

Sectigo Orchestration Gateway for Sectigo Certificate Manage (SCM)

Orchestrating SCM automation at scale

As enterprises operate across hybrid and multi-cloud environments, certificate management has evolved into a core infrastructure discipline. Shorter certificate lifecycles, growing numbers of digital identities, and increasingly distributed systems have changed how certificates must be issued, deployed, and maintained, placing new demands on automation and operational consistency.

Operational pressure points:

- **Fragmented operations:** Certificate tasks are often spread across legacy connectors, custom scripts, and manual steps, making them difficult to standardize.
- **Manual processes persist:** Despite rising scale and complexity, 95% of organizations still rely on manual certificate operations.
- **Growing certificate volumes:** Zero trust initiatives, expanding machine-to-machine authentication, and shorter lifecycles are increasing certificate issuance across servers, applications, and platforms.
- **Evolving requirements:** Regulatory expectations, crypto-agility planning, and continuous verification are raising the bar for consistency and control.

[\[State of Crypto Agility Report 2025\]](#)

When certificate operations remain fragmented, the cost is paid in reliability and control. Missed renewals and inconsistent workflows increase the risk of outages. When automation depends on separate VMs, scripts, and connectors for each platform, scaling becomes a risk multiplier. As certificate volumes grow and renewal cycles accelerate, legacy automation approaches don't just struggle to keep up, they become a liability, preventing IT and security teams from delivering the resilience and trust the business depends on.

What IT teams should expect from modern certificate automation

- ✔ **One optimized automation layer**
A consolidated approach that replaces per-integration VMs, connectors, and scripts with a single automation layer covering the environments that matter most.
- ✔ **Built for shorter lifecycles**
Automation that keeps pace with growing certificate volumes and accelerated renewal cycles without added operational load.
- ✔ **Secure key handling by default**
Just-in-time retrieval of privileged credentials ensures access is granted only when necessary, reducing key exposure.
- ✔ **Ready for what's next**
Flexibility to adapt to new platforms, evolving crypto standards, and regulatory change without re architecting automation.
- ✔ **Consistency at scale**
Standardized workflows that behave predictably across hybrid and multi cloud infrastructure as volume and renewal frequency increase.
- ✔ **Clear operational visibility**
Practical, real-time insight into where certificates live, when they expire, and how lifecycle events unfold.
- ✔ **Low friction to deploy and maintain**
Lightweight setup, minimal maintenance, and an architecture that simplifies operations rather than adding complexity.

What is Sectigo Orchestration Gateway (SOG)?

SOG is a lightweight, modular orchestration layer purpose built to work seamlessly with [Sectigo Certificate Manager \(SCM\)](#). It executes certificate lifecycle and deployment tasks across complex, distributed, multi vendor environments, removing the burden of brittle scripts, manual touchpoints, and legacy connectors.

Working alongside SCM, SOG provides a secure, scalable, and policy-driven automation foundation designed for the realities of modern hybrid and multi-cloud infrastructure. Built as an extensible gateway, its modular architecture automates TLS certificate operations today and extends naturally into new certificate use cases as needs evolve.

Continuously growing ecosystem compatibility

Supported TLS endpoints:



Supported credential stores:



For the latest supported integrations, see our [technical documentation page](#).



When deployed with Sectigo Certificate Manager, SOG helps IT teams achieve:



Simplified, predictable certificate operations

Organizations gain a single, consistent automation layer that standardizes certificate workflows across cloud environments.

- **Unified certificate lifecycle orchestration**

Automate discovery, issuance, renewal, deployment, and revocation without juggling scripts or specialized connectors.

- **Standardized, policy-driven workflows**

Apply consistent certificate and key handling policies across hybrid and multi cloud environments, reducing drift, manual exceptions, and configuration gaps.

- **Fast and lightweight deployment**

A modular footprint allows rapid rollout with minimal prerequisites, minimizing both setup effort and ongoing maintenance.



End-to-end automation at scale

Keep pace with accelerating certificate lifecycles and exploding certificate volumes, eliminating the firefighting that often accompanies manual tracking or last-minute renewals.

- **Effortless high-frequency renewals**

Shorter cycles and high-volume renewals are fully automated, reducing operational load while ensuring continuity across distributed systems.

- **Parallel certificate operations**

Certificates can be issued, rotated, and deployed across multiple platforms at once, eliminating bottlenecks from sequential updates.

- **Full certificate lifecycle coverage**

From cloud and local discovery to endpoint deployment, all certificate operations are centrally orchestrated through SCM, automatically.

- **Complete visibility across environment**

Cloud and local discovery scan internal networks and external-facing systems together, maintaining a current inventory and removing blind spots.





Secure key handling by default

Key security is strengthened at every step, reducing exposure and ensuring hygiene at scale.

- **Eliminates key sprawl**

Private keys are generated fresh on each endpoint just-in-time, eliminating sprawl and ensuring controlled, predictable key management.

- **Per-certificate key generation**

Every certificate receives its own private key generated at the endpoint, eliminating reuse and shrinking the attack surface.

- **No shared key storage**

Avoid centralized repositories and shared vault structures that create risk as certificate volumes grow.



Automation built to evolve with your environment

A modular and forward-looking architecture ensures automation remains future-ready.

- **Extensible, modular architecture**

Support for new servers, platforms, vaults, and PAM systems can be added without redesigning existing workflows.

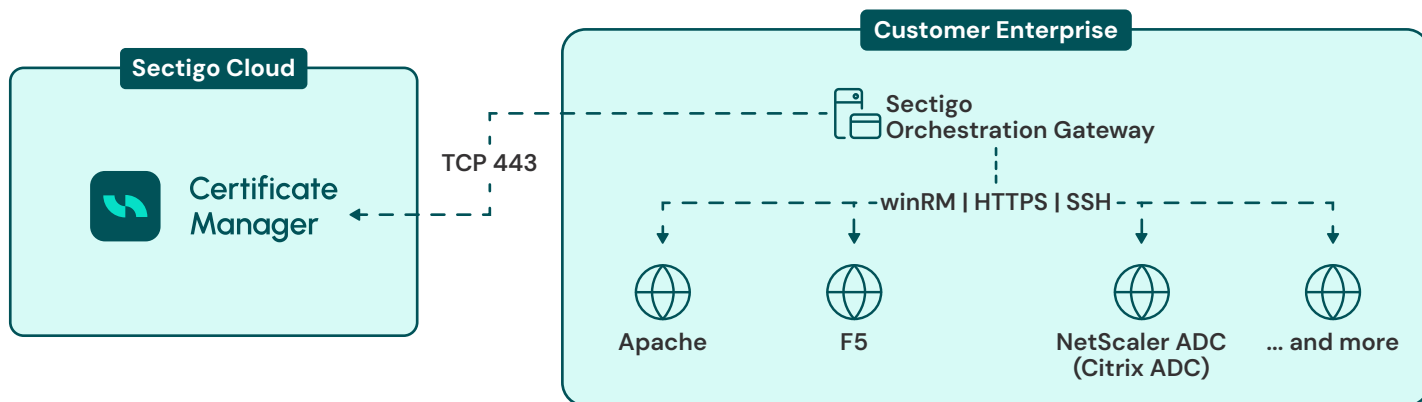
- **One-to-many automation**

A single gateway instance connects to multiple endpoints across the network, replacing integration-specific VMs, HA setups, and patching cycles with one install.

- **Crypto-agility readiness**

Prepares organizations for new cryptographic standards and algorithm transitions, including post-quantum requirements, without requiring operational re-architecture.

How it works



Visit the [technical documentation page](#) for the full list of supported Orchestration Gateway integrations.

The Sectigo Advantage

Sectigo combines deep PKI expertise with purpose built orchestration to help enterprises modernize certificate operations without introducing additional complexity. SCM provides centralized visibility, governance, and policy control. SOG extends that control into real environments through secure, purpose built orchestration, including policy driven execution, just in time credential access, and consistent lifecycle handling across platforms. Together, they replace fragmented scripts and point tools with predictable, end to end CLM execution across hybrid and multi cloud infrastructure.

This integrated approach reduces operational overhead, minimizes configuration drift, and removes renewal driven risk, while providing a modular foundation that evolves alongside changing environments and cryptographic requirements. With Sectigo, IT teams gain an automated trust infrastructure built for today's scale and designed to adapt for what's next.

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 on Sectigo Orchestration Gateway or certificate management solutions, please contact Sectigo Sales at sales@sectigo.com.

