SECTIGO

Sectigo Automation

Public-Key Encryption (PKI) is the gold standard in digital privacy, identity, and security, and should unquestionably be the security foundation for every device, server, user, and application in the enterprise. But using manual processes to install, monitor, and renew all the PKI certificates now required is labor intensive, technically demanding, and risky. Plus, the costs can add up quickly. A minimal manual SSL certificate installation (single webserver and domain instance) involves multiple steps and can easily add up to $50 to $100 per web server.

On top of that, the industry is moving toward shorter certificate lifetimes—first from three years to two, and then from two years to one. That means installation costs are continuing to rise. And the timing couldn't be worse. As more and more companies expand their use of mobile devices, the Internet of Things (IoT), DevOps, and other digital environments, the need for PKI is escalating, as is the urgency around being able to issue, revoke, and replace certificates quickly, reliably, and at enterprise scale.

Automating SSL Certificate Installation

Clearly, automation is now critical to any certificate management system. Not only does it reduce the overall cost of ownership; but automation also enforces cryptographic compliance and prevents potential service disruptions caused by human error.

However, given the disparate systems, applications, and devices that use and integrate with digital certificates, a one-size-fits-all approach is unlikely to address the automation needs of various use cases. That's why Sectigo offers several different automation options.

For SSL Certificate Installation, Sectigo provides:

- **Support for Automated Certificate Management Environment (ACME) protocol:** Sectigo Certificate Manager supports ACME, allowing you to automate certificate issuance and installation for a wide range of web servers, load balancers, routers, firewalls, and other networking gear. Sectigo supports DV, OV, and EV certificate types via ACME and provides full control to IT administrators. Many DevOps tools support ACME to enroll and manage certificates, and a myriad of open source tools are available for this purpose. These tools are popular among IT administrators and are being feature-enhanced on a frequent basis.

  If Sectigo implements the server or Certificate Authority side of the ACME protocol standard, it will work with ACME-compliant clients, and we will support any customer project which requires that integration. Of course, that requires the client to be ACME-compliant. See the table below for a list of currently supported platforms.

- **A Proprietary Automation Tool:** Using Sectigo's Network Agent, you can automate management of certificates for a variety of systems, including Apache Tomcat, Windows IIS web servers, and F5 Big-IP load balancers. The customer premise Network Agent is integrated with Sectigo Certificate Manager which runs in the cloud for downloading the agent and scheduling issuance, installation, and renewal of certificates.

- **REST API:** In some instances, companies prefer to integrate applications more tightly with Sectigo, which is possible using Sectigo's REST API. While this requires additional development on the application side, it allows you to leverage certificate management and customize your work flow.

- **Integration with Third Party Vendors:** Sectigo is continuously looking for opportunities to integrate with third party vendors to help customers achieve full automation. For instance, F5's Big-IP load balancer provides integration from its management system to automate certificate management from Sectigo.

Currently Supported Solutions

Web Server/Network Gear/DevOps Tools		Customer Choice			
Type	Platform	Sectigo Network Agent	ACME	Sectigo REST API	Custom Integration
Web Server	Apache HTTP Server	Yes	Yes	Available	
	Apache Tomcat	Yes	Yes	Available	
	IIS	Yes	Coming Up	Available	
	NGINX		Yes	Available	
Load Balancer	F5	Yes	Yes	Available	Yes
	Citrix ADC (formerly NetScaler)		Yes	Available	Yes
IT Service Management	ServiceNow			Available	Yes
DevOps Tools	Ansible			Available	
	AWS ELB		Yes	Available	
	Chef			Available	
	Docker			Available	
	HashiCorp Vault			Available	
	Jenkins			Available	
	Kubernetes		Yes	Available	
	Puppet			Available	
	SaltStack			Available	
	Terraform			Available	

We are continuously supporting new platforms. Contact us for the latest information.

Automating Non-SSL Certificate Installation

Many sytems, applications, and devices utilize non-SSL certificates. For non-SSL Certificate Installation, Sectigo provides:

- **Enrollment over Secure Transport (EST) protocol:** Sectigo supports the EST protocol which is used for managing networking gear from many vendors. In fact, a number of vendors have EST support already built in. EST is also popular in Internet of Things (IoT) environments given the efficiency of the protocol and support of Elliptic Curve Cryptography (ECC) keys. There are several open source EST clients available as well. Sectigo Certificate Manager displays and manages the certificates issued.

- **Simple Certificate Enrollment Protocol (SCEP):** In the Sectigo environment, SCEP can be used to enroll certificates in Linux, MacOS, and other operation systems. Mobile devices, Microsoft's NDES server, and MDMs typically use SCEP.

- **Sectigo Proxy Server:** A Sectigo Proxy Server can sit between the Microsoft Desktop and the Active Directory Certificate Service. It intercepts certificate requests for a certificate over the Windows Client Certificate Enrollment Protocol (WCCE) and automatically provides the certificate to the desktop without any employee intervention.

- **Sectigo Mobile Certificate Manager (MCM):** Sectigo MCM issues and manages certificates and keys across iOS and Android mobile devices without user intervention. It supports all certificate types and is interoperable with all leading devices, operating systems, and enrollment protocols.

As you can see, Sectigo offers a variety of certificate installation options, as well as the convenience and security of a seamless solution with one pane of glass for both public and private certificate issuance and management. Moreover, with Sectigo, you will never run into a certificate volume cap, as you might with open source alternatives. Sectigo enables your security team to easily enforce cryptographic security policy; protect communications; prevent data loss via unauthorized access; and future-proof systems, applications, and devices across the enterprise.

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.**