

Sectigo Orchestration Gateway para Sectigo Certificate Manager (SCM)

Orquestando la automatización de SCM a escala

A medida que las empresas operan en entornos híbridos y multicloud, la gestión de certificados se ha convertido en una disciplina de infraestructura fundamental. La reducción del periodo de validez de los certificados, el aumento del número de identidades digitales y la creciente distribución de los sistemas han cambiado la forma en que se deben emitir, desplegar y mantener los certificados, imponiendo nuevas exigencias a la automatización y a la consistencia operativa.

Puntos de presión operativa:

- **Operaciones fragmentadas:** Las tareas de certificados a menudo se dividen entre conectores heredados, scripts personalizados y pasos manuales, lo que dificulta su estandarización.
- **Volúmenes de certificados en crecimiento:** Las iniciativas Zero Trust, la expansión de la autenticación máquina a máquina y las validez más cortas están aumentando la emisión de certificados en servidores, aplicaciones y plataformas.
- **Persistencia de procesos manuales:** A pesar del aumento de la escala y la complejidad, el 95 % de las organizaciones aún depende de operaciones manuales de certificados.
- **Requisitos en evolución:** Las expectativas regulatorias, la planificación de la agilidad criptográfica y la verificación continua están elevando el nivel de exigencia en términos de control y consistencia.

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

Cuando las operaciones de certificados permanecen fragmentadas, el coste se paga en fiabilidad y control. Las renovaciones no realizadas y los flujos de trabajo inconsistentes aumentan el riesgo de caídas del servicio. Cuando la automatización depende de máquinas virtuales, scripts y conectores independientes para cada plataforma, la escala se convierte en un multiplicador de riesgos. A medida que los volúmenes de certificados crecen y los ciclos de renovación se aceleran, los enfoques de automatización heredados no solo luchan por mantenerse al día, sino que se convierten en un factor de vulnerabilidad que impide a los equipos de TI y seguridad ofrecer la resiliencia que el negocio necesita.

Lo que los equipos de TI deben esperar de una automatización moderna de certificados

- ✓ **Una capa de automatización optimizada**
Un enfoque consolidado que reemplaza las máquinas virtuales por integración, conectores y scripts por una única capa de automatización que cubre los entornos clave.
- ✓ **Consistencia a escala**
Flujos de trabajo estandarizados que se comportan de manera predecible en infraestructuras híbridas y multicloud a medida que aumentan el volumen y la frecuencia de renovación.
- ✓ **Diseñado para ciclos de vida más cortos**
Automatización que sigue el ritmo del aumento del volumen de certificados y los ciclos acelerados sin añadir carga operativa.
- ✓ **Visibilidad operativa clara**
Información práctica y en tiempo real sobre dónde se ubican los certificados, cuándo caducan y cómo se desarrollan los eventos del ciclo de vida.
- ✓ **Gestión segura de claves por defecto**
La obtención justo a tiempo de credenciales privilegiadas garantiza que el acceso se conceda solo cuando sea necesario, reduciendo la exposición de las claves.
- ✓ **Baja fricción en despliegue y mantenimiento**
Configuración ligera, mantenimiento mínimo y una arquitectura que simplifica las operaciones en lugar de añadir complejidad.
- ✓ **Preparado para el futuro**
Flexibilidad para adaptarse a nuevas plataformas, estándares criptográficos en evolución y cambios regulatorios sin tener que rediseñar la automatización.

¿Qué es Sectigo Orchestration Gateway (SOG)?

SOG es una capa de orquestación ligera y modular diseñada específicamente para funcionar sin problemas con [Sectigo Certificate Manager \(SCM\)](#). Sectigo Certificate Manager (SCM). Ejecuta tareas de despliegue y ciclo de vida de certificados en entornos complejos, distribuidos y de múltiples proveedores, eliminando la carga de los scripts frágiles, los puntos de contacto manuales y los conectores heredados.

Al trabajar junto a SCM, SOG proporciona una base de automatización segura, escalable y basada en directivas, diseñada para las realidades de las infraestructuras híbridas y multicloud modernas. Construido como una pasarela extensible, su arquitectura modular automatiza las operaciones de certificados TLS hoy en día y se amplía de manera natural hacia nuevos casos de uso a medida que evolucionan las necesidades.

Compatibilidad del ecosistema en continuo crecimiento

Endpoints TLS compatibles:



Baúles de credenciales compatibles:



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



Al desplegarse con Sectigo Certificate Manager, SOG ayuda a los equipos de TI a lograr:



Operaciones de certificados simplificadas y predecibles

Las organizaciones obtienen una capa de automatización única y consistente que estandariza los flujos de trabajo de certificados en entornos cloud.

- **Orquestación unificada del ciclo de vida de certificados**

Automatice el descubrimiento, la emisión, la renovación, el despliegue y la revocación sin tener que lidiar con scripts o conectores especializados.

- **Flujos de trabajo estandarizados y basados en directivas**

Aplice directivas consistentes de gestión de claves y certificados en entornos híbridos y multicloud, reduciendo desviaciones, excepciones manuales y brechas de configuración.

- **Despliegue rápido y ligero**

Una huella modular permite una implementación rápida con requisitos previos mínimos, reduciendo tanto el esfuerzo de configuración como el mantenimiento continuo.



Automatización de extremo a extremo a escala

Mantenga el ritmo de la aceleración de los ciclos de vida y la explosión del volumen de certificados, eliminando la gestión de crisis que suele acompañar al seguimiento manual o a las renovaciones de última hora.

- **Renovaciones de alta frecuencia sin esfuerzo**

Los ciclos más cortos y las renovaciones de gran volumen están totalmente automatizados, lo que reduce la carga operativa al tiempo que garantiza la continuidad en los sistemas distribuidos.

- **Operaciones paralelas de certificados**

Los certificados se pueden emitir, rotar y desplegar en múltiples plataformas a la vez, eliminando los cuellos de botella de las actualizaciones secuenciales.

- **Cobertura completa del ciclo de vida de certificados**

Desde el descubrimiento local y en la nube hasta el despliegue en endpoints, todas las operaciones de certificados se orquestan centralmente a través de SCM, de forma automática.

- **Visibilidad completa en todo el entorno**

El descubrimiento local y en la nube escanea redes internas y sistemas externos simultáneamente, manteniendo un inventario actualizado y eliminando puntos ciegos.



Gestión segura de claves por defecto

La seguridad de las claves se refuerza en cada paso, reduciendo la exposición y garantizando la máxima higiene a escala.

- **Elimina la dispersión de claves**

Las claves privadas se generan de forma única en cada endpoint justo a tiempo, eliminando la dispersión y garantizando una gestión de claves controlada y predecible.

- **Generación de claves por certificado**

Cada certificado recibe su propia clave privada generada en el endpoint, lo que elimina la reutilización y reduce la superficie de ataque.

- **Sin almacenamiento compartido de claves**

Evite repositorios centralizados y estructuras de baúles compartidos que crean riesgos a medida que crecen los volúmenes de certificados.



Automatización creada para evolucionar con su entorno

Una arquitectura modular y orientada al futuro garantiza que la automatización permanezca preparada para los próximos desafíos.

- **Arquitectura extensible y modular**

Se puede añadir soporte para nuevos servidores, plataformas, baúles y sistemas PAM sin rediseñar los flujos de trabajo existentes.

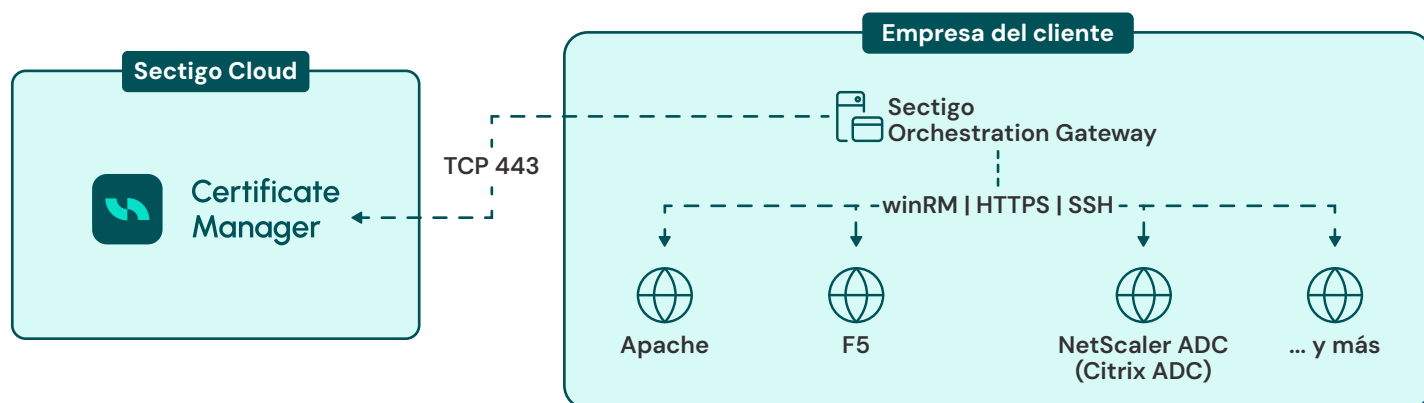
- **Automatización uno-a-muchos**

Una sola instancia de pasarela se conecta a múltiples endpoints en la red, reemplazando las máquinas virtuales específicas de integración, las configuraciones de alta disponibilidad y los ciclos de parches por una sola instalación.

- **Preparación para la agilidad criptográfica**

Prepara a las organizaciones para los nuevos estándares criptográficos y las transiciones de algoritmos, incluidos los requisitos poscuánticos, sin requerir reestructuraciones operativas.

Cómo funciona



Visite la [página de documentación técnica](#) para obtener la lista completa de integraciones compatibles con Orchestration Gateway.

La ventaja de Sectigo

Sectigo combina una profunda experiencia en PKI con una orquestación diseñada a medida para ayudar a las empresas a modernizar las operaciones de certificados sin introducir complejidad adicional. SCM proporciona visibilidad centralizada, gobernanza y control de directivas. SOG extiende ese control a los entornos reales mediante una orquestación segura y especializada, que incluye la ejecución basada en directivas, el acceso a credenciales justo a tiempo y la gestión consistente del ciclo de vida en todas las plataformas. Juntos, reemplazan scripts fragmentados y herramientas aisladas con una ejecución CLM de extremo a extremo predecible en infraestructuras híbridas y multicloud.

Este enfoque integrado reduce la carga operativa, minimiza la desviación de configuración y elimina los riesgos derivados de las renovaciones, al tiempo que proporciona una base modular que evoluciona junto con los entornos cambiantes y los requisitos criptográficos. Con Sectigo, los equipos de TI obtienen una infraestructura de confianza automatizada creada para la escala actual y diseñada para adaptarse a lo que venga a continuación.

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.

Para obtener más información sobre Sectigo Orchestration Gateway o las soluciones de gestión de certificados, póngase en contacto con el equipo de ventas de Sectigo en sales@sectigo.com.

