

Mobile Device Management Integration

Securing Mobile Identities & Devices

The proliferation of mobile devices presents tremendous opportunities for organizations to empower employees and increase business efficiency.

As the use of mobile devices and applications grows, so do the rate and sophistication of network and identity attacks on organizations and individuals. This momentum is compounded by the introduction of numerous management and provisioning challenges.

Enterprise Mobility & BYOD

Enterprises face a diverse set of challenges with personal and company-issued mobile devices co-existing within secure corporate infrastructures — all core to enterprise mobility and bring-your-own-device (BYOD) movements.

Mobile Foundation: Issuance, Management & Authentication

Organizations require a methodical and proven solution to issue and manage mobile devices. Administrators need to know who is accessing corporate networks and what information is stored on the devices.

The Mobile Enterprise

Today's leading mobile device management (MDM) solutions offer organizations the ability to manage mobile platforms, enforce policy and ultimately empower organizations to enable enterprise mobility.

However, granting secure access to corporate networks from mobile devices needs a strong and simple approach. Due to low security and unfriendly user experiences, usernames and passwords no longer suffice in the mobile world.

Powerful Digital Certificates

Security-conscious organizations rely on digital certificates as the foundation of their identity-based access and security measures. Digital certificates provide strong device identities to enable secure Wi-Fi or VPN access. In addition, organizations also may leverage digital certificates on mobile devices to enable secure email (S/MIME) communication.

The Solution — Entrust MDM Integration

Entrust integrates with the leading MDM platforms to allow organizations to deploy and leverage strong identities for mobile devices. Using this approach, Entrust digital identities are transparently deployed on mobile devices to grant secure access to corporate networks and enable secure email.

Solution Benefits

- Leverage mobile device management (MDM) platforms to enable strong device identity
- Eliminate reliance on mobile usernames and passwords for VPN and Wi-Fi access
- Enhance user experience with transparent authentication to VPN and Wi-Fi access points
- Provision and manage digital identities and devices in BYOD environments
- Secure mobile devices communicating with customer or enterprise environments
- Leverage a variety of deployment methods, including cloud and on-premise models

 entrust.com/mobile

ENTRUST MDM INTEGRATION ARCHITECTURE

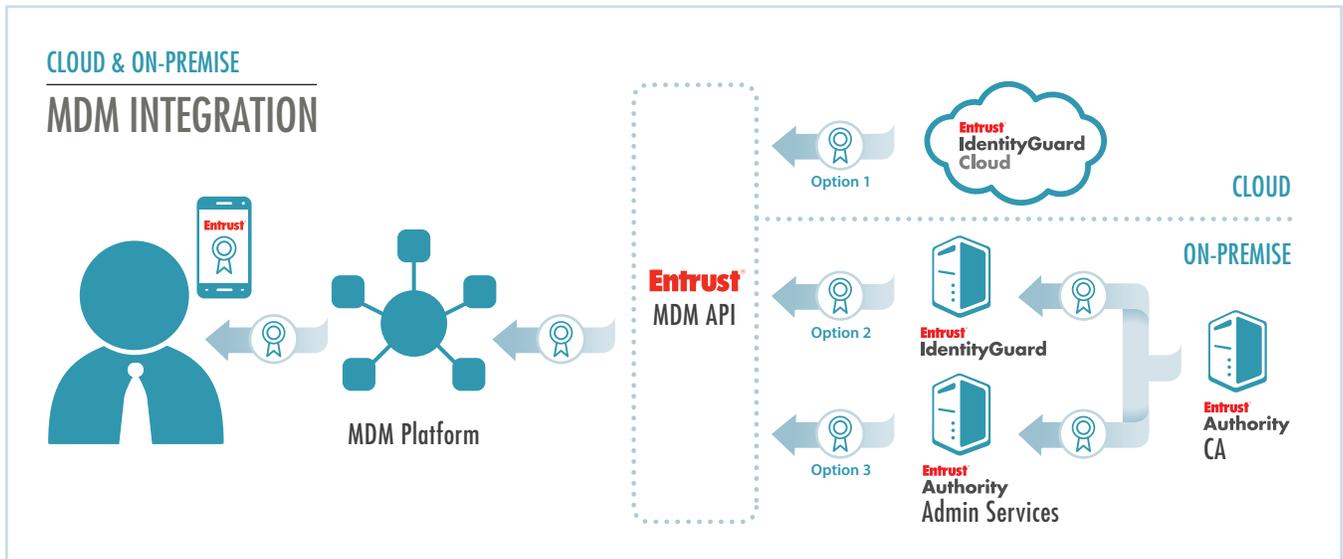


Figure 1: Entrust offers a range of on-premise, hosted and pre-integrated mobile device management (MDM) capabilities to suit the needs of your organization.

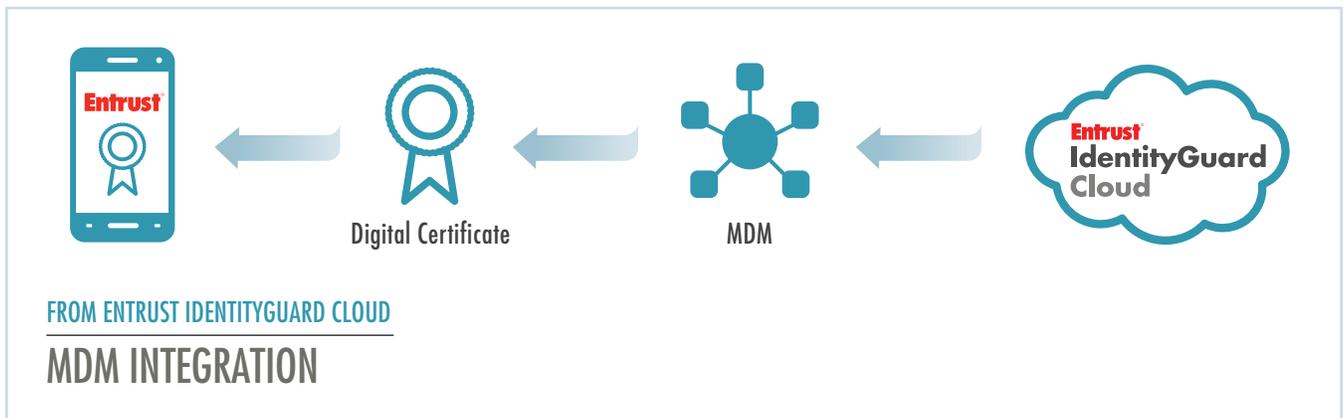
DIRECT MDM INTEGRATION

Digital certificates may be provisioned and managed through a variety of methods. Whether deployed via cloud or on-premise models, organizations may select the method that best suits their security needs, budget and environment.

From Entrust IdentityGuard Cloud

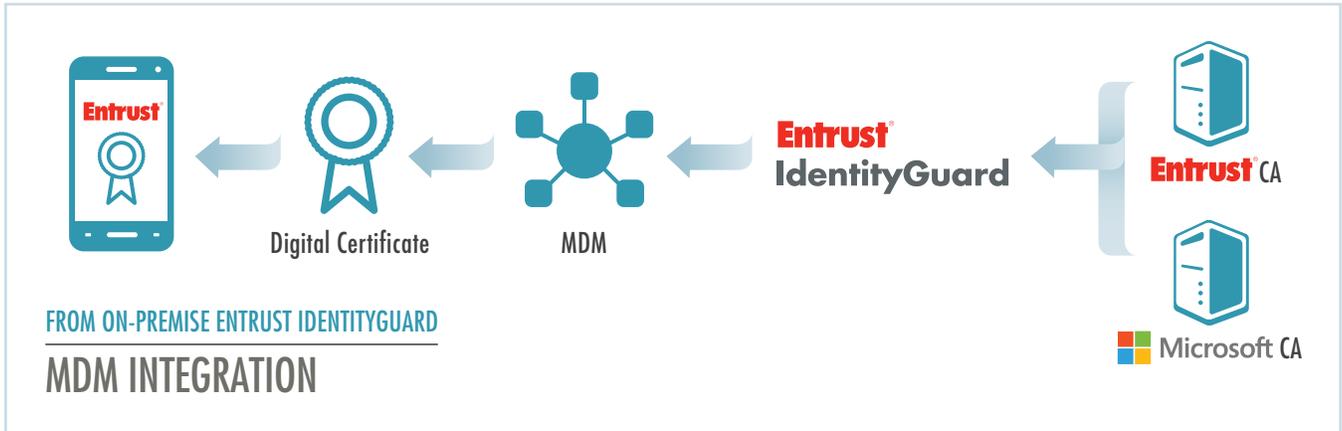
With Entrust IdentityGuard Cloud, organizations may seamlessly provision and manage digital certificates and identities — for both users and devices. This approach reduces costs, increases efficiency and simplifies setup and deployment.

Digital certificates are transparently delivered to mobile devices through a variety of leading cloud and on-premise MDM solutions. Entrust IdentityGuard Cloud removes the burden of deploying and managing an on-premise PKI/certification authority (CA).



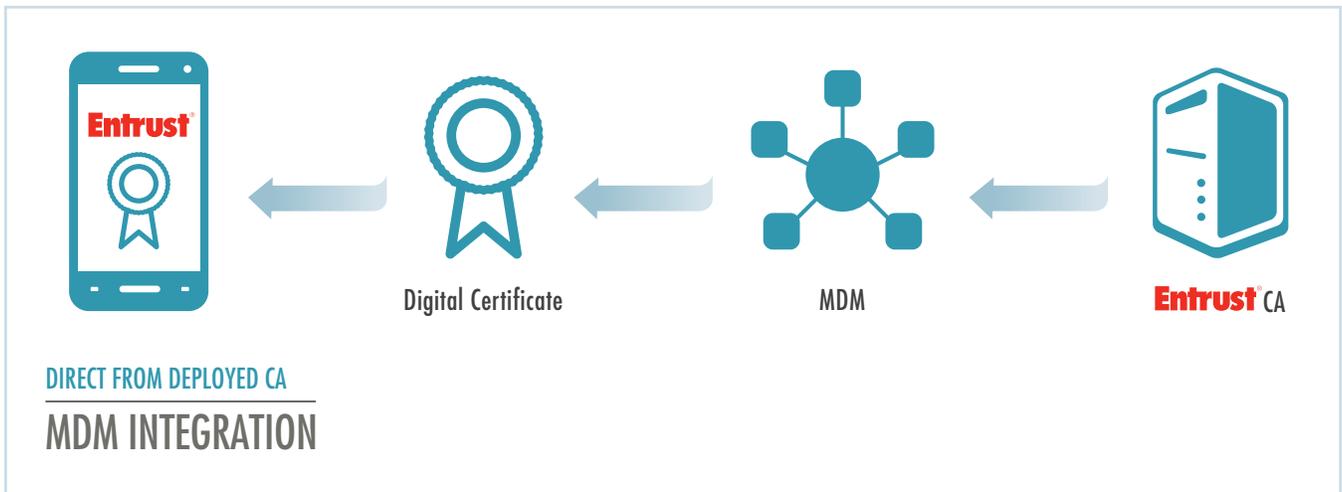
From On-Premise Entrust IdentityGuard

In addition to the platform's strong authentication capabilities, organizations may further leverage Entrust IdentityGuard to integrate with existing PKI and MDM solutions. This provides administrators and IT managers a holistic control of all authenticators.



Direct from Deployed CA

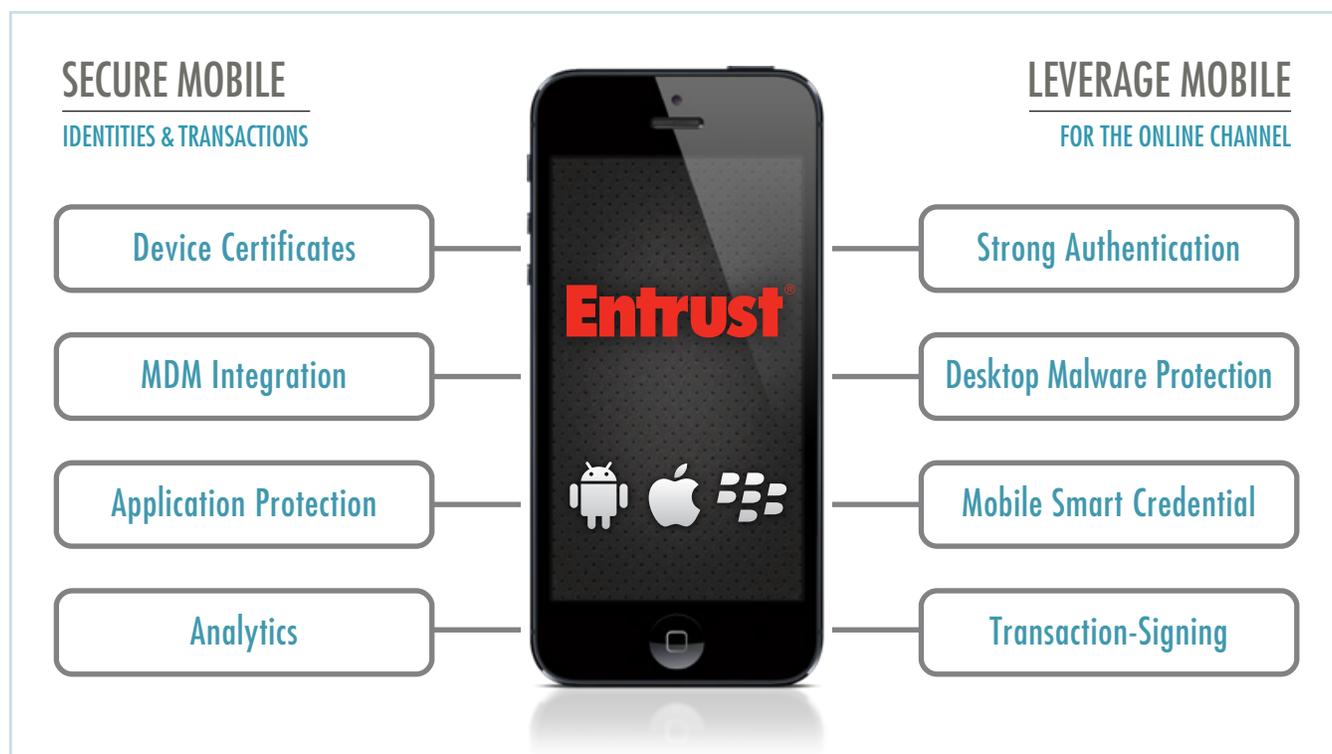
Many organizations rely on Entrust PKI to accomplish a wide range of high-assurance security measures. Featuring direct integration, Entrust Authority PKI supports a number of market-leading MDM solutions so organizations may utilize existing MDM deployments to provision and manage Entrust certificates on mobile devices.



SECURITY
ON

SECURE MOBILE, LEVERAGE MOBILE

Entrust solutions help secure mobile identities and transactions, but also allow organizations to leverage mobile devices to improve overall security. Whether to enhance strong authentication or eliminate usernames and passwords, Entrust helps organizations secure their mobile devices and subsequently leverage them to strengthen identity-based security.



MORE INFORMATION

The smart choice for properly securing digital identities and information, Entrust solutions represent the right balance between affordability, expertise and service. Discover how this will benefit you by contacting us at **888.690.2424** or via email at entrust@entrust.com.

Company Facts

Website: www.entrust.com
 Employees: 359
 Customers: 5,000
 Offices: 10 globally

Headquarters

Three Lincoln Centre
 5430 LBJ Freeway, Suite 1250
 Dallas, TX 75240 USA

Sales

North America: 1-888-690-2424
 EMEA: +44 (0) 118 953 3000
 Email: entrust@entrust.com

About Entrust

A trusted provider of identity-based security solutions, Entrust secures governments, enterprises and financial institutions in more than 5,000 organizations spanning 85 countries. Entrust's award-winning software authentication platforms manage today's most secure identity credentials, addressing customer pain points for cloud and mobile security, physical and logical access, citizen eID initiatives, certificate management and SSL. For more information about Entrust products and services, call **888-690-2424**, email entrust@entrust.com or visit www.entrust.com.

Entrust[®] Securing Digital Identities & Information