Enterprise Mobility Management

Guía del usuario

Versión R9

Español

Marzo 20, 2015

Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at http://www.kaseya.com/legal.aspx. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement."

Contenido

Introducción

Enterprise Mobility Management es un nuevo módulo que proporciona una solución integrada de clase empresarial para administrar dispositivos móviles, aplicaciones y acceso seguro a los datos de una compañía por política. Esto incluye la implementación más rápida de la industria para incorporar a las organizaciones cliente y a sus usuarios. Los dispositivos móviles pueden pertenecer a la compañía o a los empleados. Los activos empresariales siempre se aíslan de los datos personales. Los datos se protegen mediante el cifrado AES-256 en modo activo e inactivo.

Una interfaz de usuario integrada y fácil de usar le permite realizar lo siguiente con rapidez:

- Incorporar organizaciones cliente nuevas y existentes a **Enterprise Mobility Management** mediante un asistente para configuración.
- Aplicar políticas de seguridad alta, media y baja que puede personalizar.
- Usar perfiles de configuración prestablecidos para cada nivel de seguridad.
- Enviar invitaciones a los usuarios para registrar sus dispositivos. Al registrarse, se instala una aplicación de agente de Kaseya en el dispositivo, denominada *MobileManage*.
- Administrar varios dispositivos para cada usuario.
- Requerir o no permitir la instalación de aplicaciones en dispositivos móviles.
- Identificar las aplicaciones instaladas en los dispositivos móviles.
- Auditar todos los dispositivos móviles, lo que proporciona un inventario del sistema operativo, información del dispositivo, las propiedades de plataforma y de red.
- Habilitar o deshabilitar el seguimiento de la ubicación de los dispositivos móviles en tiempo real y el mantenimiento de un historial de ubicación.
- Forzar que suene una alarma en los dispositivos para ayudar a los usuarios a localizar los dispositivos perdidos.
  - Bloquear, borrar o restablecer dispositivos perdidos o robados.
  - Recibir alertas si un dispositivo perdido se registra o no cumple los requisitos.
  - Enviar mensajes de texto desde **Enterprise Mobility Management** hacia los dispositivos móviles.
  - Proporcionar a los usuarios de los dispositivos móviles acceso seguro a los sitios web y los documentos internos de la compañía mediante dos aplicaciones contenedoras.
    - ✓ La aplicación de explorador de sitios web se denomina *WorkBrowser*. Opcionalmente, puede controlar el acceso a los sitios web internos vinculados con *WorkBrowser* mediante direcciones URL de proxy.
    - ✓ La aplicación de explorador de documentos se denomina *WorkBrowser*. *WorkDocs* permite que un usuario edite y guarde documentos de forma local, o cargue los documentos modificados a las redes internas de la compañía.

Licencias

- Las licencias se otorgan por la cantidad de usuarios que se administran con **Enterprise Mobility Management**. Cada usuario con licencia puede tener una cantidad ilimitada de dispositivos administrados con **Enterprise Mobility Management**.

Interfaz de usuario simplificada

La interfaz de usuario consta de una única página con cuatro pestañas. En cada pestaña, se incluyen cuatro menús desplegables para lo siguiente:

- Usuarios
- Dispositivos
- Aplic
- Políticas

Integración con Active Directory

Enterprise Mobility Management usa la instancia de Active Directory de una organización cliente para identificar a los usuarios que recibieron la invitación para registrar sus dispositivos móviles. Las políticas de seguridad de **Enterprise Mobility Management** se aplican a un dispositivo según su asociación a un usuario de Active Directory. **Enterprise Mobility Management** no almacena credenciales de usuario, sino que simplemente funciona como un medio para retransmitir la autenticación de Active Directory.

Dispositivos móviles compatibles

Enterprise Mobility Management admite los siguientes dispositivos móviles:

- iOS versión 7.0 y superiores
- Android versión 4.0.3 y superiores

Lanzamiento inicial

Para el lanzamiento inicial, **Enterprise Mobility Management** solo se admite en entornos locales. Al actualizar a R9 en un entorno local, se elimina la administración de dispositivos móviles y se agrega **Enterprise Mobility Management**. No se admite la migración de datos de la administración de dispositivos móviles a **Enterprise Mobility Management**.

> **Nota:** **Enterprise Mobility Management** solo puede usar la **dirección IP externa** *(http://help.kaseya.com/webhelp/ES/VSA/9000000/index.asp#248.htm)* especificada para el VSA en el momento en que se lo instaló o se actualiza a R9. El módulo **Enterprise Mobility Management** no admite el cambio de la dirección IP externa del VSA después de la instalación o la actualización.

Requisitos del módulo Enterprise Mobility Management

Kaseya Server

- El módulo Enterprise Mobility Management R9 requiere un VSA R9 local. Mobile Device Management se desinstala al realizar la actualización.

  > **Nota:** Los entornos SaaS del VSA continúan usando Mobile Device Management al actualizar a R9.

- Este módulo requiere que el VSA tenga acceso a Internet y esté habilitado con SSL mediante un certificado de una autoridad reconocida.
- Las organizaciones cliente deben tener Active Directory para agregar usuarios a Enterprise Mobility Management.

Requisitos para todos los dispositivos móviles administrados

- iOS versión 7.0 y superiores
- Android versión 4.0.3 y superiores

Requisitos para los servidores de Active Directory

- Permitir el acceso desde el VSA. El puerto 389 o 636 debe estar abierto. Si el VSA no comparte la misma intranet que una instancia de Active Directory, dicha instancia debe estar disponible en una dirección IP pública. Por motivos de seguridad, esta dirección IP solo sebe ser accesible desde la dirección IP del VSA de MSP. Los dispositivos móviles retransmiten sus solicitudes de autenticación a través del VSA para llegar a una instancia de Active Directory. Las organizaciones cliente deben *incluir la dirección IP del VSA en una lista blanca* para los servidores que hospedan instancias Active Directory de clientes.
- Habilitar SSL/TLS

Requisitos para los servidores WebDAV

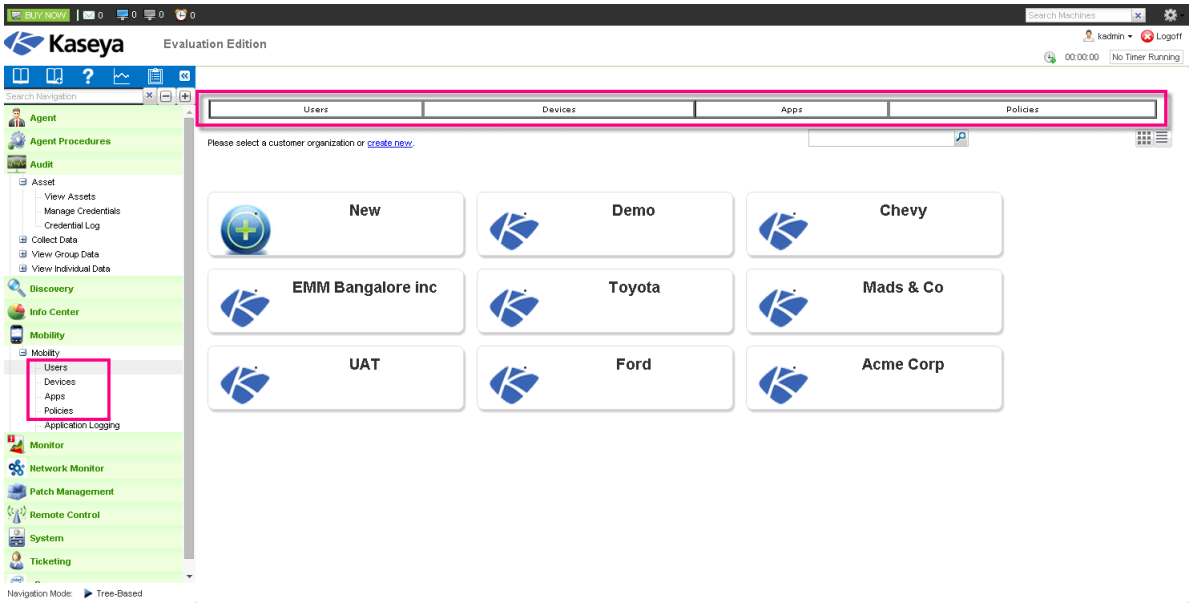
- Habilitar NTLM si se requiere autenticación.
- El host del VSA debe tener acceso a los servidores WebDAV. Si el VSA no comparte la misma intranet que un servidor WebDAV, dicho servidor debe estar disponible en una dirección IP pública. Por motivos de seguridad, esta dirección IP solo sebe ser accesible desde la dirección IP del VSA. Los dispositivos móviles retransmiten sus solicitudes a través del VSA para llegar a estos servidores WebDAV. Las organizaciones cliente deben *incluir la dirección IP del VSA en una lista blanca* para los servidores que hospedan servidores WebDAV.

Interfaz de usuario

Enterprise Mobility Management se identifica como el módulo **Mobility** en el panel de navegación del VSA. El módulo se organiza en una única interfaz de usuario integrada. En la parte superior de cada página o en el lado del panel de navegación, figuran las mismas cuatro funciones:

- Usuarios
- Dispositivos
- Aplic
- Políticas

La primera vez que ve el módulo **Mobility**, aparece una vista de mosaico de las organizaciones cliente existentes, similar a la imagen que figura a continuación. *Todas las tareas que se realizan en el módulo* **Mobility** *comienzan con esta misma interfaz de usuario.*



Configuración de la integración con Active Directory

Enterprise Mobility Management usa la instancia de Active Directory de una organización cliente para identificar a los usuarios que recibieron la invitación para registrar sus dispositivos móviles. Las políticas de seguridad de **Enterprise Mobility Management** se aplican a un dispositivo según su asociación a un usuario de Active Directory.

Conceptos clave de integración

- Las organizaciones cliente deben tener Active Directory para agregar usuarios a Enterprise Mobility Management. Consulte **Requisitos del módulo Enterprise Mobility Management** *(página 2)* para obtener los requisitos adicionales de Active Directory.
- Los registros de usuarios se importan de Active Directory a **Enterprise Mobility Management**.
- El grupo de seguridad al que pertenece un usuario en Active Directory determina el perfil de política que se le asigna en **Enterprise Mobility Management**. Al pasar un usuario a otro grupo de seguridad en Active Directory, se lo reasigna a otro perfil de política en **Enterprise Mobility Management**.
- Los dispositivos se asignan a los usuarios una vez que se instala y se registra el agente de Kaseya en los dispositivos con el código de activación exclusivo que reciben por correo electrónico.
- Los dispositivos móviles del usuario no necesitan acceder a Active Directory para realizar la autenticación. Se envía una solicitud de aplicación del dispositivo a **Enterprise Mobility Management**, lo que transmite la solicitud a Active Directory.
- El componente de autenticación de AD de **Enterprise Mobility Management** no almacena credenciales de usuario, sino que simplemente funciona como un medio para retransmitir la autenticación de AD.

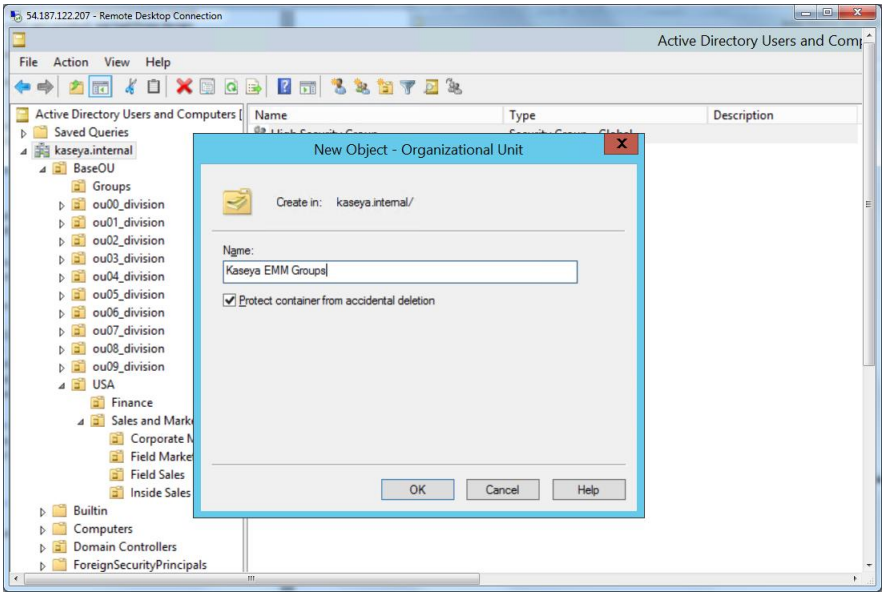
Creación de tres grupos de seguridad de Active Directory

Enterprise Mobility Management requiere la creación de tres grupos de seguridad en Active Directory. Estos se asignan a tres políticas de seguridad en **Enterprise Mobility Management**:

- `Política de seguridad alta`
- `Política de seguridad media`
- `Política de seguridad baja`

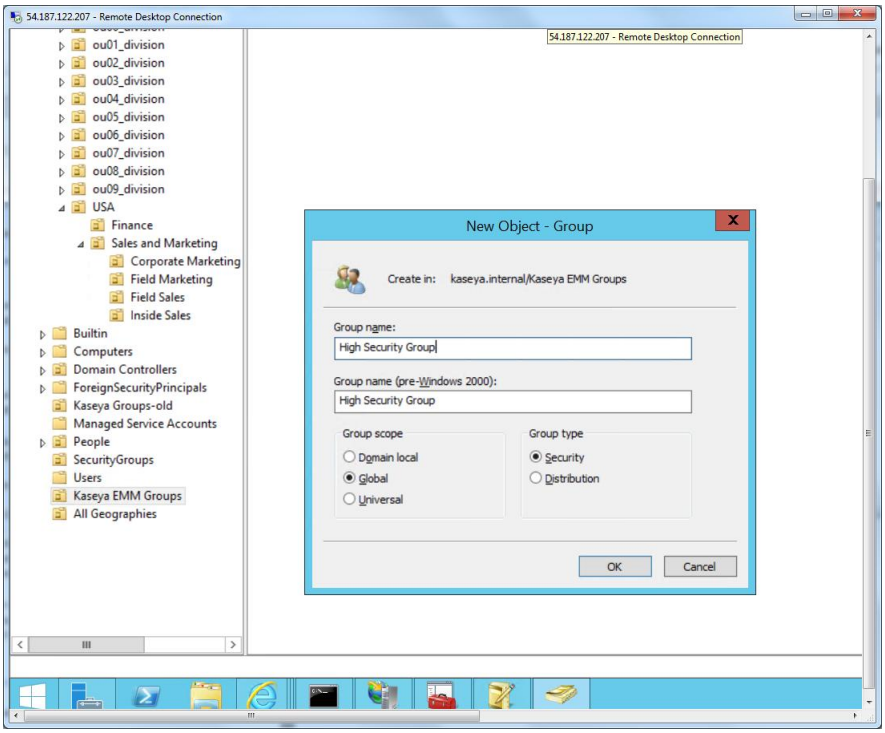
Todos los registros de usuarios de Active Directory que se deben importar a **Enterprise Mobility Management** se deben incluir en uno de estos tres grupos de seguridad.

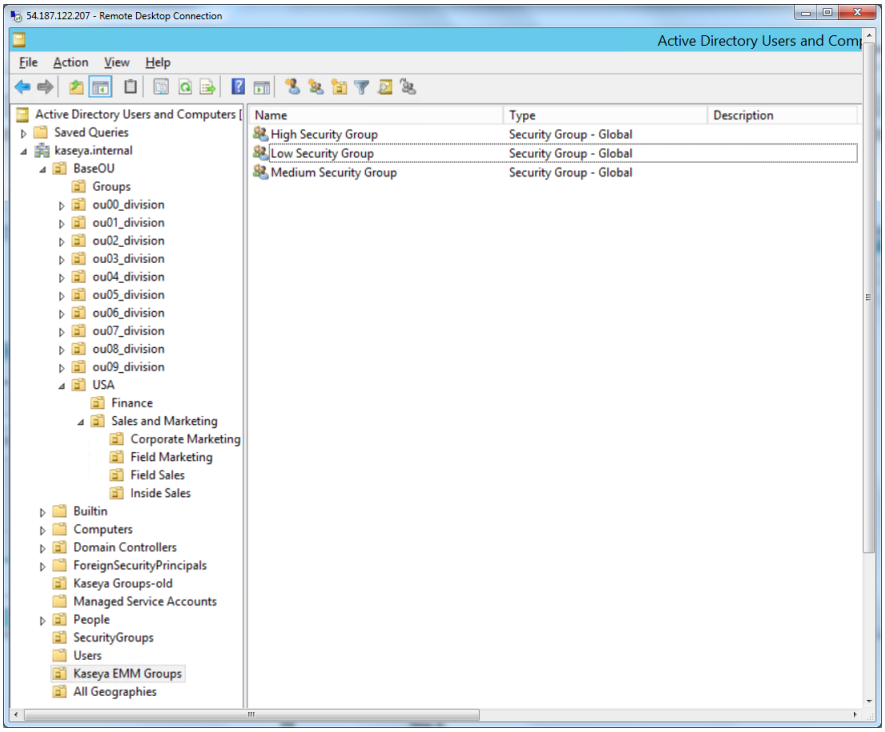
1. Abra la consola de Active Directory y cree una nueva *unidad organizativa* denominada `Kaseya EMM Groups` en el dominio principal.



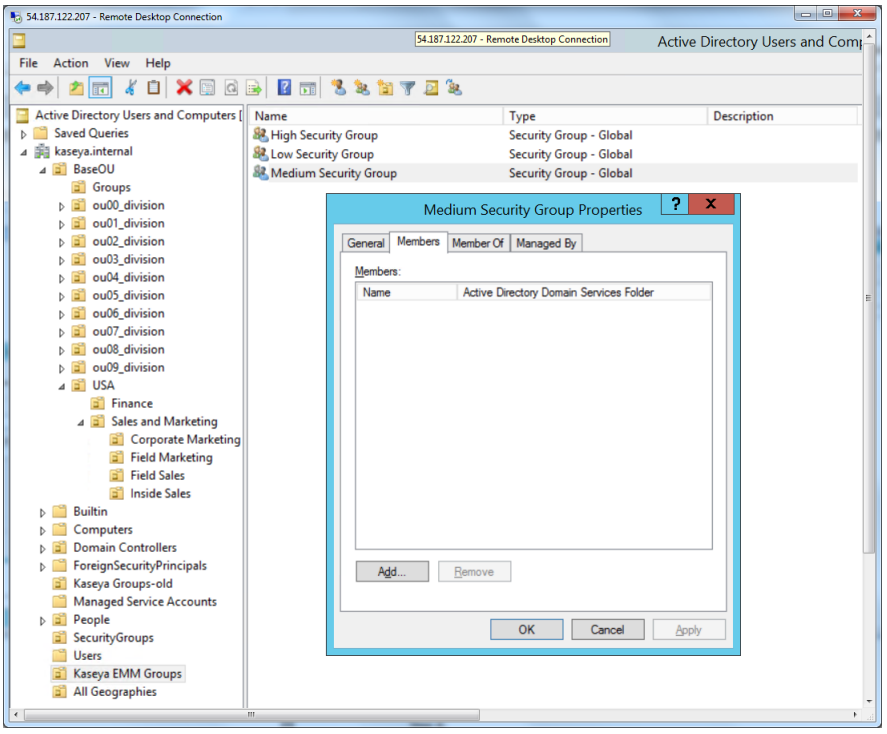
2. Cree tres grupos de seguridad en `Kaseya EMM Groups`. Asígneles los nombres `High Security Group`, `Medium Security Group` y `Low Security Group`.

> **Nota:** Puede asignarles otros nombres, pero para facilitar la asignación a **Enterprise Mobility Management**, se recomienda usar estos.

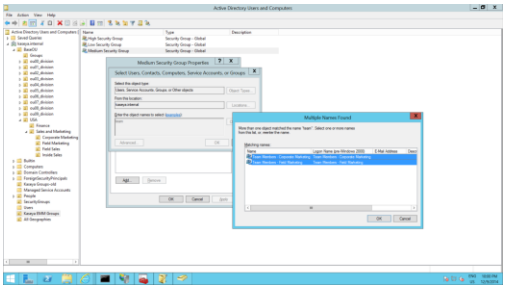




3. Haga clic con el botón secundario en cada uno de los tres `Kaseya EMM Groups` y, a continuación, haga clic en la opción `Properties`. Abra la pestaña `Members` y, a continuación, haga clic en el botón `Add`.



4. En Active Directory, busque los usuarios que se deben agregar a cada uno de los tres `Kaseya EMM Groups`.



Ya creó los tres grupos de seguridad de EMM (alta, media y baja) y les asignó los usuarios correspondientes.

5. Una vez que se complete la configuración, anote lo siguiente. Esta información se necesita para conectarse a cualquier instancia de Active Directory que desee asociar a una organización en **Enterprise Mobility Management**.
   - El nombre de dominio o la dirección IP del servidor de Active Directory.
   - El puerto LDAP que usa Active Directory. El puerto LDAP predeterminado es el 389. El puerto LDAP SSL predeterminado es el 636.
   - El DN (nombre distintivo) base que se debe buscar. Ejemplo: `OU=Kaseya EMM Groups,DC=company,DC=com`
   - La credencial que se debe usar para autenticar el acceso de lectura a este nombre distintivo. Se recomienda usar una credencial exclusiva.

Incorporación de clientes

Se deben agregar organizaciones cliente a **Enterprise Mobility Management** antes de invitar usuarios para que registren sus dispositivos.

Requisito previo: Antes de comenzar, cada organización cliente que agregue *debe tener una instancia de Active Directory configurada para integrar en* **Enterprise Mobility Management**. Consulte **Configuración de la integración con Active Directory** *(página 3)*.

Creación de una nueva organización en el VSA

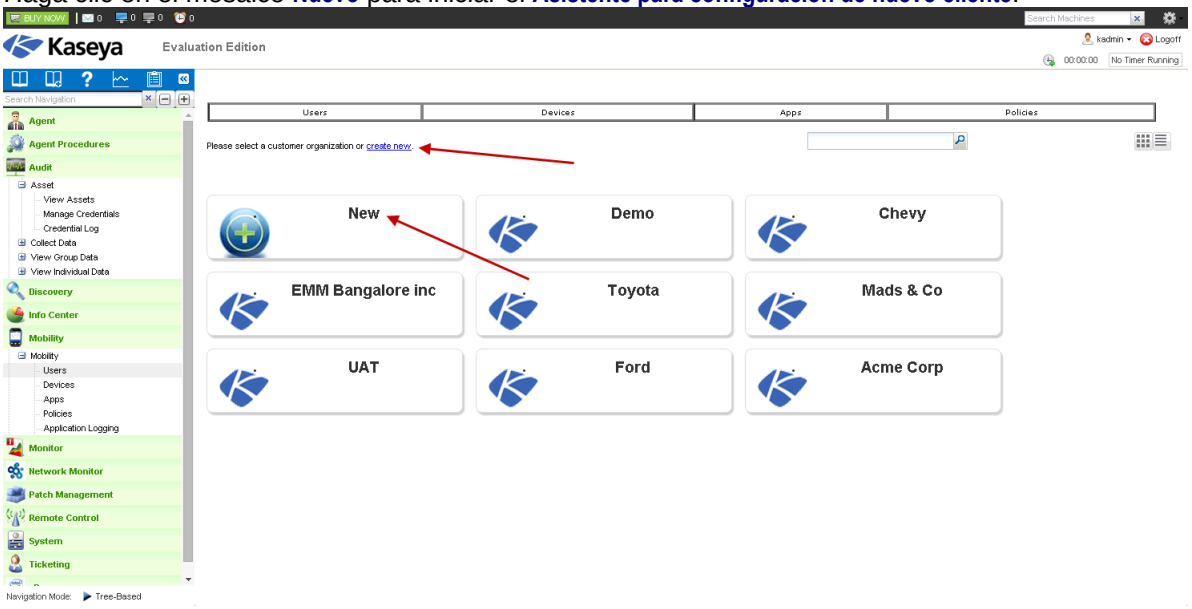
Siga este procedimiento si la organización cliente que desea agregar es nueva en todo el VSA.

1. Navegue a la página **Administrar** en Sistema > Orgs/Grupos/Deptos/Personal.
2. Haga clic en **Nuevo** para que aparezca el cuadro de diálogo **Agregar organización**.
3. Introduzca un **ID** y un **nombre de organización** para identificar la nueva organización cliente.
4. Haga clic en **Guardar**.

Se creó la nueva organización cliente. A continuación, regrese al módulo **Mobility** para agregar la organización cliente a **Enterprise Mobility Management**.

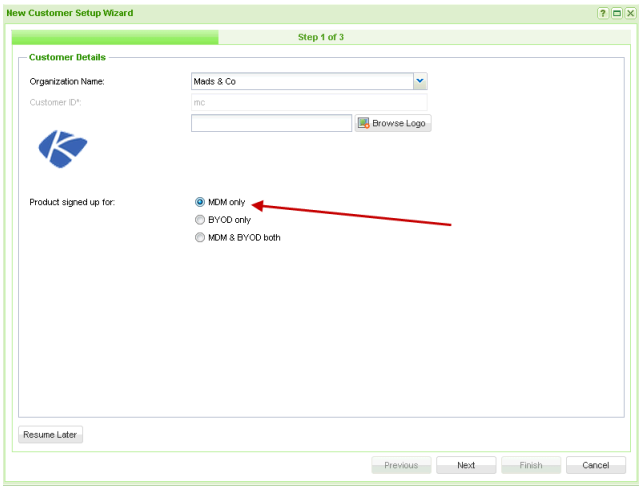
Cómo agregar una organización cliente al módulo Mobility

1. Haga clic en el mosaico **Nuevo** para iniciar el **Asistente para configuración de nuevo cliente**.



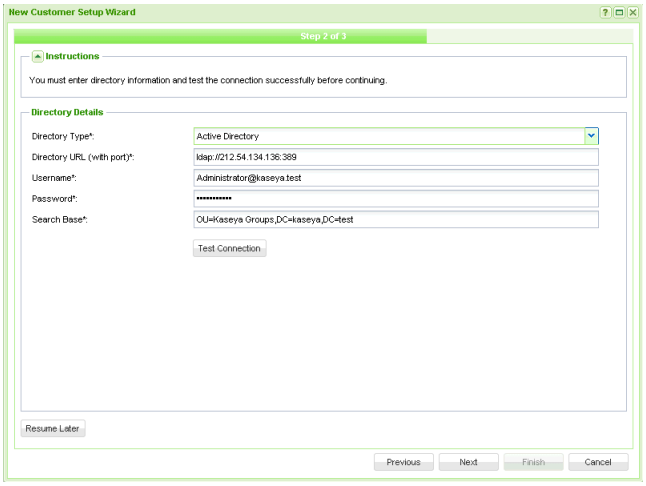
2. Seleccione la organización cliente que desea agregar al módulo **Mobility**.
3. Opcionalmente incluya un logotipo de cliente.
4. Seleccione **Solo MDM**, **Solo BYOD** o **MDM y BYOD**. La selección determina las opciones y los perfiles de política que se muestran en la interfaz de usuario cuando se selecciona esta organización cliente.

5. Haga clic en **Siguiente**.



6. Especifique los parámetros de Active Directory que debe usar **Enterprise Mobility Management** para identificar usuarios en la organización cliente.

> **Nota:** Cada organización cliente que agregue *debe tener una instancia de Active Directory configurada para integrar en* **Enterprise Mobility Management**. Consulte **Configuración de Active Directory para la integración** *(página 3)*.
>
> **Nota:** Si aún no configuró Active Directory, haga clic en **Reanudar más adelante**. Puede hacer clic en el mosaico de esta organización cliente para regresar a este paso del asistente. Para indicar que aún no se configuró Active Directory, se muestra un asterisco en el mosaico de una organización cliente.

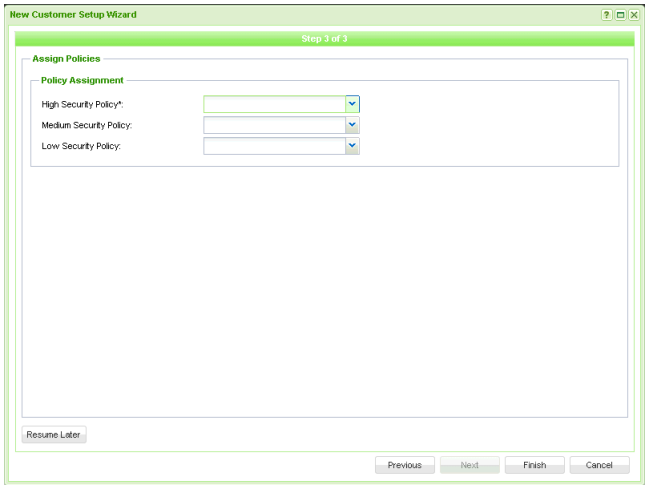


- **Tipo de directorio**: **Active Directory** es la única opción.
- **URL del directorio (con puerto)**: introduzca una URL LDAP. El puerto predeterminado para LDAP es el `389`. Ejemplo: `ldap://212.54.134.136:389`
- **Nombre de usuario**: introduzca un nombre de usuario de Active Directory que proporcione acceso al *nombre distintivo* especificado en el campo **Buscar base**.
- **Contraseña**: introduzca la contraseña.
- **Buscar base**: introduzca el *nombre distintivo* utilizado para buscar los tres grupos de usuarios en esta instancia de Active Directory que cumplen con los requisitos para registrar sus dispositivos en **Enterprise Mobility Management**. Ejemplo: `OU=Kaseya EMM Groups,DC=company,DC=com`

7. Haga clic en el botón **Probar conexión** para verificar la conexión a Active Directory.

- Si es correcta, haga clic en **Siguiente** para completar **Enterprise Mobility Management** con los tres grupos de usuarios que cumplen con los requisitos para registrar sus dispositivos en **Enterprise Mobility Management**.
- Si la prueba no es correcta, verifique que los valores introducidos en esta página del asistente coincidan con la configuración de Active Directory. La prueba debe ser correcta para continuar con la incorporación de esta organización cliente.

8. Asigne políticas de dispositivos móviles de **Enterprise Mobility Management** a la nueva organización cliente.
   - Puede asignar una política `alta`, una `media` y una `baja` a cada organización cliente que registre en **Enterprise Mobility Management**.
   - Seleccione las políticas `altas`, `medias` y `bajas` predeterminadas si aún no creó políticas específicas del cliente.

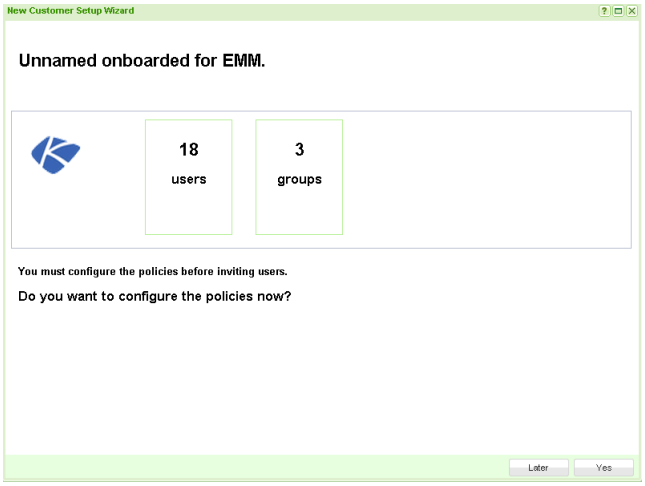


9. En la última página del asistente, se devuelven recuentos para los usuarios y los grupos que devolvió la búsqueda de Active Directory. Estos usuarios y grupos se importan a **Enterprise Mobility Management**. Se presentan dos opciones:
   - Haga clic en **Más tarde** para aceptar las políticas predeterminadas predefinidas para la organización cliente incorporada recientemente. *Esta opción omite la configuración de propiedades personalizables específicas de la organización cliente.*

     Nota: Es posible que desee invitar usuarios de inmediato para que registren un dispositivo móvil en **Enterprise Mobility Management**. Consulte **Incorporación de usuarios** *(página 10)* para obtener detalles.

   - Haga clic en **Sí** para *configurar nuevas políticas específicas del cliente que incluyan tanto propiedades predefinidas como personalizables.*

> **Nota:** Consulte **Configuración de políticas** *(página 17)* para obtener detalles acerca de la selección de esta opción.



Incorporación de usuarios

De manera automática, los usuarios reciben una invitación para instalar un agente de Kaseya en sus dispositivos móviles no bien se importan usuarios de Active Directory a Enterprise Mobility Management (página 7). Cuando ve la lista de usuarios en esta página por primera vez, el estado de usuario ya se muestra como `Invitado`. Es posible que desee invitar a un usuario una vez más si este no recibió la invitación original por correo electrónico.

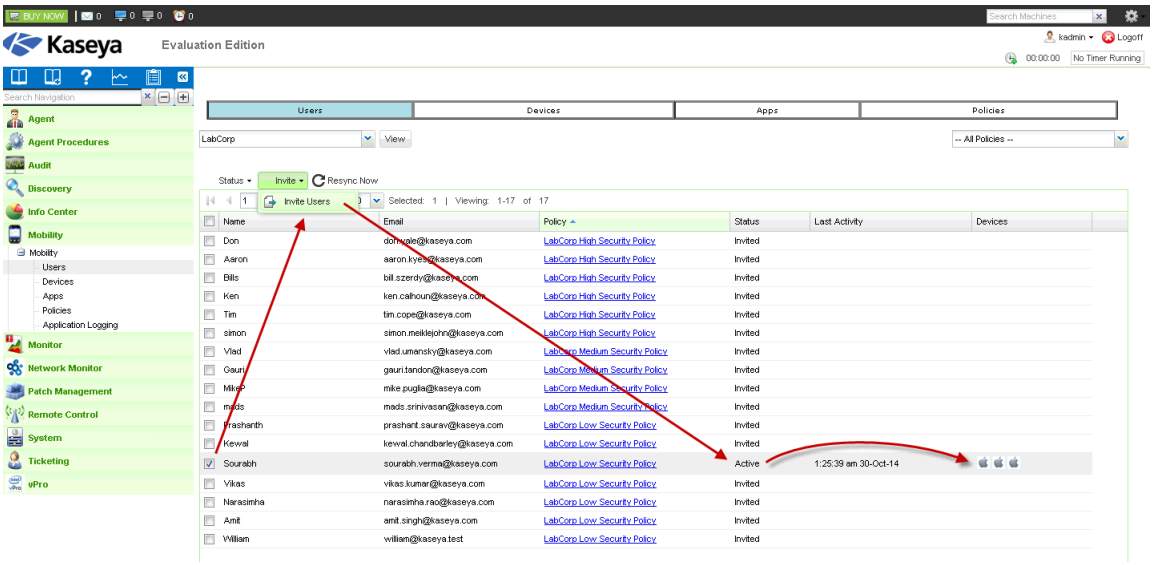
Para volver a invitar usuarios, haga lo siguiente:

1. Navegue a la página **Usuarios**.
2. Seleccione uno o más usuarios.

> **Nota:** Si no ve un usuario que esperaba ver, puede hacer clic en el botón **Resincronizar ahora**. Con esto, se vuelve a conectar a la instancia de Active Directory de la organización cliente y se actualiza la lista de usuarios para la organización cliente seleccionada.

3. Haga clic en Invitar > opción **Invitar usuarios**.
   - En la columna **Estado**, se muestra `Invitado` cuando se envió una invitación a un usuario.
   - En la columna **Estado**, se muestra `Activo` cuando el usuario instala el agente **Enterprise Mobility Management** en al menos uno o dos dispositivos.
   - La cantidad de dispositivos que administra **Enterprise Mobility Management** para ese usuario se indica con los íconos de dispositivo en la columna **Dispositivos**.

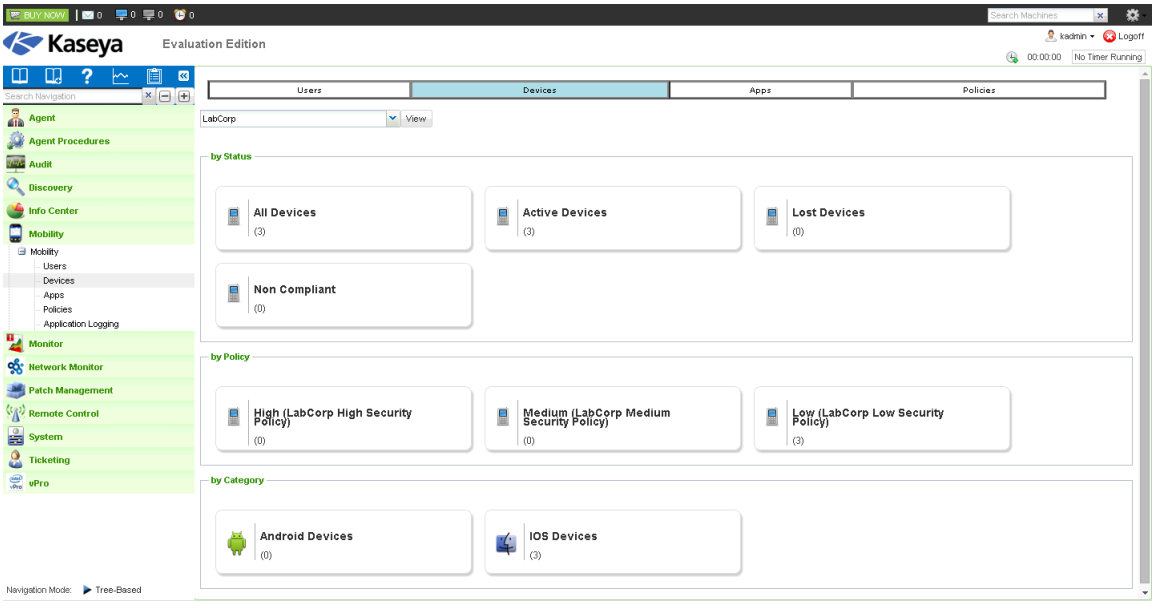
> **Nota:** Consulte **Administración de dispositivos** *(página 11)* para obtener detalles acerca de la administración de dispositivos móviles.



Administración de dispositivos

Una vez que los usuarios registran dispositivos en **Enterprise Mobility Management**, se pueden administrar estos dispositivos.

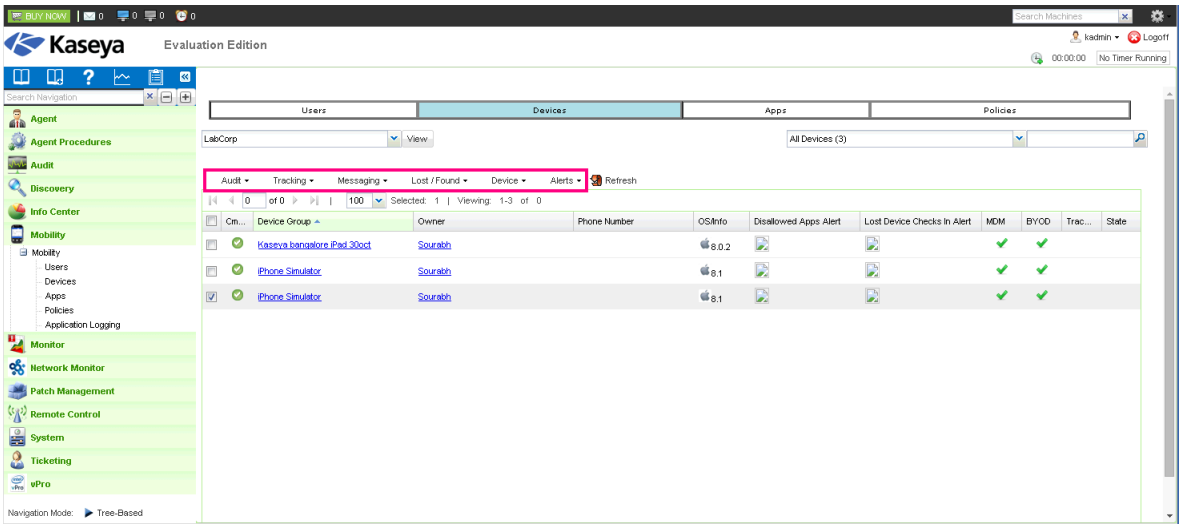
1. Navegue a la página **Dispositivos**.
2. Seleccione una organización cliente.
3. Seleccione uno de los mosaicos. Los mosaicos se organizan de la siguiente manera:
   - **Por estado**
   - **Por política**
   - **Por categoría**



Se muestra una lista de dispositivos con el filtro seleccionado.

4. Seleccione una o más filas de la lista de dispositivos para habilitar todas las pestañas en la parte superior de la tabla.

> **Nota:** Al hacer clic en el hipervínculo del nombre de un dispositivo en la página **Dispositivos**, se muestran los detalles del dispositivo en una serie de pestañas. Para obtener más información, consulte **Detalles de dispositivos** *(página 14)*.



5. Al hacer clic en el ícono de **Comando** de un dispositivo de la lista, aparece la ventana **Estado del comando** *(página 12)*.
6. Las acciones que puede realizar en los dispositivos se organizan en las siguientes pestañas. Consulte cualquiera de los siguientes temas para obtener más detalles.
   - **Auditar** *(página 13)*
   - **Rastreo** *(página 13)*
   - **Mensajería** *(página 13)*
   - **Perdido/Encontrado** *(página 13)*
   - **Dispositivos** *(página 14)*
   - **Alertas** *(página 14)*

Estado de comando

Al hacer clic en el ícono de **Comando** de un dispositivo de la lista, aparece la ventana **Estado del comando**. En esta ventana, se muestra el estado de los comandos que se envían a un dispositivo.

- El comando está pendiente. El agente no se registró para recuperarlo.
- El agente está procesando el comando.
- La operación se completó.
- Se produjo un error en el comando.

Use la opción **Marcar completo** para establecer de forma manual uno o más comandos para completar .

Acciones de Auditoría

Las auditorías se realizan no bien el usuario instala un agente de Kaseya en el dispositivo móvil. A partir de entonces, las auditorías se ejecutan a diario de manera predeterminada.

- **Programar auditoría**: permite programar una auditoría para dispositivos seleccionados a una hora especificada. Se puede programar por única vez o en forma periódica. En cada tipo de periodicidad (a diario, semanalmente, mensualmente), se muestran opciones adicionales adecuadas para ese tipo de periodicidad. La programación periódica incluye configurar las fechas de inicio y de finalización para la recurrencia.
- **Ejecutar auditoría ahora**: permite ejecutar la auditoría de un dispositivo seleccionado de inmediato.
- **Obtener registros**: *el registro de dispositivos es únicamente para propósitos de soporte técnico de Kaseya.* En el registro de dispositivos, se muestran los mensajes reales que se envían entre el VSA y el dispositivo seleccionado.

Acciones de Seguimiento

Puede realizar cualquiera de las siguientes acciones de **Seguimiento** en un dispositivo.

- **Habilitar seguimiento**: permite iniciar el seguimiento de la ubicación de los dispositivos seleccionados. Una vez que se inicia, puede ver el seguimiento del dispositivo en la pestaña **Ubicación** del dispositivo. Consulte **Vista de detalles de dispositivos** *(página 14)*.
- **Deshabilitar seguimiento**: permite detener el seguimiento de la ubicación de los dispositivos seleccionados.
- **Obtener ubicación actual**: devuelve la ubicación actual de un dispositivo seleccionado a petición, sin realizar un seguimiento continuo de su ubicación.
- **Historial de ubicación**: se muestra el historial de ubicación de un dispositivo.

Acciones de Mensajería

Puede realizar cualquiera de las siguientes acciones de **Mensajería** en un dispositivo.

- **Ver**: se muestra el historial de mensajes enviados al usuario.
- **Enviar**: se muestra un cuadro de diálogo que puede usar para introducir y enviar un mensaje de texto al usuario.

Acciones de Perdido/Encontrado

Puede realizar cualquiera de las siguientes acciones de **Perdido/Encontrado**.

- **Hacer sonar alarma de robo**: si está activada, los dispositivos repiten la frase “Este teléfono es robado” cada vez que se encienden. Consulte **Silenciar alarma** a continuación.
- **Eliminar datos**: si está activada, se restablece la configuración predeterminada de los dispositivos seleccionados. **Al eliminar los datos de un dispositivo, se eliminan todos los datos del usuario**, incluida la aplicación *MobileManage*. Después de borrar los datos del dispositivo, la aplicación *MobileManage* ya no puede registrarse.
- **Borrar código de acceso**: permite restablecer los códigos de acceso *de nivel de dispositivo* en los dispositivos iOS seleccionados. El restablecimiento desbloquea el dispositivo, lo que permite que el usuario lo use sin un código de acceso o que establezca uno nuevo. Al borrar el código de acceso, no se modifica el perfil de seguridad subyacente. Si el dispositivo está configurado para solicitar un código de acceso de nivel de dispositivo, se solicita al usuario que introduzca uno nuevo de inmediato.

- **Solicitar registro**: se indica a los usuarios de los dispositivos seleccionados que toquen el ícono de la aplicación *MobileManage* para abrirla. Al abrir la aplicación *MobileManage*, la aplicación se registra de inmediato.
- **Marcar como perdido**: marca los dispositivos seleccionados como perdidos.
- **Marcar como encontrado**: marca los dispositivos seleccionados como encontrados.
- **Silenciar alarma**: detiene las alarmas establecidas con las acciones de **Hacer sonar alarma de robo** en los dispositivos seleccionados.

Acciones de Dispositivos

Puede realizar cualquiera de las siguientes acciones de **Dispositivos** en un dispositivo.

- **Bloquear dispositivo**: si está activada, los dispositivos seleccionados se bloquean y no permiten el acceso de usuarios.
- **Eliminar**: elimina las cuentas de los dispositivos seleccionados en **Enterprise Mobility Management**.

Acciones de Alertas

Puede realizar cualquiera de las siguientes acciones de **Alertas** en un dispositivo.

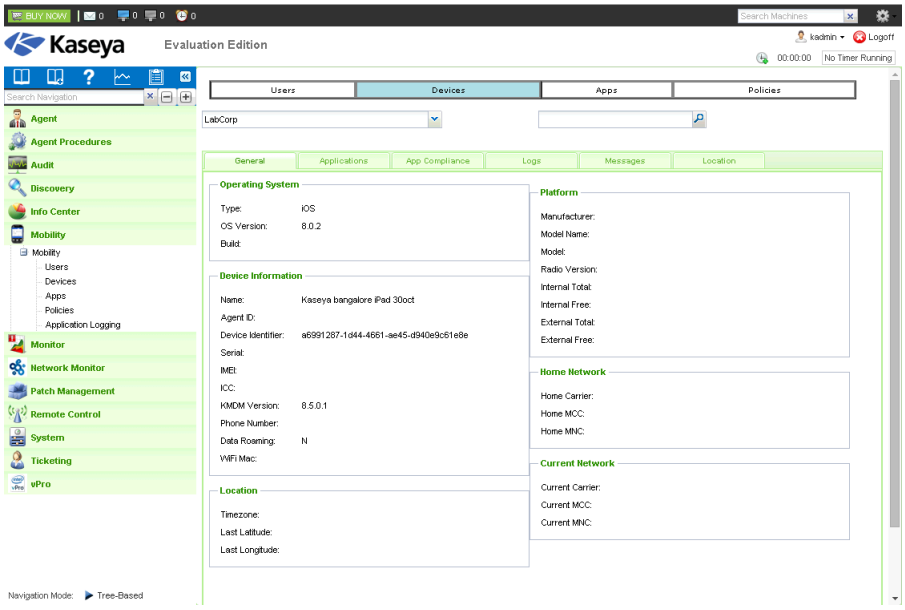
- **Detalles**: se muestra una ventana **Detalles de alerta** para los dispositivos seleccionados.
  - **Nombre de alerta**: el tipo de alerta, `Alerta de dispositivo perdido registrado` o `Verificación de cumplimiento de aplicaciones`.
  - **Habilitado**: las alertas están siempre habilitadas.
  - **Estado**: `alerta` o `normal` ✔.
  - **Detalles**: para una `Alerta de cumplimiento de aplicaciones`, se muestran los recuentos de las `aplicaciones requeridas` o las `aplicaciones no permitidas`.
  - **Acción**: resuelve la alerta y la restablece al estado normal.
- **Resuelto**: resuelve las alertas, por tipo de alerta, de los dispositivos seleccionados. Al resolverse una alerta, se notifica a los usuarios de los dispositivos móviles seleccionados.

Vista de detalles de dispositivos

Al hacer clic en el hipervínculo del nombre de un dispositivo en la página **Dispositivos**, se muestran los detalles del dispositivo en una serie de pestañas.

- **General**
- **Aplicación**
- **Cumplimiento de aplicaciones**
- **Registros**
- **Mensajes**

- **Ubicación**



Pestaña general

Sistema Operativo

- **Tipo**: el tipo de sistema operativo en el dispositivo.
- **Versión del SO**: la versión del sistema operativo que utiliza el dispositivo.
- **Versión**: el número de versión del sistema operativo.

Información de dispositivo

- **Nombre**: el nombre que utiliza el dispositivo para identificarse.
- **ID de agente**: el GUID del agente de Kaseya.
- **Identificador del dispositivo**: un identificador único asignado al dispositivo por el fabricante.
- **Número de serie**: el número de serie del dispositivo.
- **IMEI**: el identificador único del conjunto principal del dispositivo, independiente de la tarjeta SIM conectada a este. El número IMEI se aplica a los teléfonos móviles GSM, WCDMA e iDEN.
- **ICC**: el identificador único de la tarjeta SIM conectada en un dispositivo.
- **Versión de KMDM**: versión de la aplicación *MobileManage* en el dispositivo.
- **Número de teléfono**: el número de teléfono del dispositivo. Algunos dispositivos móviles no tienen números de teléfono.
- **Roaming de datos**: `verdadero` o `falso`.
- **MAC de WiFi**: el ID de MAC del dispositivo.

Ubicación

- **Zona horaria**: la zona horaria que utiliza el dispositivo.
- **Última latitud**: la última latitud que devolvió el dispositivo.
- **Última longitud**: la última longitud que devolvió el dispositivo.

Plataforma

- **Fabricante**: el fabricante del hardware del dispositivo.
- **Nombre del modelo**: el nombre del modelo de hardware del dispositivo.

- **Modelo**: el número del modelo del hardware del dispositivo.
- **Versión de radio**: la versión del firmware de módem que utiliza el dispositivo. También se denomina versión de “banda base”.
- **Interna total**: la memoria total disponible incorporada en el hardware.
- **Interna libre**: la memoria libre disponible incorporada en el hardware.
- **Externa total**: la memoria externa total disponible.
- **Externa libre**: la memoria externa libre disponible.

Red nacional

- **Proveedor de servicios de telefonía móvil nacional**: el principal proveedor de servicios del dispositivo.
- **MCC nacional**: el código de telefonía móvil de país en el que se encuentra el dispositivo. Los países de gran extensión pueden tener más de un código de telefonía móvil de país.
- **MNC nacional**: el código de red de telefonía móvil del proveedor u operador de servicios de telefonía móvil nacional del dispositivo.

Red actual

- **Proveedor de servicios de telefonía móvil actual**: el proveedor de servicios de telefonía móvil que usa actualmente el dispositivo.
- **MCC actual**: el código de país de telefonía móvil que usa actualmente el dispositivo.
- **MNC actual**: el código de red de telefonía móvil del proveedor u operador de servicios de telefonía móvil que usa actualmente el dispositivo.

Pestaña Aplicaciones

En la pestaña **Aplicaciones**, se muestra una lista de las aplicaciones instaladas en el dispositivo móvil administrado seleccionado.

Pestaña Cumplimiento de aplicaciones

En la pestaña **Cumplimiento de aplicaciones**, se muestran las **Aplicaciones requeridas que faltan en el dispositivo**.

- **Nombre del paquete**: nombre completo de la aplicación en formato de dominio inverso. Ejemplo: `com.kaseya.enterprise.agent`.
- **Nombre de la aplicación**: el nombre descriptivo de la aplicación. Ejemplo: `Agent`.

Pestaña Registros

En la pestaña **Registros**, se muestran las entradas del registro del dispositivo. *El registro de dispositivos es únicamente para propósitos de soporte técnico de Kaseya.* En el registro de dispositivos, se muestran los mensajes reales que se envían entre el VSA y el dispositivo seleccionado.

Mensajes

En la pestaña **Mensajes**, se muestra un historial de los mensajes enviados al dispositivo y de este.

- **Dirección**
  -  Enviado desde el dispositivo.
  -  Enviado desde el administrador del VSA.
- **Fecha**: la fecha y la hora del mensaje.
- **De**: *se aplica solo a los mensajes del dispositivo.* El identificador del dispositivo y el grupo de máquinas.
- **Mensaje**: texto del mensaje.

Ubicación

En la pestaña **Ubicación**, se muestran los datos de seguimiento de ubicación de un dispositivo seleccionado. Cada marcador numerado en el mapa hace referencia a una lista de números en el lado derecho de este. La lista numerada permite identificar la fecha y la hora en que el dispositivo se encontró en esa ubicación. Los datos que se muestran se filtran por un intervalo de fechas y horas específico.

> **Nota:** Si no ve el marcador de ubicación para un dispositivo al que realiza un seguimiento, intente restablecer el filtro para que se muestre un intervalo de fechas anterior.

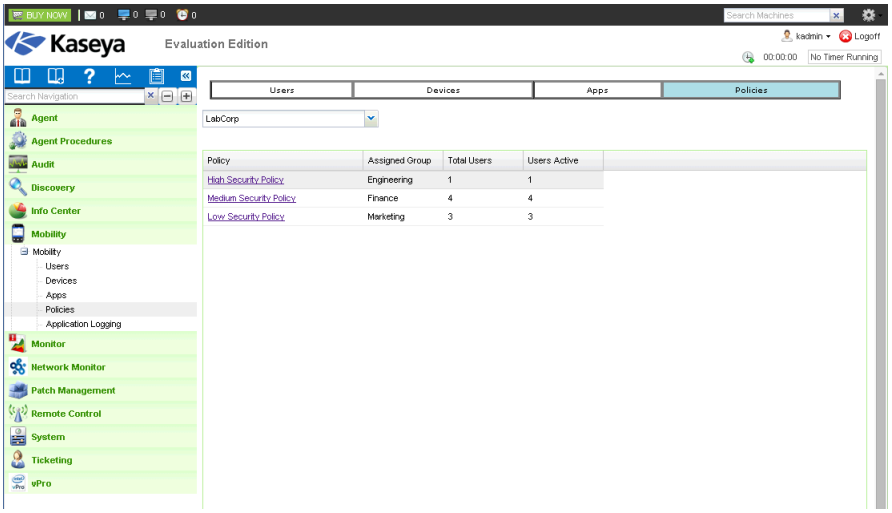
- **Fecha y hora**: puede optar por cambiar el filtro de fecha y hora. El filtro limita las ubicaciones de dispositivos que se muestran a un intervalo de fechas y horas.
- **Actualizar**: actualiza el mapa después de restablecer el filtro **Fecha y hora**.

Configurar políticas

En la página **políticas**, se asignan políticas de **Enterprise Mobility Management** por organización cliente y por grupo de seguridad de Active Directory.

Puede aumentar el detalle de cualquier política para lo siguiente:

- Revisar la configuración de las políticas predefinidas.
- Crear una nueva política y configurar ajustes personalizables para esa organización cliente.



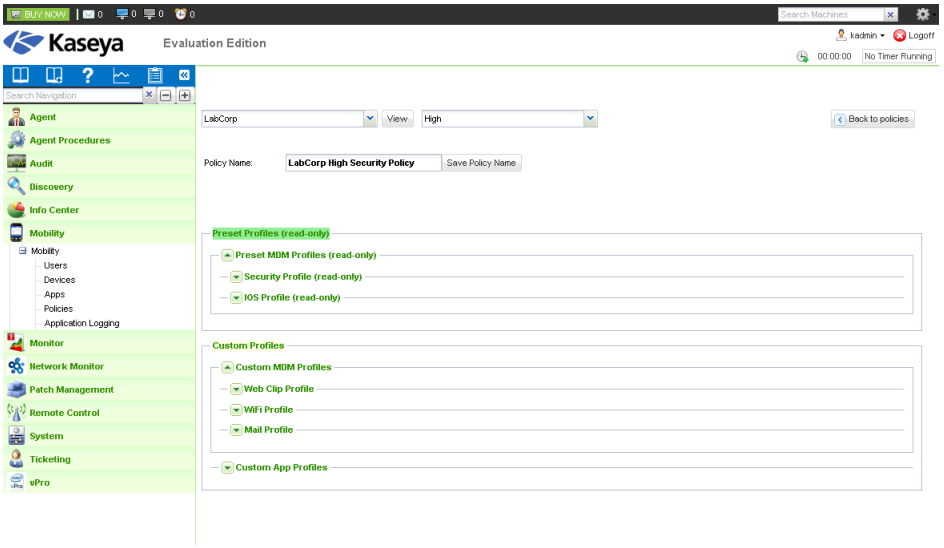
Creación y configuración de una nueva política

1. En la página **Políticas**, seleccione la organización cliente que desee ver.
2. Haga clic en el hipervínculo de cualquiera de las políticas de la lista.

   En la página de detalles, se muestran dos tipos de perfiles:

   - **Perfiles prestablecidos (solo lectura)**: Kaseya determinó la configuración correcta para estas propiedades. No es necesario ajustarlas. Cada tipo de política —`Alta`, `Media` y `Baja`— tiene una configuración de perfil prestablecida ligeramente distinta.

- **Perfiles personalizados**: esta configuración es específica del cliente. *Siempre cree una nueva política en lugar de configurar estas propiedades para las políticas predeterminadas* `Alta`, `Media` *y* `Baja`.



3. Introduzca un nuevo nombre en el campo **Nombre de política**. Por ejemplo, para la compañía `Acme`, puede introducir `Acme High Security Policy`.
4. Confirme que se seleccionó el *tipo de política* correcto: `Alta`, `Media` o `Baja` de la lista desplegable. Si es necesario, cambie por el tipo de política correcto.
5. Haga clic en el botón **Guardar nombre de política**.

   Ya creó una nueva política y la asignó a la organización cliente seleccionada.
6. Expanda **Perfiles MDM personalizados** para agregar detalles de configuración a cualquiera de los siguientes perfiles:
   - **Perfil de clip de la Web** *(página 18)*
   - **Perfil WiFi** *(página 19)*
   - **Perfil de correo electrónico** *(página 19)*
7. Expanda **Perfiles de aplicaciones personalizados** para agregar una o más aplicaciones al perfil de aplicaciones personalizado de esta organización cliente. Esta característica se describe en detalle en los siguientes temas:
   - **Administración de aplicaciones en los dispositivos** *(página 25)*
   - **Configuración del catálogo de aplicaciones** *(página 26)*
   - **Configuración de perfiles de aplicaciones en una política** *(página 22)*
8. Expanda **Perfiles BYOD personalizados** para agregar detalles de configuración y acceder de forma segura a los sitios web y los documentos internos de una organización cliente.
   - **Perfil de URL** *(página 21)*
   - **Perfil de documento** *(página 21)*
   - **Perfil de lista de proxy** *(página 21)*

Políticas MDM personalizadas

Configuración de un perfil de clip web

- Este tipo de perfil no es compatible con dispositivos iOS. En los dispositivos iOS, la URL debe comenzar con HTTP o HTTPS.

- Este perfil no se admite en Android.

El **perfil de clip web** especifica un "acceso directo" de una aplicación web a una URL a la que puede acceder el dispositivo. Es posible que una organización desee instalar en los dispositivos accesos directos dirigidos a sus páginas web o documentos de referencia.

- **Nombre**: el nombre del perfil.
- **Descripción**: la descripción del perfil.
- **URL**: la URL del acceso directo a la aplicación web.
- **Etiqueta**: un nombre descriptivo para el acceso directo a la aplicación web.
- **Ícono**: carga un archivo png para usarlo como el ícono del acceso directo.
- **Puede quitarse**: si está seleccionada, el usuario puede quitar el acceso directo a la aplicación web.

Configuración de un perfil de WiFi

- Este tipo de perfil es compatible con dispositivos iOS y Android.

En el **Perfil de WiFi**, se establecen las opciones de WiFi en los dispositivos.

- **Tipo de perfil**: el tipo de perfil.
- **Nombre**: el nombre del perfil.
- **Descripción**: una descripción del perfil.
- **SSID**: un identificador único de una red inalámbrica.
- **Red oculta**: si está seleccionada, la red inalámbrica no difunde su SSID.
- **Tipo de cifrado**: el tipo de cifrado que usa el dispositivo inalámbrico. Asegúrese de que estos valores coincidan exactamente con las capacidades del punto de acceso a la red. Si no está seguro del tipo de cifrado o prefiere que se aplique a todos los tipos de cifrado, use el valor `Any`.
  - `WEP`: privacidad equivalente por cable.
  - `WPA`: acceso protegido por WiFi. Incluye WPA y WPA2.
  - `Cualquiera`: cualquier otro tipo de protocolo de WiFi.
- **Contraseña**: la contraseña de WiFi.

Configuración de un perfil de correo electrónico

- Este tipo de perfil no es compatible con dispositivos iOS.
- Si los campos Nombre para mostrar del usuario, Dirección de correo electrónico, Nombre de usuario o Contraseña están en blanco, se completan con el registro del dispositivo.
- Este tipo de perfil es parcialmente compatible con dispositivos Android.

En el **perfil de correo electrónico**, se configura el cliente de correo electrónico en un dispositivo móvil administrado.

- **Nombre**: el nombre del perfil.
- **Descripción**: una descripción del perfil.
- **Tipo de cuenta**: `IMAP`, `POP`, `Gmail` o `Exchange`. La opción `Gmail` es una configuración IMAP predefinida para una cuenta de Gmail. Sólo se deben rellenar los campos de nombre de usuario y contraseña para completar la configuración IMAP de `Gmail`. Consulte **Configuración de un perfil de correo electrónico de Exchange** a continuación.
- **Nombre para mostrar del usuario**: el nombre para mostrar de la cuenta de correo electrónico.

  Nota: En iOS, si los campos **Nombre para mostrar del usuario** y **Dirección de correo electrónico** se dejan en blanco, se pide al usuario que introduzca su nombre de usuario y su dirección de correo electrónico cuando se aplica el perfil al dispositivo.

- **Dirección de correo electrónico**: la dirección de correo electrónico del usuario.

- **IP o nombre de host del servidor de entrada**: el servidor de correo electrónico entrante IMAP o POP3. Por ejemplo, `pop.sucorreoelectronico.com` o `imap.suservidordecorreoelectronico.com`.
- **Puerto del servidor de entrada**: el número de puerto que usa el servicio de correo electrónico entrante. En el caso de POP3, suele ser `110` o, si SSL está habilitado, `995`. Si está habilitado IMAP, suele ser `143` o, si SSL está habilitado, `993`.
- **El servidor de entrada requiere contraseña**: si está seleccionada, el servidor de correo electrónico entrante requiere una contraseña.
  - **Contraseña del servidor de entrada**: introduzca la contraseña.
- **Usar SSL para correo electrónico entrante**: si aparece `Sí`, la comunicación con el servidor de correo electrónico entrante se cifra mediante SSL. Para usar esta característica, su servidor de correo electrónico entrante debe ser compatible con SSL.
- **Dejar mensajes en el servidor**: si aparece `Sí`, el correo electrónico permanece almacenado en el servidor de correo electrónico entrante después de que se entrega al dispositivo.
- **IP o nombre de host del servidor de salida**: el servidor de correo electrónico saliente SMTP. Por ejemplo, `smtp.suservidordecorreoelectronico.com`.
- **Puerto del servidor de salida**: el número de puerto que usa el servidor de correo electrónico de salida. Suele ser `25` o, si SSL está habilitado, `465`.
- **Nombre de usuario del servidor de salida**: si está activada la autenticación de salida, es el nombre de usuario del correo electrónico de salida.
- **Usar la misma contraseña que el servidor de entrada**: si está seleccionada, tanto el servidor de entrada como el de salida usan la misma contraseña de entrada. Si no está seleccionada, especifique una contraseña.
  - **Contraseña del servidor de salida**: introduzca una contraseña.
- **Usar SSL para correo electrónico saliente**: si aparece `Sí`, la comunicación con el servidor de correo electrónico saliente se cifra mediante SSL. Para usar esta característica, su servidor de correo electrónico saliente debe ser compatible con SSL.

Configuración de un perfil de correo electrónico de Exchange

Establezca lo siguiente para configurar un perfil de correo electrónico de Exchange en **Enterprise Mobility Management**:

- **Tipo de cuenta**: seleccione `Exchange`.
- **Dirección de correo electrónico**: introduzca una dirección de correo electrónico.
- **IP o nombre de host del servidor de entrada**: introduzca el nombre de host del servidor Exchange.
- **Nombre de usuario del servidor de entrada**: introduzca un nombre de usuario de dominio con el formato `dominio\nombredeusuario`.
- **El servidor de entrada requiere contraseña**: active esta casilla de verificación.
- **Contraseña**: introduzca la contraseña para el nombre de usuario de dominio.
- **Puerto del servidor de entrada**: tiene como valor predeterminado `143`.
- **Puerto del servidor de salida**: tiene como valor predeterminado `25`.
- **Usar SSL para el correo electrónico entrante**: está activada de manera predeterminada.
- **Usar la misma contraseña que la entrante**: active esta casilla de verificación.

Nota: *Solo para dispositivos iOS*, debe crear perfiles independientes en **Enterprise Mobility Management** para cada perfil de correo electrónico de iOS y especificar el nombre de usuario, la dirección de correo electrónico y la contraseña.

Perfiles BYOD personalizados

Puede configurar tres perfiles BYOD personalizados para una organización cliente seleccionada y un grupo de seguridad de Active Directory. Expanda cualquiera de los **perfiles MDM personalizados** para agregar detalles de configuración a los siguientes perfiles:

- **Perfil de URL**
- **Perfil de documento**
- **Perfil de lista de proxy**

Lista blanca del VSA

Si el VSA no comparte la misma intranet que un servidor WebDAV, dicho servidor debe estar disponible en una dirección IP pública. Por motivos de seguridad, esta dirección IP solo sebe ser accesible desde la dirección IP del VSA. Los dispositivos móviles retransmiten sus solicitudes a través del VSA para llegar a estos servidores WebDAV. Las organizaciones cliente deben *incluir la dirección IP del VSA en una lista blanca* para los servidores que hospedan servidores WebDAV.

Perfil de URL

Agregue las URL *directamente accesibles* a la conexión de red de un dispositivo. Para acceder a estas URL, los usuarios usan **WorkBrowser** *(página 27)*.

- **Nombre**: introduzca el nombre de este elemento de menú.
- **URL**: introduzca una URL.
- **Proxy requerido**: si está seleccionada, el acceso a un vínculo en una página web con un `http://<subdominio>.<dominio>` diferente requiere que se incluya en el **Perfil de lista de proxy**. De lo contrario, se niega el acceso al usuario. Ejemplo: Si **Proxy requerido** está seleccionada, un vínculo a `sales.acme.com` de una página web de `support.acme.com` significa que `support.acme.com` o `*.acme.com` se debe agregar al **Perfil de lista de proxy**.

  Si no está seleccionada, se permite el acceso a un vínculo en una página web con un `http://<subdominio>.<dominio>` diferente, lo que puede representar un riesgo de seguridad.

Perfil de documento

Agregue los documentos WebDAV que desee que estén disponibles para los usuarios móviles con **WorkDocs** *(página 27)*.

- **Nombre**: una descripción del documento.
- **URL**: la URL del origen del documento WebDAV.
- **Proxy requerido**: si está seleccionada, el acceso a un vínculo en un documento con un `http://<subdominio>.<dominio>` diferente requiere que se incluya en el **Perfil de lista de proxy**. De lo contrario, se niega el acceso al usuario. Ejemplo: Si **Proxy requerido** está seleccionada, un vínculo a `sales.acme.com` de un documento de `support.acme.com` significa que `support.acme.com` o `*.acme.com` se debe agregar al **Perfil de lista de proxy**.

  Si no está seleccionada, se permite el acceso a un vínculo en un documento con un `http://<subdominio>.<dominio>` diferente, lo que puede representar un riesgo de seguridad.

La aplicación contenedora **WorkDocs** admite lo siguiente:

- La visualización y la edición de documentos PDF y de Microsoft Office compartidos y locales
- La creación y el almacenamiento de documentos locales protegidos en el dispositivo móvil del usuario. Los documentos almacenados de forma local se cifran y permanecen aislados del resto del entorno del dispositivo móvil del usuario.

Perfil de lista de proxy

Se aplica si un `http://<subdominio>.<dominio>` agregado al **perfil de URL** anterior tiene la casilla de verificación **Proxy requerido** activada. Especifica otro `http://<subdominio>.<dominios>` al que el usuario puede acceder cuando hace clic en un vínculo incorporado a las páginas de cualquier

`http://<subdominio>.<dominio>` de **Perfil de URL** o documento de **Perfil de documento**. Acepta la especificación *.*. Ejemplo: `*.acme.com` incluye `sales.acme.com`, `support.acme.com`, `it.acme.com`.

Políticas de aplicaciones personalizadas

Se pueden asignar perfiles de aplicaciones personalizados a una política. Un perfil de aplicaciones personalizado determina las aplicaciones requeridas o no permitidas en los dispositivos administrados de una organización cliente.

Antes de realizar este paso, se deben completar los pasos que se indican a continuación:

- **Administración de aplicaciones en los dispositivos** *(página 25)*
- **Configuración del catálogo de aplicaciones** *(página 26)*

Configuración de un perfil de aplicaciones en una política

1. En la página **Políticas**, seleccione la organización cliente que desee ver.
2. Haga clic en el hipervínculo de cualquiera de las políticas de la lista.
3. Expanda los **perfiles de aplicaciones personalizados** para agregar una o más aplicaciones al perfil de aplicaciones personalizado de esta organización cliente.
4. Haga clic en el botón **Agregar**.
5. Seleccione una o más aplicaciones para agregar al perfil de aplicaciones personalizado.
6. Haga clic en el botón **Agregar aplicaciones**.
7. Establezca el **estado** de la aplicación en `No permitida` o `Requerida`.
   - Si hay una aplicación `no permitida`, **Enterprise Mobility Management** no la desinstala automáticamente. Se le solicita al usuario que realice la desinstalación de forma manual.
   - Si hay una aplicación `requerida` y esta es una *aplicación de tienda*, **Enterprise Mobility Management** envía una invitación a los usuarios del dispositivo con un vínculo para instalarla. Si hay una aplicación `requerida` y esta es una *aplicación empresarial*, la aplicación se inserta automáticamente en el dispositivo.
8. Opcionalmente elimine una aplicación seleccionada del perfil de aplicaciones personalizado con la opción **Eliminar fila**.
9. Haga clic en **Guardar** para completar la configuración.

Políticas prestablecidas (solo lectura)

Kaseya determina la configuración correcta de las propiedades prestablecidas. No es necesario ajustarlas. Cada tipo de política —Alta, Media y Baja— tiene una configuración de perfil prestablecida ligeramente distinta.

Perfiles MDM prestablecidos (solo lectura)

Perfil de seguridad (solo lectura)

En el **Perfil de seguridad**, se configuran las políticas relacionadas con la creación de PIN (códigos de acceso) de *nivel de dispositivo*. Los usuarios usan los PIN para desbloquear los dispositivos móviles.

> **Nota:** Android solo es compatible con la siguiente configuración: permitir simple, forzar pin, longitud mínima, requerir alfanumérico, inactividad máxima y cantidad máxima de intentos incorrectos.

- **Permitir simple**: si está seleccionada, permite que los usuarios usen caracteres secuenciales o repetidos en los PIN (códigos de acceso). Por ejemplo, esto permite los códigos de acceso `3333` o `DEFG`.
- **Forzar PIN**: si está seleccionada, el usuario debe proporcionar un PIN (código de acceso) para acceder a todo el dispositivo móvil. Si no está seleccionada, no se requiere ningún PIN.

> Nota: **Perfiles BYOD prestablecidos** *(página 24)* también puede aplicar un PIN de *nivel de aplicación*. Ambos PIN son independientes entre sí.

- **Cantidad máxima de intentos incorrectos**: determina la cantidad de intentos de PIN incorrectos que se pueden hacer antes de que se eliminen los datos del dispositivo. El comportamiento predeterminado depende del fabricante del dispositivo.
- **Inactividad máxima**: la cantidad de segundos que se debe esperar antes de bloquear el dispositivo mientras el usuario no lo usa.
- **Tiempo de uso máximo del PIN en días**: la cantidad máxima de días que se puede usar el mismo PIN.
- **Cantidad mínima de caracteres complejos**: la cantidad mínima de caracteres complejos que se requieren en un PIN.
- **Longitud mínima**: la longitud mínima requerida para un PIN.
- **Solicitar alfanumérico**: si está seleccionada, solicita caracteres alfabéticos y numéricos.
- **Historial de PIN**: si está seleccionada, mantiene un historial de PIN.
- **Máximo período de gracia**: especifica cuán pronto se puede volver a desbloquear el dispositivo después de su uso, sin volver a solicitar el PIN.

Perfil de iOS (solo lectura)

- **Tipo de perfil**: el tipo de perfil.
- **Nombre**: el nombre del perfil.
- **Descripción**: una descripción del perfil.
- **Permitir la instalación de aplicaciones**: si está seleccionada, se pueden instalar aplicaciones.
- **Permitir cámara**: si está seleccionada, se habilita la cámara en el dispositivo.
- **Máximo de intentos incorrectos**: si el usuario supera la cantidad de intentos de código de acceso permitidos (en general 10), se bloquea el teléfono. La única forma de volver a usar el teléfono es restaurarlo a la configuración de fábrica, lo que elimina todos los datos del teléfono en el proceso. Después de restaurar el teléfono, se lo puede restaurar a la última copia de seguridad que se realizó.
- **Permitir captura de pantalla**: si está seleccionada, el dispositivo puede crear capturas de su propia pantalla.
- **Permitir YouTube**: si está seleccionada, se habilita YouTube™.
- **Permitir iTunes**: si está seleccionada, se habilita iTunes™.
- **Permitir Safari**: si está seleccionada, se habilita el explorador web Safari.
- **Permitir FaceTime**: si está seleccionada, los usuarios pueden realizar o recibir llamadas de video por FaceTime.
- **Permitir sincronización automática durante roaming**: si está seleccionada, los dispositivos se sincronizan durante el roaming. Si no está seleccionada, los dispositivos se sincronizan solo cuando el usuario accede a una cuenta.
- **Permitir Siri**: si está seleccionada, los usuarios pueden usar Siri, comandos de voz o dictado.
- **Permitir marcación por voz**: si está seleccionada, los usuarios pueden marcar el teléfono por medio de comandos de voz.
- **Permitir compra de aplicaciones**: si está seleccionada, los usuarios pueden realizar compras de aplicaciones.
- **Forzar al usuario a introducir la contraseña de iTunes Store para todas las compras**: si está seleccionada, se requiere a los usuarios que introduzcan su contraseña de ID de Apple antes de realizar

cualquier compra. Normalmente, hay un período de gracia breve después de que se realiza una compra antes de que los usuarios deban identificarse para realizar compras subsiguientes.

- **Permitir juego multijugador**: si está seleccionada, los usuarios pueden usar juegos para varios jugadores en Game Center.
- **Permitir agregar amigos en Game Center**: si está seleccionada, los usuarios pueden agregar amigos en Game Center.
- **Forzar advertencia de fraude**: si está seleccionada, Safari hace una advertencia a los usuarios cuando visitan sitios web identificados como fraudulentos o con pérdida de confidencialidad.
- **Habilitar JavaScript**: si está seleccionada, Safari ejecuta javascript en los sitios web.
- **Bloquear ventanas emergentes**: si está seleccionada, se habilita la característica de bloqueo de ventanas emergentes de Safari.
- **Aceptar cookies**: elija cuándo aceptar cookies entre `Nunca`, `De sitios visitados`, `Siempre`.
- **Permitir copia de seguridad**: si está seleccionada, los usuarios pueden hacer una copia de seguridad de su dispositivo en iCloud.
- **Permitir la sincronización de documentos**: si está seleccionada, los usuarios pueden almacenar documentos en iCloud.
- **Permitir fotos en streaming (deshabilitarla puede causar la pérdida de datos)**: si está seleccionada, los usuarios pueden habilitar la función de fotos en streaming.
- **Permitir que se envíen datos de diagnóstico a Apple**: si está seleccionada, se envía información de diagnóstico de iOS a Apple.
- **Permitir que el usuario acepte certificados TLS no confiables**: si está seleccionada, se le pregunta a los usuarios si desean confiar en certificados que no se pueden verificar. Este parámetro se aplica a Safari y a las cuentas de correo electrónico, contactos y calendario.
- **Forzar copias de seguridad cifradas**: si no está seleccionada, el usuario puede elegir cifrar o no una copia de seguridad del dispositivo a una máquina local en iTunes. Si está seleccionada, se fuerza al usuario a que cifre la copia de seguridad en iTunes. Cuando se cifra una copia de seguridad, un cuadro de mensaje en el dispositivo solicita al usuario que introduzca una contraseña cifrada.
- **Permitir música y podcasts explícitos**: si está seleccionada, se muestra el contenido musical o de video explícito en iTunes Store en lugar de ocultarlo. Cuando se muestra contenido explícito en iTunes Store, los proveedores del contenido le agregan una marca indicadora.

Políticas BYOD prestablecidas (solo lectura)

Perfil de acceso (solo lectura)

- **Los usuarios nuevos necesitan la aprobación del administrador antes de usar el dispositivo**: si se requiere la aprobación de un administrador, el usuario recibe el mensaje “Se requiere aprobación” la primera vez que intenta acceder a **Enterprise Mobility Management**.
- **El dispositivo del usuario se bloquea después de n intentos incorrectos**: cantidad de intentos.

Perfil de seguridad (solo lectura)

- **El acceso móvil requiere la introducción de un PIN**: si está seleccionada, requiere un PIN (código de acceso) de *nivel de aplicación* cada vez que inicia la aplicación. Si está seleccionada, se indica al usuario que cree un código de acceso la primera vez que intenta acceder a la aplicación.

  Nota: **Perfiles MDM prestablecidos** *(página 22)* también puede aplicar un PIN de *nivel de dispositivo*. Ambos PIN son independientes entre sí.

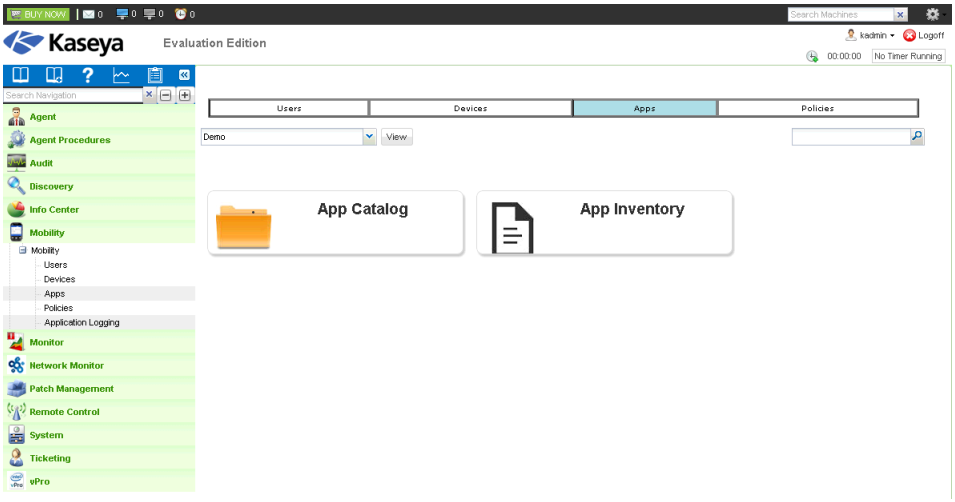
  - Solo si lo habilita el usuario
  - Cada vez que se activa la aplicación
  - Después de N minutos de inactividad
- **El acceso móvil requiere la introducción de una contraseña cada**: N minutos, horas o días.
- **Los usuarios pueden enviar contenido del elemento por correo electrónico a otros**: sí o no.

- **Los usuarios pueden abrir contenido del elemento con aplicaciones que no son del conjunto**: sí o no.
- **Los usuarios pueden guardar imágenes en la biblioteca de imágenes del dispositivo**: sí o no.
- **Los usuarios pueden imprimir contenido que no pertenece al conjunto**: sí o no.
- **Los usuarios pueden copiar y pegar en aplicaciones que no pertenecen al conjunto**: sí o no. Si no se permite, se muestra un mensaje de `paste blocked by policy` cuando un usuario intenta copiar de una aplicación contenedora protegida a una aplicación externa. La copia de una aplicación externa a una aplicación contenedora protegida nunca está bloqueada.

Administración de aplicaciones en los dispositivos

Enterprise Mobility Management puede requerir o no permitir aplicaciones en dispositivos móviles. Esto incluye las aplicaciones que se descargan de tiendas de aplicaciones, así como de *aplicaciones empresariales* exclusivas.

1. Navegue a la página **Aplicaciones**.
2. Seleccione una organización cliente.



3. Puede seleccionar una de dos opciones:
   - En la página **Catálogo de aplicaciones** *(página 26)*, se mantiene un catálogo de *elementos de aplicaciones*. Un elemento de aplicación es un registro que identifica de manera exclusiva a una única aplicación que puede ser necesaria o no estar permitida en un dispositivo móvil.

     Nota: Antes de poder incluir una aplicación en el perfil de aplicaciones de una organización cliente específica, se la debe agregar al **catálogo de aplicaciones**.

   - En la página **Inventario de aplicaciones**, se genera una lista de elementos de aplicaciones posibles sobre la base de una auditoría de todos los dispositivos móviles que administra **Enterprise Mobility Management**. Úsela para determinar el formato de los registros de aplicaciones que desee agregar al **catálogo de aplicaciones**.
4. Para esta versión beta, haga clic en **Catálogo de aplicaciones**. Para completar la configuración de las aplicaciones en los dispositivos administrados, se deben seguir dos pasos:
   - **Configurar el catálogo de aplicaciones** *(página 26)*.
   - **Configurar perfiles de aplicaciones en una política** *(página 22)*.

Configuración del catálogo de aplicaciones

En **Catálogo de aplicaciones**, se mantiene un catálogo de elementos de aplicaciones. Cada elemento de aplicación identifica de manera exclusiva a una única aplicación que puede ser necesaria o no estar permitida en un dispositivo móvil. Una vez agregados al catálogo, los elementos de aplicaciones se pueden agregar al **perfil de aplicaciones** *(página 22)* de una política asignada a una organización cliente.

Nota: Para cada organización cliente, se mantiene un **catálogo de aplicaciones** de forma individual.

Cómo agregar un nuevo elemento de aplicación

1. Si es necesario, seleccione la organización cliente correcta.
2. Haga clic en **Nuevo**. El *tipo de aplicación* que seleccione especifica si la aplicación se instala desde una tienda de aplicaciones o si se descarga del VSA como una aplicación empresarial.
   - **Aplicación de tienda**: si está seleccionada, se debe especificar una **URL**.
   - **Aplicación empresarial**: si está seleccionada, se debe cargar un **binario de aplicación**.
3. Si selecciona una **aplicación de tienda**, aparece un cuadro de diálogo **Nueva aplicación de tienda**.
   - Seleccione el botón de opción **Android** o **iOS**.
   - Opcionalmente introduzca un término de búsqueda para filtrar la lista de aplicaciones que devuelve la tienda seleccionada.
   - Seleccione una aplicación de la lista.
   - Haga clic en el botón **Agregar** o **Agregar y crear nueva**.

   Se agregó la aplicación al **catálogo de aplicaciones**.
4. Si selecciona una **aplicación empresarial**, aparece un cuadro de diálogo **Nueva aplicación empresarial**.
   - Seleccione el botón de opción **Android** o **iOS**.
   - Introduzca el **nombre** para la aplicación en el **catálogo de aplicaciones**.
   - Busque el **paquete** que desea seleccionar para cargarlo al VSA. El **paquete** es un archivo `.apk` de Android o un archivo `.ipa` de iOS.
   - Haga clic en el botón **Agregar** o **Agregar y crear nueva**.

   Se agregó la aplicación al **catálogo de aplicaciones**.

Trabajo con elementos de aplicaciones existentes

El menú **Acciones** proporciona las siguientes opciones para las aplicaciones existentes del **catálogo de aplicaciones**.

- **Editar**: edita un elemento de aplicación seleccionado en el **Catálogo de aplicaciones**.
- **Eliminar**: elimina un elemento de aplicación seleccionado del **Catálogo de aplicaciones**.
- **Invitar**: permite enviar un mensaje para invitar a uno o más usuarios a que instalen las aplicaciones seleccionadas en sus dispositivos móviles.

Vista del inventario de aplicaciones

Enterprise Mobility Management > Aplicaciones > Inventario de aplicaciones

En la página **Inventario de aplicaciones**, se genera una lista de elementos de aplicaciones sobre la base de las aplicaciones detectadas en los dispositivos móviles administrados para la organización cliente y el perfil de políticas que se seleccionan. Úsela para determinar el formato de los registros de aplicaciones que desee agregar al **catálogo de aplicaciones** *(página 26)*.

Columnas de tabla

- **SO**: `Android` o `iOS`.
- **Nombre del paquete**: nombre completo de la aplicación en formato de dominio inverso. Ejemplo: `com.kaseya.enterprise.agent`.
- **Nombre de la aplicación**: el nombre descriptivo de la aplicación. Ejemplo: `Agent`.
- **Versión**: el número de versión de la aplicación. Ejemplo: `1.2.0.0`.

WorkBrowser y WorkDocs

Enterprise Mobility Management proporciona a los usuarios de los dispositivos móviles acceso seguro a los sitios web y los documentos internos de la compañía mediante dos aplicaciones contenedoras.

- **WorkBrowser** *(página 27)*: proporciona acceso seguro a los sitios web internos.
- **WorkDocs** *(página 27)*: permite ver y editar de forma segura los documentos de las redes internas o almacenados localmente en los dispositivos móviles.

Uso de WorkBrowser

WorkBrowser es ideal para todo aquel que trabaja fuera de la oficina y necesita permanecer conectado a esta. **WorkBrowser** proporciona acceso seguro —en modo activo e inactivo— a las intranets, los archivos y los directorios internos. Mediante **WorkDocs** *(página 27)*, se pueden editar los archivos seleccionados.

Descarga de WorkBrowser

- Dispositivos Apple: descargar mediante el vínculo proporcionado en la invitación de correo electrónico.
- **Dispositivos Android:** *(https://play.google.com/store/apps/details?id=com.kaseya.byodsuite.workbrowser)* descargar mediante el vínculo proporcionado en la invitación de correo electrónico.

Requisitos para todos los dispositivos móviles administrados

- iOS versión 7.0 y superiores
- Android versión 4.0.3 y superiores

Códigos de acceso

Es posible que deba crear un código de acceso (PIN) *de la aplicación* para usar **WorkBrowser**. En adelante, debe introducir este PIN cada vez que acceda a la aplicación **WorkBrowser**.

Sitios

En la lista **Sitios**, se indican todos los sitios web a los que puede acceder mediante **Enterprise Mobility Management**.

Vista y edición de archivos

Al examinar sitios web en **WorkBrowser**, puede ver archivos. Mediante **WorkDocs** *(página 27)*, se pueden editar los archivos que se ven.

Uso de WorkDocs

WorkDocs le permite ver o editar los documentos almacenados en una red interna o localmente en la

sección **Almacenamiento seguro** de su dispositivo móvil. Además, puede mover, copiar o eliminar documentos. Los documentos almacenados de forma local se cifran y permanecen aislados del resto del entorno del dispositivo móvil.

Descarga de WorkDocs

- Dispositivos Apple: descargar mediante el vínculo proporcionado en la invitación de correo electrónico.
- **Dispositivos Android: https://play.google.com/store/apps/details?id=com.kaseya.byodsuite.workdocs** descargar mediante el vínculo proporcionado en la invitación de correo electrónico.

Requisitos para todos los dispositivos móviles administrados

- iOS versión 7.0 y superiores
- Android versión 4.0.3 y superiores

Códigos de acceso

Es posible que deba crear un código de acceso *(PIN) de la aplicación* para usar **WorkDocs**. En adelante, debe introducir este PIN cada vez que acceda a la aplicación **WorkDocs**.

Sitios

En la lista **Sitios**, se indican todos los sitios de **WorkDocs** a los que puede acceder mediante **Enterprise Mobility Management**. En cada sitio de **WorkDocs**, se proporciona acceso a un árbol de navegación de carpetas y documentos. *Estos documentos no se almacenan en el dispositivo, a menos que estén en* **Almacenamiento seguro**.

Almacenamiento seguro

En el sitio **WorkDocs**, también se muestra una carpeta de **Almacenamiento seguro** con los documentos locales almacenados en el dispositivo. Esta misma carpeta **Almacenamiento seguro** se comparte en todos los sitios de **WorkDocs** a los que tiene acceso.

Autorización

Según la autorización asignada al documento, es posible que deba introducir credenciales.

Edición de documentos

La selección de un archivo le permite obtener una vista previa del archivo. Seleccione el botón **Editar** en la vista previa del archivo para iniciar el editor de archivos.

Cuando se carga el editor, puede seleccionar el ícono de **Archivo** y usar la opción **Guardar como** para guardar el archivo actual con un nuevo nombre o en otra ubicación. Una vez que comienza a editar el archivo, se puede usar el ícono de **Archivo** para guardar el archivo actual con el mismo nombre y en la misma ubicación del archivo original. Si no se puede guardar, verifique que tenga acceso de escritura a la ubicación del documento.

Mover, copiar y eliminar archivos

Puede mover, copiar y eliminar archivos desde cualquier ubicación.

- Seleccione **Editar** en la parte superior de la lista de archivos de origen del documento para ver estas opciones.
- Seleccione los archivos que desee mover, copiar o eliminar.
- Para **Copiar** y **Mover**, debe proporcionar el nombre y la ubicación del nuevo archivo. Para guardar una copia local del archivo, cópiela o muévala a **Almacenamiento seguro**.
- Para eliminar un archivo, seleccione el botón **Eliminar**. Debe confirmar que desea eliminar los archivos.

Favoritos

Toda carpeta que esté debajo del directorio raíz se puede guardar como **Favorita**. Para marcar una carpeta como **Favorita**, seleccione el ícono de estrella de la parte inferior de la lista de archivos. El ícono de estrella se oscurece para indicar que esta carpeta ahora forma parte de **favoritos**.

Las carpetas marcadas como **Favoritas** se muestran junto con los orígenes de documentos. La selección de **Favorita** proporciona un acceso directo para ir directamente a esa ubicación.

Registro de la actividad de módulo

Puede revisar la actividad de las aplicaciones en el módulo **Mobility** en la página **Registros de aplicaciones**. Si se modificó o se quitó información de manera inesperada, revise esta página para determinar cuáles son los eventos y los administradores que pueden estar involucrados.

Las entradas incluyen lo siguiente:

- **ID de Evento**
- **Nombre de evento**
- **Mensaje**
- **Admin**
- **Fecha de evento**

Los eventos registrados incluyen lo siguiente:

Borrar código de acceso
Dispositivo creado
Dispositivo eliminado
Dispositivo encontrado
Invitación reenviada
Bloquear dispositivo
Dispositivo perdido
Marcar comandos como completados
Procesar alerta
Solicitar registro
Solicitar registros
Ejecutar auditoría
Auditoría programada
Hacer sonar alarma en el dispositivo
Iniciar seguimiento de dispositivo
Detener seguimiento de dispositivo
Dispositivo actualizado
Eliminar datos del dispositivo

Índice