

Sectigo Orchestration Gateway pour Sectigo Certificate Manager (SCM)

Orchestrer l'automatisation SCM à grande échelle

Alors que les entreprises évoluent dans des environnements hybrides et multi-cloud, la gestion des certificats est devenue une discipline d'infrastructure essentielle. Des durées de vie de certificats plus courtes, le nombre croissant d'identités numériques et des systèmes toujours plus distribués ont modifié la façon dont les certificats doivent être émis, déployés et entretenus, imposant de nouvelles exigences en matière d'automatisation et de cohérence opérationnelle.

Points de pression opérationnels :

- **Opérations fragmentées** : Les tâches liées aux certificats sont souvent réparties entre des connecteurs hérités, des scripts personnalisés et des étapes manuelles, ce qui rend leur standardisation difficile.
- **Persistance des processus manuels** : Malgré l'augmentation de l'échelle et de la complexité, 95 % des organisations dépendent toujours d'opérations manuelles sur les certificats.
- **Volumes de certificats en croissance** : Les initiatives Zero Trust, l'extension de l'authentification machine-à-machine et le raccourcissement des durées de vie augmentent l'émission de certificats sur les serveurs, applications et plateformes.
- **Évolution des exigences** : Les attentes réglementaires, la planification de l'agilité cryptographique et la vérification continue élèvent le niveau d'exigence en matière de contrôle et de cohérence.

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

Lorsque les opérations de certificats restent fragmentées, le coût se paie en fiabilité et en contrôle. Les renouvellements manqués et les flux de travail incohérents augmentent le risque de pannes. Lorsque l'automatisation dépend de machines virtuelles, de scripts et de connecteurs distincts pour chaque plateforme, la mise à l'échelle devient un multiplicateur de risques. À mesure que les volumes de certificats augmentent et que les cycles de renouvellement s'accélèrent, les approches d'automatisation traditionnelles ne se contentent pas de peiner à suivre le rythme : elles deviennent un facteur de vulnérabilité, empêchant les équipes IT et de sécurité d'offrir la résilience et la confiance dont dépend l'entreprise.

Ce que les équipes IT doivent attendre d'une automatisation moderne des certificats

- ✓ **Une couche d'automatisation optimisée**
Une approche consolidée qui remplace les VM par intégration, les connecteurs et les scripts par une couche d'automatisation unique couvrant les environnements essentiels.
- ✓ **Cohérence à grande échelle**
Des flux de travail standardisés qui se comportent de manière prévisible sur les infrastructures hybrides et multi-cloud à mesure que le volume et la fréquence de renouvellement augmentent.
- ✓ **Conçue pour des cycles de vie plus courts**
Une automatisation qui suit le rythme de la croissance des volumes et des cycles accélérés sans charge opérationnelle supplémentaire.
- ✓ **Visibilité opérationnelle claire**
Des informations pratiques et en temps réel sur l'emplacement des certificats, leur date d'expiration et le déroulement des événements du cycle de vie.
- ✓ **Gestion sécurisée des clés par défaut**
La récupération juste-à-temps des identifiants privilégiés garantit que l'accès n'est accordé que lorsque cela est nécessaire, réduisant ainsi l'exposition des clés.
- ✓ **Faible friction de déploiement et de maintenance**
Une configuration légère, une maintenance minimale et une architecture qui simplifie les opérations plutôt que d'ajouter de la complexité.
- ✓ **Prête pour l'avenir**
La flexibilité nécessaire pour s'adapter aux nouvelles plateformes, à l'évolution des normes cryptographiques et aux changements réglementaires sans réarchitecturer l'automatisation.

Qu'est-ce que Sectigo Orchestration Gateway (SOG) ?

Le SOG est une couche d'orchestration légère et modulaire conçue spécifiquement pour fonctionner en toute fluidité avec [Sectigo Certificate Manager \(SCM\)](#). Il exécute les tâches de déploiement et de gestion du cycle de vie des certificats au sein d'environnements complexes, distribués et multi-fournisseurs, éliminant ainsi le fardeau des scripts fragiles, des interventions manuelles et des connecteurs hérités.

Travaillant aux côtés de SCM, le SOG fournit une base d'automatisation sécurisée, évolutive et pilotée par des politiques, conçue pour les réalités des infrastructures hybrides et multi-cloud modernes. Conçu comme une passerelle extensible, son architecture modulaire automatise aujourd'hui les opérations de certificats TLS et s'étend naturellement vers de nouveaux cas d'utilisation au fil de l'évolution des besoins.

Compatibilité écosystémique en croissance continue

Endpoints TLS pris en charge :



Coffres-forts d'identifiants pris en charge :



Pour obtenir la liste la plus récente des intégrations prises en charge, consultez notre [page de documentation technique](#).

Déployé avec Sectigo Certificate Manager, le SOG aide les équipes IT à obtenir :



Des opérations de certificats simplifiées et prévisibles

Les organisations bénéficient d'une couche d'automatisation unique et cohérente qui standardise les flux de travail des certificats sur les environnements cloud.

- **Orchestration unifiée du cycle de vie des certificats**

Automatisez la découverte, l'émission, le renouvellement, le déploiement et la révocation sans jongler entre scripts ou connecteurs spécialisés.

- **Workflows standardisés et pilotés par les politiques**

Appliquez des politiques cohérentes de gestion des clés et des certificats sur les environnements hybrides et multi-cloud, réduisant ainsi les écarts, les exceptions manuelles et les lacunes de configuration.

- **Déploiement rapide et léger**

Une empreinte modulaire permet un déploiement rapide avec un minimum de prérequis, minimisant à la fois l'effort d'installation et la maintenance continue.



Automatisation de bout en bout à grande échelle

Suivez le rythme de l'accélération des cycles de vie et de l'explosion des volumes de certificats, en éliminant la gestion de crise qui accompagne souvent le suivi manuel ou les renouvellements de dernière minute.

- **Renouvellements haute fréquence sans effort**

Les cycles plus courts et les renouvellements à fort volume sont entièrement automatisés, réduisant la charge opérationnelle tout en assurant la continuité sur les systèmes distribués.

- **Opérations de certificats parallèles**

Les certificats peuvent être émis, renouvelés et déployés sur plusieurs plateformes simultanément, éliminant les goulots d'étranglement liés aux mises à jour séquentielles.

- **Couverture complète du cycle de vie des certificats**

De la découverte cloud et locale au déploiement sur les points d'accès, toutes les opérations sont orchestrées de manière centralisée et automatique via SCM.

- **Visibilité complète dans tout l'environnement**

La découverte cloud et locale analyse simultanément les réseaux internes et les systèmes externes, maintenant un inventaire à jour et éliminant les angles morts.



Gestion sécurisée des clés par défaut

La sécurité des clés est renforcée à chaque étape, réduisant l'exposition et garantissant une hygiène rigoureuse à grande échelle.

- **Élimine la dispersion des clés**

Les clés privées sont générées au moment nécessaire sur chaque point d'accès, éliminant la dispersion et garantissant une gestion contrôlée et prévisible.

- **Génération de clés par certificat**

Chaque certificat reçoit sa propre clé privée générée sur l'endpoint, éliminant la réutilisation et réduisant la surface d'attaque.

- **Pas de stockage de clés partagé**

Évitez les référentiels centralisés et les structures de coffres partagés qui créent des risques à mesure que les volumes de certificats augmentent.



Une automatisation conçue pour évoluer avec votre environnement

Une architecture modulaire et tournée vers l'avenir garantit que l'automatisation reste prête pour les évolutions futures.

- **Architecture extensible et modulaire**

La prise en charge de nouveaux serveurs, plateformes, coffres-forts et systèmes PAM peut être ajoutée sans réarchitecturer les workflows existants.

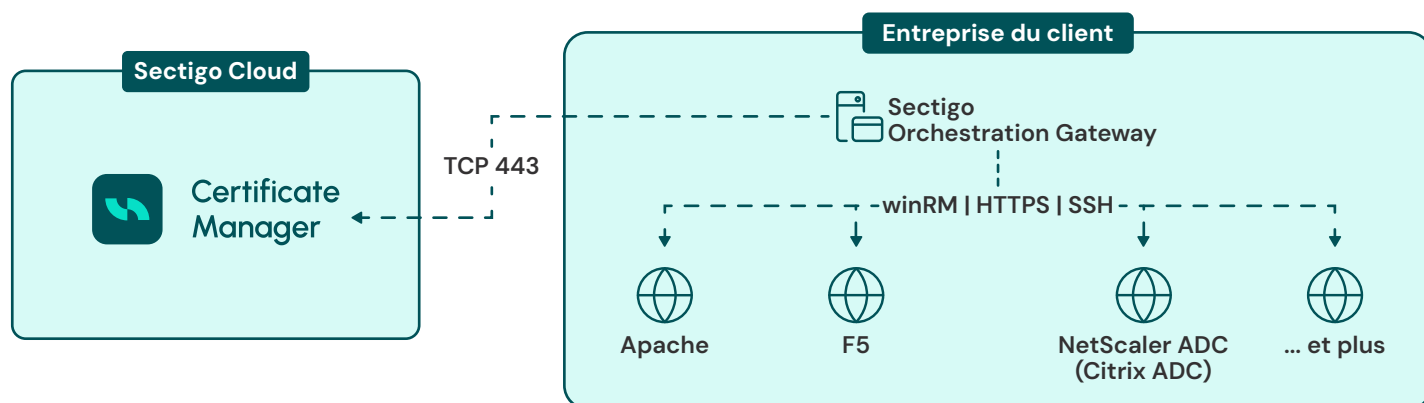
- **Automatisation un-vers-plusieurs**

Une seule instance de passerelle se connecte à plusieurs endpoints sur le réseau, remplaçant les VM spécifiques aux intégrations, les configurations HA et les cycles de correctifs par une seule installation.

- **Préparation à l'agilité cryptographique**

Prépare les organisations aux nouvelles normes cryptographiques et aux transitions d'algorithmes, y compris les exigences post-quantiques, sans nécessiter de refonte opérationnelle.

Comment ça marche



Consultez la [page de documentation technique](#) pour la liste complète des intégrations compatibles avec l'Orchestration Gateway.

L'avantage Sectigo

Sectigo combine une profonde expertise en PKI avec une orchestration sur mesure pour aider les entreprises à moderniser leurs opérations de certificats sans introduire de complexité supplémentaire. SCM fournit une visibilité, une gouvernance et un contrôle des politiques centralisés. Le SOG étend ce contrôle dans les environnements réels grâce à une orchestration sécurisée et dédiée, incluant l'exécution basée sur des politiques, l'accès aux identifiants juste-à-temps et une gestion cohérente du cycle de vie sur l'ensemble des plateformes. Ensemble, ils remplacent les scripts fragmentés et les outils ponctuels par une exécution CLM prévisible et de bout en bout sur les infrastructures hybrides et multi-cloud.

Cette approche intégrée réduit la charge opérationnelle, minimise la dérive de configuration et élimine les risques liés aux renouvellements, tout en fournissant une base modulaire qui évolue aux côtés des environnements changeants et des exigences cryptographiques. Avec Sectigo, les équipes IT bénéficient d'une infrastructure de confiance automatisée conçue pour les volumes d'aujourd'hui et préparée aux évolutions de demain.

À propos de Sectigo

Sectigo est un leader de la gestion du cycle de vie des certificats (CLM), aidant les entreprises à sécuriser les identités humaines et machines tout en réduisant les risques masqués de la confiance numérique moderne. À mesure que les volumes de certificats augmentent et que leurs durées de vie se réduisent, les certificats non gérés deviennent une source de pannes, de faiblesses de conformité et de perturbations opérationnelles. Sectigo utilise l'Automatisation Orchestrée pour offrir la Simplicité à Grande Échelle grâce à sa plateforme CLM native dans le cloud, réunissant visibilité, contrôle et gestion du cycle de vie au sein d'environnements complexes. Avec plus de 700 000 clients, dont 65 % du Fortune 500, Sectigo est l'une des autorités de certification les plus importantes et les plus anciennes, forte de plus de 20 ans d'expérience au service de la confiance numérique.

Pour plus d'informations sur Sectigo Orchestration Gateway ou les solutions de gestion de certificats, veuillez contacter l'équipe commerciale de Sectigo à sales@sectigo.com.

