Aranda Enterprise Mobility Management

Gestione y proteja los dispositivos móviles de su empresa con facilidad. Simplifique la administración, optimice el acceso a recursos y refuerce la seguridad con una solución integral y automatizada. Garantice el cumplimiento de políticas corporativas y mantenga el control total de su entorno móvil desde una única plataforma.

Desafíos

En el mundo digital actual, la movilidad empresarial se ha convertido en una necesidad estratégica para las organizaciones. La transformación digital y el auge del trabajo remoto e híbrido han impulsado el uso de dispositivos móviles, como smartphones y tablets, en el entorno corporativo, permitiendo a los empleados acceder a aplicaciones y datos desde cualquier ubicación. Sin embargo, esta expansión también trae consigo importantes desafíos en seguridad, administración y cumplimiento normativo.

La falta de visibilidad y control sobre los dispositivos móviles puede derivar en accesos no autorizados a información sensible, riesgos de seguridad y dificultades en la gestión de aplicaciones y contenidos corporativos. Además, la diversidad de sistemas operativos y configuraciones hace que la administración manual de estos dispositivos sea ineficiente, costosa y propensa a errores.

Para abordar estos retos, las empresas necesitan una solución centralizada que les permita gestionar de forma remota y segura los dispositivos móviles. Esto garantiza el cumplimiento de políticas de seguridad, el control de aplicaciones y el acceso seguro a la información sin afectar la productividad de los usuarios.

Solución

Aranda Enterprise Mobility Management (AEMM) es la solución integral para la administración segura y eficiente de smartphones y tablets en el entorno corporativo.

A través de una plataforma centralizada, AEMM permite gestionar de forma remota la configuración, seguridad y cumplimiento normativo de los dispositivos móviles, garantizando protección de datos, control de aplicaciones y acceso seguro a la información empresarial.

Su enfoque en automatización, visibilidad y cumplimiento diferencia a AEMM, ofreciendo a las organizaciones una gestión ágil y segura que maximiza la productividad sin comprometer la seguridad.

Beneficios clave

- **Seguridad de la información**
  Proteja los datos corporativos mediante la encriptación de información y la gestión de aplicaciones, asegurando que solo usuarios autorizados accedan a contenido sensible.
- **Gestión centralizada**
  Administre todos los dispositivos móviles desde una única consola, facilitando el control y la implementación de políticas de seguridad en toda la organización.
- **Soporte para BYOD**
  Implemente políticas de "Bring Your Own Device" de manera segura, separando los datos personales de los corporativos, garantizando la privacidad de los empleados.
- **Automatización de tareas**
  Optimice procesos mediante la automatización de configuraciones, actualizaciones y políticas de seguridad, reduciendo errores y aumentando la eficiencia operativa.
- **Geolocalización y control remoto**
  Monitoree en tiempo real la ubicación de los

dispositivos y ejecute acciones remotas como bloqueos o borrados de datos en caso de pérdida o robo.

- **Reportes personalizados**
  Genere informes detallados sobre el estado y uso de los dispositivos, facilitando la toma de decisiones estratégicas basadas en datos.
- **Cumplimiento normativo**
  Asegure que todos los dispositivos cumplan con regulaciones y políticas internas, minimizando riesgos legales y operativos.
- **Control del uso de aplicaciones**
  Defina qué aplicaciones pueden instalarse o ejecutarse en los dispositivos corporativos, evitando el uso de software no autorizado o potencialmente riesgoso.

Funcionalidades Clave de Aranda Enterprise Mobility Management

Gestión integral de dispositivos móviles

AEMM centraliza la gestión de dispositivos Android y iOS, garantizando seguridad, monitoreo y cumplimiento normativo. Facilita la aplicación de políticas corporativas, permite el control en tiempo real y minimiza riesgos de seguridad, optimizando la eficiencia operativa.

Acciones remotas

Permite ejecutar acciones como bloqueo, restablecimiento de contraseñas, localización, envío de mensajes y formateo a fábrica sin intervención del usuario.

Protección contra dispositivos comprometidos

Identifica y restringe el acceso de dispositivos con alteraciones de seguridad (Jailbroken/Rooted), evitando riesgos de acceso no autorizado y brechas de seguridad en la red corporativa.

Gestión segura de dispositivos personales (BYOD)

Permite administrar de forma segura aplicaciones e información corporativa en dispositivos personales mediante entornos separados, garantizando la protección de datos empresariales.

Auditoría de actividad en consola

Supervisa y audita las operaciones realizadas en la consola, registrando cambios en configuración, políticas y eventos clave. Permite filtrar registros por fecha, usuario y acción, además de exportarlos para análisis.

Gestión de alertas y eventos

Ofrece un sistema centralizado de alertas ante incidentes de seguridad o cambios críticos en los dispositivos, permitiendo respuestas rápidas y mitigación de riesgos.

Ubicación y seguimiento en tiempo real

Proporciona geolocalización precisa de los dispositivos con niveles de precisión ajustables, permitiendo visualizar su ubicación en tiempo real.

Restricción de uso por ubicación (Geofencing)

Define límites geográficos para el uso de dispositivos y activa acciones automáticas al ingresar o salir de zonas predefinidas. Permite generar alertas, restringir funciones o aplicar cambios de seguridad para reforzar políticas corporativas y proteger la información sensible.

Restricción de uso por horario (Timefencing)

Configura horarios permitidos para el uso de dispositivos y ejecuta acciones automatizadas como bloqueo, cambio de contraseña, restricción de contenido o envío de alertas cuando estos ingresan o salen de los tiempos establecidos.

Restricción de uso por red Wi-Fi (WiFi-Fencing)

Supervisa y controla las redes Wi-Fi a las que se conectan los dispositivos, permitiendo ejecutar acciones como bloqueo, envío de alertas o restricciones cuando estos ingresan o salen de redes no autorizadas, reforzando la seguridad y el cumplimiento de políticas corporativas.

Localización con alerta sonora

Habilita la activación remota de sonidos para facilitar la

localización de dispositivos en espacios cerrados, optimizando la recuperación de activos móviles.

Gestion centralizada de aplicaciones

Permite la instalación, actualización y eliminación de aplicaciones de forma remota, asegurando que los dispositivos solo cuenten con software autorizado. Además, facilita la creación de listas blancas y negras para restringir o permitir el uso de aplicaciones específicas, garantizando el cumplimiento de las políticas corporativas.

Distribución segura de contenidos

Facilita el almacenamiento y acceso a documentos empresariales mediante un contenedor seguro, permitiendo la confidencialidad de la información.

Modo Kiosko para uso controlado

Configura dispositivos en modo Kiosko para restringir el acceso a solo aplicaciones aprobadas, evitando distracciones y asegurando su uso exclusivo para actividades laborales.

Restricción de funciones del dispositivo

Desactiva funciones como cámara, Bluetooth y Wi-Fi según los requisitos de seguridad, evitando riesgos de filtración de datos o accesos no autorizados.

Monitoreo de actividad en dispositivos

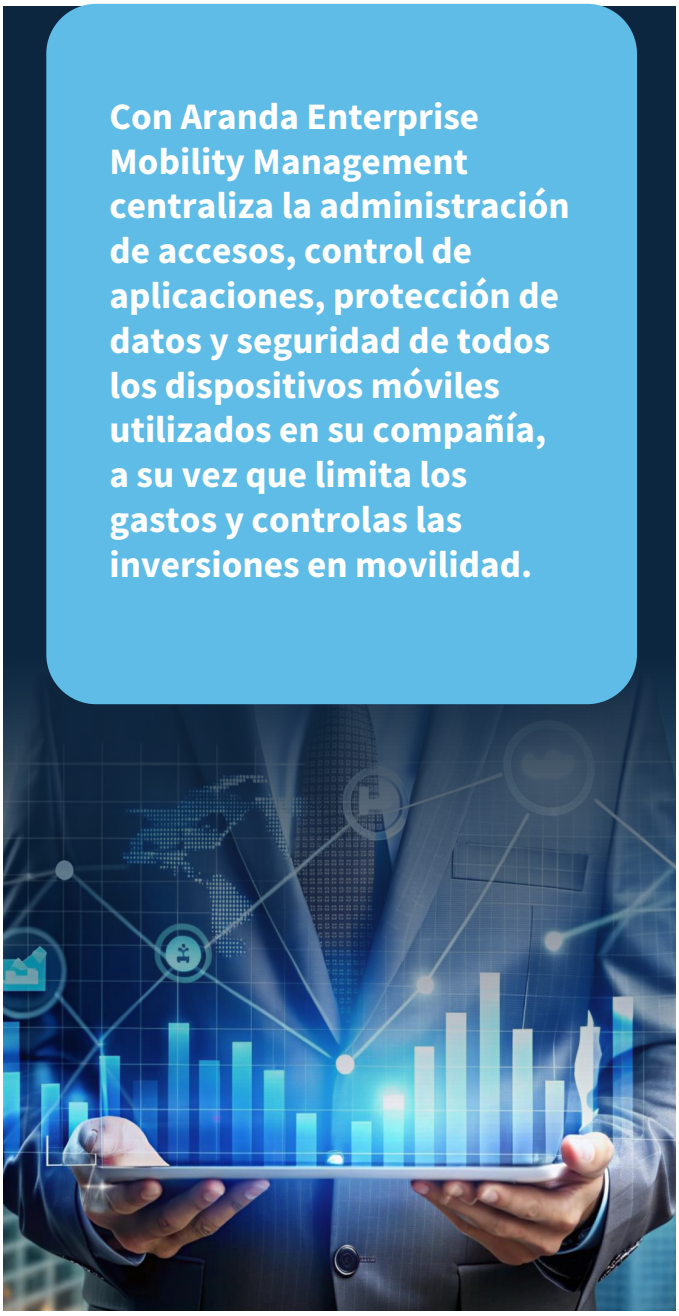
Monitorea en tiempo real los eventos ocurridos en los dispositivos, incluyendo el ciclo de vida de comandos y actividades como envío de ubicación, cambios de zona y desvinculación. Proporciona un historial detallado que garantiza trazabilidad y seguridad.

Gestión centralizada de Políticas

Permite asignar y administrar parámetros específicos en dispositivos móviles para definir su contexto de operación, incluyendo configuraciones de seguridad, restricciones de uso y ajustes personalizados. AEMM facilita la edición, aprobación y versionamiento de políticas, asegurando su cumplimiento mediante herramientas de seguimiento, reportes y notificaciones en caso de incumplimiento.

Automatización mediante Reglas

Responde de forma automática a eventos críticos como



cambios de usuario, desvinculación, consumo anómalo de datos, ubicación, conexión a Wi-Fi y horarios de operación. Ante estas situaciones, el sistema actúa de inmediato con alertas, ajustes de políticas, bloqueos y restricciones, garantizando seguridad y cumplimiento.

Cifrado de información

Protege los datos corporativos almacenados en los dispositivos mediante cifrado avanzado, evitando accesos no autorizados y garantizando la seguridad de la información.

Control con Android for Work

Proporciona herramientas avanzadas para la gestión y supervisión de dispositivos Android, asegurando su alineación con las políticas empresariales.

Control del consumo de datos

Supervisa en tiempo real el uso de voz y datos, permitiendo establecer alertas y restricciones para evitar sobrecostos en planes de telecomunicaciones.

Control Remoto

Administra dispositivos de forma remota desde la consola de AEMM, agilizando la asistencia técnica y la resolución de problemas en tiempo real. Las sesiones requieren confirmación del usuario para garantizar un acceso seguro y evitar intrusiones no autorizadas.

Administración segmentada por grupos

Asigna dispositivos a grupos y vincúlalos con especialistas según su área de responsabilidad. Esto mejora la eficiencia al garantizar que cada especialista gestione solo los equipos correspondientes, optimizando permisos y accesos. Además, facilita la distribución de configuraciones de manera estructurada.

Grupos dinámicos de dispositivos

Agrupa automáticamente dispositivos según criterios como sistema operativo, modelo o propiedad. Esto permite aplicar configuraciones, políticas y reglas de manera masiva y eficiente. Los dispositivos entran o salen de los grupos dinámicamente según sus características, asegurando que siempre reciban las acciones adecuadas.

Configuraciones manejadas para aplicaciones

Asegura que las aplicaciones empresariales se instalen con los ajustes adecuados desde el primer uso, optimizando la experiencia del usuario y reduciendo errores. Además, permite restringir configuraciones que puedan afectar la seguridad o el uso corporativo, garantizando un entorno controlado y eficiente.

Habilite de forma segura el uso de dispositivos, aplicaciones y contenidos para su fuerza de trabjo móvil

Métricas de uso de aplicaciones

Proporciona análisis detallados del consumo de datos y del tiempo de uso de cada aplicación en los dispositivos. Esta información facilita la optimización de recursos y mejora la toma de decisiones para una gestión eficiente.

Proyectos de gestión

Optimiza la configuración y administración de múltiples dispositivos mediante proyectos de gestión. A través de un archivo .CSV con los IMEI de los equipos, permite aplicar acciones en lote, como activar el modo perdido, localizar dispositivos, obtener inventarios, ejecutar scripts o instalar aplicaciones.

Scripts Remotos

Permite ejecutar scripts de manera remota en los dispositivos para anticiparse a necesidades operativas, facilitando tareas como instalación y desinstalación de aplicaciones, modificación de configuraciones y gestión de almacenamiento.

Borrado remoto de datos

Elimina de manera total o selectiva la información almacenada en dispositivos extraviados o comprometidos, garantizando la protección de datos sensibles y el cumplimiento de normativas de seguridad.

Análisis y reportería avanzada

Proporciona dashboards interactivos con métricas clave sobre inventario, estado de dispositivos y consumo de recursos, facilitando la toma de decisiones estratégicas.

Licenciamiento

AEMM se licencia por endpoint o activo gestionado. Un endpoint o activo gestionado es cualquier dispositivo móvil (Android, IOS) que requiera actividades de gestión mediante el agente.

Gestion del ciclo de vida con CMDB

Cada licencia adquirida para la gestión de endpoints o activos mediante el agente de AEMM incluye una licencia de CI en CMDB. Para administrar activos no informáticos o

activos de TI que no puedan gestionarse a través del agente, es posible adquirir paquetes adicionales de CI's.

Accesos incluidos

El licenciamiento de AEMM otorga acceso a las herramientas de reportería AQM y gestión del ciclo de vida de activos CMDB, con los siguientes accesos concurrentes:

- Cinco (5) accesos concurrentes de usuarios/técnicos para la consola de AEMM.
- Tres (3) accesos concurrentes de usuarios/técnicos para la consola de AQM.
- Tres (3) accesos concurrentes de usuarios/técnicos para la consola de CMDB.

Estos accesos están incluidos por defecto y no dependen de la cantidad de licencias adquiridas para la gestión de activos móviles.

Además, la CMDB permite administrar contratos, facturas de hardware y licencias de software, así como gestionar garantías, mantenimientos y proveedores, brindando una visión integral del costo total de propiedad (TCO) de los activos tecnológicos.

Integración con Aranda Query Manager

AEMM se integra con Aranda Query Manager para ofrecer reportes avanzados e indicadores en tiempo real sobre la infraestructura de dispositivos móviles y su cumplimiento. Los usuarios pueden visualizar métricas detalladas y gráficas sobre el inventario de dispositivos, incluyendo aplicaciones instaladas, versiones de sistema operativo, estado de cumplimiento y consumo de recursos.

Además, permite generar informes predefinidos o personalizados sobre la gestión de activos móviles y TI, con la opción de programar su envío automático. Esto facilita la toma de decisiones estratégicas, mejora la gobernanza de dispositivos y garantiza el cumplimiento normativo de la organización.

Integraciones

AEMM amplía sus capacidades al integrarse de forma nativa con nuestras soluciones de CMDB y reportería avanzada, optimizando la gestión de activos de TI y proporcionando una visión detallada de la infraestructura tecnológica.

Integración con Aranda CMDB

Conozca el ciclo de vida de sus dispositivos móviles gracias a la integración de AEMM con Aranda CMDB, que permite actualizar automáticamente los elementos de configuración mediante el descubrimiento y la detección de cambios en los inventarios de los dispositivos gestionados. Esto mejora la trazabilidad de los activos móviles y facilita su relación con los procesos de Gestión del Servicio, como incidencias, peticiones, problemas y cambios.

Desde la CMDB, puede acceder a información detallada del ciclo de vida de sus activos móviles, incluyendo:

- Ingreso del dispositivo a la compañía
- Fabricante, proveedor y usuario responsable
- Facturas, contratos, garantías y mantenimientos
- Historial de cambios y eventos registrados