sectigo

DATASHEET

Model Context Protocol (MCP) Server for Sectigo Certificate Manager (SCM)

Operationalize AI-driven certificate management inside governed PKI environments

AI agents are already part of the enterprise stack. Security and IT teams use them to query systems, trigger workflows, and automate operations through natural language. The real question is no longer whether they belong in production environments, but how their actions are governed.

That question becomes critical in certificate lifecycle management. Non-human identities are now embedded across services, containers, APIs, and AI agents, each relying on certificates with their own lifecycle. As public SSL/TLS certificate lifespans move toward 47 days, renewal shifts from periodic activity to continuous operational load.

Directly connecting AI agents to certificate infrastructure without a governed execution layer increases risk. It can introduce inconsistent access control, weak separation of duties, and fragmented auditability. The goal is not to slow AI down, but to let it execute safely, with governance built into every action.

52%

of executives in AI-active organizations have agents running in production today.

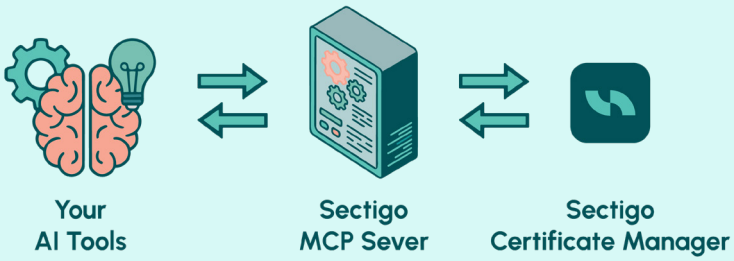
-Google Cloud's AI Agent Trends 2026

Sectigo MCP Server for SCM

Sectigo MCP Server provides your AI agent of choice with a single, governed connection to SCM via the Model Context Protocol. Your teams can now execute certificate tasks in plain language through the AI agent they already use. No UI navigation, no scripting, and no custom integration work.

Your AI agent gets immediate access to the certificate operations that matter most, all executed through SCM's existing Admin API:

- Search certificates by organization, status, expiry, and more
- Retrieve full certificate details
- Request new certificates
- Renew, revoke, or replace certificates by ID
- Download issued certificates
- List available organizations inside SCM
- Check Domain Control Validation status
- Approve/decline certificate requests



What you gain with Sectigo MCP Server

Stay in control without slowing your AI implementation down

Every agent request inherits SCM's existing authentication, role-based access controls, and approval workflows automatically.

Know exactly what your AI agents did, and when

Every certificate operation is logged within SCM. Complete visibility into what ran, who requested it, and when, without adding a separate audit layer.

Zero infrastructure burden

Sectigo operates the MCP Server endpoint. There is no infrastructure to provision, maintain, or secure. Authenticate via a permission-scoped token, and your agents are ready to work.

Your AI, your choice

Connect any MCP-compatible AI agent your organization already uses. Your existing AI investment works here without additional integration work or per-agent setup.

Handle 47-day renewal volumes with confidence

As renewal cycles compress from annual to continuous, AI agents handle the operational load through natural-language workflows while your team stays focused on oversight.

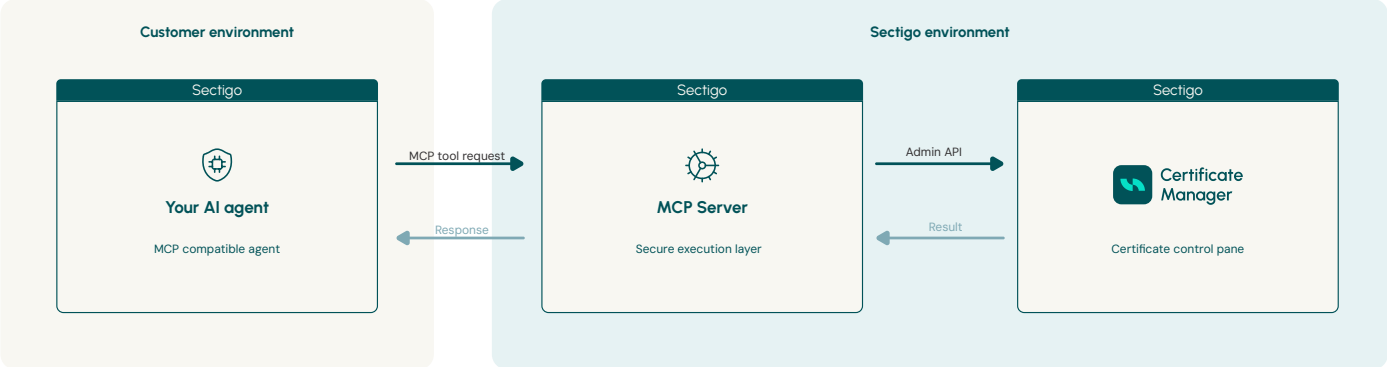
> "Mature organizations know that AI leadership is paramount to spurring transformation, establishing new enterprise competencies and capabilities, and engaging the entire enterprise in this mission."
>
> ***Gartner**, Leaders Who Fail to Embed AI Into Their Enterprise's DNA Will Be Rapidly Outpaced, ID: G00840194*

Ask your AI agent. SCM handles the rest.

Certificate operations that once required multiple steps across SCM now happen through a single instruction to the AI agent your team already uses.

	Without Sectigo MCP Server	With Sectigo MCP Server
Find expiring certificates	1. Log into SCM. 2. Open the certificate workflow. 3. Enter filter criteria. 4. Apply filters. 5. Review results manually.	"Show me SSL certificates in the Finance org expiring in the next 30 days."
Certificate renewal	1. Locate the certificate in SCM. 2. Navigate to the renewal workflow. 3. Submit manually.	"Renew SSL certificate ID 10482."
Emergency revocation	1. Identify the compromised certificate. 2. Navigate the revocation workflow. 3. Execute and confirm.	"Revoke SSL certificate ID 10482 with reason Key Compromise."
Certificate replacement	1. Locate the certificate. 2. Submit a new CSR. 3. Re-enter profile and configuration details.	"Replace SSL certificate ID 9871 with a new CSR."
Approve/decline requests	1. Log into SCM. 2. Navigate to the approval queue. 3. Review and action each request individually.	"Approve SSL certificate request ID 10482." or "Decline SSL certificate request ID 9871."
Download a certificate	1. Log into SCM. 2. Locate the issued certificate. 3. Navigate to the download screen. 4. Export manually.	"Download the issued certificate for SSL certificate ID 10482."
List available organizations	1. Log into SCM. 2. Navigate to the organization view. 3. Browse the full list manually.	"What organizations are available in my SCM account?"
Check domain validation	1. Navigate to the DCV section in SCM. 2. Locate the domain. 3. Review status manually.	"Check the DCV status for acme-corp.com."

How it works



Sectigo advantage

Sectigo MCP Server is fully hosted and accessible worldwide, with no regional restrictions and no deployment overhead. Your teams operate through a single governed endpoint regardless of where they are located.

Most MCP implementations for certificate management surface information only. Sectigo MCP Server acts on it. Your AI agents issue, renew, revoke, replace, approve, and download certificates in real time through SCM's existing Admin API. Not just queries. Real certificate actions, at enterprise scale.

Get in touch

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

About Sectigo

Sectigo is a leader in certificate lifecycle management (CLM), providing innovative and comprehensive solutions to secure both human and machine identities for some of the world's most prominent brands. Its cloud-native, automated, and universal CLM platform simplifies and enhances enterprise security by issuing and managing digital certificates from all trusted certificate authorities (CAs). With over two decades of experience, Sectigo stands as one of the largest and most established CAs, serving more than 700,000 customers worldwide.

By delivering unparalleled digital trust, Sectigo continues to empower organizations to implement robust securityprotocols with efficiency and confidence.