Aranda Enterprise Mobility Management

Gerencie e proteja os dispositivos móveis da sua empresa com facilidade. Simplifique a administração, otimize o acesso a recursos e fortaleça a segurança com uma solução integral e automatizada. Garanta a conformidade com as políticas corporativas e mantenha o controle total do seu ambiente móvel a partir de uma única plataforma.

Desafios

No mundo digital atual, a mobilidade empresarial se tornou uma necessidade estratégica para as organizações. A transformação digital e o crescimento do trabalho remoto e híbrido impulsionaram o uso de dispositivos móveis, como smartphones e tablets, no ambiente corporativo, permitindo que os funcionários acessem aplicativos e dados de qualquer local. No entanto, essa expansão também traz desafios significativos em segurança, administração e conformidade regulatória.

A falta de visibilidade e controle sobre os dispositivos móveis pode resultar em acessos não autorizados a informações sensíveis, riscos de segurança e dificuldades na gestão de aplicativos e conteúdos corporativos. Além disso, a diversidade de sistemas operacionais e configurações torna a administração manual desses dispositivos ineficiente, cara e propensa a erros.

Para enfrentar esses desafios, as empresas precisam de uma solução centralizada que permita gerenciar remotamente e com segurança os dispositivos móveis. Isso garante o cumprimento das políticas de segurança, o controle de aplicativos e o acesso seguro às informações sem comprometer a produtividade dos usuários.

Solução

Aranda Enterprise Mobility Management (AEMM) é a solução completa para a administração segura e eficiente de smartphones e tablets no ambiente corporativo.

Por meio de uma plataforma centralizada, o AEMM permite gerenciar remotamente a configuração, segurança e conformidade dos dispositivos móveis, garantindo a proteção de dados, o controle de aplicativos e o acesso seguro às informações empresariais.

Seu foco em automação, visibilidade e conformidade diferencia o AEMM, oferecendo às organizações uma gestão ágil e segura que maximiza a produtividade sem comprometer a segurança.

Principais Benefícios

- **Segurança da informação**
  Proteja os dados corporativos por meio da criptografia de informações e da gestão de aplicativos, garantindo que apenas usuários autorizados acessem conteúdos sensíveis.
- **Gestão centralizada**
  Administre todos os dispositivos móveis a partir de um único console, facilitando o controle e a implementação de políticas de segurança em toda a organização.
- **Suporte para BYOD**
  Implemente políticas de "Bring Your Own Device" de forma segura, separando os dados pessoais dos corporativos e garantindo a privacidade dos funcionários.
- **Automação de tarefas**
  Otimize processos com a automação de configurações, atualizações e políticas de segurança, reduzindo erros e aumentando a eficiência operacional.
- **Geolocalização e controle remoto**
  Monitore em tempo real a localização dos

dispositivos e execute ações remotas, como bloqueios ou exclusão de dados, em caso de perda ou roubo.

- **Relatórios personalizados**
  Gere relatórios detalhados sobre o status e o uso dos dispositivos, facilitando a tomada de decisões estratégicas baseadas em dados.
- **Conformidade regulatória**
  Garanta que todos os dispositivos cumpram com regulamentações e políticas internas, minimizando riscos legais e operacionais.
- **Controle do uso de aplicativos**
  Defina quais aplicativos podem ser instalados ou executados nos dispositivos corporativos, evitando o uso de softwares não autorizados ou potencialmente perigosos.

Principais Funcionalidades de Aranda Enterprise Mobility Management

Gestão integral de dispositivos móveis

AEMM centraliza a gestão de dispositivos Android e iOS, garantindo segurança, monitoramento e conformidade regulatória. Facilita a aplicação de políticas corporativas, permite o controle em tempo real e minimiza riscos de segurança, otimizando a eficiência operacional.

Ações remotas

Permite executar ações como bloqueio, redefinição de senhas, localização, envio de mensagens e restauração de fábrica sem a intervenção do usuário.

Proteção contra dispositivos comprometidos

Identifica e restringe o acesso de dispositivos com alterações de segurança (Jailbroken/Rooted), prevenindo riscos de acesso não autorizado e vulnerabilidades na rede corporativa.

Gestão segura de dispositivos pessoais (BYOD)

Permite administrar de forma segura aplicativos e informações corporativas em dispositivos pessoais por meio de ambientes separados, garantindo a proteção dos dados empresariais.

Auditoria de atividade no console

Monitoria e auditoria das operações realizadas no console, registrando mudanças de configuração, políticas e principais eventos. Permite filtrar registros por data, usuário e ação, além de exportá-los para análise.

Gestão de alertas e eventos

Oferece um sistema centralizado de alertas para incidentes de segurança ou mudanças críticas nos dispositivos, permitindo respostas rápidas e mitigação de riscos.

Localização e rastreamento em tempo real

Fornece geolocalização precisa dos dispositivos com níveis ajustáveis de precisão, permitindo visualizar sua localização em tempo real.

Restrição de uso por localização (Geofencing)

Define limites geográficos para o uso dos dispositivos e ativa ações automáticas ao entrar ou sair de áreas predefinidas. Permite gerar alertas, restringir funções ou aplicar mudanças de segurança para reforçar políticas corporativas e proteger informações sensíveis.

Restrição de uso por horário (Timefencing)

Configura horários permitidos para o uso dos dispositivos e executa ações automatizadas como bloqueio, alteração de senha, restrição de conteúdo ou envio de alertas quando os horários estabelecidos são violados.

Restrição de uso por rede Wi-Fi (WiFi-Fencing)

Monitora e controla as redes Wi-Fi às quais os dispositivos se conectam, permitindo ações como bloqueio, envio de alertas ou restrições ao acessar redes não autorizadas, reforçando a segurança e o cumprimento das políticas corporativas.

Localização com alerta sonoro

Habilita a ativação remota de sons para facilitar a localização de dispositivos em espaços fechados, otimizando a recuperação de ativos móveis.

Gestão centralizada de aplicativos

Permite a instalação, atualização e remoção de aplicativos remotamente, garantindo que os dispositivos possuam apenas software autorizado. Além disso, possibilita a criação de listas brancas e negras para restringir ou permitir o uso de aplicativos específicos.

Distribuição segura de conteúdos

Facilita o armazenamento e o acesso a documentos empresariais por meio de um contêiner seguro, garantindo a confidencialidade das informações.

Modo Quiosque para uso controlado

Configura dispositivos no modo Quiosque, restringindo o acesso apenas a aplicativos aprovados, evitando distrações e garantindo seu uso exclusivamente para atividades corporativas.

Restrição de funções do dispositivo

Desativa funções como câmera, Bluetooth e Wi-Fi conforme os requisitos de segurança, prevenindo riscos de vazamento de dados ou acessos não autorizados.

Monitoramento de atividades nos dispositivos

Monitora em tempo real os eventos nos dispositivos, incluindo o ciclo de vida de comandos e atividades como envio de localização, mudanças de zona e desvinculação. Oferece um histórico detalhado para garantir rastreabilidade e segurança.

Gestão centralizada de Políticas

Permite atribuir e administrar parâmetros específicos em dispositivos móveis para definir seu contexto de operação, incluindo configurações de segurança, restrições de uso e ajustes personalizados. O AEMM facilita a edição, aprovação e versionamento de políticas, garantindo sua conformidade por meio de ferramentas de monitoramento, relatórios e notificações em caso de descumprimento.

Automação por meio de Regras

Responde automaticamente a eventos críticos, como mudanças de usuário, desvinculação, consumo anômalo de dados, localização, conexão a redes Wi-Fi e horários de operação. Diante dessas situações, o sistema age imediatamente com alertas, ajustes de políticas, bloqueios e restrições, garantindo segurança e conformidade.

Com o Aranda Enterprise Mobility Management, você pode centralizar o gerenciamento de acesso, controle de aplicativos, proteção de dados e segurança para todos os dispositivos móveis usados na sua empresa, ao mesmo tempo em que limita despesas e controla os investimentos em mobilidade.

Criptografia de informações

Protege os dados corporativos armazenados nos dispositivos por meio de criptografia avançada, prevenindo acessos não autorizados e garantindo a segurança da informação.

Controle com Android for Work

Fornece ferramentas avançadas para a gestão e supervisão de dispositivos Android, garantindo seu alinhamento com as políticas empresariais.

Controle do consumo de dados

Monitora em tempo real o uso de voz e dados, permitindo estabelecer alertas e restrições para evitar custos excessivos nos planos de telecomunicações.

Controle Remoto

Gerencia dispositivos remotamente a partir da console do AEMM, agilizando o suporte técnico e a resolução de problemas em tempo real. As sessões exigem confirmação do usuário para garantir um acesso seguro e evitar invasões não autorizadas.

Administração segmentada por grupos

Atribui dispositivos a grupos e os vincula a especialistas de acordo com suas áreas de responsabilidade. Isso melhora a eficiência, garantindo que cada especialista gerencie apenas os dispositivos relevantes, otimizando permissões e acessos.

Além disso, facilita a distribuição de configurações de maneira estruturada.

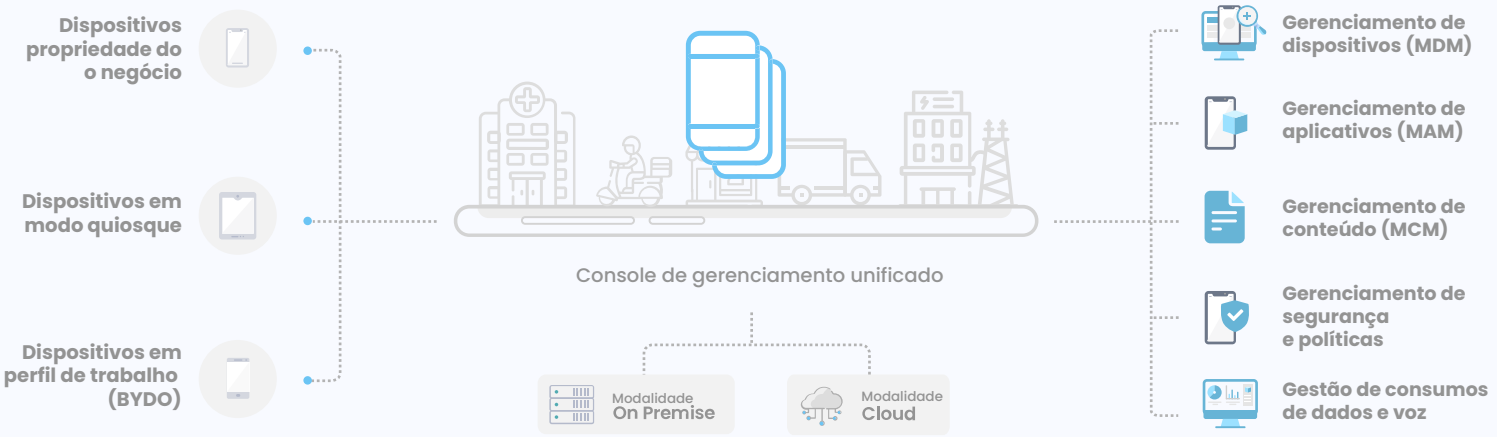
Grupos dinâmicos de dispositivos

Agrupa automaticamente dispositivos com base em critérios como sistema operacional, modelo ou propriedade. Isso permite a aplicação de configurações, políticas e regras de forma massiva e eficiente. Os dispositivos entram ou saem dos grupos dinamicamente conforme suas características, garantindo que sempre recebam as ações adequadas.

Configurações gerenciadas para aplicativos

Garante que os aplicativos corporativos sejam instalados com as configurações adequadas desde o primeiro uso, otimizando a experiência do usuário e reduzindo erros. Além disso, permite restringir configurações que possam comprometer a segurança ou o uso corporativo, garantindo um ambiente controlado e eficiente.

Habilite com segurança o uso de dispositivos e aplicativos e conteúdo para sua força de trabalho móvel



Métricas de uso de aplicativos

Fornece análises detalhadas do consumo de dados e do tempo de uso de cada aplicativo nos dispositivos. Essas informações facilitam a otimização de recursos e melhoram a tomada de decisões para uma gestão eficiente.

Projetos de gestão

Otimiza a configuração e administração de múltiplos dispositivos por meio de projetos de gestão. Através de um arquivo .CSV com os IMEIs dos dispositivos, permite aplicar ações em lote, como ativar o modo perdido, localizar dispositivos, obter inventários, executar scripts ou instalar aplicativos.

Scripts remotos

Permite a execução remota de scripts nos dispositivos para antecipar necessidades operacionais, facilitando tarefas como instalação e desinstalação de aplicativos, modificação de configurações e gerenciamento de armazenamento.

Apagamento remoto de dados

Elimina total ou seletivamente as informações armazenadas em dispositivos perdidos ou comprometidos, garantindo a proteção de dados sensíveis e a conformidade com as normas de segurança.

Análises e relatórios avançados

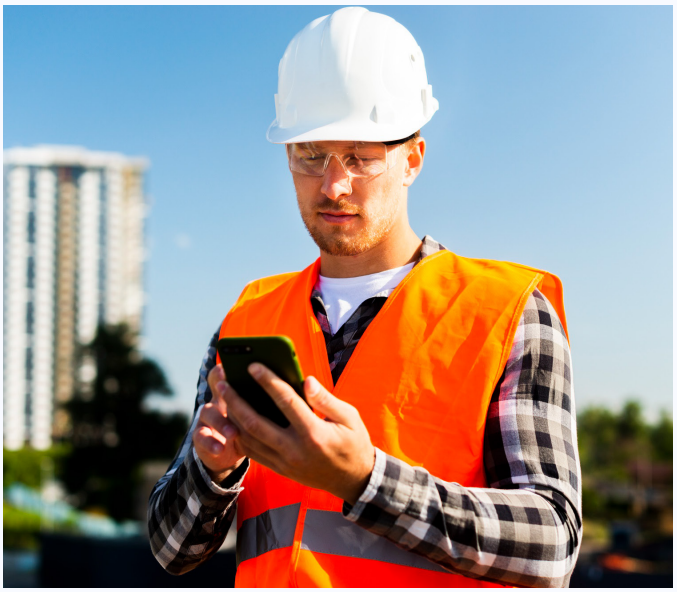
Fornece dashboards interativos com métricas-chave sobre inventário, status dos dispositivos e consumo de recursos, facilitando a tomada de decisões estratégicas.

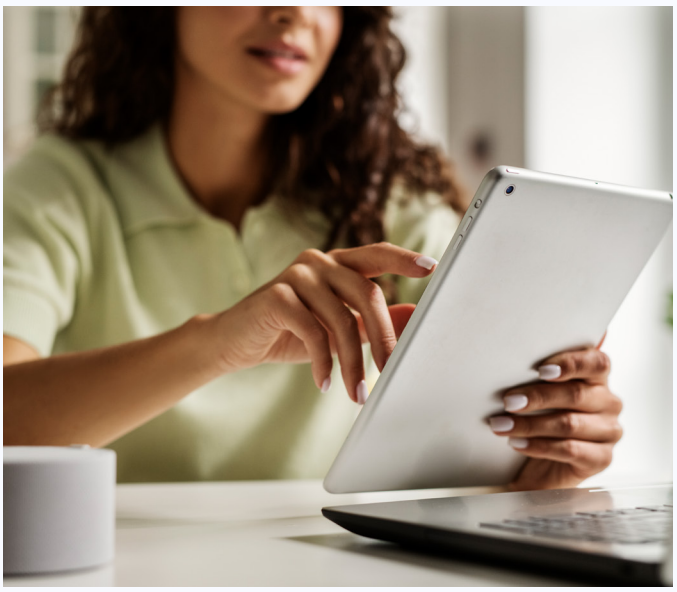
Licenciamento

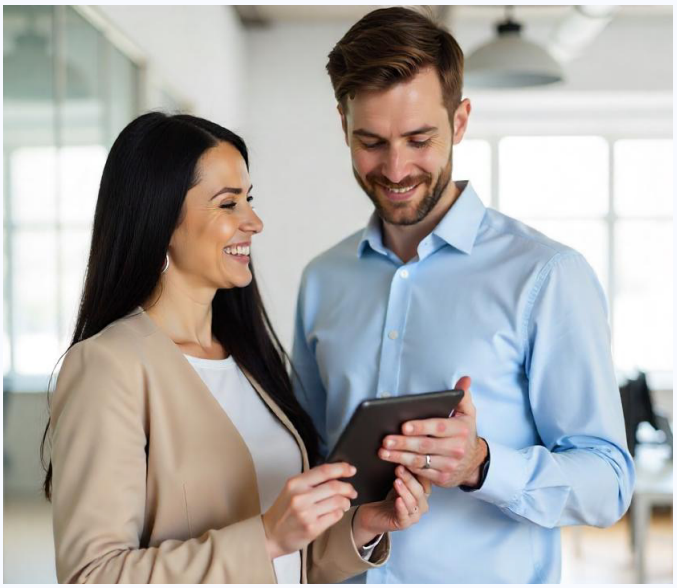
O AEMM é licenciado por endpoint ou ativo gerenciado. Um endpoint ou ativo gerenciado é qualquer dispositivo móvel (Android, iOS) que exija atividades de gestão por meio do agente.

Gestão do ciclo de vida com CMDB

Cada licença adquirida para a gestão de endpoints ou ativos por meio do agente AEMM inclui uma licença de CI no CMDB. Para administrar ativos não computacionais ou ativos de TI que não possam ser gerenciados pelo agente, é possível adquirir pacotes adicionais de CIs.







Acessos incluídos

O licenciamento do AEMM concede acesso às ferramentas de relatórios AQM e à gestão do ciclo de vida de ativos CMDB, com os seguintes acessos concorrentes:

- Cinco (5) acessos concorrentes de usuários/técnicos para o console do AEMM.
- Três (3) acessos concorrentes de usuários/técnicos para o console do AQM.
- Três (3) acessos concorrentes de usuários/técnicos para o console do CMDB.

Esses acessos estão incluídos por padrão e não dependem da quantidade de licenças adquiridas para a gestão de ativos móveis.

Integrações

AEMM amplia suas capacidades ao se integrar de forma nativa com nossas soluções de CMDB e relatórios avançados, otimizando a gestão de ativos de TI e proporcionando uma visão detalhada da infraestrutura tecnológica.

Integração com Aranda CMDB

Acompanhe o ciclo de vida de seus dispositivos móveis por meio da integração do AEMM com o Aranda CMDB. Essa integração permite atualizar automaticamente os elementos de configuração, detectando mudanças nos inventários dos dispositivos gerenciados. Isso melhora a rastreabilidade dos ativos móveis e facilita sua relação com os processos de Gestão de Serviço, como incidentes, requisições, problemas e mudanças.

A partir do CMDB, é possível acessar informações detalhadas sobre o ciclo de vida dos ativos móveis, incluindo:

- Entrada do dispositivo na empresa
- Fabricante, fornecedor e usuário responsável
- Faturas, contratos, garantias e manutenções
- Histórico de mudanças e eventos registrados

Além disso, o CMDB permite administrar contratos, faturas de hardware e licenças de software, bem como gerenciar garantias, manutenções e fornecedores. Isso proporciona uma visão completa do custo total de propriedade (TCO) dos ativos tecnológicos.

Integração com Aranda Query Manager

AEMM integrates with Aranda Query Manager to offer advanced reports and real-time indicators on the mobile device infrastructure and its compliance. Users can view detailed metrics and graphs on the device inventory, including installed applications, operating system versions, compliance status, and resource consumption.

Additionally, it allows generating predefined or customized reports on the management of mobile and IT assets, with the option to schedule their automatic delivery. This facilitates strategic decision-making, improves device governance, and ensures the organization's regulatory compliance.