

Sectigo certificate integration for F5 using ACME

Enterprises rely on F5 appliances to scale applications and keep them highly available, and every one, standalone or in an HA pair, needs an SSL/TLS certificate to stay authenticated and encrypted. As the fleet grows, managing those certificates one at a time becomes the weak point. Issuance and lifecycle management should be automated and orchestrated to keep pace.

To secure F5 appliances against attacks and unexpected outages, IT teams need a certificate lifecycle management solution that can:

- ✔ Issue, revoke, replace, and renew SSL/TLS certificates quickly, reliably, and at scale
- ✔ Protect access and communication on F5 appliances with both authentication and strong encryption
- ✔ Cut cost of time-consuming manual certificate deployment for busy IT administrators
- ✔ Eliminate the error prone, manual process of issuing certificates one at a time
- ✔ Future proof against server OS compatibility and version issues



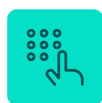
Sectigo can help

Sectigo offers a comprehensive certificate integration for F5 appliances so that enterprises can issue certificates at volume with a single click and automate the end-to-end certificate lifecycle at scale.

Automated certificate management for F5

Enterprises need reliable, scalable certificate lifecycle management to ensure critical application delivery appliances are protected without time-consuming administrative tasks or the risk of unexpected certificate expirations or outages. Sectigo's integration for F5 replaces the complexity of manual certificate management with centralized control and automation, delivering simplicity at scale across your F5 appliances.

Leveraging Sectigo certificate integration for F5 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 F5 appliances using the ACME automation standard (See diagram)



Automated certificate renewal

Near certificate expiration, Sectigo automatically renews and installs new certificates in the F5 appliances, helping ensure you avoid downtime for mission-critical systems and applications.



Full certificate lifecycle management

In addition to certificate renewal, Sectigo provides certificate revocation and replacement capabilities. This is necessary, for example, when a server is replaced.



Enhanced visibility and reporting

With the F5 ACME integration and Sectigo Certificate Manager, IT teams view the status of certificates on all devices across the organization through a single pane of glass, enabling you to see expiration dates and minimize or eliminate service disruptions.



Easy to use plugins

Sectigo certificate integration for F5 includes two certbot plugins, based on the open-source Automated Certificate Management Environment protocol (ACME).

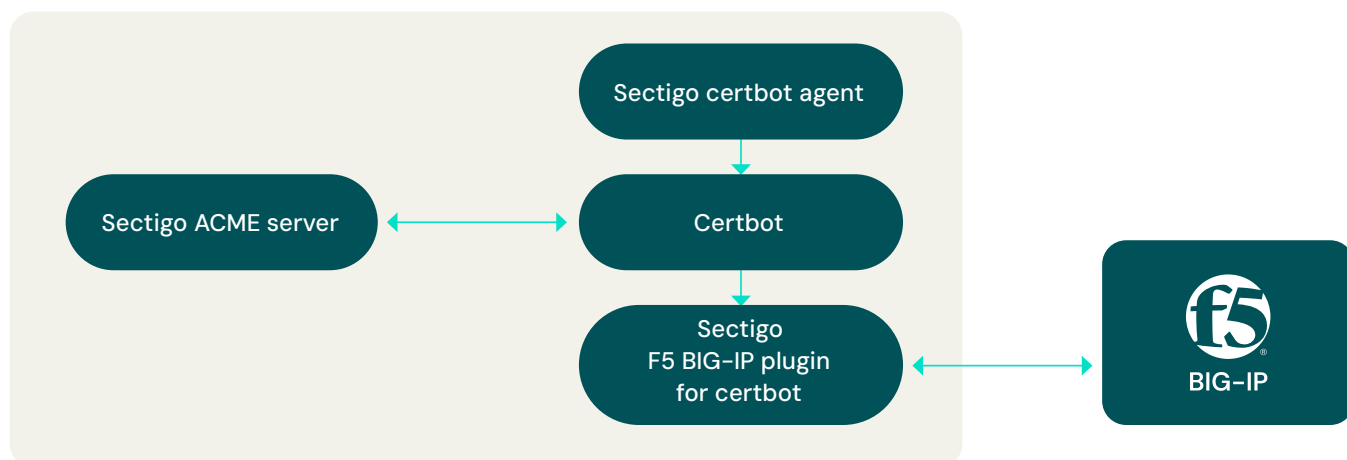


Seamless appliance support

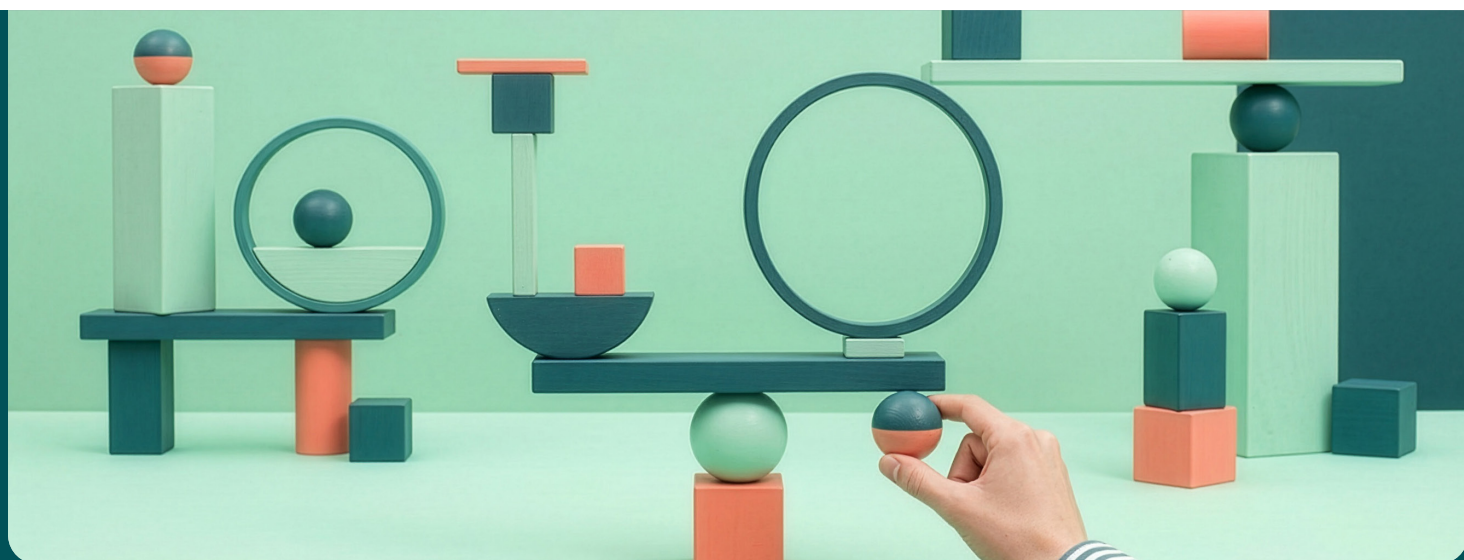
Sectigo streamlines integration with F5 server and seamlessly maintains all server OS compatibility as supported by certbot.



With Sectigo SSL/TLS certificates, you can enforce cryptographic strength, maintain compliance, and future-proof the protection of your application delivery appliances, all while minimizing costs. And with Sectigo certificate integration for F5, you can automate certificate issuance and lifecycle management for all your application delivery appliances. That eliminates time-consuming, error-prone manual processes and helps you avoid downtime to mission-critical applications.



The Sectigo advantage: The Sectigo integration for F5 provides auto-renewal for expiring certs, scalability across your F5 fleet, RSA and ECDSA support and automated issuance based on configuration. Sectigo's unique capabilities include client SSL profile management, private key protection and auto-renewal of revoked certificates.



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](#).

