

Sectigo Orchestration Gateway for Sectigo Certificate Manage (SCM)

When complexity, scale & security collide

Enterprises today are running hybrid and multi-cloud environments where shortened certificate lifecycles, rising integration complexity, and fragmented automation tooling have become core operational risks. Often teams rely on multiple connectors, brittle scripts, and inconsistent documentation, creating misconfigurations, blind spots, and barriers to scaling automation.

At the same time, certificate volumes are exploding as organizations mature zero trust architectures and expand machine to machine authentication. According to the Sectigo [State of Crypto Agility Report 2025](#), 95% of organizations still depend on manual processes, underscoring the growing friction as digital identity surfaces expand across clouds, devices, and workloads.

Evolving regulatory pressure, crypto agility requirements, and the push toward continuous verification amplify this urgency. As renewal cycles accelerate and environments diversify, enterprises need a unified orchestration layer that ensures trust, compliance, and scalability across vendors and deployment models.

Introducing the Sectigo Orchestration Gateway (SOG) for SCM

SOG is a lightweight orchestration layer purpose-built to work with [Sectigo Certificate Manager \(SCM\)](#), executing certificate lifecycle and deployment tasks across complex, multi-vendor environments.

Managed by SCM, SOG serves as a secure gateway between SCM and distributed enterprise systems, replacing brittle scripts and legacy connectors with a scalable, policy-driven automation capability. It currently automates TLS certificate operations across a broad and growing infrastructure footprint, with modular architecture built to support additional certificate use cases over time.

Why enterprises choose SCM with SOG

- ✔ Automate the full certificate lifecycle across servers, CDNs, WAFs, and access systems.
- ✔ Discover every certificate through combined cloud and local scanning.
- ✔ Scale policy-driven operations for shorter lifecycles and crypto-agility.
- ✔ Consolidate connectors, scripts, and VMs into a single gateway install.
- ✔ Enforce key hygiene and just-in-time credential retrieval via PAM and vault integrations.
- ✔ Accelerate deployment across modern, multi-vendor platforms.

As an integrated orchestration component within Sectigo Certificate Manager (SCM), the Sectigo Orchestration Gateway centralizes and streamlines automation by replacing scripts and point integrations with a single, lightweight capability. Managed through SCM policies, SOG automates TLS certificate lifecycle operations across supported servers, load balancers, CDNs, WAFs, and privileged access systems while also enabling secure, just-in-time retrieval of privileged credentials. By extending SCM's automation across servers, infrastructure, and credential stores, SOG allows teams to scale trust operations without adding operational complexity.

Streamlined and secured certificate operations

SOG centralizes automation that spans multiple servers, load balancers, and cloud platforms, replacing fragmented scripts and manual workflows. It dynamically retrieves privileged credentials from remote credential stores just-in-time, rather than storing sensitive credentials locally.

Supported Servers:



...and more

Supported credential stores:



...and more

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

Light footprint. Fast, predictable deployment

Lightweight and modular, the gateway deploys quickly on Linux, Windows, and Docker environments. Its adaptable framework integrates new platforms and services without requiring redesign, while REST API support enables seamless workflow integration and rapid rollout across distributed estates.

End-to-end automation at scale

TLS certificate discovery, issuance, renewal, deployment, and revocation are fully automated across supported servers, cloud services, and enterprise platforms with SOG. Parallel updates ensure operations keep pace with shortened certificate lifecycles and high-volume environments.



Stronger security at every step

Each certificate is paired with a unique key, eliminating shared or centrally stored keys that increase risk. Keys are managed locally or through PAM and key vault integrations, and automated rotation across servers enforces consistent cryptographic hygiene. Continuous discovery identifies unmanaged certificates across cloud environments, reducing attack surface and ensuring compliance.

Complete visibility across every environment

Cloud and local discovery work together to identify certificates across internal and external systems. 24/7 on-demand tracking removes blind spots and maintains a reliable inventory across servers, platforms, and cloud-facing services, supporting policy enforcement and proactive risk management.

Future-ready and adaptable

SOG is built for crypto agility, supporting algorithm transitions, post-quantum readiness, and emerging standards across all supported servers, platforms, and protocols. Whether modernizing legacy web servers or scaling containerized workloads, orchestration policies apply consistently without requiring integration redesign.

Operational efficiency with measurable return

With SOG, built-in integrations and automation streamline deployment and day-to-day operations. Consolidating integration-specific VMs into a single gateway reduces infrastructure footprint, maintenance effort, and points of failure, accelerating ROI. Teams eliminate repetitive work, reduce escalations, and scale certificate operations without increasing overhead.

Common SOG use cases within SCM



Automate TLS across hybrid environments

Discover, issue, install, renew, and revoke SSL/TLS certificates across servers, load balancers, and cloud platforms without manual efforts.



Simplified workflow for one-to-many

Execute policy-driven TLS certificate actions across multiple servers through a single centralized gateway, eliminating redundant tasks.



Support accelerated certificate lifecycles

Manage shortened certificate lifecycles and crypto upgrades with policy-driven automation, keeping operations aligned with modern security requirements.



Boost operational efficiency

Streamline high-volume deployments, reduce repetitive tasks, and replace fragmented scripts with centralized automation.



Gain full certificate visibility via SCM

Support SCM to scan internal and external certificates and maintain a complete inventory across servers, devices, and cloud-facing endpoints.



Discover certificates across systems

Combine cloud and local discovery to remove blind spots and support continuous compliance.



Reduce the privileged credential attack surface

Retrieve credentials just in time through PAM integrations, avoiding local storage and limiting exposure.



Compliance and audit readiness

Centralize policies, automate certificate management, and maintain consistent audit controls.



Minimize infrastructure sprawl

Replace integration-specific VMs and HA setups with a single gateway, reducing overhead and points of failure.



Multi-server and platform support

Deploy across IIS, Apache, Tomcat, F5, NGINX, Netscaler, Cloudflare, and Imperva using local or remote gateways.

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.

Sectigo's comprehensive certificate management solution empowers organizations to seamlessly automate, secure, and optimize their digital infrastructure. By simplifying complex certificate operations, strengthening security protocols, and supporting compliance requirements, organizations can confidently protect their hybrid environments and streamline IT workflows.

Reach out today for a personalized demo or contact us at sales@sectigo.com to see how Sectigo can transform your certificate management strategy.

