

Sectigo Orchestration Gateway para Sectigo Certificate Manage (SCM)

Cuando la complejidad, la escala y la seguridad colisionan

Las empresas operan hoy en entornos híbridos y multicloud donde la reducción de la validez de los certificados, la creciente complejidad de las integraciones y la automatización fragmentada se han convertido en riesgos operativos fundamentales. Con frecuencia, los equipos dependen de múltiples conectores, scripts frágiles y documentación inconsistente, lo que genera errores de configuración, puntos ciegos y obstáculos para escalar la automatización.

Al mismo tiempo, el volumen de certificados se está disparando a medida que las organizaciones consolidan arquitecturas Zero Trust y amplían la autenticación máquina a máquina. Según el informe Sectigo [State of Crypto Agility Report 2025](#), el 95 % de las organizaciones aún depende de procesos manuales, lo que remarca la creciente fricción a medida que las identidades digitales se extienden por nubes, dispositivos y cargas de trabajo.

El aumento de la presión regulatoria, los requisitos de agilidad criptográfica y la exigencia de verificación continua amplifican esta urgencia. A medida que los ciclos de renovación se aceleran y los entornos se diversifican, las empresas necesitan una capa de orquestación unificada que garantice la confianza, el cumplimiento y la escalabilidad entre proveedores y modelos de despliegue.

Presentación de Sectigo Orchestration Gateway (SOG) para SCM

SOG es una capa de orquestación ligera diseñada específicamente para funcionar con [Sectigo Certificate Manager \(SCM\)](#), ejecutando tareas de despliegue y ciclo de vida de certificados en entornos complejos y de múltiples proveedores.

Gestionado por SCM, SOG actúa como una pasarela segura entre SCM y los sistemas distribuidos de la empresa, reemplazando scripts frágiles y conectores heredados por una capacidad de automatización escalable y basada en directivas. Actualmente automatiza operaciones de certificados TLS en una infraestructura amplia y en expansión, con una arquitectura modular creada para admitir casos de uso adicionales con el tiempo.

Por qué las empresas eligen SCM con SOG:

- ✓ Automatizan todo el ciclo de vida de los certificados en servidores, CDN, WAF y sistemas de acceso.
- ✓ Descubren todos los certificados mediante escaneos combinados locales y en la nube.
- ✓ Escalan operaciones basadas en directivas para ciclos de vida más cortos y agilidad criptográfica.
- ✓ Consolidan conectores, scripts y máquinas virtuales en la instalación de una sola pasarela.
- ✓ Aplican la máxima higiene en claves y la obtención de credenciales justo a tiempo mediante integraciones con PAM y baúles de claves.
- ✓ Aceleran el despliegue en plataformas modernas de múltiples proveedores.

Como componente de orquestación integrado dentro de Sectigo Certificate Manager (SCM), Sectigo Orchestration Gateway centraliza y agiliza la automatización al sustituir scripts e integraciones puntuales por una capacidad única y ligera. Gestionado a través de las directivas de SCM, SOG automatiza las operaciones del ciclo de vida de certificados TLS en servidores, balanceadores de carga, CDN, WAF y sistemas de acceso privilegiado compatibles, al tiempo que permite la obtención segura y justo a tiempo de credenciales privilegiadas. Al extender la automatización de SCM a servidores, infraestructura y depósitos de credenciales, SOG permite a los equipos escalar las operaciones de confianza sin añadir complejidad operativa.

Operaciones de certificados optimizadas y seguras

SOG centraliza la automatización abarcando múltiples servidores, balanceadores de carga y plataformas cloud, reemplazando scripts fragmentados y flujos manuales. Obtiene dinámicamente credenciales privilegiadas desde depósitos remotos justo a tiempo, evitando almacenar datos sensibles de forma local.

Servidores compatibles:



... y más

Baúles de credenciales compatibles:



... y más

Para consultar las integraciones compatibles más recientes, visite nuestra [página de documentación técnica](#).

Huella ligera. Despliegue rápido y predecible

Ligero y modular, el gateway se despliega rápidamente en entornos Linux, Windows y Docker. Su arquitectura adaptable integra nuevas plataformas y servicios sin requerir rediseños, mientras que el soporte de API REST permite una integración de flujos de trabajo fluida y un despliegue rápido en entornos distribuidos.

Automatización de extremo a extremo a escala

El descubrimiento, la emisión, la renovación, el despliegue y la revocación de certificados TLS están completamente automatizados en los servidores, servicios cloud y plataformas empresariales compatibles con SOG. Las actualizaciones en paralelo garantizan que las operaciones sigan el ritmo del acortamiento de los certificados y de entornos con gran volumen.



Mayor seguridad en cada paso

Cada certificado se empareja con una clave única, eliminando claves compartidas o almacenadas centralmente que aumentan el riesgo. Las claves se gestionan localmente o mediante integraciones con PAM y baúles de claves, y la rotación automatizada en los servidores impone una higiene criptográfica constante. El descubrimiento continuo identifica certificados no gestionados en la nube, reduciendo la superficie de ataque y garantizando el cumplimiento.

Visibilidad completa en todos los entornos

El descubrimiento local y en la nube funcionan conjuntamente para identificar certificados en sistemas internos y externos. El seguimiento bajo demanda las 24 horas, los 7 días de la semana, elimina puntos ciegos y mantiene un inventario fiable en servidores, plataformas y servicios orientados a la nube, respaldando el cumplimiento de directivas y la gestión proactiva de riesgos.

Preparado para el futuro y adaptable

SOG está diseñado para la agilidad criptográfica, soportando transiciones de algoritmos, preparación poscuántica y estándares emergentes en todos los servidores, plataformas y protocolos compatibles. Ya sea modernizando servidores web heredados o escalando cargas de trabajo contenedorizadas, las directivas de orquestación se aplican de forma consistente sin requerir cambios de diseño.

Eficiencia operativa con retorno medible

Con SOG, las integraciones nativas y la automatización agilizan el despliegue y las operaciones diarias. La consolidación de máquinas virtuales de integración en un solo gateway reduce la huella de infraestructura, el esfuerzo de mantenimiento y los puntos de fallo, acelerando el ROI. Los equipos eliminan trabajo repetitivo, reducen escalados y escalan las operaciones de certificados sin aumentar la carga operativa.

Casos de uso comunes de SOG en SCM



Automatizar TLS en entornos híbridos

Descubrir, emitir, instalar, renovar y revocar certificados SSL/TLS en servidores, balanceadores de carga y plataformas cloud sin esfuerzo manual.



Soportar ciclos de vida acelerados

Gestionar plazos de validez más cortos y actualizaciones criptográficas mediante automatización basada en directivas, alineando el funcionamiento con los requisitos de seguridad actuales.



Flujos simplificados de uno a muchos

Ejecutar acciones de certificados TLS basadas en directivas en múltiples servidores mediante un único gateway centralizado, eliminando tareas redundantes.



Aumentar la eficiencia operativa

Agilizar despliegues de gran volumen, reducir tareas repetitivas y sustituir scripts fragmentados por automatización centralizada.



Obtener visibilidad total mediante SCM

Permitir a SCM escanear certificados internos y externos y mantener un inventario completo en servidores, dispositivos y endpoints cloud.



Descubrir certificados en todos los sistemas

Combinar descubrimiento local y cloud para eliminar puntos ciegos y respaldar el cumplimiento continuo.



Reducir la superficie de ataque de credenciales privilegiadas

Obtener credenciales justo a tiempo mediante integraciones PAM, evitando el almacenamiento local y limitando la exposición.



Cumplimiento y preparación para auditorías

Centralizar directivas, automatizar la gestión de certificados y mantener controles de auditoría constantes.



Minimizar la dispersión de infraestructura

Reemplazar máquinas virtuales específicas y arquitecturas de alta disponibilidad por un solo gateway, reduciendo la carga operativa y los puntos de fallo.



Soporte multiplataforma y multiservidor

Desplegar en IIS, Apache, Tomcat, F5, NGINX, Netscaler, Cloudflare e Imperva utilizando gateways locales o remotos.

Sobre Sectigo

Sectigo es un proveedor líder en Gestión del Ciclo de Vida de Certificados (CLM), ayudando a las organizaciones a proteger las identidades humanas y de máquinas mientras reduce los riesgos ocultos de la confianza digital moderna. A medida que los volúmenes de certificados crecen y su validez se reduce, los certificados no gestionados se convierten en una causa frecuente de caídas de servicio, fallos de cumplimiento y interrupciones operativas. Sectigo utiliza la Automatización Orquestada para ofrecer Simplicidad a Escala a través de su plataforma CLM nativa en la nube, unificando visibilidad, control y gestión del ciclo de vida en entornos complejos. Con más de 700.000 clientes, incluyendo el 65 % de las empresas Fortune 500, Sectigo es una de las autoridades de certificación más grandes y consolidadas, con más de 20 años ofreciendo una confianza digital incomparable.

La solución integral de gestión de certificados de Sectigo permite a las organizaciones automatizar, asegurar y optimizar sin problemas su infraestructura digital. Al simplificar las operaciones complejas de certificados, reforzar los protocolos de seguridad y responder a las exigencias normativas, las empresas pueden proteger sus entornos híbridos con total confianza y agilizar los flujos de trabajo de TI.

Póngase en contacto hoy mismo para solicitar una demostración personalizada o escríbanos a sales@sectigo.com para descubrir cómo Sectigo puede transformar su estrategia de gestión de certificados.

