Sectigo Certificate Manager for Microsoft Intune

Many organizations use Microsoft Intune for mobile device management (MDM). But for enterprises that use certificates for Secure/Multipurpose Internet Mail Extensions (S/MIME), Wi-Fi, VPN, and client authentication, Intune cannot issue and manage user keys, which are trusted by many mobile devices that access enterprise connections and email.

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

- Integrate with Intune to seamlessly and scalably issue user keys and provide asymmetric cryptography to mobile devices throughout the enterprise
- Automatically renew certificates due to expiry, changes in certificate subject name, or cryptographic strength, so that device use is never disrupted
- Improve visibility using a single pane of glass, alleviating the headache of multiple key management portals, across multiple MDM and cloud vendors

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. Sectigo Certificate Manager supports all certificate types and is interoperable with all leading devices, operating systems, and enrollment protocols.

SECTIGO

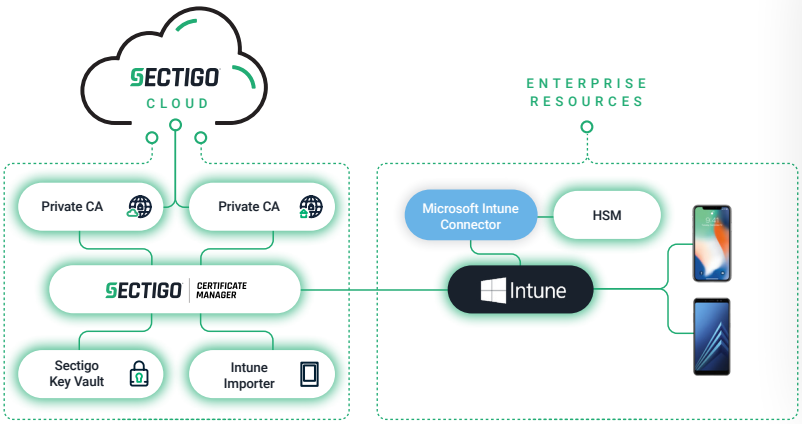
WWW.SECTIGO.COM

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 distribution of keys across devices**
  S/MIME requires that the same keys are distributed across multiple devices used for email. Sectigo is the first CA to meet that requirement through a native integration with Intune. Enrollment to native email applications uses Simple Certificate Enrollment Protocol (SCEP).
- **Zero-Touch deployment of keys for mobile MS Outlook email**
  Integration between Sectigo Certificate Manager and Intune allows Sectigo Certificate Manager 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 for Wi-Fi and VPN access, as well as for all types of SSL certificates, including DV, OV, and EV for web servers, load balancers, and API gateways.
- **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 communicates with Sectigo Key Vault transparently, eliminating the need to manage multiple certificate management portals.
- **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 hassle for your security team.
- **Future-proof certificate management**
  If keys are compromised due to an Intune deficiency or advancements in quantum computing, the administrator can use Sectigo Certificate Manager to force early renewal to cryptographically stronger certificates and keys.
- **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.

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 pair, encrypts them using a key in HSM and pushes encrypted to Intune.
- Intune uses MS connector to decrypt the key and encrypt again for the registered device using a device key.
- Device downloads the encrypted key and decrypts it using a private device key.
- Key is used to 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.

SECTIGO