

Sectigo Orchestration Gateway per Sectigo Certificate Manager (SCM)

Orchestrare l'automazione SCM su larga scala

Poiché le aziende operano in ambienti ibridi e multi-cloud, la gestione dei certificati è diventata una disciplina fondamentale per l'infrastruttura. Durate dei certificati più brevi, un numero crescente di identità digitali e sistemi sempre più distribuiti hanno modificato il modo in cui i certificati devono essere emessi, distribuiti e gestiti, imponendo nuove esigenze in termini di automazione e coerenza operativa.

Punti di pressione operativa:

- **Operazioni frammentate:** Le attività sui certificati sono spesso suddivise tra connettori legacy, script personalizzati e passaggi manuali, rendendole difficili da standardizzare.
- **Persistenza dei processi manuali:** Nonostante l'aumento della scala e della complessità, il 95% delle organizzazioni si affida ancora a operazioni manuali sui certificati.
- **Volumi di certificati in crescita:** Le iniziative Zero Trust, l'espansione dell'autenticazione machine-to-machine e la riduzione della durata dei certificati stanno aumentando le emissioni su server, applicazioni e piattaforme.
- **Requisiti in evoluzione:** Le aspettative normative, la pianificazione dell'agilità crittografica e la verifica continua stanno alzando l'asticella del controllo e della coerenza.

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

Quando le operazioni sui certificati rimangono frammentate, il costo si paga in termini di affidabilità e controllo. I rinnovi mancati e i workflow incoerenti aumentano il rischio di disservizi. Quando l'automazione dipende da VM, script e connettori separati per ciascuna piattaforma, la scalabilità diventa un moltiplicatore di rischi. Con l'aumento dei volumi e l'accelerazione dei cicli di rinnovo, gli approcci tradizionali all'automazione non solo faticano a stare al passo, ma diventano una vulnerabilità che impedisce ai team IT e di sicurezza di garantire la resilienza di cui l'azienda ha bisogno.

Cosa devono aspettarsi i team IT dall'automazione moderna dei certificati

- ✓ **Un unico livello di automazione ottimizzato**
Un approccio consolidato che sostituisce le VM per integrazione, i connettori e gli script con un unico livello di automazione che copre gli ambienti principali.
- ✓ **Coerenza su larga scala**
Workflow standardizzati che si comportano in modo prevedibile su infrastrutture ibride e multi-cloud al crescere del volume e della frequenza di rinnovo.
- ✓ **Progettato per cicli di vita più brevi**
Automazione che mantiene il passo con i volumi crescenti e i cicli di rinnovo accelerati senza costi operativi aggiuntivi.
- ✓ **Chiara visibilità operativa**
Informazioni pratiche in tempo reale su dove risiedono i certificati, quando scadono e come si svolgono gli eventi del ciclo di vita.
- ✓ **Gestione sicura delle chiavi per impostazione predefinita**
Il recupero just-in-time delle credenziali privilegiate garantisce che l'accesso sia concesso solo quando necessario, riducendo l'esposizione delle chiavi.
- ✓ **Minima frizione nel deployment e nella manutenzione**
Installazione leggera, manutenzione ridotta al minimo e un'architettura che semplifica le operazioni anziché aggiungere complessità.
- ✓ **Pronto per il futuro**
Flessibilità per adattarsi a nuove piattaforme, standard crittografici in evoluzione e modifiche normative senza riprogettare l'automazione.

Che cos'è Sectigo Orchestration Gateway (SOG)?

SOG è un livello di orchestrazione leggero e modulare, progettato specificamente per integrarsi perfettamente con [Sectigo Certificate Manager \(SCM\)](#). Esegue le attività di deployment e gestione del ciclo di vita dei certificati in ambienti complessi, distribuiti e multi-vendor, eliminando il carico di script instabili, passaggi manuali e connettori legacy.

Lavorando al fianco di SCM, SOG fornisce una base di automazione sicura, scalabile e guidata dalle policy, progettata per le realtà delle moderne infrastrutture ibride e multi-cloud. Realizzato come gateway estensibile, la sua architettura modulare automatizza oggi le operazioni sui certificati TLS e si estende naturalmente a nuovi casi d'uso con l'evolversi delle esigenze.

Compatibilità dell'ecosistema in continua crescita

Endpoint TLS supportati:



Vault di credenziali supportati:



Per l'elenco aggiornato delle integrazioni supportate, consultare la [pagina della documentazione tecnica](#)



Quando distribuito con Sectigo Certificate Manager, SOG aiuta i team IT a ottenere:



Operazioni sui certificati semplificate e prevedibili

Le organizzazioni ottengono un livello di automazione unico e coerente che standardizza i workflow dei certificati negli ambienti cloud.

- **Orchestrazione unificata del ciclo di vita dei certificati**

Automatizza l'individuazione, l'emissione, il rinnovo, il deployment e la revoca senza dover gestire script o connettori specializzati.

- **Workflow standardizzati e guidati dalle policy**

Applica policy coerenti di gestione dei certificati e delle chiavi in ambienti ibridi e multi-cloud, riducendo le discrepanze, le eccezioni manuali e le lacune di configurazione.

- **Deployment rapido e leggero**

Un'impronta modulare consente una distribuzione rapida con prerequisiti minimi, riducendo sia l'impegno di installazione che la manutenzione continua.



Automazione end-to-end su larga scala

Mantieni il passo con l'accelerazione dei cicli di vita e l'esplosione dei volumi di certificati, eliminando la gestione delle emergenze che spesso accompagna il tracciamento manuale o i rinnovi dell'ultimo minuto.

- **Rinnovi ad alta frequenza senza sforzo**

I cicli più brevi e i rinnovi ad alto volume sono completamente automatizzati, riducendo il carico operativo e garantendo al contempo la continuità tra i sistemi distribuiti.

- **Operazioni parallele sui certificati**

I certificati possono essere emessi, ruotati e distribuiti su più piattaforme contemporaneamente, eliminando i colli di bottiglia degli aggiornamenti sequenziali.

- **Copertura completa del ciclo di vita dei certificati**

Dall'individuazione cloud e locale al deployment sugli endpoint, tutte le operazioni sui certificati sono orchestrate centralmente tramite SCM, in modo automatico.

- **Visibilità completa in ogni ambiente**

L'individuazione cloud e locale scansiona contemporaneamente le reti interne e i sistemi esterni, mantenendo un inventario aggiornato ed eliminando i punti ciechi.





Gestione sicura delle chiavi per impostazione predefinita

La sicurezza delle chiavi è rafforzata ad ogni livello, riducendo l'esposizione e garantendo un'igiene rigorosa su larga scala.

- **Elimina la dispersione delle chiavi**

Le chiavi private vengono generate ex novo su ciascun endpoint just-in-time, eliminando la dispersione e garantendo una gestione controllata e prevedibile.

- **Generazione di chiavi per singolo certificato**

Ogni certificato riceve la propria chiave privata generata sull'endpoint, eliminando il riutilizzo e riducendo la superficie di attacco.

- **Nessun archivio chiavi condiviso**

Evita repository centralizzati e strutture di vault condivise che creano rischi con l'aumento dei volumi di certificati.



Automazione progettata per evolversi con il tuo ambiente

Un'architettura modulare e orientata al futuro garantisce che l'automazione rimanga pronta per gli sviluppi futuri.

- **Architettura estensibile e modulare**

Il supporto per nuovi server, piattaforme, vault e sistemi PAM può essere aggiunto senza riprogettare i workflow esistenti.

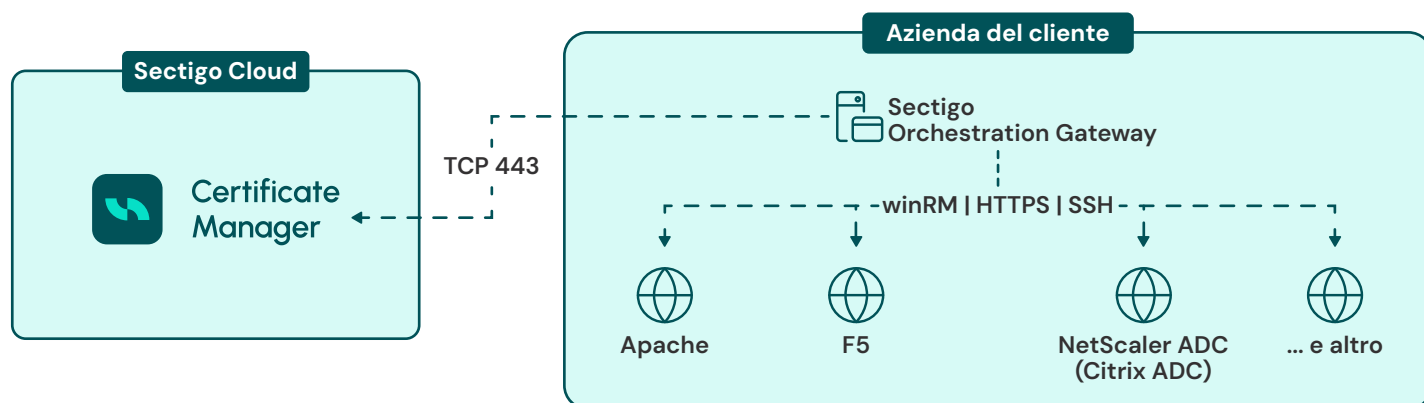
- **Automazione uno-a-molti**

Un'unica istanza di gateway si collega a più endpoint sulla rete, sostituendo VM dedicate, configurazioni HA e cicli di patch con una singola installazione.

- **Preparazione all'agilità crittografica**

Prepara le organizzazioni ai nuovi standard crittografici e alle transizioni di algoritmi, inclusi i requisiti post-quantistici, senza richiedere modifiche architetturali operative.

Come funziona



Visita la [pagina della documentazione tecnica](#) per l'elenco completo delle integrazioni supportate da Orchestration Gateway.

Il vantaggio Sectigo

Sectigo unisce una profonda competenza PKI con un'orchestratore progettato su misura per aiutare le aziende a modernizzare le operazioni sui certificati senza introdurre ulteriore complessità. SCM fornisce visibilità centralizzata, governance e controllo delle policy. SOG estende tale controllo negli ambienti reali attraverso un'orchestrazione sicura e dedicata, che include l'esecuzione basata su policy, l'accesso alle credenziali just-in-time e una gestione coerente del ciclo di vita tra le piattaforme. Insieme, sostituiscono script frammentati e strumenti isolati con un'esecuzione CLM end-to-end prevedibile su infrastrutture ibride e multi-cloud.

Questo approccio integrato riduce l'overhead operativo, minimizza la deriva di configurazione ed elimina i rischi legati ai rinnovi, fornendo al contempo una base modulare che si evolve insieme agli ambienti in cambiamento e ai requisiti crittografici. Con Sectigo, i team IT ottengono un'infrastruttura di fiducia automatizzata costruita per la scala attuale e progettata per adattarsi alle sfide di domani.

Informazioni su Sectigo

Sectigo è un provider leader nella gestione del ciclo di vita dei certificati (CLM), che aiuta le aziende a proteggere le identità umane e delle macchine riducendo i rischi nascosti della fiducia digitale moderna. Con la crescita dei volumi di certificati e la riduzione della loro durata, i certificati non gestiti diventano causa di disservizi, sanzioni di conformità e problemi operativi. Sectigo utilizza l'Automazione Orchestrata per offrire Semplificazione su Larga Scala attraverso la sua piattaforma CLM nativa in cloud, unendo visibilità, controllo e gestione del ciclo di vita in ambienti complessi. Con oltre 700.000 clienti, tra cui il 65% delle aziende Fortune 500, Sectigo è una delle autorità di certificazione più grandi e storiche, con oltre 20 anni di esperienza nel garantire la fiducia digitale.

Per maggiori informazioni su Sectigo Orchestration Gateway o sulle soluzioni di gestione dei certificati, contattare il team Sales di Sectigo all'indirizzo sales@sectigo.com.

