

Gestión de movilidad empresarial (EMM)

Asegúrese de que los dispositivos personales y de propiedad de la empresa se administren y protejan adecuadamente, para que los empleados puedan concentrarse en su trabajo sin interrupciones.

¿Qué es la gestión de la movilidad empresarial (EMM)?

Enterprise Mobility Management (EMM) se refiere a la gestión de dispositivos en un entorno corporativo. Su objetivo principal es garantizar que los dispositivos y los datos permanezcan seguros incluso cuando los empleados están trabajando sobre la marcha.

Durante algún tiempo, la gestión de dispositivos móviles (MDM) se utilizó como término general y común para describir la gestión de dispositivos. Sin embargo, a medida que las empresas comenzaron a tener requisitos más complejos para la movilidad y la gestión de dispositivos, Enterprise Mobility Management (EMM) surgió como un término más apropiado.

EMM cubre todo el conjunto de soluciones de gestión de la movilidad, mientras que MDM se centra únicamente en los dispositivos móviles y su seguridad.

¿Cómo puedes beneficiarte de EMM?

Prevenir brechas de seguridad

Aborde las amenazas de seguridad y las fugas de datos asegurando los dispositivos personales y de propiedad de la empresa y los datos almacenados en ellos

Garantizar el cumplimiento

Configure los dispositivos de acuerdo con la política corporativa y asegúrese de que todos los dispositivos cumplan.

Estas son algunas de las características:

Seguridad: bloquee, borre y cifre dispositivos, cree contenedores seguros y administre implementaciones de archivos.

Configuraciones: establezca configuraciones de correo electrónico, Wi-Fi, contraseñas y VPN automáticamente.

Gestión de aplicaciones: aplicaciones de lista negra y lista blanca. Implemente y elimine aplicaciones, archivos y certificados.

Restricciones: impida la instalación/desinstalación de aplicaciones, limite la itinerancia de datos y configure el filtrado de contenido web.

Seguimiento de ubicación: vea las ubicaciones actuales del dispositivo y acceda al historial de ubicaciones.

Políticas comerciales: aplique configuraciones, aplicaciones y archivos a grupos de dispositivos automáticamente con políticas comerciales.

Funciones admitidas por método de gestión	
Característica / Método de gestión	Dispositivo totalmente administrado
Restricción del uso de cuentas personales de Google en dispositivos Android	Sí
Controle que aplicaciones estan disponibles en la tienda Google Play administrada	Sí
Configurar aplicaciones administradas de forma remota	Sí
Configurar siempre en VPN de forma remota	Sí
Configurar el cifrado del dispositivo de forma remota	Sí
Configurar requisitos de contraseña	Sí
Configurar los ajustes de wifi	Sí
Denegar captura de pantalla	Sí
Negar el uso de camara	Sí
Implementar aplicaciones en siliencio	Sí
Implementar informacion de contacto	Sí
Implementar certificados en los dispositivos	Sí
Implementar archivos en los dispositivos	Sí
Desplegar fondo de pantalla	Si
Bloquee dispositivos en aplicaciones especificas con modo quiosco	Sí
Realizar borrado remoto para el perfil/ dispositivo completo	Sí
Evitar la intinerancia de datos	Sí
Impedir la transferencia de archivos a traves de USB	Sí
Evitra el uso de mensajes de texto (SMS)	Sí
Impedir que el usuario realice un restablecimiento de fabrica	Sí
Imedir que los usuarios monten medios externos en el dispositivo	Sí
Impedir la configuracion de Wi-Fi, Bluetooth o Tethering	Sí
Configurar dispositivos automaticamente usando Android Zero-touch	Sí
Admite la inscripcion movil de Samsung Knox	Sí