos que el usuario no ha abierto a través de Workspace ONE Content. Solo actualizaciones (para contenido descargado): El número de insignias representa el número de documentos descargados que tienen actualizaciones o versiones nuevas disponibles. Ninguno: El número de insignias se deshabilita para Workspace ONE Content.

6. Seleccione Guardar.

Descripción general para la incorporación de VMware Workspace ONE Content

La incorporación requiere que los usuarios finales revisen y examinen los materiales y vídeos de formación antes de que se les otorgue acceso completo a VMware Workspace ONE Content en sus dispositivos.

Maximice la funcionalidad de incorporación mediante la configuración de contenido requerido y la implementación del modo de aplicación única en los dispositivos de los usuarios finales. Después de la incorporación, elimine el perfil para permitir que los usuarios finales accedan a todas las funcionalidades del dispositivo.

También tiene la opción de configurar la incorporación sin el modo de aplicación única para proporcionar una experiencia más flexible a los usuarios finales. En esa configuración, los usuarios finales no podrán acceder a Workspace ONE Content hasta que hayan visto el contenido requerido, aunque sí podrán utilizar el dispositivo.

Aplicación	Con el modo de aplicación única	Sin el modo de aplicación única
VMware Workspace ONE Content	Fijo en la vista de contenido requerido	Fijo en la vista de contenido requerido
Aplicaciones de otros dispositivos	Inaccesible. El dispositivo permanece fijo en la vista de contenido requerido.	Accesible. Los usuarios finales pueden utilizar el dispositivo.

Antes de exigir la visualización de contenido, considere cómo afectan las opciones a la experiencia de los usuarios finales. Por ejemplo, distribuir contenido requerido al dispositivo de un empleado fuera de la oficina puede confundir al usuario final, lo que resulta en la apertura de un vale del servicio de asistencia. En general, la incorporación, o un escenario asistido similar, proporciona un nivel adecuado de contexto para el comportamiento limitado del dispositivo y reduce la probabilidad de que se genere confusión entre los usuarios finales.

Además, debe considerar el efecto que causará la implementación de Workspace ONE Content en el modo de aplicación única, ya que restringe la funcionalidad del dispositivo a una sola aplicación, Workspace ONE Content, en este caso. Si planea eliminar la restricción del modo de aplicación única en un momento determinado, asegúrese de que los usuarios finales no accedan a otras aplicaciones. Además, asegúrese de que los usuarios finales realicen tareas relacionadas con el trabajo en sus dispositivos mientras sus dispositivos están restringidos.

Habilitar la incorporación de VMware Workspace ONE

Content

La incorporación proporciona una opción de implementación para Workspace ONE Content que fija la aplicación en una vista que solo muestra el contenido requerido hasta que se vea el contenido.

1. Cumpla con los requisitos mínimos de aplicación y SO.
2. Determine y configure el flujo de inscripción.
3. Desplácese a Content > Ajustes > Avanzado > Incorporación.
4. Configure la opción Incorporación como Habilitado y configure los ajustes que aparecen.

Ajustes	Descripción
Código administrativo de desbloqueo	Configure este código para reemplazar el modo supervisado como un administrador.
Mensaje de bienvenida	Envíe un mensaje a los usuarios finales para explicarles que deben leer el contenido requerido antes de poder utilizar el dispositivo.
Mensaje de salida	Envíe un mensaje a los usuarios finales para explicarles que ya han leído todo el contenido requerido y que ahora ya pueden usar el dispositivo.

Cómo configurar extensiones de documentos

Las extensiones de documentos permiten a los usuarios finales interactuar con archivos de VMware Workspace ONE Content en dispositivos iOS desde aplicaciones de terceros. Esta funcionalidad requiere configuraciones específicas en la consola de UEM y consideraciones especiales para determinados tipos de servidores de archivos corporativos.

Asegúrese de que la funcionalidad de extensión de documentos aparezca en los dispositivos con Workspace ONE Content v3.1 y versiones posteriores al completar los ajustes necesarios en UEM Console.

- Deshabilitar tipo de autenticación

  Las aplicaciones con el tipo de autenticación habilitado impiden a los usuarios la carga de archivos desde la aplicación Workspace ONE Content usando extensiones de documento. Para permitir que los usuarios carguen archivos en aplicaciones de terceros, se debe deshabilitar el tipo de autenticación.

  1. Desplácese a Grupos y ajustes > Todos los ajustes > Aplicaciones > Ajustes y políticas > Políticas de seguridad.
  2. Seleccione Deshabilitado en el menú desplegable Tipo de autenticación y, a continuación, seleccione Guardar.

- Cómo deshabilitar la lista de permitidos de aplicaciones

  La lista de permitidos de aplicaciones se debe deshabilitar para permitir que los usuarios abran documentos de aplicaciones de terceros en Workspace ONE Content.

  1. Desplácese a Grupos y ajustes > Todos los ajustes > Aplicaciones > Ajustes y políticas > Políticas de seguridad.
  2. Configure Limitar que los documentos se abran solo en aplicaciones aprobadas en

No.

3. Seleccione Guardar.

- Activar Permitir que se abra en aplicaciones de terceros

  La opción Permitir que se abra en aplicaciones de terceros debe estar habilitada para que los usuarios finales puedan utilizar la funcionalidad de exportación dentro de aplicaciones de terceros.

  1. Desplácese a Content > Repositorios > Repositorios de administrador.
  2. Seleccione el icono Editar situado junto al servidor de archivos corporativos que se sincroniza con los dispositivos de los usuarios finales.
  3. En la pestaña Seguridad, seleccione Permitir abrir en una aplicación de terceros y, a continuación, Guardar.

Habilitar el acceso al almacenamiento

Los usuarios finales pueden acceder a los archivos y al almacenamiento desde aplicaciones de terceros solo cuando el acceso a los archivos y el almacenamiento está habilitado para Workspace ONE Content en dispositivos Android.

Para habilitar el acceso al almacenamiento, complete las configuraciones requeridas en la consola.

- Cómo habilitar el acceso al almacenamiento de aplicaciones de terceros con los ajustes predeterminados del SDK de Android

  Agregue una clave de configuración en el perfil de SDK predeterminado para habilitar el acceso al archivo de contenido y al almacenamiento de aplicaciones de terceros.

  1. Navegue a Aplicaciones > Ajustes y políticas > Ajustes > Ajustes personalizados.
  2. Seleccione Habilitar ajustes personalizados y pegue {“PolicyEnableFileProvider”: “true”}.
  3. Seleccione Guardar.

- Cómo habilitar el acceso al almacenamiento de aplicaciones de terceros con el perfil predeterminado del SDK de Android

  Agregue una clave de configuración en el perfil de SDK personalizado para que Workspace ONE Content habilite el acceso al archivo de contenido y al almacenamiento de aplicaciones de terceros.

  1. Si ya tiene un perfil personalizado, navegue a Aplicaciones > Ajustes > Perfiles > Perfil personalizado > Carga útil de ajustes personalizados.
  2. Si desea añadir un perfil personalizado, navegue a Aplicaciones > Ajustes > Perfiles > Agregar perfil > Perfil de SDK > Android > Ajustes personalizados > Carga útil de ajustes personalizados.
  3. Pegue {“PolicyEnableFileProvider”: “true”} y seleccione Guardar.

     Si tiene varios ajustes personalizados, pegue la clave PolicyEnableFileProvider tras la clave que ya tiene dentro de { }. Por ejemplo, {
     “CustomSetting Default”: "true”, “PolicyEnableFileProvider”: “true” }.

- También debe habilitar la opción Permitir que se abra en una aplicación de terceros para permitir que los usuarios finales accedan a los archivos desde aplicaciones de terceros. Consulte Activar Permitir que se abra en aplicaciones de terceros.

Limitación del acceso al almacenamiento desde aplicaciones de terceros (solo Android)

En la siguiente lista se describen las limitaciones del acceso al almacenamiento de aplicaciones de terceros.

- El indicador para permitir la apertura en aplicaciones de terceros se utiliza para permitir o denegar el acceso a aplicaciones de terceros. El indicador del permiso "Permitir correo electrónico" no se utiliza para un archivo concreto, puesto que no se puede determinar (en función del ID de la aplicación) si la aplicación de terceros es o no de correo electrónico.
- El marco de soporte para Android para proporcionar acceso al almacenamiento y al archivo de contenido desde aplicaciones de terceros está desactivado de forma predeterminada para poder gestionar los contenedores y los datos compartidos entre ellos.
- No es posible acceder a los archivos de almacenamiento locales puesto que la funcionalidad Abrir en para aplicaciones de terceros está desactivada de forma predeterminada.
- Cuando se active la autenticación de Workspace ONE Content, tiene que tener Workspace ONE Content desbloqueado para acceder a él por medio de una aplicación de terceros (aparece un mensaje).
- Si su administrador configuró una lista de permitidos de aplicaciones y la aplicación de terceros no aparece dentro de ella, no podrá abrir o crear archivos a través de Workspace ONE Content.
- Para el contenido administrado, todo el contenido está disponible mientras navega por medio de una aplicación de terceros. Para otros repositorios, el contenido está disponible (para un nivel) solo para las carpetas que se han sincronizado en Workspace ONE Content.

Cómo escanear código QR para acceder a las URL personalizadas (solo Android)

Utilice URL personalizadas para proporcionar a los usuarios finales acceso directo a los archivos de la aplicación Workspace ONE Content. Tras escanearlo, el código QR, que contiene las URL personalizadas, permite al usuario final buscar el archivo o verlo si se descarga el archivo.

Debe usar una consulta de búsqueda o un ID de contenido específico como la URL personalizada. Los ID de contenido se generan automáticamente para cada archivo que se carga en Workspace ONE UEM Console. Al apuntar al nombre de archivo, la ruta del archivo muestra los ID de contenido.

Las URL personalizadas son las siguientes:

- awscl://search/?query=text
- awscl://search?query=text
- awscl://search/?query=“text”

- awscl://search?query="text"
- awscl://contentid={ID de contenido}
- awscl://contentid="{content ID}"

La consulta de búsqueda busca la cadena de texto especificada y el ID de contenido específico abre el documento especificado directamente.

Cambios de comportamiento para Content en iOS con el SDK de Swift

Workspace ONE Content 5.0 para iOS es la primera versión de Content que utilizará en el SDK de Swift de Workspace ONE. Las versiones anteriores de Content utilizaban la versión Objective C de Workspace ONE SDK. Con este cambio de arquitectura, se producen algunos cambios que pueden afectar al comportamiento de la aplicación Content al cual los usuarios finales están acostumbrados.

La siguiente lista describe los cambios en el comportamiento:

- Workspace ONE SDK no admite la función de cierre de sesión en modo independiente.

  Aviso: Los usuarios deben utilizar Intelligent Hub en el modo registrado en sus dispositivos. Los usuarios no deben intentar iniciar sesión en la aplicación Content en modo independiente con dispositivos que no estén administrados mediante MDM o que no cuenten con Workspace ONE Intelligent Hub.
- La opción de trabajar sin conexión en la pantalla Nombre de usuario/contraseña ya no es compatible. El usuario puede trabajar sin conexión, desplazándose para ello a los Ajustes de la aplicación y habilitando la opción de trabajar sin conexión. Se podrán seguir realizando llamadas de red y el trabajo sin conexión se aplicará solo a las interacciones específicas de Content.
- Las pantallas de autenticación de SDK se actualizan a una nueva experiencia de usuario.
- Si el SDK no puede recuperar los ajustes de Content tras el inicio, se muestra un mensaje de error al usuario.
- Experimente la actualización del cambio de usuario sin Check-in Check-out (CICO) durante un escenario de código de acceso olvidado.

  Para obtener más información sobre los cambios de comportamiento de la aplicación Content, consulte el artículo de la base de conocimientos Cambios de comportamiento presentes en Workspace ONE Content 5.0.

Confirmación de documentos en Workspace ONE Content

Los usuarios de la aplicación Content pueden confirmar ahora los documentos que les asigne como contenido obligatorio. Los usuarios pueden ver los archivos que requieren su confirmación en la sección Sus archivos para revisar en la pantalla Para ti de la aplicación.

En Workspace ONE UEM Console, puede ver estas confirmaciones en las páginas Vista de lista de contenido y Detalles del dispositivo.

Al seleccionar Ver en la columna Estado instalado de la página Vista de lista de contenido, aparecerá una casilla emergente que muestra el número exacto de usuarios que han visto y confirmado el

contenido.

En la siguiente lista se describen las funciones de confirmación de documentos admitidas:

- Para habilitar la confirmación del contenido obligatorio, aplique el ajuste personalizado `EnableDocumentAcknowledgement: true` en UEM Console.
- No se solicitará al usuario que confirme un documento que ya ha sido confirmado.
- Se solicita al usuario que confirme de nuevo una nueva versión del documento ya confirmado.
- La página Detalles del dispositivo muestra el estado confirmado y la fecha en la que se confirmó el documento.
- El informe Detalles de contenido por dispositivo contiene el estado confirmado según cada dispositivo.

Habilitar el modo de contenido de inscripción de copia intermedia para dispositivos de varios usuarios

Para evitar la pérdida de contenido de copia intermedia en dispositivos de varios usuarios durante las sesiones de protección y desprotección del dispositivo, debe habilitar el modo de contenido de copia intermedia para la aplicación Content en Workspace ONE UEM Console. Al habilitar el modo de contenido de copia intermedia, se conserva todo el contenido al cual se le ha realizado una copia intermedia en el dispositivo, lo que ayuda al usuario a evitar volver a descargar el contenido en el siguiente inicio de sesión.

El contenido está disponible para un usuario nuevo que inicie sesión en el dispositivo solo si el nuevo usuario está asignado al contenido. El contenido se borra si este no está asignado al nuevo usuario.

Para habilitar el modo de contenido de copia intermedia, agregue la siguiente clave de configuración en Workspace ONE UEM Console.

Clave de configuración	Tipo de valor	Tipos compatibles	Descripción
{“RetainContentBetweenCheckoutSessions”: true}	Booleano	True = habilitado False (valor predeterminado) = deshabilitado	Cuando se establece en true, el contenido descargado se conserva y no se borra durante las sesiones de protección y desprotección del dispositivo. Cuando se establece en false, el contenido descargado se borra y no se conserva durante las sesiones de protección y desprotección del dispositivo.

Habilitar la compatibilidad con contenido de copias intermedias mediante el perfil de SDK predeterminado

Agregue la clave de configuración en el perfil de SDK predeterminado para habilitar el modo de copias intermedias para el contenido administrado descargado en la aplicación Content.

1. Desplácese a Grupos y ajustes > Todos los ajustes > Aplicaciones > Ajustes y políticas > Ajustes.
2. Seleccione Habilitar ajustes personalizados e introduzca las claves de configuración según sus necesidades.

```
{
    "CustomAppSettings": {
        "com_vmware_folio": {
            "SharedDeviceSettings": {
                "RetainContentBetweenCheckoutSessions":  true
            }
        }
    }
}
```

1. Seleccione Guardar.

Habilitar la compatibilidad con contenido de copias intermedias mediante el perfil de SDK personalizado

Agregue la clave de configuración en el perfil de SDK personalizado para habilitar el modo de copia intermedia para el contenido administrado en la aplicación Content.

1. Desplácese a Grupos y ajustes > Todos los ajustes.
2. Si ya tiene un perfil personalizado, navegue a Aplicaciones > Ajustes y políticas > Perfiles > Perfil personalizado > Ajustes personalizados.
3. Si desea agregar un perfil personalizado, desplácese a Aplicaciones > Ajustes y políticas > Perfiles > Agregar perfil > Perfil de SDK > iOS > Ajustes personalizados.
4. En Ajustes personalizados, seleccione Configurar e introduzca las claves de configuración según sus necesidades.

```
{
    "CustomAppSettings": {
        "com_vmware_folio": {
            "SharedDeviceSettings": {
                "RetainContentBetweenCheckoutSessions":   true
            }
        }
    }
}
```

1. Seleccione Guardar.

Casos prácticos compatibles y no compatibles con el modo de contenido de copia intermedia

A continuación, se muestran los casos prácticos que son compatibles y no compatibles con el modo de contenido de copia intermedia.

Compatible

- Nuevas instalaciones de la aplicación Content compatibles con el modo de contenido de copia intermedia.
- El tipo de autenticación en los ajustes de SDK es "Ninguno".
- Retención solo de contenido administrado.

No compatible

- Actualice a partir de una versión anterior de la aplicación Content a la versión compatible con el modo de contenido de copia intermedia.

- Cambiar entre usuarios en diferentes grupos organizativos, y tener, por tanto, diferentes ajustes de retención de contenido.
- Cambiar entre grupos organizativos principales en los que los ajustes de retención de contenido están habilitados.
- Editar y guardar un documento PDF/de Office como borrador. Si el usuario ha editado un archivo compartido entre otros usuarios, el archivo conserva las ediciones cuando se produce el cambio de usuario.
- No se admiten repositorios que no sean repositorios de contenido administrado.

Firmar digitalmente los documentos PDF mediante la aplicación PIV-D

Workspace ONE Content permite a los usuarios firmar documentos PDF de forma segura mediante la aplicación de firma de PIV-D. Al activar la aplicación PIV-D, los usuarios deben inscribirla y crear un PIN de almacén de claves. Para obtener más información sobre el proceso de activación, consulte la documentación de la aplicación PIV-D. Los usuarios pueden seguir los pasos siguientes para firmar documentos PDF de forma segura en la aplicación Content:

1. Toque el campo Firma digital y aparecerá un mensaje emergente.
2. Toque el campo Certificado e introduzca el PIN del almacén de claves. Este es el PIN que los usuarios generan al final del proceso de activación de credenciales de PIV-D.
3. Seleccione el certificado que crea PIV-D. Puede agregar su firma si lo desea.
4. El documento PDF está firmado.

Registro dirigido

Al habilitar la opción Registro dirigido en la aplicación, los usuarios pueden generar y enviar automáticamente registros sobre cualquier incidente que ocurra durante un flujo o duración específicos. La función genera y comparte dos conjuntos de archivos de registro: de inicio y de detención. Un archivo contiene registros previos a la habilitación del registro dirigido y otro archivo contiene registros entre la habilitación y la desactivación del registro dirigido.

Establecer restricciones avanzadas de DLP en Workspace ONE Content

En Workspace ONE UEM Console, puede proteger los datos de la aplicación Content mediante la configuración de las siguientes opciones avanzadas de Prevención de pérdida de datos (DLP).

- Limitar la carga de archivos a la aplicación Content: puede establecer el número máximo de archivos que los usuarios pueden cargar a la aplicación Content de una vez. Desplácese a Grupos y ajustes > Todos los ajustes > Content > Aplicación > Aplicación Workspace ONE Content > Límite de carga de archivos y configure el número de archivos que los usuarios pueden cargar. Puede permitir que los usuarios carguen hasta 40 archivos a la vez.
- Restringir a los usuarios para que carguen imágenes solo desde la cámara de su dispositivo: puede restringir el origen de las fotos desde donde los usuarios empresariales

pueden cargar imágenes en la aplicación Content. Desplácese a Content > Repositorios > Repositorios de administrador y agregue o edite el repositorio en el que desea imponer restricciones. A continuación, en la página Editar repositorio de Content, seleccione Permitir la carga solo desde la cámara.

Aviso: Para aprovechar las restricciones avanzadas de DLP, debe utilizar Workspace ONE UEM 2209 y versiones posteriores.

Restringir el acceso a aplicaciones sin administrar

Puede habilitar la administración adaptativa para configurar Workspace ONE UEM de forma que administre el dispositivo para que este pueda acceder a la aplicación. Solo los dispositivos que estén inscritos en EMM podrán instalar la aplicación y recibir políticas de aplicaciones cuando habilite esta opción. Para ello, en la página Restricciones, debe habilitar la opción Acceso administrado. Para obtener más información, consulte Guía de administración de aplicaciones móviles.

Configuraciones de la aplicación para Workspace ONE Content

Configure Workspace ONE Content con los valores de configuración de la aplicación.

Puede configurar los ajustes de su implementación de Workspace ONE Content utilizando los pares de clave de configuración y valor de configuración proporcionados por Workspace ONE UEM. Introduzca estos pares de valor y clave de configuración en el perfil de SDK personalizado o en el perfil de SDK predeterminado en Workspace ONE UEM Console.

Configurar los ajustes mediante un perfil de SDK predeterminado

Agregue las claves de configuración en el perfil de SDK predeterminado para configurar los ajustes para Workspace ONE Content.

1. Desplácese a Grupos y ajustes > Todos los ajustes.
2. En Todos los ajustes, desplácese a Aplicaciones > Ajustes y políticas > Ajustes.
3. Seleccione Habilitar ajustes personalizados y pegue las claves de configuración según sus necesidades.
4. Seleccione Guardar.

Configurar ajustes mediante el perfil de SDK personalizado

1. Desplácese a Grupos y ajustes > Todos los ajustes.
2. En Todos los ajustes, desplácese a Aplicaciones > Ajustes y políticas > Perfiles > Perfil personalizado > Ajustes personalizados.
3. Si desea agregar un perfil personalizado, desplácese a Aplicaciones > Ajustes y políticas > Perfiles > Agregar perfil > Perfil de SDK > iOS o Android > Ajustes personalizados.
4. En Ajustes personalizados, seleccione Configurar y pegue las claves de configuración según sus necesidades.
5. Seleccione Guardar.

Ajustes de privacidad para Workspace ONE Content (iOS y Android)

Las prácticas adicionales de recopilación de datos y de divulgación de privacidad se pueden implementar mediante determinadas claves de configuración en UEM Console.

A los usuarios finales que vayan a realizar una actualización o estén empezando a usar la versión más reciente de Workspace ONE Content les aparece una pantalla con el cuadro de diálogo con la nueva privacidad después del inicio de la aplicación.

La pantalla del cuadro de diálogo de privacidad permite al usuario conocer la siguiente información:

- Datos recopilados por la aplicación: proporciona un resumen de los datos que se recopilan y se procesan por la aplicación. Algunos de estos datos están visibles para los administradores de la consola administrativa de Workspace ONE UEM.
- Permisos de dispositivo: proporciona un resumen de los permisos de dispositivo solicitado para que la aplicación habilite las características del producto y la funcionalidad, como las notificaciones push al dispositivo.
- Política de privacidad de la empresa: de forma predeterminada, se muestra un mensaje al usuario para que se ponga en contacto con la empresa para obtener más información. Puede configurar la URL de la política de privacidad en la consola UEM. Una vez configurada, el usuario puede acceder a la política de privacidad de la empresa desde la aplicación.

Utilice las claves de configuración siguientes para habilitar el aviso de privacidad y la configuración de uso compartido de datos en Workspace ONE Content:

Clave de configuración	Tipo de valor	Valores admitidos	Descripción
{“DisplayPrivacyDialog”}	Número entero	0 = deshabilitado 1 = habilitado (predeterminado)	Cuando se establece en "1" (habilitado), Workspace ONE Content mostrará un aviso de privacidad a los usuarios sobre los datos que se recopilan y los permisos que se requieren en el dispositivo para el funcionamiento óptimo de la aplicación.
{“PolicyAllowFeatureAnalytics”}	Número entero	0 = deshabilitado 1 = habilitado (predeterminado)	Cuando se establece en "1" (habilitado), Workspace ONE Content mostrará un aviso a los usuarios acerca de la opción de participación en el análisis de uso de la función anónima que ayuda a VMware a mejorar la funcionalidad de los productos e inventar nuevas capacidades de producto. Cuando se establece en "0", no se muestra el aviso de uso compartido de datos y no se recopilan datos del dispositivo para optimizar la experiencia de la aplicación.
{“PolicyAllowCrashReporting”}	Booleano	True = habilitado False = deshabilitado	Cuando se establece en Verdadero, los bloqueos de la aplicación se notifican a VMware.
{“PrivacyPolicyLink”}	Cadena	“https://www.url.com”	Facilite la URL de la directiva que desea que los usuarios visiten cuando se selecciona Política de privacidad de la empresa en Aviso de privacidad.

Restricción de importación en Workspace ONE Content (solo iOS)

Puede restringir o permitir la importación de contenido de aplicaciones de terceros en Workspace ONE Content mediante el uso de determinadas claves de configuración en UEM Console. Estas claves de configuración permiten la importación de contenido únicamente desde una lista de permitidos configurada con aplicaciones nativas.

Utilice las siguientes claves de configuración para restringir o permitir la importación de contenido desde aplicaciones de terceros a Workspace ONE Content.

Clave de configuración	Tipo de valor	Valores admitidos	Descripción
{“ContentImportRestriction”}	Booleano	true = restricción habilitada false = restricción deshabilitada. Por ejemplo, {“ContentImportRestriction”: true}	Cuando se habilita, los usuarios de los dispositivos no pueden importar contenido a Workspace ONE Content desde aplicaciones de terceros que no figuren en la lista de permitidos, incluidas las aplicaciones nativas de iOS.
{“ContentImportAllowNativeApps”}	Booleano	true = se permite la importación desde aplicaciones nativas false = no se permite la importación desde aplicaciones nativas. Por ejemplo, {“ContentImportAllowNativeApps”: true}	Cuando se habilita, los usuarios de los dispositivos pueden importar contenido desde aplicaciones nativas cuando la restricción de importación está habilitada.

Los valores de configuración ContentImportRestriction y ContentImportAllowNativeApps se pueden utilizar de forma combinada para configurar la restricción de importación según sus necesidades. Si desea permitir la importación de contenido de todas las aplicaciones nativas, habilite la clave ContentImportAllowNativeApps. La clave ContentImportAllowNativeApps está habilitada de forma predeterminada y permite importar todas las aplicaciones nativas, como las aplicaciones nativas de correo electrónico, archivos, Safari, AirDrop y similares en iOS. Cuando se habilita, los usuarios de los dispositivos pueden abrir e importar contenido a Workspace ONE Content desde aplicaciones que no figuran en la lista de permitidos con las versiones web de las aplicaciones que no figuran en la lista blanca (con Safari).

Si solo desea permitir aplicaciones específicas, deshabilite la clave ContentImportAllowNativeApps y agregue las aplicaciones permitidas a la lista de permitidos.

Si desea restringir la importación de contenido desde aplicaciones nativas específicas, deshabilite la clave ContentImportAllowNativeApps y agregue las aplicaciones nativas permitidas a la lista de permitidos.

Aviso: La opción Limitar que los documentos se abran solo en aplicaciones aprobadas debe estar habilitada en el ajuste Prevención de pérdida de datos antes de habilitar los valores de la clave de configuración. Safari y AirDrop no pueden incluirse en la lista de permitidos porque no hay ningún ID de paquete asociado.

Autoguardado de PDF en Workspace ONE Content (solo iOS)

Desde Workspace ONE Content v4.13.2, los usuarios de los dispositivos pueden habilitar o deshabilitar la funcionalidad Autoguardado de PDF mediante la opción Habilitar autoguardado de PDF en la aplicación Workspace ONE Content.

La opción Autoguardado de PDF está deshabilitada de forma predeterminada. La función Autoguardado de PDF puede establecerse en 30 segundos, 60 segundos y 120 segundos

respectivamente mediante la opción Tiempo de autoguardado en segundos en Workspace ONE Content. Los administradores pueden utilizar la clave de configuración proporcionada por Workspace ONE UEM en la consola de Workspace ONE UEM para que la funcionalidad Autoguardado de PDF esté habilitada obligatoriamente en Workspace ONE Content. Cuando se habilita mediante la clave de configuración, los usuarios de los dispositivos no pueden deshabilitar la función Autoguardado de PDF y la opción Habilitar autoguardado de PDF no está disponible en Workspace ONE Content. Cuando la función Autoguardado de PDF está habilitada, no se guardan los cambios realizados en un archivo PDF cuando el autoguardado está en curso. Después de cada instancia de un autoguardado, se vuelve a cargar el documento PDF.

Utilice la siguiente clave de configuración para habilitar la función Autoguardado de PDF en Workspace ONE Content:

Clave de configuración	Tipo de valor	Valores admitidos	Descripción
{“ContentPDFAutoSaveEnabled”}	Booleano	true = habilitado false = puede ser habilitado o deshabilitado por el usuario del dispositivo	Cuando se establece en True, se habilita la funcionalidad Autoguardado de PDF y los usuarios de los dispositivos no pueden deshabilitar la opción. La opción Habilitar autoguardado de PDF en Workspace ONE Content no está disponible para los usuarios de los dispositivos.

Eliminar vínculos en PDF (solo iOS)

Utilice la siguiente clave de configuración para bloquear la capacidad de eliminar un vínculo de un PDF.

Clave de configuración	Tipo de valor	Valores admitidos	Descripción
{“DisableRemoveLink”}	Booleano	False (valor predeterminado) True	Cuando se establece en True, la clave bloquea la capacidad de eliminar un vínculo de un PDF.

Restricción de tiempo de espera de pantalla en Workspace ONE Content (solo iOS)

Puede evitar que los usuarios del dispositivo deshabiliten el tiempo de espera de la pantalla en la aplicación Workspace ONE Content mediante determinadas claves de configuración en Workspace ONE UEM Console.

Claves de configuración	Tipo de valor	Valores admitidos	Descripción

{“PolicyAllowScreenTimeoutToggle”}	Booleano	True (valor predeterminado) = habilitado False = deshabilitado	Establecer en True o False para controlar la configuración de tiempo de espera en la aplicación de Content. Si no se establece un valor, se aplica la configuración predeterminada y los usuarios pueden cambiar la configuración de tiempo de espera. Cuando se establece en false, los usuarios no pueden activar o desactivar la opción de tiempo de espera.

Autenticación moderna mediante WKWebView (solo iOS)

Por motivos de seguridad, puede agregar la siguiente clave para evitar los flujos de la autenticación moderna en Safari y permitir los flujos de la autenticación mediante WKWebView en lugar de SFSafariViewController. Esta clave, cuando se utiliza, permite la autenticación moderna sin lista de permitidos en Safari.

Aviso: La autenticación básica es compatible con repositorios de OAuth como One Drive, Google Drive, Box, Sharepoint O365 y One Drive for Business.

Clave de configuración	Tipo de valor	Valores admitidos	Descripción
{“AccountUseWebviewForOauth”}	Booleano	TRUE = habilitado FALSE = deshabilitado (valor predeterminado)	Cuando se establece en Verdadero, el flujo de oauth se presenta mediante WKWebView en lugar de SFSafariViewController.

Control de sincronización automática de los repositorios (solo Android)

Agregue una clave de configuración en el perfil de SDK predeterminado o personalizado para controlar la sincronización automática y la comprobación de autenticación de los repositorios que no son del tipo de repositorio de contenido administrado.

Clave de configuración	Tipo de valor	Valores admitidos	Descripción
{“AutoSyncEnabled”}	Booleano	TRUE (valor predeterminado) = habilitado FALSE = deshabilitado	Si se establece como falso, la sincronización automática y la comprobación de autenticación del repositorio se producen solo cuando el usuario navega al repositorio. Si se aplica el valor predeterminado, la sincronización y la comprobación de la autenticación se llevan a cabo cuando se realiza una sincronización manual o automática.

Grabación de pantalla durante el soporte remoto (solo Android)

Es posible que necesite capturas de pantalla o grabaciones de pantalla de la aplicación Content del

usuario mientras ayuda al usuario a solucionar cualquier problema durante una sesión de soporte remoto. Sin embargo, si se establece una restricción de DLP para la aplicación que no permita la grabación de pantalla, no podrá realizar una captura de pantalla.

Para anular la restricción de DLP y permitir la grabación de pantalla, agregue la siguiente clave de configuración al perfil de SDK predeterminado o personalizado en Workspace ONE UEM Console.

Clave de configuración	Tipo de valor	Valores admitidos	Descripción
{“AllowScreenRecord”}	Booleano	TRUE = habilitado FALSE = deshabilitado (valor predeterminado)	Cuando se establece en True, se permite la grabación de pantalla. Cuando se establece en false, la grabación de pantalla estará restringida.

Compatibilidad de Workspace ONE Send para Content

Al integrar Workspace ONE Send con Workspace ONE Content, puede restringir los archivos de Workspace ONE Content para que solo se abran a través de Workspace ONE Send. Para forzar la apertura de los archivos mediante la aplicación Send, agregue una clave de configuración en UEM Console.

Utilice la siguiente clave de configuración para restringir los archivos para que se abran mediante Workspace ONE Send.

Clave de configuración	Tipo de valor	Valores admitidos	Descripción
{“PolicyAllowAIPFilesToOpenInOffice”}	Booleano	True = habilitado False = deshabilitado	Cuando se establece en Verdadero, los archivos se abren a través de Workspace ONE Send.

Compatibilidad con contenido de copia intermedia para dispositivos de varios usuarios

Agregue una clave de configuración en el perfil de SDK predeterminado o personalizado para habilitar el modo de contenido de copia intermedia para dispositivos de varios usuarios. Al habilitar el modo de contenido de copia intermedia para dispositivos de varios usuarios, puede evitar la pérdida de contenido entre las sesiones de protección y desprotección del dispositivo.

Clave de configuración	Tipo de valor	Tipos compatibles	Descripción
{“RetainContentBetweenCheckoutSessions”: true}	Booleano	True = habilitado False (valor predeterminado) = deshabilitado	Cuando se establece en true, el contenido descargado se conserva y no se borra durante las sesiones de protección y desprotección del dispositivo. Cuando se establece en false, el contenido descargado se borra y no se conserva durante las sesiones de protección y desprotección del dispositivo.

Para obtener más información sobre la compatibilidad con contenido de copia intermedia, consulte Habilitar el modo de contenido de copia intermedia para dispositivos de varios usuarios.

Compatibilidad con MIME de contenido (solo iOS)

El encabezado de tipo MIME de contenido se agrega a las solicitudes de red para realizar un seguimiento de la seguridad cuando el contenido se comparte dentro de la organización. Para admitir el tipo de MIME de contenido, utilice la siguiente clave.

Clave de configuración	Tipo de valor	Valores admitidos	Descripción
{“AddContentMimeTypeForNetworkRequests”: True}	Booleano	True = habilitado False = desactivado (valor predeterminado)	Cuando se establece en True, los encabezados Accept Header y Content-Type se actualizan al tipo MIME.

Activar nombre completo en Content

Utilice la siguiente clave para mostrar los nombres completos de Repositorio, Categoría o Carpeta, y Archivo en la vista de lista. No hay ninguna restricción en cuanto a la longitud de los nombres.

Clave de configuración	Tipo de valor	Valores admitidos	Descripción
{“PolicyDisplayFullName”: True}	Booleano	True = habilitado False = desactivado (valor predeterminado)	Establezca el valor en True para mostrar el nombre completo del repositorio, la categoría o carpeta, y el archivo en la vista de lista.

Los usuarios de iPad deben habilitar el modo Expandido en las opciones de visualización en Ajustes de la aplicación para utilizar esta función. O bien, como administrador, puede utilizar la siguiente clave para que se muestre en modo Expandido de forma predeterminada.

Clave de configuración	Tipo de valor	Valores admitidos	Descripción
{“EnableExpandedContentLayout”: True}	Booleano	True = habilitado False = desactivado (valor predeterminado)	Establezca el valor en True para habilitar el modo Expandido en las opciones de visualización.

Aviso: Esta función solo se aplica cuando la vista está en modo de lista y no en modo de cuadrícula.

Optimizar la caché de sincronización (solo iOS)

Al actualizar archivos, si advierte que desaparecen de la aplicación Content, puede configurar la siguiente clave para evitar este comportamiento.

Clave de configuración	Tipo de valor	Tipos compatibles	Descripción

{“PolicyUseOptimizedSync”: false}	Booleano	True = habilitado False (valor predeterminado) = desactivado	Establezca el valor de la clave en False para desactivar la sincronización optimizada.

Desactivar las opciones de Editar páginas PDF

Puede impedir que los usuarios agreguen, dupliquen, eliminen o reordenen páginas si desactiva las opciones de Editar páginas PDF. Para ello, desactive la siguiente clave:

Clave de configuración	Tipo de valor	Tipos compatibles	Descripción
{“PolicyAllowOrganizePDFPage”: true}	Booleano	True: habilitado (valor predeterminado) False: desactivado	Cuando se establece en False, los usuarios no pueden acceder a la opción Editar páginas PDF para agregar, duplicar, eliminar o reorganizar páginas.

Administración de contenido mediante la consola de Workspace ONE

La solución Content Management le ofrece varias opciones para administrar el contenido que se almacena, sincroniza o implementa desde Workspace ONE UEM Console.

Funciones

La solución Content Management ofrece las siguientes funcionalidades para administrar contenido:

- Tablero de administración de contenido para un resumen rápido de los usuarios y del contenido administrado.
- Vista en lista para la visualización y la administración de contenido.
- Menú Ajustes de contenido para configurar repositorios y opciones de almacenamiento, implementación y administración de distintos tipos de contenido.

Opciones de menú para la administración de contenido

Además de la vista predeterminada de la consola, hay otras pantallas que simplifican la administración de contenido. Se muestran en un menú de navegación secundario en la parte izquierda del “Tablero de contenido” de la consola de UEM.

Vea las opciones de menú disponibles para la administración de contenido.

Ajustes	Descripción
Vista de lista	Alterne entre la vista de lista de Administrado por UEM y Servidor de archivos corporativos.
Repositorios	Seleccione repositorios para acceder a las opciones de ajustes del repositorio. Hay dos tipos de repositorios: los repositorios agregados por administradores y los repositorios agregados por usuarios. Los usuarios agregan repositorios utilizando las plantillas que configura en la consola.
Categorías	Agregue categorías y subcategorías. Las categorías agregadas se muestran en la pantalla como una vista en lista con un menú de acciones.
Contenido destacado	Administre el contenido destacado que agregó desde la “Vista en lista” o la “Vista en lista de categorías” en esta pantalla. El contenido destacado se muestra en una parte visible de VMware Workspace ONE Content y proporciona acceso fácil a contenido de gran volumen. Utilice esta pantalla para controlar el orden en el que se muestra el contenido destacado en Workspace ONE Content; para ello, utilice la función de arrastrar o elimine contenido irrelevante.
Estado del lote	Seleccione “Importar por lotes” y revise los detalles del lote que haya cargado desde esta pantalla.
Ajustes	Seleccione esta opción para acceder a los ajustes específicos de contenido.

Tablero “Administración de contenido móvil”

Vea y administre el estado del contenido general de la flota de dispositivos desde el tablero “Administración de contenido”, que es la vista de contenido predeterminada. Utilice esta página central de la consola para obtener información inmediata sobre los usuarios, analizar contenido para tomar decisiones corporativas y reaccionar ante las advertencias.

A continuación, se detallan las diferentes vistas y parámetros que se muestran en el tablero.

Ajustes	Descripción
Historial de almacenamiento	Se puede ver información general de las cuotas de almacenamiento utilizando un resumen gráfico de seis barras.
Estado de usuario/contenido	Puede proporcionar un resumen de la conformidad de contenido de dispositivos en una sola vista utilizando los gráficos de iconos de estado. Cada gráfico representa el porcentaje de dispositivos o archivos que no están conformes. Seleccione estos iconos para ver los dispositivos que no están conformes y tome medidas administrativas.
Interacción con el contenido	Vea qué documentos son los más útiles y más solicitados por parte de los usuarios finales, y también los documentos que está considerando dejar de usar. Seleccione la información mostrada para navegar directamente a una página en la que pueda editar el contenido.
Análisis de usuarios	Información acerca de la actividad del usuario final hoy, esta semana o este mes. Los iconos representan a los usuarios finales y se rellenan con el porcentaje de usuarios finales que están activos.

Vista en lista de administración de contenido

Lleve a cabo las acciones necesarias en el contenido administrado por UEM que haya sido cargado y contenido sincronizado por el servidor de archivos corporativos desde la vista de lista de Content en Workspace ONE UEM Console. La “Vista de lista de contenido” contiene la información que introdujo mientras cargaba su contenido o repositorios, proporcionándole así un resumen visual de todo el contenido.

Para acceder a la lista, desplácese a Content > Vista de lista.

Ajustes	Descripción
Administrado por UEM	Vea y administre el contenido que agregó directamente a la consola de UEM en esta vista de lista predeterminada.

Ajustes	Descripción
Menú administrado por UEM	Lleve a cabo las acciones necesarias en el contenido administrado por UEM mediante las opciones de vista de lista disponibles. Agregar contenido: seleccione esta opción para agregar el contenido administrado por UEM a UEM Console. Espacio de almacenamiento usado: revise la barra de estado para ver el porcentaje de almacenamiento asignado que están utilizando los usuarios finales.
Servidores de archivos corporativos	Vea y administre los repositorios sincronizados en esta vista de lista o utilice las vistas en lista de contenido de los repositorios individuales.
Menú de “Servidores de archivos corporativos”	Para mostrar repositorios configurados en la vista de lista, seleccione Mostrar repositorios.
Filtro	Busque los documentos que desee utilizando los filtros disponibles. Categoría: filtre el contenido utilizando las categorías asignadas desde UEM Console. Tipo: filtre el contenido según el tipo de archivo. Estado de caducidad: filtre el contenido para mostrar solo el contenido que caducará en los próximos 14 días.
Activo/inactivo	Información sobre la disponibilidad del contenido para los usuarios finales. Los círculos verdes se muestran junto al contenido activo. Los círculos rojos se muestran junto al contenido inactivo. Las opciones de búsqueda, vista o envío automático al dispositivo no son permitidas para contenido inactivo.
Nombre	Seleccione esta opción para editar la Información general, los Detalles, la Versión anterior, la Seguridad, la Asignación y la Implementación que configuró al agregar el contenido. También puede descargar o eliminar las versiones anteriores del contenido.
Menú de acciones	Administre el contenido utilizando las opciones de menú disponibles. Los dos menús de acción de la vista de lista de Content difieren ligeramente. Para el contenido administrado por UEM, al seleccionar un solo archivo se muestra VER DISPOSITIVOS, AGREGAR VERSIÓN, DESCARGAR y MÁS ACCIONES. Al seleccionar varios archivos solo aparece el menú MÁS ACCIONES. En este menú, seleccione ELIMINAR para suprimir varios archivos a la vez.

Opciones de administración de contenido

Utilice estas opciones para administrar el contenido cargado o sincronizado y los metadatos en la vista de lista y otros menús de Workspace ONE UEM Console.

Acción	Administrado por UEM	Servidores de archivos corporativos	Plantilla automática	Plantilla manual	Repositorio agregado por el usuario	Categoría
Editar						

Acción	Administrado por UEM	Servidores de archivos corporativos	Plantilla automática	Plantilla manual	Repositorio agregado por el usuario	Categoría
Administrar ajustes de archivos individualmente. Los ajustes editados solo afectan al archivo individual y no a los ajustes globales del repositorio.	✓	✓	✓	✓	✓	
Descargar una copia local de la versión anterior del archivo.	✓					
Eliminar de la consola una versión anterior del archivo.	✓					
Actualizar un archivo existente con una nueva versión y archivar el archivo original.	✓					
Eliminar						
Eliminar un archivo de la consola de UEM.	✓					
Eliminar metadatos del archivo de la consola de UEM.		✓	✓	✓	✓	
Iniciar una sincronización manual entre el contenido de la red y Workspace ONE UEM.		✓	✓	✓	✓	
Eliminar una categoría o subcategoría vacía de la consola de UEM.						✓
Agregar						
Actualizar un archivo existente con una nueva versión y archivar el archivo original.	✓					
Agregar una subcategoría a una categoría.						✓
Sincronizar						
Iniciar una sincronización entre Workspace ONE UEM y los servidores de archivos corporativos integrados.		✓	✓	✓	✓	
Ver dispositivos						
Abrir una lista de dispositivos, ver el dispositivo al que se ha asignado un archivo individual.	✓	✓	✓	✓	✓	
Enviar un archivo individual a un dispositivo seleccionado.	✓	✓	✓	✓	✓	

Acción	Administrado por UEM	Servidores de archivos corporativos	Plantilla automática	Plantilla manual	Repositorio agregado por el usuario	Categoría
Eliminar un archivo individual de un dispositivo seleccionado.	✓	✓	✓	✓	✓	
Opciones adicionales						
Agregar un archivo al “Contenido destacado” para que el archivo se muestre en un lugar que llame la atención dentro de VMware Workspace ONE Content.	✓	✓	✓	✓	✓	✓
Descargar una copia local del archivo.	✓	✓	✓	✓	✓	
Eliminar un archivo de la consola de UEM.	✓					
Eliminar metadatos del archivo de la consola de UEM.		✓	✓	✓	✓	

Ajustes de administración de contenido

Los ajustes de la administración de contenido incluyen una variedad de configuraciones correspondientes a la administración de contenido.

Para acceder al menú de configuraciones disponibles, seleccione Ajustes.

Ajustes	Descripción
públicas	Acceda a las pantallas de configuración de VMware Workspace Content y VMware Content Locker Sync.
Content Gateway	Configure Content Gateway y descargue el instalador. A partir de la versión 9.6 de Workspace ONE UEM Console, Unified Access Gateway (UAG) es el tipo de instalación recomendado al configurar un nodo de Content Gateway. Puede utilizar esta opción para configurar una nueva Content Gateway en Unified Access Gateway o para migrar la Content Gateway existente a Unified Access Gateway. Para obtener más información sobre cómo configurar Content Gateway en Unified Access Gateway, consulte *Componentes de Workspace ONE UEM en Unified Access Gateway* en la documentación de *UAG*. Para obtener información sobre la migración, consulte la documentación *Migración de Content Gateway a Unified Access Gateway*.
Almacenamiento del usuario	Configure las excepciones de cuota de almacenamiento para usuarios individuales. Estas excepciones proporcionan el nivel de asignación de almacenamiento más detallado y reemplazan las configuraciones del grupo organizativo o del grupo de usuarios habilitadas en “Contenido personal”.
Avanzado	Configure las restricciones de tipo de archivo, la incorporación, los requisitos de contenido para la incorporación y la integración con un proveedor de firmas electrónicas de terceros.

Aviso: La base de datos de Workspace ONE UEM no admite caracteres fuera de los límites de la intercalación. Supongamos que está intentando sincronizar Workspace ONE UEM con un repositorio externo que contiene archivos. El repositorio externo tiene dos archivos. El nombre de un archivo contiene caracteres de la intercalación de la base de datos, mientras que nombre del otro archivo

contiene caracteres de fuera de la intercalación de la base de datos. En este caso, la base de datos de UEM no puede sincronizarse porque no puede distinguir entre archivos con nombres distintos. Por lo tanto, cualquier entrada que realice como administrador o usuario guardada en la base de datos de UEM debe cumplir con el conjunto de caracteres SQL_Latin1_General_CP1_CI_AS (Latín 1 general, no distingue entre mayúsculas y minúsculas, distingue acentos, no distingue tipos de kana ni anchura para datos Unicode; orden de clasificación 52 de SQL Server en la página de códigos 1252 para datos que no son Unicode). Cualquier carácter que se desvíe de esta intercalación de base de datos puede provocar un comportamiento inesperado.