Solution Brochure

Entrust® Mobile Device Management (MDM) Integration

Trusted, seamless certificate provisioning and management

ENTRUST
SECURING A WORLD IN MOTION

OVERVIEW

Secure, frictionless access to networks

The rise of digital business brings an increased and diverse set of challenges to enterprise IT departments worldwide. Today, many employees work remotely or are hot-desking, and personal and company-issued mobile devices are coexisting, adding complexity to the corporate infrastructure. To further complicate matters, usernames and passwords aren’t secure or user-friendly in environments where users need different credentials for different applications and networks.

IT departments need to leverage secure, transparent, and simple ways of identifying corporate assets and users to ensure trusted access to the corporate network from mobile devices. Keys and certificates issued by a public key infrastructure (PKI) offer the highest levels of security, provide users with frictionless means of authenticating to networks, and enable use cases such as secure email, file encryption, and non-repudiable digital signatures.

IT needs secure, transparent, simple ways of identifying corporate assets.

An MDM integration from Entrust

Entrust, a leading provider of PKI, integrates with the industry's leading MDM vendors to allow organizations to deploy and leverage strong identities for mobile devices.

Entrust's PKI as a Service (PKIaaS) offers a zero-touch, turnkey integration with top MDM/EEM vendors for enrollment and management for Windows, Chrome OS, Android, IOS, and macOS. This allows customers to leverage Entrust PKI seamlessly with their IT management platform within minutes. With this being flexible and extensible, devices of any kind can be enrolled securely with extended key and certificate parameters to support advanced identification, authentication, and authorization schemes. PKIaaS hosts all the required components to integrate with MDM/EEM vendors so that customers do not need to install or maintain any on-premises hardware or software.

KEY FEATURES & BENEFITS

- Provides strong user and device identities
- Eliminates reliance on mobile usernames and passwords
- Enhances user experience with transparent authentication
- Manages digital identities and devices in BYOD environments
- Secures mobile devices communicating with customer or enterprise environments
- Transparently deploys digital certificates to mobile devices to secure access to corporate networks and encrypt email
- Offers a variety of deployment methods, including cloud and on-premises models
- Cloud-native PQ-ready PKI that leverages 25+ years of Entrust PKI innovation and technology

HIGHLIGHTS

Seamless access to trusted identity assurance solutions

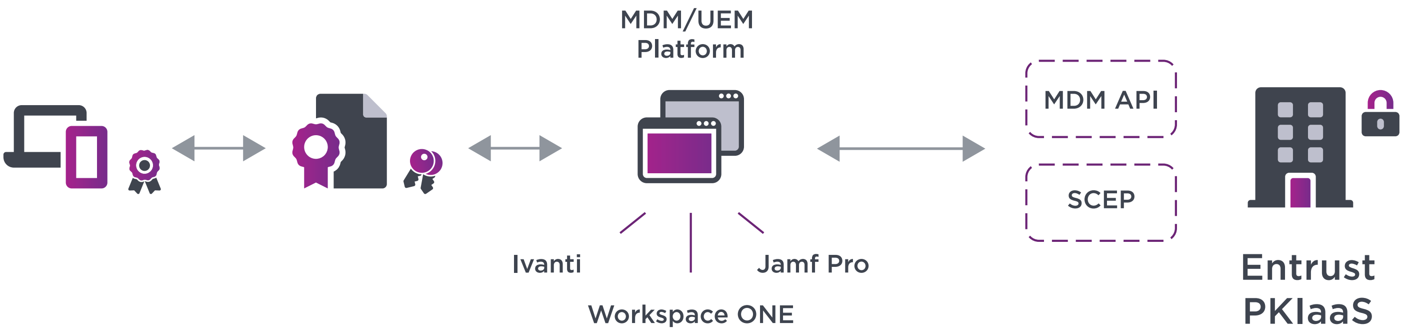
This strategic integration provides streamlined access to Entrust identity assurance solutions to companies that leverage MDM solutions, including on-premises services via Identity Enterprise and Entrust PKI and cloud services via Managed PKI.

Entrust PKI	MDM Vendors
Entrust PKI solutions provide trusted identities that protect and connect an organization's people, systems, and things. Entrust digital certificates allow organizations to leverage encryption and digital signatures. Entrust Security Manager helps organizations easily manage their security infrastructure, certificates, and digital keys.	Leading MDM solutions offer organizations the ability to manage mobile platforms, enforce policy, and ultimately enable enterprise mobility.

Key features create a strong, integrated solution

The power of this integration comes from multiple components working together to create a strong, integrated whole that makes mobile management secure and easy.

Powerful Digital Certificates	Flexible Infrastructure	Enterprise Mobility & BYOD
Entrust PKI solutions provide security-conscious organizations with digital certificates as the foundation of their identity-based access and security measures. Digital certificates allow organizations to leverage encryption and digital signatures to support a variety of security services, including user and device authentication, transaction integrity and verification, and data security. Digital certificates provide strong device identities to enable secure WiFi or VPN access. They can be leveraged on mobile devices to enable secure email (S/MIME) communication.	The Entrust offering delivers flexibility to MDM vendors, providing simple-to-use interfaces that can offer simple certificate enrollment as well as full administration and life cycle management, all from a single platform.	The integration between Entrust and MDM systems enables customers to easily manage digital identities on mobile devices. Organizations are able to leverage digital certificates on mobile devices via a simple device enrollment process and benefit from full certificate lifecycle management.



HOW IT WORKS

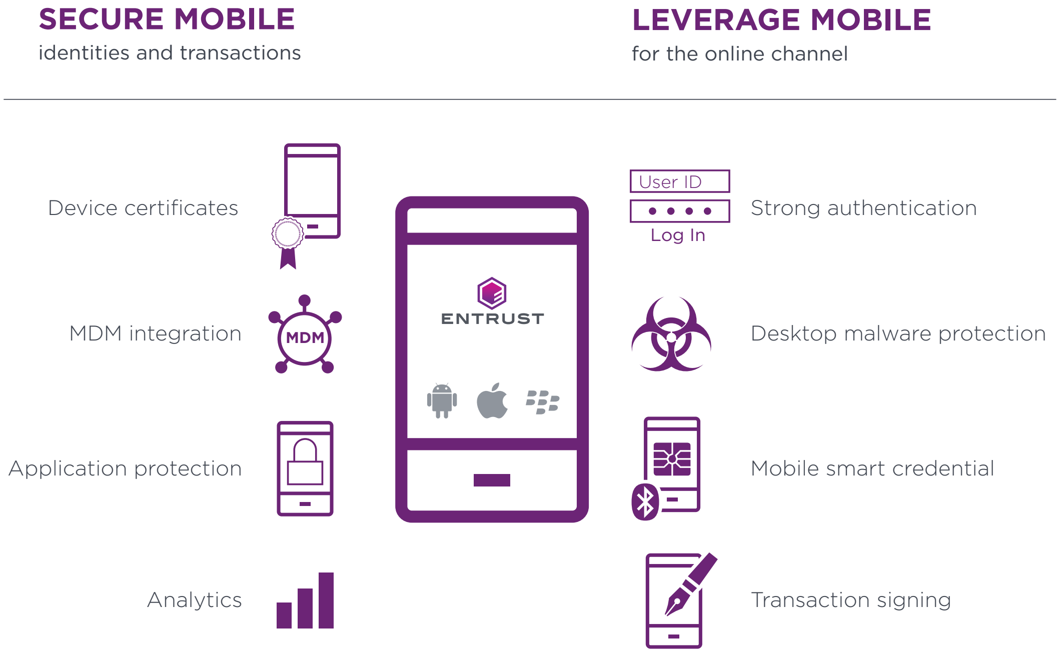
With this integrated solution, Entrust digital identities are transparently deployed on mobile devices to grant secure access to corporate networks and enable secure email. This flexible solution offers a range of Entrust on-premises, hosted, and pre-integrated MDM capabilities to suit the needs of your organization.

Certificate-based Authentication for Users and Devices

With the increase in identity-based attacks such as phishing and credential compromise, organizations need to enforce phishing-resistant authentication to secure access and mitigate cyberattacks. Certificate-based authentication is a high-assurance passwordless authentication that ensures only verified users and devices can authenticate to your network. By enabling certificate-based authentication for both users and devices, organizations can ensure that the user is trusted and verified and is authenticating themselves on a company-managed device for secure access to critical resources and data. The integrated Entrust Identity as a Service (IDaaS) and PKIaaS solution offers a turnkey solution to deploy and enable certificate-based authentication for users and devices.

Improved security, streamlined processes

Entrust offers a number of capabilities that not only help secure mobile identities and transactions but also empower organizations to leverage mobile devices to improve overall security and streamline business processes. Security controls are increased across all channels, enabling more convenience for employees and customers alike.



SECURE MOBILE
identities and transactions

Device certificates

MDM integration

Application protection

Analytics

LEVERAGE MOBILE
for the online channel

Strong authentication

Desktop malware protection

Mobile smart credential

Transaction signing

Entrust Integrations

Entrust has worked with the following vendors and solutions to deliver an integration against the Entrust MDM API or the Entrust SCEP Server:

- Microsoft Intune
- VMware AirWatch
- MobileIron
- SAP Afaria
- SOTI MobiControl
- BlackBerry
- IBM MobileFirst Protect (MaaS360)
- VMware Workspace ONE
- Google Enterprise MDM via SCEP protocol
- Ivanti
- Jamf Pro

For more information

888.690.2424
+1 952 933 1223
sales@entrust.com
entrust.com

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling strong identities, secure payments, and protected data. We offer an unmatched breadth of solutions that are critical to the future of secure enterprises, governments, the people they serve, and the data and transactions associated with them. With our experts serving customers in more than 150 countries and a network of global partners, it's no wonder the world's most trusted organizations trust us.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com entrust.com/contact