

Sectigo certificate integration for Cisco Firepower Threat Defense (FTD)

Cisco FTD is a comprehensive security appliance widely adopted by enterprises. While Cisco FTD protects against various threats, effective SSL/TLS certificate management is essential for secure data transmission and device authentication. Without proper certificate management, networks are vulnerable to attacks and unauthorized access. Issuing and managing SSL/TLS certificates to protect Cisco FTD should be fully automated and highly scalable.

When selecting a certificate lifecycle management platform, Cisco FTD users should prioritize visibility and automation within their infrastructure. The platform must enhance visibility and operational efficiency through automated workflows, accommodate future scalability, and offer reliable support and maintenance services to ensure continuous, secure, and efficient operation.

Below are a few considerations when choosing a Certificate Lifecycle Management (CLM) platform that works:

- ✔ Lists, enrolls, replaces, and renews SSL/TLS certificates quickly and reliably
- ✔ Automates workflows to handle increasing certificate needs at scale
- ✔ Supports via automation technologies like REST API and SDK
- ✔ Centralizes control and visibility without leaving the Cisco ecosystem
- ✔ Provides comprehensive support for various SSL/TLS certificates, including wildcard and multi-domain
- ✔ Provides reliable customer support and regular updates

Sectigo can help

With the Sectigo-Cisco FTD integration, you can easily manage your certificates and protect the network infrastructure behind SSL decryption, all without leaving the Cisco ecosystem. This integration offers a scalable solution to effortlessly enroll, renew, replace, and list your SSL/TLS server certificates, supported through REST API and Software Development Kit (SDK).

Sectigo connector for Cisco FTD

The Sectigo Connector for Cisco FTD is designed to simplify and automate the management of digital certificates that can be used for the SSL Decryption feature. The connector facilitates various certificate lifecycle operations, such as enrollment, renewal, and replacement, ensuring secure SSL/TLS communications.

By supporting both private and public CAs, and accommodating a range of certificate types, the Sectigo Connector enhances the security infrastructure of Cisco FTD deployments, making it an indispensable asset for robust network defense.

Leveraging Sectigo connector for Cisco FTD enables your IT teams to benefit from:



Scalable issuance of SSL/TLS certificates

Sectigo enables IT administrators to automate the issuance and installation of valid certificates to Cisco FTD appliances.



Automated certificate renewal

Sectigo offers seamless automation technologies that automatically renew and install new certificates as they approach expiration, ensuring continuous security and eliminating the risk of downtime.



Full certificate lifecycle management

In addition to certificate renewal, Sectigo provides certificate replacement capabilities. This is necessary, for example, when key size, algorithm, or SAN changes.



Strengthened security for integration credentials

Increased flexibility to protect your integration credentials with advanced encryption and decryption capabilities against unauthorized access.



Enhanced visibility

Easily monitor all certificate actions, track their usage, and access detailed insights into package versions, without leaving your preferred environment.



Easy setup

Sectigo's integration for Cisco FTD supports REST API and SDK, enabling seamless setup and operation with both private and public CAs.



Comprehensive support

Sectigo supports a wide range of SSL/TLS certificates, including wildcard and single domain, as well as RSA certificates, ensuring all your security needs are met.

The Sectigo advantage: When you integrate Sectigo CLM with Cisco FTD, you can enjoy a range of benefits. These include the convenience of seamless auto-renewal for expiring certificates, which guarantees uninterrupted protection. Our scalable solution supports Cisco FTD environments and simplifies deployment with automated certificate issuance based on predefined configurations, reducing administrative overhead.

In addition, we have implemented advanced encryption and decryption capabilities using AES-256 to ensure the security of integration credentials and sensitive data. Together, these features provide a comprehensive, streamlined security solution, enhancing the overall protection and efficiency of your Cisco environment.

Sectigo SSL/TLS certificates and CLM help you enforce cryptographic strength, maintain compliance, and prepare for a post-quantum world, all while keeping certificate operations simple at scale. Integrating Sectigo with Cisco FTD automates certificate issuance and lifecycle management, eliminating the manual processes that lead to outages. For more information on Sectigo's Cisco FTD integration, SSL/TLS certificates or certificate management in general please contact Sectigo Sales at sales@sectigo.com.



About Sectigo

Sectigo is a leading provider of Certificate Lifecycle Management (CLM), helping organizations secure human and machine identities while reducing the hidden risks of modern digital trust. As certificate volumes grow and lifespans shrink, unmanaged certificates are becoming a source of outages, compliance exposure, and operational disruption. Sectigo uses Orchestrated Automation to deliver Simplicity at Scale through its cloud native CLM platform, bringing visibility, control, and lifecycle management together across complex environments. With more than 700,000 customers, including 65% of the Fortune 500, Sectigo is one of the largest and longest standing certificate authorities, with over 20 years of delivering unparalleled digital trust. For more information, visit www.sectigo.com or follow us on [LinkedIn](#).

