AppTec360 Enterprise Mobile Manager y ContentBox

Manual de administración | Versión 5.0 (202110)

Índice

- Restricciones y ajustes
  - Aplicaciones en la lista negra y en la lista blanca
  - Restricciones de SysApp
  - App-VPN
  - Configuración de la aplicación
- App Store para empresas
  - Aplicaciones iTunes
  - En la empresa
- Modo quiosco
  - Tipo de aplicación
    - Paquete
    - URL
  - Configuración del modo quiosco

Android Enterprise – Configuración de dispositivos totalmente gestionada

General

- Resumen del perfil del grupo (sólo a nivel de grupo)
- Visión general del dispositivo (sólo a nivel de dispositivo)
- Config Revision (sólo a nivel de dispositivo)
- Registro de dispositivos (sólo a nivel de dispositivo)
  - Registro de comandos
  - Posibles estados del comando
- Ajustes del dispositivo
  - Configuración de clientes
  - Papel pintado

Gestión de activos (sólo a nivel de dispositivo)

- Información del dispositivo
  - Wi-Fi
- Móvil
- Bluetooth

Gestión de la seguridad

- Antirrobo (sólo en el dispositivo)
  - Información GPS (sólo a nivel de dispositivo)
  - Limpiar y bloquear (sólo a nivel de dispositivo)

- Mensaje (sólo a nivel de dispositivo)
- Configuración de seguridad
  - Código del dispositivo
  - Antivirus
- Fin de vida útil (sólo a nivel de dispositivo)
  - Limpiar (sólo a nivel de dispositivo)
- Configuración de restricciones
  - Restricciones
- Gestión de certificados

Gestión de conexiones

- Wifi
  - Tipo de seguridad
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
  - Tipo de VPN
    - VPN
    - VPN por aplicación
- Restricciones

Gestión PIM

- Intercambio de Gmail

Gestión de aplicaciones

- Enterprise App Manager
  - Aplicaciones instaladas (sólo en el dispositivo)
  - Aplicaciones del sistema (sólo a nivel de dispositivo)
  - Aplicaciones obligatorias
  - Listas negras y blancas
  - Aplicaciones del sistema AE
- Restricciones y ajustes
  - Configuración de App Management
- App Store para empresas
  - En la empresa
- Play Store para empresas
  - AE Play Store

- Limpiar y bloquear (sólo a nivel de dispositivo)
- Mensaje (sólo a nivel de dispositivo)
- Configuración de seguridad
  - Código
  - Cifrado
  - Antivirus
- Fin de vida útil (sólo a nivel de dispositivo)
  - Limpiar (sólo a nivel de dispositivo)
- Configuración de restricciones
  - Restricciones
  - Propietario del dispositivo AE

Contenedor BYOD

- Android para empresas
  - Android para empresas
  - Intercambio de Gmail
  - Aplicaciones del sistema AE
  - Código de acceso al contenedor
- Samsung KNOX
  - Activación
  - Código Knox
  - Seguridad Knox
  - Bolsa de Knox
  - Knox eMail
  - Aplicaciones Knox

Gestión de conexiones

- Wifi
  - Tipo de seguridad
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- VPN
- Restricciones
- APN
- Bluetooth

Gestión PIM

- Config Revision (sólo a nivel de dispositivo)
- Registro de dispositivos (sólo a nivel de dispositivo)
  - Registro de comandos
  - Posibles estados del comando
- Gestión de activos (sólo a nivel de dispositivo)
  - Información del dispositivo
  - Móvil
  - Información de sincronización
- Gestión de la seguridad
  - Antirrobo (sólo en el dispositivo)
    - Información GPS (sólo a nivel de dispositivo)
    - Ajustes GPS
  - Configuración de seguridad
    - Código
    - Antivirus
    - Centro de seguridad
    - Configuración del cortafuegos
    - Reglas del cortafuegos
  - Configuración de restricciones
    - Funcionalidad del dispositivo
  - BitLocker
    - Configuración de BitLocker
    - Estado de BitLocker
  - Gestión de certificados
    - Lista de certificados
    - Configuración de certificados
    - SCEP
- Gestión de conexiones
  - Wifi
    - Tipo de seguridad
    - Utilizar servidor proxy
  - Restricciones wifi
  - VPN
    - Tipo de conexión
    - Configuraciones VPN genéricas
  - Restricciones VPN
  - Bluetooth

Panorama general

Introducción a AppTec360

La solución de gestión móvil para empresas de AppTec ofrece la posibilidad de gestionar y configurar todos los dispositivos móviles con su intuitiva consola de gestión. En este escenario, el servidor EMM puede ejecutarse en su propio entorno o puede utilizar nuestra solución basada en la nube.

Incluso en el tema de la instalación centralizada de aplicaciones corporativas en los smartphones, ha llegado al lugar adecuado. Con Enterprise Mobile Manager, puede distribuir aplicaciones y documentos corporativos a los dispositivos en cuestión de segundos o bloquear aplicaciones no deseadas con listas blancas o negras.

El uso de dispositivos privados en las empresas plantea un nuevo reto para la seguridad de smartphones y tabletas. Debido a que los empleados quieren utilizar cada vez más sus smartphones, los administradores de TI deben proteger un gran número de tipos diferentes de dispositivos. Le ayudaremos a proteger todos los dispositivos y los datos confidenciales que se almacenan en ellos y a gestionarlos desde una consola intuitiva.

Sistemas operativos compatibles

AppTec360 es compatible con dispositivos iOS, Android y Windows. Tenga en cuenta que la capacidad de las funciones de las plataformas mencionadas puede variar de un sistema operativo a otro.

- Apple iOS 11.0 o superior*.
- Apple macOS 10.11 o superior
- Google Android 4.4 o superior** en la versión en la nube
- Google Android 4.1 o superior** en la versión OnPrem
- MS Windows 10 o superior*** (ordenador de sobremesa, portátil y tableta)

**Tenga en cuenta que los dispositivos con iOS 10 o anterior no se pueden inscribir debido a los cambios drásticos realizados por Apple en el proceso de inscripción.*

***Los dispositivos pueden conectarse y configurarse aunque utilicen una versión que ya no sea compatible con el fabricante. Tenga en cuenta que puede haber funciones que requieran una determinada versión de Android. En los casos de asistencia, seguimos el soporte oficial del fabricante. En caso de problemas o errores causados por una versión obsoleta que ya no reciba asistencia del fabricante, nos reservamos el derecho de ofrecer sólo una asistencia limitada.*

****Las versiones domésticas de Windows no son compatibles debido a las limitaciones del sistema operativo. Recomendamos encarecidamente utilizar una versión del sistema operativo que siga siendo compatible con el fabricante. No sólo por compatibilidad, sino también por razones de seguridad. Por eso recomendamos iOS 12 o superior y Android 9 o superior.*

Directorios LDAP compatibles

- Microsoft Active Directory
- Abrir LDAP

Aquí encontrará información actualizada sobre "Sistemas operativos de dispositivos compatibles" y "Directorios LDAP compatibles":

https://www.apptec360.com/products/systemrequirements/

Explicación del «modo supervisado» en los dispositivos Apple

El modo supervisado representa una interfaz ampliada para dispositivos iOS.

En el dispositivo configurado respectivamente, se pueden aplicar limitaciones adicionales, ya que pertenecen a la funcionalidad del dispositivo del usuario final. Éstas también figuran en el manual de administración y están señaladas con una pancarta.

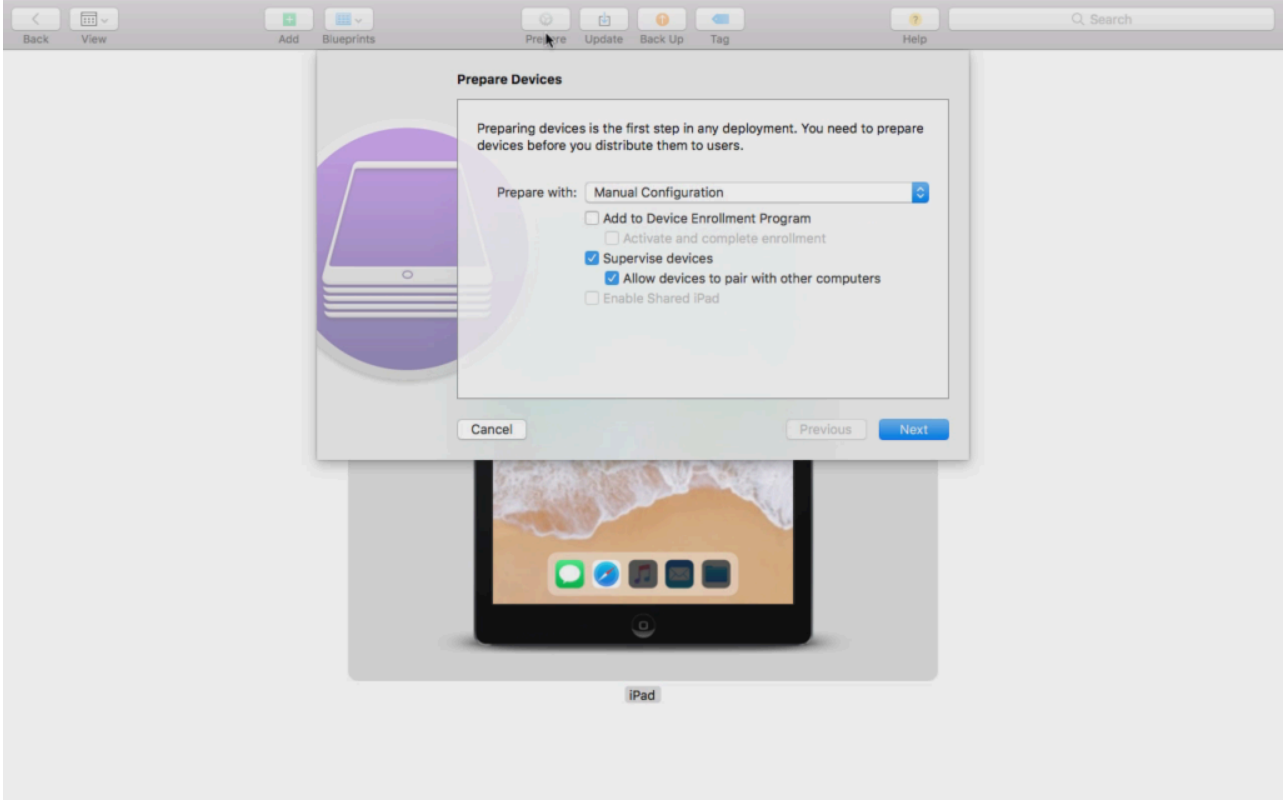
Disponible en el modo supervisado

El "Modo Supervisado" puede activarse con el programa "Apple Configurator". El Apple Configurator puede establecer los ajustes predeterminados en los nuevos dispositivos iOS como herramienta de configuración (a través de la interfaz USB).

La herramienta no sólo puede instalar perfiles de configuración, sino también aplicaciones. Es gratuito, pero requiere un ordenador Mac.

Activar el modo supervisado

1. Abra el Configurador de Apple



2. Haga clic en el dispositivo y seleccione "Preparar".
3. Seleccione "Configuración manual" y "Supervisar dispositivos".
4. Haga clic en "Siguiente".
5. (Opcional) Ahora puede añadir un servidor MDM en el que se inscribirá el dispositivo. El enlace se encuentra en "Ajustes generales - Configuración de iOS - Configurador y URL" Elija su organización o cree una nueva.
6. Elige tu Organización o crea una nueva
7. Elija los pasos que deben omitirse en la configuración inicial y haga clic en "Siguiente" (ATENCIÓN: ¡Si continúa, se borrará su dispositivo!)

Ahora tu dispositivo se pondrá en modo supervisado. Esto puede tardar unos minutos. Una vez hecho esto, el dispositivo se reiniciará.

Ahora tu dispositivo está supervisado.

Añadir un dispositivo al DEP

También puedes añadir dispositivos al DEP (Device Enrollment Programm) utilizando el Configurador de Apple, si tus dispositivos están en iOS 11 o superior.

Más información sobre DEP: https://www.apple.com/business/dep/

Siga los mismos pasos que para supervisar un dispositivo y, además, marque "Añadir al programa de inscripción de dispositivos". Se le pedirán sus datos de acceso al DEP si nunca antes ha iniciado sesión en el DEP con el Configurador de Apple.

Una vez finalizado el proceso, el dispositivo se puede encontrar en el DEP Server "Dispositivos añadidos por Apple Configurator 2". Ahora puede utilizar este servidor y conectarlo a la consola de gestión o transferir el dispositivo a un servidor ya existente.

Ha añadido correctamente un dispositivo al DEP.

Explicación de Android Enterprise

¿Qué es Android Enterprise?

Android Enterprise ofrece un mejor control de los dispositivos de trabajo que se gestionan con un MDM. Esto permite a los administradores tener un control total sobre sus dispositivos android o separar los datos de la empresa de los datos privados en los dispositivos contenedores. Además, Android Enterprise permite una inscripción más sencilla de los dispositivos y una distribución fácil de las aplicaciones.

¿Cuáles son los requisitos para utilizar Android Enterprise?.

Android Enterprise puede ser utilizado gratuitamente por todo el mundo. Solo necesitas conectar una cuenta de google al MDM para habilitar todas las funciones de Android Enterprise. Encontrará más información al respecto en la sección Android Enterprise.

Android Enterprise puede utilizarse en dispositivos con Android 5.1 o superior, a excepción del perfil de trabajo mejorado (véase más abajo). Recomendamos al menos Android 7 o superior para una inscripción más fácil o Android 11 para hacer uso de todas las funciones disponibles.

¿Cuáles son los modos disponibles con Android Enterprise?

Hay 3 modos diferentes para usar cuando se utiliza Android Enterprise.

Dispositivo totalmente gestionado AE (gestionado para el trabajo): Dispositivo totalmente gestionado que sólo se utiliza para trabajar. Esto permite al administrador un control total sobre el dispositivo. Esto no permite un uso privado del dispositivo. Para inscribir dispositivos en este modo, los dispositivos deben reiniciarse e inscribirse con un código QR (véase Inscripción AE) o inscribirse mediante Inscripción Knox o Zero Touch.

Contenedor AE BYOD: El Contenedor BYOD (traiga su propio dispositivo) permite a los usuarios acceder a los datos de la empresa en su teléfono particular en un contenedor independiente. En este modo, las aplicaciones privadas no pueden ver los datos y aplicaciones de la empresa y viceversa. Para inscribir dispositivos en este modo, hay que descargar la aplicación AppTec y escanear un código QR. Cree un dispositivo en la consola y seleccione "AE Container (BYOD & Enahnced Work Profile)" como tipo de dispositivo. Haga clic en el código QR del dispositivo recién generado para obtener el código QR y establezca el primer interruptor en "Legacy & BYOD".

AE Enhanced Work Profile: (requiere Android 11 o superior) Mientras que el mencionado BYOD Container lleva los datos de la empresa a un dispositivo privado, el Enhanced Work Profile hace lo mismo pero para un dispositivo propiedad de la empresa. Crea el mismo contenedor, pero da al administrador un poco más de control sobre el dispositivo, por lo que el usuario no puede

simplemente eliminar el MDM del dispositivo. Cree un dispositivo en la consola y seleccione "AE Container (BYOD & Enahnced Work Profile)" como tipo de dispositivo. Haga clic en el código QR del dispositivo recién generado para obtener el código QR y establezca el primer interruptor en "Perfil de trabajo mejorado". Este código QR se puede escanear después de reiniciar el dispositivo y tocar 6 veces en la pantalla como se explica en el Método 1 de la Inscripción AE.

¿Cómo puedo asignar aplicaciones a dispositivos Android Enterprise?

Primero tienes que aprobar las Apps que quieres usar en Ajustes Generales → Gestión de Apps → AE Play Store → Play Store Apps. Después de aprobar una app, puedes asignarlas a la lista de apps obligatorias → de tu perfil haciendo clic en el "+" y seleccionando la app en la pestaña "AE Play Store". Esto descargará e instalará la aplicación automáticamente. No se requiere una cuenta de google en el dispositivo y el usuario no tiene que confirmarlo ni permitirlo.

Sube tus propias aplicaciones a Google Play Store

Es posible subir tus Inhouse Apps a Google Play Store. De esta forma podrás beneficiarte de diferentes ventajas como el mecanismo de actualización de la Play Store.

Para ello, necesitas una cuenta de desarrollador de Google. Accede a través de Google Play Console(https://play.google.com/apps/publish)

Haga clic en "Crear aplicación". Elige el idioma por defecto y el título de la aplicación.

Create application

Default language *

English (United Kingdom) – en-GB ▾

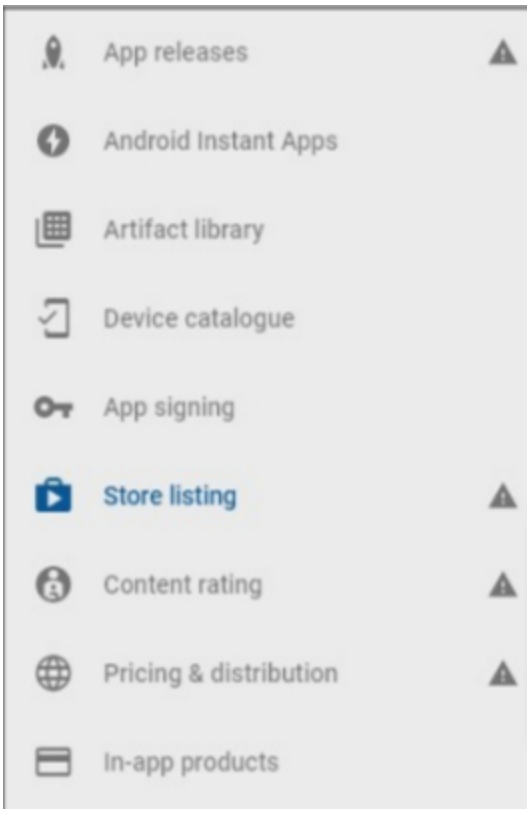
Title *

AppTec Demo App

15/50

CANCEL CREATE

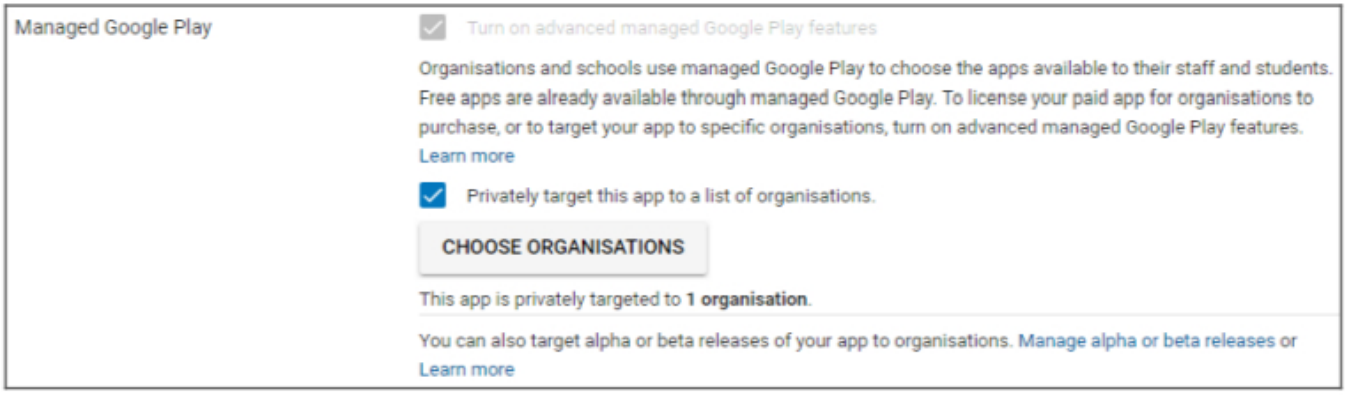
En la siguiente página se le pedirá que introduzca diferentes datos sobre su aplicación.



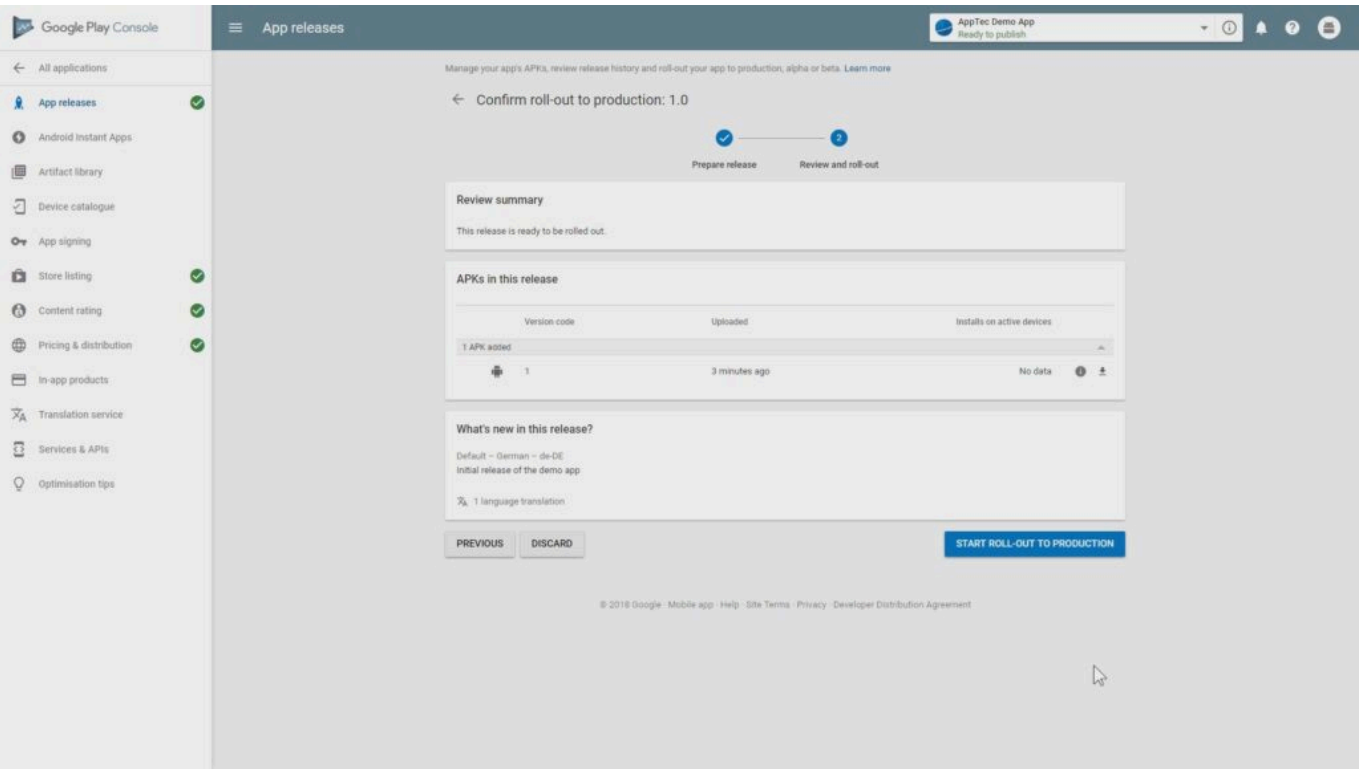
Una vez introducidos todos los datos, verás diferentes símbolos de sugerencia en el lado izquierdo.

Pasa el ratón por encima para ver los pasos que quedan y síguelos en el orden que quieras.

Nota: Asegúrate de marcar las dos casillas de verificación de "Google Play gestionado" en "Precios y distribución". De lo contrario, la aplicación será pública y todo el mundo podrá acceder a ella. Asegúrese también de elegir el país de distribución.



Una vez completados todos los pasos, puedes ir a "Lanzamientos de aplicaciones". Haz clic en "Revisar" e "Iniciar lanzamiento a producción" para finalizar el borrador y publicar la aplicación.



Puede que pase algún tiempo hasta que la aplicación esté disponible en Play Store. Una vez finalizado el proceso, puedes buscar tu aplicación en la tienda Play for Work y aprobarla. Después, sólo tienes que asignar la aplicación a los dispositivos mediante la consola EMM, igual que haces con otras aplicaciones.

Requisitos e instalación

Requisitos

Requisitos del sistema

El dispositivo virtual está disponible en formato de virtualización abierta (VMWare, VirtualBox, Citrix Xen Server) y como archivo comprimido .vhdx (Hyper-V)*.

*Nota: La máquina tiene que ser creada con la Generación 1 cuando se utiliza Hyper-V.

El disco virtual tiene un tamaño objetivo de 20 GB y la máquina necesita 4 GB de RAM.

El aparato está basado en Debian 9 64bit

Actualice la máquina importada a la compatibilidad más reciente (por ejemplo, en VMWare) y asegúrese de que el tipo de sistema operativo de la máquina está configurado correctamente en su hipervisor.

Clave de licencia

Para activar e instalar correctamente el servidor, necesitará un archivo de licencia válido. Puede obtener uno directamente de AppTec360 y/o de su distribuidor correspondiente.

Resolución de direcciones IP y DNS

El dispositivo AppTec360 debe ser accesible mediante el nombre de host para el que se ha emitido la licencia.

Para inscribir dispositivos Windows 10 también es necesario configurar un subdominio adicional en forma de "enterpriseenrollment.", que apunte al dispositivo.

Certificado SSL

Como todas las conexiones hacia y desde los dispositivos tienen que estar protegidas mediante SSL, necesita un certificado válido para el nombre de host emitido por una autoridad de certificación en la que confíe el dispositivo. La clave privada del certificado debe cargarse sin protección por contraseña. En la mayoría de los casos se requiere un certificado intermedio para la CA para que los dispositivos reconozcan el certificado del servidor.

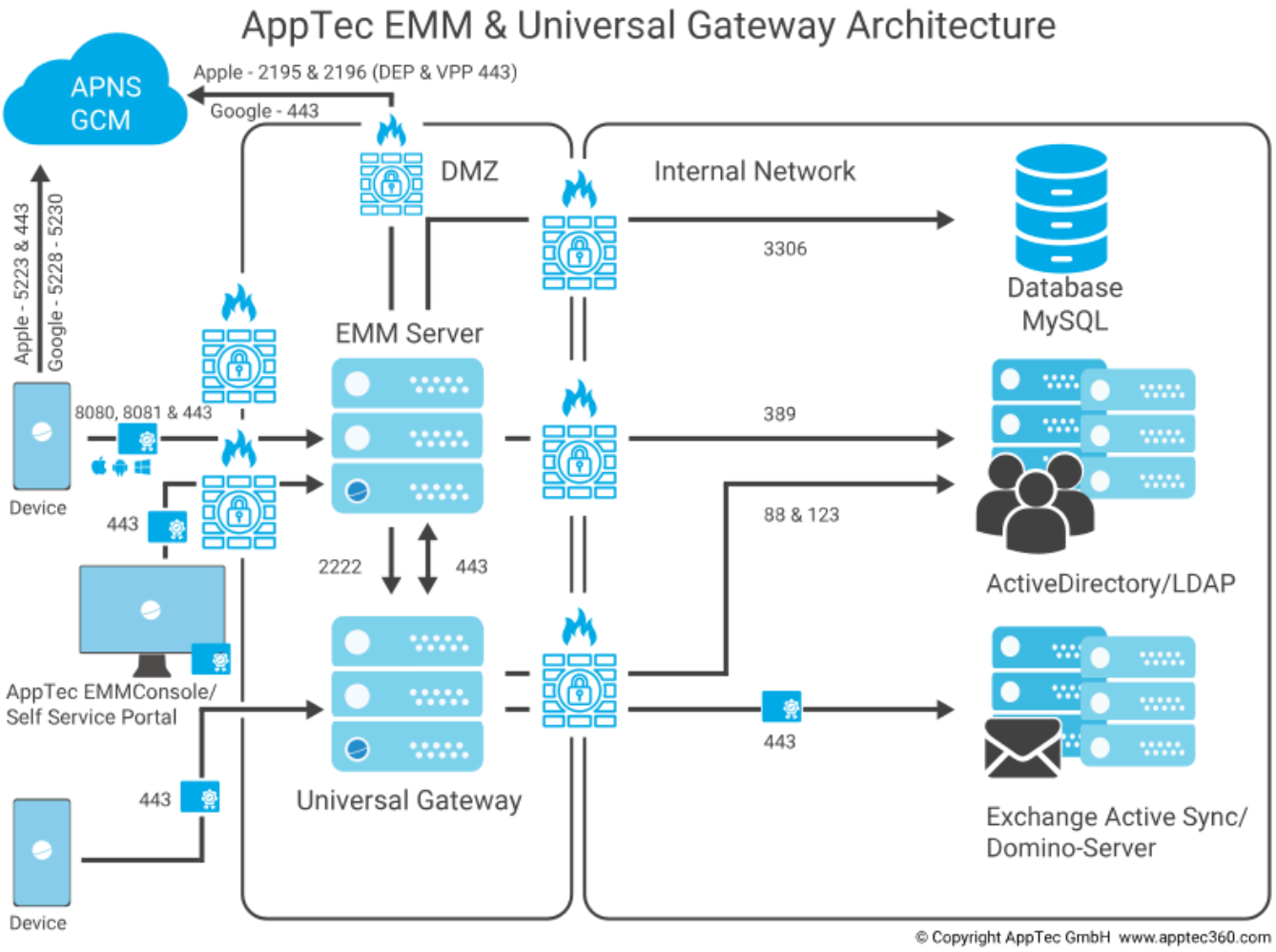
Los dispositivos Windows 10 necesitarán un certificado específico para su subdominio de inscripción de empresa.

A partir de la versión 202104 del dispositivo, también puede utilizar los certificados Let's Encrypt, que se generan automáticamente (descritos en el Paso dos - Certificado SSL).

Servidor SMTP

Para que AppTec360 EMM pueda enviar mensajes de correo electrónico (por ejemplo, para el registro de dispositivos y la validación de cuentas), se necesita un servidor de correo electrónico o un relé de correo electrónico.

Reglas del cortafuegos



Este diagrama muestra qué conexión es necesaria en función de los servicios que desee utilizar.

Para una descripción más detallada, consulte la tabla de la página siguiente.

Cualquiera (externo/Dispositivos)	→	**AppTec360 Appliance / emmconsole.com**
Puertos	443	Gestión, Enterprise AppStore y Windows Phone Communication
	8080	Comunicación Android e iOS
	80	Configura Let's Encrypt por primera vez. Después utiliza 443.
Cualquiera (Dispositivos)	→	**Cualquiera (externo)**
Puertos	5223, 443	Apple Push Service, tiene que ser accesible sin proxy, 443 como Fallback, ver https://support.apple.com/en-us/HT203609
	5228-5230	Android Push Service (FCM), tiene que ser accesible sin proxy
Aparato AppTec360	→	**Controlador de dominio**
Puertos	389, (LDAPS 636)	Sincronización de usuarios con LDAP
Aparato AppTec360	→	**Cualquier**
Puerto	443	Utilizado para el Servicio Push de Android (GCM) Búsqueda en AppStore / Play Store
Aparato AppTec360	→	**emmconsole.com**
Puertos	443	Actualizaciones de AppTec360 Appliance, generación de certificados APNS
Aparato AppTec360	→	**Red Apple (17.0.0.0/8)**
Puertos	2195, 2196	Servicio Push de Apple y Servicio de Comentarios
	443	DEP Y VPP

Actualizaciones de seguridad

El sistema operativo Debian debe actualizarse con regularidad para obtener las correcciones de seguridad más recientes. Sin embargo, asegúrese de no actualizar manualmente a una versión mayor más reciente de Debian. Cuando AppTec360 EMM sea compatible con una versión mayor más reciente, añadiremos una forma de actualizarlo en una actualización del dispositivo.

Contraseñas por defecto del dispositivo virtual

Usuario de inicio de sesión (el inicio de sesión root está desactivado. Utilice "sudo" para las tareas de administración)

apptec

Contraseña

apptec

Usuario raíz de MySQL

raíz

Contraseña raíz de MySQL

apptec

Usuario por defecto de MySQL

AppTec

Contraseña de usuario por defecto de MySQL

AppTec

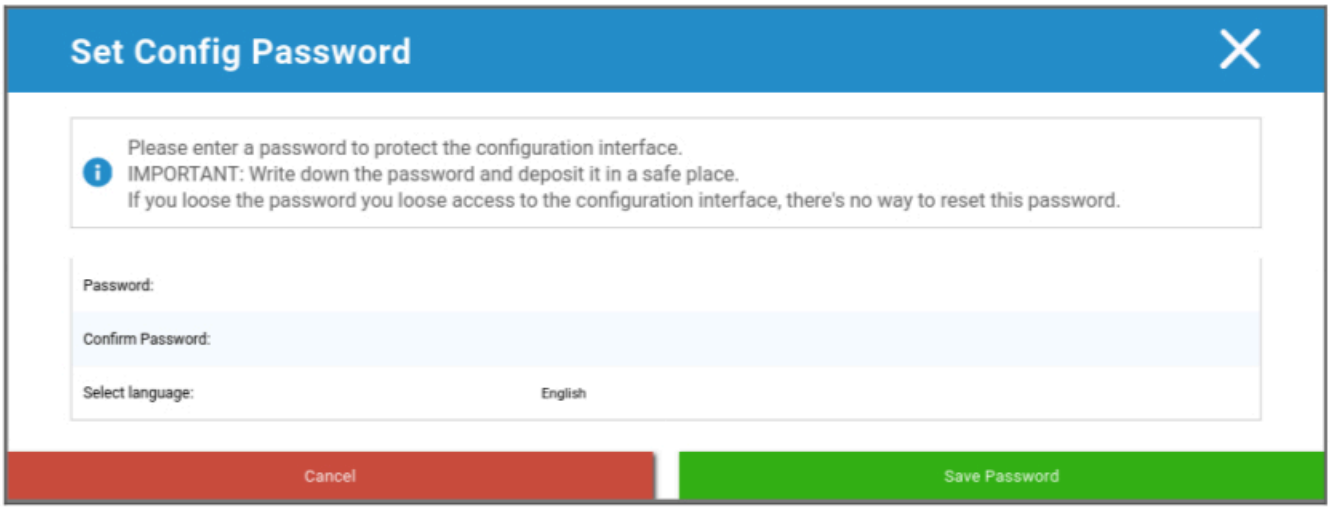
Configuración del dispositivo virtual

Importante: Antes de comenzar con la configuración del dispositivo virtual, la resolución de la pantalla debe ser de al menos 1280 x 800 píxeles.

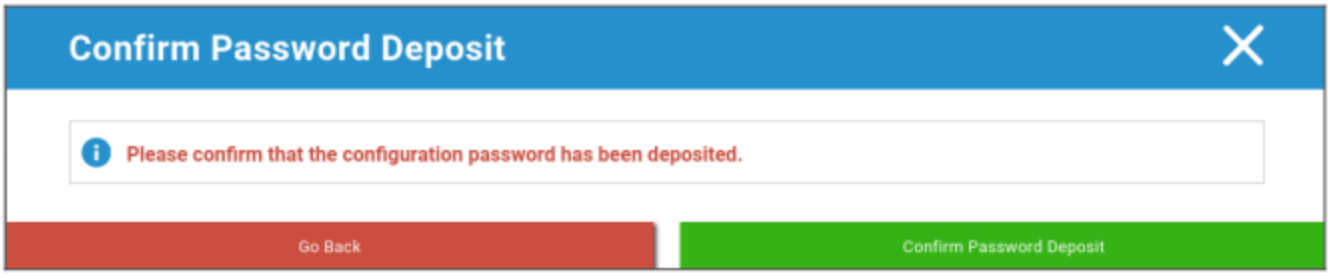
Tras conectarse al dispositivo, Firefox debería iniciarse automáticamente y mostrar la interfaz de configuración.

Preparación

En primer lugar, debe proporcionar una contraseña para la interfaz de configuración. Esta contraseña se utiliza para cifrar toda la información y los archivos introducidos en la interfaz de configuración. Aquí también puede establecer el idioma en el que debe mostrarse la interfaz (puede cambiarse posteriormente).

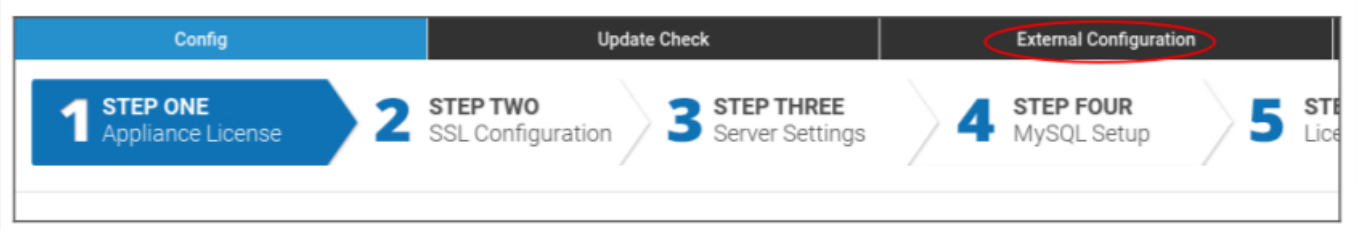


La contraseña sólo puede ser restablecida por el Soporte de AppTec360, así que asegúrese de depositarla en un lugar seguro y confirmar la próxima ventana emergente.



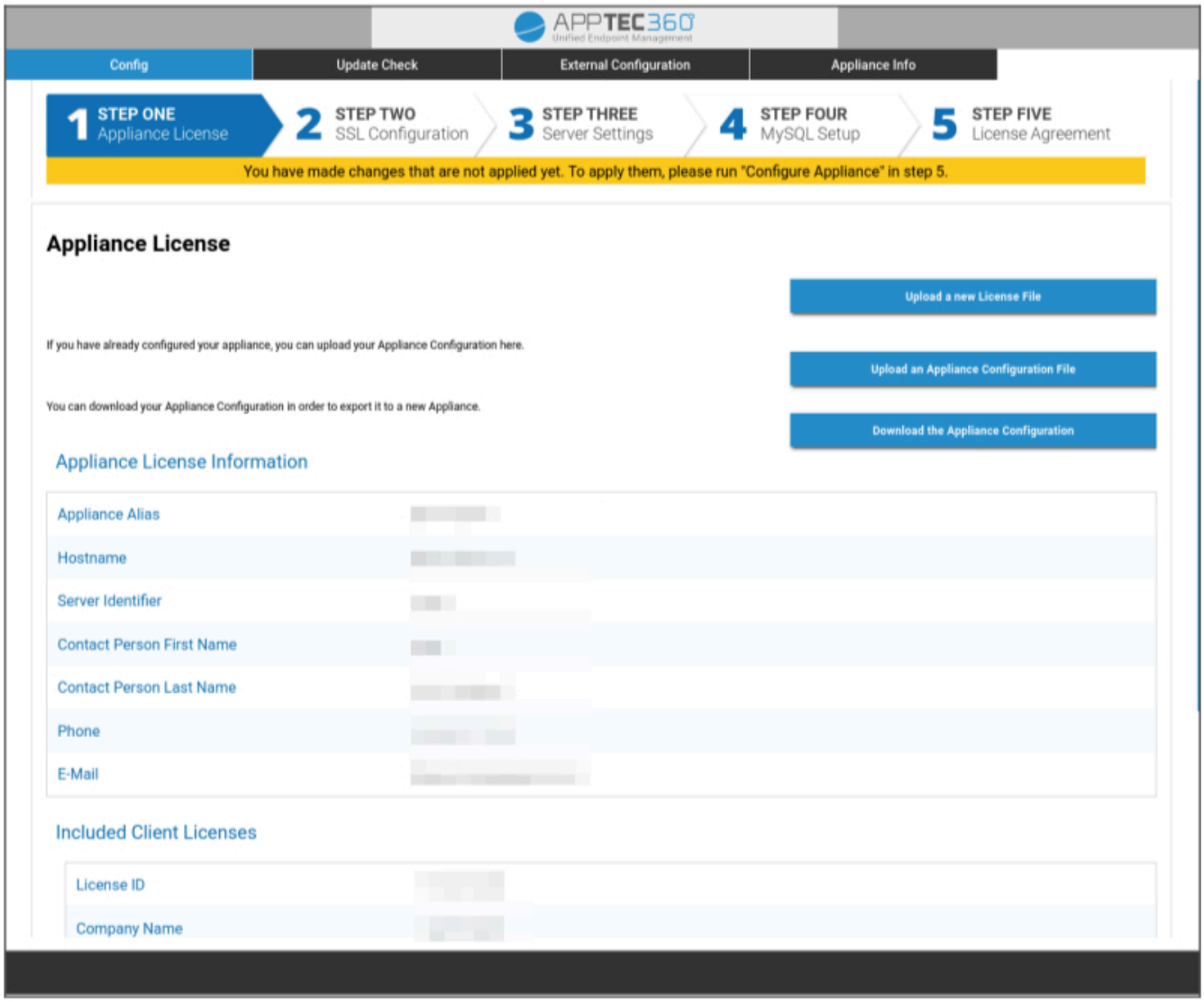
Configurar desde host externo

Para facilitar el proceso de configuración, puedes hacer que la página de configuración sea accesible desde remoto. Para ello, siga los pasos indicados en "Configurar desde host externo".



Paso uno – Licencia del aparato

1. Por favor, cargue el archivo de licencia que ha recibido de AppTec.
2. Si el archivo de licencia se ha cargado correctamente, podrá ver la información de la licencia del dispositivo como en la siguiente captura de pantalla.



Paso dos – Certificado SSL

Puede utilizar la configuración automática de certificados mediante Let's Encrypt o proporcionar los certificados usted mismo (consulte SSL-Certificate para obtener más información).

Automático

El certificado se generará automáticamente utilizando el servicio Let's Encrypt.

AppTec360 EMM utiliza el desafío HTTP-01 para la validación del dominio, lo que significa que el puerto HTTP debe estar abierto desde Internet para la primera solicitud de un certificado. Las solicitudes de renovación posteriores pueden validarse a través de HTTPS.

Cambie los botones de opción a "Automático (Let's Encrypt)" y pulse "GUARDAR VALORES". El certificado se solicitará automáticamente al aplicar la configuración en el Paso Cinco - Acuerdo de Licencia. El certificado se renovará automáticamente si es necesario y recibirá un correo electrónico si el certificado está a punto de caducar (lo que implica que la renovación podría haber fallado).

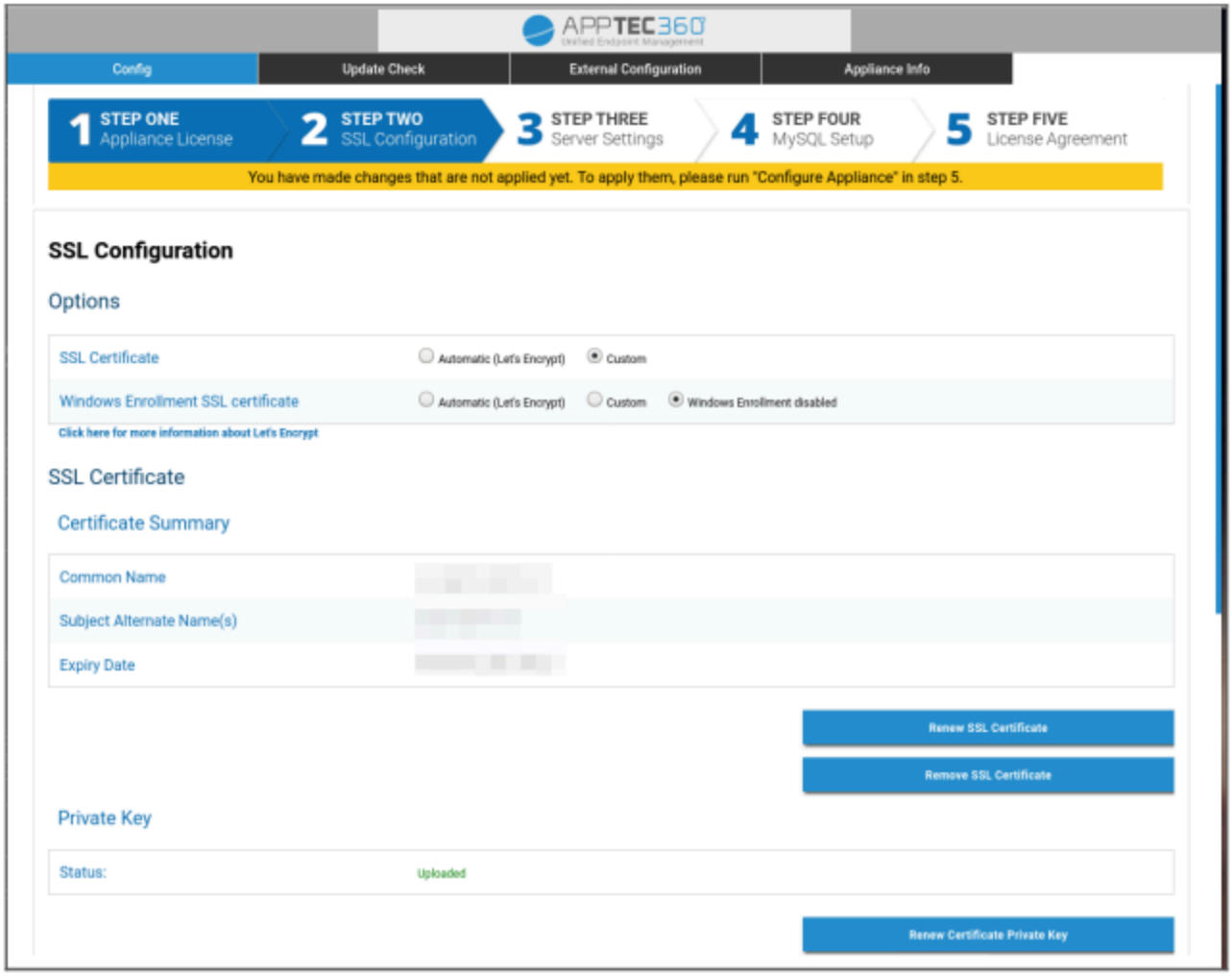
A medida

1. Cargue el certificado SSL para su nombre de host con licencia. Puede ver el nombre de host en Paso uno - Licencia del dispositivo.

2. Cargue también la clave privada del certificado y, si es necesario, el certificado intermedio.

Importante: La clave no debe estar protegida por contraseña. Si es así, elimine la contraseña antes de cargarla.

Sugerencia: Si también desea utilizar dispositivos Windows 10, debe activar "Certificado SSL de inscripción de Windows" y cargar el certificado, la clave privada y el certificado intermedio para su subdominio (descrito en Carga de direcciones IP y resolución DNS) en la parte inferior de la página.



Paso tres – Configuración del servidor

1. Introduzca una dirección de correo electrónico de asistencia global. Esta dirección se utilizará en los correos electrónicos que envíe a sus usuarios para que sepan a quién dirigirse en caso de que surja algún problema con su dispositivo.
2. Proporcione la configuración de correo electrónico que utilizará el sistema para enviar correos electrónicos. La configuración se utilizará para enviar correos electrónicos al usuario y también para enviar informes de errores y solicitudes de funciones a"support@apptec360.com". Después de guardar la configuración del correo electrónico, debe verificarla haciendo clic en "Probar configuración de correo electrónico" y siguiendo las instrucciones.

Paso 4 – Configuración de MySQL

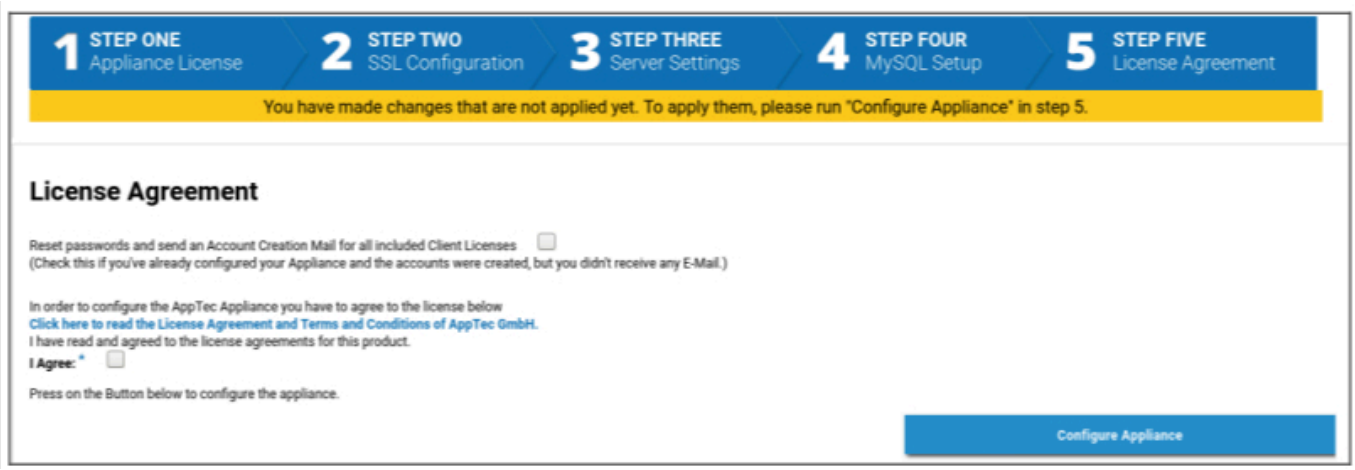
1. Si desea utilizar la base de datos interna, puede omitir este paso. De lo contrario, puede introducir la información de conexión de su servidor de base de datos externo.


1 STEP ONE Appliance License
2 STEP TWO SSL Configuration
3 STEP THREE Server Settings
4 STEP FOUR MySQL Setup
5 STEP FIVE License Agreement
You have made changes that are not applied yet. To apply them, please run "Configure Appliance" in step 5.
MySQL Setup
The MySQL connection has been successfully tested at April 7, 2021, 8:45 am.
If you change the settings after the initial configuration, you have to reconfigure your appliance by clicking on "Configure now" in step 5.
IP Address or Hostname
127.0.0.1
(Default: 127.0.0.1)
Username
AppTec
(Default: AppTec)
Password
(Default: AppTec)
Port
3306
(Default: 3306)

Paso cinco – Acuerdo de licencia

1. Por favor, lea el acuerdo de licencia.
2. Marque "Acepto" y pulse el botón "Configurar dispositivo" para aplicar los ajustes.

Sugerencia: Tendrá que ejecutar "Configurar dispositivo" cada vez que cambie los ajustes en los 5 pasos para aplicar los ajustes.



¡Felicidades!

Ha finalizado la configuración del dispositivo virtual.

Un correo electrónico incluyendo su contraseña fue enviado a la dirección que usted ha proporcionado para la licencia (visible en "Licencias de Cliente Incluidas" en el Paso Uno - Licencia de Appliance).

Ahora puedes acceder a la consola utilizando esta contraseña y la dirección de correo electrónico en la que la has recibido.

Para acceder a la consola, introduzca el nombre de host de la consola en la barra de direcciones de su navegador.

Puede encontrar el nombre de host de su dispositivo en Paso uno - Licencia del dispositivo.

Solución de problemas

1. No ha recibido un correo electrónico al configurar el dispositivo en el Paso 5 - Acuerdo de licencia:

Asegúrese de que la configuración de su correo electrónico en el Paso Tres - Configuración del Servidor es correcta. Para volver a enviar la contraseña marque "Restablecer contraseñas y enviar un correo de creación de cuenta para todas las licencias de cliente incluidas" en el Paso Cinco - Acuerdo de licencia antes de ejecutar "Configurar dispositivo" de nuevo.

2. Ha recibido un error con respecto a Let's Encrypt durante la configuración en el Paso Cinco - Acuerdo de Licencia:

Asegúrese de que el dispositivo es accesible por su nombre de dominio en el puerto 80. Let's encrypt también escribe un registro en "/var/log/letsencrypt" que puede ayudar a solucionar problemas.

Recomendaciones de seguridad

Se recomienda realizar los siguientes pasos para proteger su dispositivo AppTec360.

Esto no es un conjunto completo de instrucciones, es sólo una recomendación para una configuración básica.

- Cambiar la contraseña del usuario de AppTec360
- Cambie la contraseña de los usuarios de MySQL "root" y "AppTec" y actualice el Paso Cuatro - Configuración de MySQL en consecuencia.
- Cambiar el puerto por defecto del servidor SSH
- Bloquee el puerto 80 en su consola y no permita el tráfico HTTP entrante, utilice sólo HTTPS. Una vez configurado, también es posible una configuración externa a través de HTTPS.
- Restringir el acceso a la interfaz de gestión sólo a determinadas Ips en la parte inferior del Paso Tres - Configuración del Servidor.
- Configurar el cortafuegos

Ajustes generales

Resumen de cuenta

Información sobre la cuenta

Visión general

Aquí puede ver un resumen de su cuenta de AppTec360.

Nombre de la empresa	El nombre de tu empresa
Fecha de creación	Fecha de creación de tu cuenta
Tipo de licencia	De pago = licencia de pago Gratuito = licencia no pagada Nota: Las cuentas de un dispositivo local siempre aparecerán como pagadas por razones técnicas.
Identificador de cliente	Identificador de tu cuenta (NO es tu número de cliente)
Fecha de caducidad de la licencia	Fecha de caducidad de tu licencia de AppTec360
Licencia ContentBox	Gratis = licencia gratuita para 25 dispositivos Pagada = licencia pagada para x dispositivos
Lanzador	Muestra si puedes o no utilizar el lanzador personalizado para Android
Dispositivos	Número de licencias utilizadas actualmente / total de licencias
Persona de contacto	Persona de contacto proporcionada
Teléfono	Número de teléfono facilitado
Correo electrónico	Dirección de correo electrónico facilitada
Usuario raíz	Usuarios Root que pueden iniciar sesión
Versión de software	Versión actual del software

**Nota: La dirección de correo electrónico que aparece aquí es la que usted introdujo para registrar la Cuenta. En base a esto se creará un usuario en el árbol de usuarios/dispositivos y podrá ser modificado. Al editar este usuario cambiará la dirección de correo electrónico que debe utilizar para iniciar sesión, pero no la información de la descripción general de la cuenta..*

Informe de errores

Un informe de error puede enviarse directamente a soporte para informar de problemas o errores e incluye información y registros sobre tu cuenta y configuración.

Asunto	El asunto del informe de error. Incluye un número de ticket si quieres añadirlo a un ticket de soporte existente.
Comportamiento esperado	Describe detalladamente lo que hiciste y lo que esperabas que ocurriera
Comportamiento real	Describe detalladamente lo que ocurrió exactamente. Por favor, cita EXACTAMENTE los mensajes de error. También ayuda si añades capturas de pantalla al archivo adjunto.
¿En qué momento experimentaste el problema?	Indica la hora exacta en que recibiste el mensaje de error/problema concreto. En el mejor de los casos, incluye también los segundos, por ejemplo 18:55:27
¿Puede reproducirse el problema? En caso afirmativo, ¿cómo (detalladamente)?	Describe detalladamente cómo puedes reproducir el problema.
¿Esta función ha funcionado anteriormente como esperabas? En caso afirmativo, ¿hasta cuándo?	Déjalo vacío si no lo sabes.
¿Se hicieron cambios específicos en el sistema antes de que apareciera este problema? En caso afirmativo, ¿qué cambios (en detalle)?	Menciona siempre cuál fue tu último cambio o acción antes de que apareciera el problema, aunque creas que es irrelevante.
Si procede: ¿Qué modelos de dispositivo y versiones de SO están afectados?	Indica siempre la versión exacta del sistema operativo (por ejemplo, iOS 14.7.1 o Android 11)
Si procede: ¿Cuál es la dirección IP pública o/y el número de serie del Dispositivo?	Nombra al menos uno, aunque todos los dispositivos estén afectados.
Incluir archivos de registro	Marca esta casilla para enviar el archivo de registro con el informe de error. Se recomienda hacer esto.
Obtener el estado actual de VPP de Apple e incluirlo en el informe de errores	Incluye información sobre la asignación de licencias VPP. Actívalo sólo si te lo pide el servicio de asistencia o si tu problema tiene que ver con la VPP.

Adjunto	Adjunta cualquier archivo que pueda ser útil (por ejemplo, capturas de pantalla de un mensaje de error)

Solicitud de funciones

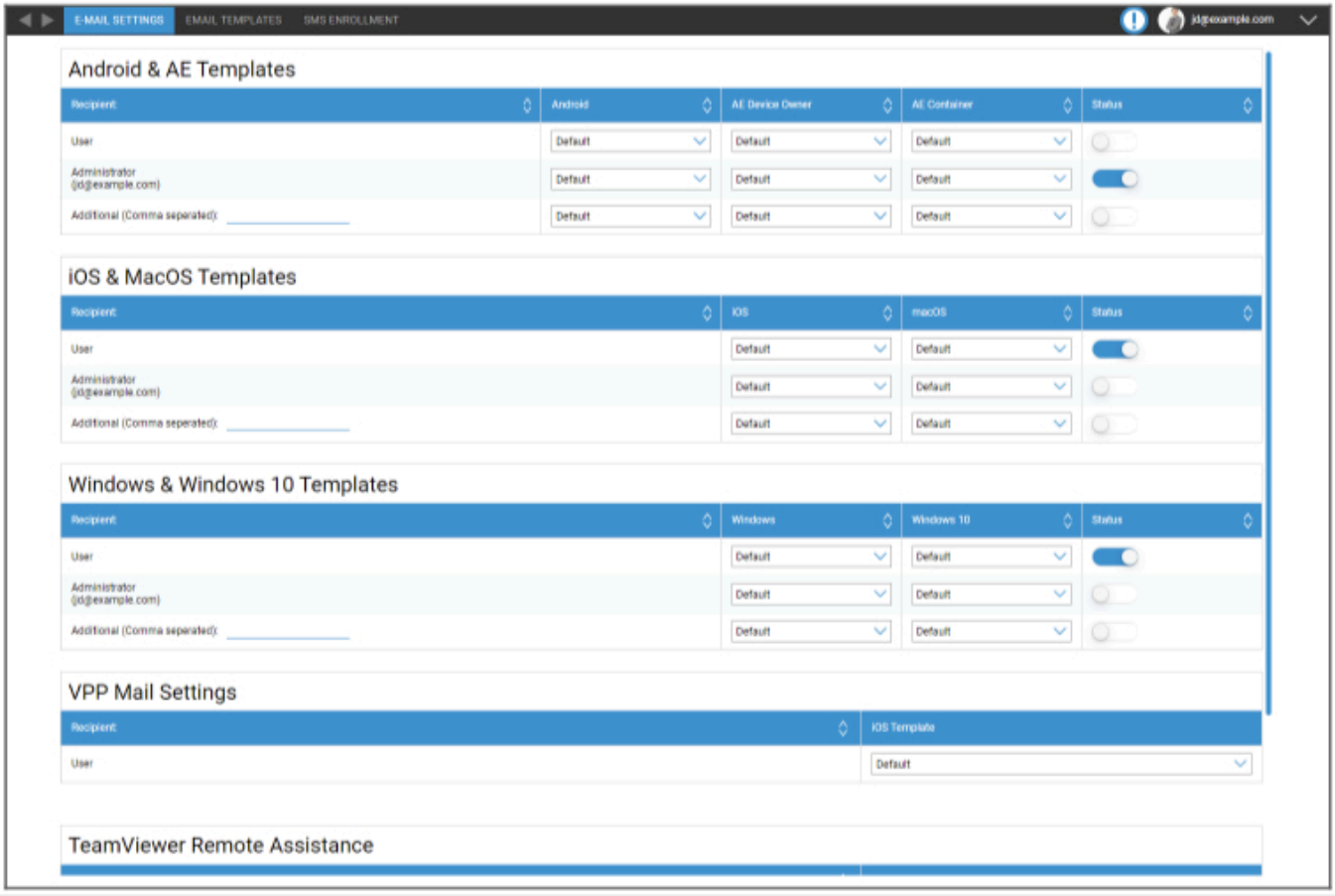
Puede enviar una solicitud de funcionalidad directamente al servicio de asistencia. Puede contener una solicitud de una función específica o una mejora para

Resumen	Una breve sinopsis de tu problema
Descripción	Una descripción detallada de tu problema, por favor, sé lo más específico posible
Adjunto	Adjuntar archivos al informe de error

Configuración global

Configuración de eMail

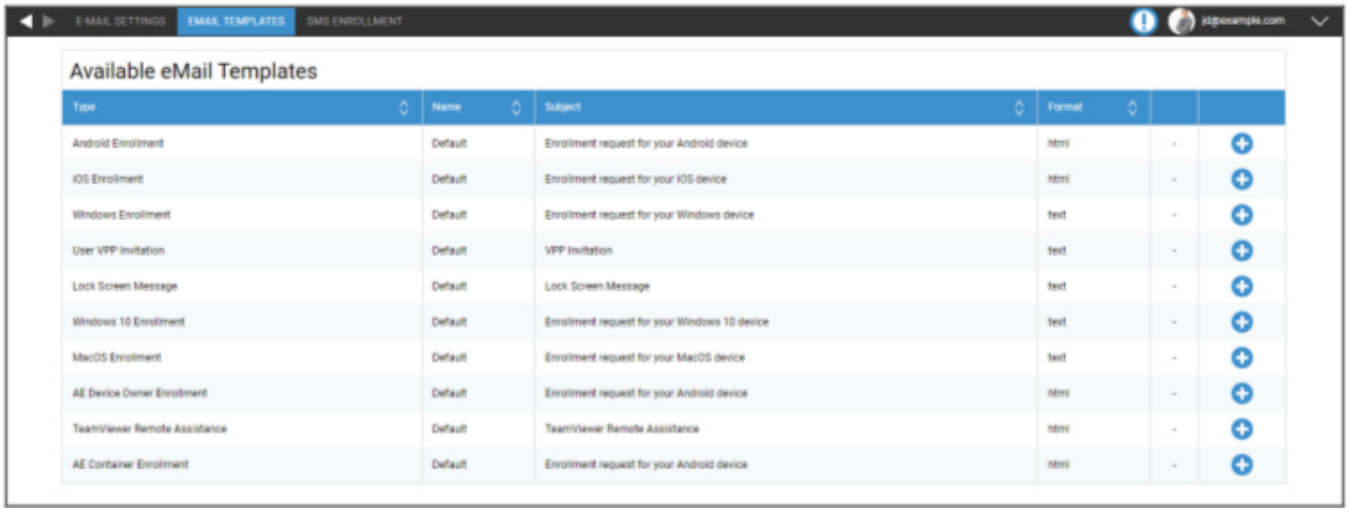
Aquí puede definir quién recibe un correo cuando se genera una solicitud de inscripción y qué plantilla de texto se utiliza para ese correo.



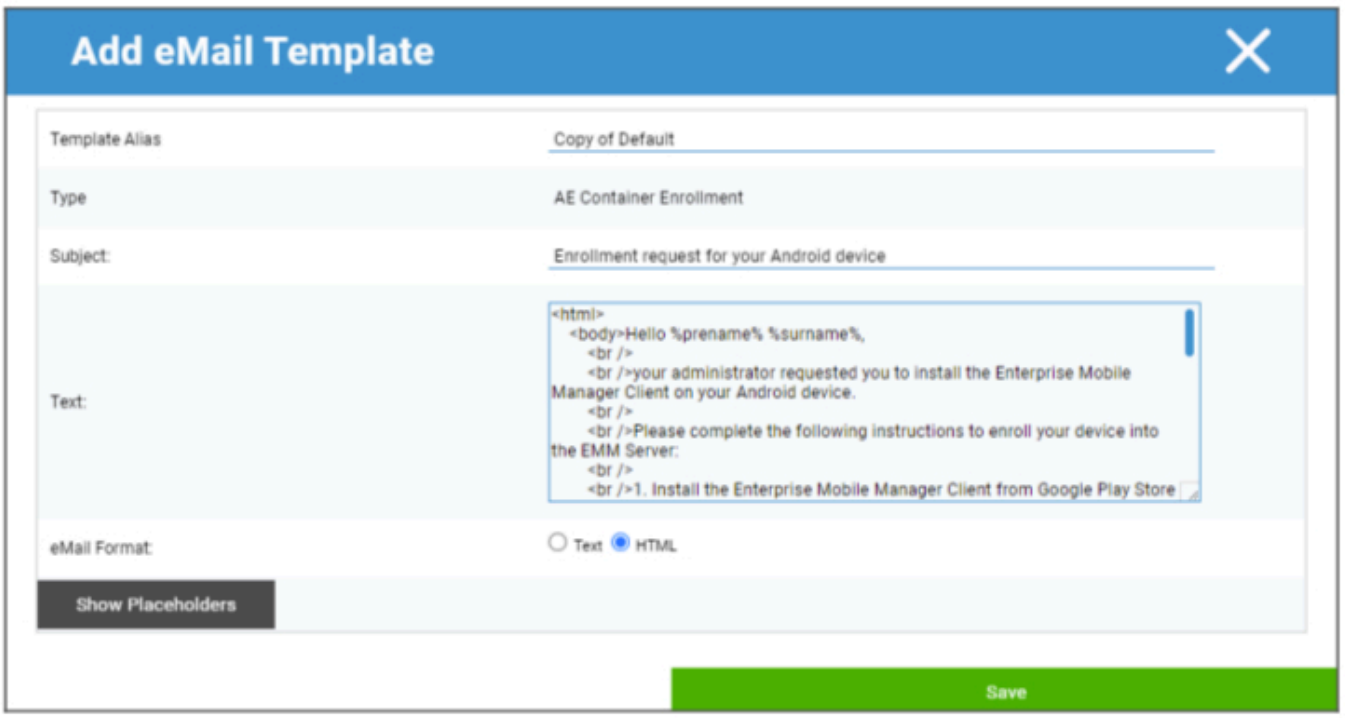
Plantillas de correo electrónico

Aquí puede generar y editar sus plantillas para diferentes escenarios. Pueden estar en formato de texto normal o en HTML. Con HTML puedes controlar mejor el formato del texto.

Las plantillas predeterminadas no se pueden editar ni borrar.



También puede utilizar marcadores de posición como variables que se sustituirán automáticamente. Haga clic en "Mostrar marcadores de posición" durante la edición para ver los marcadores de posición disponibles. Las diferentes categorías tienen diferentes marcadores de posición.



Inscripción SMS

Aquí puede desactivar el proceso de inscripción por SMS.

(Por defecto: desactivado)

También verá una pantalla que indica cuántos créditos SMS quedan disponibles.

Los créditos SMS deben adquirirse por separado.

Privacidad

Acceso GPS

Aquí puedes proteger la Vista GPS de cada dispositivo con 1 o 2 contraseñas (principio de los cuatro ojos). Se te pedirá que introduzcas tu(s) contraseña(s) cada vez que intentes acceder a la ubicación de un dispositivo.

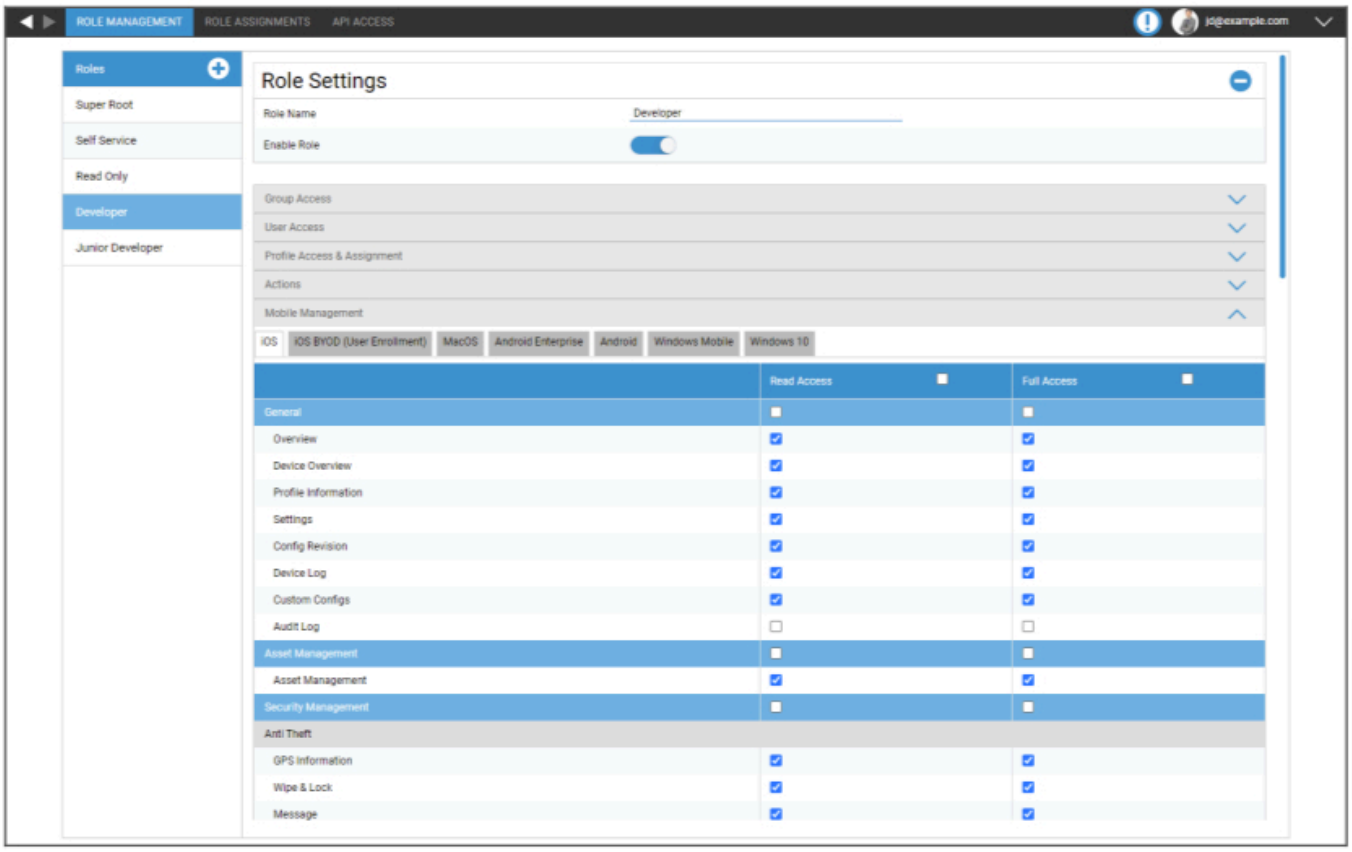
Restringir el acceso a los Ajustes del GPS	Apagado = la función está desactivada y no se necesita contraseña para localizar
	Activado = la función está activada y se requiere una contraseña para localizar
Método de protección	Utilizar una contraseña = utilizar una contraseña para localizar
	Utilizar dos contraseñas = utilizar dos contraseñas para localizar
Introducir contraseña (1)	Introduce la contraseña elegida
Repetir contraseña (1)	Vuelve a introducir la contraseña elegida
opcional: Introduce la contraseña 2	Introduce la 2ª contraseña elegida
opcional: Repite la Contraseña 2	Vuelve a introducir la 2ª contraseña elegida

Nota: Después de configurar tu(s) código(s) de acceso, tienes que introducirlo(s) una vez más antes de que esté(n) completamente activado(s).

Acceso basado en funciones

Gestión de funciones

Los Roles definen lo que un usuario puede ver y hacer cuando se conecta a la consola de gestión. Esto le permite crear usuarios que pueden iniciar sesión pero tienen una funcionalidad limitada.



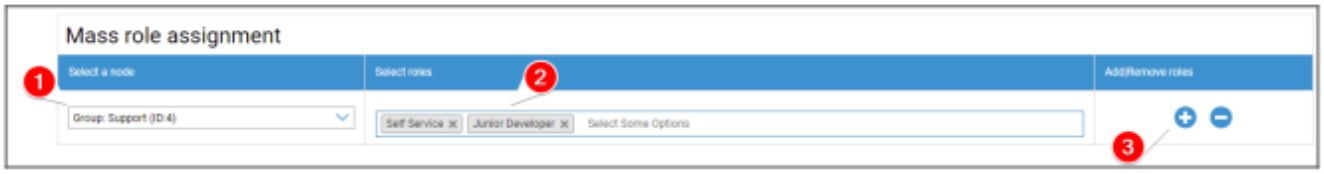
El rol Super Root es un rol por defecto que siempre puede ver y cambiar todo. No puede modificarse ni suprimirse. El rol de autoservicio sólo puede ver sus propios usuarios y dispositivos. Puede combinar Self Service y un rol personalizado para, por ejemplo, permitir a los usuarios iniciar sesión e inscribir dispositivos por su cuenta y sólo para su usuario.

Los roles personalizados pueden activarse o desactivarse manualmente. Los nuevos roles están desactivados por defecto. Los usuarios con un rol desactivado trabajan como si no tuvieran el rol. Esto le permite, por ejemplo, restringir temporalmente las acciones de un rol determinado.

Todos los permisos se dividen entre "Acceso de lectura" y "Acceso total". Dar a un rol acceso de lectura le permite ver la parte específica de la consola. Darles Acceso Completo permite al Rol ver y cambiar la parte específica de la consola.

Asignación de funciones

Aquí se obtiene una visión general de todos los usuarios que tienen un rol y ver cuál tienen. Aquí también puede asignar una función a usuarios o grupos enteros:

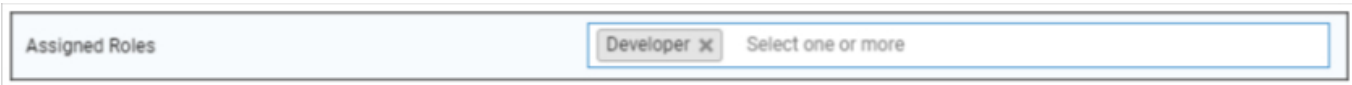


1. Seleccione para qué grupo o usuario desea añadir o eliminar funciones. Puede seleccionar un solo usuario o seleccionar un grupo. Al seleccionar un grupo, el cambio afectará a todos los usuarios de ese grupo y a todos los usuarios de los subgrupos del grupo seleccionado.
2. Seleccione la función que desea añadir o eliminar. Puede seleccionar una o varias funciones.
3. . Seleccione la operación que desea realizar. Al hacer clic en el signo "+" se añaden las funciones seleccionadas si el usuario o usuarios no las tenían ya. Al hacer clic en el signo "-" se eliminan las funciones seleccionadas de los usuarios. Si añade funciones a un usuario que todavía no tiene ninguna función, se activará automáticamente "Puede iniciar sesión" para el usuario.
4. Guardar para finalizar el proceso. Los usuarios que antes no tenían ninguna función y tenían desactivada la opción "Puede iniciar sesión" recibirán automáticamente un correo electrónico con un enlace para establecer una contraseña.

Debajo de la asignación masiva de funciones puede encontrar una visión general de las funciones asignadas. También puede cambiar manualmente las funciones de determinados usuarios.

Asignación de una función

Para asignar un rol a un usuario, tienes que ir a la Gestión de Móviles, donde encontrarás el árbol de tus grupos, usuarios y dispositivos. Edite el usuario para asignarle un rol. También puede utilizar el método anterior para usuarios únicos.



Acceso API

Acceso a la API REST de AppTec360

La API REST de AppTec360 requiere un token de autenticación (clave API) y una clave privada que deben generarse en la Consola de administración.

Para ello, inicie sesión en AppTec360 EMM y vaya a

Ajustes generales → Acceso basado en roles → Acceso API y añada una nueva Clave.

Debe seleccionar un usuario cuyos permisos se aplicarán a la clave API.

La clave privada sólo puede descargarse una vez. Una vez iniciada la descarga, se borrará la clave y desaparecerá el botón "Descargar".

Si pierde su clave privada, tendrá que generar una nueva clave API.

Normas generales

- La API REST está disponible debajo de la URL base:

/public/external/api

- Todas las solicitudes deben enviarse mediante POST.
- La API REST sólo admite solicitudes a través de HTTPS.
- Las solicitudes deben contener las siguientes cabeceras:

Nombre de la cabecera	Valor de cabecera	Descripción
Tipo de contenido	aplicación/json	fijo
auth	123...xyz	Clave API desde la pestaña "Acceso API
firma	Firma codificada en Base64	Firma de la carga útil generada con el Clave privada de la pestaña "Acceso API

- El cuerpo de la solicitud debe ser un objeto codificado json que debe contener los siguientes valores:

Campo	Campo Ejemplo Valor	Descripción
api	v2/dispositivo/listadispositivos	Nombre de la API
tiempo	1529662725	Marca de tiempo Unix (UTC) de la máquina cliente. La diferencia de tiempo máxima permitida entre el cliente y el servidor es de 30 minutos.

- En caso de éxito, la API devuelve los datos solicitados (véanse las consultas más abajo) y un código de estado HTTP 200.
- Si se produce un error, el código de estado HTTP será entre 4xx y 5xx dependiendo del error y el objeto de respuesta contendrá un array con la clave "errors", que contiene una lista de mensajes de error legibles por humanos.
- Si no hay datos coincidentes para un dispositivo, se devolverá una matriz vacía.
- Si un Id de dispositivo no existe, sus datos de retorno serán nulos.

Ejemplo de solicitud

POST /public/external/api HTTP/1.1
Host: myapptecemm.com
Accept: /
Content-Type: application/jsonauth: 1234567890abcdefghijklmnopqrstuvwxyz
signature: a/bnOV466a0SiyVfsbpspZ+NxiTpmeF18NkfnOIq+OrEZDu9+VW7ESKziPXvw
kTM5B9j/t1WGN1mRcIKe80m8fDKPj+lr3BqoMJe7wGXift+uy6iS7Chpdz2iZA4KPxxU9Z
GU2cdQ/SQceX57pi+ch7ApxBeVX2+lJapTwA6CfB0mJFaf4MPcg/
7LZWkzKxKF7LNzNJHiy/vSpZcqjbXjpC4HWrX6j2uZG5eSP8kYcTR
9VQfGtkX9pcyaNAwguR7zOOwMu/8L0oKq21/19rkabE4ZgUjtKS2+
+q+rh6mrP1g4BCZ7Xq/wvgZkaP
b0CStBdMRvj46i3enxCXcLQQ==
Content-Length: 74
{"api":"v2/device/listposition","time":1529665112,"params":{"ids": [10]}}

Consultas

Listar todos los dispositivos

Funcionalidad: Devuelve una lista de todos los dispositivos que contienen el ID de dispositivo, IMEI y serie.
URI de la API: v2/device/listdevices
Parámetros obligatorios: ninguno
Parámetros opcionales: ninguno

Ejemplo de cuerpo de solicitud


```
{
"api": "v2/device/listdevices",
"time": 1529662725
}
```


Ejemplo de cuerpo de respuesta


```
{
"errors": [],
"list":[
{ "id":"10","serial":"987612345","imei":"899938455454"},
{ "id":"11","serial":"619723118","imei":"713032378599"}
]
}
```

Obtener lista de posiciones (GPS)

Funcionalidad: Devuelve una lista de todas las entradas de registro de posición almacenadas para los identificadores de dispositivo
URI de la API: v2/dispositivo/listado
Parámetros obligatorios: "ids" - Matriz de ID de dispositivo
Parámetros opcionales: ninguno

Ejemplo de cuerpo de solicitud


```
{
"api": "device/listposition",
"params": {
"ids": [10, 11]
},
"time": 1529662725
}
```


Ejemplo de cuerpo de respuesta


```
{
"errors": [],
"list":[
"10":[
{"time":"1529632725","pos":"47.5572,7.5967"},
{"time":"1529642725","pos":"47.5572,7.5968"},
{"time":"1529652725","pos":"47.5573,7.5969"},
],
"88":[],
]
}
```

Obtener mapa de activos

Funcionalidad:
Devuelve una lista de todos los posibles activos almacenados que se pueden solicitar mediante Obtener datos de cualquier activo.
Para solicitar los datos, puede utilizar el formulario de lectura humana o la etiqueta de activo.
URI de la API: v2/device/getassetmap
Parámetros obligatorios: ninguno
Parámetros opcionales: ninguno

Ejemplo de cuerpo de solicitud

{
"api": "v2/device/getassetmap",
"time": 1529662725
}

Ejemplo de cuerpo de respuesta

Esta respuesta se ha acortado para facilitar su lectura.

{
"AssetKeys": {
"UDID": "AT001",
"Device Alias": "AT002",
"OS Version WinMobile iOS MacOS": "AT003",
"Model Name": "AT004",
"Serial Number": "AT005",
"Total Storage": "AT006",
"Free Storage": "AT007",
"IMEI": "AT008",
…
"apptecID": "APPTECID"
},
"errors": []
}

Obtener datos de cualquier activo

Funcionalidad: Devuelve una lista de los datos de activos solicitados para los identificadores de dispositivo
URI de la API: v2/device/getassetdata
Parámetros obligatorios: "ids" - Matriz de ID de dispositivo
Parámetros opcionales:
"assetkeys" - Claves de datos de activos a devolver. Si no se especifica, todos los datos de activos disponibles serán
devuelto. Puede obtener una lista de claves de activos utilizando Obtener mapa de activos.

Ejemplo de cuerpo de solicitud


```
{
"api": "v2/device/getassetdata",
"time": 1529662725,
"params": {
"ids": [
26
],
"assetkeys": [
"imei"
]
}
}
```


Ejemplo de cuerpo de respuesta


```
{
"result": {
"26": {
"imei": "349157642516427”
}
},
"errors": []
}
```

Código de ejemplo en Python3

```
! /usr/bin/python
import base64
from Crypto.Hash import SHA512
from Crypto.Signature import PKCS1_v1_5
from Crypto.PublicKey import RSA
import os
import time
import json
import urllib.request
import urllib.parse
import urllib.error
import http.client
applianceDomain = "YOURAPPLIANCE.COM"
apiURL = "https://"+applianceDomain+"/public/external/api"
privateKeyPath = "/path/to/PrivateKey-XXXXXXXXXXX.pem"
apptecAPIAuthToken = "7eXXXXXXXXXXXXXXXXXXXXXXXXXXX20"
currentTimestamp = int(time.time())
# Get Devices
#requestData = {"api": "v2/device/listdevices", "time": currentTimestamp}
# Get Positions
#requestData = {"api": "v2/device/listposition", "time": currentTimestamp,
"params":{"ids":[26]}}
# Get AssetData
requestData = {"api": "v2/device/getassetdata", "time": currentTimestamp,
"params":{"ids":[26], "assetkeys": ["imei"]}}
# encode the request data to json
print(json.dumps(requestData, indent=1))
jsonEncodedRequestData = json.dumps(requestData)
# Sign the request data json with the API private key
message = jsonEncodedRequestData.encode('utf-8')
print("Body:", message)
digest = SHA512.new()
digest.update(message)
```

```
# Read private key from file
with open(privateKeyPath, "r") as myKeyFile:
private_key = RSA.importKey(myKeyFile.read())
```

```
# Load private key and sign message
signer = PKCS1_v1_5.new(private_key)
signatureOfRequestData = signer.sign(digest)
Base64EncodedSignature = base64.b64encode(
signatureOfRequestData).decode("utf-8")

headers = {"Content-type": "application/json",
"auth": apptecAPIAuthToken, "signature": Base64EncodedSignature}
print("Headers:", headers, "\n")

# Send request to Server
httpsClient = http.client.HTTPSConnection(applianceDomain, 443, timeout=10)
httpsClient.request("POST", apiURL, jsonEncodedRequestData, headers)

# Get answer
response = httpsClient.getresponse()
status = response.status
data = response.read()

if data == False:
print("Invalid answer from the server")
else:
print("Answer:")
print(json.dumps(json.loads(data), indent=1))
if status != 200:
print("http error: lastReceivedHttpCode")
print(status)
```

Configuración de Apple

Certificado APNS

Aquí puede cargar un certificado APNS. Es necesario para gestionar dispositivos iOS y macOS.

Nota: El Certificado APNS sólo es válido durante un año. Debe renovarse antes de que caduque. El proceso de renovación es idéntico al de creación (véase más abajo) y sólo dura unos minutos.

Si olvida renovarla a tiempo, no podrá realizar cambios en los dispositivos ya inscritos **y tendrá que volver a inscribir todos los dispositivos** .

Primer paso

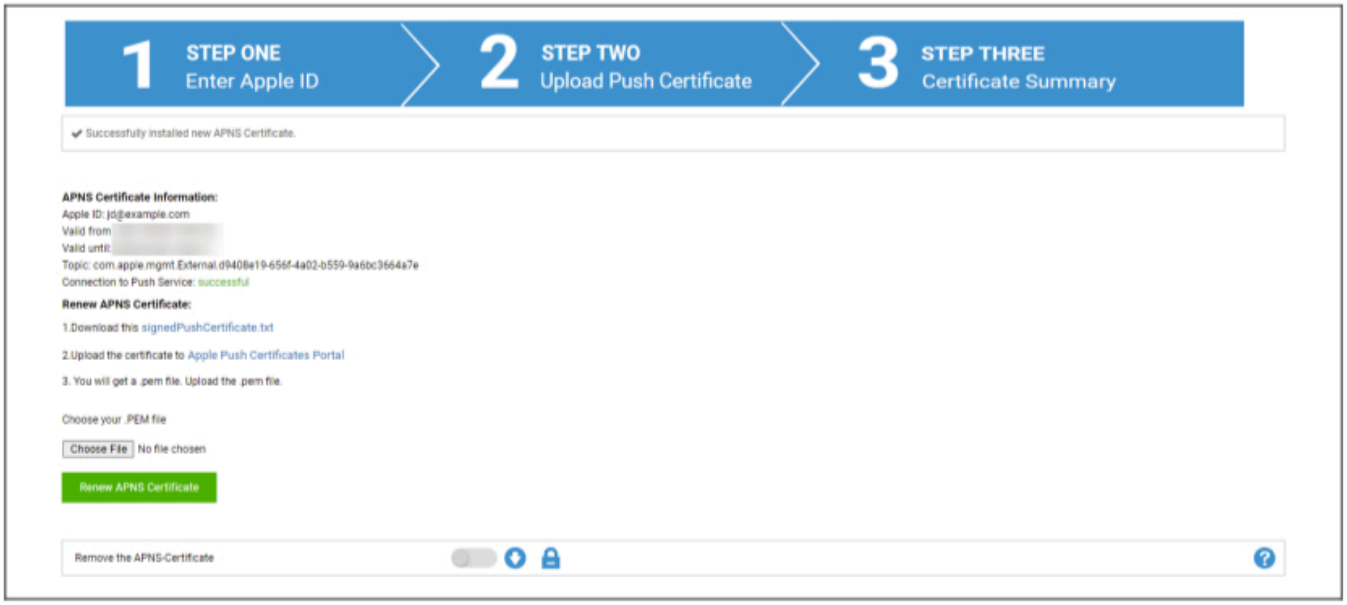
- En primer lugar, introduzca el ID de Apple que desea utilizar para crear el certificado APNS.

Nota: Este ID de Apple sólo se utiliza para la creación del certificado APNS. Este ID de Apple no tiene nada que ver con los dispositivos y los dispositivos no sabrán nada de este ID de Apple. Además, también necesita acceder a este ID de Apple para renovar el certificado APNS. Por lo tanto, se recomienda utilizar algún ID de Apple genérico y documentar los datos de acceso. Se envía un recordatorio a la dirección de correo utilizada del ID de Apple antes de que caduque el certificado APNS.

- Haga clic en "Siguiente paso" para continuar.
- (opcional) También puede recuperar el certificado APNS eliminado anteriormente si lo borró por accidente

Paso 2

- Descargar signedPushCertificate.txt
- Vaya a https://identity.apple.com/pushcert/ e inicie sesión con el ID de Apple del paso 1.
- Haga clic en "Crear un certificado".
- (opcional) introduzca una Nota. Esto puede ser útil si gestiona varios inquilinos para identificarlos fácilmente.
- Haga clic en "Seleccionar archivo" para seleccionar el archivo signedPushCertificate.txt descargado anteriormente.
- Haga clic en "Cargar".
- Ahora verá la confirmación de que ha creado un certificado APNS.
- Haz clic en "Descargar" y guárdalo.
- Vuelva a la consola de gestión.
- Haga clic en "Elegir archivo" y seleccione el certificado APNS que desea cargar.
- Haga clic en "Cargar".



Paso 3

Ya ha configurado correctamente el certificado APNS y puede gestionar dispositivos iOS y MacOS.

En el paso 3 verá un resumen de su certificado APNS utilizado actualmente.

También tiene la opción de renovar el certificado APNS siguiendo los pasos que se muestran en pantalla. No olvide renovarlo antes de que caduque.

Cuando renueve el certificado APNS, tenga en cuenta que debe iniciar sesión con el ID de Apple que se muestra en el paso 3 y también que debe renovar el certificado utilizado anteriormente y NO crear uno nuevo. Verá el "tema" del Certificado APNS en el Paso 3 y al pulsar sobre la "i" en el Portal de Certificados Push de Apple. Es el identificador único que identifica el certificado. Esto le ayudará a identificar la correcta y renovar la correcta.

Si aparece el mensaje "Error: El certificado push tiene un tema diferente", significa que ha renovado otro certificado o ha creado uno nuevo.

Si desea cargar un nuevo certificado, por ejemplo, si ya no puede acceder al ID de Apple utilizado anteriormente, primero debe eliminar el certificado cargado actualmente.

En cualquier caso, borrar el certificado APNS significa que ya no podrá realizar cambios en los dispositivos actualmente registrados hasta que los registre de nuevo. Así que asegúrese de que está preparado para ello y sólo retire el Certificado si no hay otro remedio.

Acceso gestionado

Aquí puede activar la Inscripción de usuarios para dispositivos iOS y el iPad compartido para dispositivos iOS.

Inscripción de usuarios

La "Inscripción de usuarios" habilita un modo especial para dispositivos BYOD.

Para cada usuario debe crearse una Apple-ID gestionada en el Apple Business Portal.

Durante el proceso de inscripción se pedirá a los usuarios sus credenciales Apple-ID.

La "Inscripción del usuario" garantiza la máxima seguridad para el usuario, ya que sólo permite configurar un conjunto limitado de ajustes y restricciones por parte del MDM.

Dominio gestionado:

Dominio utilizado para asignar la dirección de correo electrónico del usuario a su Apple-ID gestionado (debe tener el formato "@appleid.company.com"). Por ejemplo, john.doe@example.com se asignará a john.doe@appleid.company.com.

Comprueba en Apple Business Manager tu dominio gestionado

iPad compartido

Un iPad compartido es un dispositivo DEP configurado con un perfil DEP especial.

Esto permite que varios usuarios inicien sesión en el dispositivo utilizando su Apple-ID gestionada.

La Apple-ID gestionada debe crearse en el Apple Business Portal o en el Apple School Manager.

A los usuarios que inician sesión en un iPad compartido se les piden sus credenciales Apple-ID gestionadas.

Dominio gestionado:

Dominio utilizado para asignar la dirección de correo electrónico del usuario a su Apple-ID gestionado (debe tener el formato "@appleid.company.com"). Por ejemplo, john.doe@example.com se asignará a john.doe@appleid.company.com.

Comprueba en Apple Business Manager tu dominio gestionado

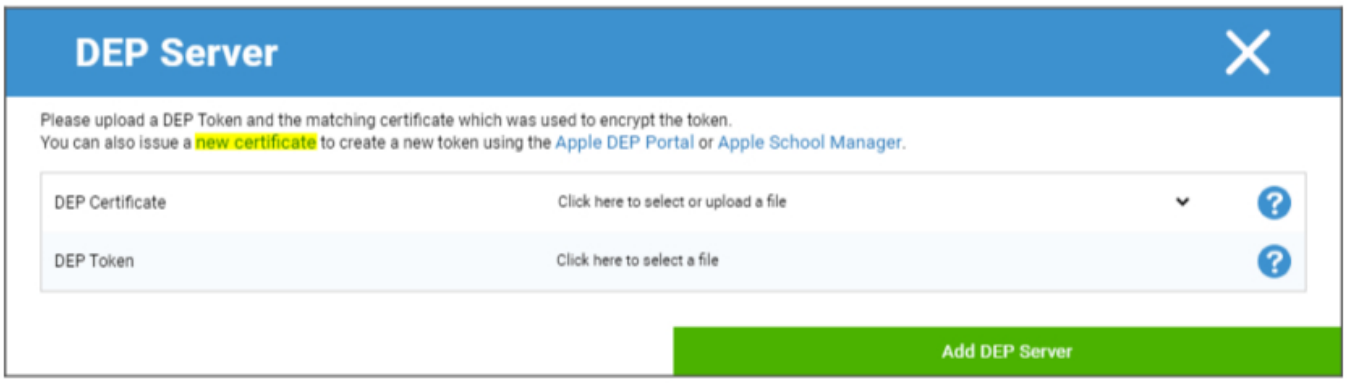
DEP

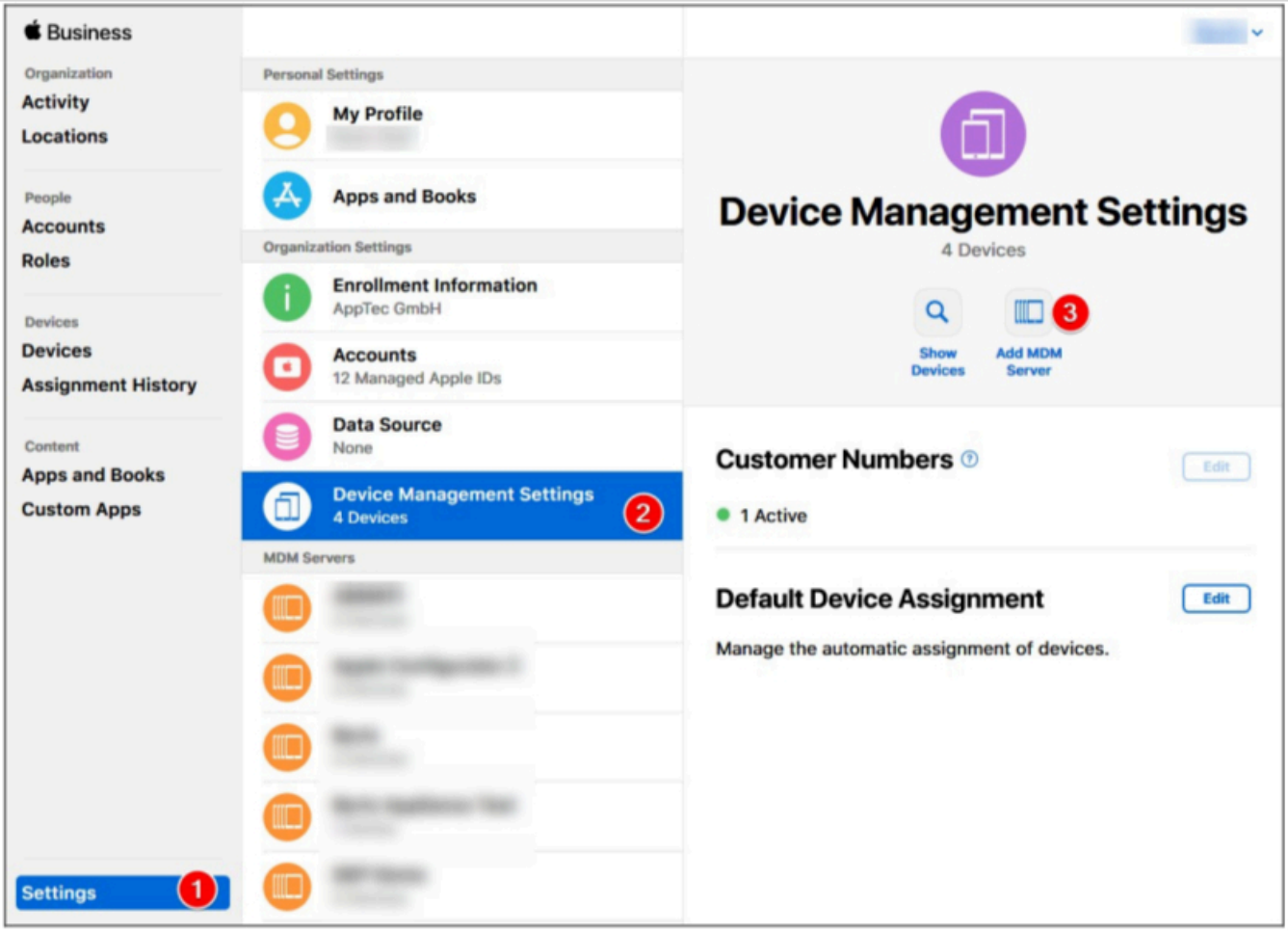
El DEP (Programa de inscripción de dispositivos) permite inscribir fácilmente dispositivos en el MDM. Al utilizar DEP, los dispositivos se conectarán automáticamente al MDM al configurar el dispositivo. También puedes saltarte casi todos los pasos de configuración que suelen ser obligatorios en iOS.

Ten en cuenta que tienes que comprar los dispositivos a un distribuidor que admita DEP. Para más información, ponte en contacto con tu distribuidor o con Apple.

Más información sobre DEP: https://www.apple.com/business/dep/

Haga clic en el signo "+" para añadir un código DEP. En la ventana emergente, haga clic en "nuevo certificado" en el texto (marcado en amarillo en la imagen inferior). Esto generará y descargará un certificado DEP. A continuación, vaya a Apple Business Manager(https://business.apple.com/) o Apple School Manager(https://school.apple.com/).

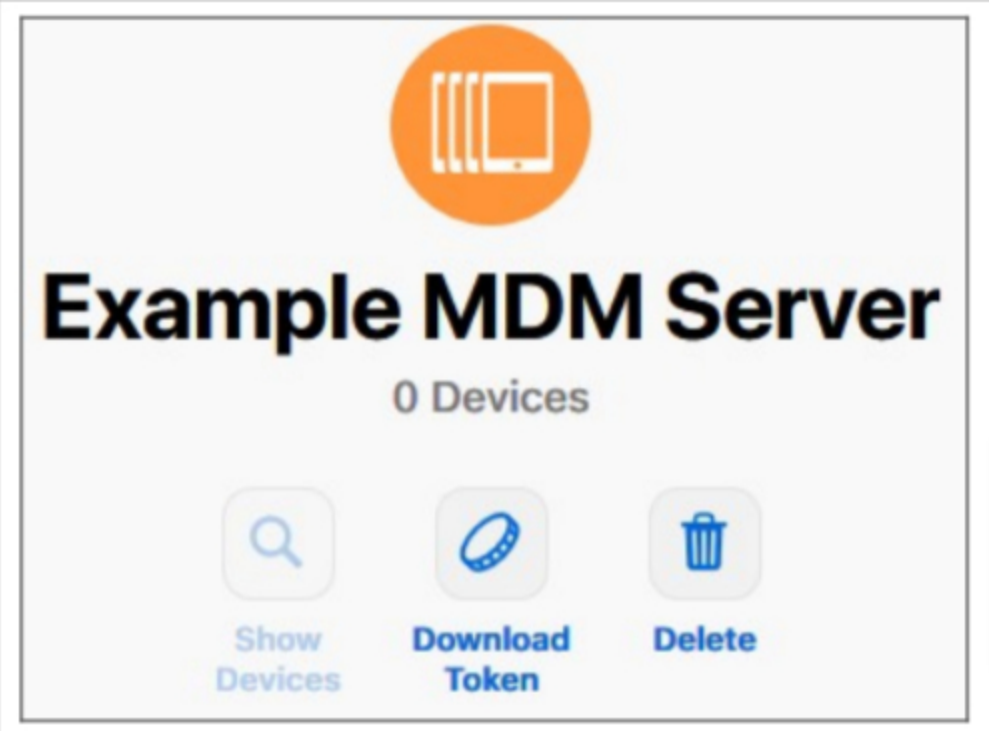




En Apple Business Manager, siga los pasos que se muestran en la imagen anterior. Ajustes → Ajustes de administración de dispositivos → Añadir servidor MDM.

Dé al Servidor el nombre que desee y cargue el Certificado DEP previamente descargado en Configuración del Servidor MDM → Cargar Clave Pública y haga clic en "Guardar".

Ahora tendrá la opción "Descargar Token". Haz clic en él y guárdalo. El vale sólo es válido durante un año. Pero con sólo hacer clic de nuevo en "Descargar Token", obtendrá uno nuevo, lo que hace que renovar el token sea muy fácil.



Ahora puede volver al MDM, donde previamente descargó el Certificado DEP. Si no cerró la pestaña, la ventana emergente para añadir un Servidor DEP debería seguir abierta y el Certificado DEP ya debería estar seleccionado. Ahora puede cargar su Token en el campo "DEP Token" y hacer clic en DEP Server.

En la columna "**Dispositivos**" verá la cantidad de dispositivos que están asignados a este Servidor DEP. Los dispositivos añadidos a este servidor DEP se crearán automáticamente en el DEP Pool de Mobile Management.

Puede hacer clic en este número para obtener una visión general de todos sus dispositivos DEP y su estado.

Nota: Dependiendo de su flujo de trabajo o configuración en el Business Manager es posible que tenga que asignar manualmente estos dispositivos al Servidor DEP. También puede establecer un servidor DEP predeterminado en Apple Business Manager para los nuevos dispositivos.

En la columna "**Perfiles**" verá la cantidad de perfiles DEP que tiene. También puede hacer clic en este número para ver los detalles de sus perfiles DEP y puede eliminar aquí los perfiles antiguos o no utilizados. Actualmente no es posible modificarlos. Si quieres hacer un cambio, tienes que crear uno nuevo.

En la columna "**Última sincronización**" puede sincronizar manualmente el DEP Server (por ejemplo, si acaba de añadir un nuevo dispositivo al DEP) y ver la fecha de la última sincronización realizada con éxito.

En la columna "**Perfil automático**" puede establecer un perfil DEP como predeterminado automático. Este perfil se asignará automáticamente a los nuevos dispositivos. Si no establece un perfil automático, tendrá que asignar manualmente un perfil a los nuevos dispositivos cada vez.

En la columna "**Añadir perfil**" puede añadir un nuevo perfil DEP. El dispositivo lo recibirá al principio de la configuración del dispositivo. El perfil DEP define cómo se configura el dispositivo y qué pasos de configuración se omitirán.

Nota: después de registrar un dispositivo, estos ajustes sólo se pueden cambiar realizando un restablecimiento de fábrica y registrando el dispositivo con un nuevo perfil. Esto es especialmente relevante para "**Extraíble**" y "**Permitir emparejamiento**". En el caso de "**Permitir emparejamiento**" se recomienda activarlo, ya que se puede desactivar mediante restricciones MDM, pero no se puede volver a activar si se desactiva en el perfil DEP.

En la columna "**Editar**" puede cargar un nuevo token, por ejemplo, al renovar el token.

Configurador y URL

URL de inscripción en el Pool

Aquí puede crear una URL de inscripción y un código QR de inscripción que sea válido una cantidad determinada de inscripciones y hasta una fecha determinada. Esto le permite inscribir varios dispositivos con un solo enlace o código QR.

Los dispositivos registrados con esta URL o código QR aparecerán en el Grupo de la Gestión de Móviles y tendrás que asignarlos manualmente a un grupo o usuario después.

Nota: esto es sólo para la inscripción manual. No utilice esta URL si inscribe los dispositivos a través de Apple Configurator

Perfil MDM – Configurador de Apple

Aquí puede obtener la URL que necesita para registrar dispositivos a través de Apple Configurator. Mientras prepara los dispositivos con el Apple Configurator, puede añadir los dispositivos al MDM en el mismo proceso. El Configurador de Apple requiere esta URL para ello.

Los dispositivos añadidos a través de Apple Configurator aparecerán en el Grupo de la Gestión de Móviles y tendrás que asignarlos manualmente a un grupo o usuario después.

También encontrará aquí un archivo .mobileconfig que se puede utilizar para registrar los dispositivos a través de Apple Configurator. En cualquier caso, se recomienda utilizar la URL.

Configuración de Android

Configuración de Android

Desinstalar Protección	Si esta función está activada, el usuario no puede desactivar el administrador del dispositivo, sin introducir la contraseña establecida por el Administrador MDM. La contraseña se establece durante la inscripción, por lo que hay que volver a inscribir los dispositivos para actualizar la contraseña. Hay dos opciones para eliminar los administradores de dispositivos: 1. Manualmente en el dispositivo ◦ Abre la aplicación EMM en el dispositivo ◦ Cambia a la pestaña Estado ◦ Toca en "Desinstalar protección". ◦ Introduce la contraseña Puedes utilizar la Revisión para obtener la contraseña correcta del "Historial de contraseñas" de la consola. ◦ Desplázate hacia abajo y toca el punto recién añadido, "Toca para desinstalar AppTec360 MDM App" (tienes 20 segundos para realizar esta tarea). ◦ Confirma el diálogo "Desinstalar AppTec360 MDM App" con "ok". Esto desinstalará el dispositivo de la consola. ◦ Para eliminar la App del dispositivo confirma el diálogo "AppTec360 MDM se desinstalará" con "DESINSTALAR" 2. el automático (Consola) ◦ Selecciona el Dispositivo en la consola ◦ Haz clic en el icono azul de engranaje y selecciona "Borrado de empresa". Nota: Sólo disponible con Android 4.x y versiones inferiores o en dispositivos con la API KNOX (dispositivos Samsung)

Contraseña de desinstalación (Revisión x)	La contraseña establecida, con la que el usuario puede eliminar al administrador del dispositivo Revisión x = contador, cuántas veces se ha cambiado ya la contraseña Es importante qué contraseña necesita el usuario, porque es posible que el dispositivo no se haya comunicado con el Servidor AppTec360 y, por tanto, no se haya transmitido aún la contraseña más reciente
Historial de contraseñas	Cuando pulses el botón azul ("Mostrar historial"), podrás ver las contraseñas establecidas anteriormente
Protección de desinstalación ampliada	Esta Opción ofrece protección contra dispositivos no seguros Mientras este ajuste esté activado, no es posible desactivar fácilmente el administrador del dispositivo
¿Pedir al usuario que desinstale las Apps bloqueadas?	Si es posible, las Apps bloqueadas no sólo se bloquearán, sino que también se desinstalarán automáticamente. Se pedirá al usuario que desinstale las Aplicaciones bloqueadas si no es posible la desinstalación automática.
Sistema Inteligente de Bloqueo de Apps	Si la Lista blanca está activada, el Cliente MDM de Android bloquea todas las aplicaciones instaladas por el usuario. Activa esta opción para bloquear todas las aplicaciones de sistema ejecutables en el modo Lista blanca.

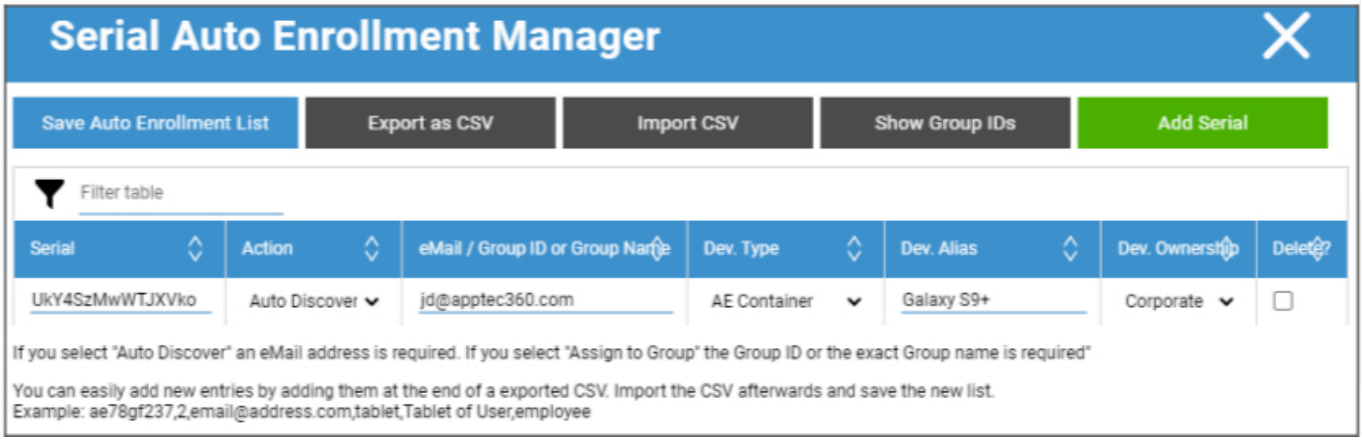
Inscripción automática

Aquí puede activar la función de inscripción automática para inscribir sus dispositivos automáticamente cuando se abra el cliente MDM de AppTec360 en el dispositivo.

Importante: Este método de inscripción está obsoleto y ya no funciona en Android 10 o superior. De todos modos, cuando se utiliza Android 7 o superior debe inscribirse dispositivos como Android Enterprise totalmente gestionado de todos modos. Si desea utilizar el contenedor BYOD de Android Enterprise y dispone de Android 10 o superior, deberá registrar manualmente el dispositivo mediante credenciales, código QR o SMS. En cualquier caso, la lista de inscripción automática se sigue utilizando para automatizar el proceso de inscripción, por ejemplo, para la inscripción AE, la inscripción Knox, etc.

En cualquier caso, la lista de inscripción automática se sigue utilizando para automatizar el proceso de inscripción, por ejemplo, para la inscripción AE, la inscripción Knox, etc.

Haciendo clic en "Serial Manager" o "IMEI Manager" puedes añadir el número de serie o el IMEI de tus dispositivos respectivamente. No es necesario hacer las dos cosas, con una es suficiente.



La **acción** define si los dispositivos se inscribirán en el grupo, en un usuario o en un grupo.

También puede exportar e importar un archivo .csv y filtrar las entradas por palabras clave.

Android para empresas

Aquí puede configurar Android Enterprise. Esto es necesario para utilizar todas las funciones de Android Enterprise.

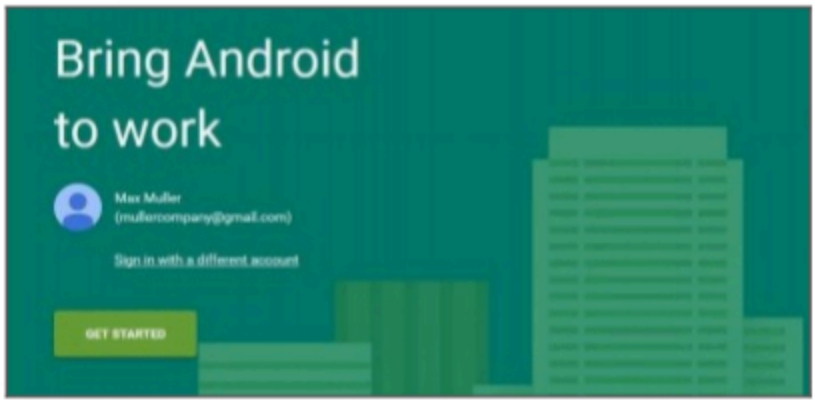
Primer método: Cuenta de empresa de Android (cuenta de Google)

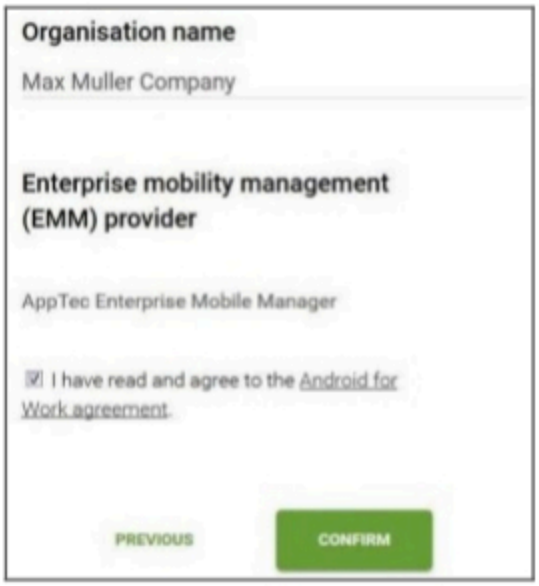
En primer lugar, pulse "Preparar configuración" y, al cabo de unos instantes, aparecerá el botón "Iniciar configuración".

Esto le llevará a la página de configuración de Android Enterprise de Google.

Inicia sesión con la cuenta de Google que quieras utilizar, si aún no lo has hecho, y pulsa "Empezar".

Ahora puede introducir el nombre de su empresa. Una vez hecho esto, marque la casilla de verificación y pulse "Confirmar".





En el último paso puede completar su registro y debe volver a la consola. Si todo funcionó debería verse así:

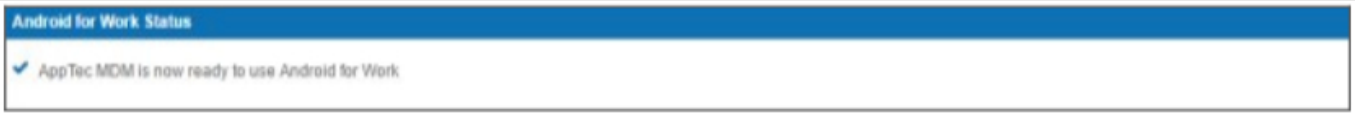
Ahora puede empezar a configurar su Android Enterprise Container.

Segundo método: Cuenta G-Suite

Pulsa "Usar G-Suite" y accede a tu cuenta de administrador de Google. Ahí vas a "Seguridad" -> "Mostrar más" -> "Gestionar proveedor EMM para Android" y generas un Token. Nota: Si no ves la configuración de Android Enterprise en tu cuenta de G-Suite, tienes que ir a "Obtener más aplicaciones y servicios" y añadir la gestión de dispositivos Android. Ahora introduzca el Token y su Dominio primario en nuestra consola y haga clic en "Guardar cambios". Cuando haya terminado, haga clic en "Usar cuenta de empresa de Android".

Ahora debería ver el botón "Crear cuenta de servicio". Haz clic en él. Este proceso puede durar unos instantes.

Si todo funcionó, debería verse así:



Ahora puede empezar a configurar su Android Enterprise Container.

Protección contra restablecimiento de fábrica

Con la protección de restablecimiento de fábrica puedes vincular tu dispositivo a una cuenta de Google de tu elección, que también anula cualquier vinculación existente a una cuenta de Google. Para utilizar la Protección de Restablecimiento de Fábrica, tienes que configurarla primero aquí y activarla después en tus perfiles.

Para configurar la Protección de Restablecimiento de Fábrica, haga clic en "Configuración FRP" y siga las instrucciones que aparecen en pantalla.

NOTA: Lea atentamente y realice los pasos. Te recomendamos que lo hagas en una nueva ventana de incógnito del navegador para evitar acceder automáticamente a la cuenta de Google incorrecta. Puedes bloquear completamente el dispositivo si introduces un ID incorrecto o pierdes el acceso a la cuenta de Google utilizada.

Inscripción AE

Aquí puedes activar la Ernolización Empresarial de Android. Usando este Método inscribirás tus Dispositivos en el Modo Propietario de Dispositivos Android Enterprise. En este modo tendrás el control total sobre el dispositivo.

Activar la inscripción AE	Activa la Inscripción AE Precaución: Si desactivas la Inscripción AE, los Códigos QR existentes y los dispositivos programadores NFC ya configurados dejarán de funcionar. Si vuelves a activar la Inscripción AE, tendrás que volver a enviar configuraciones push NFC / generar nuevos códigos QR.
Activar Descubrimiento Automático	Cuando un dispositivo se inscribe mediante "Inscripción AE", el sistema intentará asignarlo a un usuario basándose en la información establecida en la Lista blanca de serie / IMEI ("Ajustes generales" > "Configuración de Android" > "Inscripción automática").
Bloquear dispositivos desconocidos	Sólo los dispositivos que han sido incluidos en la lista blanca de serie / IMEI ("Ajustes generales" > "Configuración de Android" > "Inscripción automática") pueden registrarse.

Nota sobre los métodos 1 y 2: "Pantalla de bienvenida" se refiere a la primera pantalla que ves tras el restablecimiento de fábrica. Puede tener un aspecto diferente según la versión de Android y/o el modelo de dispositivo que estés utilizando.

Método 1: Inscripción por código QR

(requiere Android 7.0 o superior) Le recomendamos que utilice siempre este método si está ejecutando Android 7 o superior.

1. Restablecer de fábrica el dispositivo
2. Genere el código QR para la inscripción utilizando uno de los dos métodos siguientes:
    - Pulse en "Ajustes Generales -> Configuración Android -> Inscripción AE" en "Generar código QR". Elige si deseas omitir la encriptación del almacenamiento y/o si todas las aplicaciones del sistema deben ser eliminadas.
    - (alternativamente) Seleccione un dispositivo existente. En la "Vista general del dispositivo", haga clic en el código QR que aparece allí. Elige si deseas omitir la encriptación del almacenamiento y/o si todas las aplicaciones del sistema deben ser eliminadas.
3. Ahora pulse 6 veces en la pantalla de bienvenida de su dispositivo. Esto debería iniciar el Modo de Inscripción QR.
4. Ahora conéctate a una red inalámbrica y espera un poco hasta que se instale el lector de códigos QR
5. Ahora escanea el código QR

6. Ya está. Su dispositivo está ahora inscrito en el modo de dispositivo Android Enterprise.
    - a. Si ha utilizado el código QR en "Configuración general", puede encontrar su dispositivo en "Grupo -> Dispositivos del propietario del dispositivo AE". (Sugerencia: Es posible que tenga que recargar el sitio para ver los dispositivos). Si marcó "Activar Auto Discover" lo encontrará dentro de su usuario Auto Discover.
    - Si ha utilizado el código QR de un perfil de dispositivo existente, el dispositivo se inscribirá en este perfil.

Método 2: Inscripción NFC

(requiere NFC y Android 6.0 o superior)

Preparación: Introduzca su información WiFi en "Ajustes Generales -> Configuración Android -> Inscripción AE -> Datos para aprovisionamiento NFC". Ahora utiliza "Dispositivo NFC" para buscar el dispositivo que se convertirá en el programador. Este dispositivo se utilizará para enviar la información de inscripción a los demás dispositivos a través de NFC.

1. Restablecer de fábrica el dispositivo
2. Abre la aplicación de emparejamiento NFC de AppTec360 en tu programador
3. Elige si deseas omitir la encriptación del almacenamiento y/o si todas las aplicaciones del sistema deben ser eliminadas.
4. Sujeta ambos dispositivos espalda con espalda
5. Ahora, la inscripción de Android para empresas debe marcar
6. Ahora encontrarás tu dispositivo en la consola
    - a. En el pool, si no ha configurado Auto Discover
    - b. Dentro del usuario, ha configurado para el Auto Discover
    - c. Sugerencia: Es posible que tenga que recargar el sitio para ver los dispositivos

Método 3: Cuenta de Google

(requiere Android 5.1 o superior)

(Nota: Si utiliza este método, el dispositivo no se inscribirá automáticamente. En su lugar, tendrá que inscribirlo manualmente o automatizar el proceso mediante la inscripción automática).

1. Restablecer de fábrica el dispositivo
2. Sigue los pasos de configuración hasta que puedas iniciar sesión con una cuenta de Google.
3. Introduzca "afw#apptec" como Nombre de usuario/Correo electrónico
4. Pulse "Siguiente".
5. Su dispositivo es ahora un dispositivo Android para empresas

Inscripción KNOX

Aquí puedes activar la inscripción en KNOX y encontrar la información que necesitas para crear un perfil de inscripción en KNOX en el Portal de implantación de KNOX. Necesitas una Cuenta en el Portal de implantación de KNOX para configurarlo y utilizarlo.

(https://www.samsungknox.com/en/knox-deployment-program)

Activar la inscripción en KNOX	Activa la Inscripción KNOX. Atención: Si desactivas la Inscripción KNOX, los perfiles MDM existentes dejarán de funcionar. Si vuelves a habilitar la Inscripción KNOX, tendrás que actualizar el campo "Datos JSON personalizados" de tu perfil MDM
Activar Descubrimiento Automático	Cuando un dispositivo se inscribe mediante "Inscripción KNOX", el sistema intentará asignarlo a un usuario basándose en la información establecida en la Lista blanca de serie / IMEI ("Ajustes generales" > "Configuración de Android" > "Inscripción automática").

1. Inicie sesión en el portal de inscripción de Samsung KNOX Mobile https://eukme.samsungknox.com/itadmin
2. Ir a "Perfiles MDM"
3. Haga clic en "Añadir".
4. Elija "URI del servidor no requerido para mi MDM" y haga clic en "Siguiente".
5. Ahora cree un perfil con la información mostrada en la consola de gestión

Ahora este perfil de inscripción KNOX puede ser instalado directamente en el dispositivo por Samsung si usted adquiere los dispositivos de Samsung directamente.

También puede descargar la aplicación KNOX Deployment, iniciar sesión con su cuenta KNOX Deployment y enviar el perfil de inscripción KNOX a través de NFC a otros dispositivos.

Si el dispositivo tiene instalado un perfil de inscripción KNOX, descargará nuestra aplicación e inscribirá el dispositivo, si dispone de una conexión a Internet operativa.

La inscripción de dispositivos a través de KNOX Enrollment se encuentra en "Pool -> KNOX Enrollment", o dentro del usuario especificado en el Auto Discover.

Sin contacto

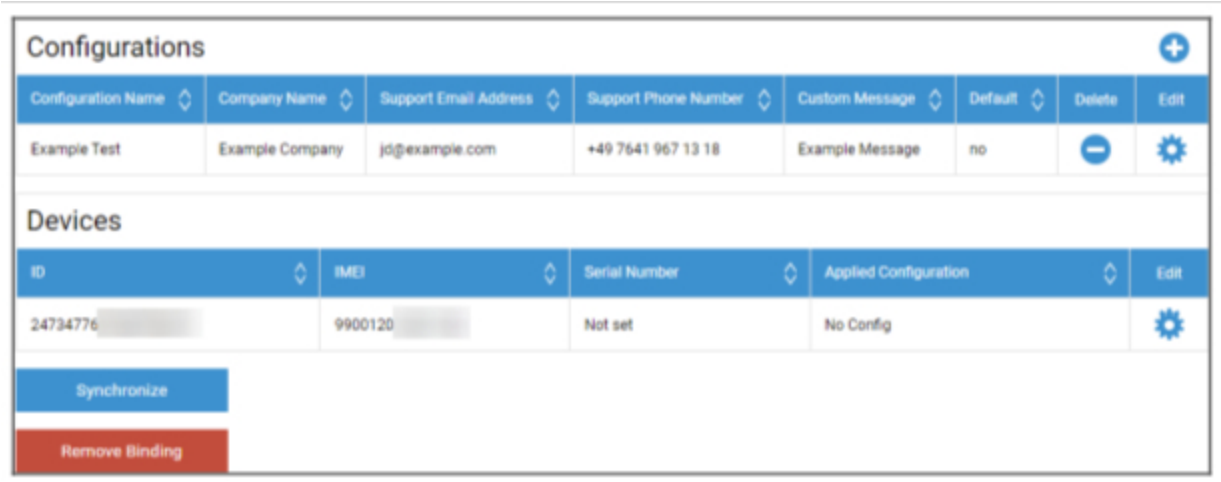
Con Zero-Touch puede registrar fácilmente sus dispositivos sin necesidad de tocarlos ni configurar nada en el propio dispositivo. Sólo tienes que encenderlo, proceder a la configuración de forma normal y el dispositivo recibirá toda la información sobre cómo configurar y conectarse al MDM de forma totalmente automática.

Para utilizar Zero-Touch tienes que comprar tus dispositivos a un distribuidor que admita Zero-Touch. El mismo revendedor también está creando una cuenta para usted en el Portal Cero Contacto. Póngase en contacto con su distribuidor para obtener más información sobre el procedimiento o si tiene problemas para acceder al portal Zero-Touch.

Haga clic en "Start Setup" para iniciar la configuración. Se te redirigirá a una página de inicio de sesión en la que tendrás que seleccionar tu cuenta de Google, que tiene acceso al Portal Zero-Touch.

NOTA: Es posible seleccionar CUALQUIER cuenta. Así que asegúrese de seleccionar la Cuenta correcta en este paso. Si no ve sus dispositivos/configuraciones, es probable que haya utilizado una cuenta incorrecta.

Una vez completado el inicio de sesión, tendrá el siguiente aspecto:



Haga clic en el signo "+" para añadir una configuración y rellene los campos que aparecen en pantalla. Si habilita la Configuración como Configuración por defecto, se asignará automáticamente a los nuevos dispositivos. Crear o establecer una configuración por defecto no la asigna a dispositivos ya existentes.

Si un dispositivo no tiene asignada ninguna configuración, se configurará como un dispositivo normal y no se conectará al MDM. Por lo tanto, asegúrese de que sus dispositivos tienen asignada una Configuración.

Una vez que hayas conectado tu Cuenta, tus dispositivos sean visibles y tengas una Configuración asignada a ellos, podrás empezar a configurar los dispositivos.

Puede añadir los dispositivos a la lista de inscripción automática para que se inscriban automáticamente en un grupo o usuario determinado. Si no ha configurado nada en la lista Inscripción automática, los dispositivos se inscribirán en el Grupo.

Configuración de Windows

Configuración de Windows

Aquí tienes la opción de habilitar las siguientes configuraciones en tu PC con Windows 10:

Conexión DM instantánea	
Tiempo de reintento inicial	Establece el primer intento de conexión con el dispositivo, este valor aumenta exponencialmente
Reintentos de conexión	Indica cuántos intentos de conexión debe realizar el cliente DM, durante un error de conexión
Tiempo máximo de sueño	Indica el tiempo máximo de reposo tras un error de conexión
Primeros intentos de sincronización	Intervalos en los que el dispositivo debe comunicarse con el servidor, tras la primera conexión
Primer intervalo de reintento	Relacionado con "Primeros reintentos de sincronización" Aquí se indican los tiempos en minutos Por ejemplo, en "Primeros reintentos de sincronización" aparece el valor "2" y en "Primer intervalo de reintentos" aparece el valor "4 minutos", de esta forma el dispositivo se comunica 2 veces cada 4 minutos, después de la primera conexión
Segundos reintentos de sincronización	Intervalos, en los que el dispositivo debe comunicarse con el servidor, tras completar los "Primeros reintentos de sincronización"
Segundo intervalo de reintento	El mismo principio que para "Primer intervalo de reintentos", sólo que aquí se aplica a "Segundos reintentos de sincronización"
Reintentos regulares de sincronización	Intervalos, de la frecuencia con la que el dispositivo debe comunicarse con el servidor en el futuro Por defecto: "Infinito" Te recomendamos que no cambies este valor, porque si introduces "10", el dispositivo se comunicará con el servidor 10 veces y luego se detendrá ¡Por lo tanto, se desconecta la comunicación con el servidor AppTec360!
Intervalo regular de reintentos	El mismo principio que para "Primer/Segundo intervalo de reintento", sólo que aquí aplica los ajustes para el futuro
Intervalo regular de reintentos	El mismo principio que para "Primer/Segundo intervalo de reintento", sólo que aquí aplica los ajustes para el futuro

ContentBox

Configuración

Aquí puedes configurar el ContentBox. Puedes colocar archivos para grupos en el ContentBox, a los que se puede acceder con la aplicación ContentBox del dispositivo.

Activar ContentBox	Activar ContentBox. Desactivarlo si no utilizas ContentBox, puede ahorrar recursos en las máquinas OnPremise.
Utilizar una instalación externa de ContentBox	El ContentBox también puede funcionar con tu propio Nextcloud.
URL	URL completa de la entidad Nextcloud
Usuario raíz	Usuario raíz de la cuenta Nextcloud
Contraseña raíz	Contraseña raíz de la cuenta Nextcloud
Permisos de carpeta de grupo por defecto	Permisos de carpeta de grupo por defecto, pueden modificarse individualmente por grupo (en Gestión de Móviles)
Compartir carpeta de grupo con subgrupos	Si está activo, cada subgrupo puede leer todas las carpetas del grupo principal, también se puede configurar individualmente para cada grupo (Gestión de Móviles)
Permisos para subgrupos	Permisos para subgrupos se puede configurar individualmente para cada grupo (Gestión de Móviles)
Permitir compartir	Permite al usuario compartir el contenido a través de Enlaces, puede configurarse individualmente para cada grupo
Tamaño máximo de subida de archivos en MB	Tamaño máximo de un archivo Estándar: 512 MB Configuración máxima: 2048
Credenciales WebDAV	
URL WebDAV	También puedes abrir la ContentBox con WebDAV. Por favor, no elimines las siguientes carpetas, bajo ningún concepto: /apptecgroups /apptecgroups/AppTecGroup-X
Usuario raíz	Nombre de los usuarios raíz
Contraseña	Contraseña de los Usuarios Raíz

La sincronización con la ContentBox se produce automáticamente. Sin embargo, puedes realizar una sincronización manual con "Sincronizar ContentBox".

Además, aquí puedes activar/desactivar el ContentBox en cada dispositivo individual.

Esto sólo es relevante, si usted no ha licenciado adicionalmente el ContentBox, entonces usted todavía tiene acceso a 25 dispositivos con los que puede probar el ContentBox - aquí usted puede activar esto para los dispositivos respectivos.

Configuración LDAP

Visión general de LDAP

Aquí puedes establecer una conexión con tu Directorio Activo mediante LDAP para importar en masa usuarios y grupos. La sincronización debe realizarse manualmente. Puedes configurar varias conexiones LDAP a diferentes sistemas o con diferentes configuraciones/filtros.

Nombre del servidor	El nombre para mostrar del servidor
Tipo	Actualmente sólo se admiten los Directorios Activos que soportan LDAP
Dominio LDAP	El dominio LDAP principal (por ejemplo, ejemplo.com)
Anfitrión LDAP	Sólo es necesario si no se puede acceder al host LDAP en el dominio LDAP indicado.
Puerto	Déjalo vacío para utilizar el puerto estándar (389 o 636 para SSL)
Nombre de usuario	Por ejemplo: CN=John,OU=Usuarios,DC=EXAMPLE,DC=COM Nota: La mayoría de los sistemas requieren el nombre de usuario en este formato y no aceptan "John" como nombre de usuario
Contraseña	
Confirmar contraseña	
Seguridad de la conexión	Nota: cuando utilices SSL o TLS, se comprobará el certificado del Directorio Activo. Si está autofirmado, tienes que añadir la CA raíz al almacenamiento de confianza de la máquina local. Si estás en la Nube, el Directorio Activo tiene que proporcionar un certificado de confianza o la conexión sólo funcionará sin Encriptación.
Sincronización automática.	Activa la sincronización automática del directorio LDAP en el intervalo de tiempo especificado en la configuración general de LDAP.
Base DN	Si no quieres sincronizar todo el directorio, puedes especificar aquí una OU.Ej. OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM
Miembro de	Todos los usuarios importados se añadirán al grupo seleccionado
¿Sólo usuarios activados?	Cuando esté activado, se tendrá en cuenta el atributo userAccountControl, los usuarios sin ese atributo no se importarán.
Filtro LDAP	Puedes utilizar el Filtro LDAP para filtrar qué Usuarios se importan
Filtro Regex	Puedes utilizar el Filtro Regex para filtrar qué Usuarios se importan

Conexión de prueba	Prueba la conexión al guardar la configuración
¿Restablecer la estructura de directorios en la sincronización?	Si es verdadero, todas las entradas LDAP se moverán a su ubicación original en el árbol LDAP. Se recomienda activarlo.
¿Reimportar usuarios y grupos eliminados?	Si está activada, se volverán a crear los usuarios y grupos que se hayan eliminado. Se recomienda activarlo.
¿Sincronizar eliminaciones?	Si se activa, los grupos y usuarios se eliminarán cuando se borren en el servidor LDAP. También se borrarán los dispositivos de los usuarios eliminados.

Debajo de la lista de tus Configuraciones LDAP puedes definir el periodo en el que el sistema se sincronizará automáticamente. Sólo utiliza para la sincronización automática las Configuraciones LDAP que tengan activada la opción correspondiente.

Gestión de aplicaciones

Aplicación interna DB

Android

Aquí puede cargar las aplicaciones Android que su empresa ha desarrollado y distribuirlas posteriormente en Mobile Management en perfiles de dispositivo o grupo.

Tenga en cuenta que le aconsejamos que sólo distribuya de este modo aplicaciones que no estén disponibles en Google Play Store.

Haz clic en el "+" para subir el APK de una App que quieras subir. Actualmente sólo se admite el formato APK.

El límite de carga de los dispositivos locales puede aumentarse en el paso 3 de la configuración del dispositivo. Si desea aumentar el límite de carga en la nube, póngase en contacto con el servicio de asistencia para obtener más información.

Ten en cuenta que normalmente los APK son un poco más pequeños que su contenido. Es posible que una subida falle debido a esto, ya que el APK se descomprime en el proceso. Por ejemplo, es posible que un APK de 95 MB falle con un límite de carga de 100 MB. En este caso, aumente el límite de carga como se ha mencionado anteriormente.

También te aconsejamos que primero muevas manualmente el APK a un dispositivo de prueba (por ejemplo, a través de USB) e intentes instalarlo manualmente con la aplicación Archivos del dispositivo. Si esto no funciona por alguna razón, también fallará a través de MDM.

Objetivo de actualización

Con la función "Actualizar destino" puedes elegir qué versión de una aplicación debe instalarse o a qué versión debe actualizarse una aplicación si has activado "Mantener al día" para una aplicación.

Si no ha seleccionado un objetivo de actualización, se utilizará la versión más alta.

Ten en cuenta que Android no puede degradar aplicaciones. Tenga en cuenta también que el "Código de versión" determina si una versión es superior, inferior o la misma. Así que asegúrese de aumentar correctamente esta versión en su aplicación al crear una actualización.

iOS

Aquí puedes subir las aplicaciones iOS que has desarrollado y distribuirlas más tarde en Mobile Management en el perfil de tu dispositivo o grupo.

Haz clic en el "+" para cargar el IPA de una App que quieras subir. Por ahora sólo se admite el formato IPA.

El límite de carga de los dispositivos locales puede aumentarse en el paso 3 de la configuración del dispositivo. Si desea aumentar el límite de carga en la nube, póngase en contacto con el servicio de asistencia para obtener más información.

Objetivo de actualización

Con la función "Actualizar destino" puedes elegir qué versión de una aplicación debe instalarse o a qué versión debe actualizarse una aplicación si has activado "Mantener al día" para una aplicación.

Si no ha seleccionado un objetivo de actualización, se utilizará la versión más alta.

MacOS

Aquí puede cargar las aplicaciones macOS que haya desarrollado y distribuirlas posteriormente en Mobile Management en su perfil de dispositivo o grupo.

Haga clic en el signo "+" para cargar el PKG de una aplicación que desee cargar. Por ahora sólo se admite el formato PKG.

El límite de carga de los dispositivos locales puede aumentarse en el paso 3 de la configuración del dispositivo. Si desea aumentar el límite de carga en la nube, póngase en contacto con el servicio de asistencia para obtener más información.

Objetivo de actualización

Con la función "Actualizar destino" puedes elegir qué versión de una aplicación debe instalarse o a qué versión debe actualizarse una aplicación si has activado "Mantener al día" para una aplicación.

Si no ha seleccionado un objetivo de actualización, se utilizará la versión más alta.

Windows 10

Aquí puedes subir las Windows 10 Apps y distribuirlas más tarde en Mobile Management en el perfil de tu dispositivo o grupo.

Haz clic en el "+" para subir el APPX, APPXBUNDLE o MSI de una App que quieras subir. Por ahora sólo se admite el formato APPX, APPXBUNDLE o MSI.

También puede cargar y definir Dependencias para una App, que se distribuirán e instalarán automáticamente antes de instalar la App deseada.

El límite de subida en los Dispositivos Locales puede aumentarse en el Paso 3 de la Configuración del Dispositivo. Si quieres aumentar el Límite de subida en la Nube, ponte en contacto con el soporte para obtener más información.

Objetivo de actualización

Con la función "Actualizar destino" puedes elegir qué versión de una aplicación debe instalarse o a qué versión debe actualizarse una aplicación si has activado "Mantener al día" para una aplicación.

Si no ha seleccionado un objetivo de actualización, se utilizará la versión más alta.

Paquete Win32 (.exe)

También puedes distribuir archivos .exe/instaladores a tus dispositivos.

Nombre del paquete	El nombre que se mostrará en el MDM
Descripción	Descripción mostrada en el MDM
Archivo del paquete	Sólo se permiten archivos .zip. Coloca los archivos que quieras desplegar en este archivo zip.
Contexto de despliegue	**Sistema**: El comando de instalación se ejecuta con privilegios de sistema, que son superiores a los de "Usuario". Además, cuando se utiliza "Sistema", el proceso no tiene interfaz de usuario, por lo que será silencioso y no se podrá acceder al perfil de usuario, por ejemplo, a variables de entorno como %AppDat%. **Usuario**: El comando de instalación tiene acceso al perfil de usuario y puede mostrar la IU si es necesario. Nota: Algunos procesos sólo pueden funcionar en un contexto. Por ejemplo, si un programa se instala en AppData, sólo funcionará al seleccionar "Usuario".
Comando de instalación	El comando utilizado para instalar el programa. Por ejemplo, el comando de instalación de un archivo zip que contiene "setup.exe" en su raíz, que admite el parámetro "/s" para una instalación silenciosa, el comando de instalación sería "setup.exe /s". Ten en cuenta que los distintos programas pueden tener parámetros diferentes.
Comando de desinstalación	El comando a ejecutar para desinstalar el software a través de MDM. Normalmente apunta al desinstalador. Por ejemplo, "C:\Archivos de Programa\N-EjemploSoftware\uninstall.exe".
Requisitos	
Nota: Deben cumplirse todos los requisitos establecidos para que se instale el software. De lo contrario, no se instalará. Algunos campos pueden ser obligatorios. Si no se establece ningún valor para un requisito, éste se ignorará.	
Arquitectura del SO	Arquitectura del SO
Versión mínima del SO	Versión mínima del SO
Espacio libre mínimo en disco (MB)	Espacio libre mínimo en disco (MB)
Memoria física mínima (MB)	Memoria física mínima (MB)

Número mínimo de procesadores lógicos	Número mínimo de procesadores lógicos
Velocidad mínima de la CPU (MHz)	Velocidad mínima de la CPU (MHz)
Requisitos adicionales	Si lo deseas, también puedes definir reglas manualmente o cargar un script aquí para realizar comprobaciones de requisitos adicionales.
Reglas de detección	
Método de detección	Aquí puedes definir cómo detectar si la app está instalada en el dispositivo. Los comandos de instalación sólo se ejecutarán cuando estas reglas detecten que la app NO está instalada. Los comandos de desinstalación sólo se ejecutarán cuando estas reglas detecten que la app no está instalada. **Definir reglas manualmente**: Te permite definir manualmente una o varias reglas para comprobar, por ejemplo, si está presente un determinado archivo, carpeta, MSI o clave del registro. Si todas las reglas de detección dadas son verdaderas, se considerará que la app está presente. **Utilizar script**: Sube tu propio script con tus propias comprobaciones. Si el script devuelve "$TRUE", la aplicación se considerará presente.
Reglas de detección	

Configuración de la aplicación

Ajustes de la aplicación iOS

Aquí puede definir la configuración predeterminada para añadir una aplicación a las aplicaciones obligatorias o a la tienda de aplicaciones de la empresa.

Nota: Esto sólo establece lo que se selecciona por defecto al añadir aplicaciones. Esto NO cambia la configuración existente para las aplicaciones que ya están añadidas en las aplicaciones obligatorias o en la tienda de aplicaciones de la empresa.

Mantente al día	Mantiene la aplicación actualizada automáticamente. Ten en cuenta que pueden pasar hasta 7 días desde que se publica una actualización hasta que se actualiza la aplicación.
Adelantar cuando no se gestiona	Si una aplicación ya está instalada como no gestionada (por el usuario), la aplicación será superada y gestionada por el MDM.
Eliminar la app cuando se elimina el perfil MDM	Desinstala la App cuando se elimina el MDM.
Evitar la copia de seguridad de los datos de la app	Impide la copia de seguridad de los datos de la app.

Ajustes de la aplicación Android

Aquí puede definir la configuración predeterminada para añadir una aplicación a las aplicaciones obligatorias o a la tienda de aplicaciones de la empresa.

Nota: Esto sólo establece lo que se selecciona por defecto al añadir. NO cambia la configuración de las aplicaciones ya añadidas en la tienda de aplicaciones obligatorias o de empresa.

Mantente al día	Mantiene la aplicación actualizada automáticamente. Sólo disponible para InHouse Apps.
Actualización controlada del cliente EMM de AppTec360	Si está activada, los administradores pueden especificar el objetivo de actualización para el Cliente EMM de AppTec360. Se mostrará una lista de todas las versiones disponibles del Cliente EMM de AppTec360 en "Configuración general" → "Gestión de aplicaciones" → "Base de datos de aplicaciones internas" → "Android".

Aplicaciones de terceros

Android

Aquí puede establecer su código de activación para Ikarus.

Seleccione "Usar código de activación" e introduzca aquí su código de activación.

Nota: Después de introducir el código y guardarlo, el código aún no se añade al perfil que se envía al dispositivo. Tienes que realizar cualquier cambio en tu perfil para que el código se añada al perfil. Por ejemplo, cambiar cualquier Interruptor del Perfil de desactivado → activado → desactivado - Guardar → Asignar ahora.

iOS

Aquí puede introducir su licencia SecurePIM. Tras introducir la licencia, pulse "Guardar cambios" y podrá utilizar las opciones de SecurePIM.

VPP / KNOX Premium

El Programa de Compras por Volumen (VPP) de Apple le permite distribuir fácilmente aplicaciones de pago y gratuitas a sus dispositivos. Esto es muy recomendable ya que no necesitas un ID de Apple en los dispositivos, los usuarios no tienen que confirmar la instalación (supervisada), los usuarios no tendrán que introducir la contraseña del ID de Apple y puedes distribuir fácilmente Apps de pago sin comprarlas de nuevo en cada Dispositivo.

Para utilizar el VPP tienes que registrarte en el Apple Business Manager.

Licencias VPP

Aquí puede obtener una visión general de sus aplicaciones VPP, cuántas licencias se utilizan y cuántas están disponibles.

Haciendo clic en la Rueda podrá ver qué dispositivos tienen una Licencia asignada y cuál es el Estado de esta Asignación.

Al hacer clic en se actualiza la caché VPP que compara las licencias asignadas en el MDM con las licencias asignadas en el lado de Apple. Esto puede resolver los problemas de licencia en algunos casos.

Ficha VPP

Aquí puedes cargar tu token VPP, que se encuentra en Apple Business Manager en Ajustes → Aplicaciones y libros. Puede cargar varias fichas VPP.

Para renovar un token, basta con descargar uno nuevo en Apple Business Manager, hacer clic en la rueda "Editar" y cargar el nuevo.

El "Modo VPP" decide cómo se gestiona la asignación de licencias. En función del escenario, deberás utilizar distintos modos:

"Basado en dispositivo" debe utilizarse al registrar los dispositivos mediante código QR, Link, Apple Configurator o DEP.

"Basado en usuario" es necesario si los dispositivos están inscritos con la inscripción de usuario o como iPad compartidos.

Si activa la "Gestión automática de licencias", a los usuarios que se trasladen de un grupo a otro se les asignarán automáticamente licencias Apple VPP en función del perfil de grupo al que se trasladen.

Las licencias Apple VPP existentes del grupo del que se han trasladado no se revocarán.

A los nuevos usuarios añadidos a un grupo se les asignarán automáticamente licencias VPP de Apple basadas en el perfil del grupo respectivo.

Llave KNOX Premium

Aquí puede introducir su clave KNOX Premium para utilizar el Samsung KNOX Container.

Tenga en cuenta que esto ya no es compatible desde Android 10. Utilice en su lugar el Android Enterprise Container.

Configuración de App Store

Región e idioma

Aquí puede establecer el idioma y la región predeterminados para la búsqueda de aplicaciones en App Management.

Ten en cuenta que la configuración de iTunes también define el modo en que el sistema obtiene información sobre determinadas aplicaciones. Si encuentra aplicaciones en sus listas que se muestran de una manera extraña (por ejemplo, falta el icono) es posible que haya establecido una región en la que la aplicación específica no está disponible.

AE Play Store

Aquí puede encontrar todas las opciones de Play Store para dispositivos Android Enterprise para aprobar aplicaciones, subir sus propias aplicaciones a Play Store o crear sus propias aplicaciones web.

Aplicaciones aprobadas

Aquí puede obtener una visión general de todas las aplicaciones que ha aprobado.

Aplicaciones Play Store

Esto cargará un iFrame mostrando la Play Store. Busca la App que quieras, haz clic en ella y apruébala. Al aprobar la aplicación, también puede definir que la aprobación se revoque si cambian los permisos requeridos. Recomendamos dejar estos ajustes por defecto al aprobar aplicaciones.

Una vez aprobada una aplicación, puede añadirla a sus perfiles.

El botón "Aprobar" cambiará a "Revocar aprobación" después de aprobarla, por lo que siempre podrás eliminar las Apps si ya no las necesitas.

Aplicaciones privadas

Aquí puedes subir tu propia App como App privada a Google Play Store. Esto le permite distribuir la aplicación a través de los servicios de Google y actualizarla a través de ellos. Esto también tiene la

ventaja de que sus propias aplicaciones se pueden instalar sin la confirmación del usuario que normalmente es necesaria.

Aplicaciones web

Aquí puede crear Web Apps, que son enlaces a determinadas Páginas Web que pueden asignarse como Apps.

También puede darle un icono personalizado y definir cómo se muestra exactamente.

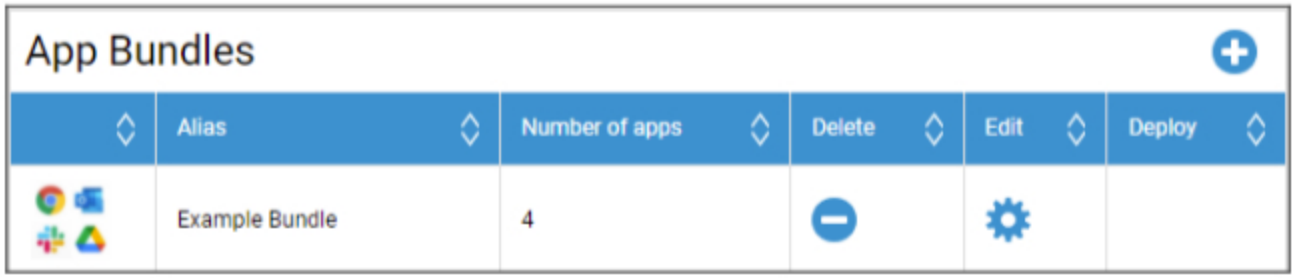
Diseño de la tienda

El diseño de la tienda define cómo se muestran las aplicaciones en Play Store o si se muestran.

Ten en cuenta, que si quieres mostrar Apps en la Play Store para que el usuario las instale manualmente, estas tienen que ser añadidas aquí en el Layout **Y** en el perfil a la Play Store de la empresa. Si añade una aplicación sólo a una de ellas, no se mostrará.

Paquete de aplicaciones

Con App Bundles puedes definir grupos de aplicaciones que pueden asignarse a perfiles de dispositivos o grupos con un solo clic.



Haga clic en "+" para crear un nuevo App Bundle. Después de crear un paquete de aplicaciones, puede hacer clic en "Editar" para añadir aplicaciones de varias fuentes al paquete.

Se puede añadir un Bundle a los perfiles como cualquier otra App. Al añadir aplicaciones tendrás una pestaña extra llamada "App Bundles" donde tendrás tus Bundles.

Si realiza algún cambio en un App Bundle aparecerá un botón en la columna "Deploy". De este modo, podrá aplicar los cambios a todos los perfiles que contengan este paquete. Así que ten en cuenta que tienes que hacer esto manualmente después de añadir o eliminar aplicaciones en un Bundle.

Mando a distancia

TeamViewer

Conector TeamViewer

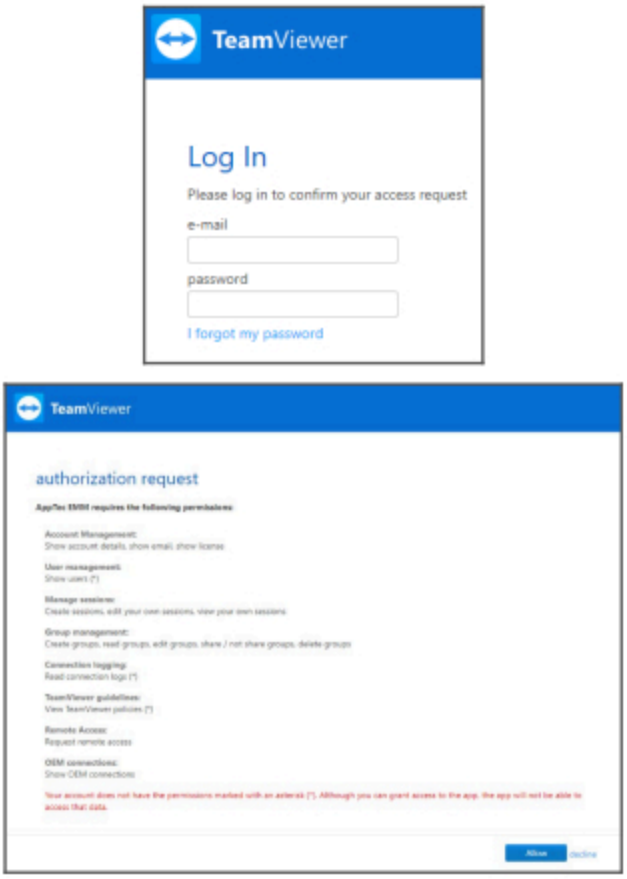
Nota: En la versión de prueba gratuita de nuestra versión en la nube no podrá conectar su cuenta de TeamViewer. En su lugar, se le vinculará automáticamente una cuenta de demostración gratuita.

Vaya a Configuración General -> Control Remoto -> TeamViewer. Aquí puede vincular su cuenta de TeamViewer con la consola o ver información sobre su cuenta actualmente conectada. También puede ver todas las sesiones activas si va a "Sesiones activas".

Para vincular su cuenta, haga clic en "Iniciar configuración".

Al hacerlo, accederá a una nueva página en la que deberá iniciar sesión con su cuenta de TeamViewer.

Después de iniciar sesión, ha autorizado a AppTec360 MDM a utilizar esta cuenta. Tras confirmarlo, hay que esperar unos segundos y la Cuenta estará conectada.


TeamViewer
Log In
Please log in to confirm your access request
e-mail
password
I forgot my password
TeamViewer
authorization request

Instalar TeamViewer QuickSupport

Añada la aplicación "TeamViewer QuickSupport" a las aplicaciones obligatorias de su perfil de dispositivo o perfil de grupo y haga clic en "Asignar ahora". Espere a que la aplicación se instale en el dispositivo.

Si intentas acceder a un dispositivo en el que la aplicación no está instalada, se instalará o se pedirá al usuario que la instale, dependiendo de la configuración del dispositivo.

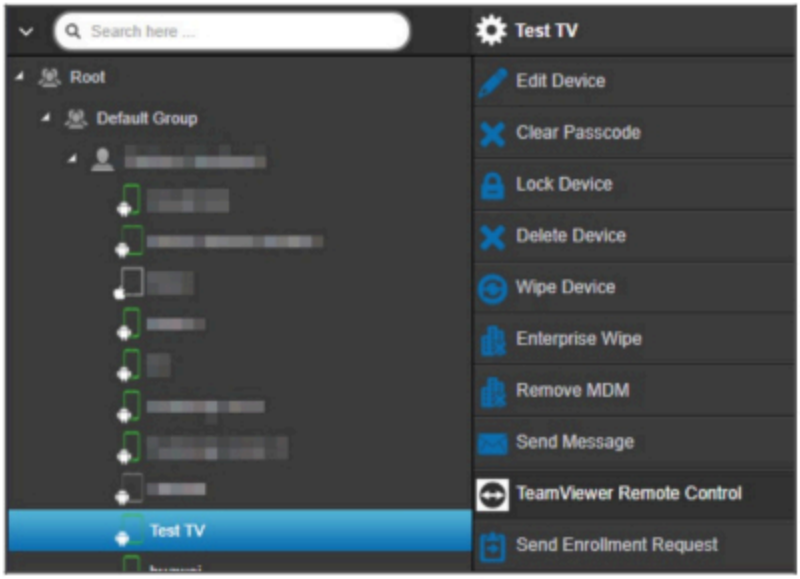
Controla tu dispositivo a distancia

Para controlar a distancia su dispositivo, seleccione el dispositivo, haga clic en la rueda y elija "TeamViewer Remote Control".

Si ya hay una sesión activa, puede utilizar la sesión antigua o crear una nueva.

Confirme que desea crear una nueva sesión de TeamViewer.

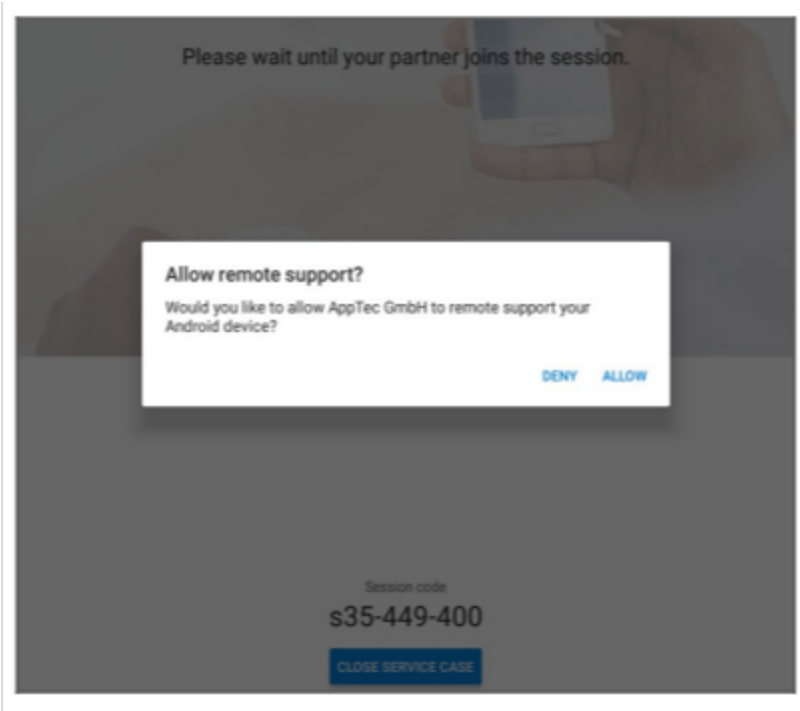
Después de unos segundos obtendrá un enlace para su sesión de TeamViewer. Puede hacer clic en "Inicio" para abrir este enlace en una nueva ventana.


Search here ...
Root
Default Group
Test TV
Test TV
Edit Device
Clear Passcode
Lock Device
Delete Device
Wipe Device
Enterprise Wipe
Remove MDM
Send Message
TeamViewer Remote Control
Send Enrollment Request


Remote Control
Supporter URL: https://get.teamviewer.com/v13/
Click on "Start" to open the TeamViewer Remote Control in a new window.
Cancel
Start

Este enlace abrirá su TeamViewer instalado y le conectará a su dispositivo.

Ahora tienes que confirmar la conexión en el propio dispositivo para controlarlo a distancia.

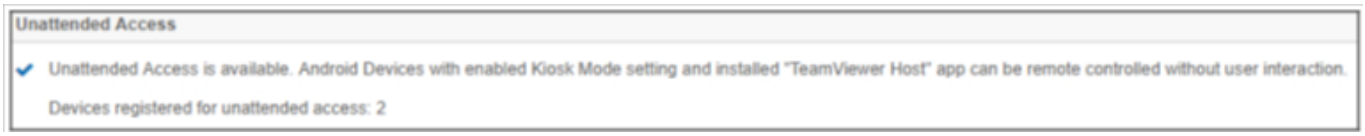


Si utiliza iOS, aparecerá un mensaje en el cliente MDM de AppTec360. Con ese enlace el dispositivo se unirá a la sesión remota. Dependiendo de la configuración de notificaciones del dispositivo es posible que no reciba una notificación y tenga que abrir el AppTec360 MDM Client manualmente.

En algunos dispositivos Android (por ejemplo, Samsung) es necesario instalar una aplicación adicional como complemento. La aplicación TeamViewer en el dispositivo le informará al respecto, si esto es necesario en su dispositivo.

Acceso sin vigilancia

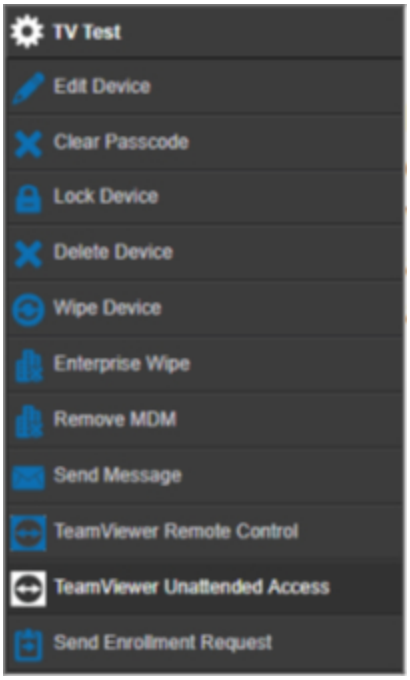
Nota: El acceso desatendido sólo es posible en dispositivos Android.



Sólo puede conectarse a sus dispositivos, sin aceptar la conexión en el dispositivo, si su cuenta TeamViewer utiliza una licencia "Tensor" o "Corporate".

Puede comprobarlo, tras vincular su cuenta, en "Ajustes generales".

Para utilizar el acceso desatendido, debe instalar la aplicación "TeamViewer Host" y activar "Activar acceso desatendido" en "Modo Quiosco y Lanzador" en su perfil. Tenga en cuenta que esto sólo es posible si utiliza el Modo Quiosco.



Ahora puedes seleccionar el acceso desatendido si seleccionas tu dispositivo y haces clic en la rueda. Esto le conectará a su dispositivo sin necesidad de confirmación en el propio dispositivo. Tenga en cuenta que puede tardar unos instantes hasta que obtenga el enlace para acceder a su dispositivo.

Splashtop

Si activa la opción Splashtop, verá las opciones de configuración de Splashtop en sus perfiles.

Para utilizar Splashtop, tienes que establecer Splashtop Streamer (com.splashtop.streamer.csrs) como aplicación obligatoria en tu perfil. Después puedes activar la Configuración Splashtop en tu perfil en "Control Remoto". Al activar esta opción, se configurará la aplicación Splashtop Streamer. Si está utilizando Splashtop Streamer pero no en combinación con el MDM, debe dejar esta opción desactivada.

En tu perfil, en "Control remoto", también tienes que establecer un código de despliegue. Vaya a https://my.splashtop.com y acceda a su cuenta Splashtop. Haga clic en "Añadir ordenador" y copie el código de despliegue de 12 dígitos de la página resultante.

Sin el código de despliegue NO es posible el control remoto.

Una vez hecho esto, puedes hacer clic con el botón derecho del ratón en tu dispositivo e iniciar una sesión remota haciendo clic en "Splashtop Remote Control".

Gestión de tarjetas Sim

Importación masiva de CSV

Muestra un resumen de las tarjetas SIM asignadas y toda la información sobre ellas. Esto le ayuda a tener toda la información, no sólo acerca de sus dispositivos, sino también acerca de sus tarjetas SIM en un solo sistema.

NOTA: Se trata de una gestión/documentación manual. No es posible obtener estos datos automáticamente de los dispositivos debido a los mecanismos de privacidad/seguridad de los sistemas operativos.

También puede exportar e importar esta lista como CSV.

Transportista y tarifa

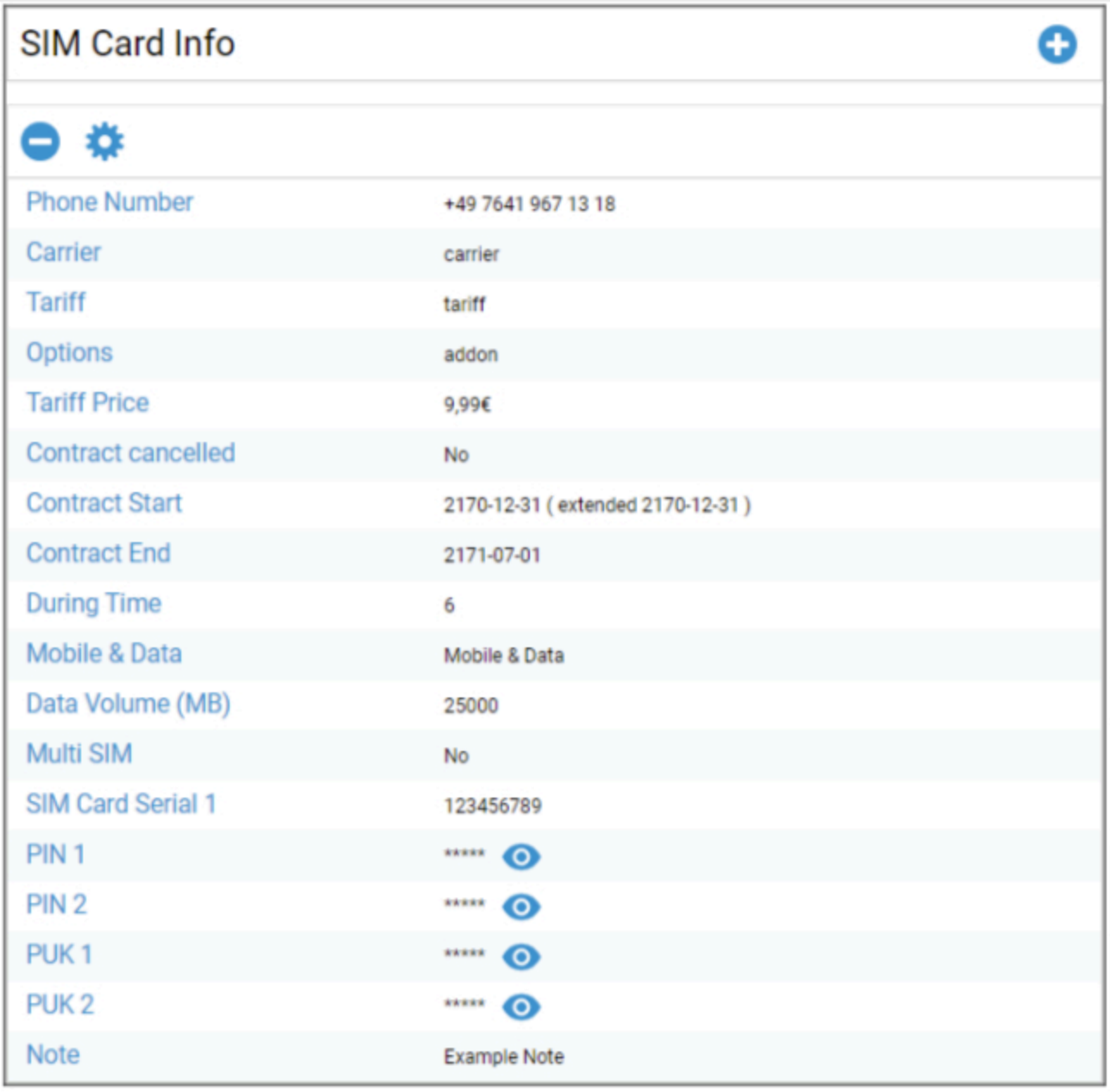
Para añadir una tarjeta Sim, primero haga clic en el botón para añadir uno o varios operadores.

A continuación, haga clic en el signo "+" de "Información sobre tarifas" para añadir una tarifa a un transportista.

Opcionalmente puede añadir Add-Ons opcionales abajo si tiene algo como esto.

Esto preparó todo lo necesario para añadir una tarjeta Sim real. Las tarjetas Sim están actualmente asignadas a un usuario. Por lo tanto, vaya a la Gestión de Móviles, seleccione un Usuario y vaya a "Visión General de la Tarjeta Sim".

Aquí puedes ver las tarjetas Sim de estos usuarios. Si hay alguna, puede editarla o eliminarla. Los usuarios pueden tener varias tarjetas Sim.

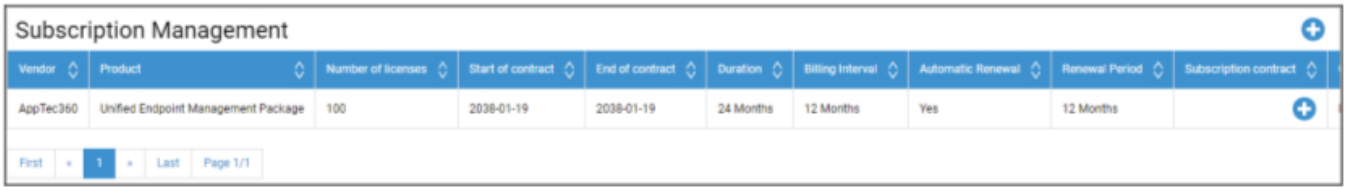


Haz clic en "+" para añadir una tarjeta SIM y añade toda la información que necesites. Estas tarjetas SIM también aparecerán en la lista de todas sus tarjetas SIM en Ajustes generales → Gestión de tarjetas SIM.

Gestión de suscripciones

Gestión de suscripciones

Aquí puede documentar las suscripciones en curso, sus detalles y también almacenar diferentes archivos, por ejemplo, el contrato firmado, la carta de rescisión, etc. También puedes configurar recordatorios que te avisen por correo antes de que finalice la suscripción y que quizá se amplíe automáticamente.



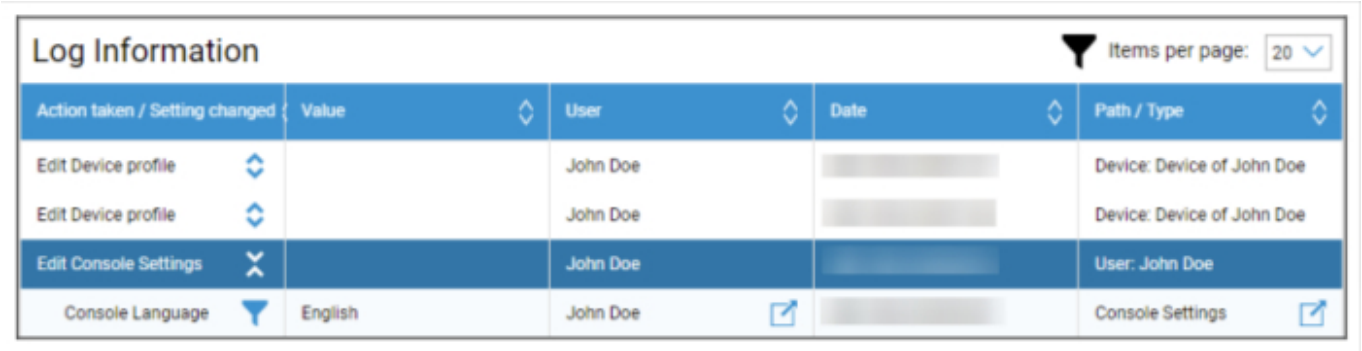
Haga clic en el signo "+" de la parte superior para añadir una suscripción. Puede añadir tantas suscripciones como desee.

Haga clic en el signo "+" en los diferentes campos para cargar archivos relativos a esta Suscripción. Técnicamente puedes subir cualquier tipo de archivo, pero ten en cuenta que no todos los tipos de archivo pueden previsualizarse en el navegador.

Registro general de auditoría

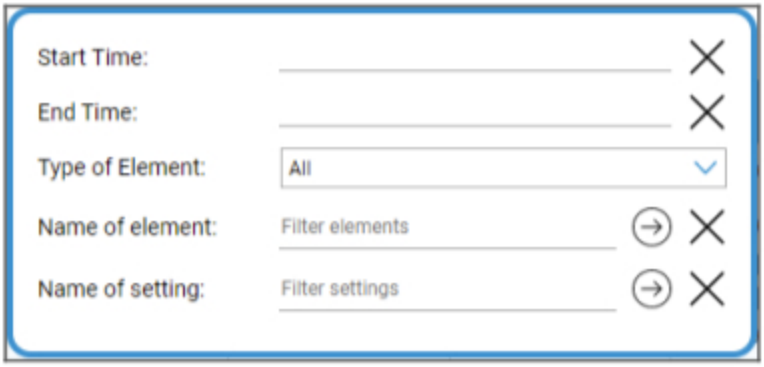
Registro de auditoría

Aquí tiene un registro de auditoría general que muestra todos los cambios realizados. Mientras que el Registro de Auditoría de un usuario o grupo sólo muestra los cambios según este usuario o grupo, esto muestra TODOS los cambios realizados en cualquier parte de la consola.



Puede ver qué se ha modificado, quién lo ha hecho, cuándo y dónde. En algunos casos también puede ampliar la Entrada para ver más detalles.

Es posible hacer clic en el usuario o en la entrada en "Ruta / Tipo" para llegar a la ubicación donde se ha realizado el cambio.



En la parte superior derecha también se puede definir un filtro que puede ayudar a encontrar determinados cambios en un entorno en el que se están produciendo muchos cambios.

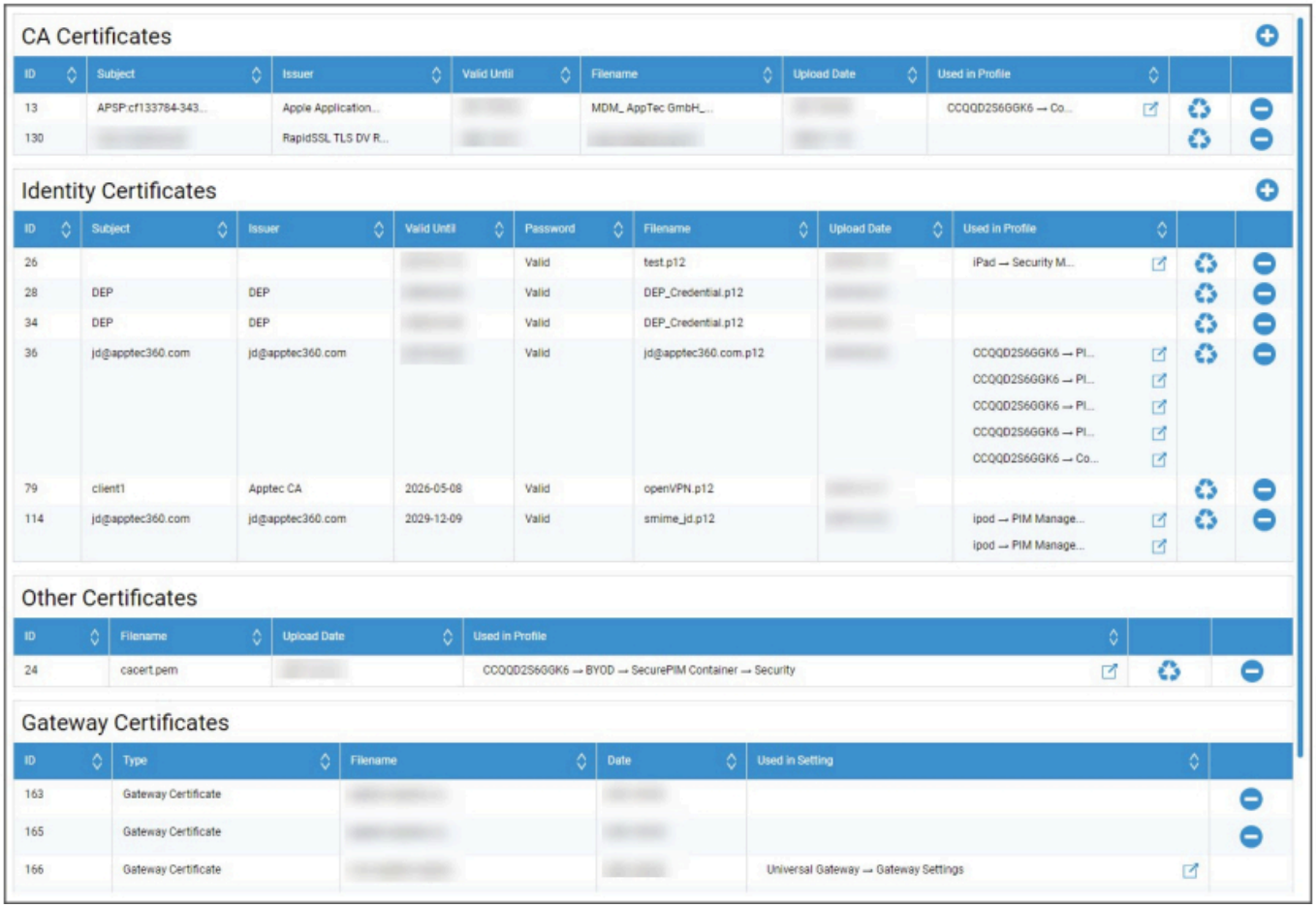
Configuración del registro de auditoría

"Periodo de Retención de Registros de Auditoría" define cuánto tiempo deben conservarse los Registros de Auditoría antes de su eliminación.

Gestión de certificados

Aquí obtendrá una visión general de todos los certificados cargados y utilizados en la Consola. Esto es sólo una visión general. La configuración real para, por ejemplo, los certificados Wi-Fi se sigue realizando en el perfil en la ubicación correspondiente.

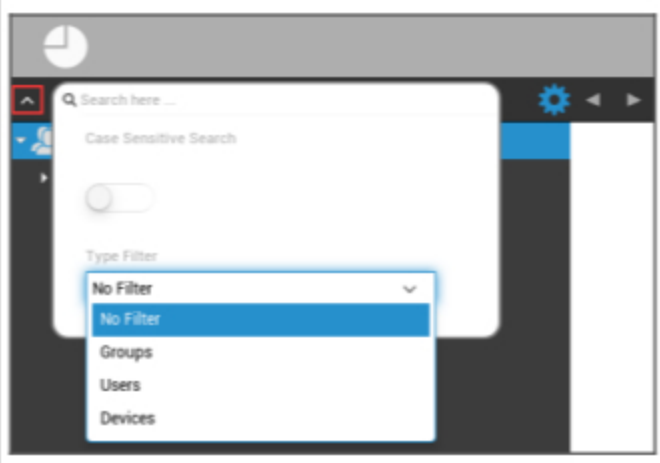
Aquí también puede eliminar o actualizar certificados, lo que se reflejará automáticamente en los perfiles afectados. Haga clic en la información de "Utilizado en el perfil" para ver exactamente dónde sigue asignado algún certificado.



Gestión de móviles

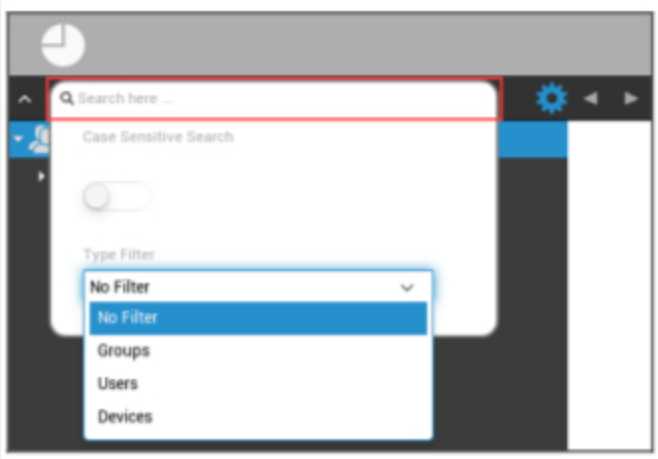
Pantalla de gestión del móvil

Filtro de dispositivos



Con un clic en la esquina superior izquierda de la pantalla, puedes encontrar una variedad de filtros para la visualización de dispositivos.

Ventana de búsqueda



La ventana de búsqueda le permite buscar todos los dispositivos y/o usuarios con una palabra clave específica.

Opciones de engranaje

Tras hacer clic en el símbolo correspondiente, aparecerá una lista de opciones disponibles.

Éstas cambian con cada ventana actual y se explican en los capítulos respectivos.

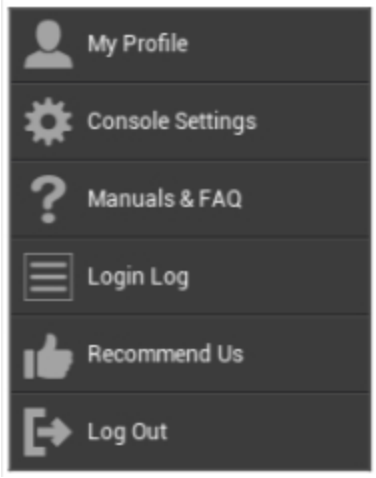
Flechas de navegación

Con un clic en la flecha de la izquierda, pasará a la página anterior.

Después, con un clic en la flecha de la derecha, volverá a la página que acaba de abandonar.

Configuración de la cuenta de administración

Al hacer clic en la dirección de correo electrónico como se ve arriba, aparece el siguiente menú:



Mi perfil	Editar los datos de la cuenta de administrador
Configuración de la consola	Configurar los ajustes de la consola para la cuenta Admins
Manuales y FAQ	Ver la página "Manuales y FAQ" en "Configuración general"
Registro de inicio de sesión	Accede al "Registro de inicio de sesión"
Recomiéndanos	Ver la página "Recomiéndanos" en "Configuración general"
Cerrar sesión	Sal de la consola MDM

Información para el usuario

Aquí puede editar los detalles de la cuenta del administrador actualmente conectado.

Nombre de usuario	Nombre de usuario y/o dirección de correo electrónico de la cuenta
Nombre	Nombre del administrador
Apellidos	Apellidos de los administradores
Nombre de usuario	Nombre de usuario del administrador
Dirección de correo electrónico	Dirección de correo electrónico de los administradores
Dirección de correo electrónico alternativa	Dirección de correo electrónico alternativa del administrador
Fotografía	Foto de perfil
Número de teléfono	Número de teléfono de los administradores
Número de móvil	Número de móvil del administrador
Extensión telefónica	Extensión telefónica
Ubicación	Ubicación
Posición	Cargo en la empresa
Grupo de usuarios	Selecciona a qué grupo de usuarios quieres asignar la cuenta admin
Comentario	Escribe un comentario
Introducir nueva contraseña	Introduce la contraseña para un cambio de contraseña
Repite la nueva contraseña	Repite la nueva contraseña para confirmarla

Ten en cuenta que el acceso de administración también puede archivarse como cuenta de usuario local en la estructura jerárquica. Sin el establecimiento de un administrador adicional, ¡éste no debe eliminarse!

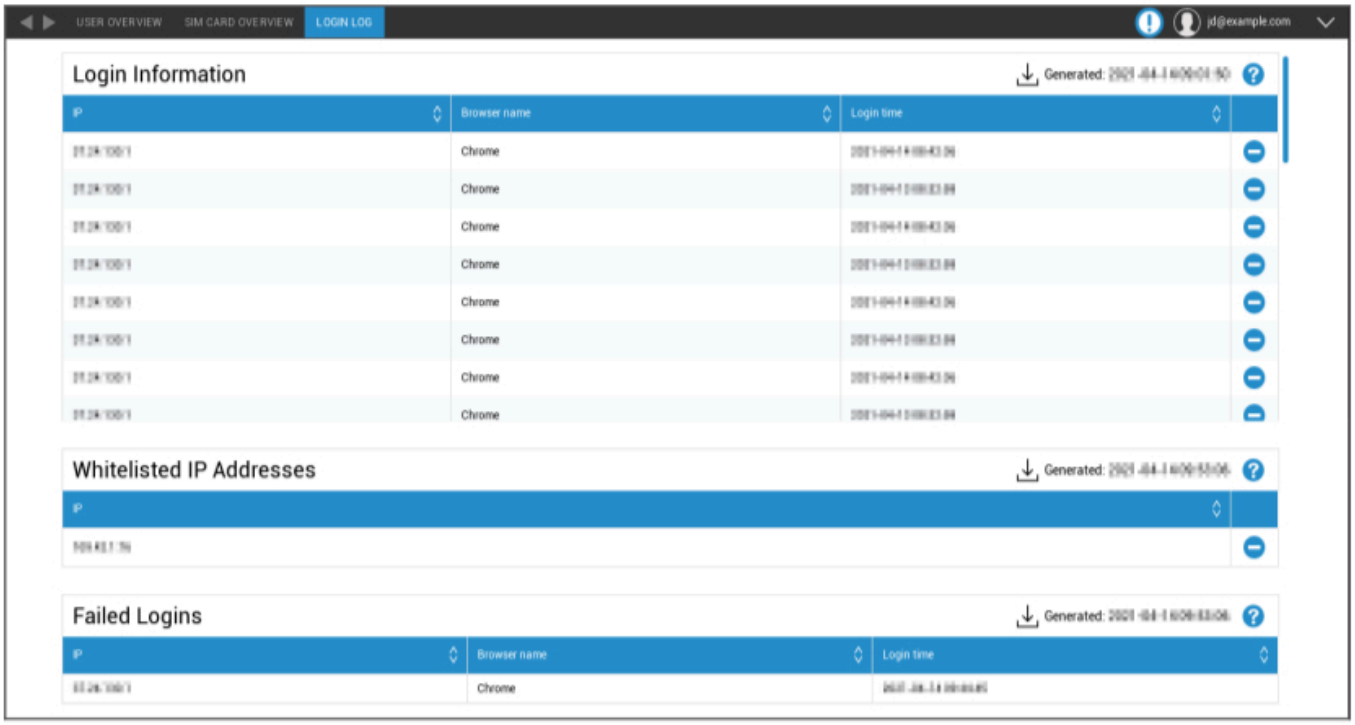
Configuración de la consola

Aquí puede configurar las siguientes opciones de la consola para la cuenta Admins:

Opciones de visualización del usuario del directorio	Define cómo deben etiquetarse los usuarios en el árbol
Opciones de visualización del dispositivo de directorio	Define cómo deben etiquetarse los dispositivos en el árbol
Tiempo de espera de la sesión	Si el usuario no hace nada en el tiempo especificado, se cerrará su sesión. El valor por defecto es 60 minutos. Por favor, cierra la sesión y vuelve a iniciarla después de cambiar esta configuración.
Zona horaria	Elige la zona horaria que se utiliza
Formato de hora	Elige cómo deben mostrarse las marcas de tiempo
Lenguaje de la consola	Elige el idioma en el que debe mostrarse la consola. Están disponibles el inglés y el alemán.
Color principal	Puedes establecer un color que se utilizará como base para la combinación de colores de la consola. Puedes utilizar el selector de color o introducir un color en notación HTML HEX. Los formadores RGB como "rosa", "amarillo" también funcionan.
Orden Guardar	La combinación de teclas para activar un guardado sin pulsar el botón "Guardar".
Utiliza la autenticación de dos factores	Activa el uso de la autenticación de dos factores al iniciar sesión. Recibirás un correo electrónico al iniciar sesión con un código que tendrás que introducir para conectarte.
Tiempo de espera de la autenticación de dos factores	Establece un periodo de tiempo durante el cual no se te pedirá una autenticación de dos factores después de una autenticación ya realizada con éxito.
Enviar código de verificación a través de	El código de verificación se enviará a las opciones seleccionadas. El mensaje del dispositivo se mostrará en la App App AppTec360 MDM en todos los dispositivos Android e iOS que te pertenezcan.
Enviar mensaje de inicio de sesión después de iniciar sesión	Si se activa, se enviará un correo electrónico por cada inicio de sesión desde una dirección IP que no esté en la lista blanca. El correo electrónico contiene información sobre el inicio de sesión (por ejemplo, IP, Navegador).

Registro de inicio de sesión

Aquí puede ver la información relativa a los inicios de sesión de la cuenta de administrador actualmente conectada.



Información de acceso	Una lista que contiene los inicios de sesión de la cuenta de administrador actualmente conectada que fueron registrados por la consola. Esta lista muestra todos tus inicios de sesión con éxito en los últimos 30 días.
Direcciones IP en lista blanca	Esta es la lista de todas tus direcciones IP en la lista blanca. Si te conectas desde una IP que aparece aquí, no recibirás el mensaje de conexión. Puedes añadir una dirección IP a esta lista haciendo clic en el botón situado junto a una entrada de la lista "Información de acceso" anterior. Puedes eliminar una dirección IP de esta lista haciendo clic en el botón situado junto a una entrada de esta lista o de la lista "Información de acceso" anterior.
Logins fallidos	Esta es una lista de todos los intentos fallidos de inicio de sesión en los últimos 30 días. Si no consigues introducir la contraseña correcta al menos 3 veces en 20 minutos, aparecerá una entrada en esta lista. También se te informará por correo electrónico de los intentos fallidos de inicio de sesión.

Administración corporativa (Root-Node) en Mobile Management

Cuando haya llegado al Nodo Raíz (primer grupo), podrá realizar una serie de ajustes para su empresa, en lo que respecta a la Gestión de Móviles.

Crear un subgrupo	Crear un subgrupo
Renombrar nodo raíz	Renombrar el Nodo Raíz (por ejemplo, el nombre de tu empresa)
Inscripción masiva	Inscribe varios dispositivos/usuarios al mismo tiempo
Asignación masiva	Asigna un perfil para los grupos respectivos, con una mirada
Administración rápida de aplicaciones	Enviar solicitudes de (Des)Instalación de una aplicación a los respectivos grupos de dispositivos
Importación de usuarios CSV	Importar usuarios desde CSV al grupo correspondiente

Crear un subgrupo

Con "Crear un subgrupo" puede crear un subgrupo adicional.

Puede establecer bajo qué grupo debe asignarse el subgrupo.

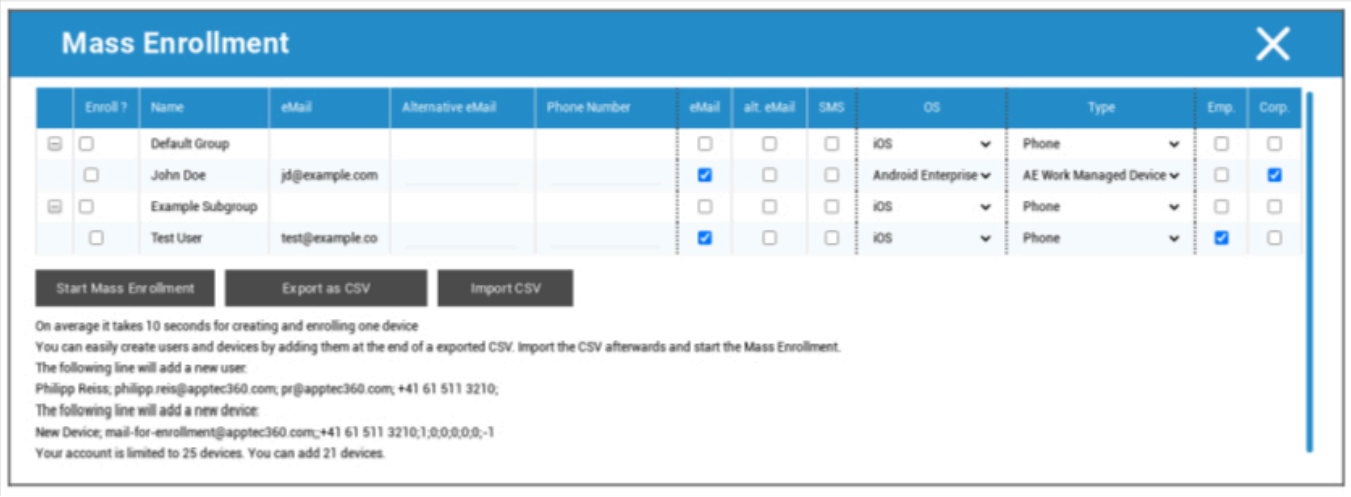
(Por defecto, se crea un nuevo grupo que se asigna como subgrupo en el nodo raíz)

Renombrar nodo raíz

Aquí puedes renombrar tu nombre-raíz. Es habitual que en este caso se utilice el nombre de la empresa.

Inscripción masiva

Con la "inscripción masiva" puede inscribir varios dispositivos y usuarios.



Puede seleccionar directamente de qué manera debe recibir el usuario la inscripción (eMail; eMail alternativo; SMS)

Dependiendo del dispositivo que vaya a recibir el usuario (iOS, Android, Windows Phone), puede marcarlo directamente aquí.

La distinción de si se trata de un Smartphone o una Tablet, también se puede configurar aquí, que tendrás que seleccionar correctamente, con una marca de verificación.

Como último paso, puede establecer si el dispositivo en cuestión es corporativo o privado (BYOD).

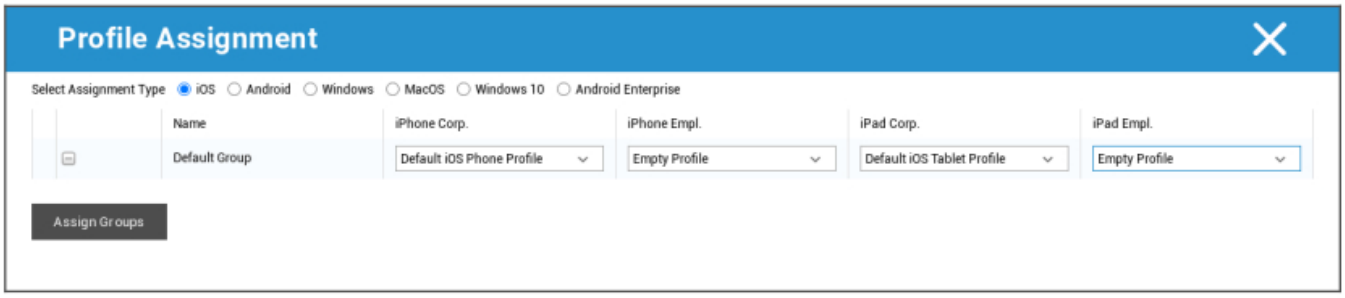
Con la opción "Exportar como CSV", puede exportar la información como un archivo de datos CSV. A cambio, también puede importar el archivo de datos CSV con "Importar CSV", el archivo debe

parecerse al ejemplo siguiente:

Philipp Reiss; philipp.reis@apptec360.com; pr@apptec360.com; +41 61 511 3210;

Asignación masiva

En Asignación masiva puedes asignar un perfil a todos los grupos, este se divide en iOS - Android - Windows - MacOS - Windows 10 - Android Enterprise

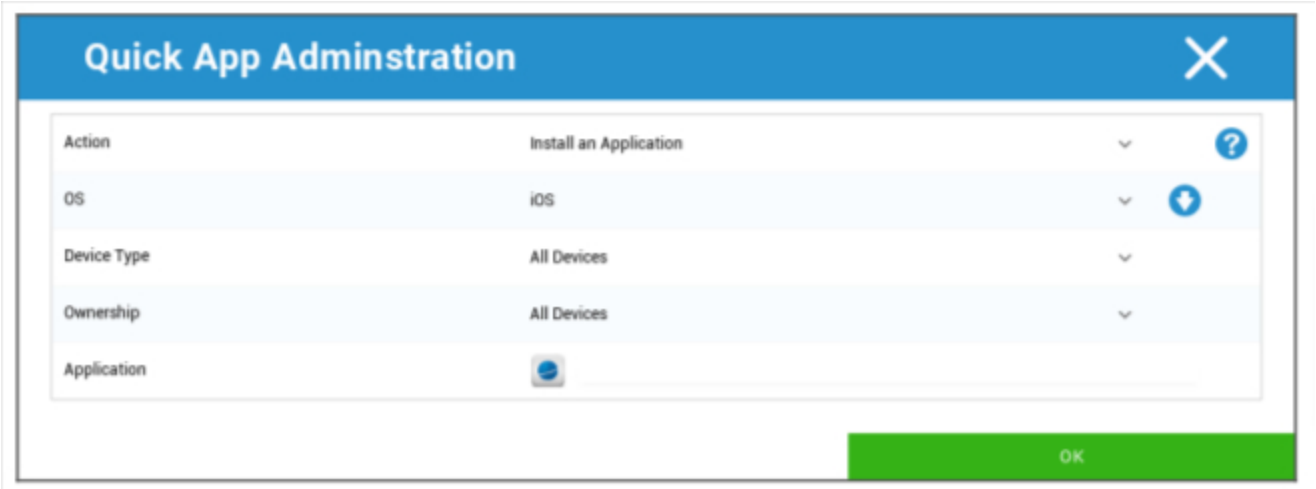


Windows - MacOS - Windows 10 - Android Enterprise

Administración rápida de aplicaciones

En Administración rápida de aplicaciones puede enviar solicitudes de instalación o desinstalación de una aplicación específica a un sistema operativo de su elección.

También puede definir si la solicitud debe enviarse a todos los tipos de dispositivos del SO seleccionado o sólo a un tipo de dispositivo específico.



Importación de usuarios CSV

Importar usuarios desde CSV al grupo correspondiente.

Con "Descargar plantilla CSV", puede exportar un archivo de plantilla CSV, que puede rellenarse (o puede utilizarse como referencia).

También puede utilizar las opciones "Mostrar identificadores de función" y "Mostrar identificadores de grupo" como referencia para crear su propio archivo CSV.

El archivo CSV puede cargarse en el MDM con "Cargar CSV".

Como último paso, puede iniciar la importación haciendo clic en "Iniciar importación".

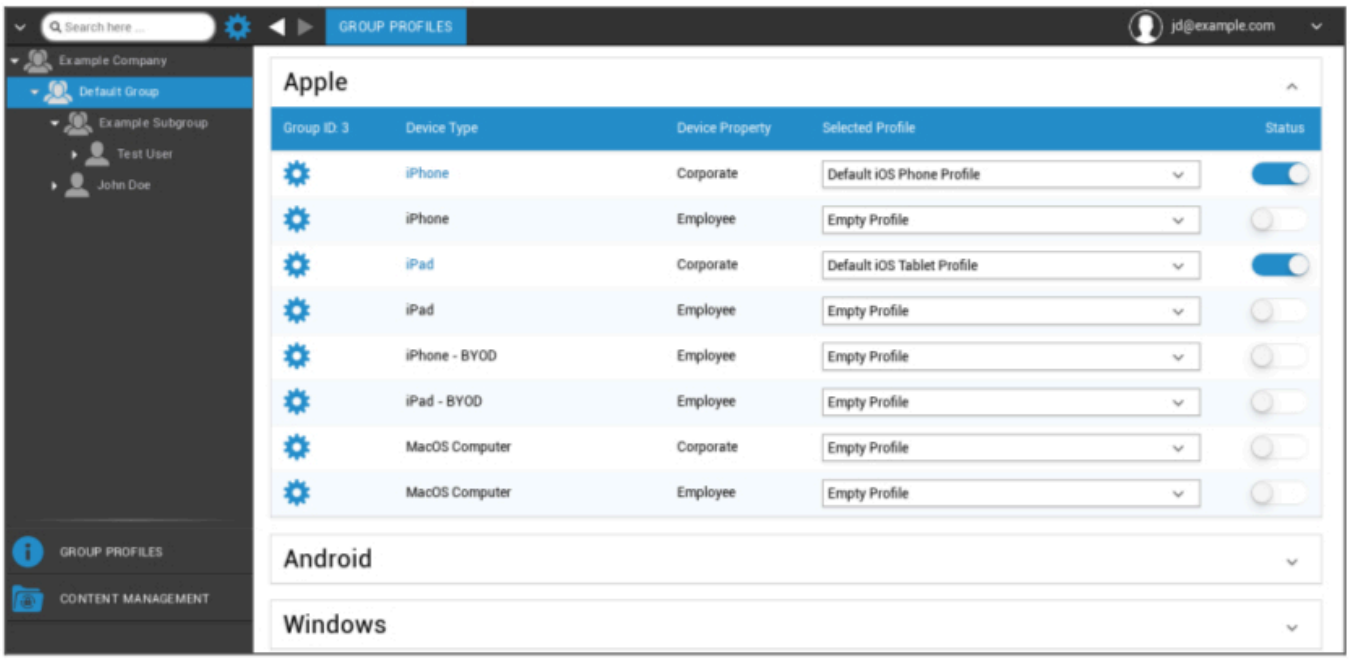
Gestión de grupos en Mobile Management

Un clic en la vista general muestra los distintos perfiles de configuración para las respectivas plataformas.

Un perfil contiene todas las opciones de configuración que pueden establecerse previamente con AppTec360 en el dispositivo del usuario final. En cada plataforma puedes crear perfiles para dispositivos corporativos (Corporate) o dispositivos Bring-Your-Own-Device (Employee).

Para diferenciar las configuraciones de los grupos de dispositivos, por ejemplo según su ubicación o función, se aconseja crear varios subgrupos.

Tenga en cuenta la gestión de perfiles en Mobile Management



Con el menú de engranajes se establecen diversos ajustes para el (sub)grupo correspondiente.

Crear un subgrupo	Crear subgrupo para el (sub)grupo correspondiente
Editar Grupo seleccionado	Editar el grupo seleccionado
Borrar grupo seleccionado	Eliminar el grupo seleccionado
Inscripción masiva	Inscribe muchos dispositivos / usuarios a la vez para el perfil seleccionado
Asignación masiva	Asignar perfiles al grupo actualmente seleccionado

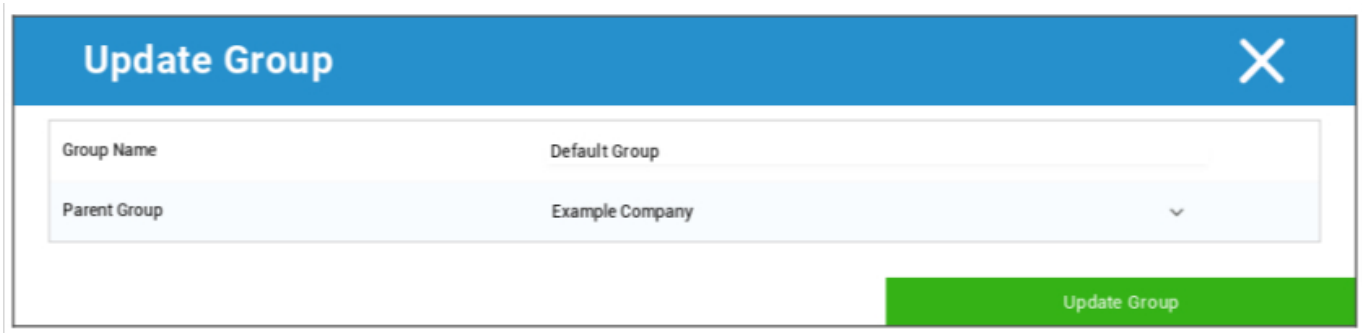
Crear un subgrupo	Crear subgrupo para el (sub)grupo correspondiente
Crear un usuario	Crear un usuario para el (sub)grupo correspondiente

Crear un subgrupo

Con "Crear un subgrupo", puede crear un subgrupo adicional.

Se puede establecer bajo qué grupo se va a asignar el subgrupo (por defecto, el subgrupo se asigna al grupo que esté seleccionado en ese momento).

Editar Grupo seleccionado



Aquí puede editar el perfil - aquí, los siguientes ajustes son posibles:

- Se puede cambiar el nombre del grupo
- Se puede cambiar el grupo de padres

Borrar grupo seleccionado

En "Eliminar grupo seleccionado" se te listan todos los usuarios y dispositivos que están en el grupo respectivo. Aquí tienes la opción de eliminarlos.

Para un usuario puede realizar los siguientes comandos de borrado:

Eliminar usuario	Usuario eliminado
Mover usuario a grupo:	Puedes mover al usuario a otro grupo (columna siguiente, ej. "Admins")

Para un dispositivo puede realizar los siguientes comandos de borrado:

Borrar y eliminar	Borrar y eliminar el dispositivo
Borrar del sistema	Quitar el dispositivo sólo de AppTec

Referencia: Inscripción masiva

Referencia: Asignación de Masas

Crear un usuario

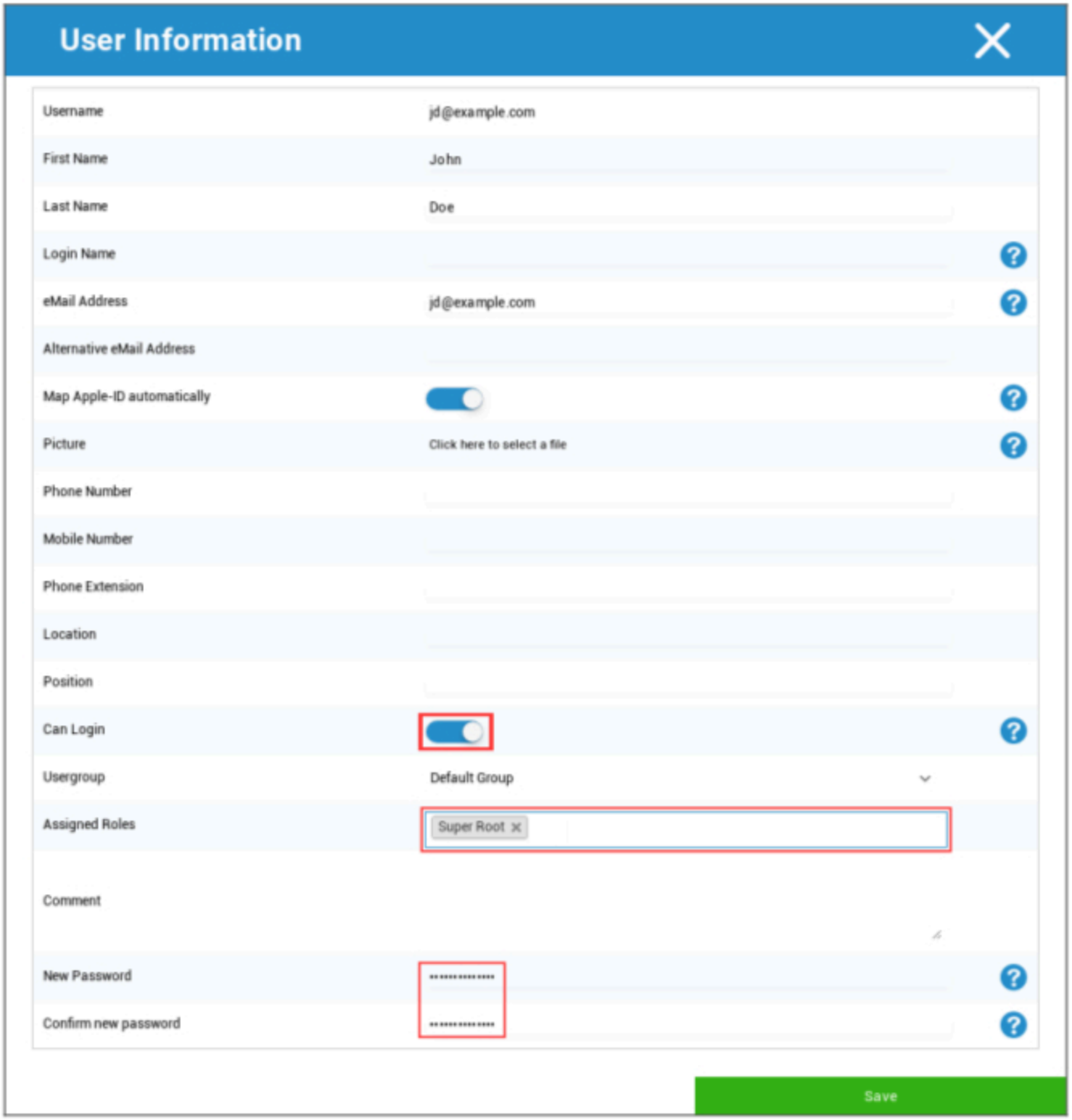
Con "Crear un usuario", puede añadir un nuevo usuario.

Crear un nuevo Admin-Usuario

Puede establecer un usuario como Admin-Usuario. Al hacerlo, obtendrá los permisos para iniciar sesión en la consola y también para cambiar usuarios/grupos/dispositivos.

Cree un usuario normal o utilice un usuario existente. Elija el usuario al que desea dar permisos de administrador, haga clic en la rueda y elija "Editar usuario":

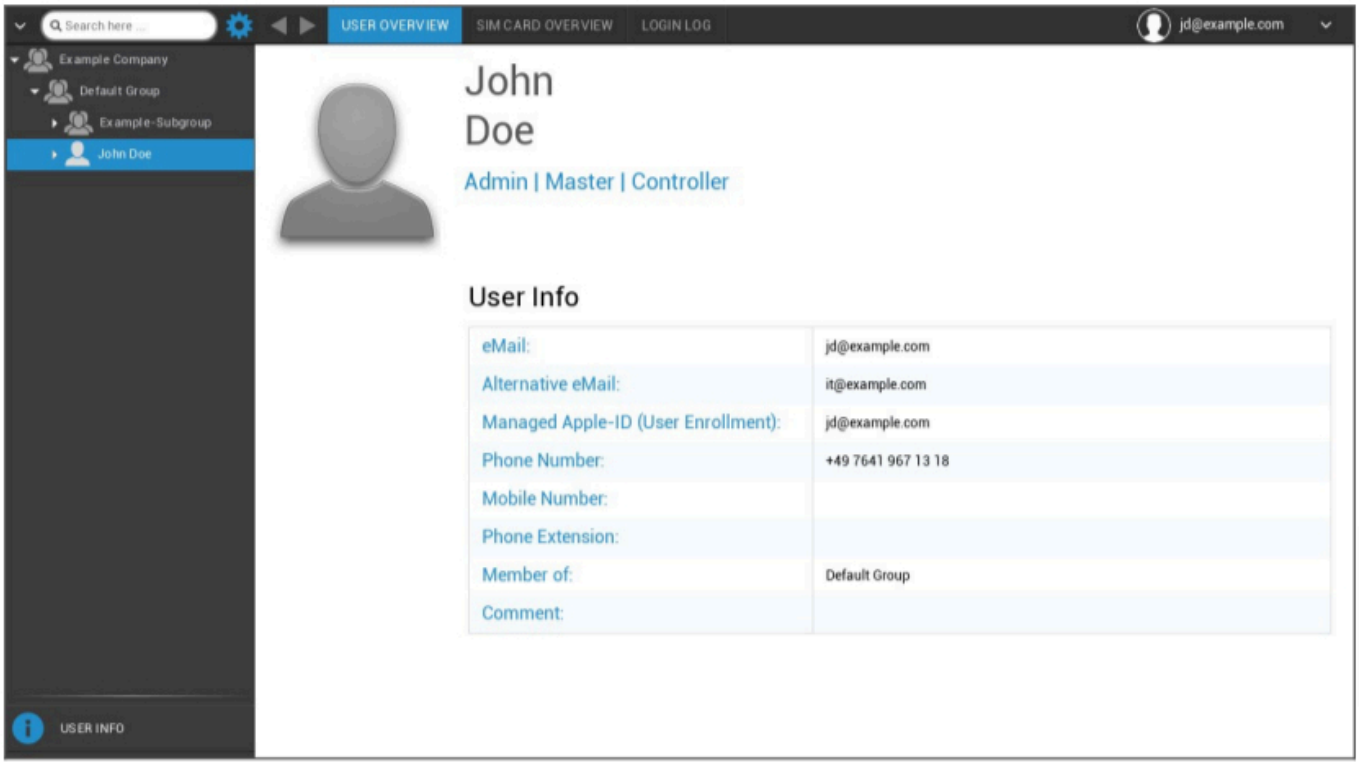
Active el interruptor para "Puede iniciar sesión", asigne el rol "Super-Root" al usuario y establezca una contraseña.



Guarde esto y el usuario ya puede iniciar sesión con el nombre de usuario y la contraseña.

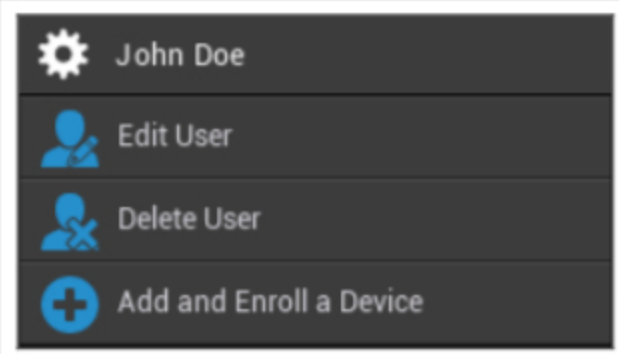
Gestión de usuarios en Mobile Management

Cuando seleccione un usuario determinado, verá el siguiente resumen:



Recibirá un resumen de toda la información que introdujo anteriormente en "Crear un usuario".

Con el engranaje que se instala en la parte superior, puede realizar las siguientes configuraciones:



Nombre de usuario	Nombre de usuario del usuario seleccionado
Editar usuario	Editar información de usuario
Eliminar usuario	Eliminar usuario • Eliminar del sistema = El dispositivo se eliminará de AppTec

	• Borrar y eliminar = El dispositivo se restablecerá a los ajustes de fábrica y se eliminará de AppTec
Añadir e inscribir un dispositivo	Inscribir un dispositivo para el usuario seleccionado

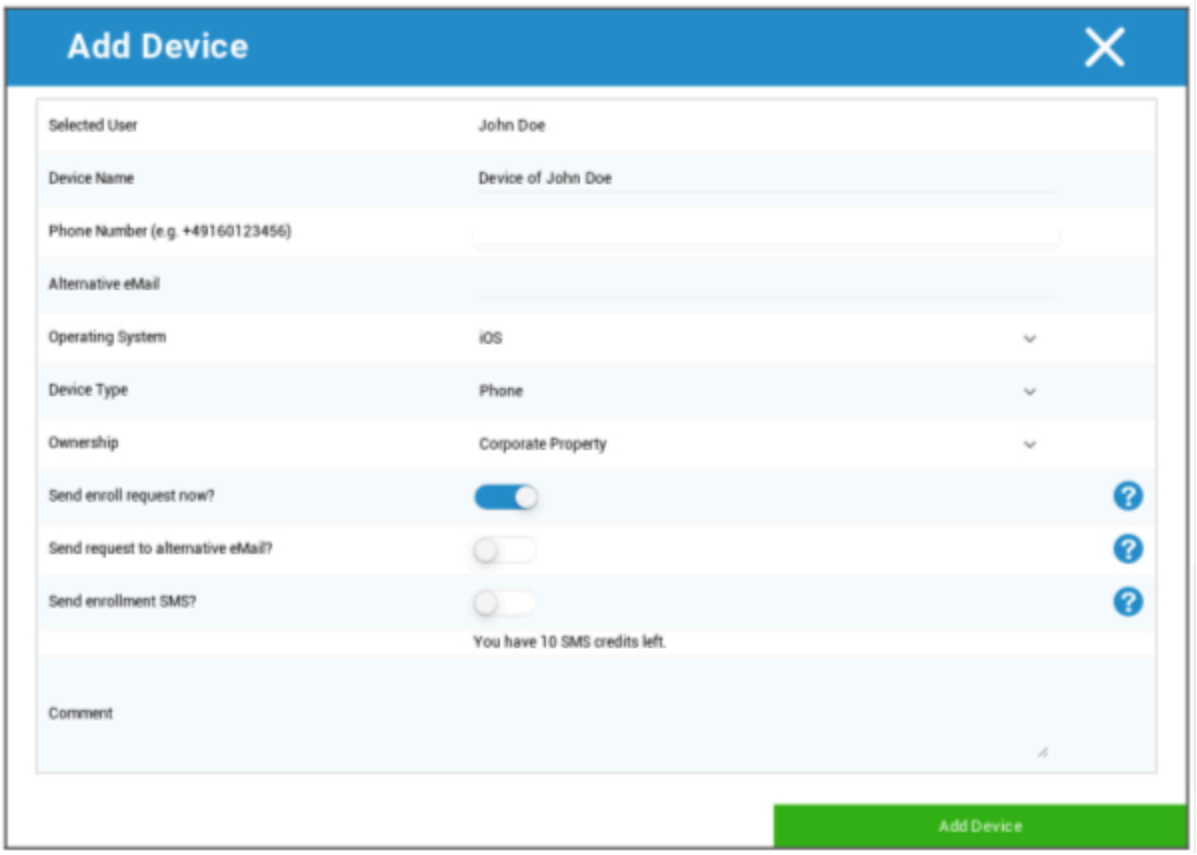
Ten en cuenta que el acceso de administración también puede archivarse como cuenta de usuario local en la estructura jerárquica. Sin el establecimiento de un administrador adicional, ¡éste no debe eliminarse!

Añadir e inscribir un dispositivo

Aquí puede seleccionar un dispositivo para el uso seleccionado.

También puedes inscribir dispositivos en un grupo directamente. Para ello, haz clic en el grupo, pulsa en la rueda y selecciona "Añadir e inscribir un Dispositivo".

Debería ver el siguiente resumen:



Dependiendo del tipo de dispositivo que desee inscribir, deberá realizar las siguientes configuraciones:

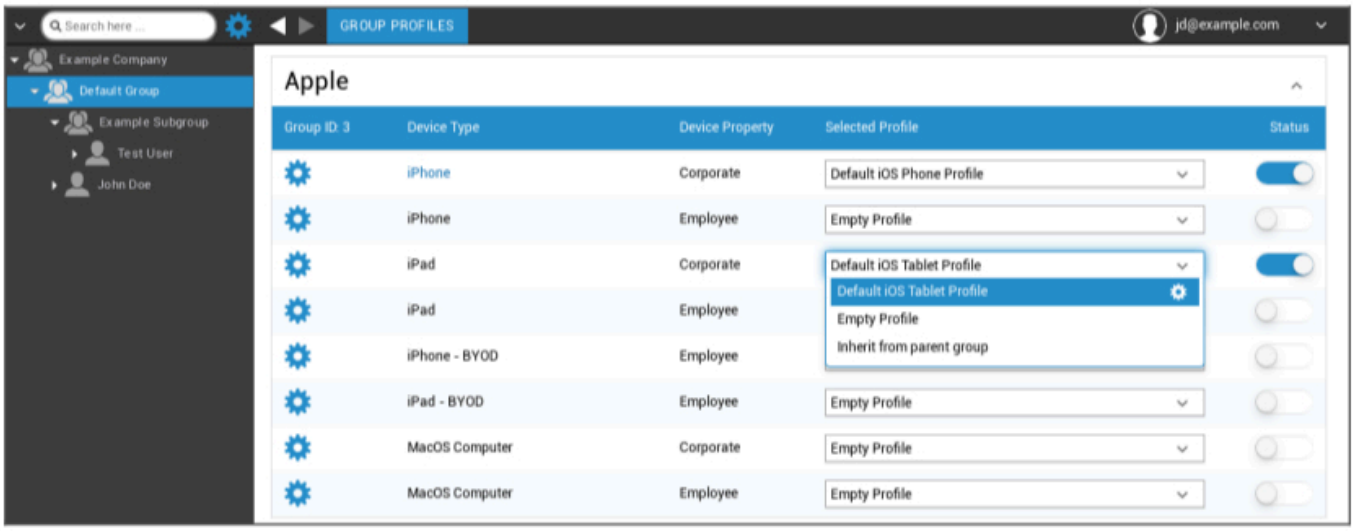
Usuario seleccionado	Usuario seleccionado (se rellenará automáticamente)
Nombre del dispositivo	Se rellenará automáticamente (dispositivo para "nombre de usuario") - no obstante, puede modificarse
Número de teléfono	Número de teléfono, se rellenará automáticamente (siempre que lo haya facilitado el usuario) - aquí, sin embargo, se puede añadir o modificar
Correo electrónico alternativo	Correo electrónico alternativo, se rellenará automáticamente (siempre que lo haya proporcionado el usuario) - aquí, sin embargo, se puede añadir o cambiar
Propietario del dispositivo	Propiedad corporativa = dispositivo corporativo Propiedad del empleado = dispositivo BYOD
Elegir sistema de funcionamiento	Aquí puedes elegir entre los siguientes sistemas operativos: • iOS • iOS BYOD (Inscripción de usuarios) • MacOS • Android para empresas • Android • Windows Mobile • Windows 10
¿Enviar solicitud de inscripción?	El correo electrónico se envía inmediatamente a la dirección de correo electrónico principal y se pide al usuario que conecte su dispositivo
¿Enviar solicitud a eMail alternativo?	Envía el correo electrónico adicional o exclusivamente (en caso de que se haya desactivado "¿Enviar solicitud de inscripción?") a la dirección de correo electrónico alternativa (el correo electrónico es diferente del correo electrónico "normal" de Solicitud de inscripción).
¿Enviar SMS de inscripción?	Envía una solicitud de inscripción por SMS (debes introducir el "Número de teléfono")

Una vez enviada la solicitud de inscripción, el dispositivo se mostrará (marcado en rojo) inmediatamente.

En cuanto el dispositivo se haya conectado correctamente, poco después se marcará en verde y estará listo para recibir restricciones, aplicaciones, etc.

Gestión de perfiles en Mobile Management

Tras hacer clic en un grupo, obtendrá una vista general de todas las plataformas de dispositivos que deben configurarse y los perfiles asignados respectivamente.



	Realiza la configuración del perfil seleccionado
Tipo de dispositivo	Tipo y/o modelo de aparato
Propiedad del dispositivo	Propietario del dispositivo (Corporativo = propiedad corporativa, Empleado = dispositivo privado de empleado)
Perfil seleccionado	Perfil seleccionado (el engranaje abre el diálogo de configuración del perfil)
Estado	Activado/Desactivado (el perfil se activa/desactiva)

Cuando selecciones la marcha, recibirás las siguientes opciones:

Crear un perfil

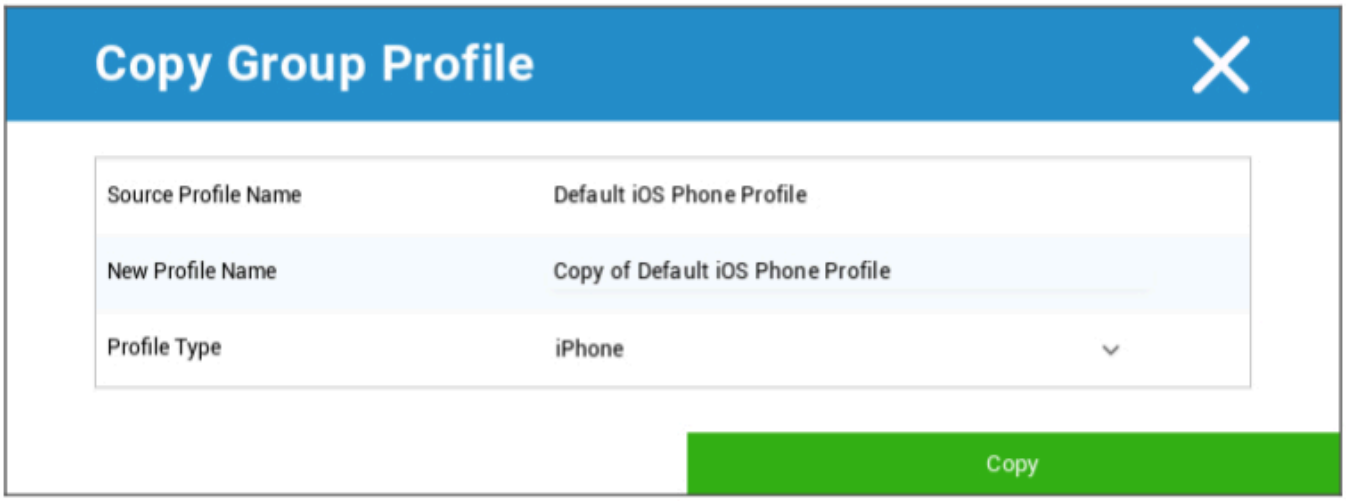
Puede crear y configurar un nuevo perfil para cada entrada y/o plataforma. Después de hacer clic en este subpunto, el perfil se creará inmediatamente y podrá comenzar con la configuración de iOS, Android y Windows Phone de inmediato.

Editar perfil

Tras hacer clic en "Editar perfil", accederá a la pantalla de configuración del perfil correspondiente, donde podrá establecer las configuraciones.

Copiar perfil

La función "Copiar perfil" permite copiar las configuraciones de un perfil ya existente y añadirlas a un perfil nuevo.

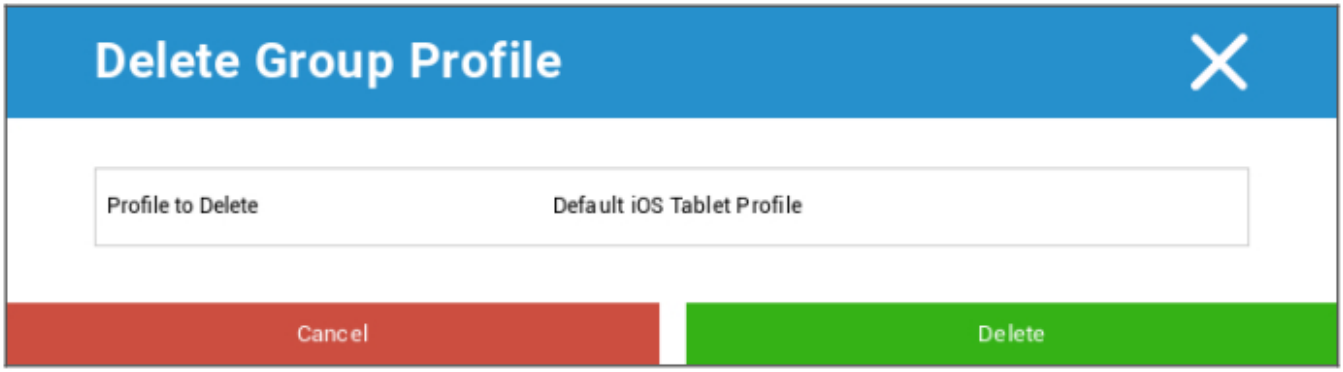


Fuente Nombre del perfil	Nombre del perfil que se va a copiar
Nuevo nombre del perfil	Nombre del nuevo perfil
Tipo de perfil	Tipo de perfil (Teléfono/Tableta)

Al hacer clic en "Copiar", el perfil se creará y podrá asignarse al grupo.

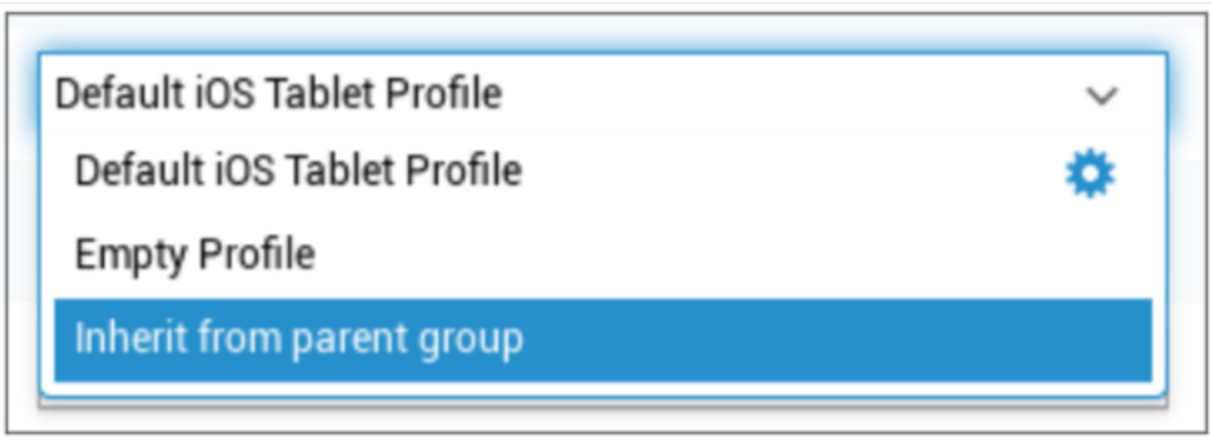
Borrar perfil

Aquí puede eliminar permanentemente un perfil. Tenga en cuenta que durante el proceso de eliminación y el siguiente proceso de "Asignar ahora" para el perfil, la configuración desaparecerá en los dispositivos respectivos de un grupo afectado y no se podrá recuperar.


Delete Group Profile
Profile to Delete
Default iOS Tablet Profile
Cancel
Delete

Herencia de perfiles

Durante la selección de los perfiles, está disponible la opción "Heredar del grupo de padres".



Si se activa el perfil, se utilizará el perfil del grupo principal para el dispositivo seleccionado (y el tipo de dispositivo correspondiente). Tenga en cuenta también que los cambios en este perfil podrían afectar a numerosos grupos.

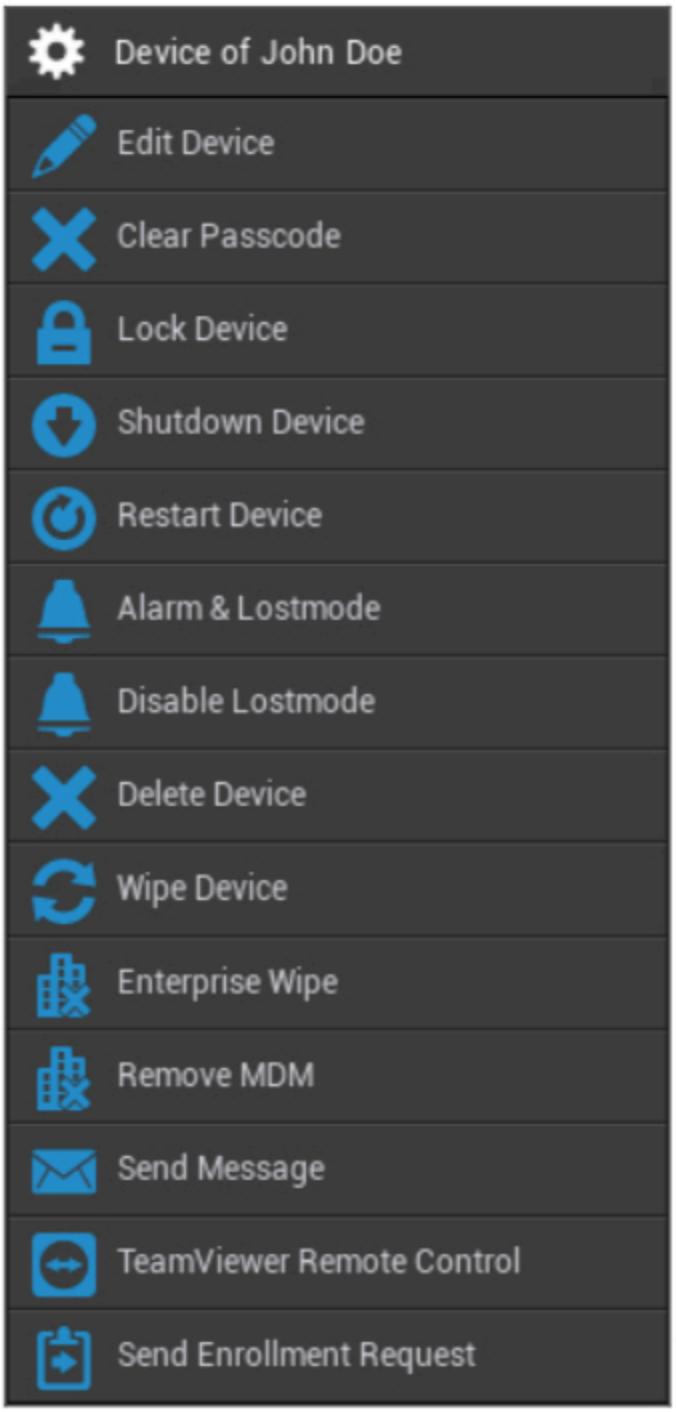
Esta configuración se establece como valor por defecto, cuando se crea un nuevo subgrupo.

También está disponible la configuración "Perfil vacío", que corresponde a un perfil vacío, lo que significa que al final no se realizará ninguna nueva configuración en el dispositivo del usuario final.

Gestión de dispositivos en Mobile Management

Al seleccionar un dispositivo, puede realizar diversas tareas a través del "engranaje". Estos son diferentes, dependiendo de las plataformas de SO (iOS, Android Enterprise, Android, Windows Mobile, Windows 10).

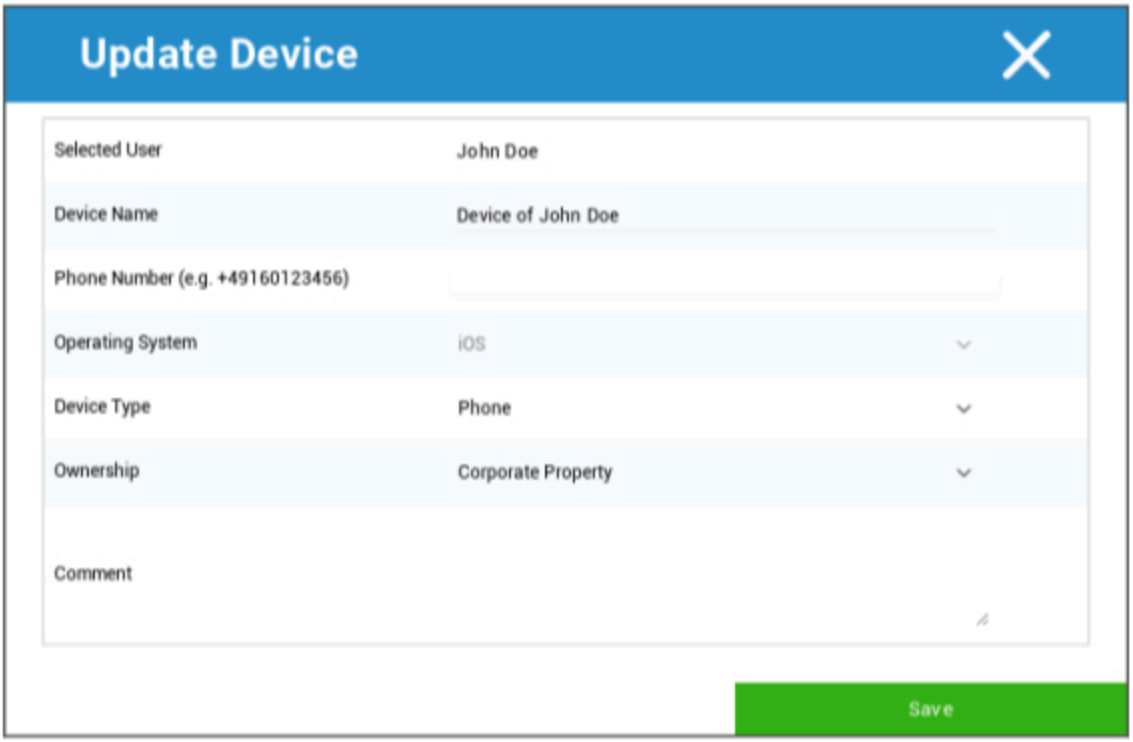
IOS



Editar dispositivo	Editar dispositivo
Borrar contraseña	Se borra el código de acceso del dispositivo
Dispositivo de bloqueo	Bloquear dispositivo (pantalla de bloqueo)

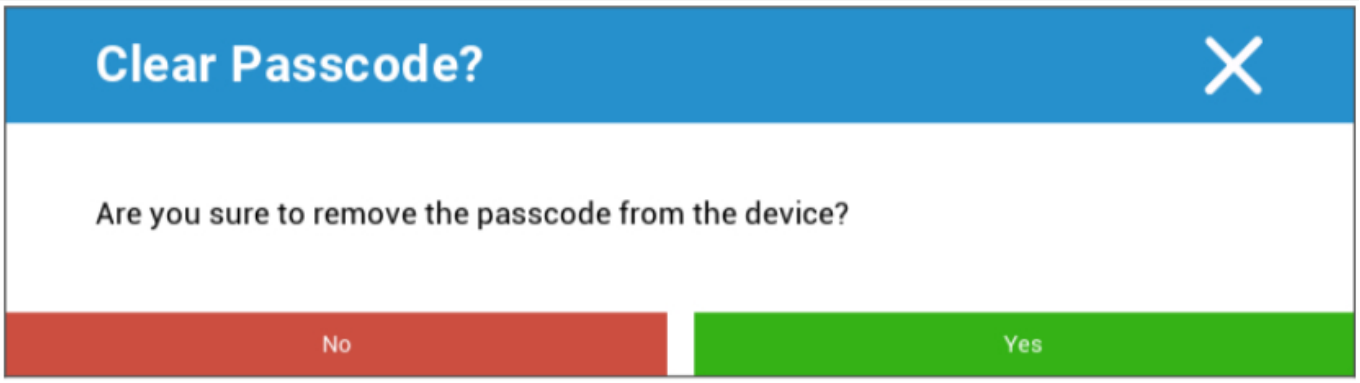
Dispositivo de apagado	Dispositivo de desconexión
Reiniciar el dispositivo	Reinicia el dispositivo
Alarma y Modo Perdido	Iniciar Alarma y Modo Perdido
Desactivar Lostmode	Desactivar Lostmode
Borrar dispositivo	Eliminar dispositivo de AppTec
Dispositivo de limpieza	Restaurar el dispositivo a los ajustes de fábrica
Limpieza de empresas	Se eliminan la información, las apps y los perfiles proporcionados por AppTec360 (el dispositivo se separa del MDM)
Eliminar MDM	
Enviar mensaje	Enviar notificaciones Push al dispositivo El mensaje se mostrará en la aplicación AppTec360 (pestaña Mensaje)
Control remoto TeamViewer	Iniciar sesión de control remoto con TeamViewer
Enviar solicitud de inscripción	Enviar (repetida) Solicitud de inscripción

Editar dispositivo



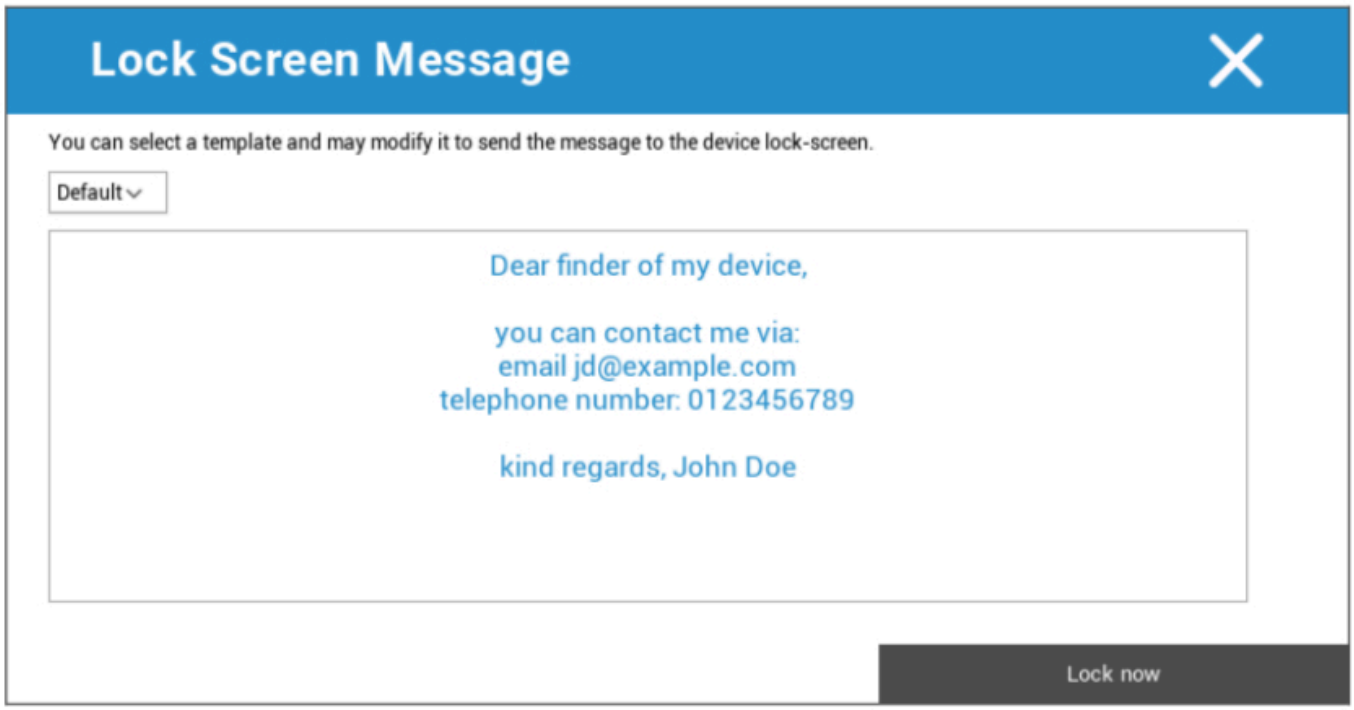
Aquí puedes actualizar diversa información sobre el dispositivo.

Borrar contraseña



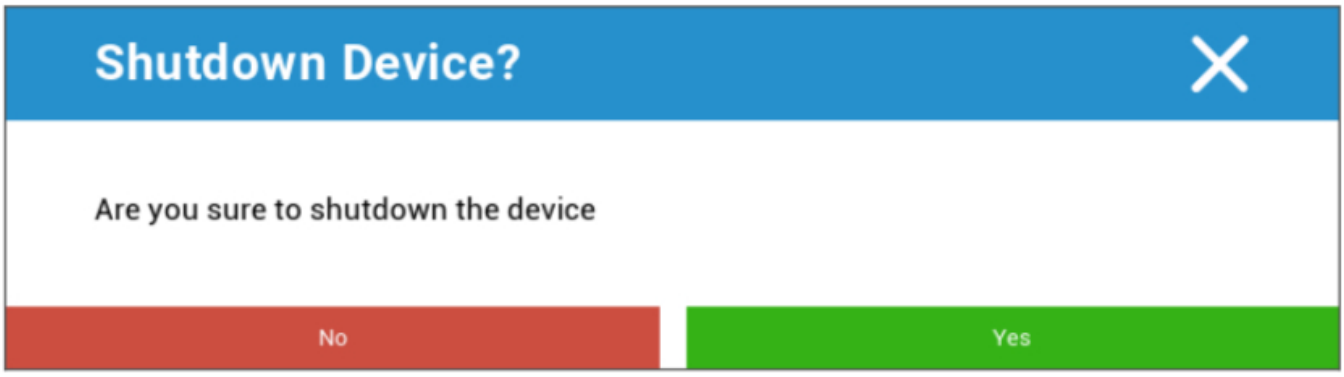
En "Borrar código de acceso" puedes eliminar el código de acceso del dispositivo de forma remota. A continuación, se pedirá al usuario que emita una nueva contraseña (según las directrices de Passcode).

Dispositivo de bloqueo



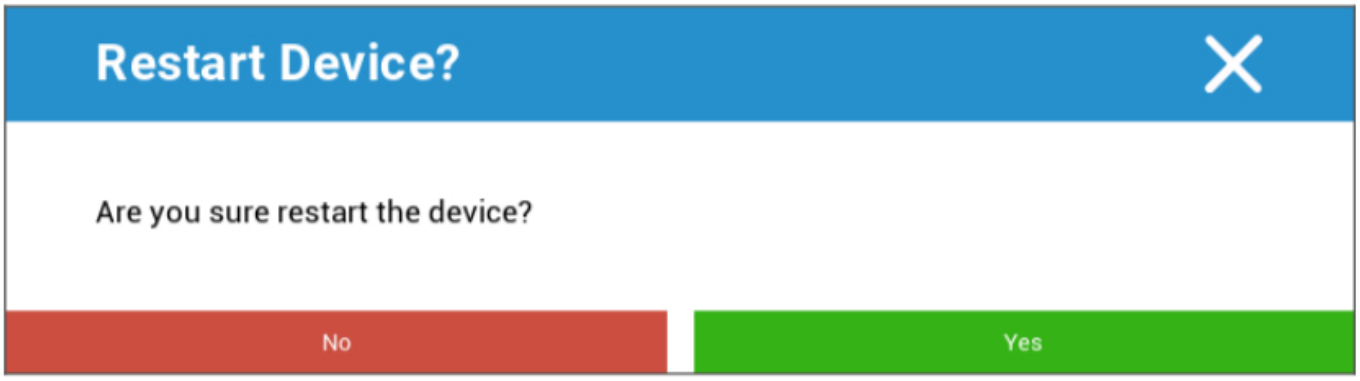
Aquí se envía una orden de bloqueo al dispositivo del usuario final (pantalla de bloqueo).

Dispositivo de apagado



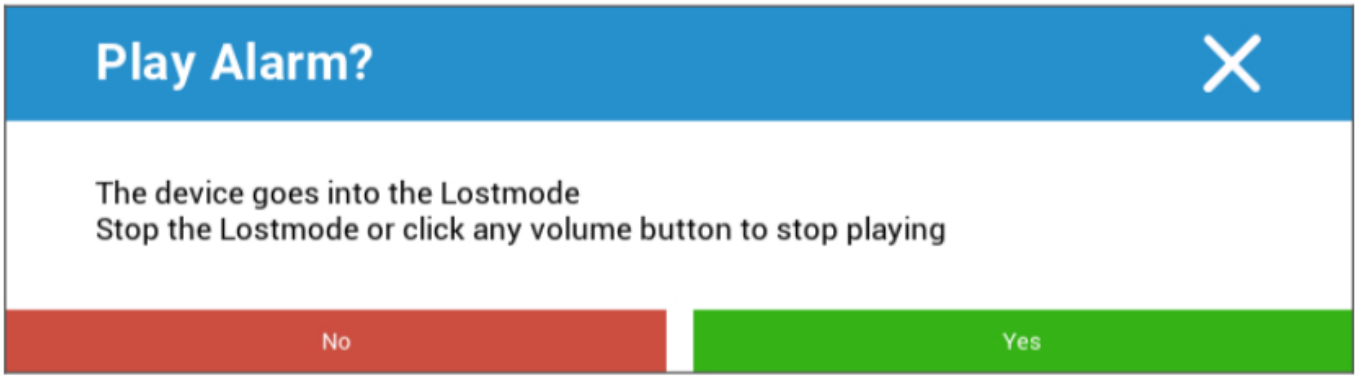
Aquí se envía una orden de apagado al dispositivo del usuario final.

Reiniciar el dispositivo

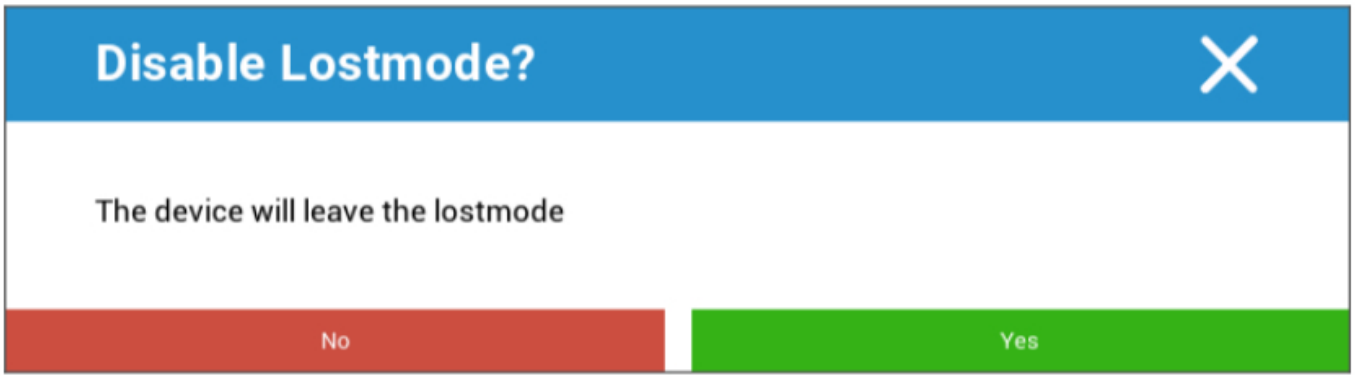


Aquí se envía una orden de reinicio al dispositivo del usuario final.

Alarma y Lostmode | Desactivar Lostmode



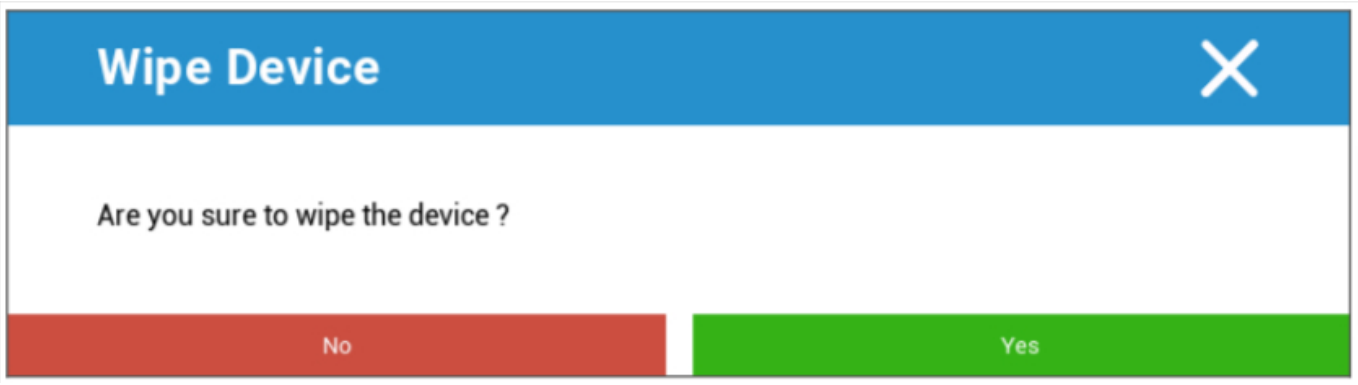
Aquí el dispositivo se puede configurar en el modo Perdido, que configura el dispositivo para que reproduzca constantemente un sonido de alarma. El Lostmode se puede detener pulsando cualquier botón de volumen del dispositivo o a distancia haciendo clic en "Desactivar Lostmode":



Borrar dispositivo

Aquí se puede ejecutar el comando de borrado. Una vez más, puede decidir si el dispositivo sólo debe eliminarse de AppTec360 ("Eliminar del sistema") o si debe eliminarse de AppTec360 y restaurarse a sus valores de fábrica ("Borrar y eliminar").

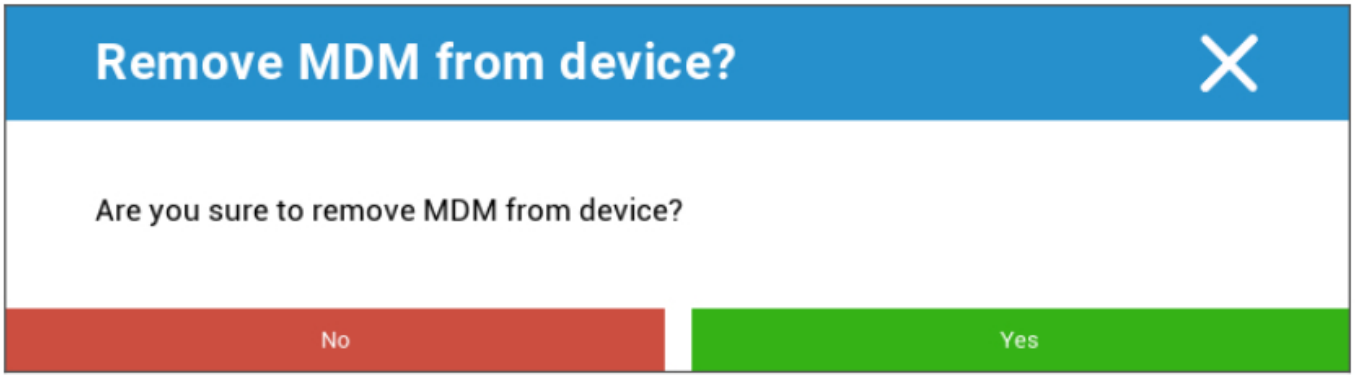
Dispositivo de limpieza



En "Borrar dispositivo" puedes realizar un borrado completo del dispositivo. Se restablecerá la configuración de fábrica del dispositivo.

Enterprise Wipe | Eliminar MDM

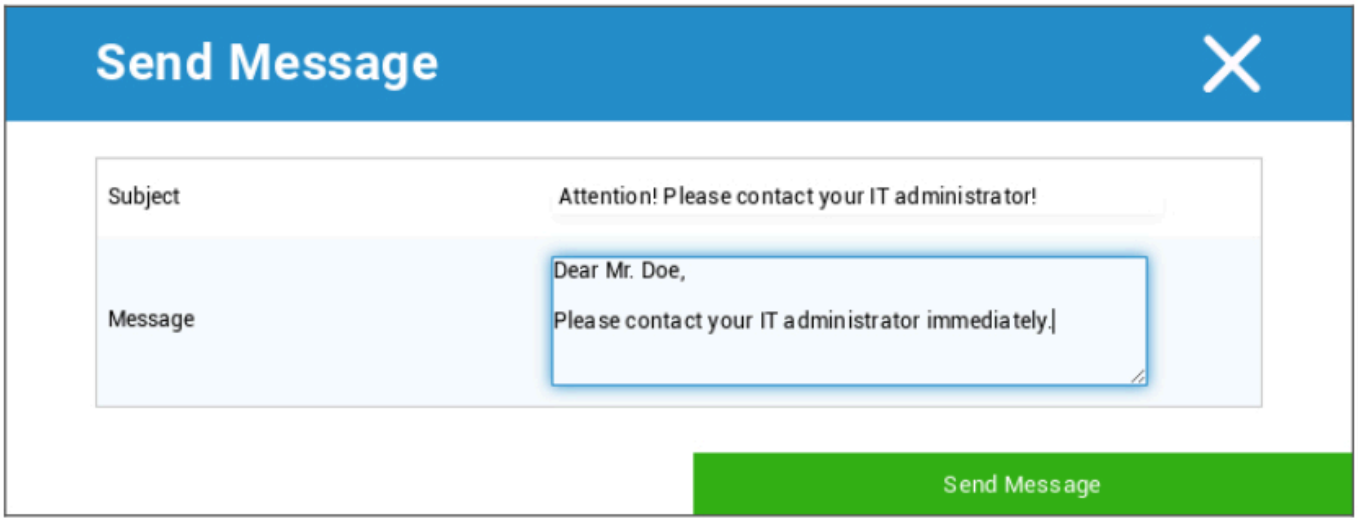
Sólo se eliminan la información, las aplicaciones y los perfiles proporcionados por AppTec360. De este modo, los datos corporativos dejarán de estar disponibles en el dispositivo del usuario final. El área privada no se ve afectada y sigue permaneciendo en el dispositivo del usuario final.



Con "Eliminar MDM" puede eliminar el perfil MDM en el dispositivo del usuario final y todos los demás elementos proporcionados por AppTec.

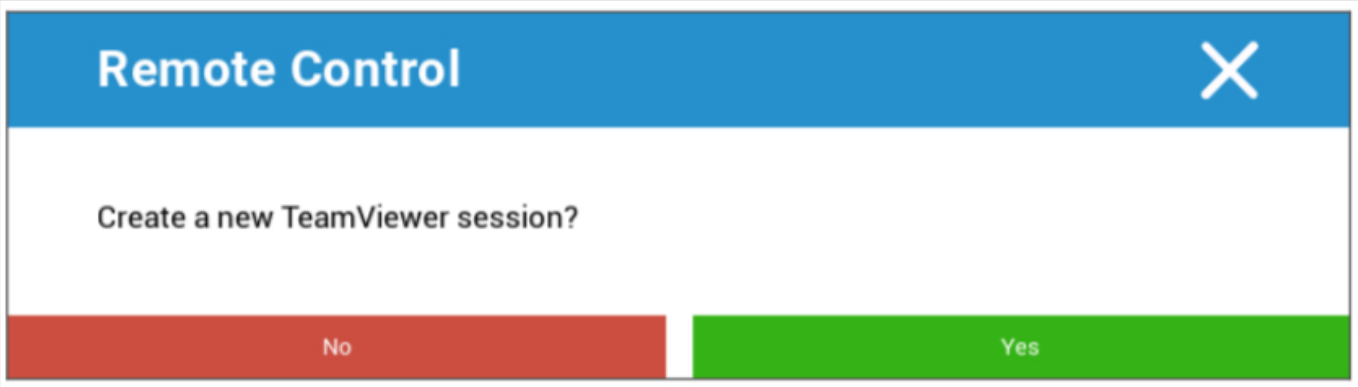
Este comando realiza la misma acción que "Enterprise Wipe".

Enviar mensaje



Aquí puede enviar una Notificación Push al dispositivo correspondiente.

Control remoto TeamViewer



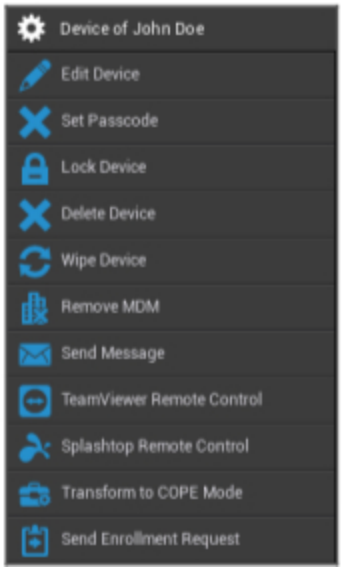
Aquí se puede iniciar una sesión de control remoto de Teamviewer.

Enviar solicitud de inscripción

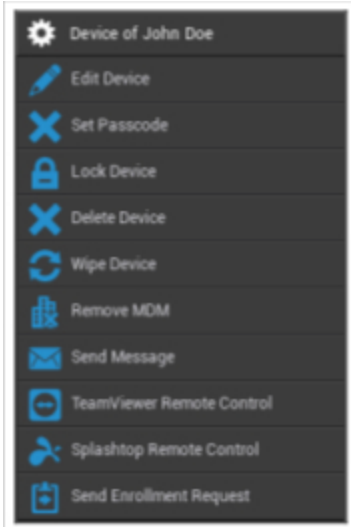
Con "Enviar solicitud de inscripción", puede enviar una solicitud de inscripción (de nuevo) al usuario correspondiente.

Android

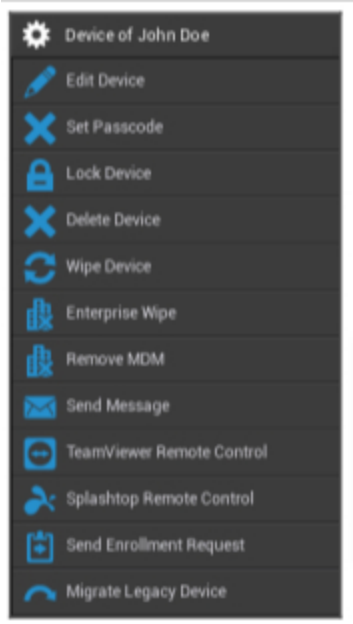
Dispositivo AE totalmente gestionado (Work Managed)



Perfil de trabajo AE (contenedor)



Teléfono Android | Tableta

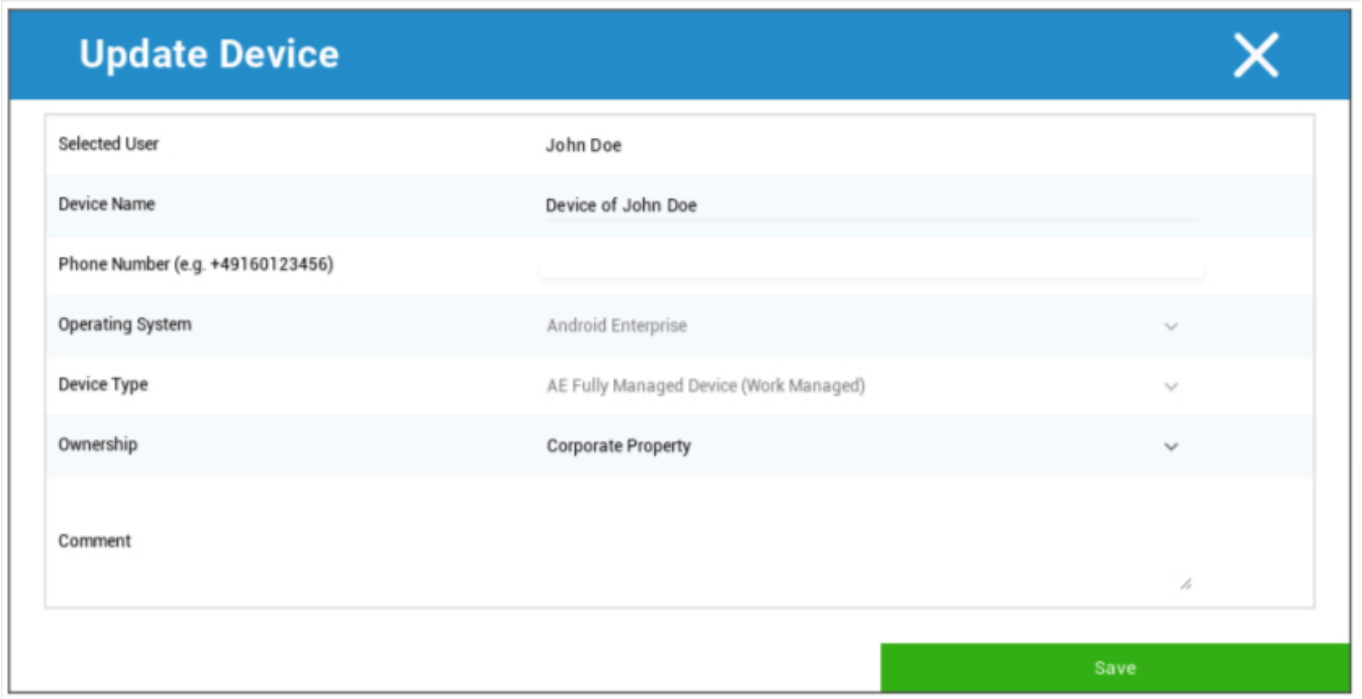


Editar dispositivo	Editar la información del dispositivo
Establecer código de acceso	Establecer el código de acceso del dispositivo
Dispositivo de bloqueo	Bloquear dispositivo (pantalla de bloqueo)
Borrar dispositivo	Borrar dispositivo de AppTec
Dispositivo de limpieza	Restaurar el dispositivo a los ajustes de fábrica
Limpieza de empresas	La información, las aplicaciones y los perfiles proporcionados por AppTec360 se eliminan (el dispositivo se separa del MDM).
Eliminar MDM	
Enviar mensaje	Enviar notificaciones Push al dispositivo El mensaje se mostrará en la aplicación AppTec360 (pestaña Mensaje)
Control remoto TeamViewer	Inicia una sesión de Control Remoto para este dispositivo utilizando TeamViewer
Mando a distancia Splashtop	Inicia una sesión de Control Remoto para este dispositivo utilizando Splashtop
Transformar a Modo COPE (sólo en Dispositivo AE Totalmente Administrado (Administrado por el Trabajo))	Crear un perfil de trabajo en este dispositivo AE totalmente gestionado (gestionado por el trabajo)
Enviar solicitud de inscripción	Enviar solicitud de inscripción (repetida)

Migrar dispositivo heredado (sólo en teléfonos / tabletas Android cuando se inscriben utilizando el Aprovisionamiento en Modo Propietario de Dispositivo)	Migración del perfil de teléfono/tableta Android al perfil de dispositivo totalmente gestionado AE (gestionado por el trabajo)

Editar dispositivo

Aquí puedes actualizar diversa información del dispositivo.



Usuario seleccionado	Usuario del dispositivo
Nombre del dispositivo	Nombre del dispositivo
Número de teléfono	Número de teléfono del dispositivo
Sistema operativo	Android para empresas Android
Tipo de dispositivo	Android Empresa: • Dispositivo AE totalmente gestionado (Work Managed) • Modo Perfil de trabajo AE (sólo contenedor) • Dispositivo totalmente gestionado AE con perfil de trabajo (COPE) Androide: • Teléfono • Tableta
Propiedad	Empresa = propiedad de la empresa

	Empleado = propiedad del empleado
Comentario	Descripciones adicionales del dispositivo

Borrar contraseña

Aquí puede eliminar el código de acceso del dispositivo seleccionado. Por defecto en Android, el código de acceso se establecerá en "123456" - esto puede y debe ser cambiado por el usuario después.

Dispositivo de bloqueo

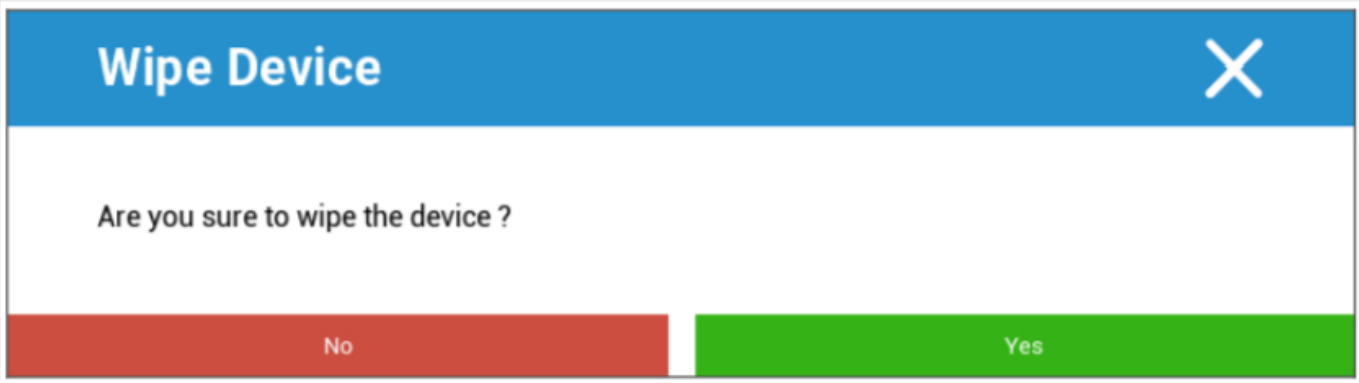
Aquí se enviará un comando de bloqueo de dispositivo al dispositivo (pantalla de bloqueo).

Borrar dispositivo

Aquí se puede realizar un comando de borrado. Una vez más, puede decidir si el dispositivo sólo debe eliminarse de AppTec360 ("Eliminar del sistema") o si debe eliminarse de AppTec360 y, además, restaurarse a sus valores de fábrica ("Borrar y eliminar").

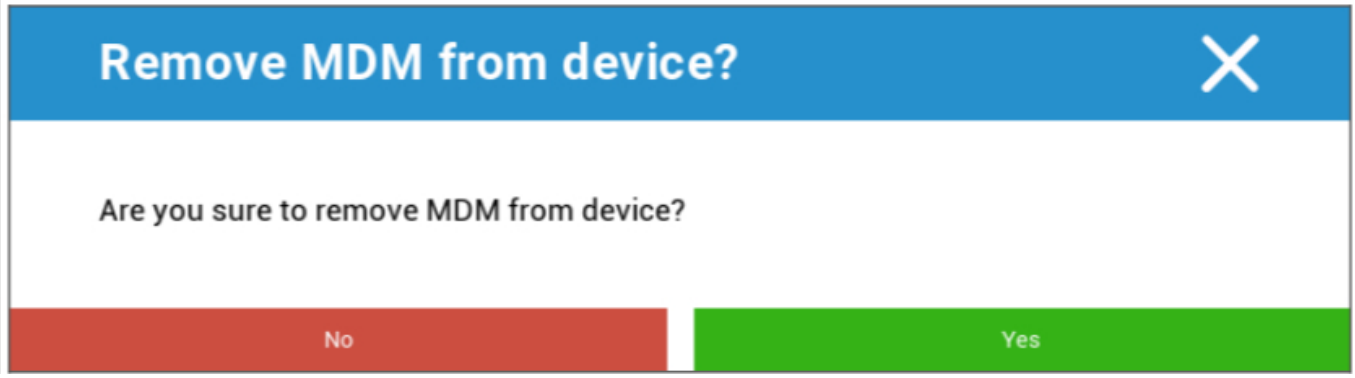
Dispositivo de limpieza

En "Borrar dispositivo" puedes realizar un borrado completo del dispositivo. A continuación, el dispositivo volverá a su configuración de fábrica.



Además, si el dispositivo contiene una tarjeta SD, puedes borrarla. Puedes conseguirlo configurando "¿Borrar también la tarjeta SD? "a "Activado".

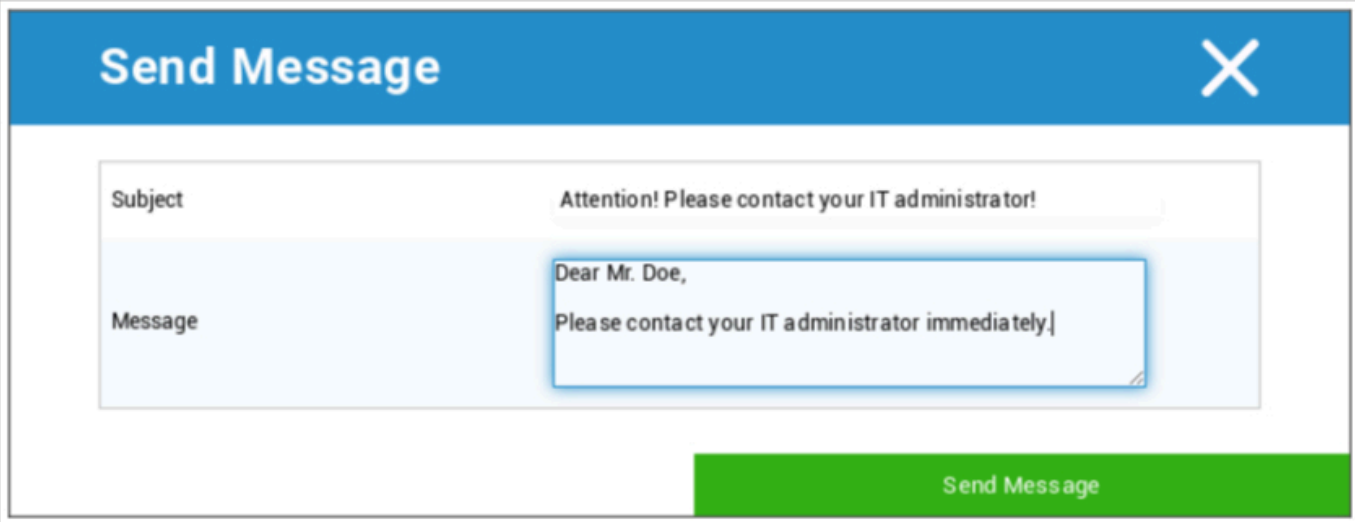
Eliminar MDM



Este es el método recomendado, para crear una separación de MDM.

Sólo se eliminan la información, las aplicaciones y los perfiles proporcionados por AppTec360, lo que significa que todos los datos corporativos dejarán de estar disponibles en el dispositivo del usuario final. La esfera privada, sin embargo, no se ve afectada y sigue permaneciendo en el dispositivo del usuario final.

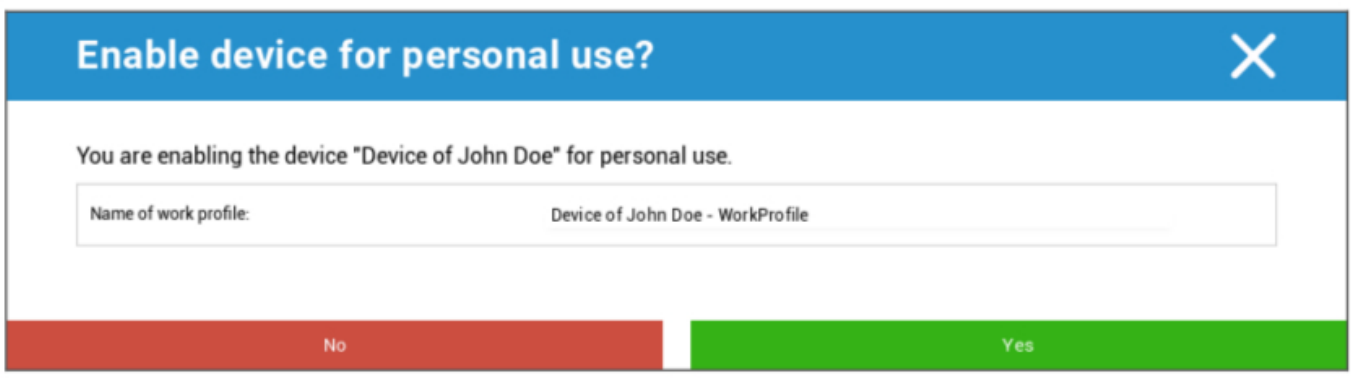
Enviar mensaje



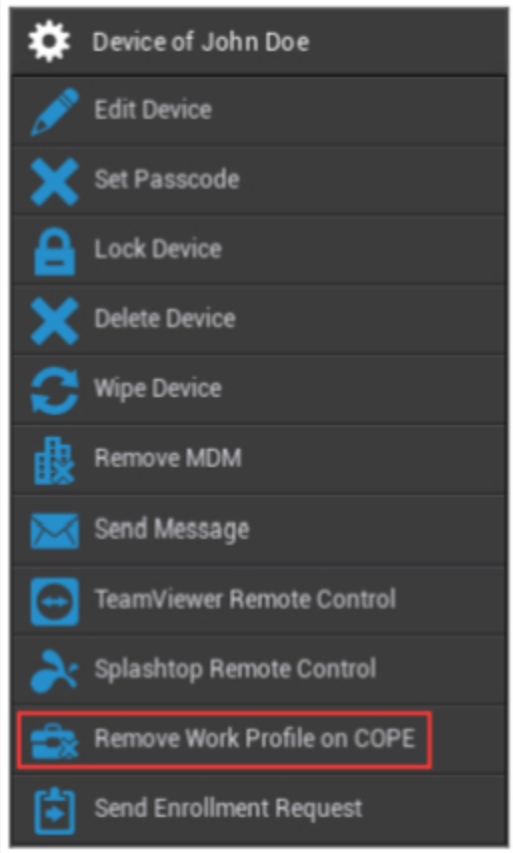
Aquí puede enviar una Notificación Push al dispositivo del usuario final correspondiente.

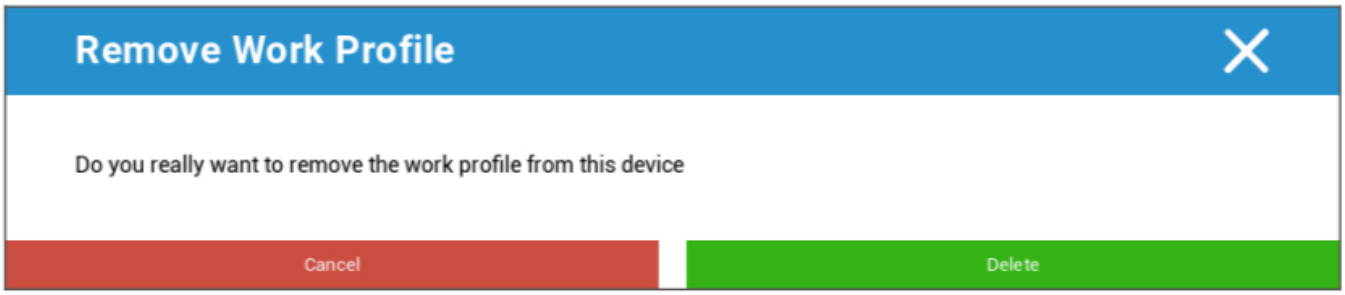
Transformación al modo COPE

Crear un perfil de trabajo en este dispositivo AE totalmente gestionado (gestionado por el trabajo)



Después de transformar el dispositivo al modo COPE, puede eliminar el perfil de trabajo haciendo clic en la opción del engranaje **Eliminar perfil de trabajo en COPE:**




Remove Work Profile
Do you really want to remove the work profile from this device
Cancel
Delete

Enviar solicitud de inscripción

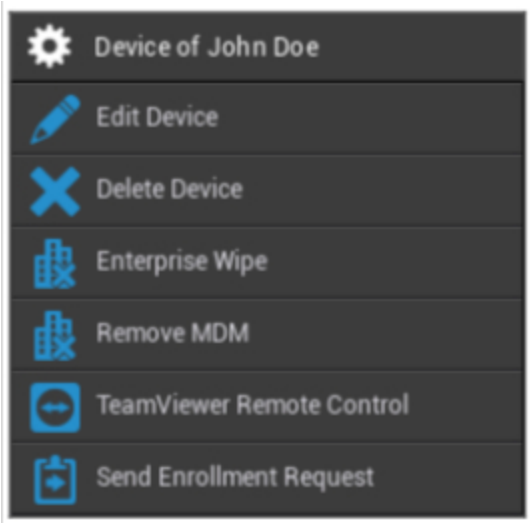
Con "Enviar solicitud de inscripción" puede enviar una solicitud de inscripción (de nuevo) al usuario correspondiente.

Tenga en cuenta que sólo es válida la solicitud de inscripción más reciente.

Migrar dispositivo heredado

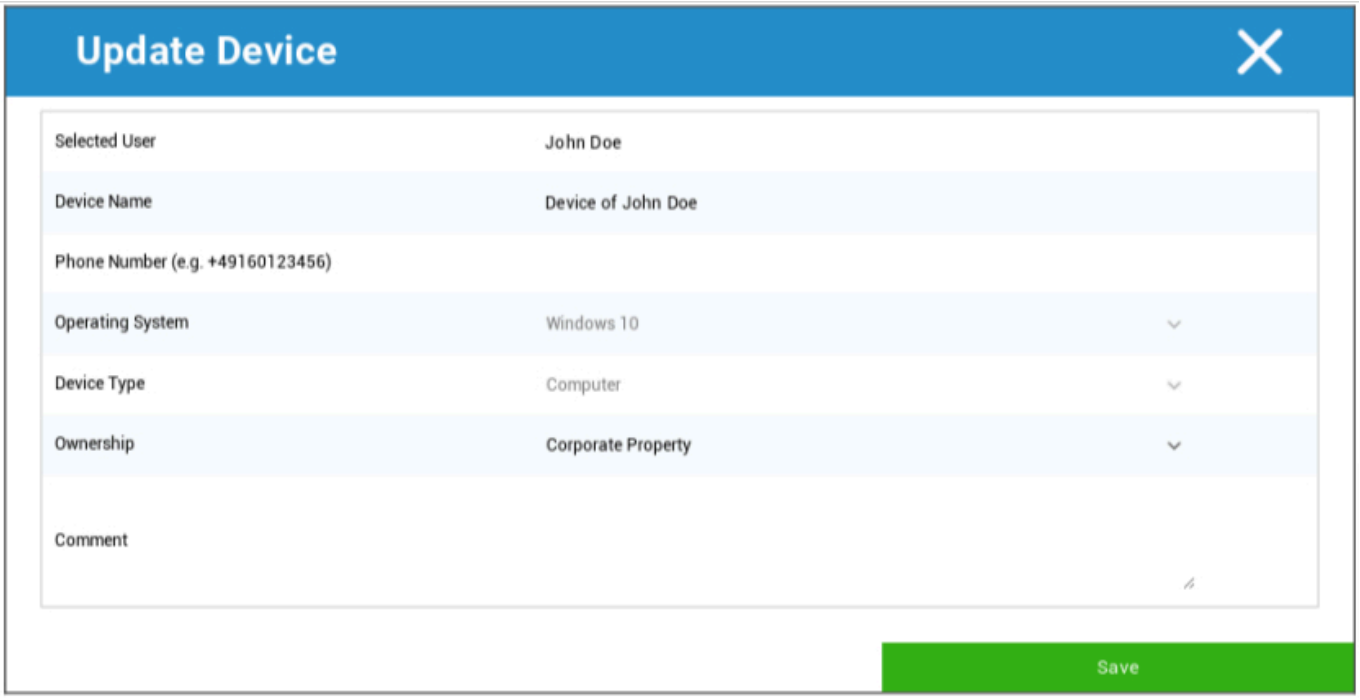
Migración del perfil de teléfono/tableta Android al perfil de dispositivo totalmente gestionado AE (gestionado por el trabajo)

Windows



Nombre del dispositivo	Nombre del dispositivo seleccionado
Editar dispositivo	Editar dispositivo
Borrar dispositivo	Eliminar dispositivo de AppTec
Limpieza de empresas	La información, las aplicaciones y el perfil proporcionados por AppTec360 se eliminan
Eliminar MDM	
Control remoto TeamViewer	Controla a distancia el dispositivo con TeamViewer
Enviar solicitud de inscripción	Enviar solicitud de inscripción (otra vez)

Editar dispositivo

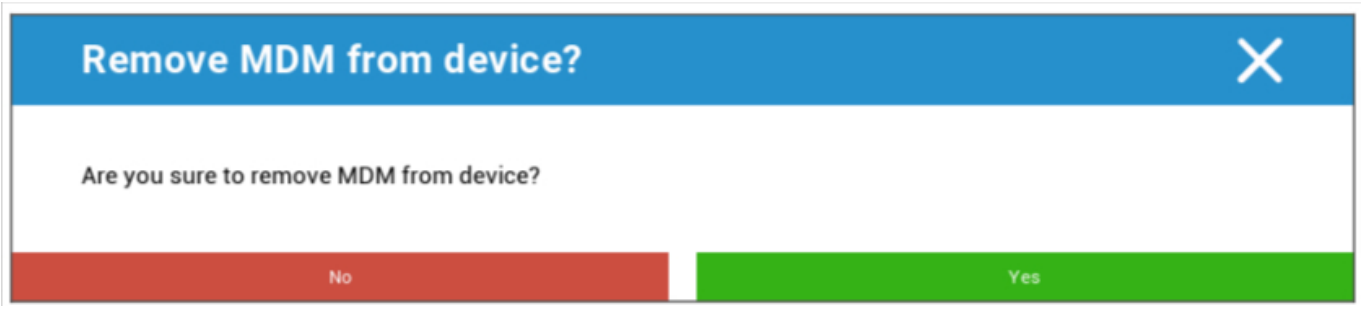


Aquí puedes actualizar diversa información sobre el dispositivo.

Borrar dispositivo

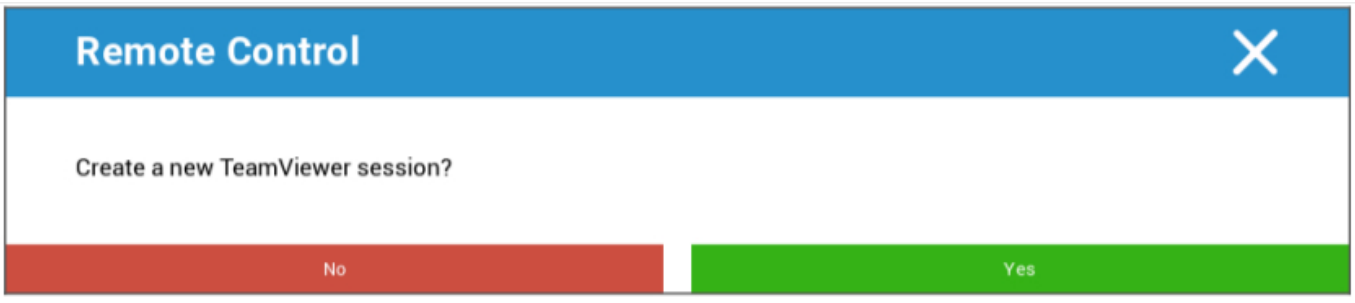
Aquí se puede ejecutar el comando de borrado que sólo elimina el dispositivo de AppTec360.

Enterprise Wipe | Eliminar MDM



Sólo se eliminan la información, las aplicaciones y los perfiles proporcionados por AppTec360. De este modo, los datos corporativos dejarán de estar disponibles en el dispositivo del usuario final. El área privada no se ve afectada y sigue permaneciendo en el dispositivo del usuario final.

Control remoto TeamViewer



Aquí puede iniciar una sesión de Control Remoto TeamViewer para este dispositivo.

Enviar solicitud de inscripción

Con "Enviar solicitud de inscripción", puede enviar una solicitud de inscripción (de nuevo) al usuario correspondiente.

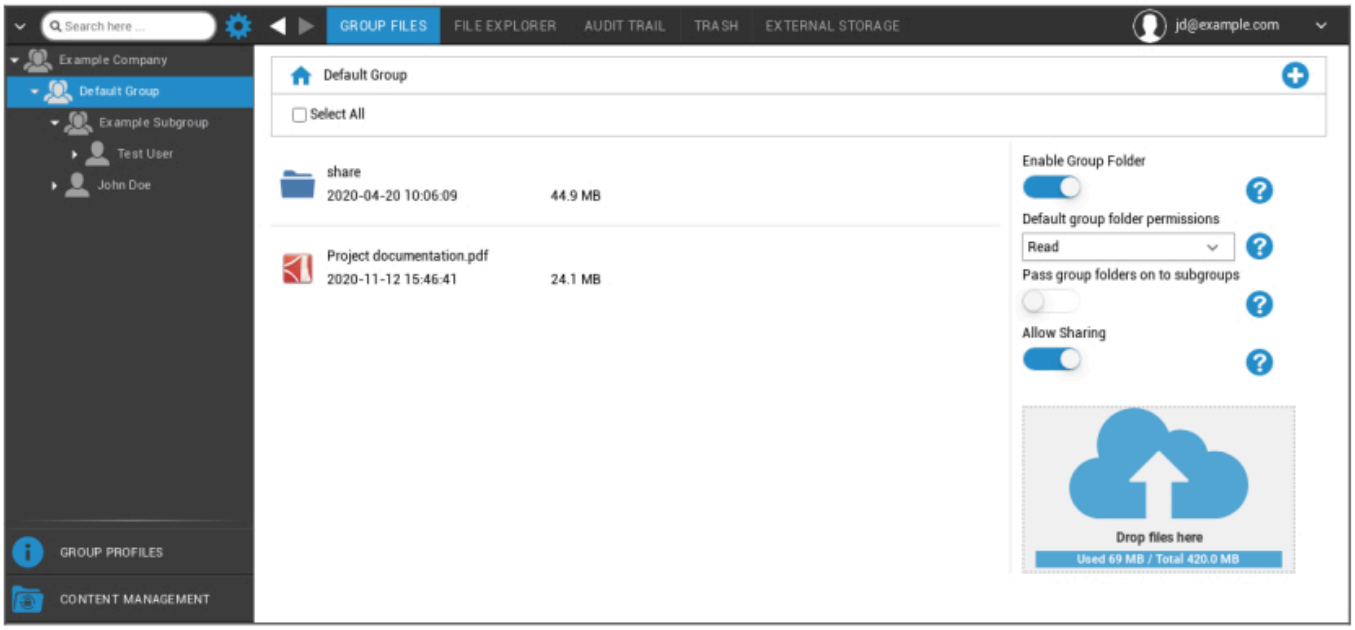
Gestión de contenidos

Cuando estás en un grupo, puedes gestionar el ContentBox de AppTec con "Gestión de contenidos".

Con Content Box puedes distribuir de forma segura documentos y otros datos corporativos a los dispositivos de los usuarios finales.

Archivos de grupo

"Agrupar Archivos" representa una parte fundamental ContentBox. Aquí estableces configuraciones, subes documentos, creas nuevas carpetas, etc.



Con el símbolo de la esquina superior derecha puede crear nuevas carpetas que se designarán al grupo correspondiente con "Añadir carpeta".

Con el símbolo de la esquina superior derecha, puede crear una nueva carpeta mediante "Añadir carpeta", que deberá asignarse al grupo correspondiente.

Puedes ponerle el nombre que quieras a la carpeta.

A través de "Cargar archivos", puedes cargar datos. Aquí se abrirá tu Explorador Estándar. Por supuesto, puedes realizar estas dos acciones en cada (sub)carpeta.

Con el símbolo de la esquina superior izquierda, puede volver al menú principal.

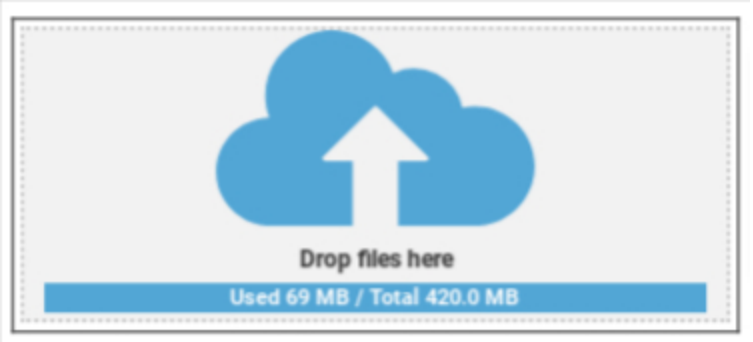
Puedes seleccionar varias carpetas y archivos y descargarlos con "Descargar" o puedes borrarlos haciendo clic en "Eliminar".

También puede seleccionar todos los archivos y carpetas con y ejecutar los comandos "Descargar" y "Eliminar".

Cuando pase el ratón por encima de una carpeta o archivo, verá la siguiente vista general:

- Con "Renombrar", puede cambiar el nombre de la carpeta/archivo
- Con "Descargar", puede descargar la carpeta/archivo
- Con "Borrar", puede borrar la carpeta/archivo

Activar carpeta de grupo	Si está activado, todos los miembros del grupo tienen acceso a la carpeta correspondiente
Permisos de carpeta de grupo por defecto	Permisos de los usuarios del grupo seleccionado: Lectura = permiso de sólo lectura Actualizar = permiso de actualización Crear = permiso de creación Borrar = permiso de borrado
Pasar carpetas de grupo a subgrupos	Si se activa, los respectivos subgrupos pueden tener acceso a los archivos de datos principales
Permisos para subgrupos	Permisos de los usuarios del subgrupo seleccionado: Lectura = permiso de sólo lectura Actualizar = permiso de actualización Crear = permiso de creación Borrar = permiso de borrado
Permitir compartir	Si está activado, el usuario puede compartir archivos a través de un enlace



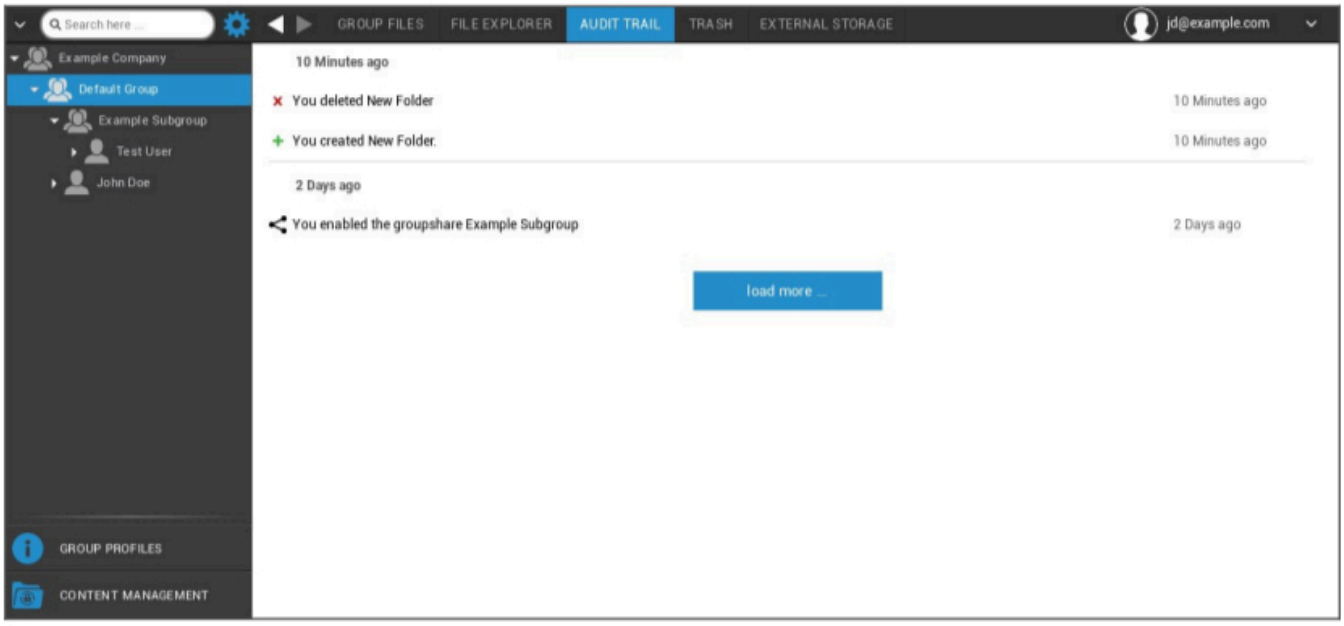
Para subir archivos, puedes utilizar este campo, arrastrando un archivo mediante arrastrar y soltar a esta ventana. También puedes hacer clic en este campo para seleccionar y subir un archivo con la ayuda de Internet Explorer.

Explorador de archivos

Con el "Explorador de archivos" puedes gestionar todas las carpetas y archivos, independientemente del grupo en el que estén archivados.

También encontrarás los ajustes y botones que conociste en "Archivos de grupo".

Registro de auditoría



En "Audit Trail", puede ver en el historial qué usuario creó, borró o compartió qué. De este modo, podrá determinar en cualquier momento qué se ha hecho con los datos de la empresa.

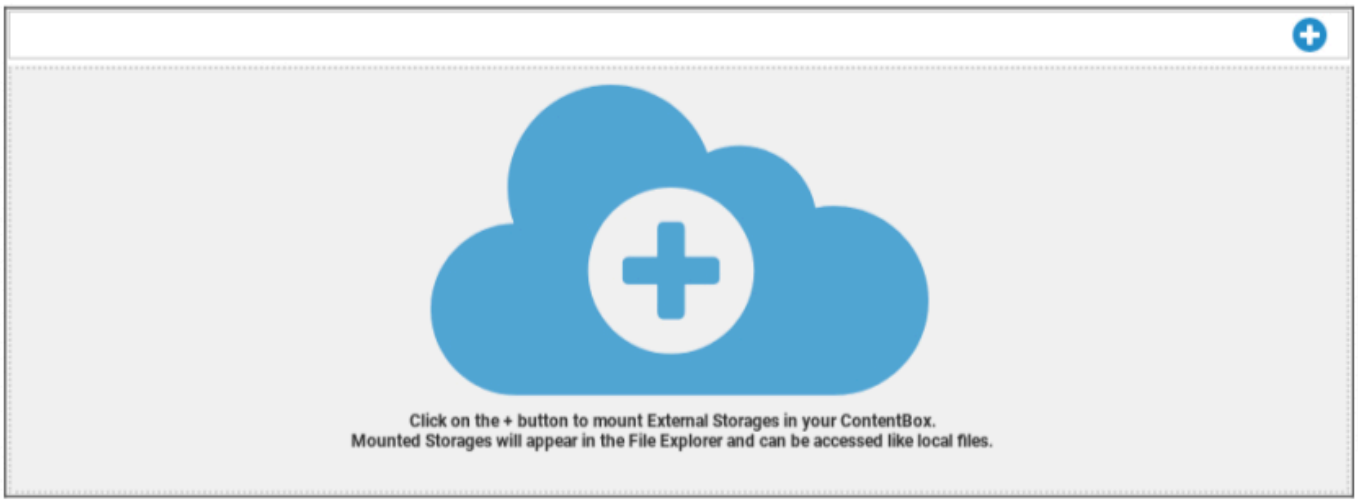
Basura

Si has borrado algo (por accidente), puedes ver las carpetas y archivos en "Papelera" y recuperarlos, según tus deseos.

- Con "Undelete", puedes recuperar los datos/carpeta.
- Con "Borrar", puede borrar definitivamente los datos/carpeta - debe confirmar el comando de borrado una vez más.

Ten en cuenta que la capacidad de almacenamiento que se está utilizando en la papelera, reduce el "Espacio Total" disponible - este es un requisito de ownCloud.

Almacenamiento externo



En el apartado "Almacenamiento externo", puedes conectar un almacenamiento externo.

Con el símbolo, se puede añadir almacenamiento (adicional).

Tipo	Amazon S3, FTP, SFTP, ownCloud, WebDAV, Windows Share, SharePoint

Amazon S3	
Mostrar nombre	Mostrar nombre
Clave de acceso	Clave de acceso
Clave secreta	Clave de seguridad
Cubo	Identidad definitiva de la subcarpeta que se te ha asignado
Nombre de host (opcional)	Nombre de host (opcional)
Puerto (opcional)	Puerto (opcional)
Región	Región (opcional)
Activar SSL	Activar SSL
Activar estilo de ruta	Borrar dirección de ruta que se te ha asignado

FTP	
Mostrar nombre	Mostrar nombre
Anfitrión	Dirección de host
Nombre de usuario	Nombre de usuario
Contraseña	Contraseña
Raíz	Menú principal
ftps seguro://	

SFTP	
Mostrar nombre	Mostrar nombre
Anfitrión	Dirección de host
Nombre de usuario	Nombre de usuario
Contraseña	Contraseña
Raíz	Menú principal

ownCloud	
Mostrar nombre	Mostrar nombre
URL	URL de ownCloud
Nombre de usuario	Nombre de usuario
Contraseña	Contraseña
Subcarpeta remota	Carpeta estándar
Asegura https://	

WebDAV	
Mostrar nombre	Mostrar nombre
URL	URL WebDAV
Nombre de usuario	Nombre de usuario
Contraseña	Contraseña
Raíz	Menú principal
Asegura https://	
Compartir en Windows	La compatibilidad con Windows Share estará disponible en breve
SharePoint	La compatibilidad con Microsoft SharePoint estará disponible en breve

Registro de auditoría

Aquí puedes encontrar un log que registra información sobre las acciones que se realizan en la consola MDM.

Con el icono de filtro puede aplicar filtros a la lista mostrada.

Con el menú desplegable **Elementos por página**: puede seleccionar la cantidad de elementos que se mostrarán en una página de la lista.

Acción tomada / Configuración modificada	La acción realizada / El ajuste modificado
Valor	El valor de la acción realizada / ajuste modificado
Usuario	El nombre del usuario que ha realizado la acción / ha cambiado la configuración
Fecha	La marca de tiempo de cuando se realizó esta acción / se cambió esta configuración
Ruta / Tipo	La ruta hacia donde se realizó esta acción / se cambió esta configuración

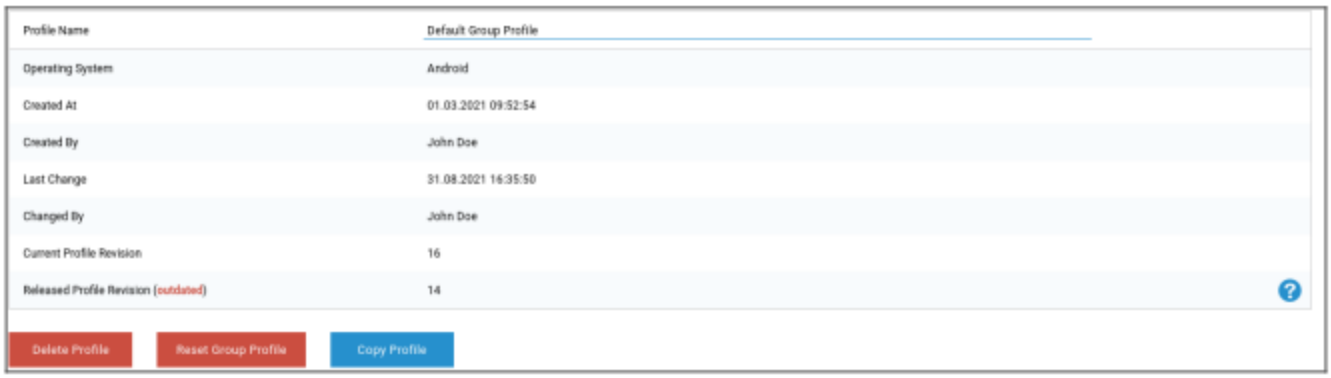
Configuración de iOS

General

Dependiendo de si ha seleccionado un grupo o un dispositivo, la visualización y sus subpuntos son diferentes.

Resumen del perfil del grupo (sólo a nivel de grupo)

Al abrir un perfil de grupo, obtendrá una rápida visión general del perfil



Nombre del perfil	Nombre del perfil (se puede cambiar aquí)
Sistema operativo	Sistema operativo para el que es el perfil
Creado en	Momento de la creación
Creado por	El creador del perfil
Último cambio	Hora de la última modificación del perfil
Cambiado por	Cuenta que realizó los últimos cambios
Revisión actual del perfil	Revisión del estado del perfil guardado
Revisión del perfil liberado	Revisión del perfil asignado ("Asignar ahora"). Si la etiqueta muestra "(obsoleto)" detrás del texto, significa que has guardado el perfil pero aún no lo has asignado, por lo que los dispositivos seguirán recibiendo una versión antigua.

Información general

Si se encuentra directamente en el dispositivo, recibirá una breve descripción del dispositivo seleccionado.

Nombre del dispositivo	Nombre del dispositivo
Número de teléfono	Número de teléfono del dispositivo
Modelo	Número de modelo
Sistema operativo	OS
Número de serie	Número de serie del dispositivo
Propiedad del dispositivo	Dispositivo corporativo o privado Corporativo = dispositivo corporativo Empleado = dispositivo privado
Tipo de dispositivo	Tipo de dispositivo (tableta o teléfono)
Jailbroken	Si hay un Jailbreak en el dispositivo
Supervisado	Indica si se trata de un dispositivo supervisado
Cumple	Si se infringió alguna directriz
Visto por última vez	Estado de la última vez que el dispositivo se comunicó con el Servidor AppTec360

Ajustes

Estos ajustes contienen el nombre del dispositivo y un fondo predefinido.

Nombrar el dispositivo con el nombre del sistema	El nombre que se emitirá en la Consola AppTec360 (en la estructura jerárquica izquierda), será el mismo que en el respectivo dispositivo del usuario final (se puede ver en la configuración del dispositivo).
Utilizar papel tapiz personalizado (sólo dispositivos supervisados)	Aquí puedes predefinir el fondo que se mostrará en el dispositivo del usuario final (por ejemplo, para un tipo de marca corporativa para el dispositivo). ¡Sólo está disponible en Modo Supervisado!
Actualizaciones automáticas del SO	Fuerza las actualizaciones del SO si están disponibles. Sólo para dispositivos DEP en modo supervisado.
Fuentes personalizadas	Aquí puedes añadir fuentes personalizadas.
Nombre	Opcional. El nombre visible para el usuario de la fuente. Este campo se sustituye por el nombre real de la fuente tras la instalación.
Fuente	Sube el archivo de fuente (.otf o .ttf).

Config Revisión

Aquí obtendrá una visión general de qué perfil de grupo está designado al dispositivo.

Si haces clic en el perfil del grupo, accederás directamente al perfil y podrás realizar ajustes.

Con el símbolo, puedes revertir las aplicaciones asignadas a la configuración del perfil de grupo.

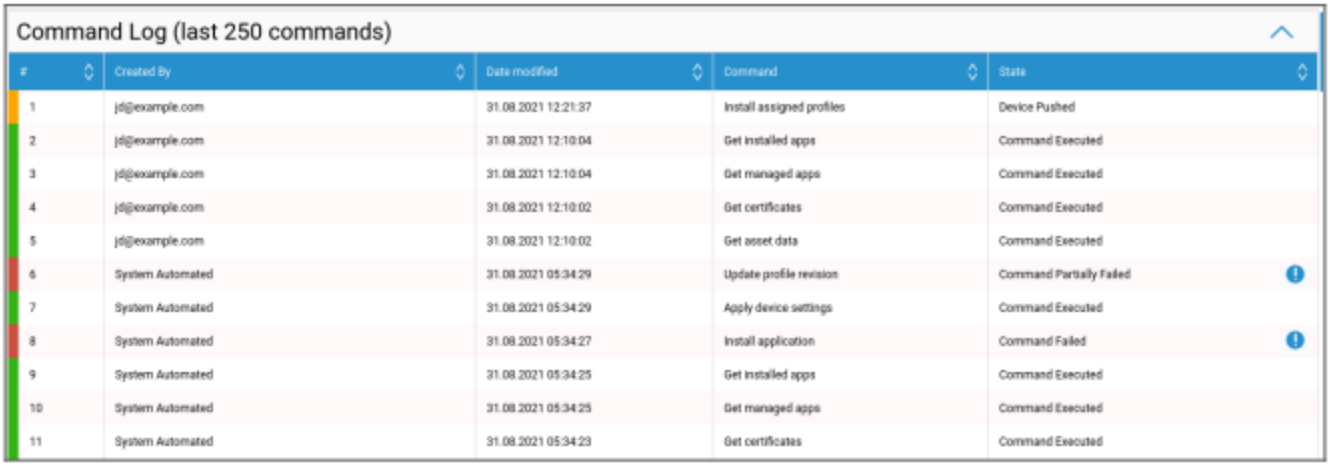
Con el símbolo, puedes restablecer el perfil del dispositivo para que no tenga ninguna configuración.

"Nueva revisión disponible" indica que el perfil de grupo se ha modificado y guardado, pero no se ha asignado. El perfil de grupo debe asignarse con "Asignar ahora" a nivel de grupo para aplicar los cambios a los dispositivos.

Registro de dispositivos (sólo a nivel de dispositivo)

Registro de comandos

Aquí puede ver qué comandos se emitieron para el dispositivo y cuál es su estado.



Los comandos creados por "Sistema automatizado" son creados automáticamente por el sistema.

Posibles estados del comando

Dispositivo Empujado	Se ha enviado una solicitud push al servicio push (por ejemplo, APNS) para indicar al dispositivo que se conecte de nuevo al servidor EMM.
Comando creado	El comando se creó en el sistema.
Orden enviada	El comando se envió al dispositivo después de que se conectara al servidor.
Orden ejecutada	El comando se ha ejecutado correctamente.
Comando fallido	El comando falló. *
Comando parcialmente fallido	Dependiendo del SO del dispositivo, algunos comandos pueden agruparse. En este fallaron algunas partes de este grupo de comandos. *
Orden ejecutada, finalmente fallida	La orden se ejecutó, pero puede que no.
Comando Repulsado	El comando fue repulsado por un usuario.
Descartado	El comando fue descartado. Por ejemplo, porque ha sido sustituido por otro comando o porque el dispositivo se ha reinscrito y se han eliminado los comandos antiguos.

Si hay un signo de exclamación detrás del mensaje, puede obtener más información pasando el cursor sobre el icono.

Gestión de activos (sólo a nivel de dispositivo)

Gestión de activos (sólo a nivel de dispositivo)

Información del dispositivo

Modelo	Número de modelo del dispositivo
Sistema operativo	OS
Versión del SO	Versión del SO
Número de serie	Número de serie
UDID	UDID del dispositivo
Nombre del dispositivo	Nombre del dispositivo
Supervisado	Muestra si el dispositivo está supervisado
Estado de la batería	Estado de la batería

Wi-Fi

Dirección IP	Dirección IP del dispositivo
WiFi MAC	Dirección MAC WiFi

Móvil

Estado	Estado (tarjeta SIM presente)
Número de teléfono	Número de teléfono
Estado de itinerancia	Estado actual de la itinerancia
Itinerancia (Voz/Datos)	Estado de itinerancia para voz/datos
Dirección IP	Dirección IP
IMEI	Número IMEI
Operador/Transportista	Proveedor de servicios móviles
SIM Red del operador	SIM red portadora
Versión portadora	Versión portadora
Firmware del módem	Firmware del módem
MCC/MNC actual	Ver "SIM MCC/MNC"
SIM MCC/MNC	El código de país móvil es una identificación de país establecida por la UIT según la Norma E.212, que, junto con el código de red móvil (MNC), se utiliza para identificar una red celular (=código de país) Por tanto, cuando entras en otra red móvil, el "MCC/MNC actual" y el "MCC/MNC de la SIM" son diferentes.

Bluetooth

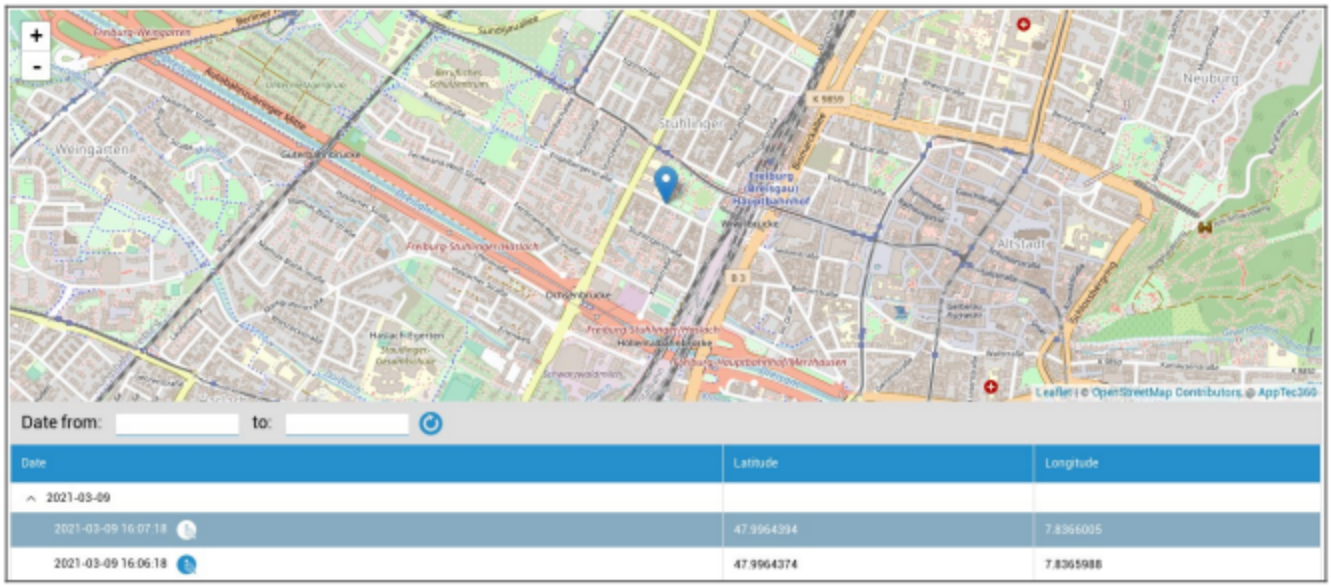
Bluetooth MAC	Dirección MAC Bluetooth

Gestión de la seguridad

Antirrobo (sólo en el dispositivo)

Información GPS (sólo a nivel de dispositivo)

Aquí puede evaluar la ubicación actual/última del dispositivo. La localización puede protegerse con una o incluso dos contraseñas - Ver: Configuración general - Privacidad - Acceso GPS



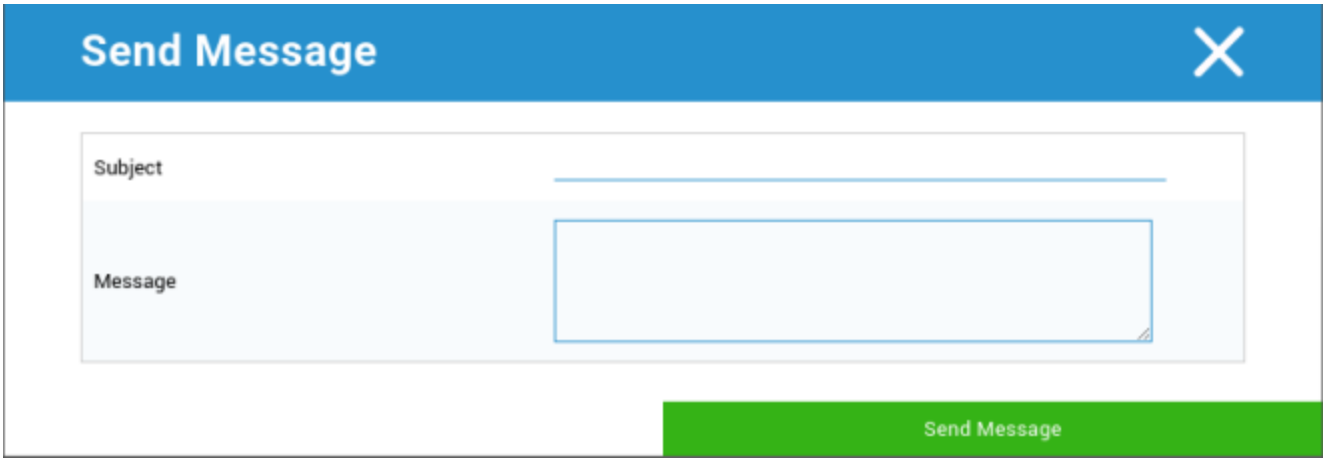
Limpiar y bloquear (sólo a nivel de dispositivo)

En "Limpiar y bloquear", puedes realizar las tres acciones siguientes:

Limpieza total	El dispositivo se restaura a sus valores de fábrica (se borran tanto los datos corporativos como los personales).
Limpieza de empresas	Sólo se eliminan los datos corporativos del dispositivo del usuario final (todas las aplicaciones, datos, etc. que fueron proporcionados por AppTec)
Pantalla de bloqueo	El bloqueo de pantalla está activado, basta con desbloquear el dispositivo con la contraseña/PIN del dispositivo
Bloqueo Forense (sólo Dispositivos Supervisados)	Si se activa esta función con el símbolo  , el dispositivo se bloqueará, mostrando un mensaje, que no se podrá cerrar. El empleado tampoco podrá desbloquear el dispositivo. Sólo el administrador puede desbloquear el dispositivo en la consola con el símbolo de desbloqueo  .
Permitir bloqueo de activación (sólo dispositivos supervisados)	Si se activa esta función, el dispositivo se bloqueará en cuanto se active "Buscar mi iPhone" en los ajustes de iCloud.

Mensaje (sólo a nivel de dispositivo)

Con la siguiente ventana, puede rellenar el asunto y un mensaje y enviarlo a un dispositivo de usuario final:



Configuración de seguridad

Código

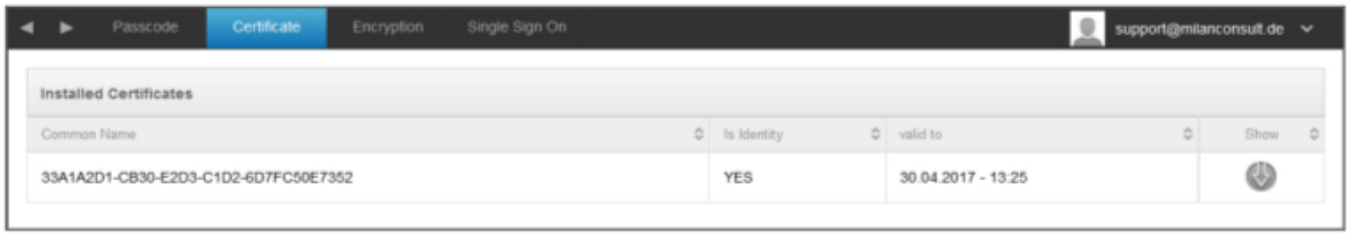
Aquí se establecen los ajustes para la contraseña del dispositivo

Se permite la desactivación del código	Cuando esta opción está activada, no se pide introducir una contraseña En cuanto se establece una contraseña, no se puede desactivar
Permitir valor simple	Permitir al usuario utilizar las mismas cadenas de números, escalando y reduciendo (ej. 1234, 1111)
Requiere valor alfanumérico	Las contraseñas deben contener al menos una letra
Longitud mínima del código de acceso	Longitud mínima de la contraseña
Número mínimo de caracteres complejos	Número mínimo de símbolos alfanuméricos en la contraseña
Edad máxima del código de acceso	Número de días tras los cuales debe cambiarse la contraseña
Bloqueo automático máximo	Tiempo máximo tras el cual se bloquea el dispositivo
Periodo máximo de gracia para el bloqueo del dispositivo	Tiempo, tras el cual el dispositivo entra en modo Stand-By bloqueado
Número máximo de intentos fallidos	Establece cuántas veces se puede introducir incorrectamente una contraseña, antes de que se realice un borrado completo del dispositivo.
Antigüedad máxima del código de acceso (1-730 días)	Antigüedad máxima de la contraseña
Historial de contraseñas (1-50 contraseñas)	Se permite el uso de una contraseña antigua después de este número

Al hacer clic en la papelera, se abre el cuadro de diálogo de restablecimiento de contraseña, con el que se puede borrar una contraseña olvidada del dispositivo.

Certificado (sólo a nivel de dispositivo)

Muestra los certificados disponibles en el dispositivo


Passcode
Certificate
Encryption
Single Sign On
support@mlianconsult.de
Installed Certificates
Common Name
Is Identity
valid to
Show
33A1A2D1-CB30-E2D3-C1D2-6D7FC50E7352
YES
30.04.2017 - 13:25

Cifrado

Exigir encriptación del almacenamiento	Activa la función de encriptación del dispositivo instalado

Inicio de sesión único

En el punto "Single Sign-On", puede configurar la autenticación Kerberos.

Aquí se establecen las credenciales de acceso y las respectivas URLs / Apps que pueden utilizar los tokens Kerberos.

Disponible en modo supervisado	
Nombre de la cuenta	Nombre de la cuenta
Nombre principal	Identidad única a la que se pueden distribuir Tickets Kerberos
Reino	Tu dominio Kerberos que se va a utilizar (por ejemplo, tu dominio)

Con el Símbolo, puede establecer URL adicionales.

Patrón de URL utilizado para limitar esta cuenta	URLs por determinar, a las que se pueden distribuir Tickets Kerberos

Con el Símbolo, puedes establecer Apps adicionales.

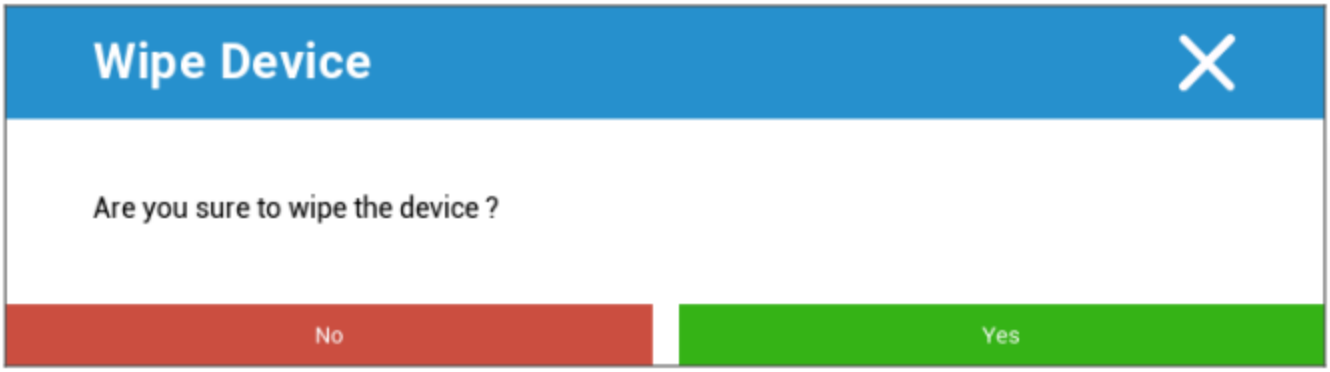
Aplicaciones para limitar esta cuenta	Apps por determinar, a las que se pueden distribuir Tickets Kerberos

Fin de vida útil (sólo a nivel de dispositivo)

Limpiar (sólo a nivel de dispositivo)

En "Borrar", puedes restaurar el dispositivo a su configuración de fábrica. Aquí se borrarán tanto los datos corporativos como los privados del dispositivo del usuario final.

Al hacer clic en el "símbolo menos" debería recibir el siguiente mensaje



Con "Sí" puede realizar el borrado.

En "Informe de limpieza" se pueden visualizar los siguientes elementos

Borrado por	Historial de quién realizó la limpieza
Fecha	Fecha
Estado	Estado (por ejemplo, si el borrado se ha realizado correctamente)

Configuración de restricciones

Funcionalidad del dispositivo

Aquí puede bloquear funcionalidades individuales del dispositivo del usuario final

Permitir instalar apps	Permitir la instalación de apps
Permitir cámara	Permitir el uso de la cámara
Permitir FaceTime	Permitir FaceTime
Permitir captura de pantalla	Permitir captura de pantalla
Permitir sincronización automática en itinerancia	Permitir sincronización automática en itinerancia
Permitir Siri	Permitir Siri
Permitir marcación por voz	Permitir marcación por voz
Permitir la compra dentro de la aplicación	Permitir la compra dentro de la aplicación
Requerir la contraseña del iTunes Store para todas las compras	Requerir la contraseña del iTunes Store para todas las compras
Permitir el juego multijugador	Permitir el juego multijugador
Permitir añadir amigos de Game Center	Permitir añadir amigos de Game Center
Permitir abrir de gestionado a no gestionado	Permitir abrir contenido de apps gestionadas en apps no gestionadas
Permitir abrir de no gestionado a gestionado	Permitir abrir contenido de apps no gestionadas en apps gestionadas
Permitir la vista de hoy en la pantalla de bloqueo	Cuando este ajuste está activado, la vista "Hoy" se mostrará en el Centro de Notificaciones de la pantalla de bloqueo
Permitir el centro de control en la pantalla de bloqueo	Permitir el Centro de Control en la pantalla de bloqueo
Permitir TouchID	Permitir TouchID
Permitir actualizaciones PKI por aire	Permitir actualizaciones PKI por aire

Permitir libreta mientras está bloqueada	Permitir libreta mientras el dispositivo está bloqueado
Limitar el seguimiento de anuncios	Esta función desactiva el Ad Tracking (por ejemplo, los anunciantes no pueden utilizar Ad Tracking para distribuir anuncios personalizados)
Permitir traspaso	Permitir traspaso
Permitir resultados de internet en primer plano	Permitir resultados de Internet en el centro de atención (por ejemplo, Bing o Wikipedia)
Requerir código de acceso en el primer emparejamiento AirPlay	Requerir código de acceso en el primer emparejamiento AirPlay
Protección de muñeca Reloj de Fuerza	Si se activa, el Apple Watch se ve obligado a utilizar la "Protección de muñeca" (reconocimiento de muñeca)
Permitir Fototeca de iCloud	Permite la Fototeca de iCloud. Si no se permite, todas las fotos que no se hayan descargado completamente de iCloud, se borrarán en el almacenamiento local
Disponible en el modo supervisado	
Permitir la modificación de la cuenta	Permitir la modificación de "correo, contactos, calendario
Permitir AirDrop	Permitir AirDrop
Permitir la Modificación Celular de la App	Este ajuste bloquea la configuración de las aplicaciones a las que se permite utilizar datos móviles Esta configuración puede, por ejemplo, establecerse manualmente en el dispositivo del usuario final y luego activar esta restricción
Permitir que Siri consulte contenido generado por el usuario desde la web	Se bloquea la búsqueda en determinados sitios web, por ejemplo Wikipedia, porque cada uno puede hacer los cambios que quiera
Activar el filtro de blasfemias de Siri	Las blasfemias dirigidas a Siri se censuran
Permitir iBook Store	Permitir iBook Store
Permitir iBook Store Erótica	Permitir iBook Store Erótica
Permitir modificar la configuración de Buscar a mis amigos	Permitir modificar la configuración de Buscar a mis amigos

Permitir Game Center	Permitir Game Center
Permitir emparejamiento de anfitriones	Emparejamiento del ordenador de control
Permitir instalar perfiles de configuración	Permitir la instalación de perfiles de configuración
Permitir Eliminar App	Controlar la eliminación de aplicaciones
Permitir iMessage	Permitir iMessage
Permitir borrar todos los contenidos y ajustes	Permitir el borrado de todos los contenidos y ajustes
Permitir configurar restricciones	Permitir configurar restricciones
Permitir Podcast	Permitir Podcast
Permitir búsqueda de definiciones	Permitir la búsqueda de definiciones
Permitir teclado predictivo	Permitir teclado predictivo
Permitir autocorrección	Permitir autocorrección
Permitir la instalación de aplicaciones UI	Si se desactiva, no se podrán instalar aplicaciones desde la AppStore pública (el icono dejará de mostrarse). Sin embargo, se pueden seguir instalando aplicaciones a través de iTunes y el Configurador
Permitir atajos de teclado	Permitir atajos de teclado, si el dispositivo está conectado a un teclado físico
Permitir el emparejamiento del Apple Watch	Prohíbe el emparejamiento entre el dispositivo y el Apple Watch, las conexiones existentes se interrumpirán
Permitir la modificación del código de acceso	Si no se permite, no se puede añadir, cambiar o eliminar ninguna contraseña de dispositivo
Permitir la modificación del nombre del dispositivo	Directriz para determinar si se puede cambiar el nombre del dispositivo
Permitir la modificación del papel pintado	Directriz para determinar si se puede cambiar el papel pintado
Permitir descargas automáticas de apps	Si se desactiva, una aplicación comprada no se instalará automáticamente en otros dispositivos. No se aplica a las actualizaciones de aplicaciones existentes
Permitir Noticias	Permitir Noticias en el dispositivo iOS

Permitir la confianza en las aplicaciones de empresa	Si se establece en false, impide confiar en las aplicaciones empresariales

iCloud

Bloquear ciertas funcionalidades durante el emparejamiento de iCloud

Permitir copia de seguridad	Permitir copia de seguridad
Permitir la sincronización de documentos	Permitir la sincronización de documentos
Permitir secuencia de fotos	Permitir secuencia de fotos
Permitir flujo de fotos compartido	Permitir flujo de fotos compartido
Permitir sincronización de llaveros en la nube	Permitir sincronización de llaveros en la nube
Permitir que las apps gestionadas almacenen datos	Permitir que las apps gestionadas almacenen datos
Permitir la sincronización de notas y destacados para los libros de empresa	Permitir la sincronización de notas y destacados para los libros de empresa
Permitir la copia de seguridad de los libros de la empresa	Permitir la copia de seguridad de los libros de la empresa

Seguridad y privacidad

Bloquear estas funcionalidades asociadas a los datos de diagnóstico

Permitir el envío de datos de diagnóstico a Apple	Permitir el envío de datos de diagnóstico a Apple
Permitir al usuario aceptar certificados TLS no fiables	Permitir al usuario aceptar certificados TLS no fiables
Forzar copias de seguridad encriptadas	Forzar copias de seguridad encriptadas

BYOD

Seguridad integrada en iOS (contenedor)

iOS siempre fue capaz de diferenciar entre gestionado (empresarial) y no gestionado (privado). Todo lo que procede del Sistema MDM se trata como gestionado. Por ejemplo, si instala una aplicación a través de MDM o configura una cuenta de Exchange, se considerará gestionada por iOS.

Todo lo demás que se configure/instale manualmente en el dispositivo se tratará como no gestionado. Por ejemplo, si el usuario instala WhatsApp por su cuenta o si añade una cuenta de Exchange. Sin embargo, esta separación nunca afectó a los contactos. Pero desde iOS 11.3 (y superior) esto también se añadió para los contactos.

Dado que se trata de una funcionalidad básica del sistema operativo, no es necesario instalar nada ni configurar un contenedor especial.

Activa la función integrada para separar las aplicaciones/información/archivos privados de los de trabajo. Este ajuste también desactivará algunas otras funciones, que de otro modo podrían apagar partes de esta separación por error.

Activación

Activar las soluciones de contenedor compatibles con AppTec360

Activar el contenedor Google Divide	Activar el contenedor Google Divide
Activar Contenedor SecurePIM	Activar Contenedor SecurePIM

Si has activado el Contenedor SecurePIM, también encontrarás el siguiente punto en "Activación". Además, enseguida se abrirán cuatro pestañas más, que se describen a continuación.

Dirección de correo electrónico de asistencia	Dirección de correo electrónico de asistencia a la que puede dirigirse un usuario con problemas

Contraseña de SecurePIM

En "Contraseña SecurePIM", puede establecer las directrices para la fuerza de seguridad de la contraseña.

Tiempo de espera de la sesión	Aquí puedes establecer después de cuántos minutos se debe volver a introducir una nueva contraseña, una vez que SecurePIM se ejecuta en segundo plano
Longitud de la contraseña	Longitud de la contraseña de acceso al Contenedor SecurePIM
Caracteres en mayúsculas	Mínimo de mayúsculas
Caracteres en minúsculas	Mínimo de caracteres en minúsculas
Caracteres especiales	Caracteres especiales mínimos
Dígitos	Dígitos mínimos
Aplicación de toallitas	Número de veces que se puede introducir incorrectamente una contraseña, antes de que se borre el contenido de SecurePIM (La App, sin embargo, sigue estando en el dispositivo del usuario final)

Seguridad SecurePIM

En "Seguridad SecurePIM", puede establecer diversos ajustes de seguridad.

Detectar dispositivos con Jailbreak	Si se activa esta opción, se bloqueará el acceso al Contenedor SecurePIM en cuanto se detecte que el dispositivo tiene jailbreak.
Campos de texto seguros	El contenido de los campos de envío estará encriptado, ninguna información llega al sistema operativo (iOS) Nota: Mientras este ajuste esté activo, la autocorrección ya no estará disponible
Exportar datos de contacto al dispositivo	Si esta opción está activada, el usuario podrá exportar los contactos de Exchange a su dispositivo local. Nota: Sólo se exportan el nombre y el número de teléfono
Mostrar lugar del evento	Si se activa este ajuste, la ubicación de los próximos eventos se mostrará en la barra de notificaciones
Mostrar título del evento	Si se activa esta opción, se mostrará el título del próximo evento en la barra de notificaciones

Navegador SecurePIM

Aquí puede configurar el navegador de SecurePIM.

Con el símbolo puede definir una nueva URL.

Con el símbolo puede volver a eliminar una URL definida.

Las "URL de la lista blanca" son URL que se pueden cargar.

Las "URL de la lista negra" son URL que no se pueden cargar y, por tanto, están bloqueadas.

Tenga en cuenta que las entradas de la lista blanca tienen mayor prioridad que las de la lista negra. En "Título del marcador" puede emitir un título. Con "URL del marcador", puede asociar la dirección URL al título del marcador - de esta forma puede distribuir marcadores individualizados a los respectivos usuarios.

Intercambio

En "Exchange" puede configurar una cuenta Exchange.

Dirección de correo electrónico de ActiveSync	Dirección de correo electrónico de Exchange (fíjate en los "Marcadores de posición")
Inicio de sesión en ActiveSync Exchange	Intercambia nombres de usuario (fíjate en los "Marcadores de posición")
Servidor Exchange ActiveSync	Dirección del servidor Exchange (FQDN)
ActiveSync Dominio Exchange	Dirección del dominio Exchange
Certificado de usuario	Certificado de usuario
Autenticación basada en certificados	El usuario se autentica con un certificado
Permitir encriptación S/MIME	Permite al usuario encriptar su correo
Permitir firma S/MIME	Permite al usuario firmar su correo
Comprobación CRL	Si está activo, el certificado privado se comparará con la CRL (Lista de Revocación de Certificados)

Gestión de conexiones

Wi-Fi

Identificador del Conjunto de Servicios (SSID)	SSID de la red que se va a conectar
Autounión	Activar la unión automática al unirse a una red
Red oculta	Activar, en caso de que el AP no emita el SSID

Configuración del proxy

Configuración de un proxy para cada punto de acceso

Ninguno	No establecer Proxy
Manual	Establecer un Proxy manual
URL del servidor proxy	Dirección para acceder a la configuración del proxy
Puerto	Establecer el puerto para el Proxy
Autenticación	Nombre de usuario para la autenticación en el Proxy
Contraseña	Contraseña para la autenticación en el Proxy
Automático	Establecer un Proxy automáticamente
URL del servidor proxy	URL para acceder a la configuración del Proxy

Tipo de seguridad

Establecer el tipo de seguridad para el AP

WEP	
Contraseña	Contraseña para el PA

WPA/WPA2	
Contraseña	Contraseña para el PA

WEP Empresa - WPA / WPA2 Empresa - Cualquier Empresa			
	Protocolos		
	TLS	Activar/Desactivar	
	TTLS	Activar/Desactivar	
	LEAP	Activar/Desactivar	
	PEAP	Activar/Desactivar	
	EAP-FAST	Activar/Desactivar	
	EAP-SIM	Activar/Desactivar	
	Utiliza PAC		Uso del PAC (Control de Acceso Protegido)
	Disposición PAC	Configuración de Provisión PAC	
	Provisión PAC Anónima	Provisión anónima de PAC	
	Autenticaciones internas	Protocolo de autenticación que debe utilizarse: PAP, CHAP, MSCHAP, MSCHAPv2	
	Nombre de usuario	Nombre de usuario de autenticación	
	No utilices la contraseña por conexión	No utilices la contraseña por conexión	
	Certificado de Identidad	Cargar/seleccionar certificado de autenticación	
	Identidad exterior	Identidad visible externamente	
	Confía en		
	Certificado de confianza 1	Subir el primer certificado de confianza	
	Certificado de confianza 2	Sube el segundo certificado de confianza	
	Certificado de confianza 3	Subir un tercer certificado de confianza	
	Nombres de certificados de servidores de confianza	Los nombres de los certificados de servidor esperados (en una lista separada por comas)	

Ninguno	No establecer seguridad

VPN

Nombre de la conexión	Nombre del perfil VPN

Tipo de VPN

VPN

Todo el tráfico de red del dispositivo se enrutará a través de una conexión VPN.

Tipo de conexión	Establecer tipo de conexión VPN
IPsec (cisco)	Protocolo IPsec de Cisco
PPTP	Protocolo PPTP
L2TP	Protocolo L2TP
Cisco AnyConnect	Protocolo AnyConnect
SSL Juniper	Protocolo SSL Juniper
F5 SSL	Protocolo SSL F5
SonicWall mConnect	Conexión móvil SonicWall
Aruba VIA	Protocolo Aruba VIA
SSL personalizado	Conexión mediante SSL personalizado
OpenVPN	Protocolo OpenVPN

VPN por aplicación

Al abrir una aplicación determinada, se establecerá una conexión VPN.

Iniciar automáticamente la conexión VPN por aplicación		Iniciar automáticamente la conexión VPN por aplicación
Tipo de conexión		Establecer tipo de conexión VPN
	Cisco AnyConnect	Protocolo AnyConnect
	SSL Juniper	Protocolo SSL Juniper
	F5 SSL	Protocolo SSL F5
	SonicWall mConnect	Conexión móvil SonicWall
	Aruba VIA	Protocolo Aruba VIA
	SSL personalizado	Conexión mediante SSL personalizado
	OpenVPN	Protocolo OpenVPN

Configuración del proxy

Configuración de un proxy para la conexión VPN

Ninguno	No establecer Proxy
Manual	Establecer manualmente un Proxy
URL del servidor proxy	Dirección para acceder a la Configuración del Proxy
Puerto	Establecer el puerto para el Proxy
Autenticación	Nombre de usuario para la autenticación en el Proxy
Contraseña	Contraseña para la autenticación en el Proxy
Automático	Establecer un Proxy automáticamente
URL del servidor proxy	URL para acceder a la configuración del Proxy

Mostrar marcadores de posición	Muestra todas las variables de usuario disponibles , que AppTec360 puede utilizar

APN

Nombre del punto de acceso	Nombre del punto de acceso
Nombre de usuario del punto de acceso	Nombre de usuario del Punto de Acceso
Contraseña del punto de acceso	Contraseña del punto de acceso
Servidor Proxy	Dirección del servidor proxy
Puerto	El puerto Proxy correspondiente

Móvil

Activar Itinerancia de Datos	Activar Itinerancia de Datos
Activar itinerancia de voz	Activar itinerancia de voz
Activar zona activa	Activar zona activa

Proxy HTTP

Tipo de proxy	
Manual	Establecer un Proxy manualmente
URL del servidor proxy	Dirección para acceder a la Configuración del Proxy
Puerto	Establecer puerto Proxy
Autenticación	Nombre de usuario para la autenticación en el Proxy
Contraseña	Contraseña para la autenticación en el Proxy
Automático	Establecer un Proxy automáticamente
URL del proxy PAC	URL del proxy PAC
Permitir conexión directa si PAC es inalcanzable	Permitir conexión directa (sin VPN), si PAC es inalcanzable
Permitir eludir el proxy para acceder a redes cautivas	Permitir eludir el proxy para acceder a redes internas cautivas

AirPrint

Dirección IP	Dirección IP de la impresora
Ruta de recursos	Ruta definida al dispositivo AirPrint

AirPlay

Nombre del dispositivo	Nombre del dispositivo
Contraseña	Contraseña de emparejamiento
Lista blanca	Define una lista de dispositivos, con los que el dispositivo puede emparejarse exclusivamente

Gestión PIM

Sincronización activa de Exchange

Nombre de la cuenta	Nombre de la cuenta de correo electrónico
Host Exchange ActiveSync	Dirección/FQDN del servidor
Permitir movimiento	Permitir el movimiento de correos electrónicos
Utilizar sólo en el correo	Las interacciones sólo pueden producirse en la App Mail nativa
Utiliza SSL	Utilizar encriptación SSL
Dominio	Dominio del servidor
Usuario	Nombre de usuario
Dirección de correo electrónico	dirección de correo electrónico (sólo a nivel de dispositivo)
Contraseña (sólo a nivel de dispositivo)	Contraseña de usuario
Certificado de Identidad	Selecciona el certificado correspondiente para la autenticación en el servidor
Días pasados de Mail to Sync	Número de días, hasta que los correos electrónicos deben sincronizarse de nuevo. Sin límite = ilimitado
Activar S/MIME	Activar la encriptación S/MIME
Certificado de firma	Sube el Certificado de Firma correspondiente
Certificado de encriptación	Sube el Certificado de Cifrado correspondiente

Correo electrónico

Configuración de cuentas POP3 / IMAP en el dispositivo del usuario final

Descripción de la cuenta	Nombre des Cuentas Email		
Tipo de cuenta	IMAP	Prefijo de la ruta	El prefijo de ruta para carpetas especiales
	POP		
Nombre para mostrar del usuario	Nombre de usuario		
Dirección de correo electrónico	Dirección de correo electrónico del usuario		
Permitir movimiento	Permitir el movimiento de correos electrónicos		
Activar S/MIME	Activar la encriptación S/MIME		
Certificado de firma	Sube el Certificado de Firma correspondiente		
Certificado de encriptación	Sube el Certificado de Cifrado correspondiente		

Correo entrante

Configuración del servidor entrante

Dirección del servidor de correo	Dirección del servidor de correo
Puerto del servidor de correo	Puerto del servidor de correo
Nombre de usuario	Nombre de usuario correspondiente
Tipo de autenticación	Tipo de autenticación
Ninguno	No Tipo de autenticación
Contraseña (sólo a nivel de dispositivo)	Indicación de contraseña
MDM Desafío-Respuesta	
NTLM	Autenticación NTLM
Resumen HTTP MD5	
Utiliza SSL	Utiliza SSL, si es necesario

Correo saliente

Configuración del servidor de salida

Dirección del servidor de correo	Dirección del servidor de correo
Puerto del servidor de correo	Puerto del servidor de correo
Nombre de usuario	Nombre de usuario respectivo
Tipo de autenticación	
Ninguno	Ningún método de autenticación
Contraseña (sólo a nivel de dispositivo)	Indicación de contraseña
MDM Desafío-Respuesta	
NTLM	Autenticación NTLM
Resumen HTTP MD5	
Utiliza SSL	Utiliza SSL, si es necesario
La contraseña saliente es la misma que la entrante	La contraseña saliente es la misma que la entrante
Utilizar sólo en correo	Activar, si todos los correos salientes deben enviarse a través de la Mail-App

CalDav

Configurar la creación y distribución de una cuenta CalDav

Descripción de la cuenta	Nombre para mostrar de la cuenta
Nombre de host	Nombre de host y/o dirección IP
Puerto	Puerto de la cuenta CalDav
URL principal	URL principal de la cuenta
Nombre de usuario	Nombre de usuario CalDav correspondiente
Contraseña (sólo a nivel de dispositivo)	Contraseña CalDav correspondiente
Utiliza SSL	Utiliza SSL, si es necesario

Calendarios suscritos

Creación y distribución de calendarios suscritos

Descripción	Nombre para mostrar de la cuenta
URL	URL de la base de datos del calendario
Nombre de usuario	Nombre de usuario de la suscripción al calendario
Contraseña (sólo a nivel de dispositivo)	Contraseña de la suscripción al calendario
Utiliza SSL	Utiliza SSL, si es necesario

LDAP

En esta área, configure una conexión LDAP para permitir un intercambio dinámico de certificados entre el dispositivo del usuario final y el Directorio Activo.

Tenga en cuenta que el usuario seleccionado requiere el permiso de lectura correspondiente.

Descripción de la cuenta	Descripción de la cuenta
Nombre de usuario de la cuenta	Usuario para acceso LDAP
Contraseña de la cuenta	Contraseña de acceso LDAP
Nombre de host de la cuenta	Nombre de host/dirección IP del servidor LDAP
Utiliza SSL	Utiliza SSL, si es necesario

En la segunda parte, puede definir filtros individuales para buscar en el registro LDAP.

Descripción	Alcance	Buscar Base
Descripción del filtro	Nivel de búsqueda en el registro LDAP	Definir el filtro individual

Gestión web

Webclips

En esta ubicación defina marcadores, con enlaces a páginas web, portales de intranet, etc., que serán visibles como aplicación en el dispositivo del usuario final.

Etiqueta	Nombre de la conexión en el dispositivo del usuario final
URL	Enlace al sitio web correspondiente
Extraíble	Si está activado, el usuario puede eliminar el webclip
Icono	A través de este diálogo, sube un logotipo para la conexión: Dimensiones 180x180, formato png
Icono precompuesto	Si está activado, no se mostrarán efectos adicionales (sombra, reflejo) en el icono
Pantalla completa	Al abrir webclips, el navegador se abre a pantalla completa

Filtro de contenidos web

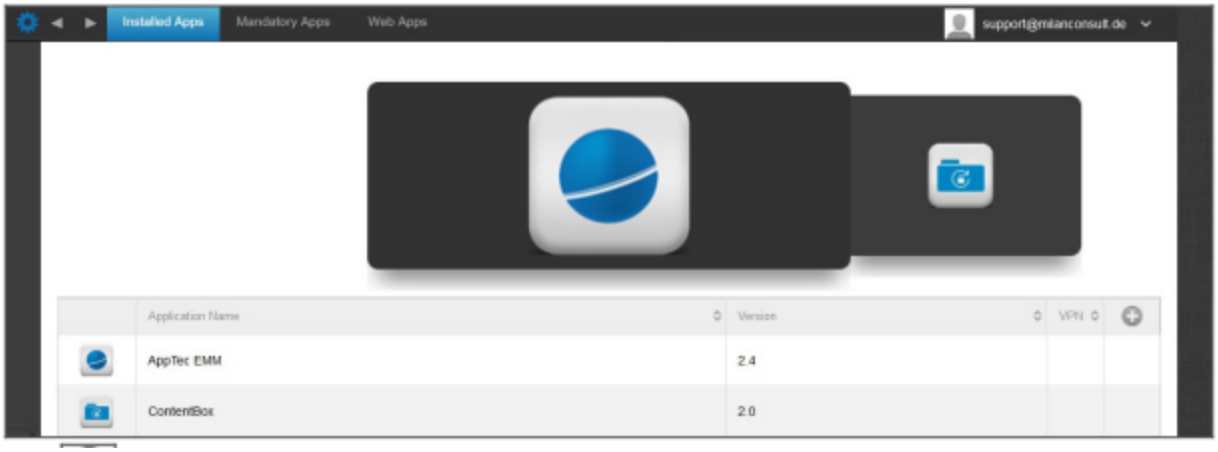
El filtro de contenidos web permite limitar el acceso a determinadas páginas de Internet.

Sitios web permitidos	
Limitar el contenido para adultos	El filtro web se aplica automáticamente al contenido para adultos
URL permitidas	Con el símbolo + añade páginas permitidas
URLs en la lista negra	Con el símbolo + añade páginas bloqueadas
Sólo sitios web específicos	Sólo se pueden mostrar contenidos específicos, que puedes añadir con el símbolo +.

Gestión de aplicaciones

Enterprise App Manager

Aplicaciones instaladas (sólo en el dispositivo)



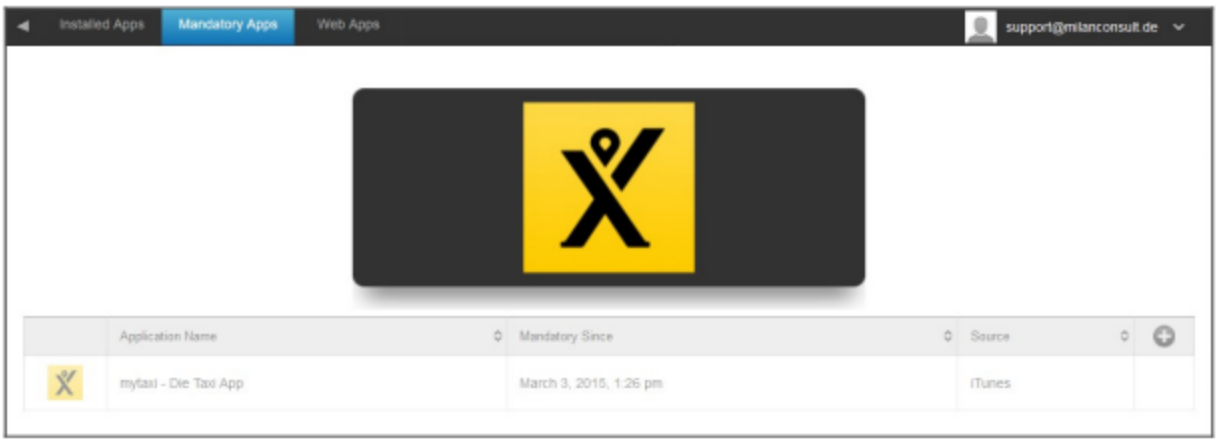
Aquí puedes ver las Apps que están actualmente instaladas en el dispositivo.

Aplicaciones obligatorias

En Aplicaciones obligatorias, puede establecer las aplicaciones necesarias.

Se recordará continuamente al usuario que instale dicha App.

A través de la , se puede definir la App obligatoria.



Puede tratarse de una aplicación de Apple App Store, pero también de una aplicación interna.

Si se trata de un dispositivo supervisado, la aplicación se instalará automáticamente.

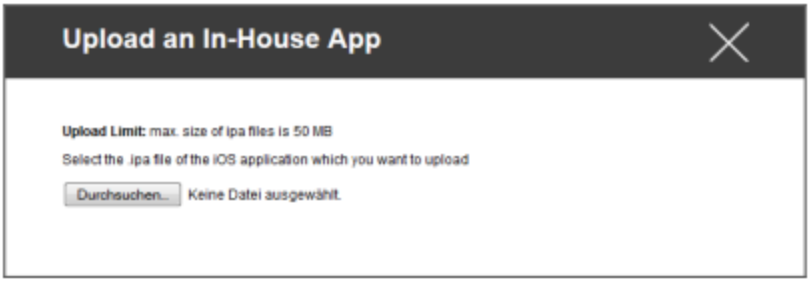
Puede insertar una aplicación "Apple AppStore" de la AppStore pública en el dispositivo, así como una aplicación interna desarrollada internamente.

También puede seleccionar la categoría "Aplicaciones internas de iOS" y elegir una aplicación interna que haya cargado en Ajustes generales.

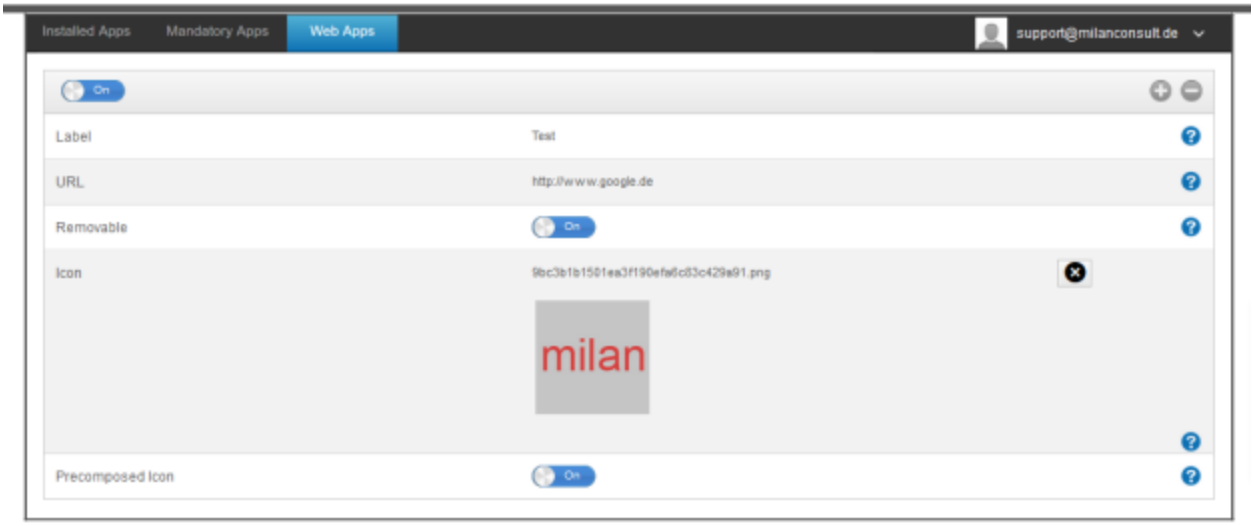
Opciones de instalación

Mantener actualizado (sólo se admite para VPP por dispositivo)	Una vez a la semana, se determinará si hay una actualización para la aplicación. En caso afirmativo, se instalará dicha actualización Para las aplicaciones internas, se utilizará para el proceso de actualización el objetivo de actualización que hayas configurado en Configuración General.
Adelantar cuando no se gestiona	Si la app ya está instalada, el MDM se hará cargo de ella y la gestionará
Eliminar la app cuando se elimina el perfil MDM	En el caso de una eliminación de gestión de dispositivos, la App se desinstalará
Evitar la copia de seguridad de los datos de la app	No se creará una copia de seguridad de los datos específicos de la app
Configuración de la aplicación	En "Configuración de la aplicación", puedes asignar a la aplicación determinados valores en primer plano (siempre que la aplicación lo admita, si es necesario pregunta al desarrollador de la aplicación).

También puede seleccionar y cargar directamente un archivo ipa, a través de "Cargar aplicación interna".



Aplicaciones web



En el punto "Aplicaciones web", puedes, de forma similar a lo que ocurre con "Clips web", insertar páginas de Internet o portales de intranet como una aplicación en el dispositivo del usuario final, en el área de Gestión web. Por defecto, las Aplicaciones Web se mostrarán en modo de pantalla completa, que puede configurarse en "Clips Web".

Etiqueta	Nombre de la conexión en el dispositivo del usuario final
URL	Enlace al sitio web correspondiente
Extraíble	Si está activado, el usuario puede eliminar el Webclip
Icono	A través de este diálogo, sube un logotipo para la conexión: Dimensiones 180x180, formato png
Icono precompuesto	Si está activado, no se mostrarán efectos adicionales (sombra, reflejo) en el icono

Restricciones y ajustes

Aplicaciones en la lista negra y en la lista blanca

Aquí puedes establecer las aplicaciones bloqueadas (o permitidas) en función de tu configuración en "Ajustes generales". Al pulsar sobre aparecerá el buscador de aplicaciones conocidas. Allí puedes buscar las aplicaciones que quieres añadir.

Tenga en cuenta que para esta función es necesario un dispositivo supervisado

Restricciones de SysApp

Bloquea aplicaciones o funciones específicas de tu dispositivo

Permitir el uso de YouTube	Permitir el uso de YouTube
Permitir el uso de iTunes Store	Permitir el uso de iTunes Store
Permitir el uso de Safari	Permitir el uso de Safari
Activar autorrelleno	Permite el autorrelleno
Advertencia de fraude a la fuerza	Fuerza el aviso de fraude
Activar JavScript	Permite el uso de JavaScript
Bloquear ventanas emergentes	Bloquea todo tipo de cachorros
Permitir cookies	Elige cuándo aceptará Safari las cookies

App-VPN

Mediante el símbolo, puede definir aplicaciones que iniciarán automáticamente la conexión VPN seleccionada al arrancar.

Configuración de la aplicación

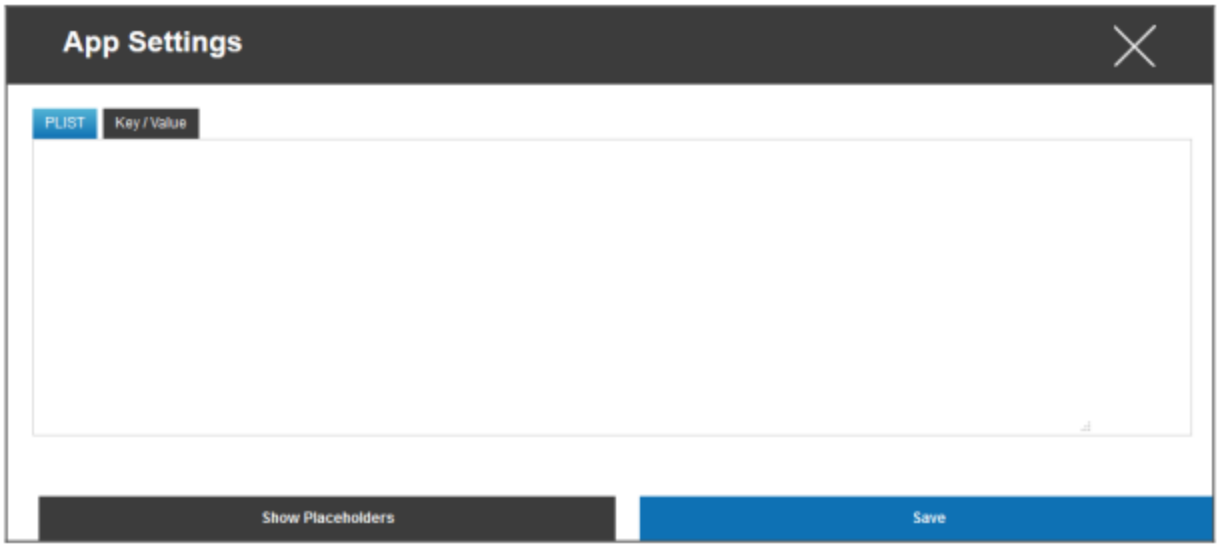
En "Configuración de la aplicación", puedes asignar a la aplicación determinados valores en primer plano (siempre que la aplicación lo admita, si es necesario pregunta al desarrollador de la aplicación).

Mediante el símbolo, añades una app (adicional). Encontrarás, una vez más, la familiar representación AppTec360 de una App-Import.

Busca aquí la App que quieras configurar y selecciónala. Los ajustes sólo se aplicarán a las apps gestionadas.

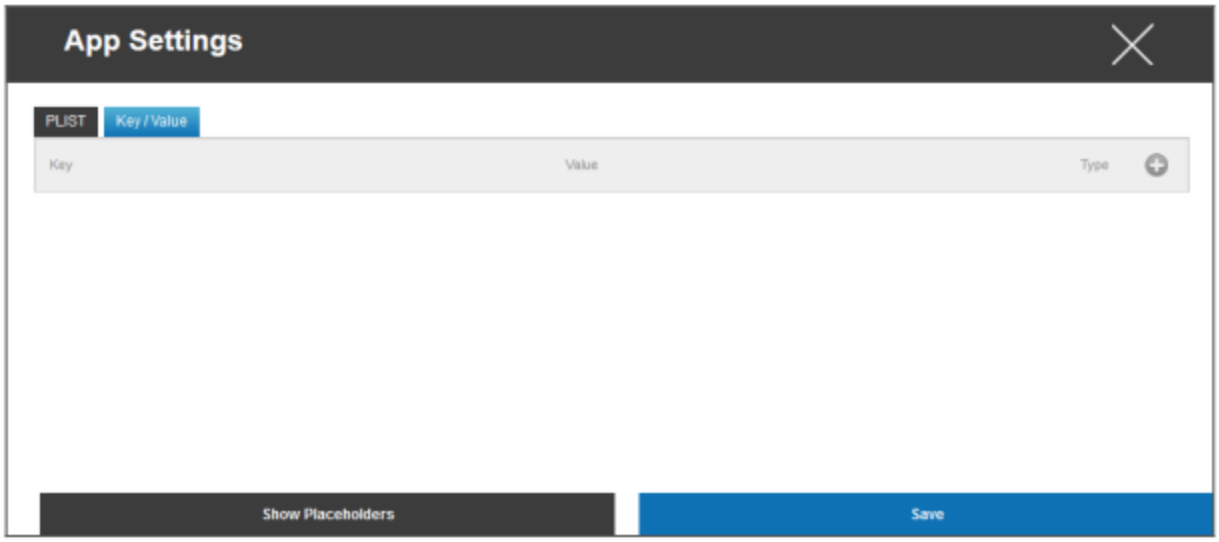
Si la Importación se ha realizado correctamente, verá la siguiente pantalla:

Ahora, con un clic en , puedes realizar diversas configuraciones. Recibirás entonces la siguiente vista general:

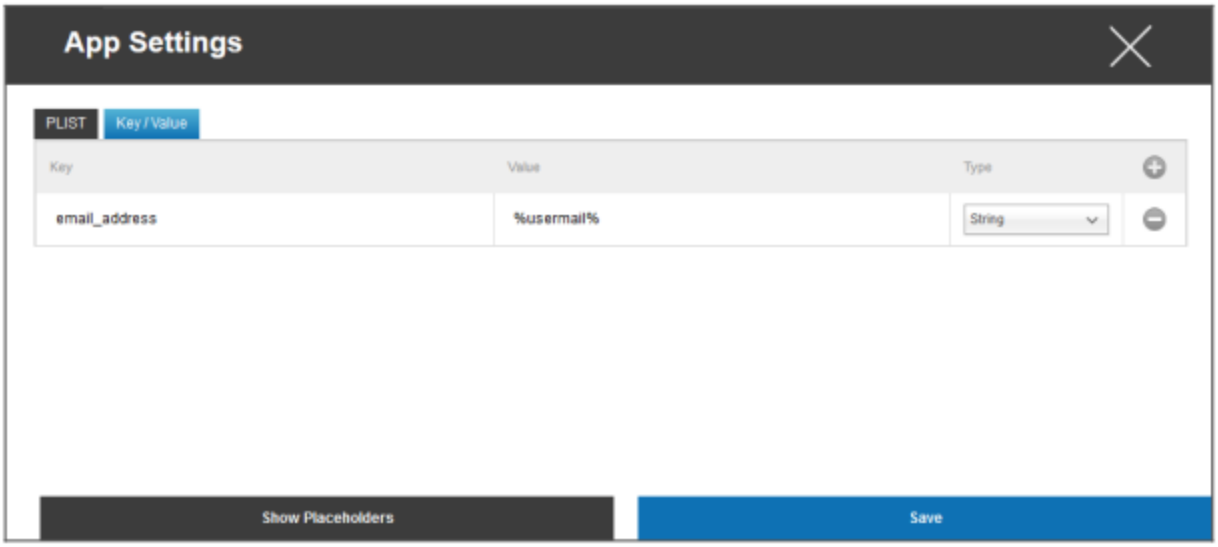


Si ya tienes una PLIST (texto fuente de configuración), puedes añadirla aquí y guardarlo todo con "Guardar".

En "Clave / Valor", puede adjuntar configuraciones específicas a la aplicación



Aquí puede establecer una nueva clave y su valor con el símbolo .



Por supuesto, todos los marcadores de posición de AppTec están a su disposición

Explicación "Tipo":

Cadena	Texto
Booleano	Verdadero/Falso
Número	Número

Con el símbolo, puedes volver a eliminar una aplicación.

App Store para empresas

Aplicaciones iTunes

En este punto, puede distribuir Apps opcionales para su Usuario.

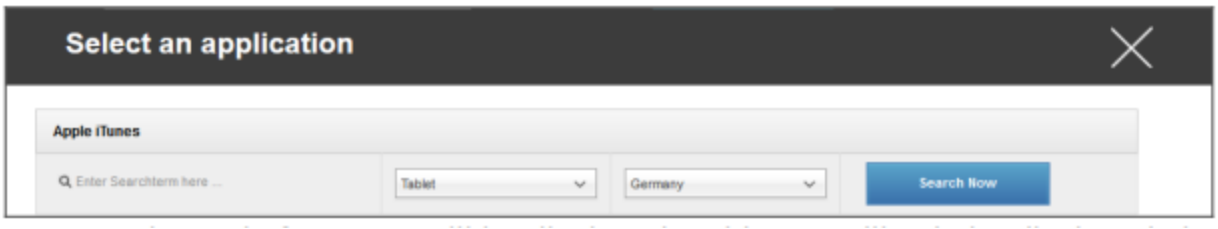
Si hay una App aquí, se instalará automáticamente en el dispositivo del usuario final de la AppTec360 Store.

Se trata simplemente de enlaces al App Store oficial de Apple. Por esta razón, cada dispositivo de usuario final debe estar equipado con un ID de Apple.

En este punto, recomendamos que cada usuario tenga su propio ID de Apple.

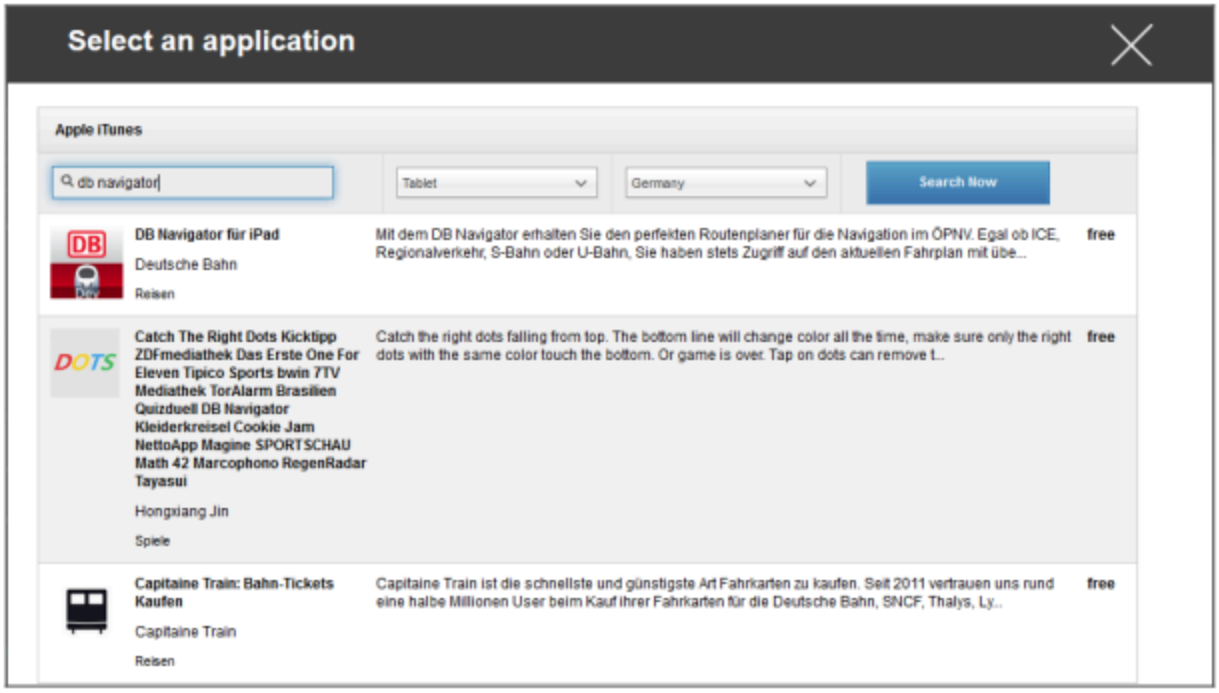
Con el símbolo, puedes añadir Apps adicionales.

A continuación, se abrirá una ventana con el siguiente resumen.



Ten en cuenta que sólo se mostrarán las aplicaciones gratuitas, las de pago sólo se mostrarán a través de VPN.

En "Escriba aquí el término de búsqueda...", puede buscar una aplicación que esté en el App Store de Apple.



Una vez que haga clic en el icono o en el nombre de la aplicación, se le pedirá de nuevo que realice configuraciones adicionales.

Mantente al día	Una vez a la semana, se determinará si hay una actualización para la aplicación. En caso afirmativo, se instalará dicha actualización
Eliminar la app cuando se elimina el perfil MDM	En el caso de una eliminación de gestión de dispositivos, la App se desinstalará
Evitar la copia de seguridad de los datos de la app	No se creará una copia de seguridad de los datos específicos de la app
App-VPN	Selecciona una conexión VPN, que se iniciará al abrir la App

Tras hacer clic en "Instalar", la aplicación se añadirá a la Enterprise App Store y podrá instalarse en el dispositivo del usuario final a través de la AppStore de AppTec360.

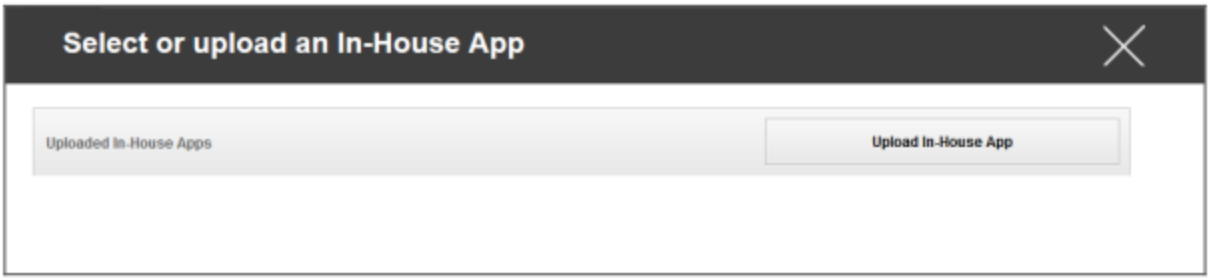
Si la importación de la App-Store se ha realizado correctamente, recibirá el siguiente resumen:

En la empresa

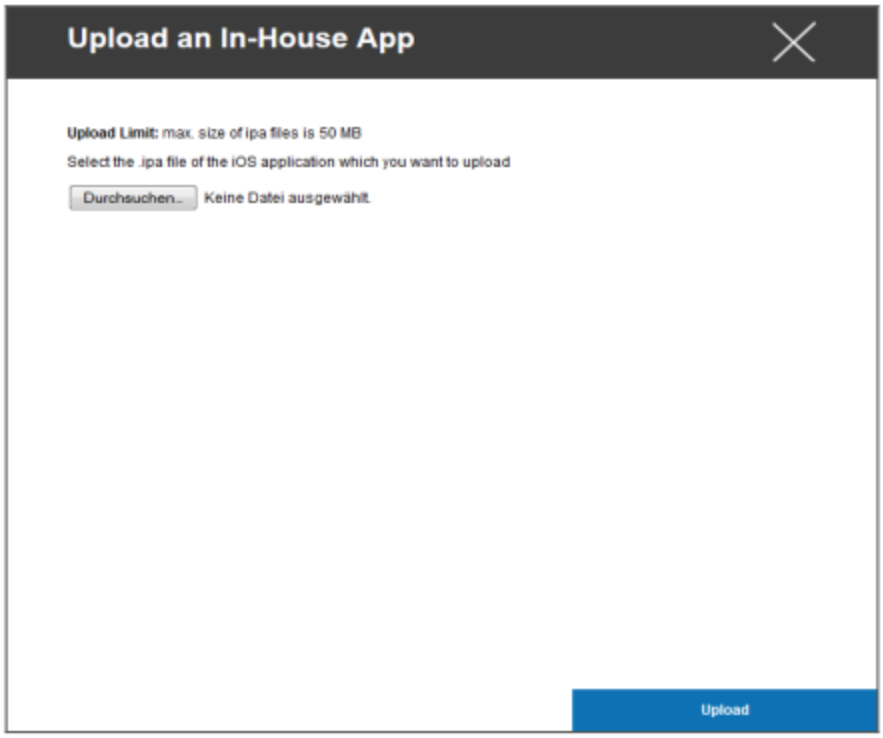
En el punto "In-House", puede cargar Apps desarrolladas internamente y distribuirlas.

Con el símbolo, puede distribuir In-House Apps adicionales.

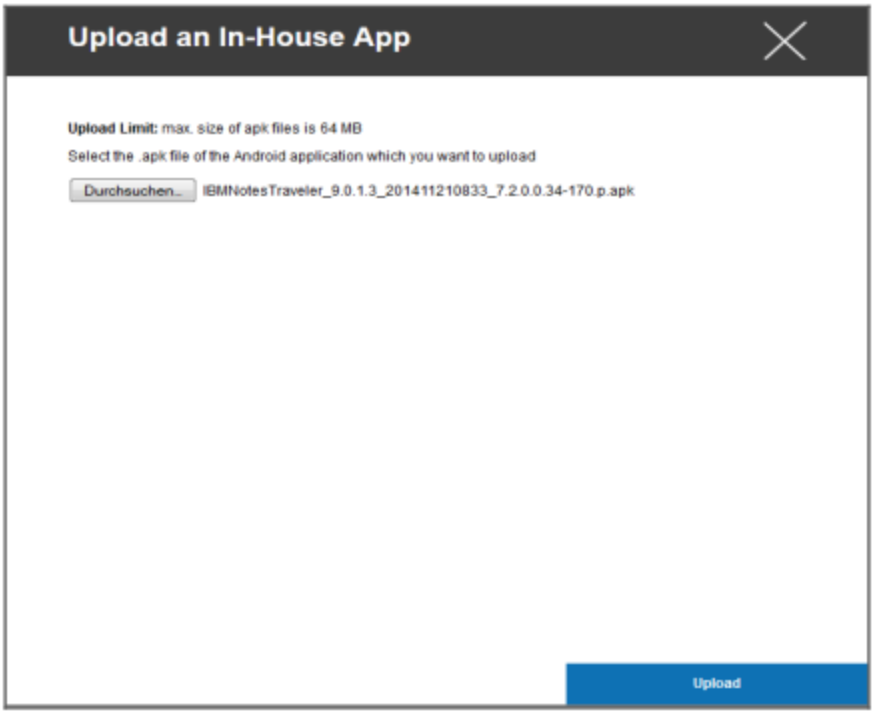
Si nunca ha distribuido In-House App, recibirá la siguiente descripción general:



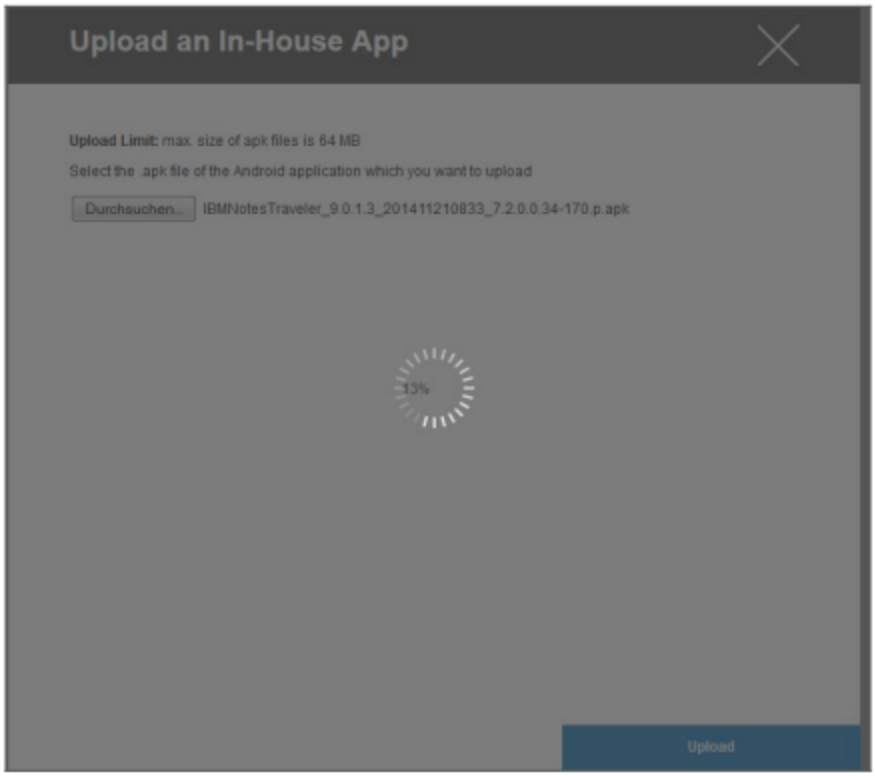
Para ello, haga clic en "Upload In-House App" (Cargar aplicación interna) y obtendrá la siguiente descripción general:



Ahora, selecciona con "Buscar... "un archivo .ipa y haz clic en "Cargar".



Su aplicación se cargará. En el centro del círculo, puede ver el porcentaje de su aplicación que ya se ha cargado.



Si la carga de la aplicación interna se ha realizado correctamente, verá la aplicación recién cargada en su catálogo de aplicaciones.

El usuario tiene ahora la opción de ver e instalar esta app en la AppTec360 Store en el dispositivo del usuario final, bajo la categoría "In-House".

Dado que no se trata de una aplicación pública de la AppStore de Apple, el usuario no necesita un ID de Apple almacenado en el dispositivo del usuario final.

Modo quiosco

El modo quiosco de iOS sólo está disponible en modo supervisado

El Modo Quiosco le permite predefinir una App o URL, de modo que será posible ejecutar/visitar esta App/URL exclusivamente.

Además, puede desactivar varios botones de hardware en el Modo Quiosco.

Tipo de aplicación

Paquete

Si desea iniciar la aplicación en modo quiosco, seleccione "Paquete" en "Tipo de aplicación".

Aplicación quiosco	Pulsa aquí para seleccionar una aplicación que se inicie en Modo Quiosco. Encontrarás la visión general actual de la Gestión de Apps Puedes seleccionar entre "Aplicaciones iTunes de Apple" y "Aplicaciones internas de iOS".

URL

Si desea iniciar una URL en el Modo Quiosco, seleccione "URL" en "Tipo de aplicación".

URL	Ahora, define la dirección URL deseada
Política del mismo origen	Si esta función está activa, el usuario sólo podrá navegar por las subpáginas de la URL predefinida Por ejemplo, si has definido la siguiente URL: www.mypage.com, entonces el usuario puede navegar en www.mypage.com/subpage
URLs en lista blanca	Aquí puedes mantener una Lista Blanca, todas estas URLs están permitidas Máximo 1 URL por línea Una URL debe empezar por http:/ o https://
URLs en la lista negra	Aquí puedes mantener una Lista Negra, todas estas URLs están desautorizadas Máximo 1 URL por línea Una URL debe empezar por http:/ o https://
Borrar Navegador tras inactividad	Tras la inactividad se vaciará la Caché del Navegador
Contraseña de salida activada	Si activas esta función, el usuario tiene la opción de finalizar el Modo Quiosco con una contraseña predefinida por ti.
Salir Contraseña	Esta es la contraseña que tú has predefinido

Configuración del modo quiosco

Modo Quiosco Programado	En función de la hora del día, puedes configurar el Modo Quiosco para que se inicie y finalice automáticamente a una hora predeterminada.
Hora de inicio	Hora de inicio
Tiempo en minutos	Tiempo en minutos, tras el cual el Modo Quiosco debe finalizar de nuevo
Desactivar Táctil	Si está activado, se desactiva la pantalla táctil
Desactivar la rotación del dispositivo	Si está activada, se desactiva la adaptación automática de la pantalla
Desactivar interruptor de timbre	Si está activado, el interruptor del timbre se desactivará. A partir de ese momento, el comportamiento dependerá de la función previamente configurada
Desactivar botones de volumen	Si está activado, se desactivarán los botones de volumen
Desactivar Botón Despertar Sueño	Si está activado, se desactivará el interruptor de encendido/apagado
Desactivar Bloqueo Automático	Si está activado, el aparato no pasará al modo de espera
Activar voz superpuesta	Si está activado, se activará el Asistente de voz en off
Activar zoom	Si está activado, se activará el zoom
Activar Invertir Colores	Si está activado, se activará el modo de visualización invertida
Activar el toque asistido	Si está activado, se activará el AssistiveTouch
Activar selección de voz	Si está activada, se activará la selección de hablar
Activar Audio Mono	Si está activado, se activará el Audio Mono
VoiceOver	Si está activado, el usuario puede activar VoiceOver
Zoom	Si está activado, el usuario puede activar el Zoom
Invertir colores	Si está activado, el usuario puede activar los colores invertidos
Tacto Asistencial	Si está activado, el usuario puede habilitar el toque asistido

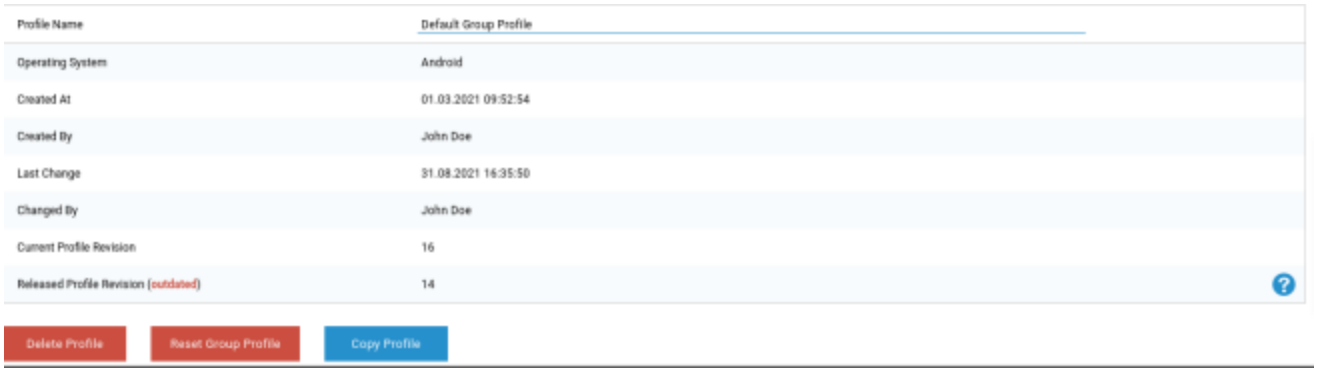
Android Enterprise – Configuración de dispositivos totalmente gestionada

Dependiendo de si ha seleccionado actualmente un perfil de grupo o un dispositivo, la vista general y sus subpuntos difieren - ¡tenga esto en cuenta!

General

Resumen del perfil del grupo (sólo a nivel de grupo)

Al abrir un perfil de grupo, obtendrás una rápida visión general del perfil.



Nombre del perfil	Nombre del perfil (se puede cambiar aquí)
Sistema operativo	Sistema operativo para el que es el perfil
Creado en	Momento de la creación
Creado por	El creador del perfil
Último cambio	Hora de la última modificación del perfil
Cambiado por	Cuenta que realizó los últimos cambios
Revisión actual del perfil	Revisión del estado del perfil guardado
Revisión del perfil liberado	Revisión del perfil asignado ("Asignar ahora"). Si la etiqueta muestra "(obsoleto)" detrás del texto, significa que has guardado el perfil pero aún no lo has asignado, por lo que los dispositivos seguirán recibiendo una versión antigua.

Visión general del dispositivo (sólo a nivel de dispositivo)

Si se encuentra en un dispositivo, recibirá un resumen general del dispositivo seleccionado:

Nombre del dispositivo	Nombre del dispositivo
Ubicación	Coordenadas de ubicación
Número de teléfono	Número de teléfono
Apps Obligatorias Asignadas	Número de Apps obligatorias asignadas
Versión del SO	Versión del SO del dispositivo
Sistema operativo	Sistema operativo (Android Enterprise)
Número de serie	Número de serie del dispositivo
Propiedad del dispositivo	Dispositivo corporativo o privado
Tipo de dispositivo	Dispositivo gestionado por AE Work
Enraizado	Estado, que indica si el dispositivo ha sido rooteado
Cumple	Cumple las directrices
Dirección IP	Dirección IP del dispositivo
Visto por última vez	Momento en que el dispositivo se conectó por última vez a AppTec
Último empujón	Momento en el que se envió la última pulsación al dispositivo
Modo Propietario del Dispositivo AE	Sí
Asignación de usuarios	El usuario o grupo al que está asignado este dispositivo

Config Revision (sólo a nivel de dispositivo)

Aquí obtendrá una visión general de qué perfil de grupo está asignado al dispositivo.

Si haces clic en el perfil del grupo, accederás directamente a este perfil y podrás realizar ajustes.

Con este símbolo, puedes revertir las aplicaciones distribuidas a la configuración del perfil de grupo.

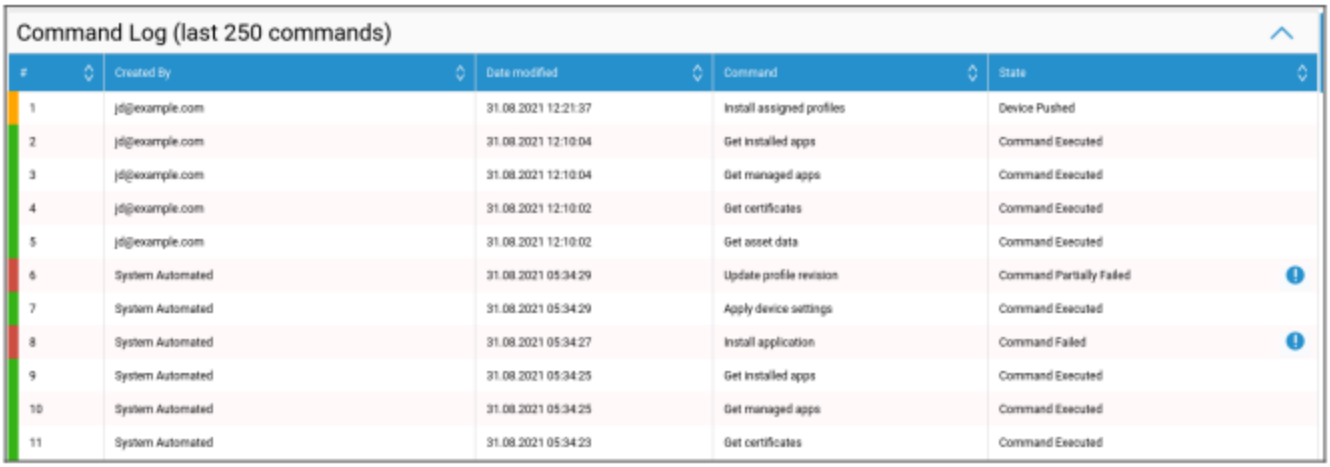
Con este símbolo, puedes revertir todas las aplicaciones utilizadas a la configuración del perfil de grupo.

"Nueva revisión disponible" indica que el perfil de grupo se ha modificado y guardado, pero no se ha asignado. El perfil de grupo debe asignarse con "Asignar ahora" a nivel de grupo para aplicar los cambios a los dispositivos.

Registro de dispositivos (sólo a nivel de dispositivo)

Registro de comandos

Aquí puede ver qué comandos se emitieron para el dispositivo y cuál es su estado.



Los comandos creados por "Sistema automatizado" son creados automáticamente por el sistema.

Posibles estados del comando

Dispositivo Empujado	Se ha enviado una solicitud push al servicio push (por ejemplo, APNS) para indicar al dispositivo que se conecte de nuevo al servidor EMM.
Comando creado	El comando se creó en el sistema.
Orden enviada	El comando se envió al dispositivo después de que se conectara al servidor.
Orden ejecutada	El comando se ha ejecutado correctamente.
Comando fallido	El comando falló. *
Comando parcialmente fallido	Dependiendo del SO del dispositivo, algunos comandos pueden agruparse. En este fallaron algunas partes de este grupo de comandos. *
Orden ejecutada, finalmente fallida	La orden se ejecutó, pero puede que no.
Comando Repulsado	El comando fue repulsado por un usuario.
Descartado	El comando fue descartado. Por ejemplo, porque ha sido sustituido por otro comando o porque el dispositivo se ha reinscrito y se han eliminado los comandos antiguos.

Si hay un signo de exclamación detrás del mensaje, puede obtener más información pasando el cursor sobre el icono.

Ajustes del dispositivo

Configuración de clientes

Aquí puedes realizar las siguientes configuraciones en tu dispositivo Android:

Tiempo de incumplimiento	El límite de tiempo de espera de respuesta del usuario tras el cual se aplica la acción coercitiva.
Acción coercitiva tras el plazo de cumplimiento	Acción coercitiva cuando un usuario no realiza acciones que conducen a un estado de dispositivo conforme
Frecuencia de recogida de datos	Frecuencia con la que debe recogerse la información del dispositivo/GPS
Frecuencia de latidos del dispositivo	Intervalo en el que el dispositivo debe ponerse en contacto con el Servidor AppTec360 Mín. 1 minuto Máx. 24 horas
Activar actualizaciones de ubicación	Si está activado, el dispositivo envía actualizaciones de ubicación al Servidor AppTec360
Lugar Hora de actualización	Determina en qué intervalos de tiempo el dispositivo envía actualizaciones de ubicación a AppTec360
Utiliza la precisión de ubicación de Google para actualizar la ubicación	Si se activa, se utilizará la ubicación de red para las actualizaciones de ubicación (si se desactivó en "Restricciones", este ajuste no afectará a nada).
Utilizar la localización GPS para actualizar la ubicación	Si está activado, se utilizará el GPS para actualizar la ubicación
Permitir Ubicaciones Simuladas (Falsas)	Permite falsificar la información de localización a través de apps de terceros
Acción de conexión perdida	Si está activada, puedes especificar una acción para el caso de que un dispositivo no consiga una conexión con el servidor MDM en el intervalo de latido. Por ejemplo, si el dispositivo tiene un tiempo de latido de 5 minutos, se conecta al servidor a las 10:35 AM. Después, el dispositivo sale del alcance Wi-Fi. El siguiente heartbeat a las 10:40 AM fallará, y se ejecutará la acción especificada.

	Acción	La acción que debe emprenderse en cuanto un aparato deje de ser conforme. • Dispositivo de bloqueo = dispositivo de bloqueo • Borrar dispositivo = el dispositivo se restablecerá a los ajustes de fábrica • Borrar dispositivo y tarjeta SD = el dispositivo se restablecerá a los ajustes de fábrica y se borrará el almacenamiento de la tarjeta SD
	Umbral	Puedes especificar un umbral de latidos fallidos necesarios para activar la acción especificada.

Modo de aplicación de la política	Por defecto:	Periódicamente se pedirá a los usuarios que ejecuten las acciones pendientes
	Aplicación perezosa de la política:	Nunca se pedirá a los usuarios que ejecuten las acciones pendientes. Todas las acciones abiertas se mostrarán en el Cliente AppTec360
	Aplicación agresiva de la política:	A los usuarios se les pedirá sin parar que ejecuten las acciones pendientes
AppTec360 Bloqueo de versión	Si está activada, se puede especificar un código de versión para el Cliente MDM de AppTec360. El cliente AppTec360 sólo se actualizará a la versión especificada. Las versiones más recientes serán ignoradas. NO es posible un downgrade.	
Código de versión	Código de versión para el Cliente MDM de AppTec360 que se va a bloquear.	
Desactivar la notificación de AppTec360	Si se desactiva, el Cliente AppTec360 no mostrará una Notificación en la Barra de Notificaciones. Así, los usuarios pueden cerrar el cliente AppTec360 a través del administrador de tareas. Si el cliente AppTec360 está cerrado, varias funciones, como el Modo Quiosco y la Lista Negra/Blanca de Aplicaciones, no funcionarán correctamente. Los dispositivos Samsung ofrecen un mecanismo de protección para el Cliente AppTec360. La notificación está desactivada por defecto en los dispositivos Samsung compatibles con las API KNOX. La notificación no debería desactivarse en dispositivos con Android 8.0 o superior.	

Papel pintado

Establecer fondo de pantalla personalizado	Activar/Desactivar el fondo de pantalla personalizado
Papel pintado	Configura el modo de papel tapiz para utilizar un código de color o una imagen
Especifica un color	Especifica un color de fondo como valor hexadecimal, por ejemplo #000000 para el negro o #ffffff como blanco
Establecer imagen como fondo de pantalla	Sube el archivo de imagen que quieras utilizar como fondo de pantalla

Gestión de activos (sólo a nivel de dispositivo)

Información del dispositivo

Modelo	Designación del modelo de aparato
Sistema operativo	OS
Versión del SO	Versión del SO
Número de serie	Número de serie
Nombre del dispositivo	Nombre del dispositivo
Estado de la batería	Estado de la batería
Memoria Libre / Total	Memoria libre / total
Caja fuerte Samsung	Interfaz Samsung SAFE, necesaria para diversas opciones de configuración
Tarjeta SD disponible	Tarjeta SD disponible
Tarjeta SD emulada	Tarjeta SD emulada
Tarjeta SD extraíble	Tarjeta SD extraíble
SD Memoria Libre / Total	SD Libre / Memoria total de la tarjeta SD

Wi-Fi

Dirección IP	Dirección IP del dispositivo
WiFi MAC	Dirección MAC WiFi

Móvil

Estado	Estado (tarjeta SIM instalada)
Número de teléfono	Número de teléfono
Itinerancia (Voz / Datos)	Itinerancia de voz/datos
Estado de itinerancia	Estado actual de la itinerancia
Dirección IP	Dirección IP
Operador/Transportista	Operador/Transportista
Tecnología celular	Tecnología celular
IMEI	Número IMEI
ICCID	Es el identificador de la tarjeta SIM, a menudo también tarjeta inteligente o tarjeta de circuito integrado (ICC).
IMSI	La Identidad Internacional de Abonado Móvil (IMSI) proporciona en las redes móviles GSM y UMTS una identificación definitiva de los usuarios de la red La IMSI se compone de un máximo de 15 dígitos y se configura de la siguiente manera: • Código de país del móvil (MCC), 3 dígitos • Código de red móvil (MNC), 2 ó 3 dígitos • Número de identificación de abonado móvil (MSIN), de 1 a 10 dígitos
MCC/MNC actual	Ver "SIM MCC/MNC"
SIM MCC/MNC	El Código de país móvil es un identificador de país establecido, fijado por la UIT según la Norma E.212. Funciona junto con el Código de Red Móvil (MNC) para la identificación de la red móvil. Significa el código de país/red móvil de la tarjeta SIM. Si te desplazas a otra red móvil, lógicamente, el "MCC/MNC actual" y el "MCC/MNC de la SIM" serán diferentes.

Bluetooth

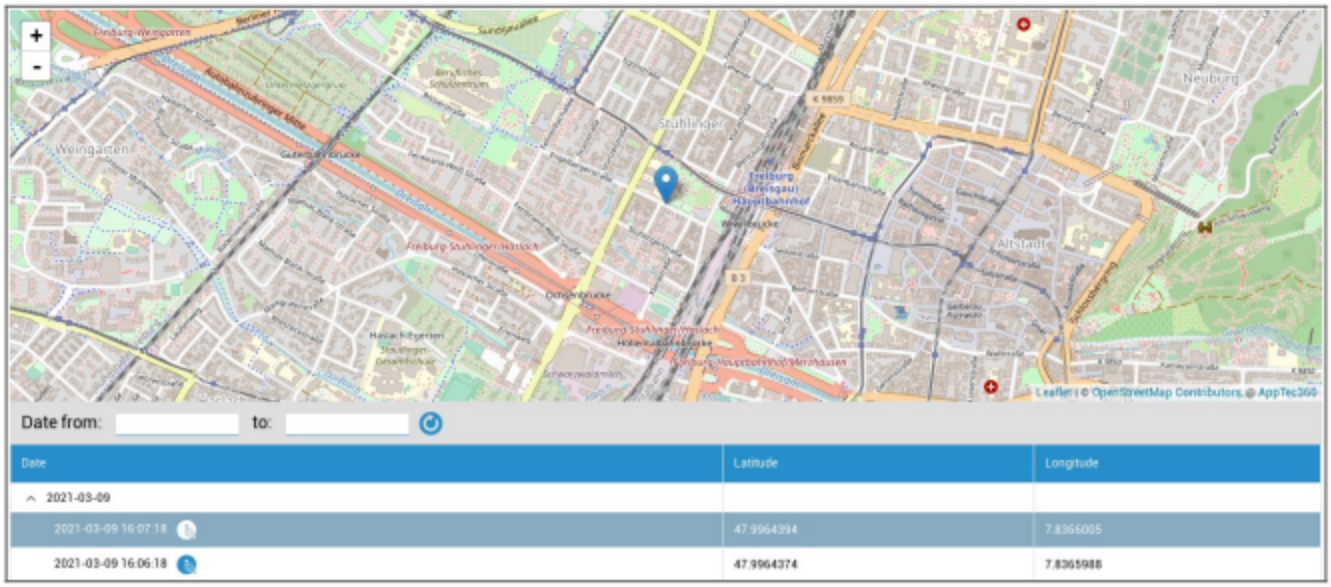
Bluetooth MAC	Dirección MAC Bluetooth

Gestión de la seguridad

Antirrobo (sólo en el dispositivo)

Información GPS (sólo a nivel de dispositivo)

Aquí puede establecer la ubicación actual/última del dispositivo. La localización puede protegerse con una o incluso dos contraseñas - Ver: Ajustes Generales - Privacidad - Acceso GPS



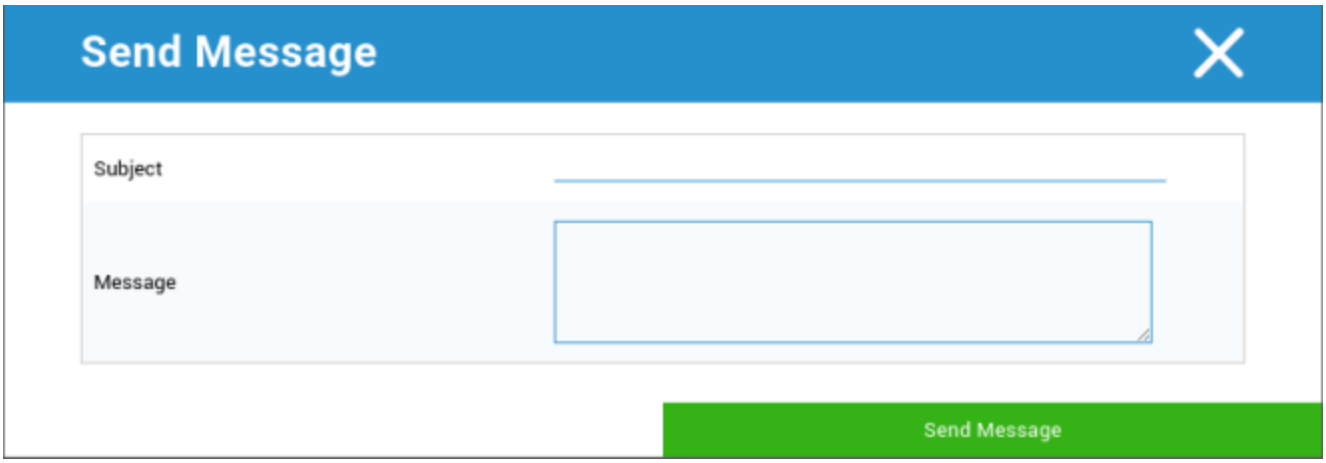
Limpiar y bloquear (sólo a nivel de dispositivo)

En "Limpiar y bloquear", puedes realizar las tres acciones siguientes:

Limpieza total	El dispositivo se restaura a sus valores de fábrica (se borran tanto los datos corporativos como los personales).
Limpieza de empresas	Sólo se eliminan los datos corporativos del dispositivo del usuario final (todas las aplicaciones, datos, etc. que fueron proporcionados por AppTec360)
Pantalla de bloqueo	El bloqueo de pantalla está activado, basta con desbloquear el dispositivo con la contraseña/PIN del dispositivo

Mensaje (sólo a nivel de dispositivo)

Aquí puede rellenar el asunto y un mensaje y enviarlo a un dispositivo de usuario final.



Configuración de seguridad

Código del dispositivo

En "Código de acceso" puede asignar una contraseña al dispositivo, con las siguientes opciones de configuración

Longitud mínima de la contraseña	Establece, el número mínimo de símbolos que debe tener una contraseña	
Calidad de la contraseña	Sin especificar	Esta política no tiene requisitos para la contraseña.
	Biometría Débil	Esta política permite tecnologías de reconocimiento biométrico de baja seguridad. Esto implica tecnologías que pueden reconocer la identidad de un individuo hasta aproximadamente un PIN de 3 dígitos (la detección falsa es inferior a 1 entre 1.000).
	Algo	Esta política requiere que se establezca algún tipo de contraseña o patrón, pero no impone ninguna regla específica.
	Alfabético	El usuario debe haber introducido una contraseña que contenga al menos caracteres alfabéticos (u otros símbolos).
	Alfanumérico	El usuario debe haber introducido una contraseña que contenga, al menos, caracteres numéricos y alfabéticos (u otros símbolos).
	Complejo	El usuario debe haber introducido una contraseña que contenga al menos una letra, un dígito numérico y un símbolo especial, por defecto. Con esta calidad de contraseña, se puede restringir que las contraseñas contengan varios conjuntos de caracteres, como al menos una letra mayúscula, etc.
Longitud mínima de la contraseña	Establece el número de caracteres necesarios para la contraseña. Por ejemplo, puedes exigir que el PIN o las contraseñas tengan al menos seis caracteres.	
Dígitos numéricos mínimos requeridos en la contraseña	Dígitos numéricos mínimos requeridos en la contraseña	
Mínimo de letras minúsculas	Mínimo de letras minúsculas requeridas en la contraseña	

requeridas en la contraseña	
Mínimo de letras mayúsculas requeridas en la contraseña	Mínimo de letras mayúsculas requeridas en la contraseña
Mínimo de caracteres no alfabéticos requeridos en la contraseña	Mínimo de caracteres no alfabéticos requeridos en la contraseña
Símbolos mínimos requeridos en la contraseña	Símbolos mínimos requeridos en la contraseña

Bloqueo de tiempo máximo de inactividad	Inactividad máxima del usuario hasta el bloqueo temporal
Tiempo de caducidad de la contraseña	Establece, después de qué intervalo de tiempo la contraseña caduca y se debe emitir una nueva contraseña
Restricción del historial de contraseñas	Número de contraseñas utilizadas anteriormente que no están permitidas
Número máximo de intentos fallidos de contraseña	Establece cuántas veces se puede introducir incorrectamente una contraseña, antes de que se realice un borrado completo del dispositivo.
Permitir autenticación biométrica	Permite la autenticación mediante huella dactilar o escáner de iris. Sólo para Samsung KNOX 2.1 y superior

Antivirus

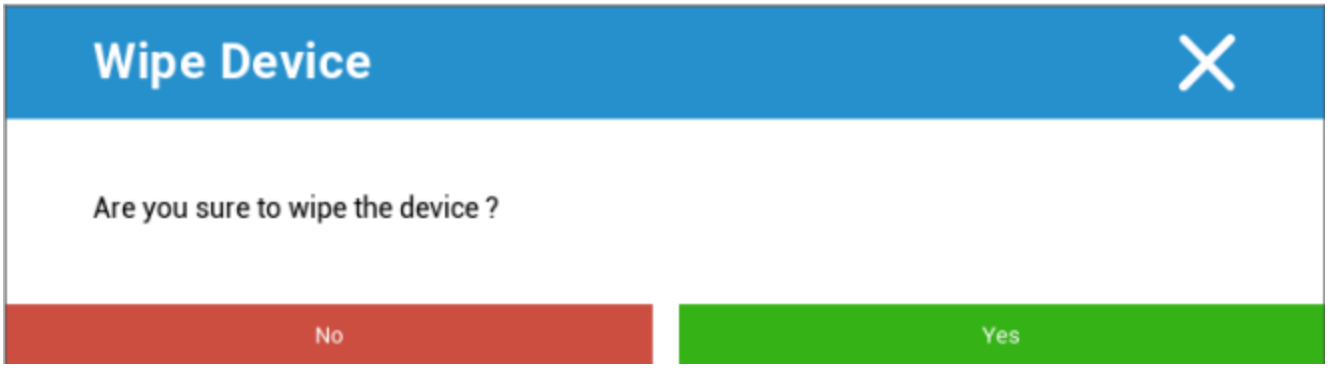
Escaneado automático	Activar escaneos automáticos periódicos
Intervalo de exploración	Intervalo para el examen (Rápido / Completo)
Escaneado automático completo	Activar escaneos automáticos completos
Actualizaciones automáticas	Activar las actualizaciones automáticas
Intervalo de comprobación de actualización	Con qué frecuencia deben actualizarse la aplicación y su base de datos (virus / código dañado)
Protección de aplicaciones	Activar el escaneo automático de apps
Protección de tarjetas SD	Activar el escaneo automático de la tarjeta SD
Actualización sólo Wi-Fi	Si está activada, las actualizaciones sólo se aplicarán cuando el dispositivo se conecte correctamente a una red Wi-Fi

Fin de vida útil (sólo a nivel de dispositivo)

Limpiar (sólo a nivel de dispositivo)

En "Borrar", puedes restaurar el dispositivo a su configuración de fábrica. Aquí se borrarán tanto los datos corporativos como los privados del dispositivo del usuario final.

Al hacer clic en el "Símbolo de menos" recibirá el siguiente mensaje:



Con "Sí" puede realizar el borrado.

En "Informe de limpieza" se pueden visualizar los siguientes elementos

Borrado por	Historial de quién realizó la limpieza
Fecha	Fecha
Estado	Estado (por ejemplo, si el borrado se ha realizado correctamente)

Configuración de restricciones

Restricciones

Aquí se pueden restringir y bloquear diversas cosas.

Activar cámara	Permitir el uso de la cámara	
Forzar sincronización automática	En	La sincronización está permanentemente activada
	Fuera de	La sincronización se desactiva permanentemente
	Elección del usuario	Seleccionado por el usuario
Fuerza Bluetooth	En	El Bluetooth está activado permanentemente
	Fuera de	El Bluetooth está permanentemente desactivado
	Elección del usuario	Seleccionado por el usuario
Fuerza GPS	En	El GPS está activado permanentemente
	Fuera de	El GPS está permanentemente desactivado
	Elección del usuario	Seleccionado por el usuario
Ubicación de la Red de Fuerzas	En	Localización permanente en Internet
	Fuera de	Desactivación permanente de la localización en Internet
	Elección del usuario	Seleccionado por el usuario

Seguridad		
No permitir compartir ubicación	Especifica si un usuario no puede activar el uso compartido de la ubicación.	
No permitir el Arranque Seguro	Especifica si no se permite al usuario reiniciar el dispositivo en modo de arranque seguro.	
No permitir el reinicio de la red	Especifica si un usuario tiene prohibido restablecer la configuración de red desde Configuración.	
No permitir el restablecimiento de fábrica	Especifica si un usuario tiene prohibido reiniciar el dispositivo.	
Activar ADB	Permite la Conexión a un PC mediante ADB	
Desactivar Keyguard	Desactiva Keyguard	
Información de la pantalla de bloqueo del propietario del dispositivo	Establece la información del propietario del dispositivo que se mostrará en la pantalla de bloqueo.	
Cumplimiento de la normativa	Modo Preguntar al usuario	Se pedirá al usuario que realice las acciones necesarias.
	Modo Bloqueo Contenedor	Ocultar todas las apps hasta que se cumplan todos los requisitos

Gestión de aplicaciones	
Permitir la vinculación de aplicaciones entre perfiles	Permite a las aplicaciones del perfil padre gestionar los enlaces web del perfil gestionado.
No permitir el control de aplicaciones	Especifica si a un usuario se le prohíbe modificar aplicaciones en Ajustes o lanzadores.
No permitir la instalación de aplicaciones	Especifica si un usuario tiene prohibido instalar aplicaciones.
No permitir desinstalar aplicaciones	Especifica si un usuario tiene prohibido desinstalar aplicaciones.
Política de permisos en tiempo de ejecución	Especifica cómo se gestionarán las nuevas solicitudes de permisos de las aplicaciones.
Permitir fuentes desconocidas	Si está activada, los usuarios pueden cargar aplicaciones de forma lateral instalando un archivo .apk.

Conectividad	
No permitir configuración de red móvil	Especifica si un usuario tiene prohibido configurar redes móviles.
Config. inhabilitar anclaje a red	Especifica si un usuario tiene prohibido configurar Tethering y puntos de acceso portátiles.
No permitir Config VPN	Especifica si un usuario tiene prohibido configurar una VPN.
No permitir configuración wifi	Especifica si un usuario tiene prohibido cambiar de punto de acceso WiFi.
No permitir el haz NFC saliente	Especifica si no se permite al usuario utilizar NFC para transmitir datos desde las aplicaciones.
Bloquear configuración WiFi	Este ajuste controla si las configuraciones WiFi creadas por una app Propietario del dispositivo deben estar bloqueadas (es decir, ser editables o eliminables sólo por la app Propietario del dispositivo, ni siquiera por la app Configuración).
Activar Itinerancia de Datos	Activa la Itinerancia de Datos

Bluetooth	
No permitir Bluetooth	Especifica si el bluetooth está deshabilitado en el dispositivo. Requiere Android 8.0
No permitir compartir Bluetooth	Especifica si no se permite compartir bluetooth saliente en el dispositivo. Requiere Android 8.0
No permitir la configuración Bluetooth	Especifica si un usuario tiene prohibido configurar el bluetooth.

Gestión de cuentas	
No permitir añadir perfil gestionado	Especifica si un usuario tiene prohibido añadir perfiles gestionados. Requiere Android 8.0
No permitir añadir Usuarios	Especifica si un usuario tiene prohibido añadir nuevos usuarios.
No permitir Eliminar perfil gestionado	Especifica si los perfiles gestionados de este usuario pueden ser eliminados, salvo por su propietario de perfil. Requiere Android 8.0
No permitir la modificación de la cuenta	Especifica si un usuario tiene prohibido añadir y eliminar cuentas, a menos que sean añadidas mediante programación por Authenticator.

Telefonía	
No permitir llamadas salientes	Especifica que el usuario no puede realizar llamadas telefónicas salientes.
No permitir SMS	Especifica que el usuario no puede enviar ni recibir mensajes SMS.

Sistema	
No permitir la creación de ventanas	Especifica que no se deben crear ventanas aparte de las de la app.
No permitir establecer icono de usuario	Especifica si un usuario no puede cambiar su icono.
No permitir establecer papel tapiz	Restricción de usuario para no permitir establecer un fondo de pantalla.
Desactivar la barra de estado	Desactivar la barra de estado bloquea las notificaciones, los ajustes rápidos y otras superposiciones de pantalla que permiten escapar de un dispositivo de un solo uso.
Activar Hora Automática	Ajusta la hora automáticamente.
Activar Zona Horaria Automática	Establece la zona horaria automáticamente.
Permanece encendido mientras está enchufado	El aparato permanecerá activo mientras esté conectado a una fuente de alimentación.

Almacenamiento	
Desactivar la verificación de aplicaciones	Especifica si un usuario tiene prohibido desactivar la verificación de aplicaciones.
No permitir montar medios físicos	Especifica si un usuario tiene prohibido montar soportes físicos externos.
Activar el servicio de copia de seguridad	El servicio de copia de seguridad gestiona todos los mecanismos de copia de seguridad y restauración del dispositivo. Configurarlo como falso impedirá que se realicen copias de seguridad o se restauren datos. El servicio de copia de seguridad está desactivado por defecto. Requiere Android 8.0
Activar almacenamiento masivo USB	Activa el uso del almacenamiento masivo USB.

Teclado	
No permitir autorrelleno	Especifica si un usuario no puede utilizar los Servicios de Autorrelleno. Requiere Android 8.0
No permitir copiar y pegar entre perfiles	Especifica si lo que se copia en el portapapeles de este perfil se puede pegar en perfiles relacionados.

Sonido	
Rechazar el ajuste de volumen	Especifica si un usuario tiene prohibido ajustar el volumen maestro.
Desactivar Micrófono	Especifica si un usuario no puede ajustar el volumen del micrófono.
Dispositivo de silencio	Dispositivo de silencio.

Gestión de certificados

Aquí puede distribuir certificados de confianza y certificados de identidad a sus dispositivos.

Se requiere Android 8 o superior para distribuir Certificados de Confianza y Android 9 o superior para distribuir Certificados de Identidad.

Con el signo "+" puede añadir varios certificados.

Los certificados de confianza deben estar en formato PEM.

Los certificados de identidad deben estar en formato PKCS12

Gestión de conexiones

Wifi

Para esta configuración, realiza la preconfiguración de los dispositivos de usuario final, para el acceso a los Puntos de Acceso internos

Identificador del Conjunto de Servicios (SSID)	SSID de la red que se va a conectar
Red oculta	Activar, en caso de que el AP no emita el SSID

Tipo de seguridad

Establecer el tipo de seguridad del AP

WEP

Contraseña	Contraseña para el PA

WPA/WPA2

Contraseña	Contraseña para el PA

802.1x EAP

Método EAP

PWD	Identidad	Identidad
	Contraseña	Contraseña

PEAP	Protocolo de autenticación de fase 2	ninguno	Sin protocolo adicional
		MSCHAPV2	Protocolo MSCHAPV2
		GTC	Protocolo GTC
	Certificado CA	Certificado CA	
	Identidad	Identidad	
	Identidad anónima	Identidad anónima	
	Contraseña	Contraseña	

TTLS	Protocolo de autenticación de fase 2	ninguno	Sin protocolo adicional
		PAP	Protocolo PAP
		MSCHAP	Protocolo MSCHAP
		MSCHAPV2	Protocolo MSCHAPV2
		GTC	Protocolo GTC
	Certificado CA	Certificado CA	
	Identidad	Identidad	
	Identidad anónima	Identidad anónima	
	Contraseña	Contraseña	

TLS	Certificado CA	Certificado CA
	Identidad	Identidad
	Contraseña	Contraseña

VPN

Nombre de la conexión	Nombre de la conexión VPN

Tipo de VPN

VPN

Cliente VPN

Cliente VPN AppTec360	
Configuración de la puerta de enlace	Selecciona la Configuración VPN de la **Pasarela**(Ver **Configuración General > Pasarela Universal > Configuración VPN**)
VPN siempre activa	Activar Bloqueo Nativo
Activar el bloqueo de AppTec360	Activar el bloqueo de AppTec360

Integrado (sólo disponible en dispositivos Samsung)			
Tipo de conexión	PPTP	Servidor	Servidor
		Activar el cifrado PPTP	Activar el cifrado PPTP
	L2TP / IPSec PSK	Servidor	Servidor
		Clave precompartida IPSec	Clave precompartida IPSec
		Activar Secreto L2TP	Activar Secreto L2TP
		Secreto L2TP	Secreto L2TP
	IPSec XAuth PSK	Servidor	Servidor
		Identificador IPSec	Identificador IPSec
		Clave precompartida IPSec	Clave precompartida IPSec
Búsqueda DNS Dominios	Búsqueda DNS Dominios		
Ajustes expertos	Servidores DNS	Servidores DNS	
	Rutas de reenvío	Rutas de reenvío	

VPN abierta		
Servidor	Servidor	
Perfil OpenVPN	Perfil OpenVPN	
Aplicación OpenVPN	OpenVPN para Android (recomendado)	
	Conexión OpenVPN	
Ajustes expertos	Servidores DNS	Servidores DNS
	Rutas de reenvío	Rutas de reenvío

Samsung / Cisne fuerte			
Tipo de conexión	PPTP	Servidor	Servidor
		Nombre de usuario	Nombre de usuario
		Contraseña	Contraseña
		Activar el cifrado PPTP	Activar el cifrado PPTP
	L2TP / IPSec PSK	Servidor	Servidor
		Clave precompartida IPSec	Clave precompartida IPSec
		Nombre de usuario	Nombre de usuario
		Contraseña	Contraseña
		Activar Secreto L2TP	Secreto L2TP
	IPSec XAuth PSK	Servidor	Servidor
		Identificador IPSec	Identificador IPSec
		Clave precompartida IPSec	Clave precompartida IPSec
		Nombre de usuario	Nombre de usuario
		Contraseña	Contraseña
Ajustes expertos	Servidores DNS	Servidores DNS	
	Rutas de reenvío	Rutas de reenvío	

Cisco Any Connect		
Servidor	Servidor	
Modo Certificado	Discapacitados	Discapacitados
	Automático	Automático
Ajustes expertos	Servidores DNS	Servidores DNS
	Rutas de reenvío	Rutas de reenvío

VPN por aplicación

Cliente VPN

Cliente VPN AppTec360		
Configuración de la puerta de enlace	Selecciona la Configuración VPN de la **Pasarela**(Ver **Configuración General > Pasarela Universal > Configuración VPN**)	
Aplicaciones VPN	Aplicaciones VPN	
VPN siempre activa	Activar Bloqueo Nativo	VPN siempre activa
Activar el bloqueo de AppTec360	Activar el bloqueo de AppTec360	

Samsung / Cisne fuerte			
Tipo de conexión	PPTP	Servidor	Servidor
		Aplicaciones VPN	Aplicaciones VPN
		Nombre de usuario	Nombre de usuario
		Contraseña	Contraseña
		Activar el cifrado PPTP	Activar el cifrado PPTP
	L2TP / IPSec PSK	Servidor	Servidor
		Aplicaciones VPN	Aplicaciones VPN
		Clave precompartida IPSec	Clave precompartida IPSec
		Nombre de usuario	Nombre de usuario
		Contraseña	Contraseña
		Activar Secreto L2TP	Secreto L2TP
	IPSec XAuth PSK	Servidor	Servidor
		Aplicaciones VPN	Aplicaciones VPN
		Identificador IPSec	Identificador IPSec
		Clave precompartida IPSec	Clave precompartida IPSec
		Nombre de usuario	Nombre de usuario
		Contraseña	Contraseña
Ajustes expertos	Servidores DNS	Servidores DNS	
	Rutas de reenvío	Rutas de reenvío	

Restricciones

Aquí puede establecer las restricciones, en relación con la gestión de la conexión.

Permitir itinerancia de datos	Permitir datos móviles en itinerancia
Forzar itinerancia de datos	Si se activa, la itinerancia para datos móviles se activa permanentemente (¡no se recomienda!) Este ajuste sobrescribe el ajuste "Permitir itinerancia de datos".
Los siguientes ajustes sólo están disponibles en SAFE 2.x o superior	
Permitir sólo llamadas de emergencia	Permitir sólo llamadas de emergencia
Permitir WiFi	Permitir WiFi
Nivel mínimo de seguridad de la red WiFi	Nivel mínimo de seguridad de la red WiFi Abierto = se permiten todos los tipos de WiFi
Prohibir al usuario añadir redes WiFi	El usuario no puede añadir una red WiFi por sí mismo Este ajuste sólo es posible si se ha definido un perfil WiFi en "Gestión de conexiones".
Permitir SMS y MMS	Todos = Se permite todo el tráfico de SMS y MMS Sólo SMS entrantes = Sólo se permiten mensajes SMS entrantes Sólo SMS salientes = Sólo se permiten mensajes SMS salientes Ninguno = No se permite el tráfico SMS / MMS
Permitir sincronización en itinerancia	Permitir sincronización en itinerancia Encendido = activado Apagado = desactivado Elección del usuario = elección del usuario
Permitir itinerancia de voz	Permitir itinerancia de voz Encendido = activado Apagado = desactivado Elección del usuario = elección del usuario
Utilizar el servidor proxy http del sistema	El uso de un servidor proxy HTTP, que se proporciona mediante la configuración del sistema en ajustes, depende de la red conectada (WiFi o APN).

Gestión PIM

Intercambio de Gmail

Información: Esta Configuración se aplicará a la aplicación de Gmail. Así que tienes que aprobar e instalar Gmail.

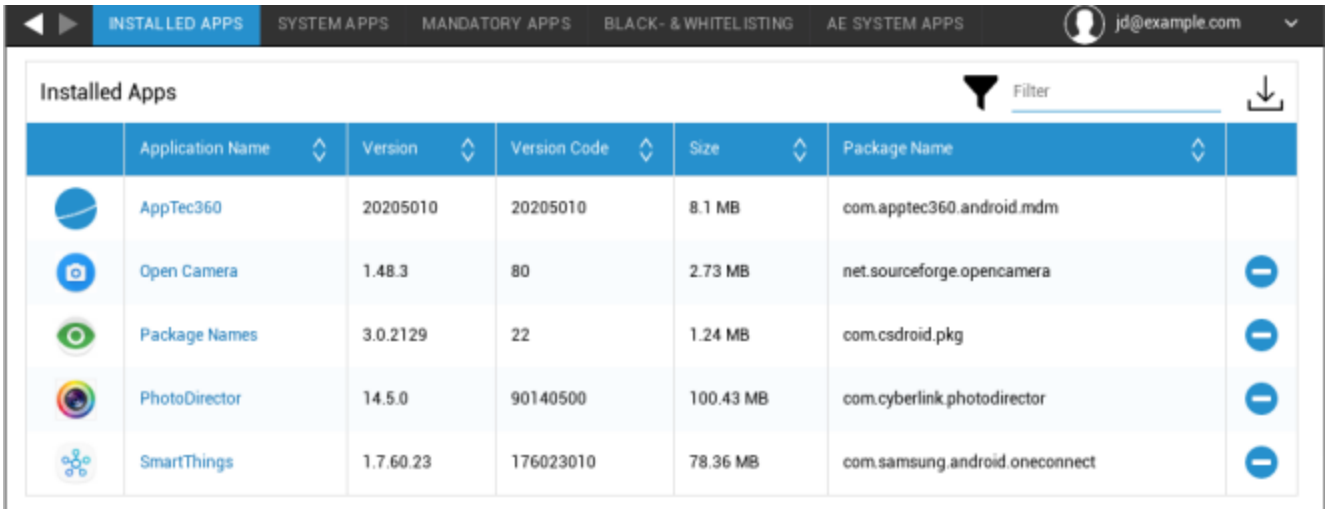
Dirección de correo electrónico	La dirección de correo electrónico del usuario facilitada Ten en cuenta los "Marcadores de posición", que puedes utilizar para trabajar con credenciales y no realizar cambios manualmente en cada dispositivo Con un clic puedes visualizarlos tú mismo
Nombre de host del servidor	Dirección del servidor de tus servidores Exchange
Nombre de usuario	El nombre de inicio de sesión para el dispositivo del usuario final correspondiente, ten en cuenta también los "Marcadores de posición aquí".
Firma	Se puede adjuntar una firma (Sugerencia: Algunos dispositivos requieren formato HTML para la firma)
Número de días anteriores a sincronizar	Número de días, que determina cuándo se sincronizan de nuevo los correos electrónicos
Identificador del dispositivo	Es una cadena que contiene el EAS DeviceID. Forma parte de los protocolos EAS y sólo está permitida en algunos países.
Utiliza la Capa de Conexión Segura (SSL)	Utilizar una conexión SSL
Acepta todos los certificados	Se aceptan todos los certificados. Selecciona esta opción si tu Exchange Server utiliza un certificado autofirmado

Gestión de aplicaciones

Enterprise App Manager

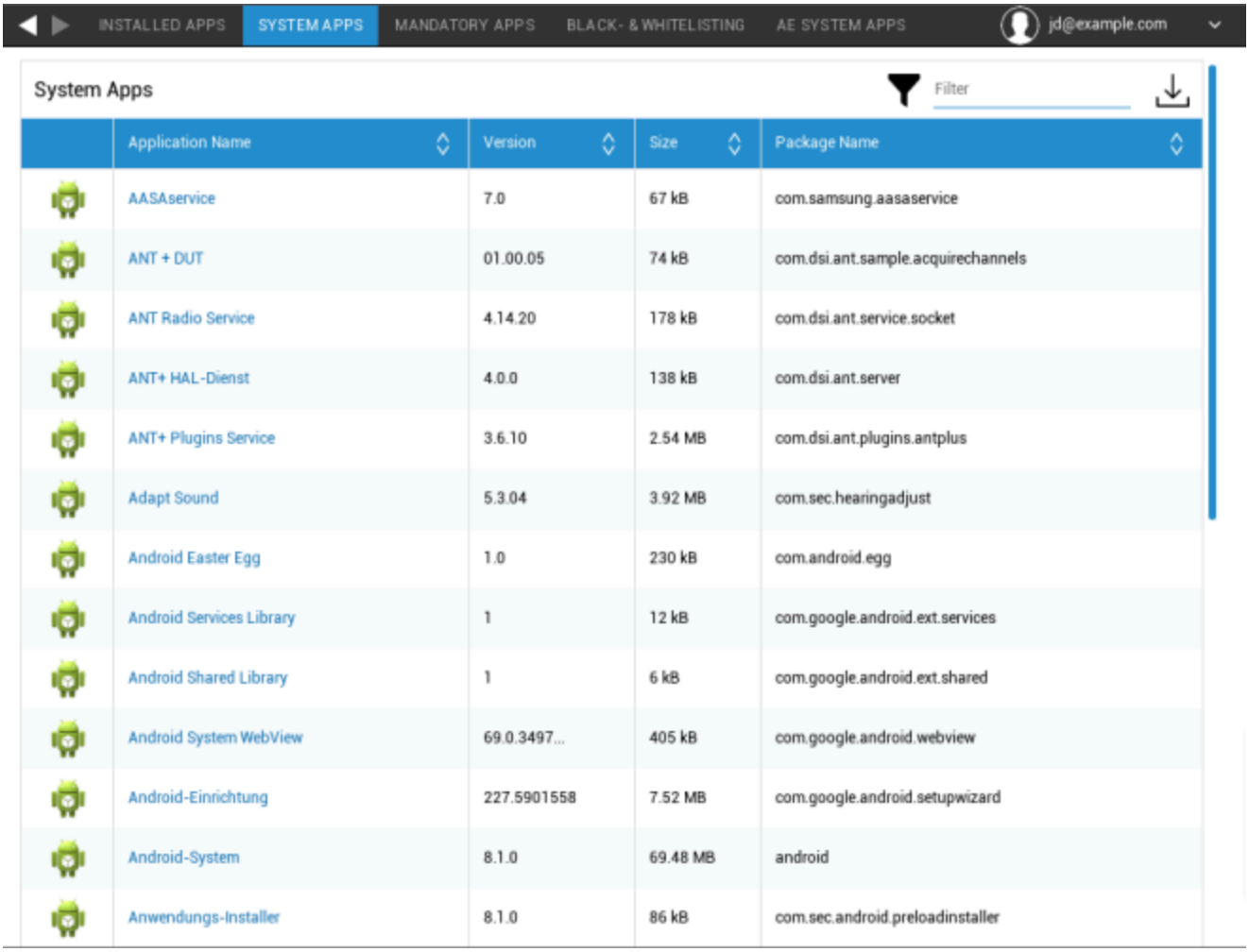
Aplicaciones instaladas (sólo en el dispositivo)

Aquí se mostrarán todas las aplicaciones instaladas actualmente en el dispositivo del usuario final.



Aplicaciones del sistema (sólo a nivel de dispositivo)

En "Aplicaciones del sistema", aparecerán todas las aplicaciones y servicios que el fabricante del dispositivo ya ha instalado en el dispositivo del usuario final.



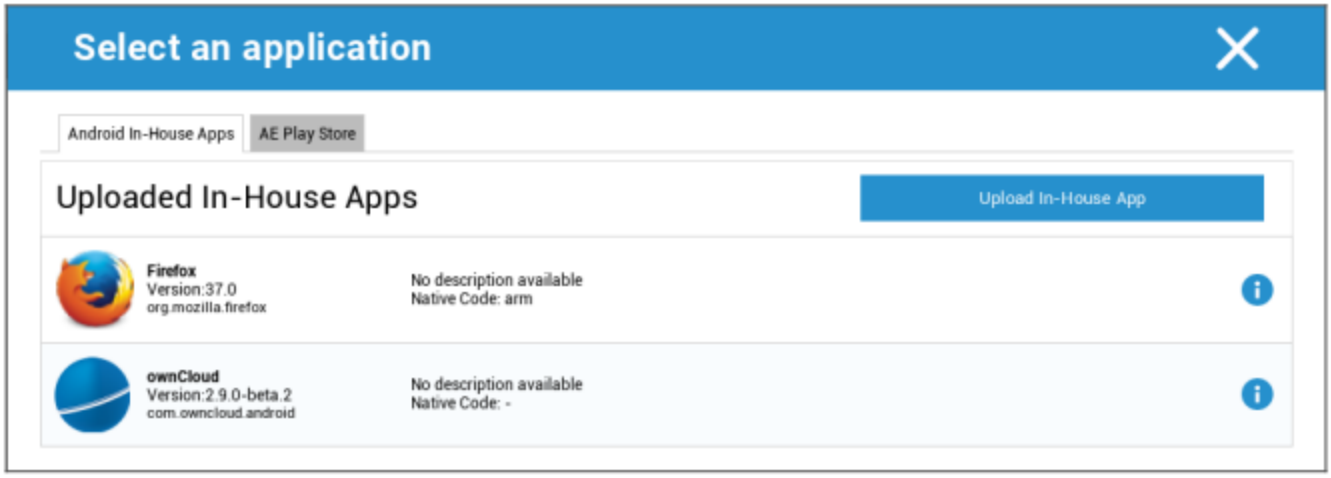
Application Name	Version	Size	Package Name
AASAservice	7.0	67 kB	com.samsung.aasaservice
ANT + DUT	01.00.05	74 kB	com.dsi.ant.sample.acquirechannels
ANT Radio Service	4.14.20	178 kB	com.dsi.ant.service.socket
ANT+ HAL-Dienst	4.0.0	138 kB	com.dsi.ant.server
ANT+ Plugins Service	3.6.10	2.54 MB	com.dsi.ant.plugins.antplus
Adapt Sound	5.3.04	3.92 MB	com.sec.hearingadjust
Android Easter Egg	1.0	230 kB	com.android.egg
Android Services Library	1	12 kB	com.google.android.ext.services
Android Shared Library	1	6 kB	com.google.android.ext.shared
Android System WebView	69.0.3497...	405 kB	com.google.android.webview
Android-Einrichtung	227.5901558	7.52 MB	com.google.android.setupwizard
Android-System	8.1.0	69.48 MB	android
Anwendungs-Installer	8.1.0	86 kB	com.sec.android.preloadinstaller

Aplicaciones obligatorias

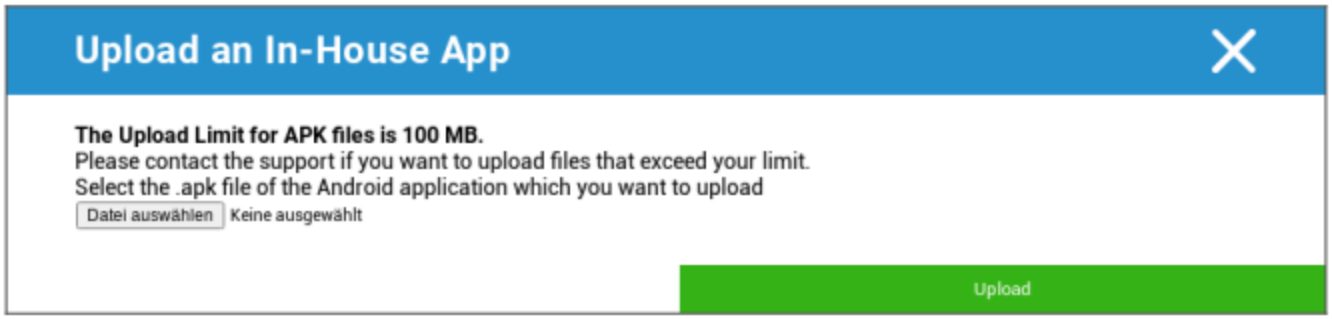
En Aplicaciones obligatorias, puede establecer las aplicaciones obligatorias requeridas. Se pedirá continuamente al usuario que instale esta aplicación designada.

A través del , se puede definir la aplicación obligatoria requerida.

Puede ser una In-House App de las "Android In-House Apps", que has cargado en Ajustes Generales.

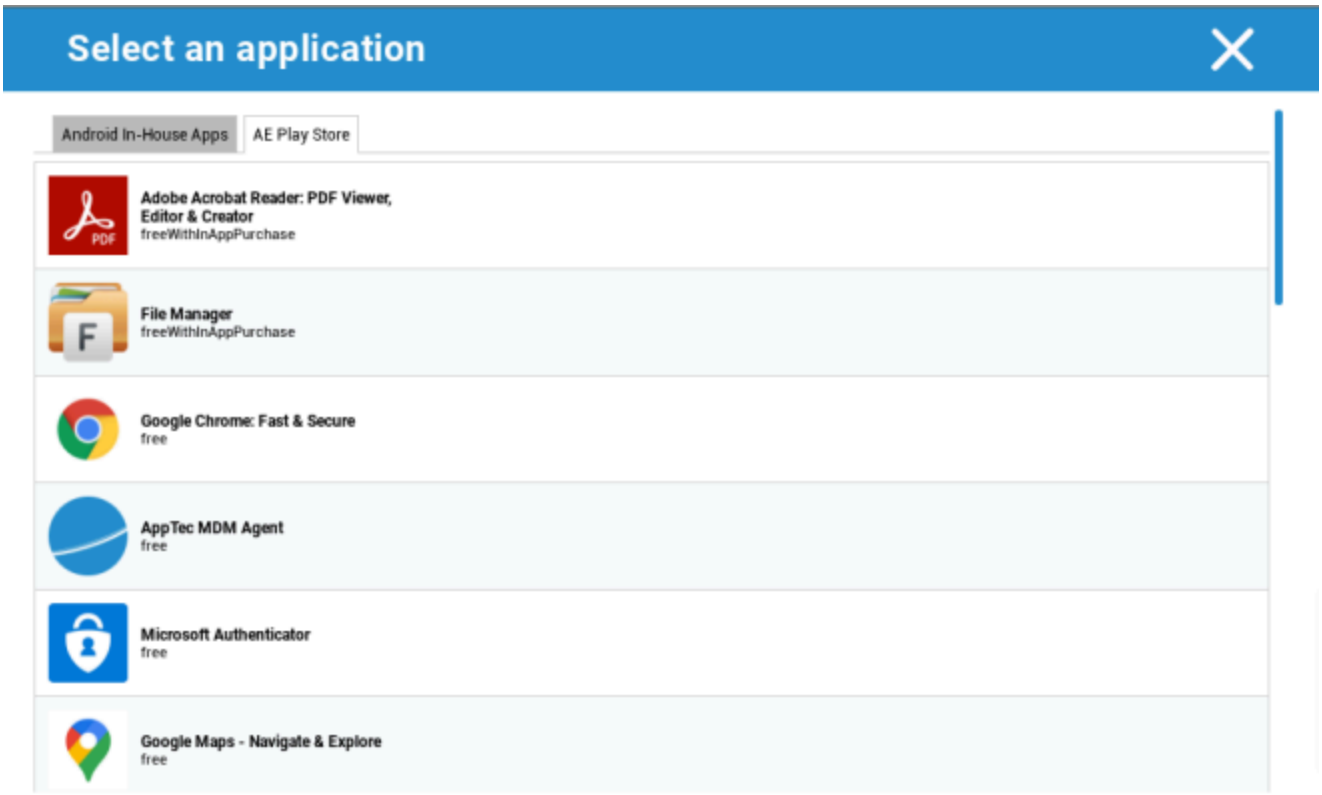


También puede seleccionar y cargar directamente un archivo apk con "Cargar aplicación interna".



Si está instalando una aplicación interna, tendrá la posibilidad de activar "Mantener al día". Si está activada y ha definido una versión más reciente en la base de datos de aplicaciones internas, la aplicación se actualizará en el dispositivo.

O puede ser una aplicación "AE Play Store" de Google Work Play Store.



En esta pestaña sólo se mostrarán las "AE Play Store Apps" aprobadas.

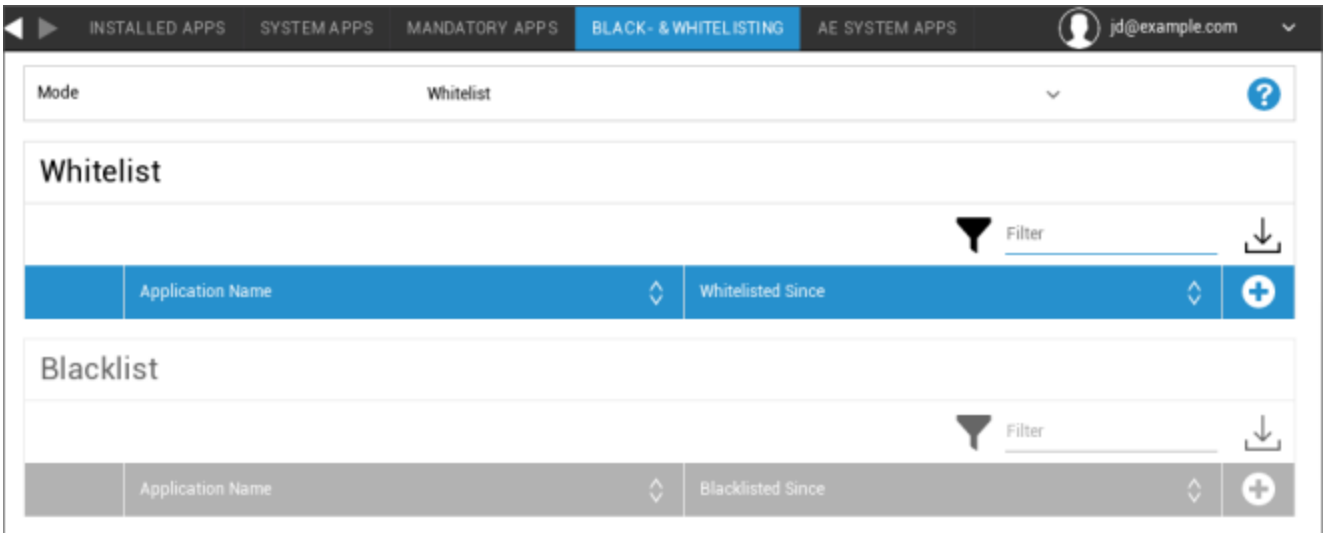
Para aprobar una "AE Play Store App" por favor vaya a "Ajustes Generales" > "Gestión de Apps" > "AE Play

Store" y añadir una aplicación a través del botón que le redirigirá a la pestaña "Play Store Apps" (o usted
puede ir directamente a la pestaña "Play Store Apps").

En la pestaña "Play Store Apps" puedes buscar aplicaciones. Al hacer clic en una aplicación, se abre la página de la aplicación
y aquí puede aprobar la aplicación haciendo clic en "Aprobar".

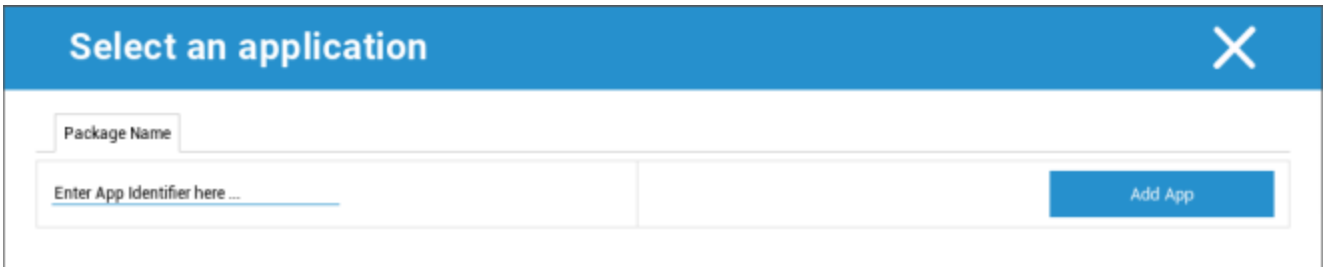
Listas negras y blancas

En "Listas negras y blancas", puede elegir entre el modo "Lista blanca" y el modo "Lista negra".



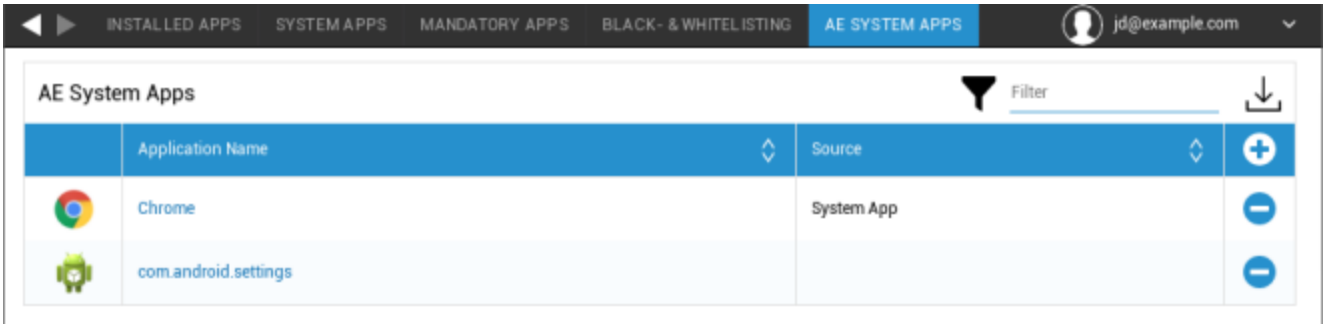
Lista blanca	Sólo las aplicaciones y servicios que se añadan a la lista podrán instalarse en el dispositivo del usuario final. Si ya están preinstalados en el dispositivo del usuario final, se activarán y configurarán para que el usuario pueda ejecutarlos.
	Todas las demás apps que no se añadan a la lista no podrán instalarse en el dispositivo del usuario final. Si ya están preinstaladas en el dispositivo del usuario final, se desactivarán y se configurarán para que el usuario no pueda ejecutarlas.
Lista negra	Las aplicaciones y servicios que se añadan a la lista no podrán instalarse en el dispositivo del usuario final. Si ya están preinstalados en el dispositivo del usuario final, se desactivarán y se configurarán para que el usuario no pueda ejecutarlos.
	Todas las demás aplicaciones que no se añadan a la lista pueden instalarse en el dispositivo del usuario final. Si ya están preinstaladas en el dispositivo del usuario final, se activarán y configurarán para que el usuario pueda ejecutarlas.

A través de la , añades aplicaciones o servicios adicionales a la lista actualmente utilizada.
A través de la , añades aplicaciones o servicios adicionales a la lista actualmente inactiva.
Puedes definir un "Nombre de paquete":

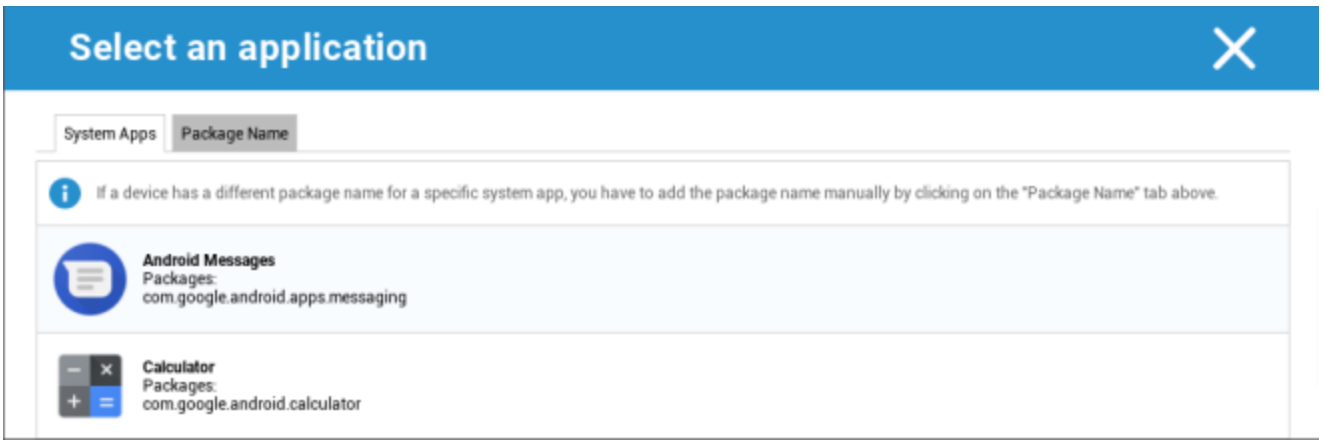

Select an application
Package Name
Enter App Identifier here ...
Add App

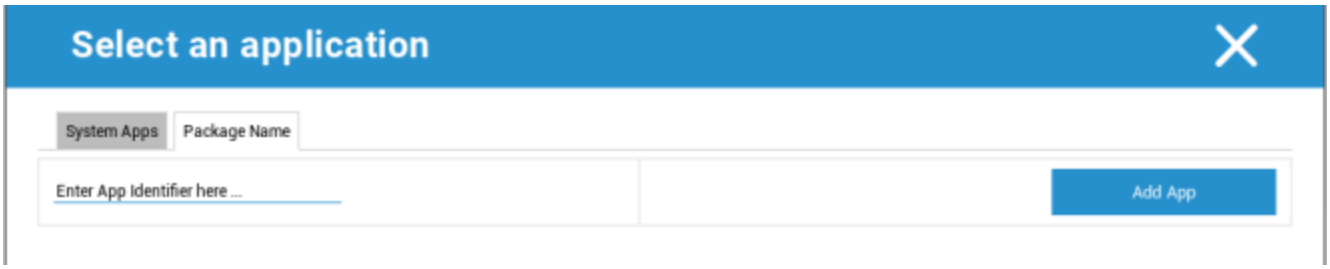
Aplicaciones del sistema AE

Aquí puede definir una lista que contenga aplicaciones específicas del sistema que deban activarse en los dispositivos.



Si hace clic en el botón, puede elegir entre una lista de posibles aplicaciones del sistema proporcionada por Google o introducir directamente el nombre del paquete de una aplicación del sistema que deba activarse.





Ten en cuenta que las aplicaciones de sistema de la lista proporcionada por Google son sólo aplicaciones que pueden ser aplicaciones de sistema, pero no tienen por qué ser necesariamente aplicaciones de sistema en tus dispositivos.

Sin embargo, esta lista sólo afecta a las aplicaciones que ya están preinstaladas.

La adición de aplicaciones que no estén preinstaladas en tus dispositivos no afectará a los mismos, independientemente de si la aplicación procede de la lista proporcionada por Google o de si se introduce directamente el nombre del paquete de la aplicación.

Restricciones y ajustes

Configuración de App Management

Aquí puedes configurar el comportamiento del dispositivo con respecto a las actualizaciones de aplicaciones.

Actualizar frecuencia de comprobación	Especifica en qué intervalo el Cliente AppTec360 buscará actualizaciones de la aplicación. El valor por defecto es 24 horas.
Umbral Wi-Fi	Las aplicaciones que superen el tamaño especificado se descargarán a través de Wi-Fi. Si se selecciona "Sólo Wi-Fi", todas las apps se descargarán a través de Wi-Fi.

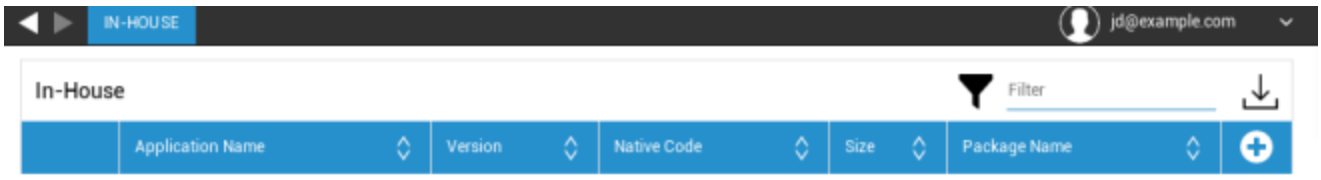
App Store para empresas

En la empresa

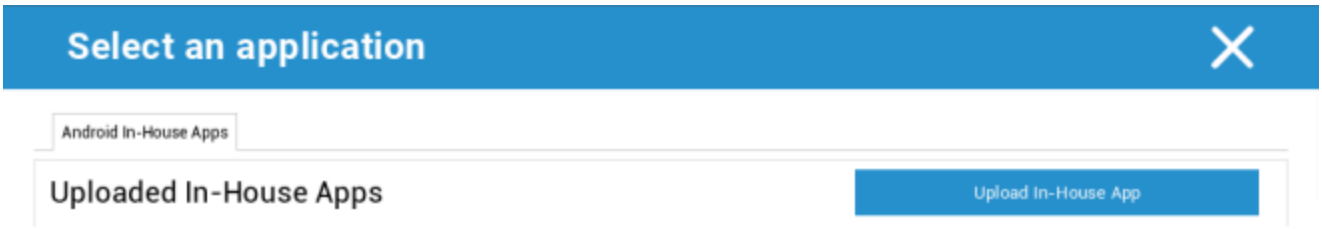
En el punto "In-House", puede cargar y distribuir aplicaciones desarrolladas internamente.

Con el símbolo, puede distribuir In-House Apps adicionales.

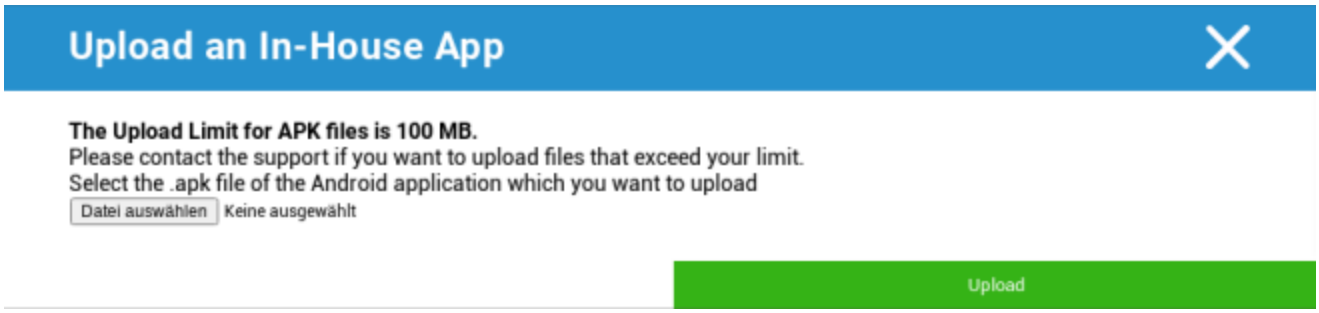
Si está instalando una aplicación interna, tendrá la posibilidad de activar "Mantener al día". Si está activada y ha definido una versión más reciente en la base de datos de aplicaciones internas, la aplicación será
actualizado en el dispositivo.



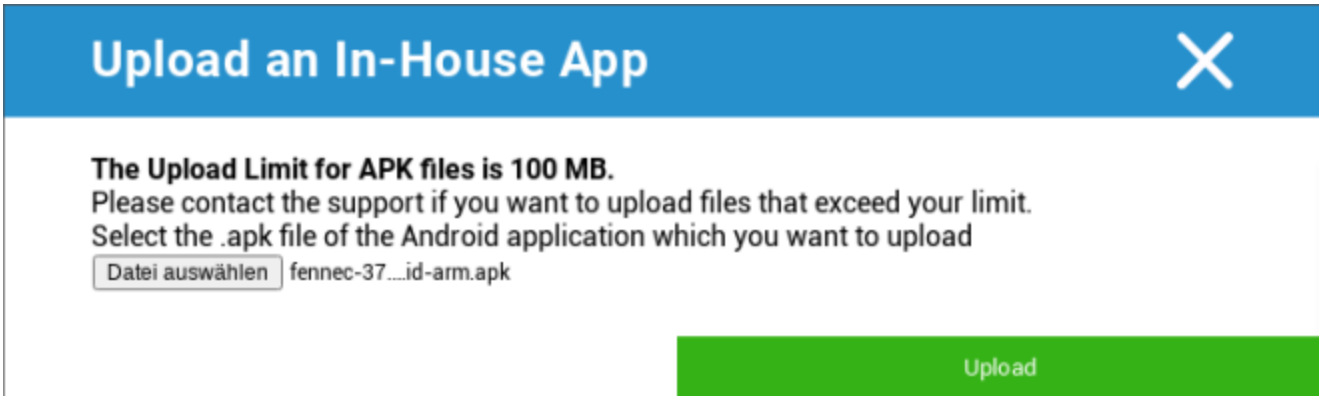
Si no ha distribuido In-House Apps, recibirá el siguiente resumen:



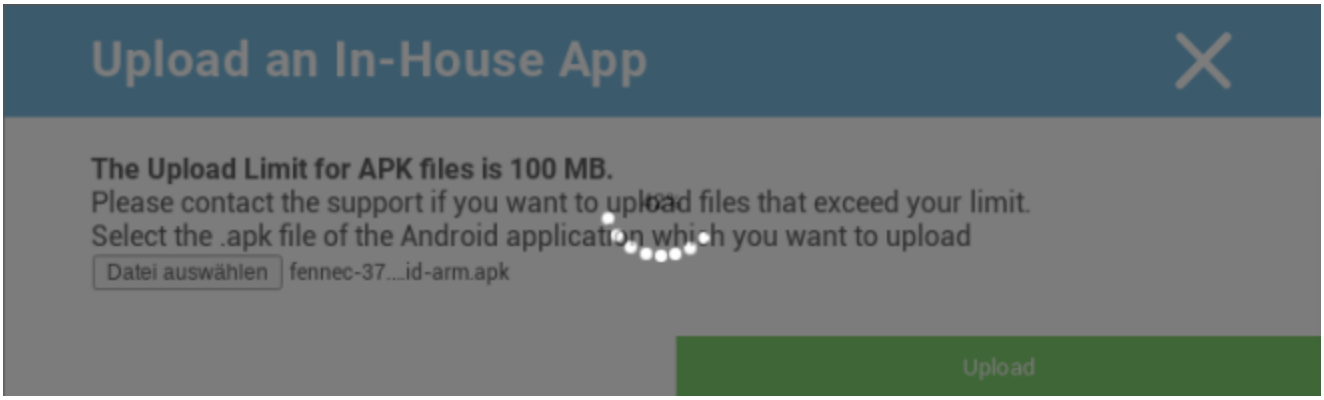
Para ello, haga clic en "Cargar aplicación interna" y obtendrá el siguiente resumen:



Ahora, elige con "Buscar... "un archivo .apk y haz clic en "Cargar".



Tu aplicación se cargará ahora, en el centro del círculo verás un indicador de porcentaje, que muestra qué parte de tu aplicación ya se ha cargado.



Si la carga de su aplicación interna se ha realizado correctamente, podrá encontrar la aplicación cargada.
en su catálogo de aplicaciones.

El usuario ahora tiene la opción de ver e instalar esta aplicación en la AppTec360 Store en el usuario final
dispositivo, en la categoría "In-House".

Debido al hecho de que esto no implica una aplicación de Google PlayStore, el usuario no necesita un almacenamiento de Google
ID en su respectivo dispositivo de usuario final.

Play Store para empresas

AE Play Store

Aquí puede añadir aplicaciones a la Play Store de Android Enterprise. Tenga en cuenta que tiene que aprobar
Apps con su cuenta de administrador AE antes de poder añadirlas.

Para aprobar una aplicación, consulte las instrucciones en Aplicaciones obligatorias.

Modo quiosco y lanzador

Modo quiosco

El Modo Quiosco te permite predefinir una app o una URL. Entonces será posible exclusivamente ejecutar/visitar esta app y/o URL.

Del mismo modo, se pueden desactivar varios botones de hardware en el Modo Quiosco diverso.

Inicio automático	Inicia automáticamente el Modo Quiosco, en cuanto el perfil llega al dispositivo del usuario final
¿Modo Quiosco Programado?	Puedes planificar una hora para el Modo Quiosco, que se iniciará y finalizará automáticamente a la hora que tú establezcas.
Hora de inicio	Hora de inicio
Tiempo en minutos	Tiempo en minutos, tras el cual el Modo Quiosco debe finalizar de nuevo

Tipo de aplicación

Aplicación única	Si quieres iniciar la App en el Modo Quiosco, selecciona Paquete" en "Tipo de Aplicación".
Aplicación quiosco	Pulsa aquí, para seleccionar una aplicación que deba iniciarse en Modo Quiosco Encontrarás el resumen habitual de App Management Puedes seleccionar entre "Google Play Store", "Aplicaciones internas de Android" y "Nombre del paquete".

Tipo de aplicación

URL	Si quieres lanzar una URL en el Modo Quiosco, selecciona "URL" en "Tipo de aplicación". A continuación, define la dirección URL que desees
Limpiar el navegador tras inactividad	Aquí puedes definir un intervalo de tiempo en minutos, tras el cual debe relanzarse el Modo Quiosco
Borrar caché web y cookies	Si activas esta función, después de reiniciar el Modo Quiosco, se borrará la Caché Web (cookies e imágenes almacenadas en caché)
Política del mismo origen	Si esta función está activa, el usuario sólo podrá navegar por las subpáginas de una URL definida Por ejemplo, has definido la siguiente URL:www.mypage.com Entonces, el usuario puede navegar en: www.mypage.com/subpage
URLs en lista blanca	Aquí puedes mantener una Lista Blanca, todas estas URLs están permitidas Máximo 1 URL por línea Una URL debe empezar por http:/ o https://
URLs en la lista negra	Aquí puedes mantener una Lista Negra, todas estas URLs no están permitidas Máximo 1 URL por línea Una URL debe empezar por http:/ o https://
Orientación de la pantalla	Este ajuste está relacionado con los ajustes de pantalla Automático = automático Vertical = formato vertical Paisaje = modo paisaje

Multi App	Si seleccionas el Modo Quiosco "Multi App", se impondrá el uso del AppTec360 Launcher.
Aplicaciones	Aplicación: Selecciona una aplicación de Playstore o una aplicación propia como aplicación de quiosco. También es posible introducir un nombre de paquete. La Aplicación de Quiosco seleccionada debe estar instalada en el dispositivo. Recuerda establecer la Aplicación de Quiosco como obligatoria. Acceso directo en la pantalla de inicio: Si está activado, se creará un acceso directo en la pantalla de inicio. Si está desactivado, la aplicación seguirá apareciendo en la Lista de aplicaciones.

Contraseña de salida activada	Si activas esta función, el usuario podrá finalizar el Modo Quiosco con una contraseña predefinida por ti.
Salir Contraseña	Esta es la contraseña predefinida por ti
Contraer automáticamente la barra de estado	Si está activada, la Barra de Estado se coloreará automáticamente. Con esta opción, los usuarios pueden ver la información de la Barra de Estado, pero no pueden acceder a sus funciones.
Desactivar la barra de estado	La barra de estado contiene notificaciones, accesos directos e información. Sólo disponible para dispositivos Samsung con SAFE 4.0 o superior.
Desactivar teclas de volumen	Desactivar las teclas de volumen (sólo disponible en dispositivos Samsung con SAFE 3.0 o superior)
Desactivar el interruptor de encendido/apagado	Desactivar el interruptor de Encendido/Apagado (sólo disponible en dispositivos Samsung con SAFE 3.0 o superior)
Desactivar Botón Inicio	Desactivar botón Inicio. Si se ha activado esta función, el Modo Quiosco sólo se puede finalizar en la Consola AppTec360 (sólo disponible en dispositivos Samsung con SAFE 3.0 o superior)
Desactivar la barra de navegación	Con esto puedes desactivar la Barra de Navegación (Atrás / Menú) Si se ha activado esta función, el Modo Quiosco sólo se puede finalizar en la Consola AppTec360 (sólo disponible en dispositivos Samsung con SAFE 3.0 o superior)

Lanzador AppTec360

Activar AppTec360 Launcher	Activado: Activa el Lanzador de AppTec360. El usuario tiene que configurarlo como Lanzador por defecto una vez. Nota: Si el Modo Quiosco está activado, y el Modo Quiosco está configurado como "Multi App", se impondrá el uso del lanzador AppTec360.
Iconos grandes	Activado: Muestra una versión más grande de los iconos de la aplicación en el lanzador.
Ocultar el icono de la aplicación AppTec360	Activado: Oculta completamente la aplicación AppTec360
Ocultar el icono de la tienda AppTec360	Activado: Oculta completamente la AppStore de AppTec360 Enterprise

Configuración de AppTec360

Activar la App de Configuración de AppTec360	La App de Configuración AppTec360 proporciona control sobre las conexiones WiFi y Bluetooth
Activar Ajustes en Multi App Modo quiosco	Si está activado, los usuarios pueden acceder a la App de Configuración de AppTec360 mientras el Modo Kiosko Multi App está activo

Mando a distancia

Splashtop

Para iniciar una sesión de control remoto de su dispositivo, es necesario instalar la aplicación "Splashtop Streamer" en el dispositivo añadiéndola a **App Management** → **Enterprise App Manager** → **Mandatory Apps**.

A continuación, configure los siguientes ajustes para Splashtop:

Activar Splashtop	Si está activada, AppTec360 configurará la aplicación Splashtop para permitir el control remoto
Despliega el código	Ve a https://my.splashtop.com e inicia sesión en tu cuenta Splashtop. Haga clic en "Añadir ordenador" y copie el código de despliegue de 12 dígitos de la página resultante.
¿Establecer pasarela de despliegue personalizada?	Despliega la Pasarela
Despliega el dominio / host de la pasarela	Despliega la Pasarela
Verificación de certificados	Verificación de certificados

A continuación, puede utilizar la opción Splashtop Remote Control el menú contextual (engranaje junto a la barra de búsqueda, cuando el dispositivo está seleccionado o haga clic derecho sobre el dispositivo en el árbol) para iniciar la sesión de control remoto.

TeamViewer

Para iniciar una sesión de control remoto para su dispositivo, es necesario instalar la aplicación "TeamViewer QuickSupport" en el dispositivo añadiendo la aplicación a **App Management** → **Enterprise App Manager** → **Aplicaciones obligatorias**.

A continuación, puede utilizar la opción **TeamViewer Remote Control** el menú contextual (engranaje junto a la barra de búsqueda, cuando el dispositivo está seleccionado o haga clic derecho sobre el dispositivo en el árbol) para iniciar la sesión de control remoto.

Gestión de contenidos

ContentBox

Aquí puede activar el ContentBox.

En cuanto active la opción "Activar ContentBox", se instalará una aplicación ContentBox independiente.
automáticamente en el dispositivo del usuario final.

Navegador seguro

Aquí puede configurar los ajustes del AppTec360 Secure Browser.

En cuanto cambies la sección de "Navegador seguro" a "Activado", se instalará automáticamente una aplicación de navegador independiente
en el dispositivo del usuario final.

Requerir contraseña	Exige al usuario que establezca y utilice una contraseña para acceder al navegador.
Longitud mínima requerida de la contraseña	Establece el número de caracteres necesarios para la contraseña
Calidad de contraseña requerida	Establece la calidad de la contraseña requerida
Restringir descargas / Abrir en	
Restringir subidas	
Cargar lista blanca	Una lista de URLs para las que siempre se permitirá la subida.
Permitir copia	Permite copiar, cortar o compartir texto dentro de las páginas web.
Permitir Captura de Pantalla	Permite hacer capturas de pantalla.
Frecuencia de limpieza de datos	Selecciona con qué frecuencia deben eliminarse automáticamente TODOS los datos del usuario (historial, caché, etc.).
Marcadores de empresa	Los marcadores aparecerán en la carpeta "Marcadores de empresa" de los marcadores del navegador. No son editables por el usuario.
Ocultar barra de direcciones	
Listas blancas en el navegador (sin Universal Gateway)	Activa la lista blanca de URL del cliente. • Los marcadores de empresa siempre están en la lista blanca • Sólo se admiten 100 URL • Utiliza la pasarela universal para crear listas negras y blancas ilimitadas
URLs en lista blanca	Una lista de URL permitidas.
Listas negras y blancas basadas en la puerta de	Las listas negras tienen los siguientes requisitos:

enlace	• Una pasarela universal AppTec360 en funcionamiento ("Configuración general" → "Pasarela universal") • Una configuración VPN operativa con un servidor DNS especificado ("Configuración general" → "Pasarela universal" → "Configuración VPN") • Una configuración de Lista Negra ("Configuración General" → "Pasarela Universal" → "Lista Negra de Dominios") • Una conexión VPN válida en el perfil ("Gestión de conexiones" → "VPN")

API adicional

Samsung KNOX

Restricciones

Permitir tarjeta SD	
Permitir escritura en tarjeta SD	
Permitir Captura de Pantalla	
Permitir Portapapeles	
Copia de seguridad de la configuración y los datos de la app en Google Cloud	
Restaurar la configuración desde Google Cloud al reinstalar una aplicación	
Permitir depuración USB	
Permitir informe de colisión de Google	
Permitir reinicio de fábrica	
Permitir actualización OTA	
Permitir almacenamiento host USB	Si se activa, el usuario puede conectar cualquier pen drive (almacenamiento USB portátil), disco duro externo o lector de tarjetas Secure Digital (SD), y se monta como unidad de almacenamiento en el dispositivo.
Permitir reproductor multimedia USB (MTP,PTP)	
Permitir micrófono	Desactiva el micrófono para aplicaciones de terceros
Permitir NFC (Comunicación de Campo Cercano)	
Permitir fuentes desconocidas (APK Sideloading)	Si está activada, se permite la carga lateral de aplicaciones (archivos APK). Una vez desactivado este ajuste, el usuario tiene que activarlo manualmente cuando vuelvas a permitir la instalación de APKs de fuentes desconocidas.

Permitir la creación de usuarios	Si está activada, se permite al usuario crear varias cuentas en el dispositivo, por ejemplo, Cuentas de invitado

Correo electrónico

Dirección de correo electrónico	
Protocolo del servidor entrante	
Dirección del servidor entrante	
Puerto del servidor entrante	
Nombre de usuario/contraseña del servidor entrante	
Contraseña del servidor entrante	
El servidor entrante utiliza SSL	
El servidor entrante utiliza TLS	
El servidor entrante acepta todos los certificados	
Protocolo del servidor saliente	
Dirección del servidor saliente	
Puerto del servidor saliente	
El servidor saliente utiliza credenciales adicionales	Si se desactiva, el sistema utiliza las credenciales entrantes también para el servidor saliente.
Nombre de usuario del servidor saliente	
Contraseña del servidor saliente	
El servidor saliente utiliza SSL	
El servidor saliente utiliza TLS	
El servidor saliente acepta todos los certificados	
Establecer firma	
Firma	Nota: En algunos dispositivos, la firma debe especificarse en formato HTML.
Notificar al usuario la recepción de un nuevo eMail	

Intercambio

Dirección de correo electrónico	
Nombre de host del servidor	El nombre de host del servidor Exchange
Nombre de usuario	El nombre de usuario que se utiliza para acceder al Servidor Exchange
Dominio	Si está activada una configuración de puerta de enlace ACL y el campo Dominio no está vacío, la puerta de enlace universal AppTec360 autenticará el dispositivo con el siguiente nombre "Dominio\NNombre de inicio de sesión
Contraseña	
Número de días anteriores a sincronizar	
Frecuencia para sincronizar eMail	
Sincronizar en itinerancia	
Establecer firma	
Firma	Nota: En algunos dispositivos, la firma debe especificarse en formato HTML.
Cuenta por defecto	
Utiliza la Capa de Conexión Segura (SSL)	
Utiliza la Seguridad de la Capa de Transporte (TLS)	
Acepta todos los certificados	

APN

Nombre para mostrar APN	
Nombre del punto de acceso	Nombre del APN
Protocolo del servidor saliente	
MCC - Código de país del móvil	Dejar vacío para utilizar el mmc de la SIM instalada
MNC - Código de red móvil	Dejar vacío para utilizar el mnc de la SIM instalada
Dirección del servidor	
Número de puerto del servidor	
Dirección proxy del servidor	
Dirección del servidor MMS	Dejar vacío por defecto
Número de puerto MMS	Dejar vacío por defecto
Dirección proxy MMS	Dejar vacío por defecto
Nombre de usuario	
Contraseña	
Tipo de punto de acceso	Los tipos aceptados son "por defecto", "mms", "supl".
	Si se pasa nulo o vacío, por defecto se utiliza "por defecto,supl,mms".
	Déjalo vacío por defecto.
APN preferido	

Bluetooth

Permitir la detección de dispositivos mediante Bluetooth	
Permitir emparejamiento Bluetooth	
Permitir dispositivos Auriculares Bluetooth	
Permitir dispositivos manos libres Bluetooth	
Permitir dispositivos Bluetooth A2DP	A2DP, Perfil Avanzado de Distribución de Audio permite la transmisión de audio entre dispositivos
Permitir llamadas salientes	
Permitir la transferencia de datos por Bluetooth	
Permitir anclaje Bluetooth	
Permitir la conexión con el ordenador mediante Bluetooth	

Conexión

Permitir sólo llamadas de emergenciaPermitir Wi-Fi	
Nivel mínimo de seguridad de la red Wi-Fi	
Prohibir al usuario añadir redes Wi-Fi	Esta restricción sólo puede activarse si se define al menos un Perfil Wi-Fi activo en Gestión de conexiones
Permitir SMS y MMS	
Permitir sincronización en itinerancia	
Permitir itinerancia de voz	

Android Enterprise – Dispositivo totalmente gestionado con perfil de trabajo (COPE)

Explicación general de la COPE

COPE es la abreviatura de **Corporate Owned Personally Enabled**(**propiedad de**la empresa **y habilitación personal**).

El modo COPE permite inscribir un dispositivo Android como **Android Enterprise - Dispositivo totalmente gestionado** con perfil integrado **Android Enterprise - Contenedor**.

Puede tratarse de un dispositivo Android que ya esté inscrito como **Android Enterprise - Dispositivo totalmente gestionado** y en la que el **Android Enterprise - Contenedor** se configura adicionalmente, o un dispositivo Android recién inscrito que se inscribe directamente como un **Android Enterprise - Dispositivo totalmente gestionado** junto con el **Android Enterprise - Contenedor** encima.

El modo COPE sólo está disponible para dispositivos con Android 8, 9 y 10

Configuración de perfiles para dispositivos COPE

Dado que no existe un perfil de configuración para el modo COPE propiamente dicho, la configuración de **Android Enterprise - Dispositivo totalmente gestionado** y **Android Enterprise - Contenedor** se separa en dos perfiles dentro del perfil COPE. Es posible pasar de un perfil a otro para la configuración de cada perfil pulsando el botón correspondiente en la parte izquierda de la consola:

Ambos perfiles pueden configurarse como se describe para cada perfil individual:

Android Enterprise - Dispositivo totalmente gestionado

Android Enterprise - Contenedor

Volver al dispositivo totalmente gestionado AE

El perfil **Android Enterprise - Container** puede eliminarse como se describe en **Gestión de móviles**.

Al eliminar el perfil Contenedor, el perfil COPE se transformará en un perfil **Android Enterprise - Dispositivo totalmente gestionado**.

Android Enterprise – Configuración de contenedores

Dependiendo de si ha seleccionado actualmente un perfil de grupo o un dispositivo, la vista general y sus subpuntos difieren - ¡tenga esto en cuenta!

General

Visión general del perfil (sólo a nivel de perfil)

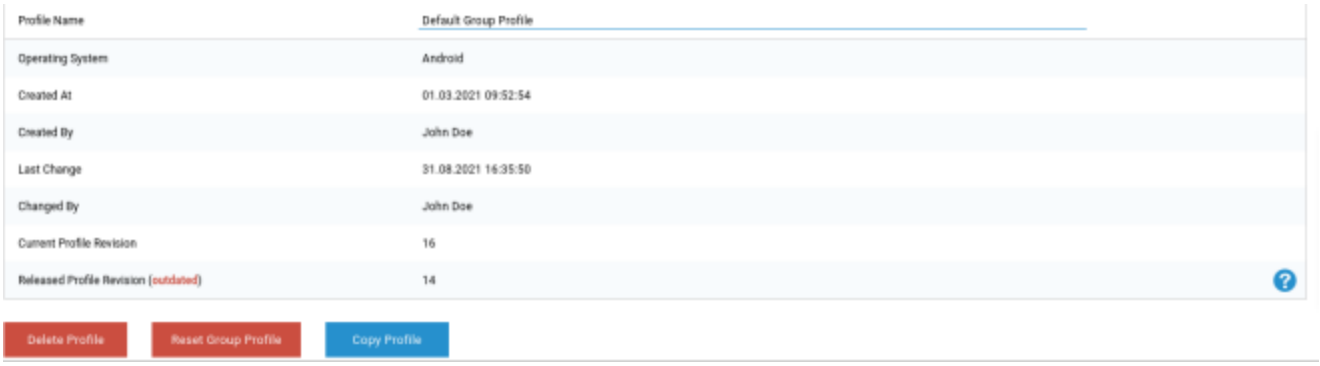
Si se encuentra en un perfil, recibirá una breve descripción del mismo, en cuanto a nombre, sistema operativo, fecha de creación, autor, etc.

Nombre del perfil	Nombre del perfil - se puede renombrar directamente aquí
Sistema operativo	SO válido para el perfil
Creado en	Fecha de creación
Creado por	Creado por
Último cambio	Fecha de la última modificación
Cambiado por	El Usuario que realizó los últimos cambios en este perfil
Revisión actual del perfil	Número de veces que ya se ha actualizado el perfil
Revisión del perfil liberado	Número de veces que el perfil ya ha sido actualizado y se le han asignado dispositivos

Borrar perfil	Borrar perfil
Restablecer perfil de grupo	Restablecer perfil de grupo
Copiar perfil	Copiar perfil

Resumen del perfil del grupo (sólo a nivel de grupo)

Al abrir un perfil de grupo, obtendrás una rápida visión general del perfil.



Nombre del perfil	Nombre del perfil (se puede cambiar aquí)
Sistema operativo	Sistema operativo para el que es el perfil
Creado en	Momento de la creación
Creado por	El creador del perfil
Último cambio	Hora de la última modificación del perfil
Cambiado por	Cuenta que realizó los últimos cambios
Revisión actual del perfil	Revisión del estado del perfil guardado
Revisión del perfil liberado	Revisión del perfil asignado ("Asignar ahora"). Si la etiqueta muestra "(obsoleto)" detrás del texto, significa que has guardado el perfil pero aún no lo has asignado, por lo que los dispositivos seguirán recibiendo una versión antigua.

Visión general del dispositivo (sólo a nivel de dispositivo)

Si se encuentra en un dispositivo, recibirá un resumen general del dispositivo seleccionado:

Nombre del dispositivo	Nombre del dispositivo
Ubicación	Coordenadas de ubicación
Número de teléfono	Número de teléfono
Apps Obligatorias Asignadas	Número de Apps obligatorias asignadas
Versión del SO	Versión del SO del dispositivo
Sistema operativo	Sistema operativo (Android Enterprise)
Número de serie	Número de serie del dispositivo
Propiedad del dispositivo	Dispositivo corporativo o privado
Tipo de dispositivo	Dispositivo gestionado por AE Work
Enraizado	Estado, que indica si el dispositivo ha sido rooteado
Cumple	Cumple las directrices
Dirección IP	Dirección IP del dispositivo
Visto por última vez	Momento en que el dispositivo se conectó por última vez a AppTec
Último empujón	Momento en el que se envió la última pulsación al dispositivo
Asignación de usuarios	El usuario o grupo al que está asignado este dispositivo

Config Revisión

Aquí obtendrá una visión general de qué perfil de grupo está asignado al dispositivo.

Si haces clic en el perfil del grupo, accederás directamente a este perfil y podrás realizar ajustes.

Con este símbolo, puedes revertir las aplicaciones distribuidas a la configuración del perfil de grupo.

Con este símbolo, puedes revertir todas las aplicaciones utilizadas a la configuración del perfil de grupo.

"Nueva revisión disponible" indica que el perfil de grupo se ha modificado y guardado, pero no se ha asignado. El perfil de grupo debe asignarse con "Asignar ahora" a nivel de grupo para aplicar los

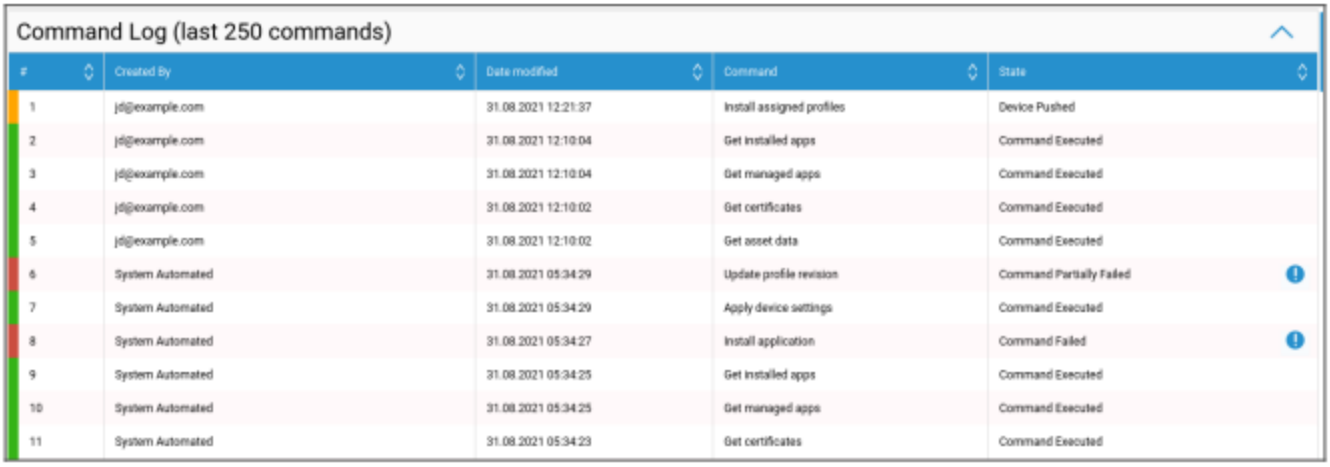
cambios a los dispositivos.

Registro de dispositivos (sólo a nivel de dispositivo)

Aquí recibirá varios registros de dispositivos. En caso necesario, aquí puede averiguar directamente la causa de un error.

Registro de comandos

Aquí puede ver qué comandos se emitieron para el dispositivo y cuál es su estado.



Posibles estados del comando

Dispositivo Empujado	Se ha enviado una solicitud push al servicio push (por ejemplo, APNS) para indicar al dispositivo que se conecte de nuevo al servidor EMM.
Comando creado	El comando se creó en el sistema.
Orden enviada	El comando se envió al dispositivo después de que se conectara al servidor.
Orden ejecutada	El comando se ha ejecutado correctamente.
Comando fallido	El comando falló. *
Comando parcialmente fallido	Dependiendo del SO del dispositivo, algunos comandos pueden agruparse. En este fallaron algunas partes de este grupo de comandos. *
Orden ejecutada, finalmente fallida	La orden se ejecutó, pero puede que no.
Comando Repulsado	El comando fue repulsado por un usuario.
Descartado	El comando fue descartado. Por ejemplo, porque ha sido sustituido por otro comando o porque el dispositivo se ha reinscrito y se han eliminado los comandos antiguos.

*Si hay un signo de exclamación detrás del mensaje, puedes obtener más información pasando el cursor sobre el icono.

Ajustes del dispositivo

Configuración de clientes

Aquí puedes realizar las siguientes configuraciones en tu dispositivo Android:

Tiempo de incumplimiento	El límite de tiempo de espera de respuesta del usuario tras el cual se aplica la acción coercitiva.
Acción coercitiva tras el plazo de cumplimiento	Acción coercitiva cuando un usuario no realiza acciones que conducen a un estado de dispositivo conforme
Frecuencia de recogida de datos	Frecuencia con la que debe recogerse la información del dispositivo/GPS
Frecuencia de latidos del dispositivo	Intervalo en el que el dispositivo debe contactar con el Servidor AppTec Mín. 1 minuto Máx. 24 horas
Activar actualizaciones de ubicación	Si está activado, el dispositivo envía actualizaciones de ubicación al Servidor AppTec
Lugar Hora de actualización	Determina en qué intervalos de tiempo el dispositivo envía actualizaciones de ubicación a AppTec
Utiliza la precisión de ubicación de Google para actualizar la ubicación	Si se activa, se utilizará la ubicación de red para las actualizaciones de ubicación (si se desactivó en "Restricciones", este ajuste no afectará a nada).
Utilizar la localización GPS para actualizar la ubicación	Si está activado, se utilizará el GPS para actualizar la ubicación
Permitir Ubicaciones Simuladas (Falsas)	Permite falsificar la información de localización a través de apps de terceros
Acción de conexión perdida	Si está activada, puedes especificar una acción para el caso de que un dispositivo no consiga una conexión con el servidor MDM en el intervalo de latido. Por ejemplo, si el dispositivo tiene un tiempo de latido de 5 minutos, se conecta al servidor a las 10:35 AM. Después, el dispositivo sale del alcance Wi-Fi. El siguiente heartbeat a las 10:40 AM fallará, y se ejecutará la acción especificada.
Acción	La acción que debe emprenderse en cuanto un aparato deje de ser conforme. • Lock Dispositivo = dispositivo de bloqueo

	• Borrar dispositivo = el dispositivo se restablecerá a los ajustes de fábrica • Borrar dispositivo y tarjeta SD = el dispositivo se restablecerá a los ajustes de fábrica y se borrará el almacenamiento de la tarjeta SD
Umbral	Puedes especificar un umbral de latidos fallidos necesarios para activar la acción especificada.

Modo de aplicación de la política	Por defecto:	Periódicamente se pedirá a los usuarios que ejecuten las acciones pendientes
	Aplicación perezosa de la política:	Nunca se pedirá a los usuarios que ejecuten las acciones pendientes. Todas las acciones abiertas se mostrarán en el Cliente AppTec
	Aplicación agresiva de la política:	A los usuarios se les pedirá sin parar que ejecuten las acciones pendientes
Bloqueo de versión AppTec	Si está activada, se puede especificar un código de versión para la aplicación AppTec. El cliente de AppTec sólo se actualizará a la versión especificada. Las versiones más recientes serán ignoradas. NO es posible un downgrade.	
Código de versión	Código de versión para la aplicación AppTec que se va a bloquear.	
Desactivar Notificación AppTec	Si se desactiva, el Cliente AppTec no mostrará una Notificación en la Barra de Notificaciones. Así, los usuarios pueden cerrar el cliente AppTec a través del administrador de tareas. Si el cliente de AppTec está cerrado, varias funciones, como el Modo Quiosco y la Lista Negra/Blanca de Aplicaciones, no funcionarán correctamente. Los dispositivos Samsung ofrecen un mecanismo de protección para el Cliente AppTec. La notificación está desactivada por defecto en los dispositivos Samsung compatibles con las API KNOX. La notificación no debería desactivarse en dispositivos con Android 8.0 o superior.	

Papel pintado

Establecer fondo de pantalla personalizado	Activar/Desactivar el fondo de pantalla personalizado
Papel pintado	Configura el modo de papel tapiz para utilizar un código de color o una imagen
Especifica un color	Especifica un color de fondo como valor hexadecimal, por ejemplo #000000 para el negro o #ffffff como blanco
Establecer imagen como fondo de pantalla	Sube el archivo de imagen que quieras utilizar como fondo de pantalla

Gestión de activos (sólo a nivel de dispositivo)

Información del dispositivo

Modelo	Designación del modelo de aparato
Sistema operativo	OS
Versión del SO	Versión del SO
Número de serie	Número de serie
Nombre del dispositivo	Nombre del dispositivo
Estado de la batería	Estado de la batería
Memoria Libre / Total	Memoria libre / total
Caja fuerte Samsung	Interfaz Samsung SAFE, necesaria para diversas opciones de configuración
Tarjeta SD disponible	Tarjeta SD disponible
Tarjeta SD emulada	Tarjeta SD emulada
Tarjeta SD extraíble	Tarjeta SD extraíble
SD Memoria Libre / Total	SD Libre / Memoria total de la tarjeta SD

Wi-Fi

Dirección IP	Dirección IP del dispositivo
WiFi MAC	Dirección MAC WiFi

Móvil

Estado	Estado (tarjeta SIM instalada)
Número de teléfono	Número de teléfono
Itinerancia (Voz / Datos)	Itinerancia de voz/datos
Estado de itinerancia	Estado actual de la itinerancia
Dirección IP	Dirección IP
Operador/Transportista	Operador/Transportista
Tecnología celular	Tecnología celular
IMEI	Número IMEI
ICCID	Es el identificador de la tarjeta SIM, a menudo también tarjeta inteligente o tarjeta de circuito integrado (ICC).
IMSI	La Identidad Internacional de Abonado Móvil (IMSI) proporciona en las redes móviles GSM y UMTS una identificación definitiva de los usuarios de la red La IMSI se compone de un máximo de 15 dígitos y se configura de la siguiente manera: • Código de país del móvil (MCC), 3 dígitos • Código de red móvil (MNC), 2 ó 3 dígitos • Número de identificación de abonado móvil (MSIN), de 1 a 10 dígitos
MCC/MNC actual	Ver "SIM MCC/MNC"
SIM MCC/MNC	El Código de país móvil es un identificador de país establecido, fijado por la UIT según la Norma E.212. Funciona junto con el Código de Red Móvil (MNC) para la identificación de la red móvil. Significa el código de país/red móvil de la tarjeta SIM. Si te desplazas a otra red móvil, lógicamente, el "MCC/MNC actual" y el "MCC/MNC de la SIM" serán diferentes.

Bluetooth

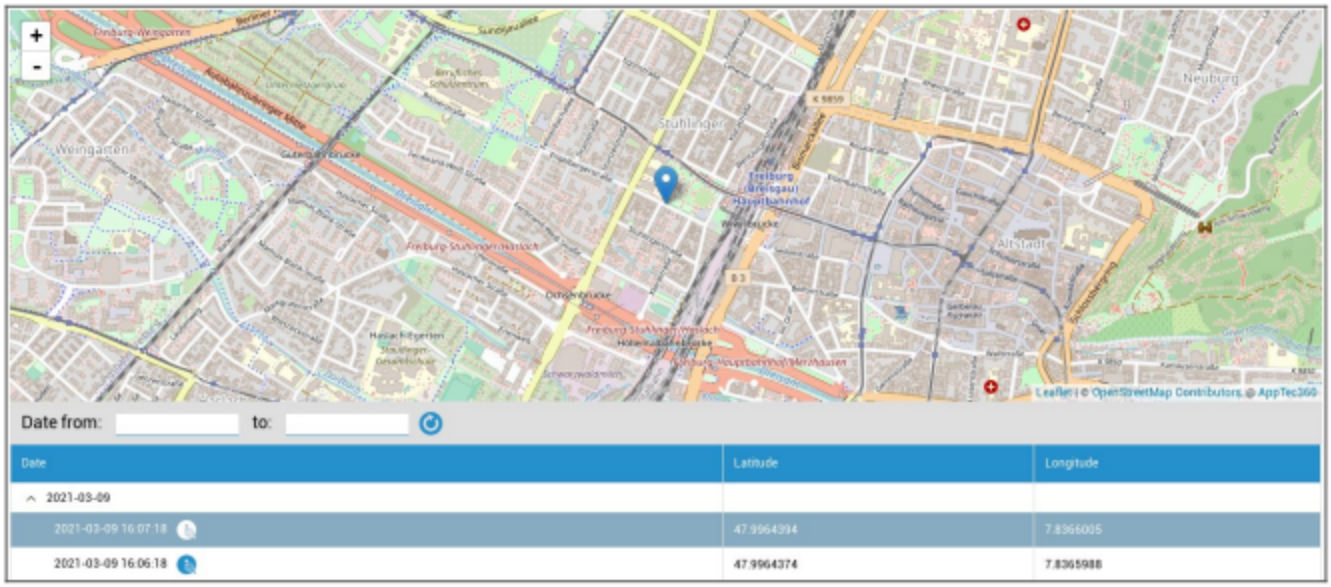
Bluetooth MAC	Dirección MAC Bluetooth

Gestión de la seguridad

Antirrobo (sólo en el dispositivo)

Información GPS (sólo a nivel de dispositivo)

Aquí puede establecer la ubicación actual/última del dispositivo. La localización puede protegerse con una o incluso dos contraseñas - Ver: Ajustes Generales - Privacidad - Acceso GPS



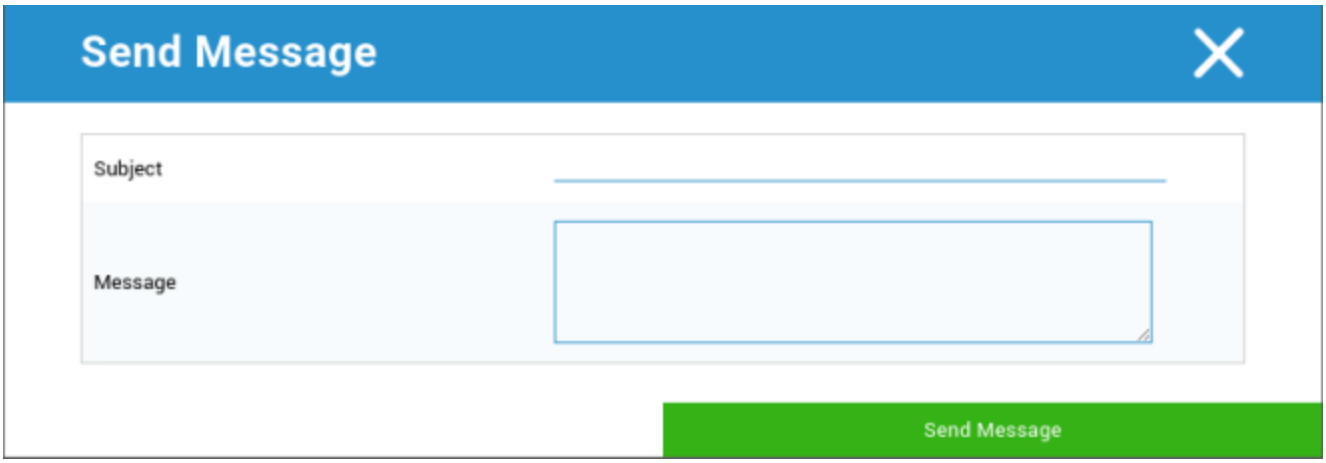
Limpiar y bloquear (sólo a nivel de dispositivo)

En "Limpiar y bloquear", puedes realizar las tres acciones siguientes:

Limpieza total	El dispositivo se restaura a sus ajustes de fábrica (se borran tanto los datos corporativos como los personales). Sólo funciona para el Perfil de Trabajo Mejorado
Limpieza de empresas	Sólo se eliminan los datos corporativos del dispositivo del usuario final (todas las aplicaciones, datos, etc. que fueron proporcionados por AppTec)
Pantalla de bloqueo	El bloqueo de pantalla está activado, basta con desbloquear el dispositivo con la contraseña/PIN del dispositivo

Mensaje (sólo a nivel de dispositivo)

Aquí puede rellenar el asunto y un mensaje y enviarlo a un dispositivo de usuario final



Configuración de seguridad

Código del dispositivo

En "Código de acceso" puede asignar una contraseña al dispositivo, con las siguientes opciones de configuración

Longitud mínima de la contraseña	Establece, el número mínimo de símbolos que debe tener una contraseña	
Calidad de la contraseña	Sin especificar	Esta política no tiene requisitos para la contraseña.
	Biometría Débil	Esta política permite tecnologías de reconocimiento biométrico de baja seguridad. Esto implica tecnologías que pueden reconocer la identidad de un individuo hasta aproximadamente un PIN de 3 dígitos (la detección falsa es inferior a 1 entre 1.000).
	Algo	Esta política requiere que se establezca algún tipo de contraseña o patrón, pero no impone ninguna regla específica.
	Alfabético	El usuario debe haber introducido una contraseña que contenga al menos caracteres alfabéticos (u otros símbolos).
	Alfanumérico	El usuario debe haber introducido una contraseña que contenga, al menos, caracteres numéricos y alfabéticos (u otros símbolos).
	Complejo	El usuario debe haber introducido una contraseña que contenga al menos una letra, un dígito numérico y un símbolo especial, por defecto. Con esta calidad de contraseña, se puede restringir que las contraseñas contengan varios conjuntos de caracteres, como al menos una letra mayúscula, etc.
Longitud mínima de la contraseña	Establece el número de caracteres necesarios para la contraseña. Por ejemplo, puedes exigir que el PIN o las contraseñas tengan al menos seis caracteres.	
Dígitos numéricos mínimos requeridos en la contraseña	Dígitos numéricos mínimos requeridos en la contraseña	
Mínimo de letras minúsculas	Mínimo de letras minúsculas requeridas en la contraseña	

requeridas en la contraseña	
Mínimo de letras mayúsculas requeridas en la contraseña	Mínimo de letras mayúsculas requeridas en la contraseña
Mínimo de caracteres no alfabéticos requeridos en la contraseña	Mínimo de caracteres no alfabéticos requeridos en la contraseña
Símbolos mínimos requeridos en la contraseña	Símbolos mínimos requeridos en la contraseña

Bloqueo de tiempo máximo de inactividad	Inactividad máxima del usuario hasta el bloqueo temporal
Tiempo de caducidad de la contraseña	Establece, después de qué intervalo de tiempo la contraseña caduca y se debe emitir una nueva contraseña
Restricción del historial de contraseñas	Número de contraseñas utilizadas anteriormente que no están permitidas
Número máximo de intentos fallidos de contraseña	Establece cuántas veces se puede introducir incorrectamente una contraseña, antes de que se realice un borrado completo del dispositivo.
Permitir autenticación biométrica	Permite la autenticación mediante huella dactilar o escáner de iris. Sólo para Samsung KNOX 2.1 y superior

Código de acceso al contenedor

En "Código de acceso" puedes asignar una contraseña de contenedor, y tienes a tu disposición las siguientes opciones de configuración

Longitud mínima de la contraseña	Establece, el número mínimo de símbolos que debe tener una contraseña	
Calidad de la contraseña	Sin especificar	Esta política no tiene requisitos para la contraseña.
	Biometría Débil	Esta política permite tecnologías de reconocimiento biométrico de baja seguridad. Esto implica tecnologías que pueden reconocer la identidad de un individuo hasta aproximadamente un PIN de 3 dígitos (la detección falsa es inferior a 1 entre 1.000).
	Algo	Esta política requiere que se establezca algún tipo de contraseña o patrón, pero no impone ninguna regla específica.
	Alfabético	El usuario debe haber introducido una contraseña que contenga al menos caracteres alfabéticos (u otros símbolos).
	Alfanumérico	El usuario debe haber introducido una contraseña que contenga, al menos, caracteres numéricos y alfabéticos (u otros símbolos).
	Complejo	El usuario debe haber introducido una contraseña que contenga al menos una letra, un dígito numérico y un símbolo especial, por defecto. Con esta calidad de contraseña, se puede restringir que las contraseñas contengan varios conjuntos de caracteres, como al menos una letra mayúscula, etc.
Longitud mínima de la contraseña	Establece el número de caracteres necesarios para la contraseña. Por ejemplo, puedes exigir que el PIN o las contraseñas tengan al menos seis caracteres.	
Dígitos numéricos mínimos requeridos en la contraseña	Dígitos numéricos mínimos requeridos en la contraseña	
Mínimo de letras minúsculas requeridas en la contraseña	Mínimo de letras minúsculas requeridas en la contraseña	

Mínimo de letras mayúsculas requeridas en la contraseña	Mínimo de letras mayúsculas requeridas en la contraseña
Mínimo de caracteres no alfabéticos requeridos en la contraseña	Mínimo de caracteres no alfabéticos requeridos en la contraseña
Símbolos mínimos requeridos en la contraseña	Símbolos mínimos requeridos en la contraseña

Bloqueo de tiempo máximo de inactividad	Inactividad máxima del usuario hasta el bloqueo temporal
Tiempo de caducidad de la contraseña	Establece, después de qué intervalo de tiempo la contraseña caduca y se debe emitir una nueva contraseña
Restricción del historial de contraseñas	Número de contraseñas utilizadas anteriormente que no están permitidas
Número máximo de intentos fallidos de contraseña	Establece cuántas veces se puede introducir incorrectamente una contraseña, antes de que se realice un borrado completo del dispositivo.

Antivirus

Escaneado automático	Activar escaneos automáticos periódicos
Intervalo de exploración	Intervalo para el examen (Rápido / Completo)
Escaneado automático completo	Activar escaneos automáticos completos
Actualizaciones automáticas	Activar las actualizaciones automáticas
Intervalo de comprobación de actualización	Con qué frecuencia deben actualizarse la aplicación y su base de datos (virus / código dañado)
Protección de aplicaciones	Activar el escaneo automático de apps
Protección de tarjetas SD	Activar el escaneo automático de la tarjeta SD
Actualización sólo Wi-Fi	Si está activada, las actualizaciones sólo se aplicarán cuando el dispositivo se conecte correctamente a una red Wi-Fi

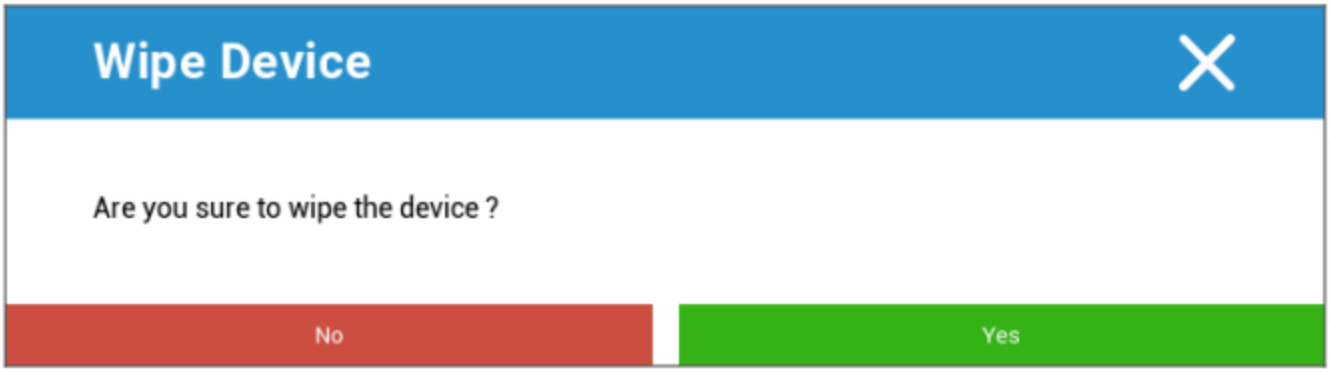
Fin de vida útil (sólo a nivel de dispositivo)

Limpiar (sólo a nivel de dispositivo)

En "Borrar", puede restaurar el dispositivo a sus valores de fábrica (sólo en el perfil de trabajo mejorado).

Aquí se eliminarán tanto los datos corporativos como los privados en el dispositivo del usuario final.

Al hacer clic en el "Símbolo de menos" recibirá el siguiente mensaje:



Con "Sí" puede realizar el borrado.

En "Informe de limpieza" se pueden visualizar los siguientes elementos

Borrado por	Historial de quién realizó la limpieza
Fecha	Fecha
Estado	Estado (por ejemplo, si el borrado se ha realizado correctamente)

Configuración de restricciones

Restricciones

Aquí se pueden restringir y bloquear diversas cosas.

Cumplimiento de la normativa	Modo Preguntar al Usuario - Se pedirá al usuario que realice las acciones necesarias. Modo Bloqueo Contenedor - Oculta todas las apps hasta que se cumplan todos los requisitos
Política de permisos en tiempo de ejecución	Preguntar al usuario para solicitar nuevos permisos Conceder siempre nuevas solicitudes de permiso Deniega siempre las nuevas solicitudes de permiso Advertencia: Algunas Apps tienen problemas para reconocer los permisos si éstos se establecen automáticamente. Si siempre concedes permisos y tienes problemas con apps que dicen que faltan permisos, establece esta opción en "solicitar al usuario" y vuelve a instalar la app
Permitir el portapapeles saliente	Permite copiar y pegar desde dentro del contenedor hacia fuera
Permitir la resolución del identificador de llamadas	Muestra el nombre de una llamada entrante basándose en los contactos del contenedor
Permitir Resolución de Búsqueda de Contactos	Permite buscar nombres en los contactos del contenedor al realizar llamadas
Permitir compartir contactos por Bluetooth	Permite acceder al contacto del contenedor en un coche
No permitir el haz NFC saliente	Desactiva NFC para el Contenedor
Permitir fuentes desconocidas	Si está activada, los usuarios pueden cargar aplicaciones de forma lateral instalando un archivo .apk.
Permitir depuración USB	Si está activada, los usuarios pueden activar la Depuración USB.
No permitir la modificación de la cuenta	Desactiva la creación, eliminación y modificación de Cuentas en el contenedor

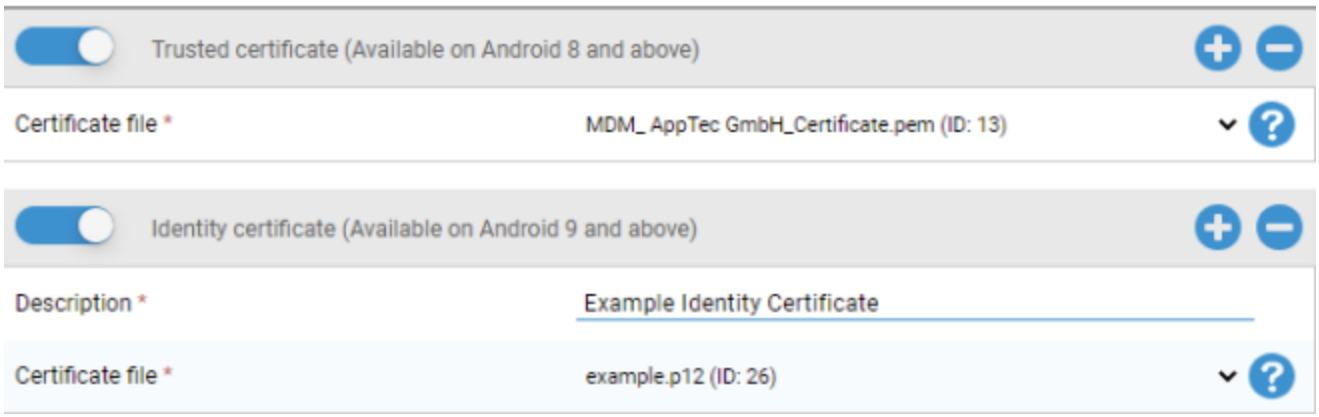
	Ten en cuenta que algunas aplicaciones necesitan crear o modificar cuentas para funcionar como es debido

Restricciones del Perfil de Trabajo. Disponible sólo en dispositivos Android 11 y superiores, con Perfil de trabajo mejorado.	
No permitir cámara	Especifica si la cámara está desautorizada en el perfil de trabajo.
No permitir Bluetooth	Especifica si el bluetooth está desautorizado en el perfil de trabajo.
Activar la protección contra el restablecimiento de fábrica	Actívala para anular la Protección de restablecimiento de fábrica de Android a la cuenta de Google que hayas definido en "Ajustes generales" → "Configuración de Android" → "Android Empresa" → "Protección de restablecimiento de fábrica" Si está activada y restableces el dispositivo, tendrás que proporcionar la cuenta de Google configurada para configurar de nuevo el dispositivo.
Controlar la actualización del SO	Actívala para establecer el comportamiento de actualización en automático, por ventanas o pospuesto.
Política de actualización	Automático: Instalar automáticamente en cuanto haya una actualización disponible. Ventana: Instala automáticamente dentro de una ventana de mantenimiento diaria. Esto también configura las aplicaciones de Play para que se actualicen dentro de la ventana. Se recomienda encarecidamente para los dispositivos de quiosco, ya que es la única forma de que las aplicaciones ancladas persistentemente en primer plano puedan ser actualizadas por Play. Posponer: Pospone la instalación automática hasta un máximo de 30 días.

Restricciones del Perfil Personal. Disponible sólo en dispositivos Android 11 y superiores, con Perfil de trabajo mejorado.	
No permitir cámara	Especifica si la cámara no está permitida en el perfil personal.
No permitir Bluetooth	Especifica si el bluetooth está desautorizado en el perfil personal.
Permitir fuentes desconocidas	Si está activada, los usuarios del perfil de trabajo pueden descargar aplicaciones instalando un archivo .apk.

Gestión de certificados

Aquí puede distribuir certificados de confianza y certificados de identidad a sus dispositivos. Se requiere Android 8 o superior para distribuir Certificados de Confianza y Android 9 o superior para distribuir Certificados de Identidad.



Con el signo "+" puede añadir varios certificados.

Los certificados de confianza deben estar en formato PEM.

Los certificados de identidad deben estar en formato PKCS12.

Gestión de conexiones

Wifi

Para esta configuración, realiza la preconfiguración de los dispositivos de usuario final, para el acceso a los Puntos de Acceso internos

Identificador del Conjunto de Servicios (SSID)	SSID de la red que se va a conectar
Red oculta	Activar, en caso de que el AP no emita el SSID

Tipo de seguridad

Establecer el tipo de seguridad del AP

WEP

Contraseña	Contraseña para el PA

WPA/WPA2

Contraseña	Contraseña para el PA

802.1x EAP

Método EAP

PWD	Identidad	Identidad
	Contraseña	Contraseña

PEAP	Protocolo de autenticación de fase 2	ninguno	Sin protocolo adicional
		MSCHAPV2	Protocolo MSCHAPV2
		GTC	Protocolo GTC
	Certificado CA	Certificado CA	
	Identidad	Identidad	
	Identidad anónima	Identidad anónima	
	Contraseña	Contraseña	

TTLS	Protocolo de autenticación de fase 2	ninguno	Sin protocolo adicional
		PAP	Protocolo PAP
		MSCHAP	Protocolo MSCHAP
		MSCHAPV2	Protocolo MSCHAPV2
		GTC	Protocolo GTC
	Certificado CA	Certificado CA	
	Identidad	Identidad	
	Identidad anónima	Identidad anónima	
	Contraseña	Contraseña	

TLS	Certificado CA	Certificado CA
	Identidad	Identidad
	Contraseña	Contraseña

VPN

Nombre de la conexión	Nombre de la conexión VPN

Tipo de VPN

VPN

Cliente VPN

Cliente VPN AppTec	
Configuración de la puerta de enlace	Selecciona la Configuración VPN de la **Pasarela**(Ver **Configuración General > Pasarela Universal > Configuración VPN**)
VPN siempre activa	Activar Bloqueo Nativo
Activar AppTec Lockdown	Activar AppTec Lockdown

Integrado (sólo disponible en dispositivos Samsung)			
Tipo de conexión	PPTP	Servidor	Servidor
		Activar el cifrado PPTP	Activar el cifrado PPTP
	L2TP / IPSec PSK	Servidor	Servidor
		Clave precompartida IPSec	Clave precompartida IPSec
		Activar Secreto L2TP	Activar Secreto L2TP
		Secreto L2TP	Secreto L2TP
	IPSec XAuth PSK	Servidor	Servidor
		Identificador IPSec	Identificador IPSec
		Clave precompartida IPSec	Clave precompartida IPSec
Búsqueda DNS Dominios	Búsqueda DNS Dominios		
Ajustes expertos	Servidores DNS	Servidores DNS	
	Rutas de reenvío	Rutas de reenvío	

VPN abierta		
Servidor	Servidor	
Perfil OpenVPN	Perfil OpenVPN	
Aplicación OpenVPN	OpenVPN para Android (recomendado)	
	Conexión OpenVPN	
Ajustes expertos	Servidores DNS	Servidores DNS
	Rutas de reenvío	Rutas de reenvío

Samsung / Cisne fuerte			
Tipo de conexión	PPTP	Servidor	Servidor
		Nombre de usuario	Nombre de usuario
		Contraseña	Contraseña
		Activar el cifrado PPTP	Activar el cifrado PPTP
	L2TP / IPSec PSK	Servidor	Servidor
		Clave precompartida IPSec	Clave precompartida IPSec
		Nombre de usuario	Nombre de usuario
		Contraseña	Contraseña
		Activar Secreto L2TP	Secreto L2TP
	IPSec XAuth PSK	Servidor	Servidor
		Identificador IPSec	Identificador IPSec
		Clave precompartida IPSec	Clave precompartida IPSec
		Nombre de usuario	Nombre de usuario
		Contraseña	Contraseña
Ajustes expertos	Servidores DNS	Servidores DNS	
	Rutas de reenvío	Rutas de reenvío	

Cisco Any Connect		
Servidor	Servidor	
Modo Certificado	Discapacitados	Discapacitados
	Automático	Automático
Ajustes expertos	Servidores DNS	Servidores DNS
	Rutas de reenvío	Rutas de reenvío

VPN por aplicación

Cliente VPN

Cliente VPN AppTec		
Configuración de la puerta de enlace	Selecciona la Configuración VPN de la **Pasarela**(Ver **Configuración General > Pasarela Universal > Configuración VPN**)	
Aplicaciones VPN	Aplicaciones VPN	
VPN siempre activa	Activar Bloqueo Nativo	VPN siempre activa
Activar AppTec Lockdown	Activar AppTec Lockdown	

Samsung / Cisne fuerte			
Tipo de conexión	PPTP	Servidor	Servidor
		Aplicaciones VPN	Aplicaciones VPN
		Nombre de usuario	Nombre de usuario
		Contraseña	Contraseña
		Activar el cifrado PPTP	Activar el cifrado PPTP
	L2TP / IPSec PSK	Servidor	Servidor
		Aplicaciones VPN	Aplicaciones VPN
		Clave precompartida IPSec	Clave precompartida IPSec
		Nombre de usuario	Nombre de usuario
		Contraseña	Contraseña
		Activar Secreto L2TP	Secreto L2TP
	IPSec XAuth PSK	Servidor	Servidor
		Aplicaciones VPN	Aplicaciones VPN
		Identificador IPSec	Identificador IPSec
		Clave precompartida IPSec	Clave precompartida IPSec
		Nombre de usuario	Nombre de usuario
		Contraseña	Contraseña
Ajustes expertos	Servidores DNS	Servidores DNS	
	Rutas de reenvío	Rutas de reenvío	

Restricciones

Aquí puede establecer las restricciones, en relación con la gestión de la conexión

Permitir itinerancia de datos	Permitir datos móviles en itinerancia
Forzar itinerancia de datos	Si se activa, la itinerancia para datos móviles se activa permanentemente (¡no se recomienda!) Este ajuste sobrescribe el ajuste "Permitir itinerancia de datos".
Utilizar el servidor proxy http del sistema	El uso de un servidor proxy HTTP, que se proporciona mediante la configuración del sistema en ajustes, depende de la red conectada (WiFi o APN).

Gestión PIM

Intercambio de Gmail

Información: Esta Configuración se aplicará a la aplicación de Gmail. Así que tienes que aprobar e instalar Gmail.

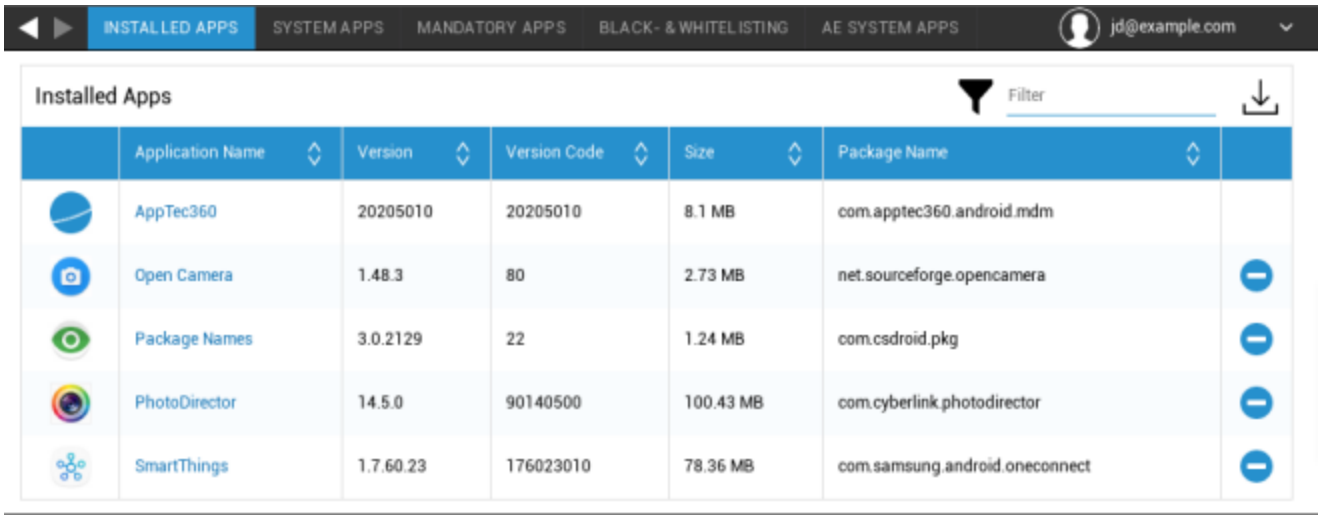
Dirección de correo electrónico	La dirección de correo electrónico del usuario facilitada Ten en cuenta los "Marcadores de posición", que puedes utilizar para trabajar con credenciales y no realizar cambios manualmente en cada dispositivo Con un clic puedes visualizarlos tú mismo
Nombre de host del servidor	Dirección del servidor de tus servidores Exchange
Nombre de usuario	El nombre de inicio de sesión para el dispositivo del usuario final correspondiente, ten en cuenta también los "Marcadores de posición aquí".
Firma	Se puede adjuntar una firma (Sugerencia: Algunos dispositivos requieren formato HTML para la firma)
Número de días anteriores a sincronizar	Número de días, que determina cuándo se sincronizan de nuevo los correos electrónicos
Identificador del dispositivo	Es una cadena que contiene el EAS DeviceID. Forma parte de los protocolos EAS y sólo está permitida en algunos países.
Utiliza la Capa de Conexión Segura (SSL)	Utilizar una conexión SSL
Acepta todos los certificados	Se aceptan todos los certificados. Selecciona esta opción si tu Exchange Server utiliza un certificado autofirmado
Permitir cuentas no gestionadas	Permitir a los usuarios añadir o eliminar cualquier cuenta de Exchange, distinta de la cuenta especificada en esta configuración gestionada. Si esta configuración está activada, no puedes impedir que los usuarios añadan otras cuentas Exchange a Gmail. Tampoco puedes controlar el intercambio de datos entre otras aplicaciones y las cuentas de Exchange añadidas por los usuarios. Esta configuración sólo debe activarse si tus usuarios necesitan mantener más de una cuenta Exchange de trabajo en Gmail.
Certificado de cliente	Certificado de cliente. Sólo es necesario si tu Servidor de Correo espera que esté presente.

Gestión de aplicaciones

Enterprise App Manager

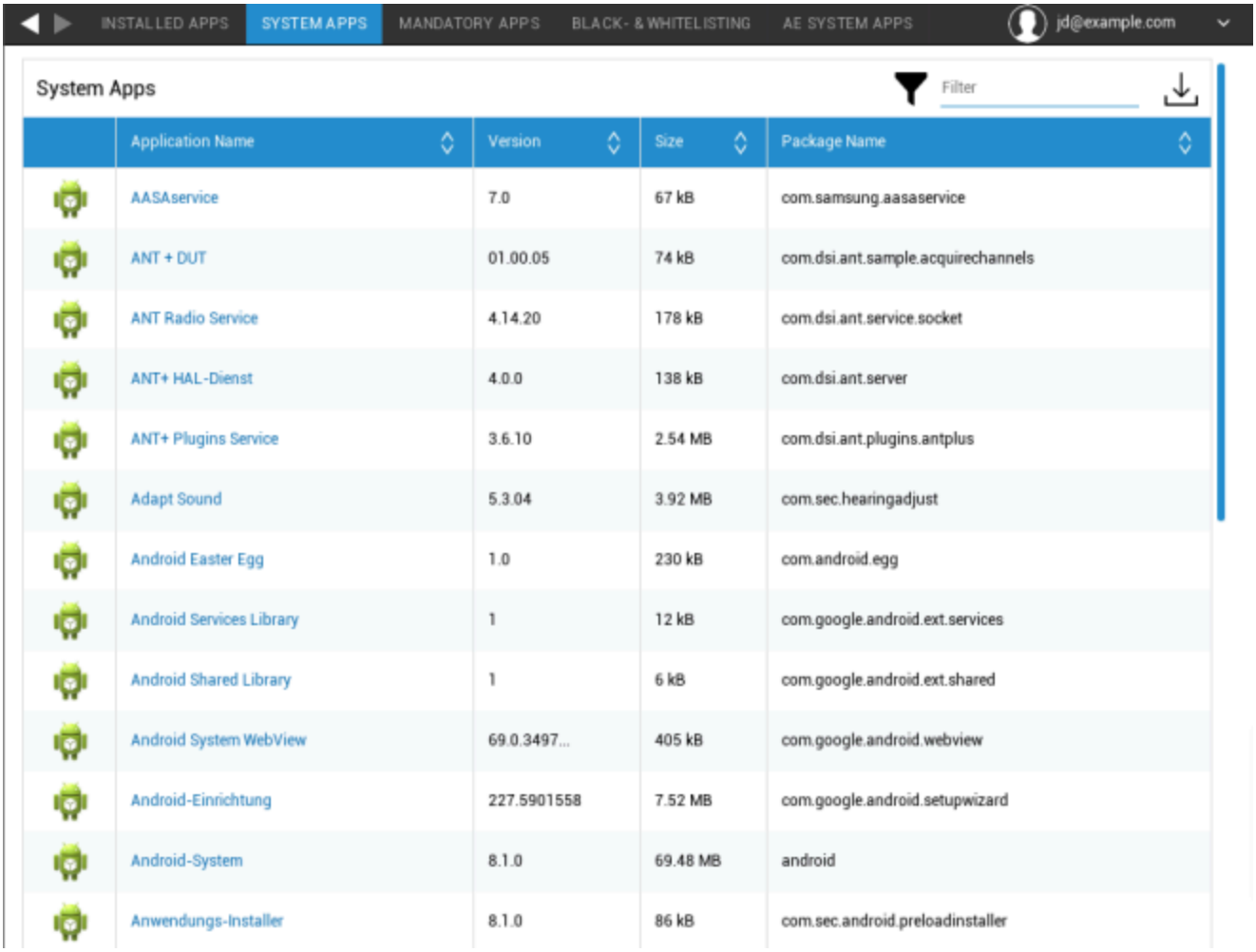
Aplicaciones instaladas (sólo en el dispositivo)

Aquí se mostrarán todas las aplicaciones instaladas actualmente en el contenedor.



Aplicaciones del sistema (sólo a nivel de dispositivo)

En "Aplicaciones del sistema", aparecerán todas las aplicaciones y servicios que el fabricante del dispositivo ya ha instalado en el dispositivo del usuario final.



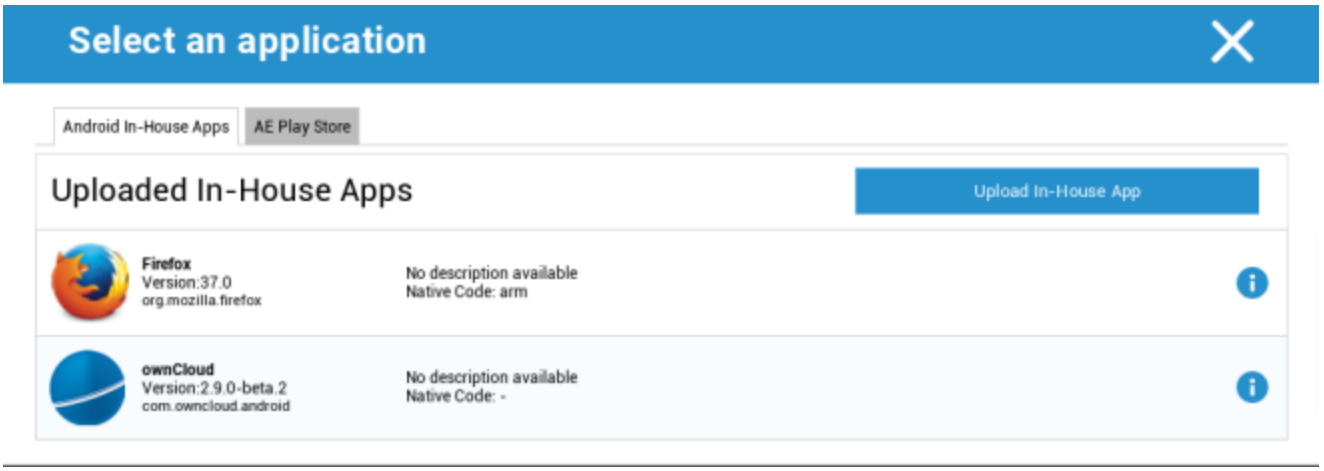
Application Name	Version	Size	Package Name
AASAservice	7.0	67 kB	com.samsung.aasaservice
ANT + DUT	01.00.05	74 kB	com.dsi.ant.sample.acquirechannels
ANT Radio Service	4.14.20	178 kB	com.dsi.ant.service.socket
ANT+ HAL-Dienst	4.0.0	138 kB	com.dsi.ant.server
ANT+ Plugins Service	3.6.10	2.54 MB	com.dsi.ant.plugins.antplus
Adapt Sound	5.3.04	3.92 MB	com.sec.hearingadjust
Android Easter Egg	1.0	230 kB	com.android.egg
Android Services Library	1	12 kB	com.google.android.ext.services
Android Shared Library	1	6 kB	com.google.android.ext.shared
Android System WebView	69.0.3497...	405 kB	com.google.android.webview
Android-Einrichtung	227.5901558	7.52 MB	com.google.android.setupwizard
Android-System	8.1.0	69.48 MB	android
Anwendungs-Installer	8.1.0	86 kB	com.sec.android.preloadinstaller

Aplicaciones obligatorias

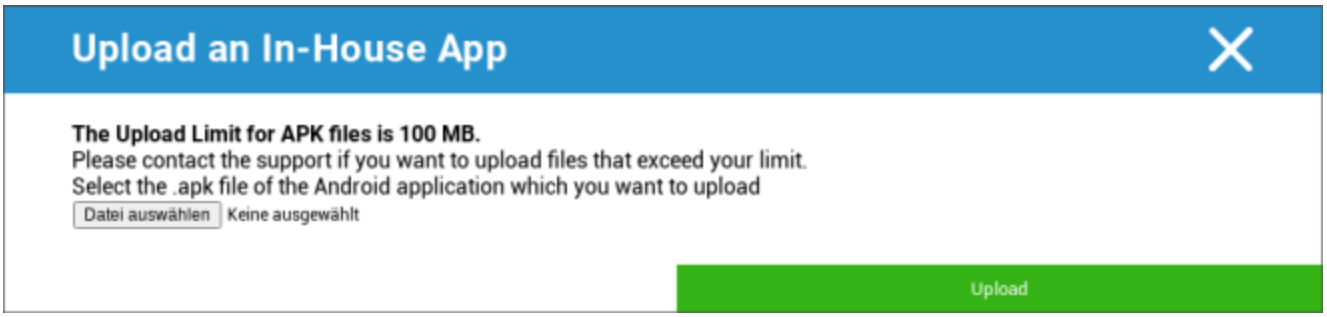
En Aplicaciones obligatorias, puede establecer las aplicaciones obligatorias requeridas. Se pedirá continuamente al usuario que instale esta aplicación designada, si se trata de una InHouse App. Las aplicaciones de Play Store se instalarán automáticamente.

A través del , se puede definir la aplicación obligatoria requerida.

Puede ser una In-House App de las "Android In-House Apps", que has cargado en Ajustes Generales.

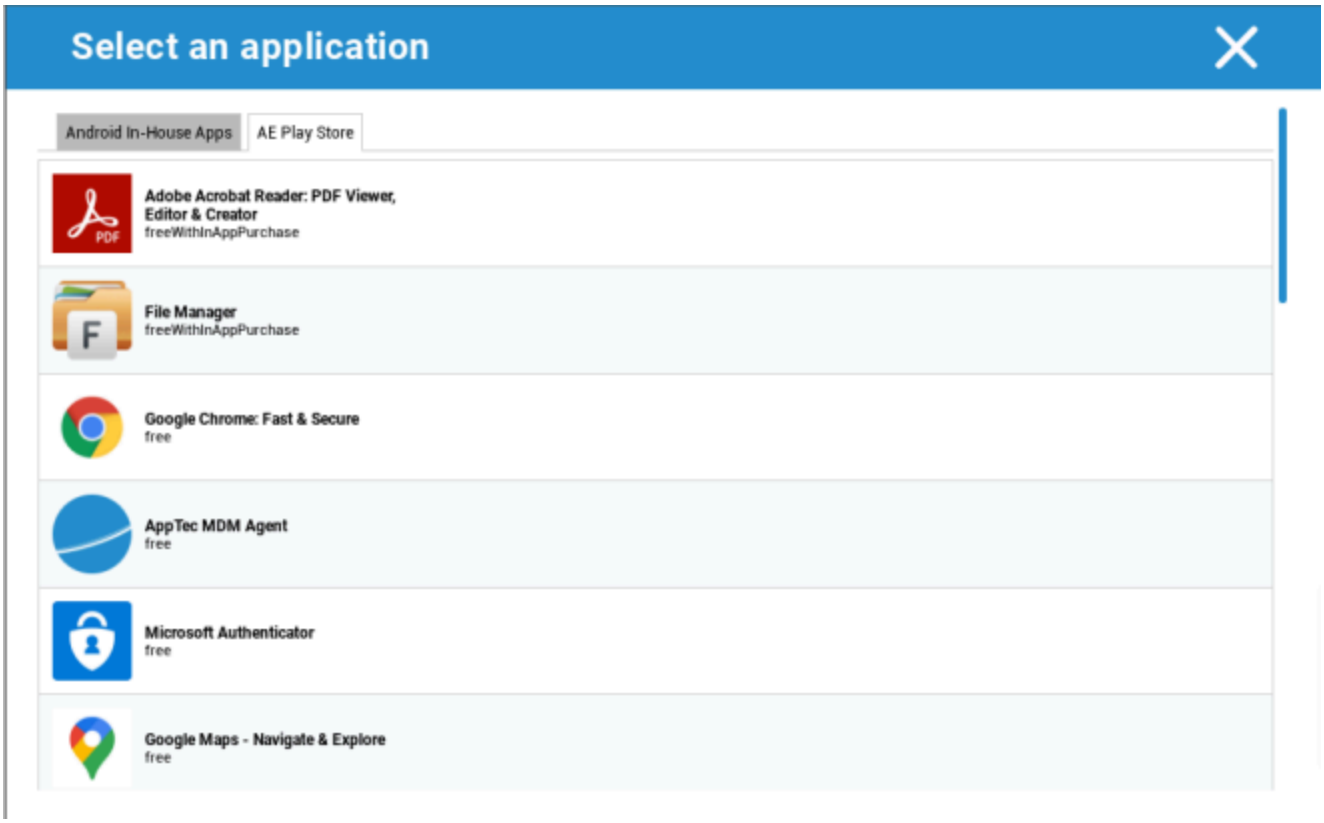


También puede seleccionar y cargar directamente un archivo apk con "Cargar aplicación interna".



Si está instalando una aplicación interna, tendrá la posibilidad de activar "Mantener al día". Si está activada y ha definido una versión más reciente en la base de datos de aplicaciones internas, la aplicación se actualizará en el dispositivo.

O puede ser una aplicación "AE Play Store" de Google Work Play Store.



En esta pestaña sólo se mostrarán las "AE Play Store Apps" aprobadas.

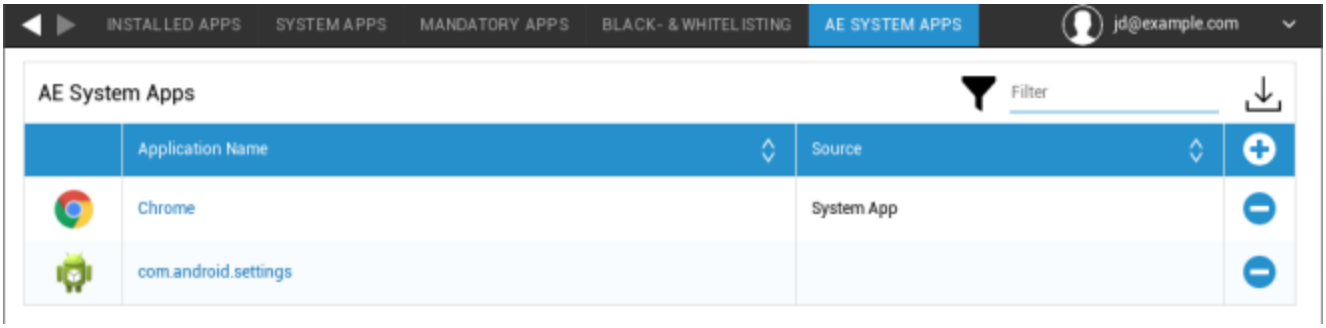
Para aprobar una "AE Play Store App" por favor vaya a "Ajustes Generales" > "Gestión de Apps" > "AE Play

Store" y añade una aplicación a través del botón que te redirigirá a la pestaña "Play Store Apps" (o puedes ir directamente a la pestaña "Play Store Apps").

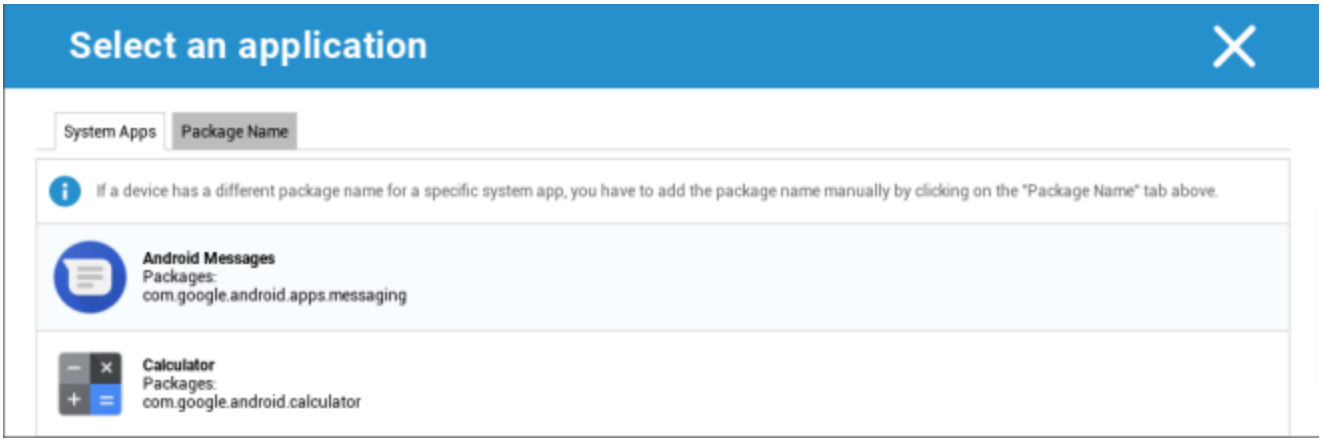
En la pestaña "Play Store Apps" puedes buscar aplicaciones. Al hacer clic en una aplicación, se abre la página de la aplicación y aquí puede aprobar la aplicación haciendo clic en "Aprobar".

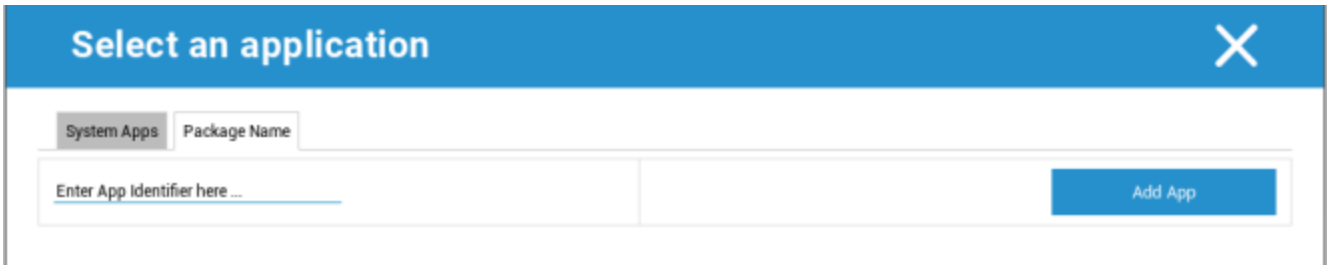
Aplicaciones del sistema AE

Aquí puede definir una lista que contenga aplicaciones específicas del sistema que deban activarse en los dispositivos.



Si hace clic en el botón, puede elegir entre una lista de posibles aplicaciones del sistema proporcionada por Google o introducir directamente el nombre del paquete de una aplicación del sistema que deba activarse.





Ten en cuenta que las aplicaciones de sistema de la lista proporcionada por Google son sólo aplicaciones que pueden ser aplicaciones de sistema, pero no tienen por qué ser necesariamente aplicaciones de sistema en tus dispositivos.

Sin embargo, esta lista sólo afecta a las aplicaciones que ya están preinstaladas.

La adición de aplicaciones que no estén preinstaladas en tus dispositivos no afectará a los mismos, independientemente de si la aplicación procede de la lista proporcionada por Google o de si se introduce directamente el nombre del paquete de la aplicación.

Restricciones y ajustes

Configuración de App Management

Aquí puedes configurar el comportamiento del dispositivo con respecto a las actualizaciones de aplicaciones.

Actualizar frecuencia de comprobación	Especifica en qué intervalo el Cliente AppTec buscará actualizaciones de aplicaciones. El valor por defecto es 24 horas.
Umbral Wi-Fi	Las aplicaciones que superen el tamaño especificado se descargarán a través de Wi-Fi. Si se selecciona "Sólo Wi-Fi", todas las apps se descargarán a través de Wi-Fi.

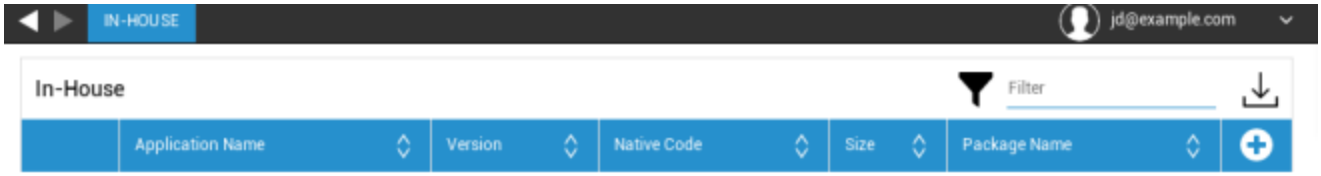
App Store para empresas

En la empresa

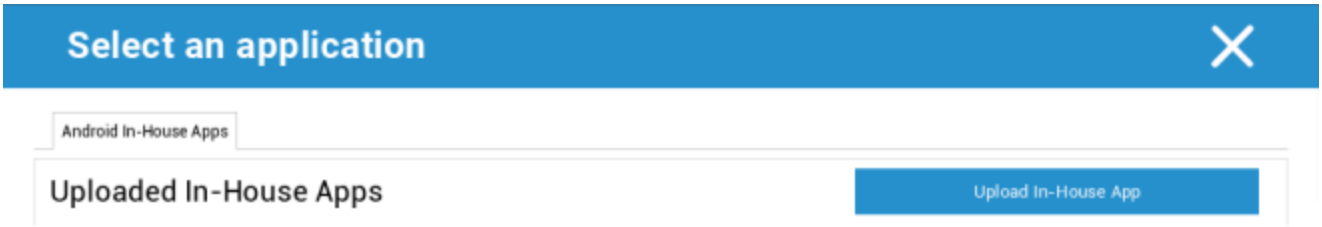
En el punto "In-House", puede cargar y distribuir aplicaciones desarrolladas internamente.

Con el símbolo, puede distribuir In-House Apps adicionales.

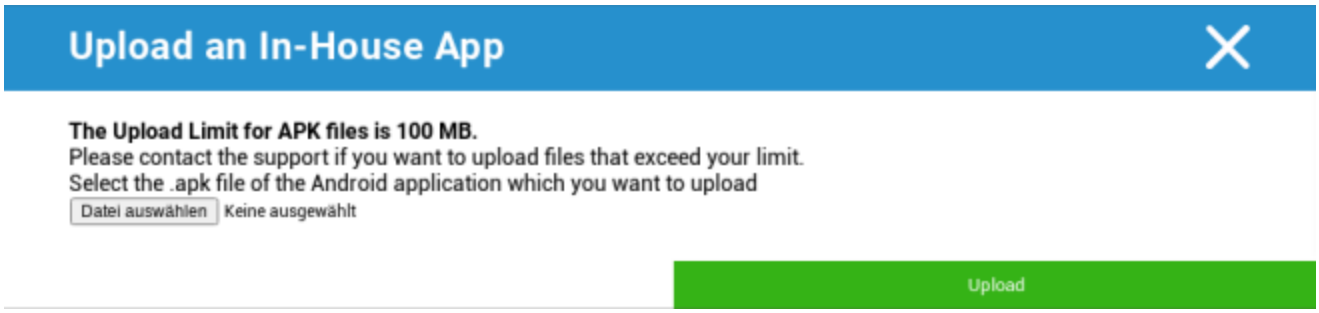
Si está instalando una aplicación interna, tendrá la posibilidad de activar "Mantener al día". Si está activada y ha definido una versión más reciente en la base de datos de aplicaciones internas, la aplicación se actualizará en el dispositivo.



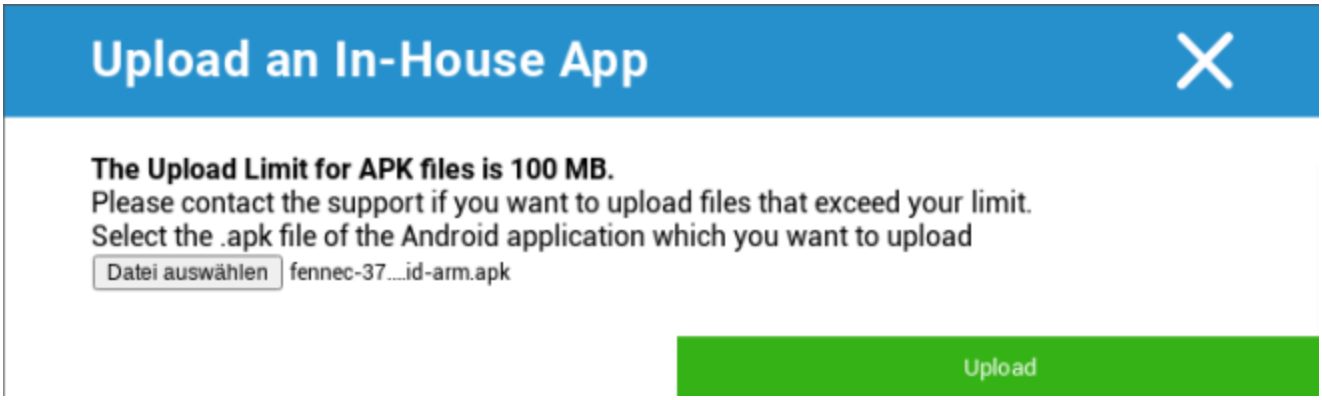
Si no ha distribuido In-House Apps, recibirá el siguiente resumen:



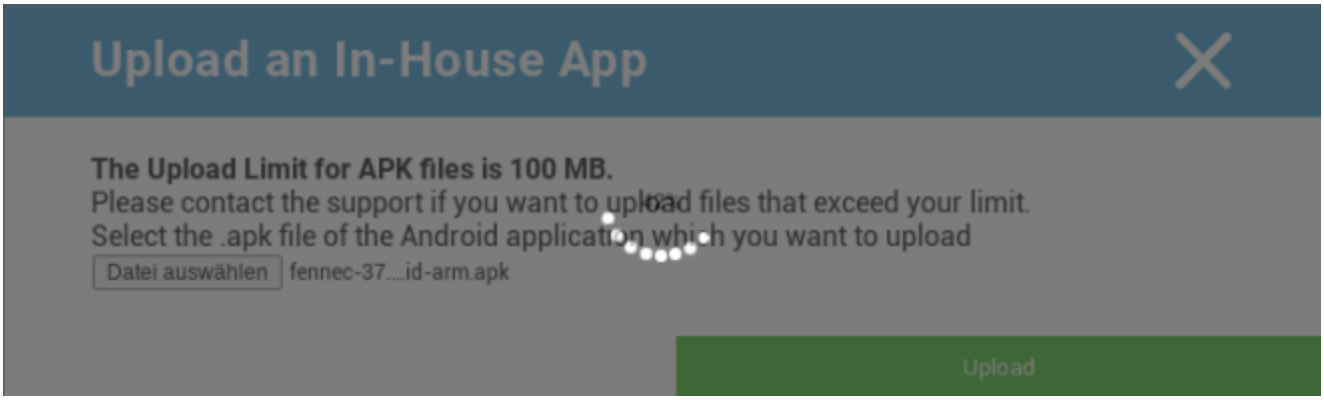
Para ello, haga clic en "Cargar aplicación interna" y obtendrá el siguiente resumen:



Ahora, elige con "Buscar... "un archivo .apk y haz clic en "Cargar".



Tu aplicación se cargará ahora, en el centro del círculo verás un indicador de porcentaje, que muestra la cantidad de tu aplicación que ya se ha cargado.



Si la carga de su aplicación interna se ha realizado correctamente, podrá encontrar la aplicación cargada en su catálogo de aplicaciones.

El usuario tiene ahora la opción de ver e instalar esta aplicación en la AppTec Store en el dispositivo del usuario final, en la categoría "In-House".

Dado que no se trata de una aplicación de Google PlayStore, el usuario no necesita un ID de Google almacenado en su dispositivo.

Play Store para empresas

AE Play Store

Aquí puede añadir aplicaciones a la Play Store de Android Enterprise. Tenga en cuenta que debe aprobar las aplicaciones con su cuenta de administrador AE antes de poder añadirlas.

Para aprobar una aplicación, consulte las instrucciones en Aplicaciones obligatorias.

Gestión de contenidos

ContentBox

Aquí puede activar el ContentBox.

En cuanto active la opción "Activar ContentBox", se instalará automáticamente una aplicación ContentBox independiente en el dispositivo del usuario final.

Navegador seguro

Aquí puede configurar los ajustes del AppTec Secure Browser.

En cuanto cambie la sección de "Navegador seguro" a "Activado", se instalará automáticamente una aplicación de navegador independiente en el dispositivo del usuario final.

Requerir contraseña	Exige al usuario que establezca y utilice una contraseña para acceder al navegador.
Longitud mínima requerida de la contraseña	Establece el número de caracteres necesarios para la contraseña
Calidad de contraseña requerida	Establece la calidad de la contraseña requerida
Restringir descargas / Abrir en	
Restringir subidas	
Cargar lista blanca	Una lista de URLs para las que siempre se permitirá la subida.
Permitir copia	Permite copiar, cortar o compartir texto dentro de las páginas web.
Permitir Captura de Pantalla	Permite hacer capturas de pantalla.
Frecuencia de limpieza de datos	Selecciona con qué frecuencia deben eliminarse automáticamente TODOS los datos del usuario (historial, caché, etc.).
Marcadores de empresa	Los marcadores aparecerán en la carpeta "Marcadores de empresa" de los marcadores del navegador. No son editables por el usuario.
Ocultar barra de direcciones	
Listas blancas en el navegador (sin Universal Gateway)	Activa la lista blanca de URL del cliente. • Los marcadores de empresa siempre están en la lista blanca • Sólo se admiten 100 URL • Utiliza la pasarela universal para crear listas negras y blancas ilimitadas
URLs en lista blanca	Una lista de URL permitidas.

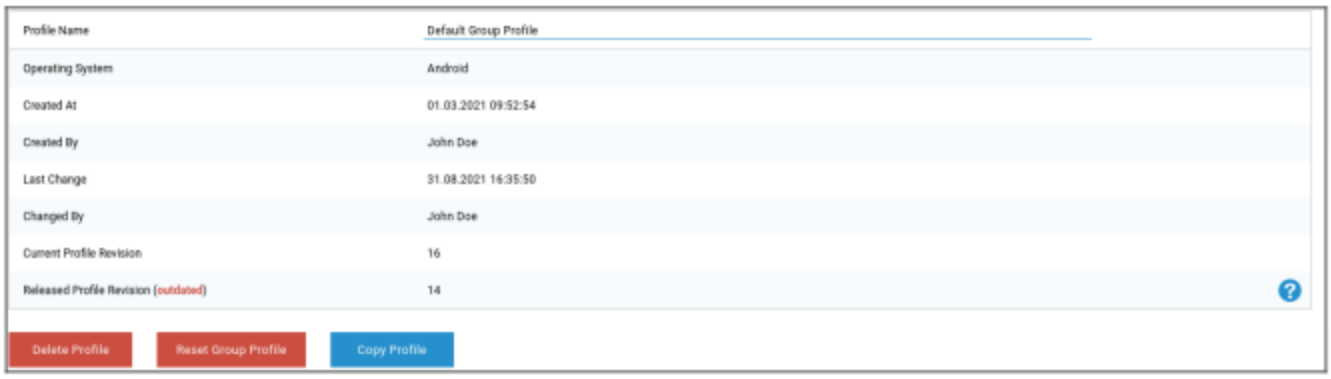
Listas negras y blancas basadas en la puerta de enlace	Las listas negras tienen los siguientes requisitos: • Una pasarela universal AppTec en funcionamiento ("Configuración general" → "Pasarela universal") • Una configuración VPN operativa con un servidor DNS especificado ("Configuración general" → "Pasarela universal" → "Configuración VPN") • Una configuración de Lista Negra ("Configuración General" → "Pasarela Universal" → "Lista Negra de Dominios") • Una conexión VPN válida en el perfil ("Gestión de conexiones" → "VPN")

Configuración de Android

General

Resumen del perfil del grupo (sólo a nivel de grupo)

Al abrir un perfil de grupo, obtendrás una rápida visión general del perfil.



Nombre del perfil	Nombre del perfil (se puede cambiar aquí)
Sistema operativo	Sistema operativo para el que es el perfil
Creado en	Momento de la creación
Creado por	El creador del perfil
Último cambio	Hora de la última modificación del perfil
Cambiado por	Cuenta que realizó los últimos cambios
Revisión actual del perfil	Revisión del estado del perfil guardado
Revisión del perfil liberado	Revisión del perfil asignado ("Asignar ahora"). Si la etiqueta muestra "(obsoleto)" detrás del texto, significa que has guardado el perfil pero aún no lo has asignado, por lo que los dispositivos seguirán recibiendo una versión antigua.

Visión general del dispositivo (sólo a nivel de dispositivo)

Si se encuentra en un dispositivo, recibirá un resumen general del dispositivo seleccionado:

Nombre del dispositivo	Nombre del dispositivo
Última localización conocida	Las últimas coordenadas GPS conocidas
Número de teléfono	Número de teléfono
Apps Obligatorias Asignadas	El número de apps obligatorias asignadas
Versión del SO	Versión del SO del dispositivo
Sistema operativo	Sistema operativo (Android / iOS / Windows Phone)
Número de serie	Número de serie del dispositivo
Propiedad del dispositivo	Dispositivo corporativo o privado
Tipo de dispositivo	Teléfono o tableta
Enraizado	Estado, que indica si el dispositivo ha sido rooteado
Cumple	Cumple las directrices
Dirección IP	Dirección IP
Visto por última vez	Momento en que el dispositivo se conectó por última vez a AppTec
Último empujón	Momento en el que el servidor envió un push al dispositivo
Asignación de usuarios	Un desplegable para asignar el dispositivo a otro usuario

Config Revision (sólo a nivel de dispositivo)

Aquí obtendrá una visión general de qué perfil de grupo está asignado al dispositivo.

Si haces clic en el perfil del grupo, accederás directamente al perfil y podrás realizar ajustes.

Con el símbolo, puedes revertir las aplicaciones asignadas a la configuración del perfil de grupo.

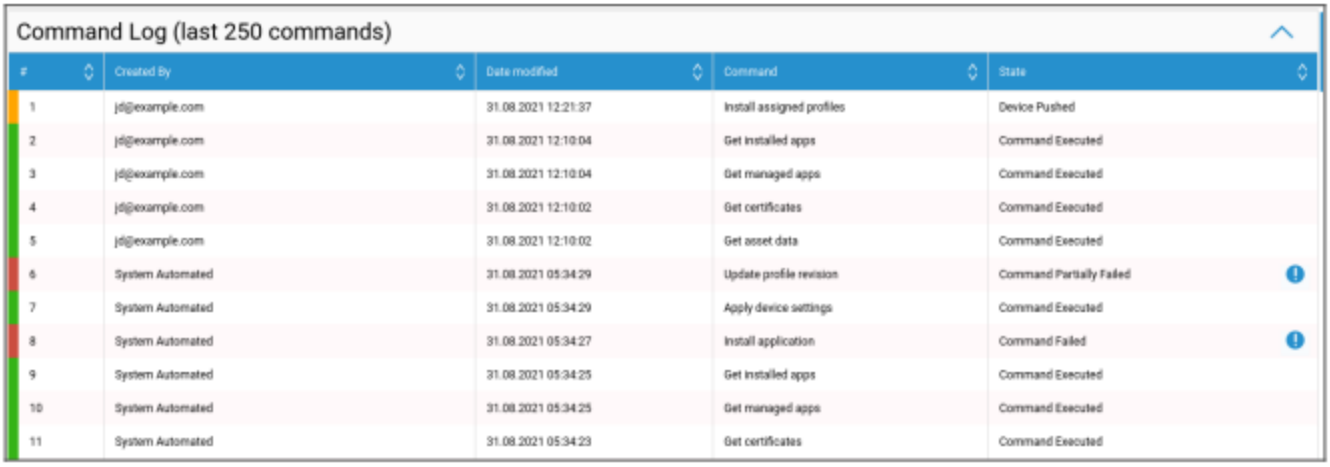
Con el símbolo, puedes restablecer el perfil del dispositivo para que no tenga ninguna configuración.

"Nueva revisión disponible" indica que el perfil de grupo se ha modificado y guardado, pero no se ha asignado. El perfil de grupo debe asignarse con "Asignar ahora" a nivel de grupo para aplicar los cambios a los dispositivos.

Registro de dispositivos (sólo a nivel de dispositivo)

Registro de comandos

Aquí puede ver qué comandos se emitieron para el dispositivo y cuál es su estado.



Los comandos creados por "Sistema automatizado" son creados automáticamente por el sistema.

Posibles estados del comando

Dispositivo Empujado	Se ha enviado una solicitud push al servicio push (por ejemplo, APNS) para indicar al dispositivo que se conecte de nuevo al servidor EMM.
Comando creado	El comando se creó en el sistema.
Orden enviada	El comando se envió al dispositivo después de que se conectara al servidor.
Orden ejecutada	El comando se ha ejecutado correctamente.
Comando fallido	El comando falló. *
Comando parcialmente fallido	Dependiendo del SO del dispositivo, algunos comandos pueden agruparse. En este fallaron algunas partes de este grupo de comandos. *
Orden ejecutada, finalmente fallida	La orden se ejecutó, pero puede que no.
Comando Repulsado	El comando fue repulsado por un usuario.
Descartado	El comando fue descartado. Por ejemplo, porque ha sido sustituido por otro comando o porque el dispositivo se ha reinscrito y se han eliminado los comandos antiguos.

*Si hay un signo de exclamación detrás del mensaje, puedes obtener más información pasando el cursor sobre el icono.

Ajustes del dispositivo

Configuración de clientes

Aquí puedes realizar las siguientes configuraciones en tu dispositivo Android:

Mensaje de advertencia tras desactivar la Gestión de Dispositivos	Mensaje de advertencia establecido tras desactivar la Gestión de Dispositivos
Tiempo de incumplimiento	Límite de tiempo, tras el cual se llevará a cabo la "Acción de aplicación tras el cumplimiento", si el dispositivo no es conforme. Mín. 1 minuto Máx. 24 horas
Acción coercitiva tras el plazo de cumplimiento	La acción que debe emprenderse en cuanto un aparato deje de ser conforme. • no hacer nada = no actuar • Dispositivo de bloqueo = dispositivo de bloqueo • Borrar dispositivo = el dispositivo se restablecerá a los ajustes de fábrica
Frecuencia de recogida de datos	Frecuencia con la que debe recogerse la información del dispositivo/GPS
Frecuencia de latidos del dispositivo	Intervalo en el que el dispositivo debe ponerse en contacto con el Servidor AppTec360 Mín. 1 minuto Máx. 24 horas
Activar actualizaciones de ubicación	Si está activado, el dispositivo envía actualizaciones de ubicación al Servidor AppTec360
Lugar Hora de actualización	Determina en qué intervalos de tiempo el dispositivo envía actualizaciones de ubicación a AppTec
Utiliza la precisión de ubicación de Google para actualizar la ubicación	Si está activada, se utilizará la Precisión de ubicación de Google (antes conocida como ubicación de red) para las actualizaciones de ubicación (si estaba desactivada en "Restricciones", esta configuración no afectará a nada).
Utilizar la localización GPS para actualizar la ubicación	Si está activado, se utilizará el GPS para actualizar la ubicación

Permitir Ubicaciones Simuladas (Falsas)	Permite falsificar la información de localización a través de apps de terceros
Acción de conexión perdida	Te permite establecer una acción determinada que se llevará a cabo tras una cantidad determinada de latidos fallidos
Modo de aplicación de la política	Define la agresividad con la que el Cliente AppTec360 pide al usuario que realice determinadas acciones que requieren la intervención del usuario. Intervalo (Predeterminado) = pregunta en intervalos, para que el usuario pueda dejar esto en segundo plano durante un tiempo. No hay Alerta = no hay ventana emergente para ninguna interacción requerida. Tienes que abrir el Cliente AppTec360 manualmente para comprobar si hay una acción requerida Alerta constante = El usuario sólo puede realizar la acción requerida. El Cliente AppTec360 se forzará a sí mismo en primer plano si el usuario intenta evitarlo
AppTec360 Bloqueo de versión	Te permite definir una versión del Cliente AppTec360 que es la versión máxima a la que se actualiza el cliente.

Papel pintado

Aquí puedes definir un fondo de pantalla personalizado.

"Especificar un color" le permite definir un color en formato hexadecimal (por ejemplo, #000000). Sólo se permiten valores hexadecimales.

"Establecer imagen como fondo de pantalla" te permite cargar una imagen. Tenga en cuenta que los diferentes dispositivos con diferentes lanzadores y versiones del sistema operativo funcionan de manera diferente. No existe una guía general de tamaño y proporción, ya que depende del dispositivo.

Utilice JPG (o JPEG) o PNG como formato de archivo.

Gestión de activos (sólo a nivel de dispositivo)

Gestión de activos

Información del dispositivo

Modelo	**Designación del modelo de aparato**
Sistema operativo	OS
Versión del SO	Versión del SO
Apoyo AE	Soporte para Android Enterprise (contenedor y totalmente gestionado)
Número de serie	Número de serie
Nombre del dispositivo	Nombre del dispositivo
Estado de la batería	Estado de la batería
Memoria Libre / Total	Memoria libre / total
Samsung KNOX	Nivel API Samsung KNOX
Tarjeta SD disponible	Tarjeta SD disponible
Tarjeta SD emulada	Tarjeta SD emulada
Tarjeta SD extraíble	Tarjeta SD extraíble
SD Memoria Libre / Total	SD Libre / Memoria total de la tarjeta SD

Wi-Fi

Dirección IP	Dirección IP del dispositivo
WiFi MAC	Dirección MAC WiFi

Móvil

Estado	Estado (tarjeta SIM instalada)
Número de teléfono	Número de teléfono
Itinerancia (Voz / Datos)	Itinerancia de voz/datos
Estado de itinerancia	Estado actual de la itinerancia
Dirección IP	Dirección IP
Operador/Transportista	Operador/Transportista
Tecnología celular	Tecnología celular
IMEI	Número IMEI
ICCID	Es el identificador de la tarjeta SIM, a menudo también tarjeta inteligente o tarjeta de circuito integrado (ICC).
IMSI	La Identidad Internacional de Abonado Móvil (IMSI) proporciona en las redes móviles GSM y UMTS una identificación definitiva de los usuarios de la red La IMSI se compone de un máximo de 15 dígitos y se configura de la siguiente manera: • Código de país del móvil (MCC), 3 dígitos • Código de red móvil (MNC), 2 ó 3 dígitos • Número de identificación de abonado móvil (MSIN), de 1 a 10 dígitos
MCC/MNC actual	Ver "SIM MCC/MNC"
SIM MCC/MNC	El Código de país móvil es un identificador de país establecido, fijado por la UIT según la Norma E.212. Funciona junto con el Código de Red Móvil (MNC) para la identificación de la red móvil. Significa el código de país/red móvil de la tarjeta SIM. Si te desplazas a otra red móvil, lógicamente, el "MCC/MNC actual" y el "MCC/MNC de la SIM" serán diferentes.

Bluetooth

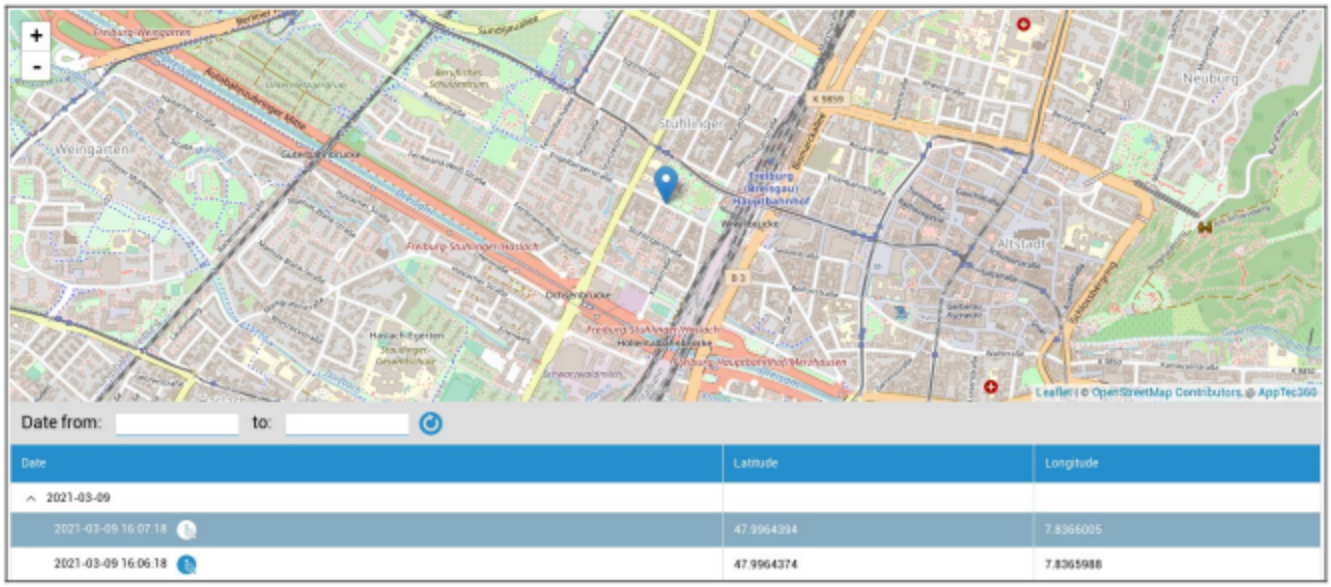
Bluetooth MAC	Dirección MAC Bluetooth

Gestión de la seguridad

Antirrobo (sólo en el dispositivo)

Información GPS (sólo a nivel de dispositivo)

Aquí puede establecer la ubicación actual/última del dispositivo. La localización puede protegerse con una o incluso dos contraseñas - Ver: Ajustes Generales - Privacidad - Acceso GPS



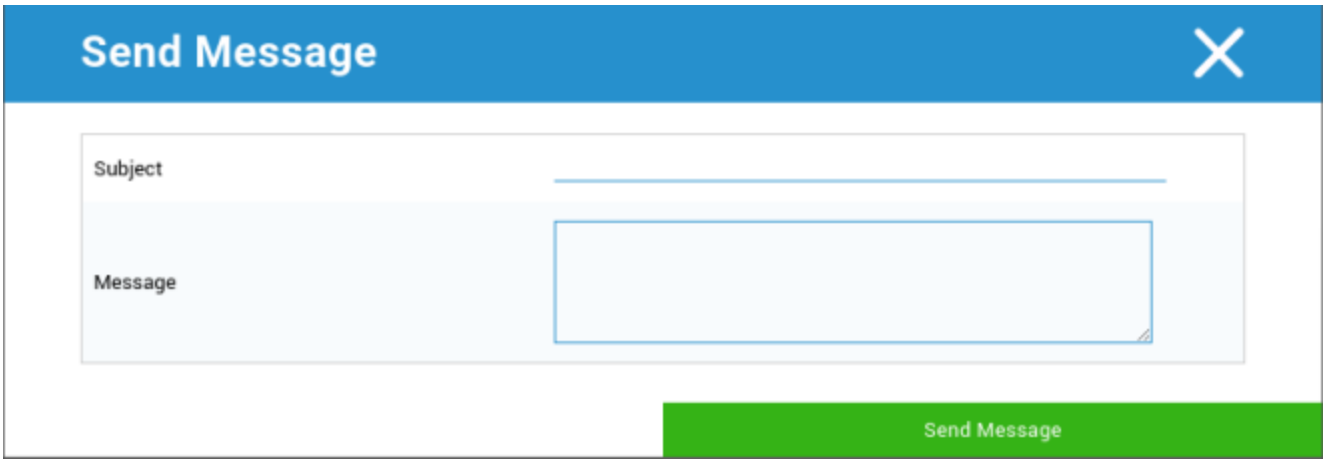
Limpiar y bloquear (sólo a nivel de dispositivo)

En "Limpiar y bloquear", puedes realizar las tres acciones siguientes:

Limpieza total	El dispositivo se restaura a sus valores de fábrica (se borran tanto los datos corporativos como los personales).
Limpieza de empresas	Sólo se eliminan los datos corporativos del dispositivo del usuario final (todas las aplicaciones, datos, etc. que fueron proporcionados por AppTec360)
Pantalla de bloqueo	El bloqueo de pantalla está activado, basta con desbloquear el dispositivo con la contraseña/PIN del dispositivo

Mensaje (sólo a nivel de dispositivo)

Puede rellenar el asunto y un mensaje y enviarlo a un dispositivo de usuario final. Este mensaje se mostrará en el cliente AppTec360.



Configuración de seguridad

Código

En "Código de acceso" puede asignar una contraseña al dispositivo, con las siguientes opciones de configuración

Longitud mínima de la contraseña	Establece, el número mínimo de símbolos que debe tener una contraseña
Calidad de la contraseña	Fuerza de la contraseña No especificado = no especificado Todas las contraseñas están bien = todas las contraseñas son aceptables al menos caracteres numéricos = debe contener al menos caracteres numéricos al menos caracteres complejos = debe contener al menos caracteres especiales al menos caracteres alfanuméricos = debe contener al menos caracteres alfanuméricos al menos caracteres alfabéticos = debe contener al menos caracteres alfabéticos
Bloqueo de tiempo máximo de inactividad	Tiempo máximo de espera de la pantalla. Sólo configura el valor máximo que puede seleccionar el usuario
Mínimo de letras minúsculas requeridas en la contraseña	Mínimo de letras minúsculas requeridas en la contraseña
Mínimo de letras mayúsculas requeridas en la contraseña	Mínimo de letras mayúsculas requeridas en la contraseña
Mínimo de caracteres no alfabéticos requeridos en la contraseña	Mínimo de caracteres no alfabéticos requeridos en la contraseña
Dígitos numéricos mínimos requeridos en la contraseña	Dígitos numéricos mínimos requeridos en la contraseña
Símbolos mínimos requeridos en la contraseña	Símbolos mínimos requeridos en la contraseña
Tiempo de caducidad de la contraseña	Establece, después de qué intervalo de tiempo la contraseña caduca y se debe emitir una nueva contraseña
Restricción del historial de contraseñas	Número de contraseñas utilizadas anteriormente que no están permitidas
Número máximo de intentos fallidos de contraseña	Establece cuántas veces se puede introducir incorrectamente una contraseña, antes de que se realice un borrado completo del dispositivo.

Cifrado

En este punto, usted es capaz de cifrar la memoria interna del dispositivo, así como la memoria de la tarjeta SD.

Exigir encriptación de almacenamiento	Si se activa esta opción, la memoria del dispositivo estará encriptada, siempre que el dispositivo admita esta funcionalidad. Una vez que la memoria del dispositivo ha sido encriptada por primera vez, ya no es posible desencriptarla. Asimismo, la Política de contraseñas se cambiará automáticamente a 6 símbolos alfanuméricos
Requiere encriptación de la tarjeta SD	Este ajuste sólo se aplica a los dispositivos Samsung. Si esta opción está activada, la tarjeta SD externa puede encriptarse y sólo puede desencriptarse manualmente en el dispositivo del usuario final. Asimismo, la Política de contraseñas se cambiará automáticamente a 6 símbolos alfanuméricos

Antivirus

Al activar el Antivirus se instalará Ikarus en los dispositivos. Ten en cuenta que esto requiere una licencia independiente que se puede introducir en Configuración general → Gestión de aplicaciones → Aplicaciones de terceros.

Escaneado automático	Define si Ikarus escanea automáticamente y con qué frecuencia lo hace Si activas "Escaneo Automático Completo" se realizará un escaneo completo. De lo contrario, se realizará un escaneo rápido
Actualizaciones automáticas	Activa las actualizaciones automáticas de la base de datos de virus y establece la frecuencia con la que se realizan
Protección de aplicaciones	Activa el Escaneado de Aplicaciones además del Escaneado normal que sólo escanea Archivos
Protección de tarjetas SD	Activa la Protección de la Tarjeta SD. Sin esto, el escaneo se limita al almacenamiento local
Actualización sólo Wi-Fi	Limita la actualización a Wi-Fi

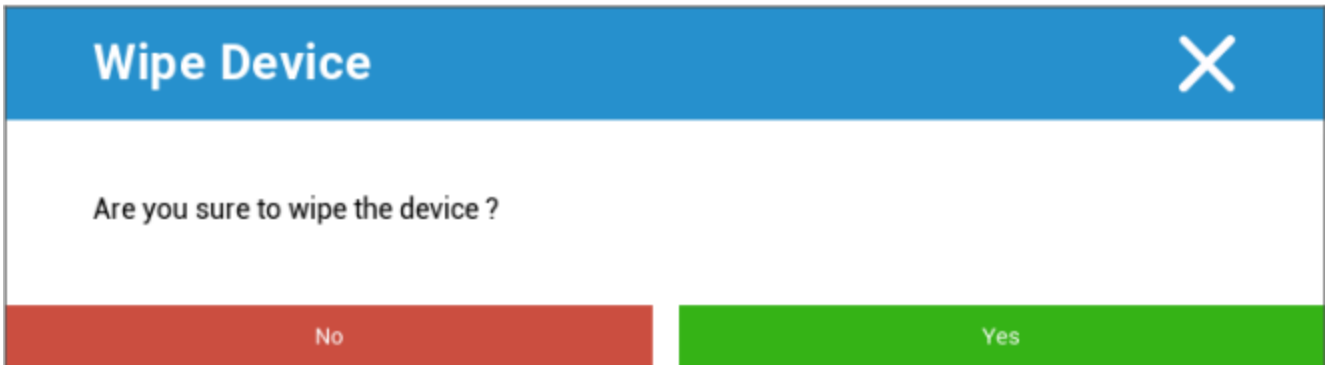
Fin de vida útil (sólo a nivel de dispositivo)

Limpiar (sólo a nivel de dispositivo)

En "Borrar", puedes restaurar el dispositivo a su configuración de fábrica. Aquí se borrarán tanto los datos corporativos como los privados del dispositivo del usuario final.

Al hacer clic en el "Símbolo de menos" debería recibir el siguiente mensaje

¿Borrar también la tarjeta SD?	La memoria de la tarjeta SD también se borrará



Con "Sí" puede realizar el borrado.

En "Informe de limpieza" se pueden visualizar los siguientes elementos

Borrado por	Historial de quién realizó la limpieza
Fecha	Fecha
Estado	Estado (por ejemplo, si el borrado se ha realizado correctamente)

Configuración de restricciones

Restricciones

Aquí se pueden restringir y bloquear diversas cosas.

Activar cámara	Permitir el uso de la cámara
Forzar sincronización automática	Relacionado con la interfaz "Sincronizar Encendido = la sincronización está activada permanentemente Apagado = la sincronización está permanentemente desactivada Elección del usuario = seleccionado por el usuario
Fuerza Bluetooth	Encendido = Bluetooth activado permanentemente Apagado = Bluetooth desactivado permanentemente Elección del usuario = seleccionado por el usuario
Fuerza GPS	Encendido = el GPS está activado permanentemente Apagado = El GPS está permanentemente desactivado Elección del usuario = seleccionado por el usuario
Forzar la precisión de la ubicación de Google	Activado = Localización permanente en Internet Desactivado = Desactivación permanente de la localización por Internet Elección del usuario = seleccionado por el usuario

Para los dispositivos Samsung con la interfaz KNOX 1.0 o superior, están disponibles las siguientes opciones de configuración.

Permitir tarjeta SD	Permitir tarjeta SD
Permitir escritura en tarjeta SD	Permitir "escribir" en la Tarjeta SD
Permitir Captura de Pantalla	Permitir captura de pantalla
Permitir Portapapeles	Permitir portapapeles
Copia de seguridad de la configuración y los datos de la app en Google Cloud	Desactivado = desactivar la copia de seguridad de Google Encendido = activar la copia de seguridad de Google Elección del usuario = seleccionado por el usuario
Permitir depuración USB	Permitir la depuración USB (se utiliza, por ejemplo, para la creación de registros de dispositivos (ADB))
Permitir informe de colisión de Google	Permitir el envío de Google Crash Report desde las apps
Permitir reinicio de fábrica	Permite al usuario restablecer los ajustes de fábrica del dispositivo
Permitir actualización OTA	Permitir actualizaciones "en el aire
Permitir almacenamiento host USB	Si está activada, se puede conectar una memoria USB, en forma de HD o un lector de tarjetas SD
Permitir reproductor multimedia USB (MTP,PTP)	Permitir reproductor multimedia USB (MTP,PTP)
Permitir micrófono	Activado = permitir micrófono para aplicaciones de terceros Desactivado = bloquear el micrófono para aplicaciones de terceros Elección del usuario = los usuarios pueden elegir, si la aplicación de terceros tiene acceso al micrófono
Permitir NFC (Comunicación de Campo Cercano)	Permitir NFC
Permitir fuentes desconocidas (APK Sideloading)	Si está activada, se permite la carga lateral de aplicaciones (archivos APK). Una vez desactivado este ajuste, el usuario tiene que activarlo manualmente cuando vuelvas a permitir la instalación de APKs de fuentes desconocidas.
Permitir la creación de usuarios	Permite la creación de varios usuarios

Propietario del dispositivo AE

(El dispositivo tiene que estar en Modo Propietario de Dispositivo Android Enterprise) Se recomienda crear los dispositivos como dispositivo "Android Enterprise" y no como dispositivo "Android".

Seguridad	
No permitir compartir ubicación	Especifica si un usuario no puede activar el uso compartido de la ubicación.
No permitir el Arranque Seguro	Especifica si no se permite al usuario reiniciar el dispositivo en modo de arranque seguro.
No permitir el reinicio de la red	Especifica si un usuario tiene prohibido restablecer la configuración de red desde Configuración.
No permitir el restablecimiento de fábrica	Especifica si un usuario tiene prohibido reiniciar el dispositivo.
Activar ADB	Permite la Conexión a un PC mediante ADB
Desactivar Keyguard	Desactiva Keyguard
Información de la pantalla de bloqueo del propietario del dispositivo	Establece la información del propietario del dispositivo que se mostrará en la pantalla de bloqueo.
Cumplimiento de la normativa	Modo Preguntar al Usuario - Se pedirá al usuario que realice las acciones necesarias. Modo Bloqueo Contenedor - Oculta todas las apps hasta que se cumplan todos los requisitos

Gestión de aplicaciones	
Permitir la vinculación de aplicaciones entre perfiles	Permite a las aplicaciones del perfil padre gestionar los enlaces web del perfil gestionado.
No permitir el control de aplicaciones	Especifica si a un usuario se le prohíbe modificar aplicaciones en Ajustes o lanzadores.
No permitir la instalación de aplicaciones	Especifica si un usuario tiene prohibido instalar aplicaciones.
No permitir desinstalar aplicaciones	Especifica si un usuario tiene prohibido desinstalar aplicaciones.
Política de permisos en tiempo de ejecución	Especifica cómo se gestionarán las nuevas solicitudes de permisos de las aplicaciones.

Permitir fuentes desconocidas	Si está activada, los usuarios pueden cargar aplicaciones de forma lateral instalando un archivo .apk.

Conectividad	
No permitir configuración de red móvil	Especifica si un usuario tiene prohibido configurar redes móviles.
Config. inhabilitar anclaje a red	Especifica si un usuario tiene prohibido configurar Tethering y puntos de acceso portátiles.
No permitir Config VPN	Especifica si un usuario tiene prohibido configurar una VPN.
No permitir configuración wifi	Especifica si un usuario tiene prohibido cambiar de punto de acceso WiFi.
No permitir el haz NFC saliente	Especifica si no se permite al usuario utilizar NFC para transmitir datos desde las aplicaciones.
Bloquear configuración WiFi	Este ajuste controla si las configuraciones WiFi creadas por una app Propietario del dispositivo deben estar bloqueadas (es decir, ser editables o eliminables sólo por la app Propietario del dispositivo, ni siquiera por la app Configuración).
Activar Itinerancia de Datos	Activa la Itinerancia de Datos

Bluetooth	
No permitir Bluetooth	Especifica si el bluetooth está deshabilitado en el dispositivo. Requiere Android 8.0
No permitir compartir Bluetooth	Especifica si no se permite compartir bluetooth saliente en el dispositivo. Requiere Android 8.0
No permitir la configuración Bluetooth	Especifica si un usuario tiene prohibido configurar el bluetooth.

Gestión de cuentas	
No permitir añadir perfil gestionado	Especifica si un usuario tiene prohibido añadir perfiles gestionados. Requiere Android 8.0
No permitir añadir Usuarios	Especifica si un usuario tiene prohibido añadir nuevos usuarios.
No permitir Eliminar perfil gestionado	Especifica si los perfiles gestionados de este usuario pueden ser eliminados, salvo por su propietario de perfil. Requiere Android 8.0
No permitir la modificación de la cuenta	Especifica si un usuario tiene prohibido añadir y eliminar cuentas, a menos que sean añadidas mediante programación por Authenticator.

Telefonía	
No permitir llamadas salientes	Especifica que el usuario no puede realizar llamadas telefónicas salientes.
No permitir SMS	Especifica que el usuario no puede enviar ni recibir mensajes SMS.

Sistema	
No permitir la creación de ventanas	Especifica que no se deben crear ventanas aparte de las de la app.
No permitir establecer icono de usuario	Especifica si un usuario no puede cambiar su icono.
No permitir establecer papel tapiz	Restricción de usuario para no permitir establecer un fondo de pantalla.
Desactivar la barra de estado	Desactivar la barra de estado bloquea las notificaciones, los ajustes rápidos y otras superposiciones de pantalla que permiten escapar de un dispositivo de un solo uso.
Activar Hora Automática	Ajusta la hora automáticamente.
Activar Zona Horaria Automática	Establece la zona horaria automáticamente.
Permanece encendido mientras está enchufado	El aparato permanecerá activo mientras esté conectado a una fuente de alimentación.

Almacenamiento	
Desactivar la verificación de	Especifica si un usuario tiene prohibido desactivar la verificación de aplicaciones.

aplicaciones	
No permitir montar medios físicos	Especifica si un usuario tiene prohibido montar soportes físicos externos.
Activar el servicio de copia de seguridad	El servicio de copia de seguridad gestiona todos los mecanismos de copia de seguridad y restauración del dispositivo. Configurarlo como falso impedirá que se realicen copias de seguridad o se restauren datos. El servicio de copia de seguridad está desactivado por defecto. Requiere Android 8.0
Activar almacenamiento masivo USB	Activa el uso del almacenamiento masivo USB.

Teclado	
No permitir autorrelleno	Especifica si un usuario no puede utilizar los Servicios de Autorrelleno. Requiere Android 8.0
No permitir copiar y pegar entre perfiles	Especifica si lo que se copia en el portapapeles de este perfil se puede pegar en perfiles relacionados.

Sonido	
Rechazar el ajuste de volumen	Especifica si un usuario tiene prohibido ajustar el volumen maestro.
Desactivar Micrófono	Especifica si un usuario no puede ajustar el volumen del micrófono.
Dispositivo de silencio	Dispositivo de silencio.

Política de actualización del sistema	
Controlar las actualizaciones del SO	Actívala para establecer el comportamiento de actualización en automático, por ventanas o pospuesto.

Contenedor BYOD

Android para empresas

Android para empresas

Activar Android Empresa	Activa Android Enterprise (AE). AE es compatible a partir de Android 5.1.
Cumplimiento de la normativa	Modo Preguntar al Usuario - Se pedirá al usuario que realice las acciones necesarias. Modo Bloqueo Contenedor - Oculta todas las apps hasta que se cumplan todos los requisitos
Política de permisos en tiempo de ejecución	Preguntar al usuario para solicitar nuevos permisos Conceder siempre nuevas solicitudes de permiso Deniega siempre las nuevas solicitudes de permiso Advertencia: Algunas Apps tienen problemas para reconocer los permisos si éstos se establecen automáticamente. Si siempre concedes permisos y tienes problemas con apps que dicen que faltan permisos, establece esta opción en "solicitar al usuario" y vuelve a instalar la app
Permitir el portapapeles saliente	Permite copiar y pegar desde dentro del contenedor hacia fuera
Permitir la resolución del identificador de llamadas	Muestra el nombre de una llamada entrante basándose en los contactos del contenedor
Permitir Resolución de Búsqueda de Contactos	Permite buscar nombres en los contactos del contenedor al realizar llamadas
Permitir compartir contactos por Bluetooth	Permite acceder al contacto del contenedor en un coche
No permitir el haz NFC saliente	Desactiva NFC para el Contenedor
Permitir fuentes desconocidas	Si está activada, los usuarios pueden cargar aplicaciones de forma lateral instalando un archivo .apk.
Permitir depuración USB	Si está activada, los usuarios pueden activar la Depuración USB.

No permitir la modificación de la cuenta	Desactiva la creación, eliminación y modificación de Cuentas en el contenedor Ten en cuenta que algunas aplicaciones necesitan crear o modificar cuentas para funcionar como es debido

Intercambio de Gmail

Te permite configurar Gmail en el Contenedor. Ten en cuenta que habilitar esta configuración no instala automáticamente la app. Todavía tienes que añadir esta aplicación como aplicación obligatoria.

Dirección de correo electrónico	Dirección de correo electrónico
Nombre de host del servidor	Nombre de host del servidor
Nombre de usuario	Nombre de usuario
Firma	Firma
Número de días anteriores a sincronizar	Número de días anteriores a sincronizar.
Identificador del dispositivo	Identificador EAS. Mantenlo vacío si tu entorno no lo requiere
Utiliza la Capa de Conexión Segura (SSL)	Activa el uso de SSL. Desactivarlo puede disminuir la seguridad
Acepta todos los certificados	Acepta todos los certificados. Activar esta opción puede reducir la seguridad
Permitir cuentas no gestionadas	Permite al usuario añadir cuentas adicionales
Certificado de cliente	Carga el certificado de cliente si tu servidor Exchange lo requiere

Aplicaciones del sistema AE

Aquí puede activar las aplicaciones del sistema para el contenedor Android Enterprise. Ten en cuenta que la aplicación especificada tiene que estar en el almacenamiento del sistema, de lo contrario no pasa nada.

Código de acceso al contenedor

Sólo para Android 7.0 o superior

Permite establecer un requisito de contraseña específico para el contenedor.

Longitud mínima de la contraseña	Establece, el número mínimo de símbolos que debe tener una contraseña
Calidad de la contraseña	Fuerza de la contraseña No especificado = no especificado Todas las contraseñas están bien = todas las contraseñas son aceptables al menos caracteres numéricos = debe contener al menos caracteres numéricos al menos caracteres complejos = debe contener al menos caracteres especiales al menos caracteres alfanuméricos = debe contener al menos caracteres alfanuméricos al menos caracteres alfabéticos = debe contener al menos caracteres alfabéticos
Bloqueo de tiempo máximo de inactividad	Tiempo máximo hasta que se bloquea el contenedor. Esto sólo configura el valor máximo que puede seleccionar el usuario
Mínimo de letras minúsculas requeridas en la contraseña	Mínimo de letras minúsculas requeridas en la contraseña
Mínimo de letras mayúsculas requeridas en la contraseña	Mínimo de letras mayúsculas requeridas en la contraseña
Mínimo de caracteres no alfabéticos requeridos en la contraseña	Mínimo de caracteres no alfabéticos requeridos en la contraseña
Dígitos numéricos mínimos requeridos en la contraseña	Dígitos numéricos mínimos requeridos en la contraseña
Símbolos mínimos requeridos en la contraseña	Símbolos mínimos requeridos en la contraseña
Tiempo de caducidad de la contraseña	Establece, después de qué intervalo de tiempo la contraseña caduca y se debe emitir una nueva contraseña
Restricción del historial de contraseñas	Número de contraseñas utilizadas anteriormente que no están permitidas
Número máximo de intentos fallidos de contraseña	Establece cuántas veces se puede introducir incorrectamente una contraseña, antes de que se borre el contenedor

Samsung KNOX

Activación

Aquí puede activar el Samsung KNOX Container. Tenga en cuenta que esto ya no es compatible con Samsung en Android 10 o superior. Utilizar Android Enterprise Container en Android 10 o superior

Código Knox

Establecer las directrices relativas a la configuración de la contraseña del dispositivo

Longitud mínima de la contraseña	Establece cuántos símbolos debe tener la contraseña
Calidad de la contraseña	Fuerza de la contraseña Todas las contraseñas son correctas = Todas las contraseñas son correctas Al menos caracteres numéricos = Debe haber un mínimo de caracteres numéricos Al menos caracteres complejos = Debe haber un mínimo de caracteres especiales Al menos caracteres alfanuméricos = Debe haber un mínimo de caracteres alfanuméricos Al menos caracteres alfabéticos = Debe haber un mínimo de caracteres alfabéticos
Mínimo de caracteres complejos requeridos	Debe haber un mínimo de caracteres complejos
Tiempo máximo de inactividad	Tiempo máximo de inactividad del usuario, antes del bloqueo del teclado
Permitir autenticación por huella dactilar	Permitir la autenticación por huella dactilar
Permitir la autenticación por iris	Permitir la autenticación por reconocimiento del iris
Edad máxima de la contraseña	Establece, después de qué tiempo caduca la contraseña y se debe emitir una nueva contraseña
Historial de contraseñas almacenadas	Número de antiguas contraseñas no permitidas
Número máximo de intentos fallidos de contraseña	Establece cuántas veces se puede introducir incorrectamente la contraseña, antes de que se produzca un borrado completo del dispositivo

Seguridad Knox

Limitar funcionalidades específicas del dispositivo

Activar cámara	Permitir el uso de la cámara
Permitir Samsung KNOX App Store	Permitir el uso de Samsung KNOX App Store
Permitir Servicios de Google Play	Permitir Servicios de Google Play
Permitir navegador	Permitir el uso del navegador nativo
Permitir capturas de pantalla	Permitir la creación de Capturas de Pantalla
Permitir la importación de contactos	Si está activado, se permite el acceso a los contactos del dispositivo desde el Contenedor KNOX
Permitir la exportación de contactos	Si está activado, se permite el acceso a los contactos KNOX desde el dispositivo
Permitir la importación de calendarios	Si está activado, se permite el acceso al calendario de dispositivos desde el Contenedor KNOX
Permitir Exportar Calendario	Si está activado, se permite el acceso a la agenda KNOX desde el dispositivo
Permitir teclado no seguro	Permitir el uso de un teclado no seguro
Activar la importación de archivos	Activar la importación de archivos en el contenedor KNOX
Activar la exportación de archivos	Activar la exportación de archivos desde el contenedor KNOX

Bolsa de Knox

Aquí puede configurar el Exchange-Profile para el contenedor KNOX

Dirección de correo electrónico	La dirección de correo electrónico del usuario facilitada Ten en cuenta los "Marcadores de posición", que puedes utilizar para trabajar con credenciales y no realizar cambios manualmente en cada dispositivo Con un clic en **Mostrar marcadores de posición** puedes mostrarlos tú mismo
Nombre de host del servidor	Dirección del servidor de tus servidores Exchange
Nombre de usuario	El nombre de inicio de sesión para el dispositivo del usuario final correspondiente, ten en cuenta también los "Marcadores de posición" aquí
Dominio	Dirección del dominio
Contraseña (sólo a nivel de dispositivo)	Opcionalmente, se puede proporcionar una contraseña a un dispositivo individual; si ésta permanece vacía, se pedirá al usuario que introduzca su contraseña de Exchange.
Número de días anteriores a sincronizar	Número de días, que determina cuándo se sincronizan de nuevo los correos electrónicos
Firma	Se puede adjuntar una firma
Cuenta por defecto	Establece, que esta cuenta de correo electrónico es la cuenta estándar
Utiliza la Capa de Conexión Segura (SSL)	Utilizar una conexión SSL
Utiliza la Seguridad de la Capa de Transporte (TLS)	Utiliza una conexión TLS
Acepta todos los certificados	Se aceptan todos los certificados. Selecciona esta opción si tu Exchange Server utiliza un certificado autofirmado

Knox eMail

Dirección de correo electrónico	La dirección de correo electrónico del usuario facilitada Ten en cuenta los "Marcadores de posición", que puedes utilizar para trabajar con credenciales y no realizar cambios manualmente en cada dispositivo Con un clic en **Mostrar marcadores de posición** puedes mostrarlos tú mismo
Protocolo del servidor entrante	Protocolo del servidor entrante IMAP o POP
Dirección del servidor entrante	Dirección del servidor entrante
Puerto del servidor entrante	Puerto del servidor entrante
Nombre de usuario/contraseña del servidor entrante	Nombre de usuario/contraseña del servidor entrante
Contraseña del servidor entrante	Contraseña del servidor entrante
El servidor entrante utiliza SSL	El servidor entrante utiliza SSL
El servidor entrante utiliza TLS	El servidor entrante utiliza TLS
El servidor entrante acepta todos los certificados	El servidor entrante acepta todo tipo de certificados
Protocolo del servidor saliente	Protocolo del servidor saliente SMTP
Puerto del servidor saliente	Puerto del servidor saliente
El servidor saliente utiliza credenciales adicionales	Credenciales adicionales para el Servidor saliente. Si está desactivado, se utilizará la configuración del servidor entrante.
Nombre de usuario del servidor saliente	Nombre de usuario del servidor saliente
Contraseña del servidor saliente	Contraseña del servidor saliente
El servidor saliente utiliza SSL	El servidor saliente utiliza SSL
El servidor saliente utiliza TLS	El servidor saliente utiliza TLS
El servidor saliente acepta todos los certificados	El servidor saliente acepta todo tipo de certificados
Firma	Aquí se puede adjuntar una firma

Notificar al usuario la recepción de un nuevo eMail	Notificar al usuario la recepción de un nuevo eMail

Aplicaciones Knox

Establece aquí las aplicaciones que quieras distribuir a los dispositivos de los usuarios finales. Éstas estarán disponibles en el KNOX-Container. Para añadir una app, procede como lo harías en el menú Apps obligatorias

Nombre de la aplicación	Nombre de la aplicación
Obligatorio desde	Momento en que se añadió la aplicación
Fuente	Fuente de la aplicación (Play Store | In-House)

Haciendo clic en el símbolo, se puede volver a eliminar la aplicación correspondiente.

Gestión de conexiones

Wifi

Para esta configuración, realice la preconfiguración de los dispositivos de usuario final, para el acceso a los Puntos de Acceso internos

Identificador del Conjunto de Servicios (SSID)	SSID de la red que se va a conectar
Red oculta	Activar, en caso de que el AP no emita el SSID
Tipo de seguridad	Establecer el tipo de seguridad del AP

Tipo de seguridad

WEP

Contraseña	Contraseña para el PA

WPA/WPA2

Contraseña	Contraseña para el PA

802.1x EAP

Método EAP	

PWD	Identidad	Identidad
	Contraseña	Contraseña

PEAP	Protocolo de autenticación de fase 2	ninguno	Sin protocolo adicional
		MSCHAPV2	Protocolo MSCHAPV2
		GTC	Protocolo GTC
	Certificado CA	Certificado CA	
	Identidad	Identidad	
	Identidad anónima	Identidad anónima	
	Contraseña	Contraseña	

Método EAP	

TTLS	Protocolo de autenticación de fase 2	ninguno	Sin protocolo adicional
		PAP	Protocolo PAP
		MSCHAP	Protocolo MSCHAP
		MSCHAPV2	Protocolo MSCHAPV2
		GTC	Protocolo GTC
	Certificado CA	Certificado CA	
	Identidad	Identidad	
	Identidad anónima	Identidad anónima	
	Contraseña	Contraseña	

TLS	Certificado CA	Certificado CA
	Identidad	Identidad
	Contraseña	Contraseña

VPN

Tipo de conexión	**Establecer tipo de conexión VPN**

Si seleccionas "VPN por aplicación" como Tipo de VPN, cambiarán los Clientes VPN disponibles. La VPN por aplicación limita la VPN a determinadas aplicaciones e inicia la conexión VPN automáticamente si se inicia una aplicación específica.

Cliente VPN AppTec360	Utiliza el Cliente VPN AppTec360 en combinación con la Pasarela Universal
Nombre de la conexión	Nombre de la conexión VPN
Configuración de la puerta de enlace	Selecciona la Configuración VPN de la Pasarela Universal
VPN siempre activa	Obliga a la VPN a estar siempre activa, para que todo el tráfico pase por la VPN.
Activar Bloqueo Nativo	Bloquea todas las redes cuando el dispositivo no está conectado a la VPN. Utilízalo con cuidado, ya que puede provocar la pérdida total de la conexión si no se configura correctamente. Sólo para Android Enterprise en Android 7 o superior
Activar el bloqueo de AppTec360	Bloquea el uso de todas las Apps hasta que se inicie la conexión VPN

Cisco AnyConnect	
Nombre de la conexión	Nombre de la conexión VPN
Servidor	Dirección del servidor
Modo Certificado	Desactivado = desactivado Automático = automático

L2TP (sólo KNOX)	Sólo disponible en dispositivos Samsung
Nombre de la conexión	Nombre de la conexión
Servidor	Dirección del servidor
Activar Secreto L2TP	
Búsqueda DNS Dominios	Dominios de búsqueda DNS

Tipo de conexión	**Establecer tipo de conexión VPN**

PPTP (sólo KNOX)	Sólo disponible en dispositivos Samsung
Nombre de la conexión	Nombre de la conexión VPN
Servidor	Dirección del servidor
Activar encriptación	Activar la encriptación
Búsqueda DNS Dominios	Dominios de búsqueda DNS

L2TP / IPSec PSK (sólo KNOX)	Sólo disponible en dispositivos Samsung
Nombre de la conexión	Nombre de la conexión VPN
Servidor	Dirección del servidor
Clave precompartida IPSec	Clave precompartida para la autenticación
Activar Secreto L2TP	
Secreto L2TP	
Búsqueda DNS Dominios	Dominios de búsqueda DNS

IPSec XAuth PSK (sólo KNOX)	Sólo disponible en dispositivos Samsung
Nombre de la conexión	Nombre de la conexión VPN
Servidor	Dirección del servidor
Identificador IPSec	Nombre de usuario para la conexión
Clave precompartida IPSec	Contraseña para la conexión
Búsqueda DNS Dominios	Dominios de búsqueda DNS

OpenVPN	

Nombre de la conexión	Nombre de la conexión
Perfil OpenVPN	Aquí es donde se copiará el contenido del archivo .ovpn
Aplicación OpenVPN	Hay dos aplicaciones diferentes para utilizar OpenVPN Recomendamos la aplicación "OpenVPN para Android". Pero como alternativa, puedes utilizar la aplicación "OpenVPN Connect

Restricciones

Aquí puede establecer las restricciones, en relación con la gestión de la conexión.

Permitir itinerancia de datos	Permitir datos móviles en itinerancia
Forzar itinerancia de datos	Si se activa, la itinerancia para datos móviles se activa permanentemente (¡no se recomienda!) Este ajuste sobrescribe el ajuste "Permitir itinerancia de datos".
Los siguientes ajustes sólo están disponibles en Samsung KNOX 2.0 o superior	
Permitir sólo llamadas de emergencia	Permitir sólo llamadas de emergencia
Permitir WiFi	Permitir WiFi
Nivel mínimo de seguridad de la red WiFi	Nivel mínimo de seguridad de la red WiFi Abierto = se permiten todos los tipos de WiFi
Prohibir al usuario añadir redes WiFi	El usuario no puede añadir una red WiFi por sí mismo Este ajuste sólo es posible si se ha definido un perfil WiFi en "Gestión de conexiones".
Permitir SMS y MMS	Todos = Se permite todo el tráfico de SMS y MMS Sólo SMS entrantes = Sólo se permiten mensajes SMS entrantes Sólo SMS salientes = Sólo se permiten mensajes SMS salientes Ninguno = No se permite el tráfico SMS / MMS
Permitir sincronización en itinerancia	Permitir sincronización en itinerancia Encendido = activado Apagado = desactivado Elección del usuario = elección del usuario
Permitir itinerancia de voz	Permitir itinerancia de voz Encendido = activado Apagado = desactivado Elección del usuario = elección del usuario
Utilizar el servidor proxy http del sistema	El uso de un servidor proxy HTTP, que se proporciona mediante la configuración del sistema en ajustes, depende de la red conectada (WiFi o APN).

APN

Los siguientes ajustes sólo están disponibles en Samsung SAFE 2.0 o superior.

Nombre para mostrar APN	Nombre para mostrar APN	
Nombre del punto de acceso	Nombre del APN	
Protocolo del servidor saliente	No fijado	
	Ninguno	
	PAP	Protocolo PAP
	CHAP	Protocolo CHAP
	PAP o CHAP	El protocolo PAP o CHAP
MCC - Código de país del móvil	El MCC se introduce aquí, deja este campo en blanco, si se debe utilizar el MCC de la tarjeta SIM insertada	
MNC - Código de red móvil	El MNC se introduce aquí, deja este campo en blanco, si se debe utilizar el MCC de la tarjeta SIM insertada	
Dirección del servidor	Dirección del servidor	
Número de puerto del servidor	Número de puerto del servidor	
Dirección proxy del servidor	Dirección proxy del servidor	
Dirección del servidor MMS	Dirección del servidor MMS, para Estándar dejar en blanco	
Número de puerto MMS	Número de puerto MMS	
Dirección proxy MMS	Dirección proxy MMS	
Nombre de usuario	Nombre de usuario	
Contraseña	Contraseña	
Tipo de punto de acceso	Los tipos permitidos son: "por defecto", "mms", "supl" Si este campo se deja en blanco, se utilizará "por defecto,supl,mms".	
APN preferido	Se prefiere APN	

Bluetooth

Aquí se pueden realizar diversos ajustes de Bluetooth.

Los siguientes ajustes sólo están disponibles en Samsung KNOX 1.0 o superior.

Permitir la detección de dispositivos mediante Bluetooth	Permitir la detección de dispositivos mediante Bluetooth
Permitir emparejamiento Bluetooth	Permitir emparejamiento Bluetooth
Permitir dispositivos Auriculares Bluetooth	Permitir dispositivos Auriculares Bluetooth
Permitir dispositivos manos libres Bluetooth	Permitir dispositivos manos libres Bluetooth
Permitir dispositivos Bluetooth A2DP	Permitir la transmisión de audio Bluetooth A2DP entre dispositivos
Permitir llamadas salientes	Permitir llamadas salientes víaBT
Permitir la transferencia de datos por Bluetooth	Permitir la transferencia de datos por Bluetooth
Permitir anclaje Bluetooth	Permite utilizar el dispositivo como módem (conexión a Internet por Bluetooth)
Permitir la conexión con el ordenador mediante Bluetooth	Permitir la conexión con el ordenador mediante Bluetooth

Gestión PIM

Intercambio

¡Sólo disponible para Samsung KNOX 1.0 o superior!

Dirección de correo electrónico	La dirección de correo electrónico del usuario facilitada Ten en cuenta los "Marcadores de posición", que puedes utilizar para trabajar con credenciales y no realizar cambios manualmente en cada dispositivo Con un clic en **Mostrar marcadores de posición** puedes mostrarlos tú mismo
Nombre de host del servidor	Dirección del servidor de tus servidores Exchange
Nombre de usuario	El nombre de inicio de sesión para el dispositivo del usuario final correspondiente, ten en cuenta también los "Marcadores de posición aquí".
Dominio	Dirección del dominio
Contraseña (sólo a nivel de dispositivo)	Opcionalmente, se puede proporcionar una contraseña a un dispositivo individual; si ésta permanece vacía, se pedirá al usuario que introduzca su contraseña de Exchange.
Número de días anteriores a sincronizar	Número de días, que determina cuándo se sincronizan de nuevo los correos electrónicos
Firma	Se puede adjuntar una firma (Sugerencia: Algunos dispositivos requieren formato HTML para la firma)
Cuenta por defecto	Establece, que esta cuenta de correo es la cuenta estándar
Utiliza la Capa de Conexión Segura (SSL)	Utilizar una conexión SSL
Utiliza la Seguridad de la Capa de Transporte (TLS)	Utiliza una conexión TLS
Acepta todos los certificados	Se aceptan todos los certificados. Selecciona esta opción si tu Exchange Server utiliza un certificado autofirmado

Correo electrónico

Aquí puede distribuir cuentas IMAP y POP a los respectivos dispositivos de usuario final.

Los siguientes ajustes sólo están disponibles en Samsung KNOX 1.0 o superior.		
Dirección de correo electrónico	La dirección de correo electrónico del usuario facilitada Ten en cuenta los "Marcadores de posición", que puedes utilizar para trabajar con credenciales y no realizar cambios manualmente en cada dispositivo Con un clic en **Mostrar marcadores de posición** puedes mostrarlos tú mismo	
Protocolo del servidor entrante	Protocolo del servidor entrante	IMAP o POP
Dirección del servidor entrante	Dirección del servidor entrante	
Puerto del servidor entrante	Puerto del servidor entrante	
Nombre de usuario/contraseña del servidor entrante	Nombre de usuario/contraseña del servidor entrante	
Contraseña del servidor entrante (sólo a nivel de dispositivo)	Contraseña del servidor entrante (sólo a nivel de dispositivo)	
El servidor entrante utiliza SSL	El servidor entrante utiliza SSL	
El servidor entrante utiliza TLS	El servidor entrante utiliza TLS	
El servidor entrante acepta todos los certificados	El servidor entrante acepta todo tipo de certificados	
Protocolo del servidor saliente	Protocolo del servidor saliente	SMTP
Puerto del servidor saliente	Puerto del servidor saliente	
El servidor saliente utiliza credenciales adicionales	Credenciales adicionales para el servidor saliente. Si está desactivado, se utilizará la configuración del servidor entrante.	
Nombre de usuario del servidor saliente	Nombre de usuario del servidor saliente	
Contraseña del servidor de salida (sólo a nivel de dispositivo)	Contraseña del servidor saliente	
El servidor saliente utiliza SSL	El servidor saliente utiliza SSL	
El servidor saliente utiliza TLS	El servidor saliente utiliza TLS	
El servidor saliente acepta todos los certificados	El servidor saliente acepta todo tipo de certificados	

Firma	Puedes adjuntar una firma aquí (Sugerencia: Algunos dispositivos requieren formato HTML para la firma)
Notificar al usuario la recepción de un nuevo eMail	Notifica al usuario la recepción de un nuevo correo electrónico

AE Gmail Exchange

Información: Esta Configuración se aplicará a la aplicación de Gmail. Así que tienes que aprobar e instalar Gmail.

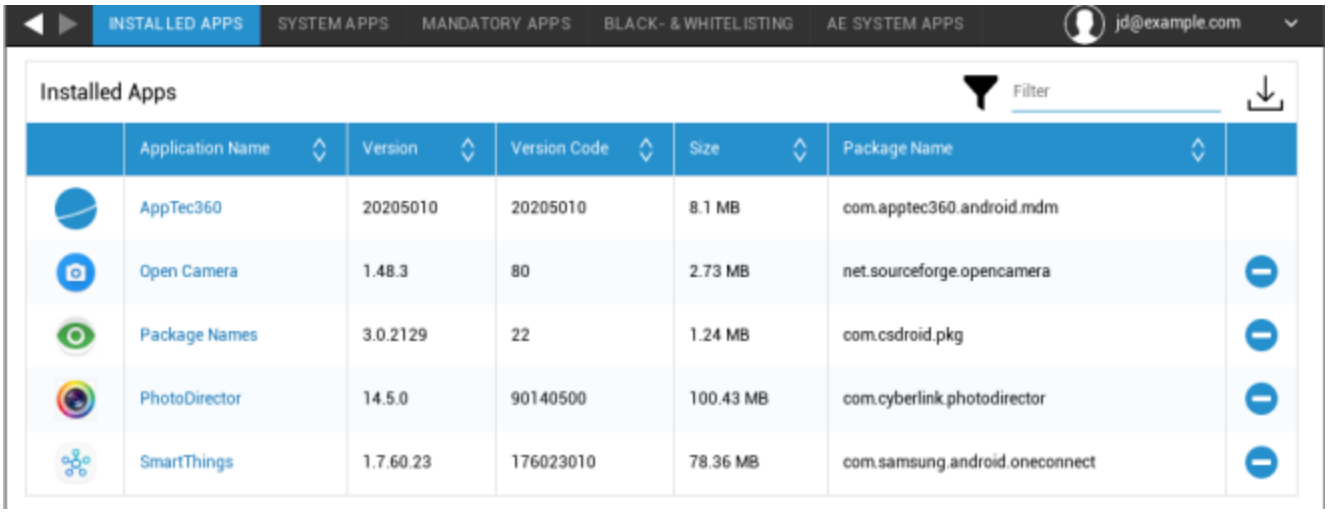
Dirección de correo electrónico	La dirección de correo electrónico del usuario facilitada Ten en cuenta los "Marcadores de posición", que puedes utilizar para trabajar con credenciales y no realizar cambios manualmente en cada dispositivo Con un clic en Mostrar marcadores de posición puedes mostrarlos tú mismo
Nombre de host del servidor	Dirección del servidor de tus servidores Exchange
Nombre de usuario	El nombre de inicio de sesión para el dispositivo del usuario final correspondiente, ten en cuenta también los "Marcadores de posición aquí".
Firma	Se puede adjuntar una firma (Sugerencia: Algunos dispositivos requieren formato HTML para la firma)
Número de días anteriores a sincronizar	Número de días, que determina cuándo se sincronizan de nuevo los correos electrónicos
Identificador del dispositivo	Identificador EAS. Mantenlo vacío si tu entorno no lo requiere
Utiliza la Capa de Conexión Segura (SSL)	Utilizar una conexión SSL
Acepta todos los certificados	Se aceptan todos los certificados. Selecciona esta opción si tu Exchange Server utiliza un certificado autofirmado
Permitir cuentas no gestionadas	Permite al usuario añadir cuentas adicionales
Certificado de cliente	Carga el certificado de cliente si tu servidor Exchange lo requiere

Gestión de aplicaciones

Enterprise App Manager

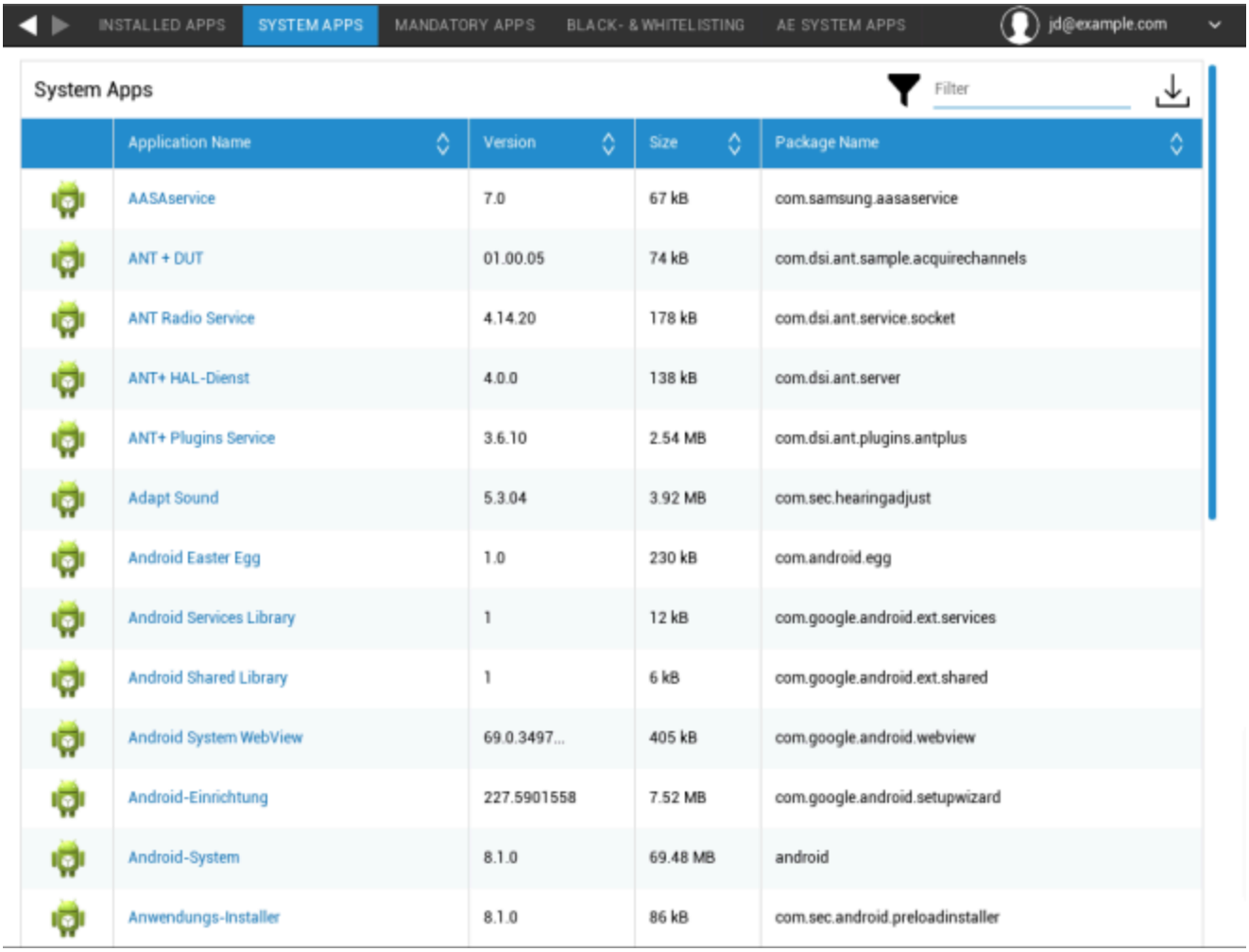
Aplicaciones instaladas (sólo en el dispositivo)

Aquí se mostrarán todas las aplicaciones instaladas actualmente en el dispositivo del usuario final.


INSTALLED APPS
SYSTEM APPS
MANDATORY APPS
BLACK- & WHITELISTING
AE SYSTEM APPS
jd@example.com
Installed Apps
Filter
Application Name
Version
Version Code
Size
Package Name
AppTec360
20205010
20205010
8.1 MB
com.apptec360.android.mdm
Open Camera
1.48.3
80
2.73 MB
net.sourceforge.opencamera
Package Names
3.0.2129
22
1.24 MB
com.csdroid.pkg
PhotoDirector
14.5.0
90140500
100.43 MB
com.cyberlink.photodirector
SmartThings
1.7.60.23
176023010
78.36 MB
com.samsung.android.oneconnect

Aplicaciones del sistema (sólo a nivel de dispositivo)

En "Aplicaciones del sistema", aparecerán todas las preinstaladas con su nombre de paquete y versión.



Application Name	Version	Size	Package Name
AASAservice	7.0	67 kB	com.samsung.aasaservice
ANT + DUT	01.00.05	74 kB	com.dsi.ant.sample.acquirechannels
ANT Radio Service	4.14.20	178 kB	com.dsi.ant.service.socket
ANT+ HAL-Dienst	4.0.0	138 kB	com.dsi.ant.server
ANT+ Plugins Service	3.6.10	2.54 MB	com.dsi.ant.plugins.antplus
Adapt Sound	5.3.04	3.92 MB	com.sec.hearingadjust
Android Easter Egg	1.0	230 kB	com.android.egg
Android Services Library	1	12 kB	com.google.android.ext.services
Android Shared Library	1	6 kB	com.google.android.ext.shared
Android System WebView	69.0.3497...	405 kB	com.google.android.webview
Android-Einrichtung	227.5901558	7.52 MB	com.google.android.setupwizard
Android-System	8.1.0	69.48 MB	android
Anwendungs-Installer	8.1.0	86 kB	com.sec.android.preloadinstaller

Aplicaciones obligatorias

En Aplicaciones obligatorias puede definir qué aplicaciones deben instalarse en el dispositivo. Dependiendo de la configuración y del dispositivo, la aplicación se instalará automáticamente o se pedirá al usuario que la instale.

Tenga en cuenta que se recomienda utilizar Android Enterprise para facilitar la gestión de las aplicaciones.

Los escenarios son los que se indican a continuación:

Aplicaciones normales de Play Store

Las instalaciones de aplicaciones en Play Store siempre necesitan la interacción del usuario. Además, hay que configurar una cuenta de Google en el dispositivo.

Instalación interna de la aplicación

En los dispositivos Samsung, estas aplicaciones se instalarán de forma silenciosa. La única excepción es el contenedor, donde el usuario debe confirmar la instalación.

En cualquier otro caso, el usuario debe confirmar la instalación de la aplicación.

Aplicaciones Android Enterprise Play Store

Estas aplicaciones se instalarán siempre de forma silenciosa, sin interacción del usuario.

Para añadir una aplicación obligatoria, haga clic en "+" y seleccione la aplicación deseada de la lista. Tenga en cuenta que no podrá instalar aplicaciones desde la pestaña "Google Play Store" si el dispositivo está configurado con Android Enterprise como totalmente gestionado o como contenedor.

Si utiliza Android Enterprise, seleccione las aplicaciones de la sección "AE Play Store". Para que las apps estén disponibles aquí, confírmalas en la tienda Google Enterprise Play yendo a Ajustes generales → AE Play Store → Play Store Apps.

Al eliminar una aplicación obligatoria, también se desinstalará del dispositivo.

Puede hacer clic en el nombre de una aplicación en la lista de aplicaciones obligatorias y acceder a la pestaña "configuración" para configurar una aplicación. Esto requiere el uso de Android Enterprise y la aplicación tiene que soportarlo. Por lo tanto, las opciones disponibles dependen de la aplicación seleccionada.

Aplicaciones del sistema AE

Aquí puede habilitar las aplicaciones del sistema para los dispositivos Android Enterprise. Ten en cuenta que la aplicación especificada tiene que estar en el almacenamiento del sistema, de lo contrario no pasa nada. 296

Restricciones y ajustes

Listas negras y blancas

Aquí puede definir una lista negra o blanca. Se bloquearán todas las aplicaciones de la lista negra. Todas las aplicaciones que no estén en la lista blanca serán bloqueadas. Una lista negra vacía no bloquea nada, mientras que una lista blanca vacía bloquea todo*.

**Todas las aplicaciones obligatorias y las de la Enterprise App Store se incluirán automáticamente en la lista blanca. No es necesario añadirlos manualmente*

Al hacer clic en el signo "+", puede buscar una aplicación que desee añadir a su lista negra o blanca o introducir el nombre de un paquete manualmente.

Restricciones de las aplicaciones del sistema

En "Sys App Restrictions" puedes, entre otras cosas, bloquear las aplicaciones y servicios preinstalados que desees.

Desactivar Navegador	Desactiva el navegador estándar
Desactivar Calendario	Desactivar calendario nativo
Desactivar Calculadora	Desactivar calculadora
Desactivar el navegador Chrome	Desactiva el navegador Chrome
Desactivar Reloj	Desactivar reloj
Desactivar contactos	Desactivar contactos
Desactivar Marcador	Desactivar el marcador nativo
Desactivar eMail	Desactivar correo electrónico
Desactivar Intercambio	Desactivar cuentas Exchange
Desactivar Facebook	Desactivar la aplicación de Facebook
Desactivar Galería	Desactiva la app nativa de la galería
Desactivar Gmail	Desactivar Gmail
Desactivar la Búsqueda de libros de Google	Desactivar la Búsqueda de libros de Google
Desactivar Google Play Kiosk	Desactivar Google Play Kiosk
Desactivar Google Maps	Desactivar Google Maps
Desactivar Google Music	Desactivar Google Music
Desactivar Google Movies	Desactivar Google Movies
Desactivar Google Play Store	Desactiva Google Play Store (App Store pública)
Desactivar Google Plus	Desactivar Google Plus
Desactivar la Búsqueda en Google	Desactivar la Búsqueda en Google
Desactivar Google Talk / Google Hangouts	Desactivar Google Talk / Google Hangouts
Desactivar el reproductor de música	Desactiva la aplicación nativa de reproducción de música
Desactivar ajustes	Desactivar ajustes del dispositivo
Desactivar Sim Toolkit	Desactivar los servicios del Sim Toolkit
Desactivar SMS / MMS	Desactivar SMS / MMS
Desactivar Street View	Desactivar los servicios de Street View
Desactivar Youtube	Desactivar Youtube

Aplicaciones Samsung

En "Samsung Apps", puede definir ajustes y/o restricciones adicionales para los dispositivos Samsung.

Desactivar AllShare Play / Samsung Link	Desactivar AllShare Play / Samsung Link
Desactivar ChatON	Desactivar ChatON
Desactivar Game Hub	Desactivar Game Hub
Desactivar Juego en Grupo	Desactivar Juego en Grupo
Desactivar Ayuda	Desactivar la Ayuda de Samsung
Desactivar KNOX	Desactivar Contenedor Samsung KNOX
Desactivar Memo	Desactivar nota de voz
Desactivar Mis Archivos	Desactivar Mis Archivos
Desactivar Lector Óptico	Desactivar Lector Óptico
Desactivar Polaris Office	Desactivar Polaris Office
Desactivar Readers Hub / Samsung Books	Desactivar Readers Hub / Samsung Books
Desactivar S Memo	Desactiva la aplicación Samsung Memo
Desactivar Traductor S	Desactiva la aplicación Traductor de Samsung
Desactivar Voz S	Desactivar el asistente de voz S
Desactiva las aplicaciones de Samsung	Desactivar Samsung App Store
Desactivar Samsung Hub	Desactivar las Tiendas de Entretenimiento de Samsung
Desactivar el reproductor de vídeo	Desactivar el reproductor de vídeo
Desactivar Grabadora de Voz	Desactivar Grabadora de Voz
Desactivar WatchON	Desactiva WatchON (simula un mando a distancia)

Aplicaciones Huawei

En "Aplicaciones Huawei", puede definir ajustes adicionales y/o restricciones en el dispositivo Huawei.

Desactivar DLNA	Desactivar DLNA
Desactivar el instalador de aplicaciones	Desactivar el instalador de aplicaciones
Desactivar el Gestor de Archivos	Desactivar el Gestor de Archivos
Desactivar el Gestor de Copias de Seguridad	Desactivar el Gestor de Copias de Seguridad
Desactivar el Actualizador del Sistema	Desactivar el Actualizador del Sistema
Desactivar Caja de Herramientas	Desactivar Caja de Herramientas
Desactivar Tiempo	Desactivar Tiempo
Desactivar Radio FM	Desactivar Radio FM

Configuración de App Management

Aquí puede definir el comportamiento de actualización de InHouse Apps.

La frecuencia de comprobación de actualizaciones define la frecuencia con la que la aplicación AppTec360 busca actualizaciones para las aplicaciones internas. Una vez detectada una nueva versión, se descargará e instalará.

Umbral Wi-Fi define si la descarga debe limitarse a las conexiones Wi-Fi si la aplicación es mayor que el umbral configurado. Si el es menor o no defines un umbral, la aplicación se descargará en Wi-Fi y en una red celular.

App Store para empresas

Tenga en cuenta que las aplicaciones que se añadan aquí (Enterprise App Store) NO se instalarán automáticamente en los dispositivos. El usuario tiene que abrir la Enterprise App Store en el dispositivo e instalar la aplicación manualmente.

Si desea instalar automáticamente aplicaciones en el dispositivo, vaya a "App Management" → "Enterprise App Manager" → "Mandatory Apps" y añada las aplicaciones deseadas.

En este punto, puede distribuir Apps opcionales a sus usuarios.

Playstore

Haz clic en el signo "+" para añadir una aplicación de Play Store a la tienda. Si utiliza Android Enterprise, vaya a "App Management Enterprise Play Store". Tenga en cuenta también que debe configurarse una cuenta de Google en → el dispositivo para instalar las apps definidas aquí.

En la empresa

En el punto "In-House", puede cargar y distribuir aplicaciones desarrolladas internamente.

Haga clic en el signo "+" para añadir una aplicación InHouse a la tienda de aplicaciones de la empresa, que podrá ser instalada por el usuario. En este diálogo también puedes cargar una nueva aplicación InHouse.

Play Store para empresas

Ten en cuenta que las aplicaciones que se añadan aquí (Enterprise Play Store) NO se instalarán automáticamente en los dispositivos. El usuario tiene que abrir Play Store en el dispositivo e instalar la aplicación manualmente.

Si desea instalar automáticamente aplicaciones en el dispositivo, vaya a "App Management" → "Enterprise App Manager" → "Mandatory Apps" y añada las aplicaciones deseadas.

En este punto, puede distribuir Apps opcionales a sus usuarios.

Aquí puede añadir aplicaciones a la Play Store de Android Enterprise. Tenga en cuenta que tiene que aprobar Apps en Ajustes generales → AE Play Store → Play Store Apps. Estas aplicaciones se añadirán a la tienda normal Google Play Store.

Ten en cuenta también que primero tienes que definir un Diseño con Apps en Ajustes generales → Gestión de Apps → AE Play Store → Diseño de la tienda.

Las aplicaciones tienen que estar en un Layout antes de que puedas añadirlas con éxito a la tienda.

Modo quiosco y lanzador

Modo quiosco

El Modo Quiosco te permite predefinir una app o una URL. Entonces será posible ejecutar/visitar exclusivamente esta app y/o URL.

Del mismo modo, se pueden desactivar varios botones de hardware en el Modo Quiosco diverso.

Inicio automático	Inicia automáticamente el Modo Quiosco, en cuanto el perfil llega al dispositivo del usuario final
¿Modo Quiosco Programado?	Puedes planificar una hora para el Modo Quiosco, que se iniciará y finalizará automáticamente a la hora que tú establezcas.
Hora de inicio	Hora de inicio
Tiempo en minutos	Tiempo en minutos, tras el cual el Modo Quiosco debe finalizar de nuevo

Tipo de aplicación

Aplicación única	Si quieres iniciar la App en el Modo Quiosco, selecciona Paquete" en "Tipo de Aplicación".
Aplicación quiosco	Pulsa aquí, para seleccionar una aplicación que deba iniciarse en Modo Quiosco Encontrarás el resumen habitual de App Management Puedes seleccionar entre "Google Play Store", "Aplicaciones internas de Android" y "Nombre del paquete".

Tipo de aplicación

URL	Si quieres lanzar una URL en el Modo Quiosco, selecciona "URL" en "Tipo de aplicación". A continuación, define la dirección URL que desees
Limpiar el navegador tras inactividad	Aquí puedes definir un intervalo de tiempo en minutos, tras el cual debe relanzarse el Modo Quiosco
Borrar caché web y cookies	Si activas esta función, después de reiniciar el Modo Quiosco, se borrará la Caché Web (cookies e imágenes almacenadas en caché)
Política del mismo origen	Si esta función está activa, el usuario sólo podrá navegar por las subpáginas de una URL definida Por ejemplo, has definido la siguiente URL:www.mypage.com Entonces, el usuario puede navegar en: www.mypage.com/subpage
URLs en lista blanca	Aquí puedes mantener una Lista Blanca, todas estas URLs están permitidas Máximo 1 URL por línea Una URL debe empezar por http:/ o https://
URLs en la lista negra	Aquí puedes mantener una Lista Negra, todas estas URLs no están permitidas Máximo 1 URL por línea Una URL debe empezar por http:/ o https://
Orientación de la pantalla	Este ajuste está relacionado con los ajustes de pantalla Automático = automático Vertical = formato vertical Paisaje = modo paisaje

Multi App	Si seleccionas el Modo Quiosco "Multi App", se impondrá el uso del AppTec360 Launcher.
Aplicaciones	Aplicación: Selecciona una aplicación de Playstore o una aplicación propia como aplicación de quiosco. También es posible introducir un nombre de paquete. La Aplicación de Quiosco seleccionada debe estar instalada en el dispositivo. Recuerda establecer la Aplicación de Quiosco como obligatoria. Acceso directo en la pantalla de inicio: Si está activado, se creará un acceso directo en la pantalla de inicio. Si está desactivado, la aplicación seguirá apareciendo en la Lista de aplicaciones.

Contraseña de salida activada	Si activas esta función, el usuario podrá finalizar el Modo Quiosco con una contraseña predefinida por ti.
Salir Contraseña	Esta es la contraseña predefinida por ti
Contraer automáticamente la barra de estado	Si está activada, la Barra de Estado se coloreará automáticamente. Con esta opción, los usuarios pueden ver la información de la Barra de Estado, pero no pueden acceder a sus funciones.
Desactivar la barra de estado	La barra de estado contiene notificaciones, accesos directos e información. Sólo disponible para dispositivos Samsung con KNOX 1.0 o superior.
Desactivar teclas de volumen	Desactivar teclas de volumen (sólo disponible en dispositivos Samsung con KNOX 1.0 o superior)
Desactivar el interruptor de encendido/apagado	Desactivar el interruptor de encendido/apagado (sólo disponible en dispositivos Samsung con KNOX 1.0 o superior)
Desactivar Botón Inicio	Desactivar botón Inicio. Si se ha activado esta función, el Modo Quiosco sólo se puede finalizar en la Consola AppTec360 (sólo disponible en dispositivos Samsung con KNOX 1.0 o superior)
Desactivar la barra de navegación	Con esto puedes desactivar la Barra de Navegación (Atrás / Menú) Si se ha activado esta función, el Modo Quiosco sólo se puede finalizar en la Consola AppTec360 (sólo disponible en dispositivos Samsung con KNOX 1.0 o superior)

Ajustes de actualización de la app	
Permitir actualizaciones de la app	Se pedirá a los usuarios que realicen actualizaciones de las aplicaciones incluso cuando el Modo Quiosco esté activo. En los dispositivos con Samsung KNOX, las aplicaciones se actualizarán silenciosamente.
Ventana de actualización	Establece un intervalo en el que se pedirá a los usuarios que instalen actualizaciones de la aplicación.

TeamViewer	
Activar el acceso desatendido	Si se activa, los administradores pueden controlar remotamente el dispositivo sin interacción del usuario. La aplicación TeamViewer Host debe estar instalada en el dispositivo.

Lanzador AppTec360

Activar AppTec360 Launcher	Activado: Activa el Lanzador de AppTec360. El usuario tiene que configurarlo como Lanzador por defecto una vez. Nota: Si el Modo Quiosco está activado, y el Modo Quiosco está configurado como "Multi App", se impondrá el uso del lanzador AppTec360.
Iconos grandes	Activado: Muestra una versión más grande de los iconos de la aplicación en el lanzador.
Ocultar el icono de la aplicación AppTec360	Activado: Oculta completamente la aplicación AppTec360
Ocultar el icono de la tienda AppTec360	Activado: Oculta completamente la AppStore de AppTec360 Enterprise

Configuración de AppTec360

Activar la App de Configuración de AppTec360	La App de Configuración AppTec360 proporciona control sobre las conexiones WiFi y Bluetooth
Activar Ajustes en Multi App Modo quiosco	Si está activado, los usuarios pueden acceder a la App de Configuración de AppTec360 mientras el Modo Kiosko Multi App está activo

Mando a distancia

Splashtop

Muestra el estado actual de la configuración de Splashtop. Aquí verás los pasos que debes realizar para acceder remotamente al dispositivo a través de Splashtop. Aquí también tienes que introducir el código de despliegue que puedes obtener en el sitio web de Splashtop. El código de despliegue es necesario para conectarse al dispositivo.

Teamviewer

Muestra el estado actual de la configuración de Teamviewer. Aquí verás los pasos que debes realizar para acceder remotamente al dispositivo a través de Teamviewer.

Gestión de contenidos

Cuadro de contenido

Aquí puede activar el Contentbox para este dispositivo. Una vez activada, la aplicación Contentbox se instalará en el dispositivo.

Navegador seguro

Aquí puedes activar el Navegador Seguro para este dispositivo. Una vez activado, se instalará la aplicación del Navegador Seguro en el dispositivo. Este Navegador puede configurarse para ofrecer un Navegador Web en el dispositivo limitado a tus necesidades.

Requerir contraseña	Exige al usuario que establezca y utilice una contraseña para acceder al navegador.
Restringir descargas / Abrir en	Bloquea las descargas de sitios web
Restringir subidas	Restringe las subidas a determinadas URL. No proporciones ninguna URL para bloquear la subida por completo
Permitir copia	Permite copiar, cortar o compartir texto dentro de las páginas web.
Permitir Captura de Pantalla	Permite hacer capturas de pantalla.
Frecuencia de limpieza de datos	Selecciona con qué frecuencia deben eliminarse automáticamente TODOS los datos del usuario (historial, caché, etc.).
Marcadores de empresa	Los Marcadores aparecerán en la carpeta "Marcadores de la empresa" en los marcadores del navegador. No son editables por el usuario.
Ocultar barra de direcciones	Oculta la Barra de Direcciones para que el Usuario no vea la URL que está visitando
Listas blancas en el navegador (sin Universal Gateway)	Permite crear listas blancas de URL en el lado del cliente. - Los marcadores de empresa siempre están en la lista blanca - Sólo se admiten 100 URL - Utiliza la pasarela universal para listas negras y blancas ilimitadas
Listas negras y blancas basadas en la puerta de enlace	Las listas negras tienen los siguientes requisitos: - Una pasarela universal AppTec360 en funcionamiento ("Configuración general" → "Pasarela universal") - Una configuración VPN en funcionamiento con un servidor DNS especificado ("Configuración general" → "Pasarela universal" → "Configuración VPN") - Una configuración de lista negra ("Configuración general" → "Pasarela universal" →

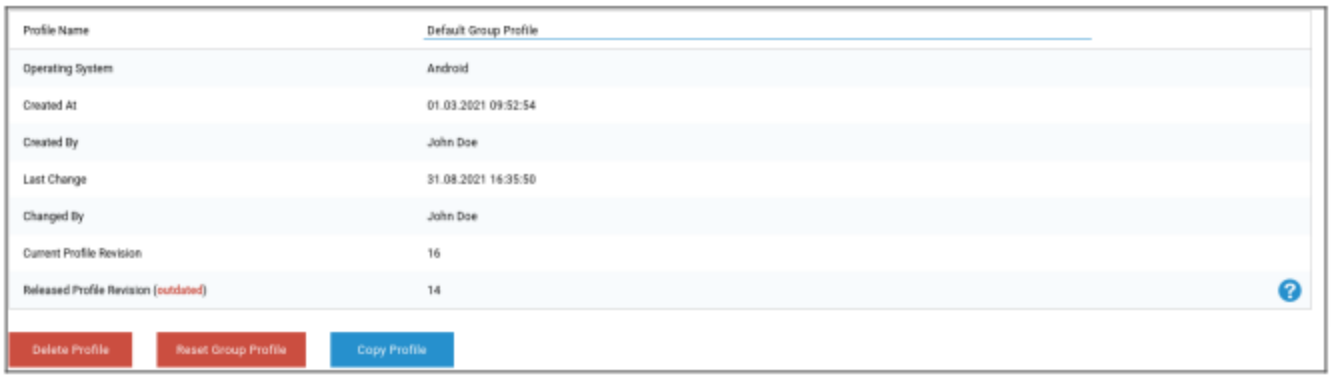
	"Lista negra de dominios") - Una conexión VPN válida en el perfil ("Gestión de conexiones" → "VPN")

Configuración Windows 10 PC

General

Resumen del perfil del grupo (sólo a nivel de grupo)

Al abrir un perfil de grupo, obtendrás una rápida visión general del perfil.



Nombre del perfil	Nombre del perfil (se puede cambiar aquí)
Sistema operativo	Sistema operativo para el que es el perfil
Creado en	Momento de la creación
Creado por	El creador del perfil
Último cambio	Hora de la última modificación del perfil
Cambiado por	Cuenta que realizó los últimos cambios
Revisión actual del perfil	Revisión del estado del perfil guardado
Revisión del perfil liberado	Revisión del perfil asignado ("Asignar ahora"). Si la etiqueta muestra "(obsoleto)" detrás del texto, significa que has guardado el perfil pero aún no lo has asignado, por lo que los dispositivos seguirán recibiendo una versión antigua.

Visión general del dispositivo (sólo a nivel de dispositivo)

El resumen del dispositivo, que contiene lo siguiente:

Nombre del PC	Nombre del PC
Cliente	Los dispositivos tipo Windows
Última localización conocida	La latitud y longitud de la última ubicación conocida de los dispositivos
Apps Obligatorias Asignadas	Número de Apps obligatorias asignadas al dispositivo
PC UID	UID del PC
Edición OS	Muestra tu Edición de Windows
Versión del SO	Versión de Windows instalada actualmente
Sistema operativo	Compilación actual de Windows
Sistema operativo	Sistema operativo instalado actualmente
Número de serie	Número de serie del dispositivo
Propiedad del dispositivo	El Tipo de Propiedad configurado
Tipo de dispositivo	El tipo de dispositivo
Enraizado	Muestra si el Dispositivo está rooteado
Cumple	Muestra si el dispositivo es conforme
Visto por última vez	Fecha y hora en que se realizaron los cambios en el perfil
Asignación de usuarios	Muestra el usuario o grupo al que está asignado actualmente este dispositivo. Puedes mover el dispositivo seleccionando un usuario o grupo diferente de la lista desplegable.

Ajustes

Permitir actualización automática	Permitir o no las actualizaciones automáticas del sistema operativo.

Config Revision (sólo a nivel de dispositivo)

Aquí obtendrá una visión general de qué perfil de grupo está asignado al dispositivo.

Si haces clic en el perfil del grupo, accederás directamente al perfil y podrás realizar ajustes.

Con el símbolo, puedes revertir las aplicaciones asignadas a la configuración del perfil de grupo.

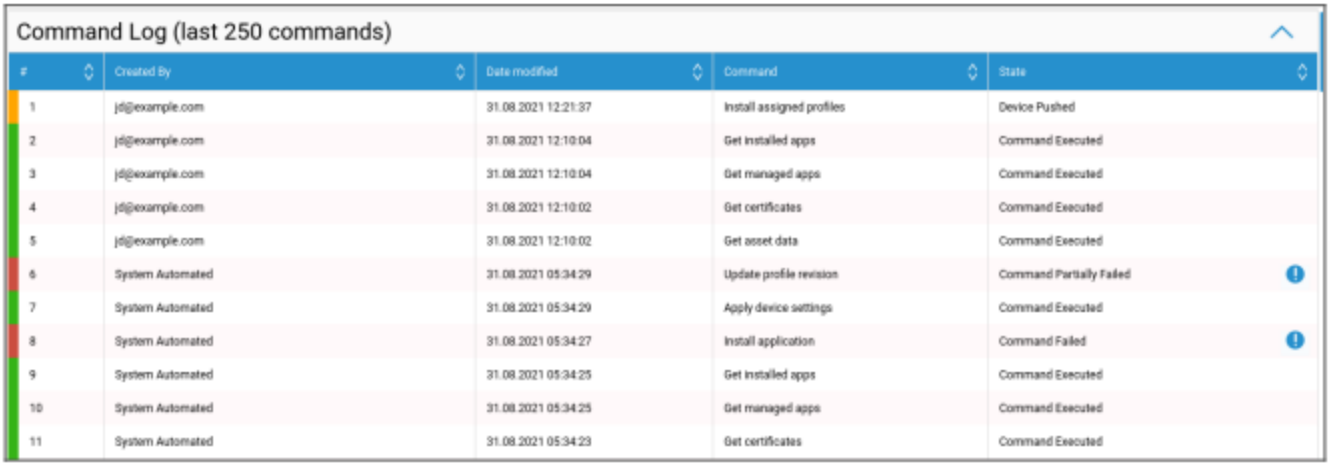
Con el símbolo, puedes restablecer el perfil del dispositivo para que no tenga ninguna configuración.

"Nueva revisión disponible" indica que el perfil de grupo se ha modificado y guardado, pero no se ha asignado. El perfil de grupo debe asignarse con "Asignar ahora" a nivel de grupo para aplicar los cambios a los dispositivos.

Registro de dispositivos (sólo a nivel de dispositivo)

Registro de comandos

Aquí puede ver qué comandos se emitieron para el dispositivo y cuál es su estado.



Los comandos creados por "Sistema automatizado" son creados automáticamente por el sistema.

Posibles estados del comando

Dispositivo Empujado	Se ha enviado una solicitud push al servicio push (por ejemplo, APNS) para indicar al dispositivo que se conecte de nuevo al servidor EMM.
Comando creado	El comando se creó en el sistema.
Orden enviada	El comando se envió al dispositivo después de que se conectara al servidor.
Orden ejecutada	El comando se ha ejecutado correctamente.
Comando fallido	El comando falló. *
Comando parcialmente fallido	Dependiendo del SO del dispositivo, algunos comandos pueden agruparse. En este fallaron algunas partes de este grupo de comandos. *
Orden ejecutada, finalmente fallida	La orden se ejecutó, pero puede que no.
Comando Repulsado	El comando fue repulsado por un usuario.
Descartado	El comando fue descartado. Por ejemplo, porque ha sido sustituido por otro comando o porque el dispositivo se ha reinscrito y se han eliminado los comandos antiguos.

*Si hay un signo de exclamación detrás del mensaje, puedes obtener más información pasando el cursor sobre el icono.

Gestión de activos (sólo a nivel de dispositivo)

Información del dispositivo

Fabricante	Fabricante del aparato
Modelo	Modelo de aparato
Número de modelo	Número de modelo
Sistema operativo	Sistema operativo
Versión del SO	Versión del SO
Número de serie	Número de serie
ExchangeID	ExchangeID
RAM total	RAM total
Resolución de la pantalla	Resolución de la pantalla
Idioma del teléfono	Idioma del dispositivo
Versión del Firmware	Versión del firmware
Versión del cliente DM	Versión del cliente de gestión de dispositivos
Versión de hardware	Versión de hardware del dispositivo
Arquitectura de la CPU	Arquitectura de la CPU (tipo de procesador)

Móvil

SIM Red del operador	Red de transportistas
Número de teléfono	Número de teléfono
Estado de itinerancia	Estado de itinerancia
IMEI	IMEI
IMSI	IMSI
Firmware del módem	Firmware del módem

Información de sincronización

Conexión DM instantánea	El dispositivo debería crear inmediatamente una conexión con AppTec
Tiempo de reintento inicial	Tiempo de reintento inicial para esta primera conexión
Reintentos de conexión	Número de reintentos de nueva conexión, tras una desconexión del Gestor de Conexiones o un error a nivel de WinInet
Tiempo máximo de sueño	Tiempo máximo de reposo tras error de envío del paquete
Primeros intentos de sincronización	Tiempo de la primera etapa tras la inscripción
Primer intervalo de reintento	Tiempo de la primera etapa tras la inscripción
Segundos reintentos de sincronización	Tiempo para la segunda fase después de la inscripción
Segundo intervalo de reintento	Tiempo para la segunda fase después de la inscripción
Reintentos regulares de sincronización	Tiempo para las etapas adicionales después de la inscripción
Intervalo regular de reintentos	Tiempo para las etapas adicionales después de la inscripción

Gestión de la seguridad

Antirrobo (sólo en el dispositivo)

Información GPS (sólo a nivel de dispositivo)

Aquí puede establecer la ubicación actual/última del dispositivo. La localización puede protegerse con una o incluso dos contraseñas - Ver: "Ajustes generales" > "Privacidad" > "Acceso GPS"

Ajustes GPS

Activar seguimiento GPS	Activa la sincronización periódica de la información GPS.
Intervalo de seguimiento	Establece el intervalo de sincronización de la información GPS.

Configuración de seguridad

Código

Longitud mínima de la contraseña	Longitud mínima de la contraseña	
Composición de la contraseña	Especifica el número de caracteres específicos que debe contener la contraseña Se componen de mayúsculas, minúsculas, números y símbolos especiales	
Calidad de la contraseña	Aquí puedes establecer la calidad de la contraseña	
	Alfanumérico	Sólo números y letras
	Numérico	Sólo números
	Numérico o Alfanumérico	Números o números y letras
Tiempo máximo de inactividad Bloqueo	Número de minutos de inactividad del usuario en el dispositivo, tras los cuales éste se bloqueará. El usuario debe desbloquear el dispositivo después de este tiempo, introduciendo su contraseña de dispositivo.	
Caducidad de la contraseña	Establece el tiempo hasta que debe establecerse una nueva contraseña	
Restricción del historial de contraseñas	Número de contraseñas utilizadas anteriormente, que no están permitidas	
Número máximo de intentos fallidos de contraseña	Número de veces que se puede introducir incorrectamente la contraseña, antes de que se realice un borrado completo del dispositivo	

Antivirus

Configuración del antivirus - Establecer la configuración del análisis	
Tipo de escaneado	Selecciona si realizar un escaneo rápido o un escaneo completo
Establecer inicio de exploración	Selecciona la hora del día a la que Windows Defender iniciará el análisis
Frecuencia de exploración	Selecciona el día en que debe ejecutarse el análisis de Windows Defender
Frecuencia de actualización de las firmas	Especifica el intervalo en horas que se utilizará para comprobar si hay firmas

Configurar el tipo de archivos a escanear	
Permitir el escaneo de archivos comprimidos	Permitir o no el escaneo de archivos comprimidos (como .zip) cuando se accede a ellos.
Permitir el escaneo de scripts	Permite o desactiva la funcionalidad de Análisis de Script de Windows Defender.
Permitir el escaneo de correos electrónicos	Permitir o no el escaneo de correos electrónicos.
Permitir el escaneo de archivos de red	Permitir o no el escaneo de archivos de red.
Permitir el escaneo completo de las unidades de red asignadas	Permitir o no el escaneo de unidades de red mapeadas (sólo se activa cuando está activado el escaneo completo).
Controlar la exploración bidireccional	Controla qué conjuntos de archivos deben supervisarse.
Permitir el escaneo completo de unidades extraíbles	Permitir o no el escaneo completo de unidades extraíbles. Sólo se inicia el escaneo completo.

Tipo de archivos a excluir del escaneo	
Ignorar tipos de archivo para escanear	Define un conjunto de extensiones de tipo de archivos. Cada extensión de archivo para cada campo.
Ignorar rutas de directorios	Define un conjunto de rutas de directorio para no escanearlas. Una ruta por campo. Ejemplos: "C:\ Ejemplo", "C:\Windows" o "C:\Usuarios".
Excluir procesos del escaneo	Excluye los archivos que hayan sido abiertos por procesos específicos de los análisis del Antivirus Microsoft Defender. . Una ruta por campo. Ejemplos: "C:\myFile.exe", "C:\Windows\myProcess.exe", "C:\myScript.bat

Ajustes adicionales	
Permitir la supervisión en tiempo real	Permitir o denegar la funcionalidad de Supervisión en tiempo real de Windows Defender
Permitir la supervisión del comportamiento	Permitir o desautorizar la función de Supervisión del Comportamiento de Windows
Permitir la protección en la nube	Permite o no que Windows Defender envíe información a Microsoft sobre cualquier problema que encuentre. Microsoft analizará esa información, obtendrá más información sobre el problema que afecta al dispositivo y ofrecerá soluciones mejoradas
	Comportamiento en el envío de muestras
Permitir la protección IOAV de Windows Defender	Activar o desactivar la protección IOAV de Windows Defender
Permitir el acceso a la interfaz de usuario "Protección de acceso" de Defenders	
Factor medio de carga de la CPU	Representa el factor medio de carga de la CPU para el análisis de Windows Defender (en porcentaje)

Tratamiento del malware	
Gravedad baja	Puedes definir para cada nivel de gravedad cómo gestiona el dispositivo el malware. Las opciones disponibles son: • Limpia • Cuarentena • Elimina • Permite • Definido por el usuario • Bloque
Gravedad moderada	
Gravedad alta	
Gravedad grave	
Días para conservar el Malware limpio	Periodo de tiempo en días que los archivos/elementos en cuarentena se almacenarán en el sistema. El valor por defecto es 0, que mantiene los elementos en cuarentena y no los elimina automáticamente. El valor máximo es 90.

Centro de seguridad

Centro de Seguridad de Windows - Configuración de la Seguridad de Windows	
Desactivar la interfaz de usuario de protección frente a virus y amenazas	
Ocultar la IU de recuperación de datos del ransomware	
Desactivar la IU de protección de cuentas	
Desactiva la interfaz de usuario del cortafuegos y la protección de red	
Desactivar la interfaz de usuario de control de aplicaciones y navegador	
No permitir cambios en la protección contra Exploit	No permitir al usuario realizar cambios en la configuración de la protección contra Exploit
Desactivar la IU de seguridad del dispositivo	
Ocultar la solución de problemas del TPM	Ocultar la configuración de solución de problemas del TPM
Desactivar el botón Borrar TPM	
Desactivar la interfaz de rendimiento y salud del dispositivo	
Desactivar la IU de opciones familiares	

Personaliza las tostadas	
Activar información de soporte personalizada	Activa la opción de mostrar información de contacto de asistencia personalizada para tu empresa en la parte inferior derecha de la aplicación del centro de seguridad.
Dirección de correo electrónico	Establecer la dirección de correo electrónico de la empresa
Nombre de la empresa	Establecer el nombre de la empresa
Teléfono de la empresa	Establecer el teléfono de la empresa
URL de ayuda	Establecer la URL de ayuda de la empresa

Ajustes adicionales	
Desactivar notificaciones	Desactiva la visualización de las Notificaciones del Centro de Seguridad de Windows Defender.
Ocultar las recomendaciones de actualización del firmware del TPM	Oculta la recomendación de actualizar el Firmware TPM cuando se detecte un firmware vulnerable.
Mostrar el nombre de la empresa y las opciones de contacto	Muestra el nombre de tu empresa y las opciones de contacto en una tarjeta de contacto desplegable en el Centro de seguridad de Windows Defender.
Ocultar el Arranque Seguro	Ocultar el área de Arranque de Seguridad.
Ocultar el control del área de notificación de seguridad	Ocultar el control del área de notificación de Seguridad de Windows.

Configuración del cortafuegos

Configuración del cortafuegos - Configuración global	
Ignorar la autenticación establecida	Ignorar todo el conjunto de autenticación si no admiten todas las suites de autenticación especificadas en el conjunto
Tipo de cola de paquetes	Especifica cómo se activa el escalado del software en el lado de recepción, tanto para la ruta de recepción encriptada como para la ruta de reenvío transparente en el escenario de pasarela de túnel IPsec.
Desactivar realizar filtrado FTP con estado	Si está desactivado, no realizará el filtrado del Protocolo de Transferencia de Archivos (FTP) con estado para permitir conexiones secundarias
Tiempo de inactividad de la asociación de seguridad	Este campo configura el tiempo de inactividad de la asociación de seguridad, en segundos. Las asociaciones de seguridad se eliminan después de que no se vea tráfico de red durante este periodo de tiempo especificado.
Codificación de clave precompartida	Establece la codificación de la clave precompartida
Excepciones IPSec	Configurar las excepciones del Protocolo de Internet
Comprobación de la lista de revocación de certificados	

Perfiles de cortafuegos (Perfil de dominio / Perfil privado / Perfil público)	
Activar Firewall para este perfil	
Desactivar notificaciones	Desactivar la visualización de notificaciones al usuario cuando se bloquea la escucha de una aplicación en un puerto.
Bloquear las respuestas unidifusión a las difusiones multidifusión	
Hacer cumplir las reglas autorizadas del cortafuegos de aplicaciones	Si no se aplica, las reglas autorizadas del cortafuegos de aplicaciones en el almacén local se ignoran y no se aplican
Aplicar reglas globales de cortafuegos de puertos	Si no se aplica, las reglas globales del cortafuegos de puertos del almacén local se ignoran y no se aplican. La configuración sólo tiene sentido si se establece o enumera en el almacén de la directiva de grupo o si se enumera desde el almacén GroupPolicyRSoPStore
Aplicar las reglas del cortafuegos	Si no se aplica, las reglas del cortafuegos del almacén local se ignoran y no se aplican
Aplicar reglas de seguridad de conexión	Si no se aplica, las reglas de seguridad de conexión del almacén local se ignoran y no se aplican.
Acción de salida por defecto	La acción que el cortafuegos realiza por defecto en las conexiones salientes
Acción de entrada por defecto	La acción que el cortafuegos realiza por defecto en las conexiones entrantes
Desactivar el modo Sigilo	El modo oculto es un mecanismo del Firewall de Windows que ayuda a impedir que los usuarios malintencionados descubran información sobre los ordenadores de la red y los servicios que ejecutan.
Desactivar la prevención de la respuesta al tráfico no solicitado	Si están desactivadas, las reglas del modo oculto del cortafuegos no deben impedir que el ordenador host responda al tráfico de red no solicitado si ese tráfico está protegido por IPsec

Reglas del cortafuegos

Reglas del cortafuegos	
Nombre	Nombre de la norma
Descripción	Descripción de la norma
Acción	Especifica si esta regla bloqueará el tráfico o lo permitirá. Ten en cuenta que la opción Bloquear también podría bloquear el tráfico (dependiendo del resto de la configuración) entre el servidor MDM y el Dispositivo
Dirección	
Activar traspasar bordes (Sólo disponible cuando **Dirección** está configurada como **tráfico entrante**)	Indica que el tráfico entrante específico puede pasar por túneles a través de NAT y otros dispositivos de borde utilizando la tecnología de túneles Teredo.

Programas y servicios	
Definir aplicaciones, todo lo demás	Si no está activada, considerará todas las solicitudes
Nombre de la familia de paquetes	El nombre de la familia de paquetes a la que se aplicará la regla.
Ruta del archivo de la aplicación	La aplicación completa como C:\Windows\System\Notepad.exe a la que se aplicará la regla
Nombre binario completo	El Nombre Binario Completamente Cualificado al que se aplicará la regla. Un FQBN es una cadena de la siguiente forma: {Publisher\Product\Filename,Version}
Nombre del servicio	Introduce el nombre de un Servicio (por ejemplo, "EventLog"). Puedes obtener una lista de Nombres de Servicio en Powershell ejecutando el comando "Get-Service".

Protocolos y puertos				
Protocolo	El protocolo utilizado por la regla.			
	Valores disponibles: - Cualquiera - A medida - HOPORT - ICMPv4 - IGMP - TCP - UDP - IPv6 - Ruta IPv6 - IPv6-Frag - GRE - ICMPv6 - IPv6-NoNxt - Opciones IPv6 - VRRP - PGM - L2TP	Cuando se ajusta a Personalizado	Introduce un número de protocolo entre 0 y 255	El número de protocolo
		Cuando se establece en TCP o UDP	Especifica los puertos locales, de lo contrario se utilizarán todos	Puertos locales que utilizará la regla, también se permiten puertos de rango
			Puerto local	Un solo puerto o un rango de puertos. Por ejemplo, 100-120,200,300-320.
			Especifica los puertos remotos, de lo contrario se utilizarán todos	Puertos remotos que utilizará la regla, también se permiten puertos de rango
			Puerto remoto	Un solo puerto o un rango de puertos. Por ejemplo, 100-120,200,300-320.

Alcance	
Especifica IP locales, cualquier IP en caso contrario	Conjunto de IPs locales, también puede ser un rango de IPs separadas por -.
Dirección IP local	Conjunto de IPs individuales o un rango de IPs separadas por -.
Especifica IP remotas, cualquier IP remota en caso contrario	Especifica un conjunto de IPs remotas, puede ser también un rango de IPs separadas por "-".
Dirección IP remota	Especifica IPs individuales o un rango de IPs
Fichas	Tokens que se pueden establecer junto con Direcciones Remotas. Los tokens Intranet, RmtIntranet y Ply2Renders son compatibles con Windows 10, versión 1809 y posteriores.

Ajustes avanzados	
Especifica los perfiles, de lo contrario se utilizarán todos	Si se desactiva, se utilizarán todos los perfiles
Dominio	Perfil del dominio
Privado	Perfil privado
Público	Perfil público
Especifica las interfaces, de lo contrario se utilizarán todas	Si se desactiva, se utilizarán todas las interfaces
Red de área local	Interfaz de red de área local
Acceso remoto	Interfaz de acceso remoto
Inalámbrico	Interfaz inalámbrica

Directores locales	
Añadir usuarios locales autorizados	Permitir añadir una lista de usuarios locales que utilizarán esta regla
Usuarios autorizados	Lista de usuarios locales autorizados para esta regla. El usuario debe estar en formato del lenguaje de Definición de la Descripción de Seguridad (SDDL), por ejemplo, PC_NAME\USERNAME. Este campo no debe rellenarse si se establece un nombre de servicio para utilizar esta regla

Configuración de restricciones

Funcionalidad del dispositivo

Permitir tarjeta SD	Permitir el uso de una tarjeta SD
Permitir cámara	Permitir el uso de la cámara
Permitir Servicio de Localización	Permitir el servicio de localización del dispositivo
Permitir la carga lateral de aplicaciones	Permitir la instalación de aplicaciones de fuentes desconocidas
Permitir Modo Desarrollador	Permite el modo desarrollador
Permitir itinerancia de datos móviles	Permitir la itinerancia de datos móviles
Permitir Cortana	Permitir el asistente de voz Cortana
Permitir que la Búsqueda utilice la Localización	Permitir que la búsqueda utilice la ubicación
Permitir añadir una cuenta de correo electrónico que no sea de Microsoft	Especifica si el usuario puede añadir cuentas de correo electrónico que no sean MSA.
Permitir la conexión de cuentas Microsoft	Especifica si se permite utilizar la cuenta MSA para la autenticación y los servicios de conexión no relacionados con el correo electrónico.
Permitir Sincronizar Mi Configuración	Permite sincronizar los ajustes de todo el dispositivo
Nombres de dominio protegidos para empresas	Especifica los nombres de dominio de empresa separados por ";".
Permitir al usuario desactivar la Restauración del Sistema	Permite al usuario desactivar la Restauración del Sistema. **ADVERTENCIA** Esta función sólo debe utilizarse en dispositivos que sean propiedad o estén proporcionados por la empresa u organización o en un dispositivo propiedad del usuario, cuando éste permita que el dispositivo sea gestionado totalmente por la empresa. Si deshabilitas esta configuración de directiva, se desactiva

	Restaurar sistema y no se puede acceder al Asistente para Restaurar sistema. También se desactiva la opción de configurar Restaurar sistema o crear un punto de restauración a través de Protección del sistema.
Permitir la baja de usuarios	Permite al usuario eliminar la parte corporativa del dispositivo y desconectarse así de los servidores AppTec360. Si esto ocurre, ya no será posible gestionar el dispositivo **¡ADVERTENCIA!** Esta función sólo debe utilizarse en dispositivos que sean propiedad o estén proporcionados por la empresa u organización o en un dispositivo propiedad del usuario, cuando éste permita que el dispositivo sea gestionado completamente por la empresa. Si deshabilitas esta configuración de directiva, los usuarios no podrán eliminar las inscripciones en MDM. Especifica si el usuario puede eliminar la cuenta del puesto de trabajo a través del panel de control del puesto de trabajo. El servidor MDM siempre puede eliminar la cuenta de forma remota.

BitLocker

Configuración de BitLocker

Ajustes generales	
Exigir la encriptación del dispositivo	Pedir a los usuarios que activen la encriptación del dispositivo.Dependiendo de la edición de Windows y de la configuración del sistema, se puede pedir a los usuarios: - Para confirmar que la encriptación de otro proveedor no está activada. - Para desactivar el Cifrado de unidad BitLocker y volver a activar BitLocker.
Métodos de encriptación	
Método de cifrado para unidades del sistema operativo	
Método de encriptación para unidades de datos fijas	
Método de cifrado para unidades de datos extraíbles	
Desactivar la advertencia sobre la encriptación de discos de terceros	Desactiva el aviso de advertencia sobre un servicio de encriptación de disco de terceros que se esté utilizando en el dispositivo. A partir de Windows 10, versión 1803, esta configuración sólo es compatible con los dispositivos unidos a Azure Active Directory.
Permitir ejecutar la encriptación mientras un usuario no administrador está conectado	Sólo se admite para dispositivos unidos a Azure Active Directory

Extensiones AppTec360	
Encriptación silenciosa	Si se selecciona junto con "Requerir encriptación del dispositivo", el Servicio de Gestión de AppTec360 ejecutará una encriptación silenciosa automática de las unidades del dispositivo.
Generar automáticamente credenciales de usuario	La unidad del SO encriptada estará protegida con credenciales de usuario generadas automáticamente. O bien un PIN TPM, cuando se disponga de un TPM, o bien una contraseña textual de 6 dígitos. Las credenciales generadas se envían a la dirección de correo electrónico registrada para el dispositivo en cuestión. Si esta opción está desactivada, la única protección posible para el cifrado silencioso es utilizar el TPM. En ese caso, para los dispositivos sin TPM, el cifrado silencioso fallará.
Cifrar unidades fijas	Cualquier unidad de datos fija disponible también estará encriptada y protegida con "Desbloqueo automático" mediante una clave almacenada en la unidad del SO.

Configuración de la unidad OS

Requerir autenticación adicional al inicio	Este ajuste te permite configurar si BitLocker requiere una autenticación cada vez que se inicia el ordenador. Este ajuste se aplica durante la configuración de BitLocker. Si activas esta opción, los usuarios pueden configurar opciones avanzadas de inicio en el asistente de configuración de BitLocker.
Bloquear BitLocker sin un TPM compatible	
Sólo TPM	
TPM y PIN	
TPM y llave	
TPM, llave y PIN	Si quieres exigir el uso de un PIN y una unidad flash USB (llave), el usuario debe configurar BitLocker utilizando la herramienta de línea de comandos "manage-bde" en lugar del asistente de configuración del Cifrado de unidad BitLocker.

Requerir longitud mínima del PIN

	Caracteres mínimos

Configurar el mensaje de recuperación previo al arranque y la URL	Configura todo el mensaje de recuperación o sustituye la URL existente que se muestra en la pantalla de recuperación previa a la clave de arranque cuando la unidad del SO está bloqueada. Nota: No todos los caracteres e idiomas son compatibles con el prearranque. Se recomienda encarecidamente que compruebes que los caracteres que utilizas aparecen correctamente en la pantalla de recuperación del prearranque.
	Opción de mensaje de recuperación previo al arranque
	Mensaje de recuperación personalizado
	URL de recuperación personalizada

Opciones de recuperación de la unidad OS		Esta configuración te permite controlar cómo se recuperan las unidades del sistema operativo protegidas por BitLocker en ausencia de las credenciales necesarias. Este ajuste se aplica durante la configuración de BitLocker. Por defecto, se permite un agente de recuperación de datos basado en certificados, las opciones de recuperación pueden ser especificadas por el usuario, incluyendo la contraseña de recuperación y la clave de recuperación, y no se realiza una copia de seguridad de la información de recuperación en AD DS.
	Agente de recuperación de datos basado en certificados de bloque	Especifica si se puede utilizar un agente de recuperación de datos con unidades del sistema operativo protegidas por BitLocker. Antes de poder utilizar un agente de recuperación de datos, debe añadirse desde el elemento Políticas de clave pública de la Consola de administración de directivas de grupo o del Editor local de directivas de grupo. Consulta la Guía de Implantación del Cifrado de Unidades BitLocker en Microsoft TechNet para obtener más información sobre cómo añadir agentes de recuperación de datos.
	Configuración de la contraseña de recuperación de BitLocker	
	Configuración de la clave de recuperación de BitLocker	
	Guardar la información de recuperación de BitLocker en los Servicios de Dominio de Active Directory	
	Configuración del almacenamiento de recuperación AD DS BitLocker	Almacenar el paquete de claves permite recuperar datos de una unidad que se ha dañado físicamente.
	Requerir almacenamiento de datos de recuperación en AD DS	Evita que los usuarios activen BitLocker a menos que el ordenador esté conectado al dominio y

Ajustes fijos del accionamiento	
Opciones de recuperación de unidades fijas	Esta configuración te permite controlar cómo se recuperan las unidades fijas protegidas con BitLocker en ausencia de las credenciales necesarias. Este ajuste se aplica durante la configuración de BitLocker. Por defecto, se permite un agente de recuperación de datos basado en certificados, las opciones de recuperación pueden ser especificadas por el usuario, incluyendo la contraseña de recuperación y la clave de recuperación, y no se realiza una copia de seguridad de la información de recuperación en AD DS.
Agente de recuperación de datos basado en certificados de bloque	
Configuración de la contraseña de recuperación de BitLocker	
Configuración de la clave de recuperación de BitLocker	
Guardar la información de recuperación de BitLocker en los Servicios de Dominio de Active Directory	
Configuración del almacenamiento de recuperación AD DS BitLocker	Almacenar el paquete de claves permite recuperar datos de una unidad que se ha dañado físicamente.
Requerir almacenamiento de datos de recuperación en AD DS	Evita que los usuarios habiliten BitLocker a menos que el ordenador esté conectado al dominio y la copia de seguridad de la información de recuperación de BitLocker en AD DS se realice correctamente. Nota: La contraseña de recuperación se genera automáticamente.
Denegar el acceso de escritura a unidades fijas no protegidas	

Configuración de la unidad extraíble	
Denegar el acceso de escritura a unidades extraíbles desprotegidas	Deniega el acceso de escritura a las unidades de datos extraíbles que no estén protegidas por Bitlocker. Nota: Si "Discos extraíbles: Denegar acceso de escritura" está activada en la política de grupo, se ignorará esta configuración de política.
Denegar el acceso de escritura a dispositivos configurados en otra organización	Sólo se dará acceso de escritura a las unidades cuyos campos de identificación coincidan con los campos de identificación del ordenador. Estos campos están definidos por la configuración de la directiva de grupo "Proporciona los identificadores únicos de tu organización".

Estado de BitLocker

Aquí puede ver el estado actual de las unidades cifradas con BitLocker

C [OS Drive]
Estado de encriptación
Cifrado (%)
Estado de protección
Método de encriptación
Protectores de llaves
Recuperar contraseña

Con un clic en el botón "Girar contraseña de recuperación" puede girar la contraseña de recuperación de BitLocker.

Gestión de certificados

Lista de certificados

Aquí se muestra una lista de los certificados que están instalados en el dispositivo que se está visualizando.

Configuración de certificados

Aquí puede configurar los certificados y cómo se instalarán en el dispositivo.

Certificado de confianza	
Descripción	Descripción del certificado
Alcance	Ámbito de despliegue del certificado: Usuario actual vs Dispositivo
Almacén de certificados	"Certificados no fiables" sólo está disponible a partir de Windows 10, versión 1803
Archivo de certificado	Subir un archivo PKCS#1

Certificado de identidad			
Descripción	Descripción del certificado		
Alcance	Ámbito de despliegue del certificado: Usuario actual vs Dispositivo		
Ubicación clave	El proveedor de almacenamiento de claves en el que instalar la clave privada.		
		TPM. Fallo si no hay TPM	
	TPM. Si no hay TPM, vuelve al Software KSP		
	Proveedor de almacenamiento de claves de software		Marcar la clave privada como exportable
	Windows Hello para empresas	Nombre del contenedor	Especifica el nombre del contenedor de Windows Hello for Business (anteriormente conocido como Microsoft Passport for Work).
		Texto del PIN	Especifica el texto personalizado que se mostrará en la solicitud de PIN de Windows Hello for Business durante la inscripción del certificado.
Credencial	Subir un archivo PKCS#12		

SCEP

Descripción	Descripción del servidor SCEP		
Alcance del despliegue	Alcance del despliegue del certificado: Dispositivo actual vs Usuario		
URL del servidor SCEP	Uno o varios servidores que emiten certificados a través de SCEP		
Asunto	Representación de un nombre X.500. Por ejemplo, "C=US, O=Microsoft Corporation, CN=foo, 1.2.5.3=bar".		
Nombres alternativos del tema	Tipo	Dirección de correo electrónico	
		DNS	
		URI	
		Nombre de usuario principal (UPN)	
Huella dactilar CA	La huella digital SHA1 del certificado de la Autoridad de Certificación. E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5		
Unidades del periodo de validez	Días, meses o años		
Periodo de validez			
Desafío	Se utiliza como secreto precompartido para la inscripción automática		
Reintentos	El número de veces que el dispositivo debe reintentarlo si el servidor envía una respuesta PENDIENTE. El valor por defecto es 5. El valor máximo es 30.		
Retraso de reintento	Número de minutos que hay que esperar antes de reintentar. El valor por defecto es 5. El valor mínimo es 1.		
Tamaño de la llave	Tamaño de la clave en bits		
Algoritmo hash	Familia de algoritmos hash		
Claves de uso	La extensión de uso de la clave define la finalidad (por ejemplo, cifrado, firma) de la clave contenida en el certificado. Es necesario seleccionar al menos una de las opciones "Firma digital" o "Cifrado de claves".		

Uso ampliado de la llave	Especifica los usos extendidos de la clave.Sujeto a la configuración del servidor SCEP. Especifica la lista de OID correspondientes, por ejemplo 1.3.6.1.5.5.7.3.2 (Autenticación de cliente)		
Ubicación clave	El proveedor de almacenamiento de claves en el que instalar la clave privada.		
		TPM. Fallo si no hay TPM	
	TPM. Si no hay TPM, vuelve al Software KSP		
	Proveedor de almacenamiento de claves de software		
	Windows Hello para empresas	Nombre del contenedor	Especifica el nombre del contenedor de Windows Hello for Business (anteriormente conocido como Microsoft Passport for Work).
		Texto del PIN	Especifica el texto personalizado que se mostrará en la solicitud de PIN de Windows Hello for Business durante la inscripción del certificado.

Gestión de conexiones

Wifi

En esta configuración, realice la preconfiguración de los dispositivos de usuario final para el acceso a los puntos de acceso internos

Identificador del Conjunto de Servicios (SSID)	SSID de la red a la que se establecerá la conexión
Autounión	Activar la unión automática a la red
Red oculta	Activar, en caso de que el AP no emita el SSID

Tipo de seguridad

Establecer el tipo de seguridad AP

Sistema abierto WEP	
Contraseña	Contraseña para el PA

WPA PSK	
Contraseña	Contraseña para el PA

WPA EAP	
Tipo de autenticación	Tipo de autenticación, sólo posible con "PEAP-MSCAHPv2"
Reconexión rápida	Los dispositivos pueden cambiar entre Puntos de Acceso, sin tener que autenticarse de nuevo
Acceso de invitados	El usuario no tiene cuenta, por lo que debe registrarse como invitado
Controles de cuarentena	El cliente debe realizar comprobaciones NAP (Network Access Protection) y compartir los resultados con el sistema, que entonces decide si el cliente puede conectarse.
Requerir enlace criptográfico	La autenticación sólo es posible mediante el enlace criptográfico
Validación del servidor	El cliente comprueba si el certificado del servidor es válido. Si es así, se establecerá una conexión
Solicitar certificados	Permite al usuario aceptar certificados no fiables
Nombres de servidores	Ofrece la opción de mostrar el nombre del Servidor RADIUS, que ofrece la autenticación y autorización de red

WPA2-PSK	
Contraseña	Contraseña AP

WPA2 EAP	
Tipo de autenticación	Tipo de autenticación, sólo posible con "PEAP-MSCAHPv2"
Reconexión rápida	
Acceso de invitados	
Controles de cuarentena	Activa la protección de acceso a la red NAP
Requerir enlace criptográfico	La autenticación sólo es posible mediante el enlace criptográfico
Validación del servidor	
Solicitar certificados	Solicita un certificado de servidor validado, un nombre o un certificado raíz de autenticación (CA)
Nombres de servidores	Listado de los servidores en los que deben confiar los dispositivos
Ninguno	No hay seguridad establecida
Utilizar servidor proxy	Uso de un servidor proxy
Dirección del servidor	Dirección del servidor proxy
Puerto del servidor	Puerto del servidor proxy

Utilizar servidor proxy

Activar el uso del servidor proxy.

Dirección del servidor	Dirección del servidor proxy utilizado por esta red.
Puerto del servidor	Puerto del servidor proxy utilizado por esta red.

Restricciones wifi

Aquí puedes definir varias restricciones Wifi.

Permitir WiFi	Permitir/denegar WiFi
Permitir compartir Internet	Permitir el uso de un Hotspot
Permitir la conexión automática a puntos de acceso WiFi Sense	Permitir la conexión automática a puntos de acceso WiFi Sense
Permitir la configuración manual de WiFi	Permitir al usuario conectarse a redes WiFi que no hayan sido definidas por AppTec
Frecuencia de exploración WLAN	Establece el intervalo de escaneo WLAN. Aquí, un valor más alto aumenta la capacidad de reconocer redes WIFI.

VPN

Realice aquí los ajustes adecuados para configurar las conexiones VPN

Nombre de la conexión	Nombre de la conexión indicada		
Tipo de VPN	Una conexión VPN por aplicación se utiliza para proteger el tráfico de determinadas aplicaciones.		
	VPN	Siempre activado	Esto conectará automáticamente la VPN al iniciar sesión y permanecerá conectada hasta que el usuario la desconecte manualmente.
	VPN por aplicación	Aplicaciones VPN	Definir las aplicaciones que utilizan esta conexión VPN
		Bloqueo por aplicación	El Bloqueo por Aplicación hace que las aplicaciones seleccionadas sólo tengan conectividad a través de esta conexión VPN. Esta función depende del Firewall de Windows Defender.
	Perfil WIP	Dominio WIP para esta conexión	ID de empresa, necesario para conectar este perfil VPN con una política de Protección de Información de Windows (WIP)

Tipo de conexión

AppTec360 VPN	
Para "AppTec360 VPN" es necesario que se permita la carga lateral de aplicaciones. Activa "Permitir carga lateral de aplicaciones" en "Gestión de seguridad" → "Configuración de restricciones" → "Funcionalidad del dispositivo".	
Configuración de la puerta de enlace	Para configurar una conexión VPN con lista negra, selecciona una configuración VPN con un servidor DNS especificado. Puedes establecer una configuración VPN en "Configuración general" → "Pasarela universal" → "Configuración VPN".

IKEv2		
Servidores	Lista de servidores VPN	
Dispositivo Túnel	Activar la conexión antes de que el usuario inicie sesión.	
Método de autenticación	EAP	EAP XML
	Certificados de máquinas	
Algoritmo de encriptación		
Algoritmo de comprobación de integridad		
Grupo de Diffie-Hellman		
Algoritmo de transformación de cifrado		
Algoritmo de transformación de autenticación		
Grupo de secreto perfecto hacia adelante (PFS)		

PPTP		
Servidores	Lista de servidores VPN	
Método de autenticación	EAP	EAP XML

L2TP		
Servidores	Lista de servidores VPN	
Método de autenticación	EAP	EAP XML
Algoritmo de encriptación		
Algoritmo de comprobación de integridad		
Grupo de Diffie-Hellman		
Algoritmo de transformación de cifrado		
Algoritmo de transformación de autenticación		
Grupo de secreto perfecto hacia adelante (PFS)		

Automático		
Servidores	Lista de servidores VPN	
Método de autenticación	EAP	EAP XML

Configuraciones VPN genéricas

Recordar las credenciales en cada inicio de sesión	
Registrar direcciones IP con DNS interno	
Reglas de filtrado del tráfico de red	Limita la conexión VPN al conjunto de reglas definido.
Lista de búsqueda de sufijos DNS	Sufijos DNS para añadir a la lista de búsqueda DNS para enrutar nombres cortos.
Reglas de la tabla de políticas de resolución de nombres (NRPT)	Las reglas de la tabla de Políticas de Resolución de Nombres (NRPT) definen cómo el DNS resuelve los nombres cuando se conecta a la VPN.
Detección de redes de confianza	Lista de sufijos DNS para identificar la red de confianza.
Túnel dividido	La tunelización dividida significa que el tráfico puede pasar por cualquier interfaz, según determine la pila de red.
Rutas de túnel divididas	Lista de rutas que deben añadirse a la tabla de enrutamiento de la interfaz VPN.
Configuración del proxy	Configura el Proxy utilizado con esta red
Dirección del apoderado	Dirección del servidor proxy como un nombre de host completo o una dirección IP.
Puerto	Puerto del servidor proxy.
URL de configuración automática del proxy	URL para recuperar automáticamente la configuración del proxy.

Restricciones VPN

Aquí puede definir varias restricciones de VPN.

Permitir configuración VPN	Esta directriz permite/prohíbe al usuario desactivar y cambiar la configuración de la VPN
Permitir VPN por móvil	Permite/prohibe al dispositivo establecer una conexión VPN, si el dispositivo está utilizando datos móviles
Permitir la itinerancia VPN por móvil	Permite/prohibe al dispositivo establecer una conexión VPN, si el dispositivo está en itinerancia

Bluetooth

Aquí puede establecer, si Bluetooth debe ser permitido/prohibido.

Permitir Bluetooth	Activar/desactivar Bluetooth

Gestión PIM

Sincronización activa de Exchange

Configuración de la cuenta ActiveSync en el dispositivo del usuario final

Nombre de la cuenta	Nombre de la cuenta de correo electrónico
Nombre del host del servidor	Dirección del servidor/FQDN
Nombre de dominio	Dominio del servidor
Dirección de correo electrónico	Dirección de correo electrónico
Nombre de usuario	Nombre de usuario
Contraseña de usuario	Opcionalmente, aquí ya puedes adjuntar una contraseña al usuario
Utiliza SSL	Utilizar conexión SSL
Intervalo de sincronización	Aquí se puede establecer el intervalo de sincronización Sincronización manual = El usuario debe descargar sus correos y realizar una sincronización manual
Filtro de edad del correo	Cantidad de tiempo, hasta que los correos electrónicos deben sincronizarse Sin filtro = ilimitado
Nivel de registro	Establecimiento de los niveles de registro para el tráfico de ActiveSync
Sincronizar correo electrónico	Activado = los correos electrónicos están sincronizados
Sincronizar contactos	Activado = los contactos están sincronizados
Sincronizar Calendario	Activado = el calendario está sincronizado
Sincronizar tareas	Activado = las tareas están sincronizadas

Correo electrónico

Establecimiento de cuentas POP3/IMAP4 en el dispositivo del usuario final.

Descripción de la cuenta	Nombre de la cuenta de correo electrónico
Nombre del remitente	Nombre del remitente mostrado
Nombre de dominio	Nombre de dominio de la cuenta de correo electrónico
Dirección de correo electrónico	Dirección de correo electrónico del usuario
Nombre de usuario	Nombre de usuario
Contraseña de usuario	Opcionalmente, aquí ya puedes adjuntar una contraseña al usuario
Credenciales alternativas del servidor saliente	Aquí se puede definir, si se requieren otras credenciales para el servidor saliente
Nombre de dominio saliente	Nombre de dominio saliente
Nombre de usuario del servidor saliente	Nombre de usuario del servidor saliente
Contraseña del servidor saliente	Contraseña del servidor saliente
Protocolo de correo electrónico	POP3 o IMAP4, puede utilizarse como protocolo
Nombre de host del servidor de correo entrante	Nombre de host del servidor de correo entrante
Utiliza SSL para los correos entrantes	Utiliza SSL para los correos entrantes
Nombre del host del servidor de correo saliente	Nombre de host del servidor de correo saliente
Utilizar SSL para los correos salientes	Utiliza SSL para los correos salientes
Autenticación del servidor saliente	Se requiere una autenticación del servidor saliente
Intervalo de sincronización	Aquí se puede establecer el intervalo de sincronización Sincronización manual = El usuario debe descargar sus correos y realizar una sincronización manual
Filtro de edad del correo	Cantidad de tiempo, hasta que los correos electrónicos deben sincronizarse Sin filtro = ilimitado

Gestión de aplicaciones

Enterprise App Manager

Aplicaciones instaladas

Aquí se muestra una lista de las aplicaciones que están instaladas actualmente en el dispositivo que se está visualizando.

Aplicaciones obligatorias

Aquí puedes configurar una lista de aplicaciones que son obligatorias en el dispositivo.

Esta lista se comprobará cada vez que el dispositivo se conecte al MDM e instalará todas las aplicaciones de esta lista que no estén instaladas en el dispositivo, independientemente de si la aplicación se ha desinstalado o no se ha instalado nunca.

Puedes subir Windows 10 In-House Apps y luego añadirlas a esta lista o puedes añadir configuraciones de Microsoft Office que necesitan ser configuradas de antemano en "General Settings" > "App Management" > "Microsoft Office".

Restricciones de las aplicaciones del sistema

Apps de la bandeja de entrada
Permitir Alarmas y Reloj
Permitir calculadora
Permitir cámara
Permitir contacto de apoyo
Permitir Cortana
Permitir Explorador de archivos
Permitir Empezar
Permitir Música Groove
Permitir mapas
Permitir mensajería
Permitir Microsoft Edge
Permitir películas y TV
Permitir dinero
Permitir Noticias
Permitir OneDrive
Permitir OneNote
Permitir Calendario y Correo de Outlook
Permitir a la gente
Permitir teléfono
Permitir fotos
Permitir Powerpoint
Permitir ajustes
Permitir Skype
Permitir deportes
Permitir tienda
Permitir grabadora de voz
Permitir Cartera
Permitir el tiempo

Permitir el Feedback Hub de Windows
Permitir palabra
Permitir Xbox

Páginas de configuración
Permitir cuentas Lugar de trabajo
Permitir información avanzada
Permitir el Rincón de las Aplicaciones
Permitir Bloquear y Filtrar
Permitir perfil de color
Permitir modo de conducción
Permitir correo electrónico y cuentas
Permitir Ecualizador
Permitir teclado
Permitir barra de navegación
Permitir Modo Avión de Red
Permitir compartir Internet en red
Permitir Servicios de Red
Permitir Red Wi-Fi
Permitir Bluetooth del Sistema PC
Permitir valorar tu dispositivo
Permitir actualización de restauración
Permitir compartir
Permitir inicio
Permitir Tiempo Idioma
Permitir Tiempo Región
Permitir la pantalla de bloqueo predeterminada de Windows
Permitir cuenta de trabajo o escolar

Listas negras y blancas

En "Listas negras y blancas", puede elegir entre el modo "Lista blanca" y el modo "Lista negra".

Lista blanca	Sólo las aplicaciones y servicios que se añadan a la lista podrán instalarse en el dispositivo del usuario final. Si ya están preinstalados en el dispositivo del usuario final, se activarán y configurarán para que el usuario pueda ejecutarlos.
	Todas las demás apps que no se añadan a la lista no podrán instalarse en el dispositivo del usuario final. Si ya están preinstaladas en el dispositivo del usuario final, se desactivarán y se configurarán para que el usuario no pueda ejecutarlas.
Lista negra	Las aplicaciones y servicios que se añadan a la lista no podrán instalarse en el dispositivo del usuario final. Si ya están preinstalados en el dispositivo del usuario final, se desactivarán y se configurarán para que el usuario no pueda ejecutarlos.
	Todas las demás aplicaciones que no se añadan a la lista pueden instalarse en el dispositivo del usuario final. Si ya están preinstaladas en el dispositivo del usuario final, se activarán y configurarán para que el usuario pueda ejecutarlas.

A través de , puedes añadir otras aplicaciones o servicios a la lista de los utilizados actualmente.

A través de , puede añadir otras aplicaciones o servicios a la lista de inactivos.

Puede añadir una aplicación desde la "Tienda de aplicaciones de Windows" o introducir directamente un "Identificador de aplicación" para añadirla a la lista negra o blanca.

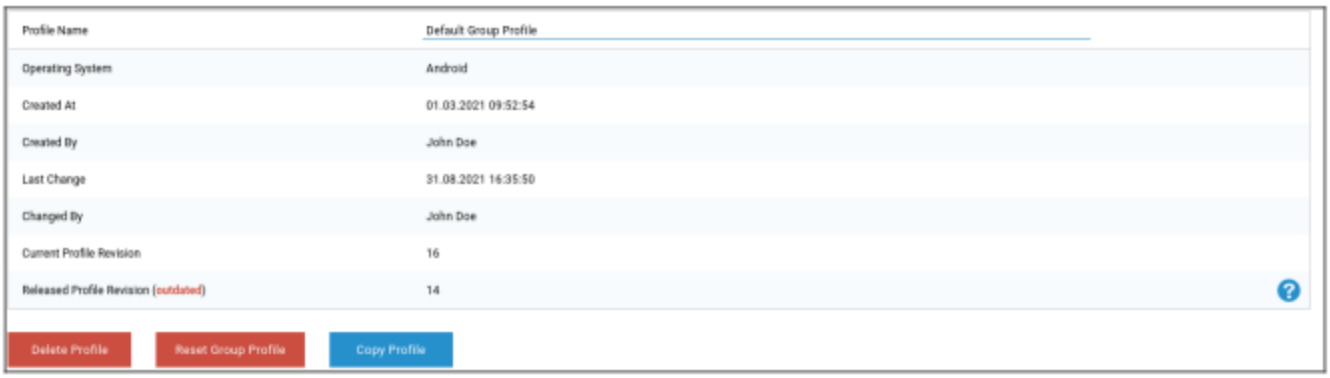
Configuración de MacOS

Dependiendo de si ha seleccionado un perfil o un dispositivo, la pantalla y sus subpuntos son diferentes - ¡preste mucha atención a esto!

General

Resumen del perfil del grupo (sólo a nivel de grupo)

Al abrir un perfil de grupo, obtendrás una rápida visión general del perfil.



Nombre del perfil	Nombre del perfil (se puede cambiar aquí)
Sistema operativo	Sistema operativo para el que es el perfil
Creado en	Momento de la creación
Creado por	El creador del perfil
Último cambio	Hora de la última modificación del perfil
Cambiado por	Cuenta que realizó los últimos cambios
Revisión actual del perfil	Revisión del estado del perfil guardado
Revisión del perfil liberado	Revisión del perfil asignado ("Asignar ahora"). Si la etiqueta muestra "(obsoleto)" detrás del texto, significa que has guardado el perfil pero aún no lo has asignado, por lo que los dispositivos seguirán recibiendo una versión antigua.

Visión general del dispositivo (sólo a nivel de dispositivo)

Resumen del dispositivo.

Nombre del dispositivo	Nombre del dispositivo
Modelo	Modelo
Sistema operativo	Sistema operativo
Número de serie	Número de serie del dispositivo
Propiedad del dispositivo	El Tipo de Propiedad configurado
Tipo de dispositivo	El tipo de dispositivo
Cumple	Muestra si el dispositivo es conforme
Dirección IP	La dirección IP desde la que el dispositivo se conectó al servidor
Visto por última vez	Hora de la última conexión desde el dispositivo
Último empujón	Hora de la última pulsación enviada al dispositivo
Asignación	Aquí puedes mover el dispositivo a otro usuario o grupo

Config Revision (sólo a nivel de dispositivo)

Aquí obtendrá una visión general de qué perfil de grupo está asignado al dispositivo.

Si haces clic en el perfil del grupo, accederás directamente al perfil y podrás realizar ajustes.

Con el símbolo, puedes revertir las aplicaciones asignadas a la configuración del perfil de grupo.

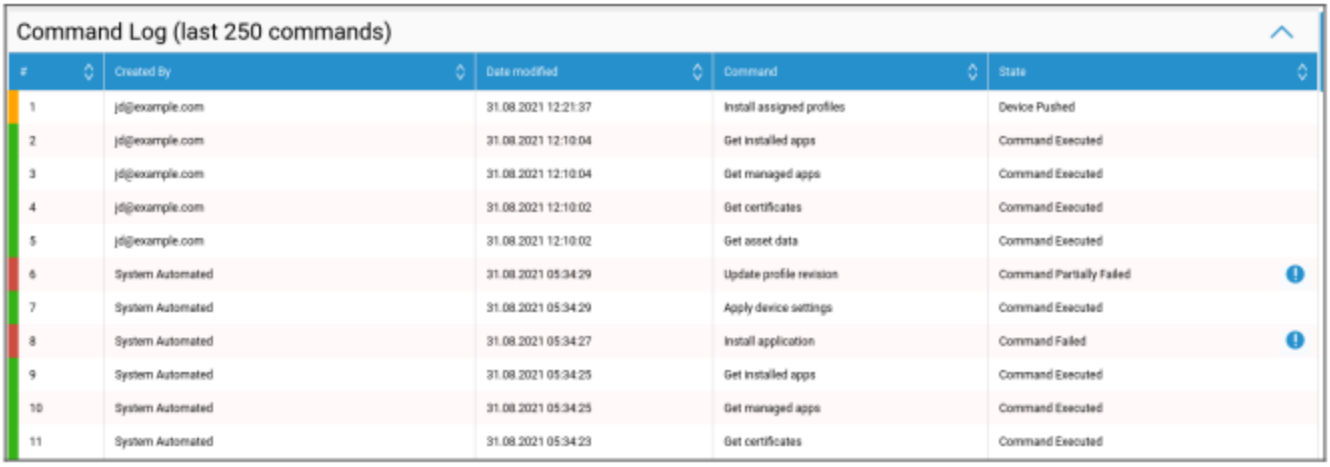
Con el símbolo, puedes restablecer el perfil del dispositivo para que no tenga ninguna configuración.

"Nueva revisión disponible" indica que el perfil de grupo se ha modificado y guardado, pero no se ha asignado. El perfil de grupo debe asignarse con "Asignar ahora" a nivel de grupo para aplicar los cambios a los dispositivos.

Registro de dispositivos (sólo a nivel de dispositivo)

Registro de comandos

Aquí puede ver qué comandos se emitieron para el dispositivo y cuál es su estado.



Los comandos creados por "Sistema automatizado" son creados automáticamente por el sistema.

Posibles estados del comando

Dispositivo Empujado	Se ha enviado una solicitud push al servicio push (por ejemplo, APNS) para indicar al dispositivo que se conecte de nuevo al servidor EMM.
Comando creado	El comando se creó en el sistema.
Orden enviada	El comando se envió al dispositivo después de que se conectara al servidor.
Orden ejecutada	El comando se ha ejecutado correctamente.
Comando fallido	El comando falló. *
Comando parcialmente fallido	Dependiendo del SO del dispositivo, algunos comandos pueden agruparse. En este fallaron algunas partes de este grupo de comandos. *
Orden ejecutada, finalmente fallida	La orden se ejecutó, pero puede que no.
Comando Repulsado	El comando fue repulsado por un usuario.
Descartado	El comando fue descartado. Por ejemplo, porque ha sido sustituido por otro comando o porque el dispositivo se ha reinscrito y se han eliminado los comandos antiguos.

*Si hay un signo de exclamación detrás del mensaje, puedes obtener más información pasando el cursor sobre el icono.

Gestión de activos (sólo a nivel de dispositivo)

Información del dispositivo

Número de modelo	Número de modelo
Nombre de host	Nombre de host
Nombre de host local	Nombre de host local
Sistema operativo	Sistema operativo
Versión del SO	Versión del SO
UDID	UDID
Memoria Libre / Total	Memoria Libre / Total

WiFi

Dirección IP	Dirección IP
WiFi MAC	WiFi MAC

Móvil

Número de teléfono	Número de teléfono
Estado de itinerancia	Estado de itinerancia
Itinerancia (Voz / Datos)	Itinerancia (Voz / Datos)
Dirección IP	Dirección IP
Operador/Transportista	Operador/Transportista
SIM Red del operador	Red de transportistas
Versión portadora	Versión portadora
ICCID	ICCID
MCC/MNC actual	MCC/MNC actual
SIM MCC/MNC	SIM MCC/MNC

Bluetooth

Bluetooth MAC	Bluetooth MAC

Gestión de actualizaciones (sólo a nivel de dispositivo)

Información actualizada

Esta pestaña muestra información sobre la configuración de actualización del sistema en el dispositivo.

Autocomprobación activada	Si el sistema está comprobando la actualización automáticamente.
App-Actualización automática activada	Si el sistema instalará las actualizaciones de la aplicación automáticamente.
Actualizaciones automáticas del SO activadas	Si el sistema instalará las actualizaciones del sistema operativo automáticamente.
Actualizaciones automáticas de seguridad activadas	Si el sistema instalará las actualizaciones de seguridad automáticamente.
Actualización de la aplicación Descarga en segundo plano activada	Si el sistema descargará actualizaciones de aplicaciones en segundo plano.
URL del catálogo	La URL del catálogo de actualizaciones de software que está utilizando el cliente.
Es catálogo por defecto	Si es "sí", Catálogo es el catálogo por defecto.
Realiza una comprobación periódica	Si la respuesta es "sí", inicia un nuevo escaneado.
Fecha de la exploración anterior	La fecha del último análisis de actualización del software.
Resultado del escaneado anterior	El código de resultado del último escaneo de actualización de software.

Gestión de la seguridad

Antirrobo

Limpiar y bloquear

Limpieza total	Envía un comando para restablecer de fábrica el dispositivo
Limpieza de empresas	Elimina el MDM del dispositivo y elimina todos los datos del MDM (por ejemplo, cuentas, aplicaciones).
Pantalla de bloqueo	Hacer que el dispositivo vuelva a la pantalla de bloqueo

Configuración de seguridad

Código

Se permite la desactivación del código	Determina si se obliga al usuario a establecer un PIN. El simple hecho de establecer este valor (y no otros) obliga al usuario a introducir un código de acceso, sin imponer una longitud o calidad.
Permitir valor simple	Permitir al usuario utilizar las mismas cadenas de números, escalando y reduciendo (ej. 1234, 1111)
Requiere valor alfanumérico	Las contraseñas deben contener al menos una letra
Longitud mínima del código de acceso	Longitud mínima de la contraseña
Número mínimo de caracteres complejos	Número mínimo de símbolos alfanuméricos en la contraseña
Edad máxima del código de acceso	Número de días tras los cuales debe cambiarse la contraseña
Bloqueo automático máximo	Tiempo máximo tras el cual se bloquea el dispositivo
Periodo máximo de gracia para el bloqueo del dispositivo	Cantidad de tiempo que el dispositivo puede estar bloqueado sin pedir la contraseña al desbloquearlo
Antigüedad máxima del código de acceso (1-730 días, o ninguna)	Días después de los cuales se debe cambiar la contraseña
Historial de contraseñas (1-50 contraseñas, o ninguna)	Número de códigos de acceso únicos antes de la reutilización

Certificado

PKCS#1	
Descripción	Introduce una Descripción para el Certificado
Credencial	Subir un archivo pkcs1

PKCS#12	
Descripción	Introduce una Descripción para el Certificado
Credencial	Subir un archivo pkcs12

Configuración de restricciones

Funcionalidad del dispositivo

Permitir cámara	Permitir el uso de la cámara
Permitir Game Center	Cuando es falso, Game Center se desactiva y su icono desaparece de la pantalla de inicio.
Permitir el juego multijugador	Cuando es falso, prohíbe el juego multijugador.
Permitir añadir amigos de Game Center	Cuando es falso, prohíbe añadir amigos a Game Center.
Permitir Fototeca de iCloud	Si se establece en false, desactiva la Fototeca de iCloud. Las fotos que no se hayan descargado completamente de la Fototeca de iCloud al dispositivo se eliminarán del almacenamiento local.
Permitir Touch ID	Si es falso, impide que Touch ID desbloquee un dispositivo.

iCloud

Bloquear ciertas funcionalidades durante el emparejamiento de iCloud

Permitir la sincronización de documentos	Permitir la sincronización de documentos
Permitir la sincronización del llavero de iCloud	Permitir la sincronización del llavero de iCloud
Permitir Notas de iCloud	Si es falso, desactiva los servicios de Notas de iCloud de macOS
Permitir BTMM de iCloud	Si es falso, desactiva el servicio iCloud de MacOS Volver a mi Mac.
Permitir iCloud FMM	Si es falso, desactiva el servicio iCloud de MacOS Buscar mi Mac.
Permitir Favoritos de iCloud	Si es falso, desactiva la sincronización de marcadores de iCloud de macOS.
Permitir iCloud Mail	Si es falso, desactiva los servicios iCloud de MacOS Mail.
Permitir Calendario de iCloud	Si es falso, desactiva los servicios iCloud de MacOS Cloud.

Permitir Recordatorios de iCloud	Si es falso, desactiva los servicios de Recordatorio de iCloud.
Permitir Libreta de direcciones de iCloud	Si es falso, desactiva los servicios de Agenda de iCloud de macOS.

Gestión de los medios de comunicación

Expulsar al cerrar sesión	Expulsar todos los soportes extraíbles al cerrar la sesión
Permitir Red	Permitir el acceso de los medios de red
Permitir Disco Interno	Permitir acceso para disco interno.
Requerir autenticación	Requerir autentificación para el uso de este medio
Sólo lectura	El Usuario sólo puede leer datos del soporte
Permitir disco externo	Permitir acceso para disco externo.
Requerir autenticación	Requerir autentificación para el uso de este medio
Sólo lectura	El Usuario sólo puede leer datos del soporte
Permitir el uso de Imágenes de Disco	Permitir el acceso a las Imágenes.
Requerir autenticación	Requerir autentificación para el uso de este medio
Sólo lectura	El Usuario sólo puede leer datos del soporte
Permitir el uso de DVD-RAM	Permitir acceso para disco DVD-RAM.
Requerir autenticación	Requerir autentificación para el uso de este medio
Sólo lectura	El Usuario sólo puede leer datos del soporte
Permitir el uso de DVD	Permitir acceso para disco DVD.
Requerir autenticación	Requerir autentificación para el uso de este medio
Permitir el uso de CDs	Permitir acceso para disco CD.
Requerir autenticación	Requerir autentificación para el uso de este medio

Gestión de conexiones

Wi-Fi

Aquí puede añadir y configurar conexiones Wi-Fi

Identificador del Conjunto de Servicios (SSID)	SSID de la red a la que se establecerá la conexión
Autounión	Activar la unión automática a la red
Red oculta	Activar, en caso de que el AP no difunda el SSID
Configuración del proxy	Configuración de un proxy para cada punto de acceso
Ninguno	No utilices un Servidor Proxy
Manual	Establecer un Proxy manual
URL del servidor proxy	Dirección para acceder a la configuración del proxy
Puerto	Establecer el puerto para el Proxy
Autenticación	Nombre de usuario para la autenticación en el Proxy
Contraseña	Contraseña para la autenticación en el Proxy
Automático	Establecer un Proxy automáticamente
URL del servidor proxy	URL del archivo de configuración del proxy
Tipo de seguridad	Establecer el tipo de seguridad para el AP
WEP	
Contraseña	Contraseña para el PA
WPA/WPA2	
Contraseña	Contraseña para el PA
WEP Empresa - WPA / WPA2 Empresa / Cualquier empresa	Ver Tabla Error: Fuente de referencia no encontrada a continuación
Ninguno	No establecer seguridad
Desactivar la aleatorización de direcciones MAC	Desactiva la aleatorización de direcciones MAC para esa red Wi-Fi mientras esté asociada a ella. Esto también muestra una advertencia de privacidad en Configuración indicando que la red tiene reducidas las protecciones de privacidad.

Configuración Wi-Fi para empresas

Nota: Sólo está disponible cuando "Tipo de seguridad" está configurado como Tipo de empresa.

Protocolos	Protocolo de autenticación admitido en la red de destino
TLS	Activar / Desactivar Uso
TTLS	Activar / Desactivar Uso
Autenticaciones internas	Protocolo de autenticación que debe utilizarse: PAP, CHAP, MSCHAP, MSCHAPv2
LEAP	Activar / Desactivar Uso
PEAP	Activar / Desactivar Uso
EAP-FAST	Activar / Desactivar Uso
EAP-SIM	Activar / Desactivar Uso
Utiliza PAC	Uso del PAC (Control de Acceso Protegido)
Disposición PAC	Configuración de Provisión PAC
Provisión PAC Anónima	Provisión anónima de PAC
Autenticación	
Nombre de usuario	Nombre de usuario de autenticación
No utilices Por conexión Contraseña	No utilices la contraseña por conexión
Contraseña	La contraseña a utilizar
Certificado de Identidad	Cargar/seleccionar certificado de autenticación
Identidad exterior	Identidad visible externamente
Confía en	
Certificado de confianza 1	Subir el primer certificado de confianza
Certificado de confianza 2	Sube el segundo certificado de confianza
Certificado de confianza 3	Subir un tercer certificado de confianza
Servidor de confianza Nombres de los certificados	Los nombres de los certificados de servidor esperados (en una lista separada por comas)

VPN

Dependiendo del Tipo de Conexión seleccionado, pueden aparecer diferentes campos.

Nombre de la conexión	Nombre del perfil VPN
Tipo de VPN	
VPN	Todo el tráfico de red del dispositivo se enrutará a través de una conexión VPN.
Tipo de conexión	Establecer tipo de conexión VPN
IPsec (cisco)	Protocolo IPsec de Cisco
L2TP	Protocolo L2TP
SSL personalizado	Conexión mediante SSL personalizado
IKEv2	Protocolo IKEv2
Configuración del proxy	Configuración de un proxy para la conexión VPN
Ninguno	No establecer Proxy
Manual	Establecer manualmente un Proxy
URL del servidor proxy	Dirección para acceder a la Configuración del Proxy
Puerto	Establecer el puerto para el Proxy
Autenticación	Nombre de usuario para la autenticación en el Proxy
Contraseña	Contraseña para la autenticación en el Proxy
Automático	Establecer un Proxy automáticamente
URL del servidor proxy	URL para acceder a la configuración del Proxy

Proxy HTTP

Tipo de proxy	
Manual	Establecer un Proxy manualmente
URL del servidor proxy	Dirección para acceder a la Configuración del Proxy
Puerto	Establecer puerto Proxy
Autenticación	Nombre de usuario para la autenticación en el Proxy
Contraseña	Contraseña para la autenticación en el Proxy
Automático	Establecer un Proxy automáticamente
URL del proxy PAC	URL del proxy PAC
Permitir conexión directa si PAC es inalcanzable	Permitir conexión directa (sin VPN), si PAC es inalcanzable
Permitir eludir el proxy para acceder a redes cautivas	Permitir eludir el proxy para acceder a redes internas cautivas

AirPrint

Dirección IP	Dirección IP de la impresora
Ruta de recursos	Ruta definida al dispositivo AirPrint

AirPlay

Nombre del dispositivo	Nombre del dispositivo
Contraseña	Contraseña de emparejamiento
Lista blanca	Define una lista de dispositivos, con los que el dispositivo puede emparejarse exclusivamente

Gestión PIM

Sincronización activa de Exchange

Nombre de la cuenta	Nombre de la cuenta.
Dirección de correo electrónico	La dirección de la cuenta (por ejemplo, max@company.com)
Nombre de host del servidor	Nombre de host interno
Nombre de usuario	"Dominio" y "Nombre de inicio de sesión" deben estar en blanco para que el dispositivo pregunte por el usuario.
Dominio	"Dominio" y "Nombre de inicio de sesión" deben estar en blanco para que el dispositivo pregunte por el usuario. Si se activa una configuración de puerta de enlace ACL y el campo Dominio no está vacío, la puerta de enlace universal AppTec360 autenticará el dispositivo con el siguiente nombre "Dominio\NNombre de inicio de sesión"
Contraseña	La contraseña de la cuenta (por ejemplo, secretUserPassword)
Días pasados de Mail to Sync	El número de días pasados de correo que hay que sincronizar
Utiliza SSL	Utilizar SSL para el Host Interno de Exchange
Opción avanzada	Mostrar opciones avanzadas
Puerto del servidor	Puerto interno
Ruta del servidor	Camino interno
Nombre de host externo	Anfitrión externo
Puerto externo	Puerto externo
Ruta externa	Ruta externa
Utilizar SSL para externos Anfitrión de intercambio	Utilizar SSL para el host Exchange externo

Correo electrónico

Configuración de cuentas POP3 / IMAP en el dispositivo del usuario final

Descripción de la cuenta	Nombre des Cuentas Email
Tipo de cuenta	
IMAP	
Prefijo de la ruta	El prefijo de ruta para carpetas especiales
POP	
Nombre para mostrar del usuario	Nombre de usuario
Dirección de correo electrónico	Dirección de correo electrónico del usuario

Correo entrante	Configuración del servidor entrante
Dirección del servidor de correo	Dirección del servidor de correo
Puerto del servidor de correo	Puerto del servidor de correo
Nombre de usuario	Nombre de usuario correspondiente
Tipo de autenticación	Tipo de autenticación
Ninguno	No Tipo de autenticación
Contraseña (sólo a nivel de dispositivo)	Indicación de contraseña
MDM Desafío-Respuesta	
NTLM	Autenticación NTLM
Resumen HTTP MD5	
Utiliza SSL	Utiliza SSL, si es necesario

Correo saliente	Configuración del servidor de salida
Dirección del servidor de correo	Dirección del servidor de correo
Puerto del servidor de correo	Puerto del servidor de correo
Nombre de usuario	Nombre de usuario respectivo
Tipo de autenticación	
Ninguno	Ningún método de autenticación
Contraseña (sólo a nivel de dispositivo)	Indicación de contraseña
MDM Desafío-Respuesta	
NTLM	Autenticación NTLM
Resumen HTTP MD5	
Utiliza SSL	Utiliza SSL, si es necesario
La contraseña saliente es la misma que la entrante	La contraseña saliente es la misma que la entrante
Utilizar sólo en correo	Activar, si todos los correos salientes deben enviarse a través de la Mail-App

CalDav

Configurar la creación y distribución de una cuenta CalDav

Descripción de la cuenta	Nombre para mostrar de la cuenta
Nombre de host	Nombre de host y/o dirección IP
Puerto	Puerto de la cuenta CalDav
URL principal	URL principal de la cuenta
Nombre de usuario	Nombre de usuario CalDav correspondiente
Contraseña (sólo a nivel de dispositivo)	Contraseña CalDav correspondiente
Utiliza SSL	Utiliza SSL, si es necesario

CardDav

Configurar la creación y distribución de una cuenta CardDav

Descripción de la cuenta	Nombre para mostrar de la cuenta
Nombre de host	Nombre de host y/o dirección IP
Puerto	Puerto de la cuenta CardDav
URL principal	URL principal de la cuenta
Nombre de usuario	Nombre de usuario CardDav correspondiente
Contraseña (sólo a nivel de dispositivo)	Contraseña CardDav respectiva
Utiliza SSL	Utiliza SSL, si es necesario

LDAP

En esta área, configure una conexión LDAP para permitir un intercambio dinámico de certificados entre el dispositivo del usuario final y el Directorio Activo.

Tenga en cuenta que el usuario seleccionado requiere el permiso de lectura correspondiente.

Descripción de la cuenta	Descripción de la cuenta
Nombre de usuario de la cuenta	Usuario para acceso LDAP
Contraseña de la cuenta	Contraseña de acceso LDAP
Nombre de host de la cuenta	Nombre de host/dirección IP del servidor LDAP
Utiliza SSL	Utiliza SSL, si es necesario

En la segunda parte, puede definir filtros individuales para buscar en el registro LDAP.

Descripción	Alcance	Buscar Base
Descripción del filtro	Nivel de búsqueda en el registro LDAP	Definir el filtro individual

Cuadro de mandos e informes

Ajustes del salpicadero

Aquí puedes ver qué Cuadros de Mando existen, editarlos o crear otros nuevos. Cada Cuadro de Mando tiene su propio conjunto de datos a mostrar y configuración de gráficos.

Control de la configuración del salpicadero

Público	Establece el Cuadro de Mando como público, para que otros usuarios puedan verlo. Los usuarios, por supuesto, tienen que poder iniciar sesión y ver los Tableros. Si "Público" no está activado, sólo el creador podrá verlo.
Por defecto	Establece el Panel de Control como predeterminado para que se abra automáticamente la próxima vez que accedas a la Vista del Panel de Control.
	Mostrar el Panel de control y sus gráficos
	Borrar el Panel de Control
	Editar el nombre y la configuración del panel de control
	Haz una copia del Panel de control
	Añadir un Panel de control completamente nuevo

Vista del salpicadero

Muestra los Datos y Gráficos del Cuadro de Mando seleccionado y también permite modificarlos.

Control del salpicadero

	Te permite definir qué datos se muestran en el Panel, la cantidad de datos a mostrar y en qué tamaño mostrar estos datos
	Te devuelve a la vista general del panel de control
	Restablece el Panel de control abierto actualmente a su valor por defecto
	Guarda todos los cambios que hayas realizado en el Panel de control abierto en ese momento (por ejemplo, qué datos mostrar).
	Cambiar el tipo de gráfico a gráfico de pilares
	Cambiar el tipo de gráfico a gráfico circular
	Cambiar el tipo de gráfico a gráfico de donuts
	Cambiar el tipo de gráfico a gráfico de área polar
	Cambiar el orden de clasificación

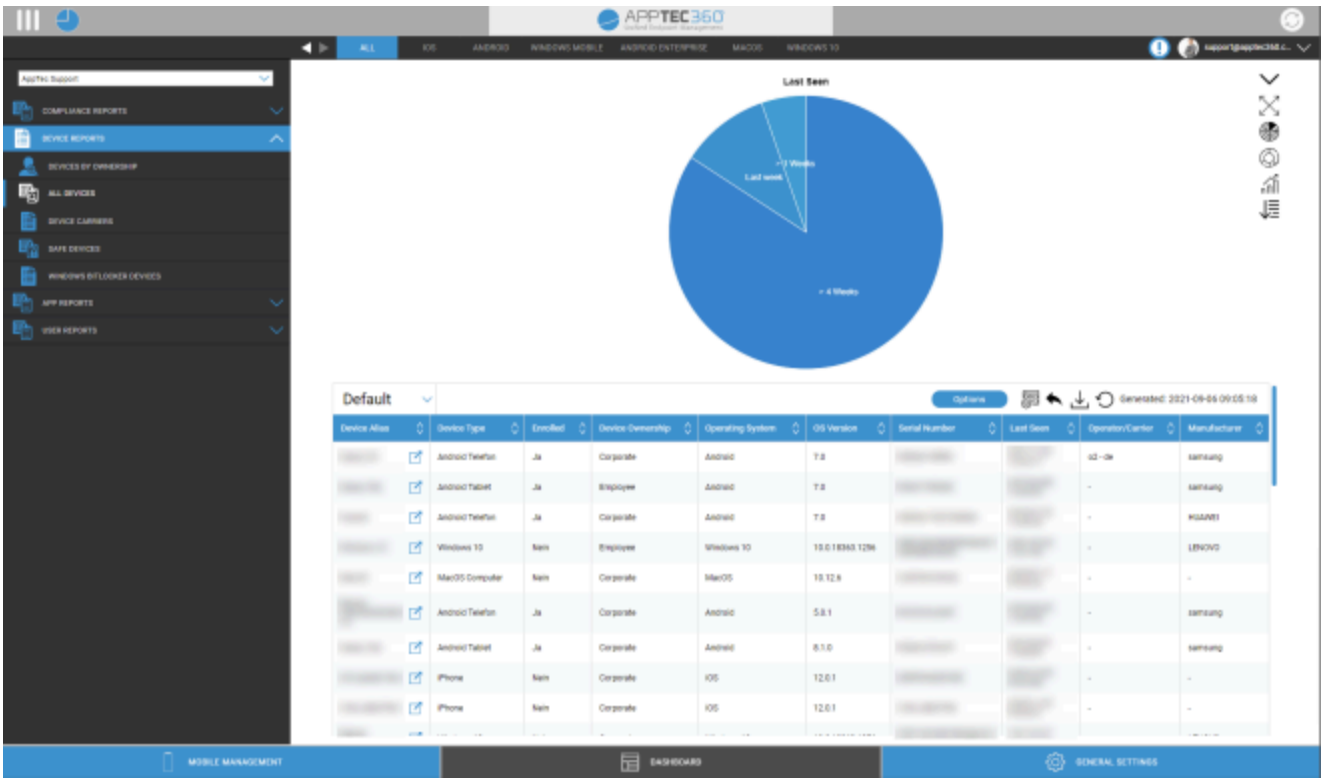
Informes ampliados

Los "Informes ampliados" ofrecen resúmenes y gráficos detallados sobre la información de los dispositivos y los usuarios.

Hay algunos informes predeterminados, pero todos ellos pueden modificarse manualmente para añadir o eliminar datos.

Ten en cuenta que sólo puedes cambiar manualmente los datos que se muestran. La categoría de informe seleccionada define los datos en los que se basa. Por ejemplo, nunca podrás ver los dispositivos Android en el informe iOS en Informes de dispositivos Todos los dispositivos iOS

En la parte superior izquierda puedes limitar los datos del informe a un determinado grupo (y a todos sus subgrupos). Por defecto, esto se establece en tu nodo raíz, por lo que tiene en cuenta TODOS los dispositivos y usuarios.



Control ampliado de informes

En cada resumen puede utilizar las siguientes funciones para modificar el informe como desee:

	Ocultar gráfico (Si se muestra el gráfico)
	Mostrar gráfico (Si el gráfico está oculto)
	Expandir gráfico (Si el gráfico está contraído)
	Contraer gráfico (Si el gráfico está expandido)
	Cambiar el tipo de gráfico a gráfico de pilares
	Cambiar el tipo de gráfico a gráfico circular
	Cambiar el tipo de gráfico a gráfico de donuts
	Cambiar el tipo de gráfico a gráfico de área polar
	Cambiar el orden de clasificación
	Modifica las siguientes partes de la vista general mostrada: • Añadir/Eliminar columnas • Especifica el orden en que se muestran las columnas • Mostrar/Ocultar el gráfico sobre la tabla • Selecciona la columna que se utiliza para el gráfico • Filtra los datos de tu tabla
	Abre el gestor de configuración para guardar y cargar distintos informes
	Restablece el Informe abierto por defecto
	Exportar el informe actual como archivo .csv
	Regenera los datos y recarga el informe actual

En las páginas siguientes encontrará una lista de todos los informes por defecto.

Informes de conformidad

Dispositivos arraigados

Visión general de los dispositivos que han sido rooteados / jailbreak.

Columnas por defecto de este informe:

Alias del dispositivo
Propietario del dispositivo
Correo electrónico
Sistema operativo
Número de teléfono
Visto por última vez
Fabricante

Dispositivos itinerantes

Resumen de todos los dispositivos en itinerancia

Columnas por defecto de este informe:

Alias del dispositivo
Propietario del dispositivo
Correo electrónico
Tipo de dispositivo
Sistema operativo
Número de teléfono
Visto por última vez

Dispositivos con itinerancia

Resumen de todos los dispositivos que han activado la itinerancia pero que no necesariamente están en itinerancia en ese momento.

Columnas por defecto de este informe:

Alias del dispositivo
Propietario del dispositivo
Correo electrónico
Tipo de dispositivo
Sistema operativo
Número de teléfono
Visto por última vez

Dispositivos supervisados

Resumen de todos los dispositivos supervisados en modo supervisado (sólo iOS)

Columnas por defecto de este informe:

Alias del dispositivo
Propietario del dispositivo
Correo electrónico
Tipo de dispositivo
Visto por última vez

Dispositivos inactivos

Resumen de todos los dispositivos que no se han conectado al servidor en los últimos 7 días

Columnas por defecto de este informe:

Alias del dispositivo
Propietario del dispositivo
Correo electrónico
Tipo de dispositivo
Sistema operativo
Visto por última vez

Informes sobre dispositivos

Dispositivos por propiedad

Aquí puede ver cuántos dispositivos se han desplegado actualmente como dispositivos corporativos (dispositivos de empresa) y dispositivos de empleado (dispositivos privados).

Columnas por defecto de este informe:

Alias del dispositivo
Propietario del dispositivo
Tipo de dispositivo
Propiedad del dispositivo
Sistema operativo

Todos los dispositivos

Aquí puedes ver un resumen de todos los dispositivos con la información más importante.

Columnas por defecto de este informe:

Alias del dispositivo
Tipo de dispositivo
Inscrito
Propiedad del dispositivo
Sistema operativo
Versión del SO
Número de serie
Visto por última vez
Operador/Transportista
Fabricante

Portadores de dispositivos

Aquí puedes ver un resumen sobre el operador (proveedor de telefonía móvil).

Columnas por defecto de este informe:

Alias del dispositivo
Propietario del dispositivo
Correo electrónico
Sistema operativo
Versión del SO
Operador/Transportista

Dispositivos SAFE

Aquí puede ver un resumen de los dispositivos que utilizan la versión SAFE.

Debido a que la vista general y/o SAFE sólo está disponible para dispositivos Samsung, no verás las pestañas habituales bajo este punto.

Columnas por defecto de este informe:

Alias del dispositivo
Propietario del dispositivo
Correo electrónico
Tipo de dispositivo
Visto por última vez
Versión SAFE

Dispositivos Windows BitLocker

Aquí puedes ver un resumen de los dispositivos Windows que utilizan BitLocker.

Columnas por defecto de este informe:

Alias del dispositivo
Propietario del dispositivo
Correo electrónico

Estado de BitLocker

Informes de aplicaciones

Aquí encontrarás una gran variedad de información general sobre las aplicaciones. En todos estos informes puede hacer clic en una entrada para ver con más detalle qué versiones están instaladas en los dispositivos y con qué frecuencia. En esta vista puede volver a hacer clic en una versión específica para ver qué dispositivos tienen instalada esta versión concreta.

Nota: Puede pasar algún tiempo hasta que el sistema reciba información actualizada del dispositivo. Además, los informes no se actualizan cada minuto. Puede que tengas que ser paciente para ver el estado actual si acabas de asignar una nueva aplicación o versión. Si recarga manualmente el informe, éste mostrará los datos más actualizados disponibles.

Aplicaciones instaladas

Aquí tienes una visión general de todas las aplicaciones instaladas.

Columnas por defecto de este informe:

Nombre	Nombre de la app y/o servicio correspondiente
Identificador	ID de app/servicio definido
Recuento total	Con qué frecuencia se ha instalado esta app / servicio en los dispositivos de los usuarios finales

Aplicaciones más instaladas

Aquí puedes ver las aplicaciones que más se han instalado.

Columnas por defecto de este informe:

Nombre	Nombre de la app y/o servicio correspondiente
Identificador	ID de app/servicio definido
Recuento total	Con qué frecuencia se ha instalado esta app / servicio en los dispositivos de los usuarios finales

Aplicaciones obligatorias

Aquí obtendrá una visión general de las aplicaciones obligatorias (requeridas por mandato).

Columnas por defecto de este informe:

Name	Name of the respective app and/or service
Identifier	Definite app/service ID
App Source	Which AppStore is involved: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Operating System

Aplicaciones en la lista negra

Aquí obtendrá una visión general de todas las aplicaciones definidas en la lista negra.

Columnas por defecto de este informe:

Nombre	Nombre de la app y/o servicio correspondiente
Identificador	ID de app/servicio definido
App Fuente	De qué AppStore se trata: • Google PlayStore (Android) • iTunes AppStore (iOS)
OS	Sistema operativo

Informes de usuarios

Tarifa

Aquí obtendrá una visión general de las tarifas telefónicas y tarjetas SIM de sus usuarios.

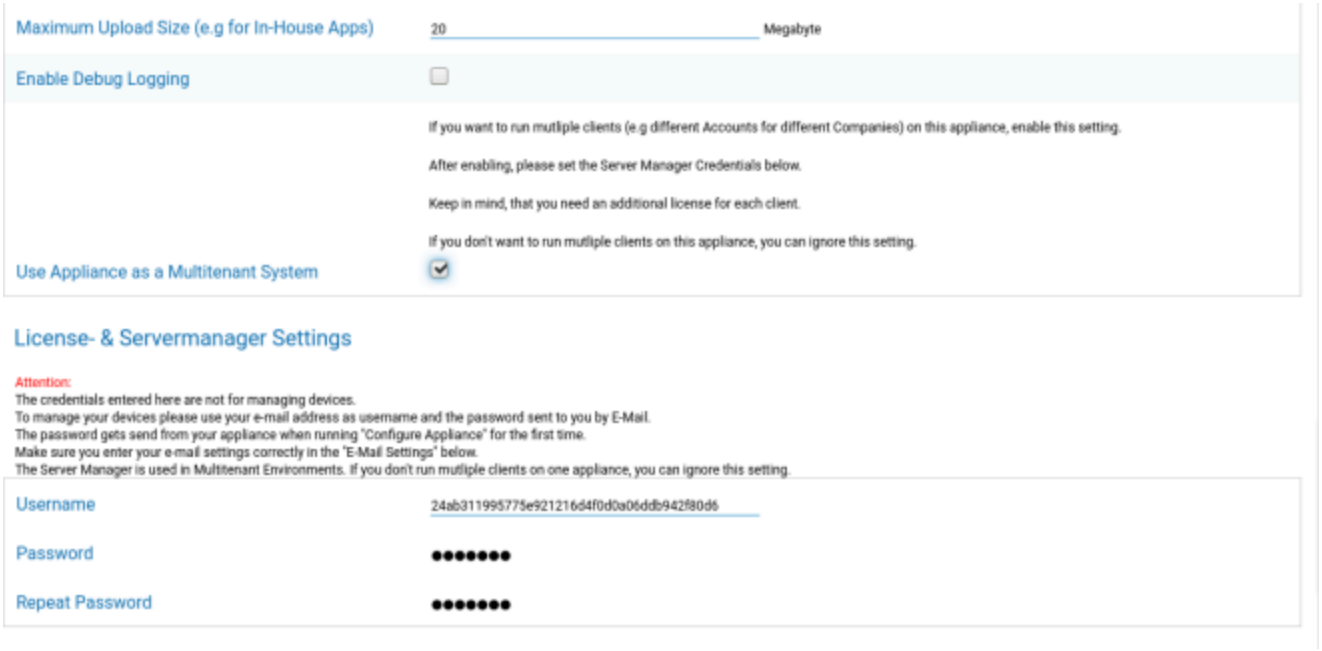
Columnas por defecto de este informe:

Correo electrónico
Nombre
número de teléfono
portador
tarifa
opción
precio
contratoCancelado
contratoInicio
duranteTiempo
móvilAndData
volumen de datos
multiSIM
tipo
simCardSerial1
simCardSerial2
simCardSerial3
pin1
pin2
puk1
puk2
nota

Gestión de multiinquilinos

AppTec360 EMM es capaz de alojar varios inquilinos independientes, cada uno con sus propios usuarios y grupos, permisos y configuraciones globales.

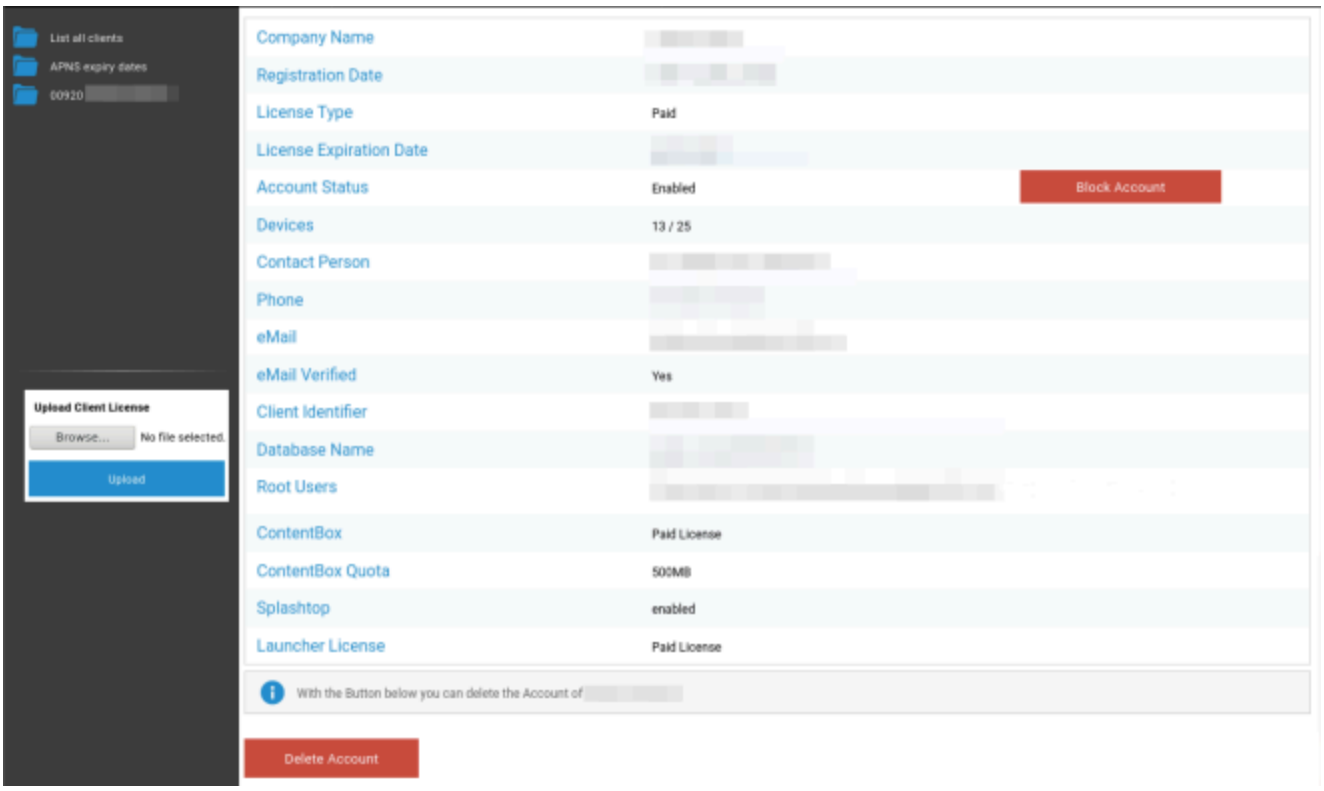
Para habilitar las capacidades Multitenant, debe habilitarlas en la interfaz de configuración del Appliance en el "Paso Tres - Configuración del Servidor".



En el nuevo menú establezca un nombre de usuario y una contraseña para el Servermanager. Guarde la configuración y ejecute "Configurar dispositivo" en el "Paso cinco - Acuerdo de licencia" para aplicar la configuración.

Una vez finalizada la configuración, puede iniciar sesión con las credenciales establecidas a través de la interfaz normal de Mobile Management.

Después de iniciar sesión puede ver la siguiente vista.



A la izquierda puedes ver todos los inquilinos (en este caso sólo uno con id 920) y a la derecha la información sobre este cliente. También tiene la opción de bloquear el acceso a la cuenta, así como de eliminar el cliente (ATENCIÓN: Esto eliminará todos los datos relacionados con ese cliente).

A la izquierda puede cargar una nueva licencia de cliente, que puede ser una actualización de licencia para un cliente existente o una nueva licencia que crea automáticamente un nuevo cliente. Cuando se crea un nuevo cliente, se envía automáticamente un correo electrónico con la contraseña de inicio de sesión a la dirección de correo electrónico para la que se emitió la licencia.

Para obtener una licencia de cliente nueva o actualizada (por ejemplo, si necesita más licencias de dispositivos), póngase en contacto con su representante de ventas.

Vistas adicionales

Lista de todos los clientes

Muestra un resumen de todos los clientes del sistema.

ID de cliente	ID de cliente
Identificador	Identificador de cliente
Base de datos	Base de datos
Nombre de la empresa	Nombre de la empresa
Correo electrónico	Persona de contacto eMail
Verificado	Si el correo electrónico de la persona de contacto está verificado o no
País	País
Dispositivos	Número de dispositivos registrados
Fecha de inscripción	Momento de la asignación de la licencia
Último acceso	Último acceso a la cuenta admin
Licencia	Visualización del tipo de licencia (Gratuita|Pagada)
Licencia CB	Tipo de licencia de ContentBox (Gratuita|Pagada)
Estado	Estado actual de AppTec-Client
Caducado	Muestra, si la licencia ha caducado
iOS	Número de dispositivos iOS
Android	Número de dispositivos Android
Windows Mobile	Número de dispositivos Windows Mobile
MacOS	Número de dispositivos macOS
Windows 10	Número de dispositivos Windows 10
Android para empresas	Número de dispositivos Android para empresas
IOS BYOD (Inscripción de usuarios)	Número de dispositivos IOS BYOD (inscripción de usuarios)
IoT	Número de dispositivos IoT

Fechas de caducidad APNS

Muestra un resumen de todas las fechas de caducidad de los certificados APNS de todos los clientes.

ID de cliente	ID de cliente
Nombre de la empresa	Nombre de la empresa
Fecha de caducidad	Fecha de caducidad del certificado APNS de Apple
Información	Información sobre la caducidad

Póngase en contacto con

¿Tiene más preguntas? Póngase en contacto con nosotros:

Para cuestiones técnicas generales

support@apptec360.com

+41 61 511 3210

Para preguntas relacionadas con la instalación de un dispositivo virtual

consulting@apptec360.com

+41 61 511 3214

Descargo de responsabilidad