

Sectigo certificate integration for Apache using ACME

Sectigo partnered with Apache to embed the ACME (Automated Certificate Management Environment) protocol for all Apache web servers. With it, ACME can automatically deploy certificates to Apache servers and load balancers both inside and outside business firewalls.

Eliminate labor costs and security risks of manual certificate management

Apache is a free and open-source webserver platform that is used to run almost a third of internet websites globally. This powerful integration between Sectigo and Apache is driven by the need to automate the deployment and renewal of digital certificates at scale.

The mismanagement of digital certificates has become a leading cause of downtime and data breaches. Due to the sharp increase in devices and users accessing business networks remotely, managing digital certificates manually is now a significant security risk.

Digital certificates built on public key infrastructure (PKI) have also come under intense scrutiny as the CA/Browser Forum drives certificate lifespans sharply downward. With the looming 47-day lifespan mandate requiring up to 12 renewals per year, manual processes can no longer keep pace. These requirements apply to websites, public-facing applications, and services.

Certificate management platforms were previously unable to automate the installation of certificates to Apache web servers using ACME because External Account Binding (EAB) was not available between the Certificate Authority and the web server/load balancer without installing additional software. The platform could be notified of a certificate having been installed, enabling it to be monitored, but it was not possible to natively automate the installation process.

Some Certificate Lifecycle Management (CLM) platform vendors offer solutions based on custom agents, but these require embedded credentials, introducing security risks and administration headaches.

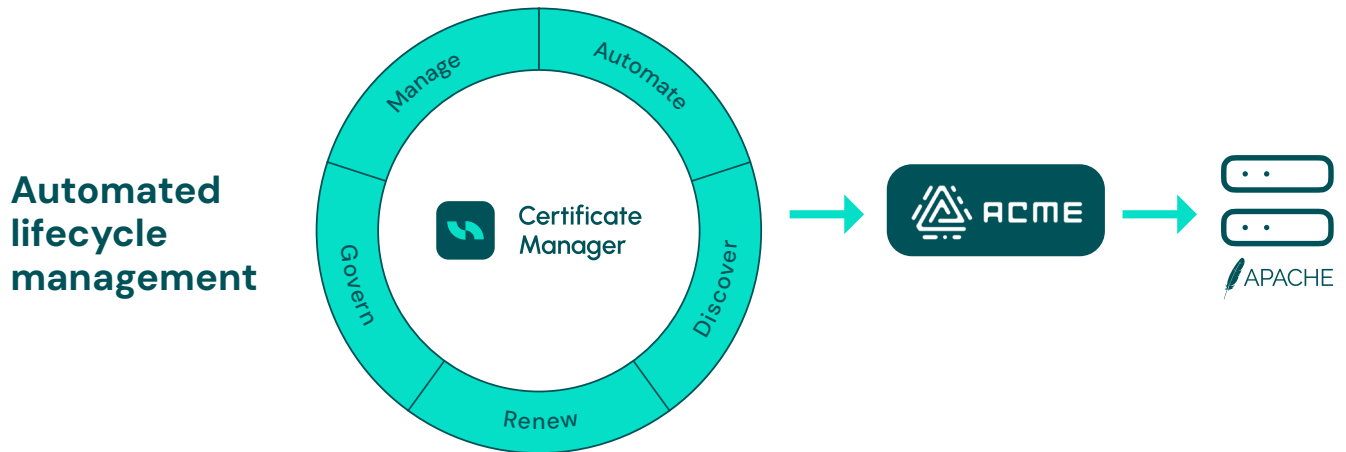


What Is ACME?

ACME is an industry-standard protocol used for the deployment and management of digital certificates to servers and web infrastructure. The use of ACME enables automation of certificate deployment, greatly reducing dependencies on manual processes and eliminating human error.

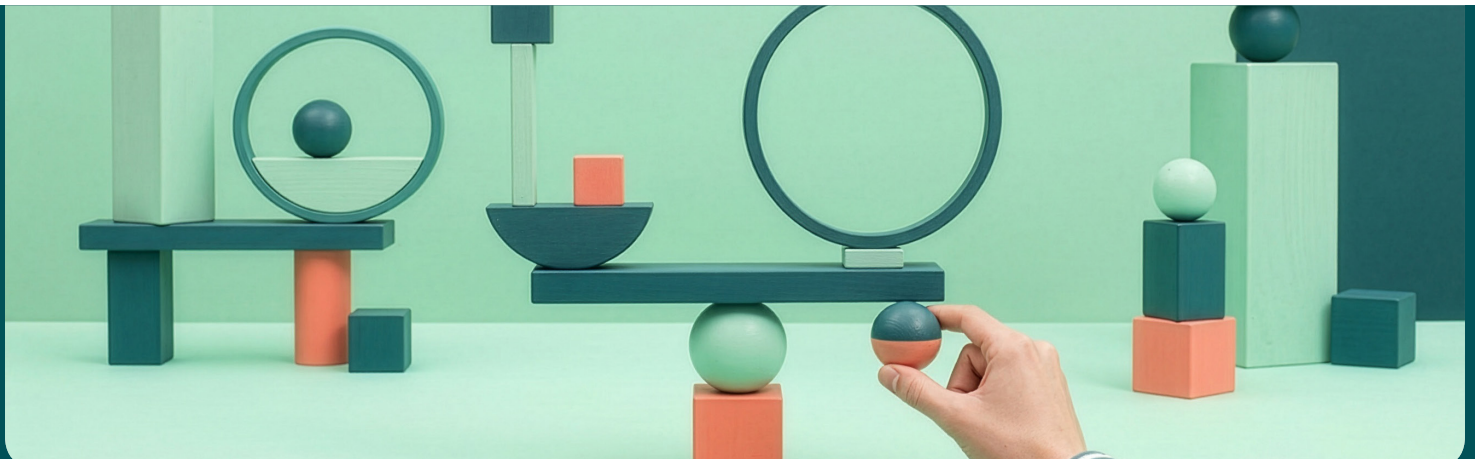
Sectigo provides full certificate lifecycle management for Apache Web Servers and load balancers

Sectigo partnered with Apache to implement the ACME protocol directly within the Apache platform, so there is no longer a requirement to install a custom software agent on the customer premises. This also removes the need to configure and manage passwords for server access, resulting in reduced risk and significantly reduced costs. ACME is an open standard, so the enterprise is not locked into a proprietary agent implementation.



ACME provides considerable benefits in the automation of certificate deployment. By partnering with Apache to implement ACME, Sectigo leads the industry in implementation and is the preferred CLM vendor for websites built on Apache

For more information on Sectigo's Apache support, 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](#).

