SECTIGO USE CASE | CERTIFICATE MANAGER FOR MICROSOFT INTUNE

Sectigo Certificate Manager for Microsoft Intune

Achieve greater visibility and control of your Mobile Device Certificates with Sectigo Certificate Manager for Microsoft Intune.

Many organizations use Microsoft Intune for mobile device management (MDM) to manage the mobile devices and the apps its employees use to securely access data and resources. Issuing digital certificates to those mobile devices provides additional protection from unauthorized access of critical business systems through WiFi, VPN, and email clients. Furthermore, certificates offer a better, more secure experience for employees with seamless authentication and can replace cumbersome passwords and multi-factor authentication (MFA) .

That is why security teams need a certificate management solution that can:

Integrate with Intune exporter or via Simple Certificate Enrollment Protocol (SCEP) to seamlessly and scalably issue user keys to mobile devices throughout the enterprise.

Automatically renew certificates upon request from Intune due to expiry, changes in certificate subject name, or cryptographic strength, so that device use is never disrupted.

Provide both publicly trusted and privately trusted certificates, as well as certificates to multiple Intune MDMs within the same enterprise, using a single pane of glass.

Sectigo can help

With Sectigo Certificate Manager, a complete management platform that automates the end-to-end lifecycle of certificates at scale, you can issue and manage the keys mobile users need across all devices. From a single dashboard, Sectigo Certificate Manager provides certificates to InTune, which installs them on the employee mobile device, and additionally installs certificates on contractors' devices which do not use the corporate InTune MDM.

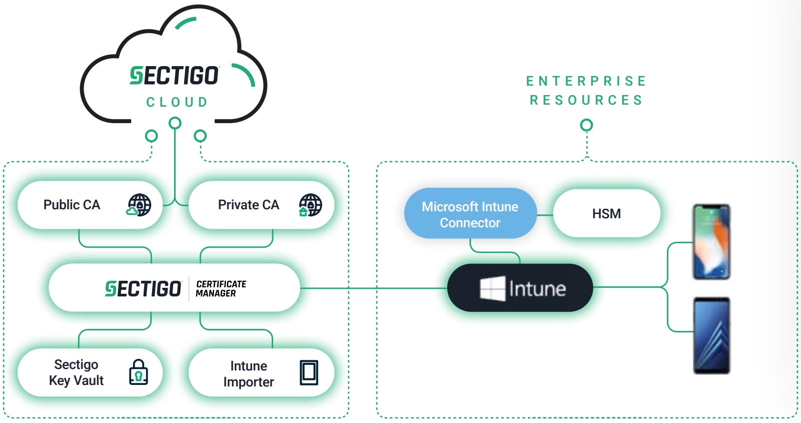
SECTIGO

Leveraging Sectigo Certificate Manager for Intune enables your security team to store and manage certificates in Sectigo Key Vault while also benefitting from:

- **Zero-Touch replication of keys for S/MIME.** Policy requires that keys are stored in a Hardware Security Module (HSM). Sectigo is the first CA to meet that requirement through a native integration with Intune and the only CA to ensure the same private key is installed in the mobile device that installed on other devices. Other certificate managers are limited to SCEP integrations, which does not support propagating the same private key to all devices owned by the user, and does not backup the private key in case of accidental destruction.
- **Zero-Touch replication of keys for mobile MS Outlook email.** Integration between Sectigo Certificate Manager and Intune allows Sectigo Certificate Manger to push keys that the MS Outlook email app can consume.
- **Zero-Touch issuance of certificates for Wi-Fi, VPN, and client authentication.** Sectigo Certificate Manager can issue certificates to mobile devices for Wi-Fi and VPN access. In addition, Sectigo can issue certificates with automatic installation to a wide range of non-mobile applications such as SSL certificates, including DV, OV, and EV for web servers, load balancers.
- **Automated certificate lifecycle management.** When Sectigo Certificate Manager is integrated with Intune, you don't have to manually issue, revoke/replace, or renew certificates. Intune requests authentication, digital signature, or encryption by the key stored in the Key Vault HSM.
- **Scalable certificate issuance.** Whether your mobile users number in the dozens, hundreds, or thousands, Sectigo Certificate Manager lets you issue certificates in an automated manner directly through Intune, minimizing the burden on your security team.
- **Future-proof certificate management.** If keys are compromised due to an Intune deficiency or advancements in quantum computing, Sectigo Certificate Manager issues a new key and Intune exporter triggers key replacement automatically as soon it detects a new key in the Sectigo Key Vault with no action needed from administrators.
- **Enhanced visibility and reporting.** Sectigo's native integration with Intune lets you view the status of the certificates in use through a single pane of glass, enabling you to see expiration dates and cryptographic strength while eliminating service disruptions for both public and private certificates.
- **Private key backup for S/MIME.** Using Intune exporter, private keys for S/MIME are backed up in Sectigo Key Vault prior to deployment to allow decryption of emails if the key is ever accidentally destroyed on the mobile device.

With Sectigo, you can enforce cryptographic strength, maintain compliance, and future-proof your business while minimizing costs. And Sectigo Certificate Manager can be used to automate issuance and lifecycle management of all other certificates throughout your organization, across a wide variety of use cases that require digital signing, authentication, and encryption.

Sectigo Certificate Manager for Microsoft Intune



- Certificate Manager generates key pairs, encrypts them using a key in HSM and pushes them, encrypted, to Intune.
- Intune uses MS Intune Connector to decrypt the key and encrypt it again for the registered device using a device key.
- The device downloads the encrypted key and decrypts it using a private device key.
- The key is used for S/MIME, WI-FI or SSL client authentication.

About Sectigo

Sectigo is a leading cybersecurity provider of digital identity solutions, including TLS / SSL certificates, DevOps, IoT, and enterprise-grade PKI management, as well as multi-layered web security. As the world's largest commercial Certificate Authority with more than 700,000 customers and over 20 years of experience in online trust, Sectigo partners with organizations of all sizes to deliver automated public and private PKI solutions for securing webservers, user access, connected devices, and applications. Recognized for its award-winning innovation and best-in-class global customer support, Sectigo has the proven performance needed to secure the digital landscape of today and tomorrow. For more information, visit www.sectigo.com and follow @SectigoHQ.