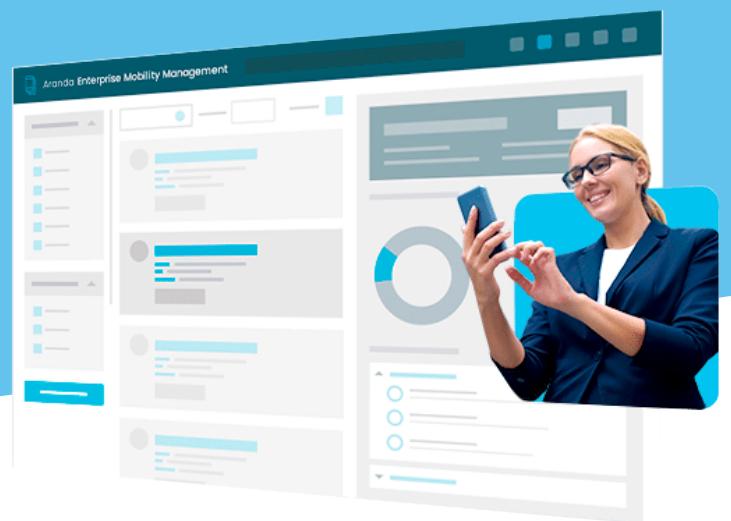


Enterprise Mobility Management



Gestão inteligente para potencializar a administração de dispositivos móveis

AEMM otimiza a gestão de dispositivos móveis, aplicativos, conteúdos e segurança a partir de uma única plataforma. Automatize processos, fortaleça a proteção de dados e melhore a produtividade com uma solução completa para a mobilidade empresarial.

Desafios

No mundo digital atual, a [mobilidade empresarial](#) tornou-se 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 lugar. 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 suscetível 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 a conformidade com as 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, a segurança e a conformidade regulatória dos dispositivos móveis, **garantindo proteção de dados, controle de aplicativos e 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 colaboradores.

Automação de tarefas

Otimize processos por meio da 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 atendam às normas 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 software não autorizado ou potencialmente perigoso.

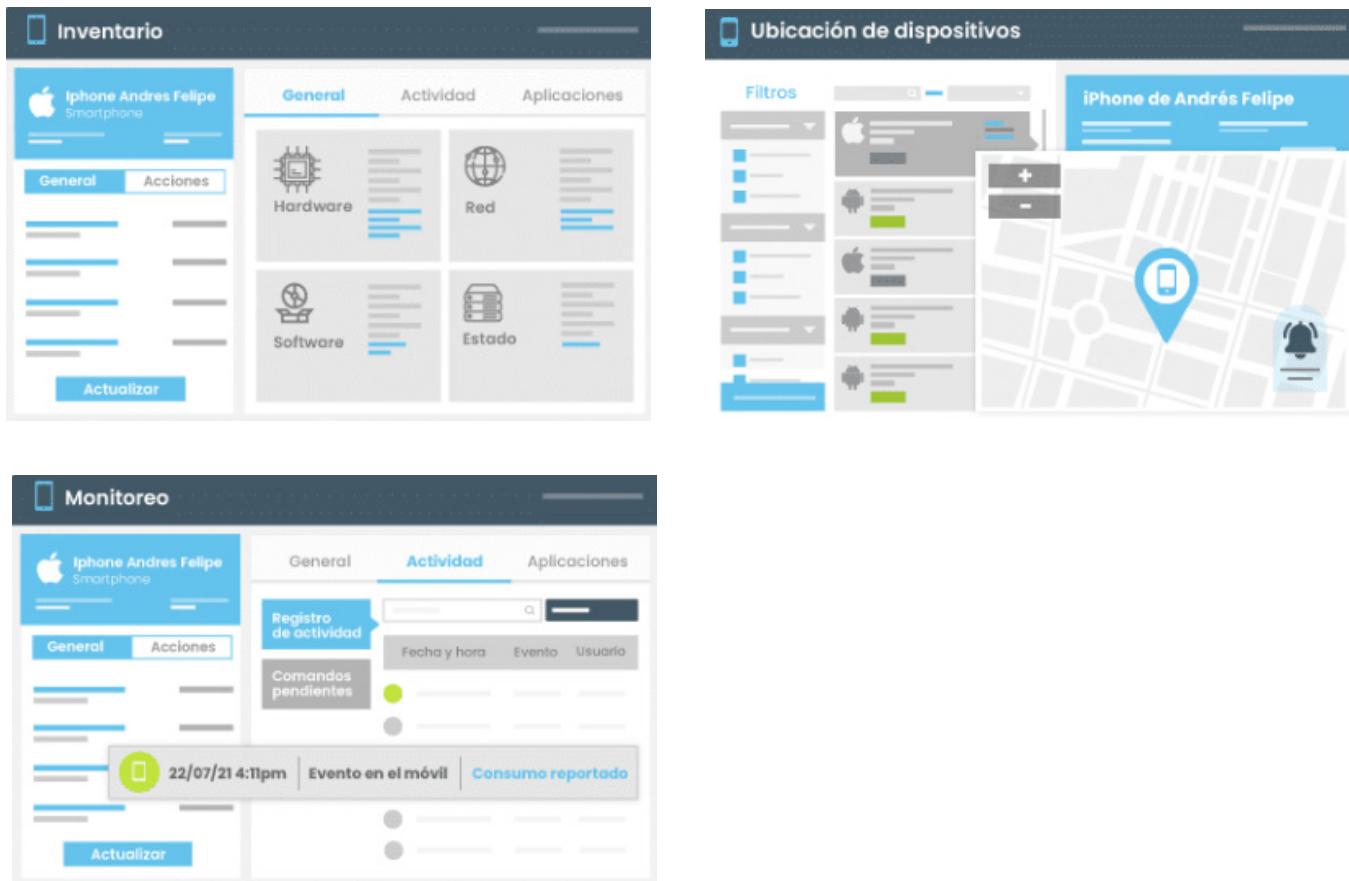


Principais competências de Aranda Enterprise Mobility Management

Gestão centralizada de dispositivos

AEMM oferece um [console único](#) para que as organizações [administrem centralmente seus dispositivos móveis](#), sejam eles [corporativos ou pessoais \(BYOD\)](#). A plataforma [automatiza](#) o inventário e permite o [monitoramento em tempo real](#) de localização, bateria, armazenamento e conectividade.

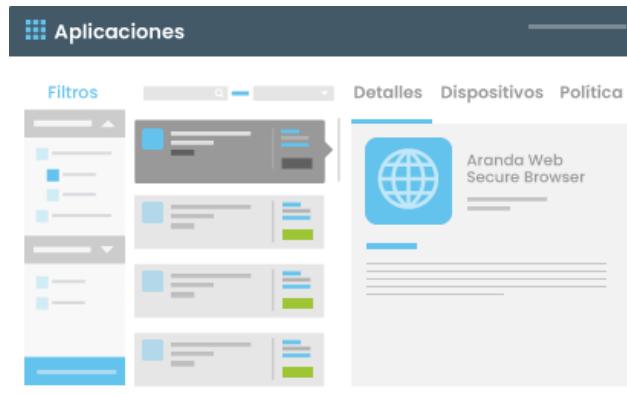
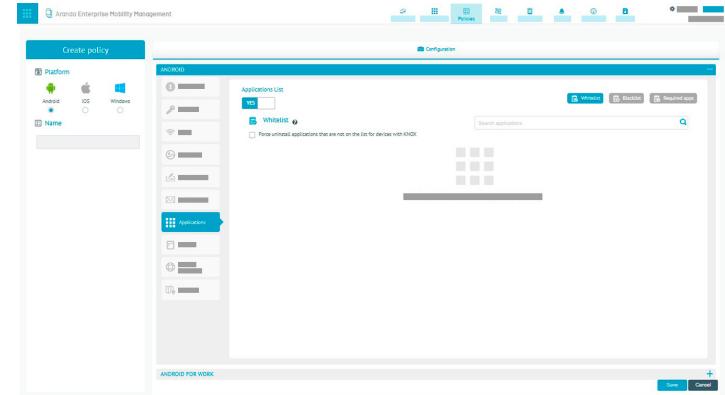
Ao [centralizar a administração](#), otimiza-se a [gestão operacional](#), [reduz-se a complexidade técnica](#) e melhora-se a eficiência, permitindo que a equipe de TI responda rapidamente a incidentes ou necessidades de configuração.



Distribuição e Gestão de Aplicações

AEMM otimiza a **implementação, atualização e supervisão de aplicativos empresariais em dispositivos móveis**. Por meio de **listas brancas e negras**, os administradores definem quais aplicativos podem ser instalados ou executados, garantindo que os usuários acessem apenas **ferramentas aprovadas**. Essa funcionalidade melhora a segurança e o desempenho do ambiente móvel, reduzindo vulnerabilidades e assegurando a conformidade com as **políticas corporativas**.

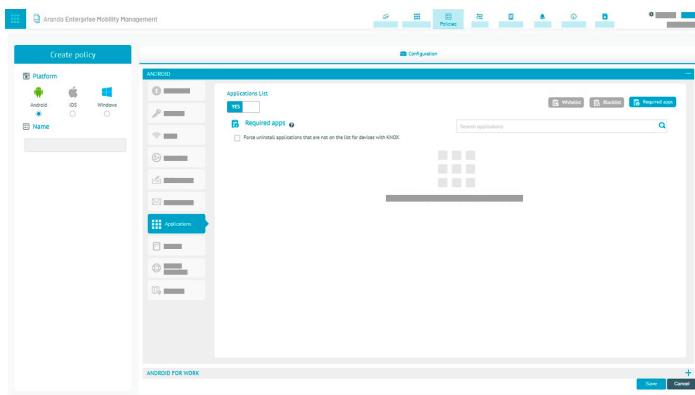
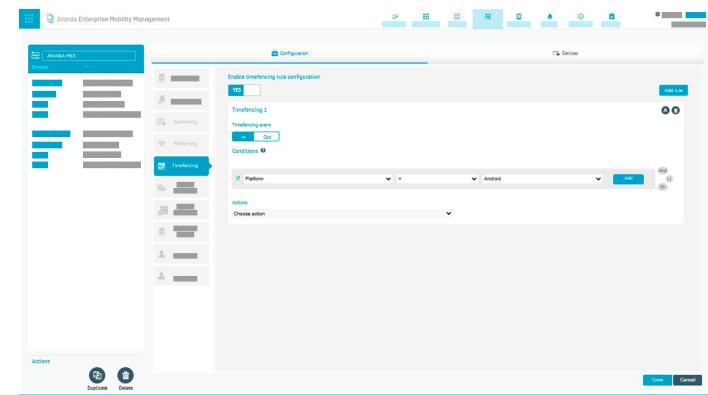
Além disso, permite a **distribuição em massa** de aplicativos internos ou de terceiros de forma remota, garantindo uma experiência homogênea e evitando **software não autorizado** que possa representar um risco de segurança ou vazamento de informações.

Controle de uso e restrições

A plataforma permite definir **políticas de uso rigorosas** para melhorar a **segurança** e otimizar os **dispositivos corporativos**. É possível estabelecer restrições no acesso a redes não seguras, no uso de aplicativos não autorizados e no consumo excessivo de dados móveis.

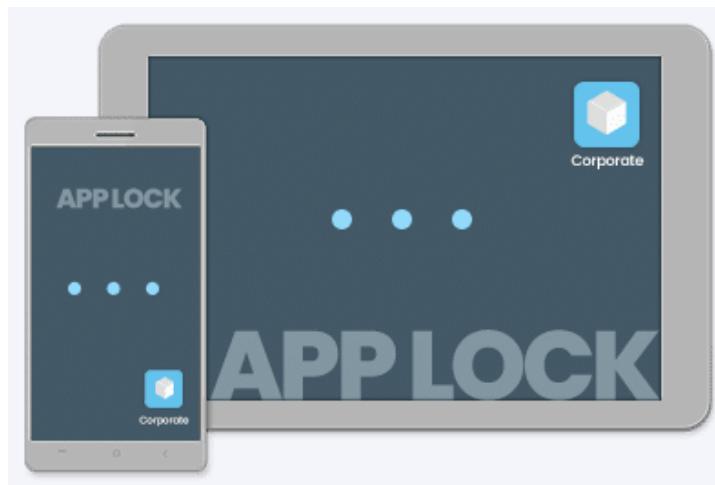
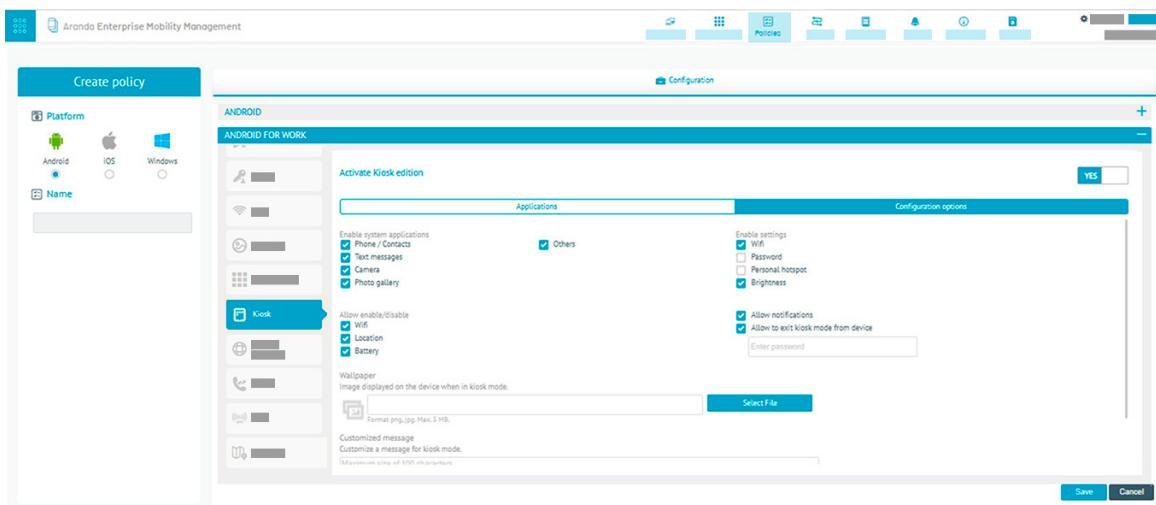
Além disso, o AEMM incorpora **geofencing, timefencing e WiFifencing**, que limitam o uso dos dispositivos a locais específicos, faixas de horário ou redes Wi-Fi autorizadas. Essas medidas possibilitam uma gestão eficiente dos **recursos tecnológicos**, reduzindo riscos, otimizando custos e garantindo um uso exclusivo para **fins profissionais**, evitando acessos indevidos a informações sensíveis.

Gestão de Dispositivos no Modo Kiosk

AEMM permite configurar dispositivos no [modo kiosk](#), restringindo sua funcionalidade a [aplicativos e configurações específicas](#). Essa funcionalidade é especialmente útil em setores que exigem dispositivos dedicados a funções como [autoatendimento, pontos de venda ou estações de consulta](#). Ao limitar o acesso a configurações não autorizadas, minimiza-se o [risco de uso indevido](#) e melhora-se a produtividade, garantindo que os dispositivos sejam utilizados apenas para os [fins previstos](#).

Além disso, o [AEMM](#) oferece opções avançadas para a [gestão remota](#), permitindo sua reconfiguração sem intervenção física, agilizando a operação e reduzindo [custos de suporte técnico](#).



Por que Aranda Enterprise Mobility Management?



Configuração sem complicações

O AEMM permite uma vinculação ágil de dispositivos sem configurações prévias, otimizando o tempo de implementação. Sua interface intuitiva e fácil de usar garante uma experiência fluida para qualquer usuário.



Nas suas instalações ou nas nossas

Você escolhe Aranda Service Management está disponível como Software-as-a-Service (SaaS) e como solução On-Premises (instalada localmente), adaptando-se às necessidades da sua organização.



Falamos o mesmo idioma

Nossa equipe de Suporte especializada atende em português e no horário da América Latina. Nossa documentação técnica está disponível em vários idiomas (inglês, espanhol, português).



Reconhecimento global com foco na América Latina

Aranda Enterprise Mobility Management é reconhecida por analistas da indústria como uma das soluções de destaque para a gestão de serviços, atendendo às necessidades das empresas da América Latina.



Gestão centralizada, acesso sem limites

Administre tudo a partir de uma única plataforma 100% web, sem a necessidade de instalar consoles nos seus dispositivos, garantindo uma experiência ágil, integrada e acessível de qualquer lugar.



A segurança dos seus dados, nosso compromisso

A Aranda Software possui um rigoroso sistema de gestão da segurança da informação de seus clientes, certificado mundialmente pela norma ISO/IEC 27001:2022.

Segurança e conformidade regulatória

AEMM incorpora [medidas avançadas](#) de segurança para proteger as [informações corporativas em dispositivos móveis](#). Inclui [criptografia de dados](#), [políticas de acesso](#) e [detecção de dispositivos](#) comprometidos ([rooteados ou com jailbreak](#)). Também permite executar [ações remotas](#), como [exclusão e bloqueio](#), em caso de perda ou roubo, garantindo a proteção dos dados. Essas funcionalidades asseguram a conformidade com padrões como [GDPR](#), [ISO 27001](#) e outras regulamentações de segurança.

AEMM fornece um painel de [alertas em tempo real](#) e ferramentas de auditoria, facilitando a gestão de riscos e a alinhamento com as melhores práticas de segurança empresarial.

