Sectigo Certificate Integration for Cisco Firepower Threat Defense (FTD)

Cisco FTD is a comprehensive security appliance that enterprises widely adopt. 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 an SSL/TLS certificate management solution, Cisco FTD users should prioritize visibility and automation within their infrastructure. The solution 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 the Certificate Lifecycle Management (CLM) solutions that work:

- List, enroll, replace, and renew SSL/TLS certificates quickly and reliably.
- Automated workflows to handle increasing certificate needs at scale.
- Support via automation technologies like REST API and SDK.
- Centralized control and visibility without leaving the Cisco ecosystem.
- Comprehensive support for various SSL/TLS certificates, including wildcard and multi-domain.
- Reliable customer support and regular updates.

Sectigo can help

With the Sectigo-Cisco FTD integration, you can easily manage your certificates and secure your network infrastructure used for SSL decryption to secure data transmission 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 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.

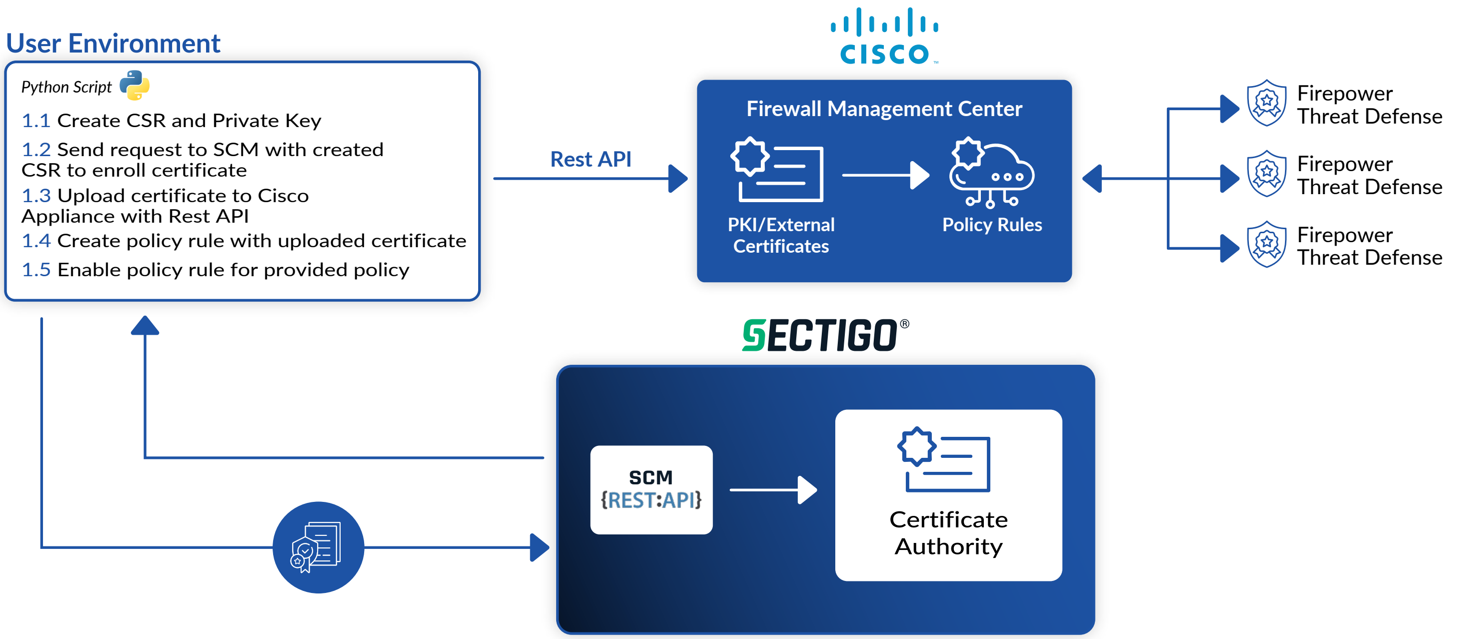
Strengthened security for integration Credentials: Increased flexibility to protect your integration credentials with advanced encryption and decryption capabilities against unauthorized access.

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

Easy set up: 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.

How it works



User Environment

Python Script

1.1 Create CSR and Private Key

1.2 Send request to SCM with created CSR to enroll certificate

1.3 Upload certificate to Cisco Appliance with Rest API

1.4 Create policy rule with uploaded certificate

1.5 Enable policy rule for provided policy

Overall architecture how connector for Cisco Firepower will work (Picture 1)

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 hundreds of Cisco FTD servers and offers robust RSA algorithm support. It 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.

About Sectigo

Sectigo is the industry's most innovative provider of comprehensive certificate lifecycle management (CLM), with automated solutions and digital certificates that secure every human and machine identity for the world's largest brands. Its automated, cloud-native, universal CLM platform issues and manages digital certificates provided by all trusted certificate authorities (CAs) to simplify and improve security protocols across the enterprise. Sectigo is one of the longest-standing and largest CAs with more than 700,000 customers and two decades of delivering unparalleled digital trust. For more information, visit www.sectigo.com, follow us on LinkedIn, and subscribe to our Webby award-winning podcast, Root Causes.

Sectigo SSL/TLS certificates and CLM solutions help you enforce cryptographic strength, maintain compliance, and future-proof your network security, all while minimizing costs. Integrating Sectigo with Cisco FTD automates certificate issuance and lifecycle management, eliminating manual processes and downtime. 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.