SOLUTION BRIEF

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

Operationalize AI-driven certificate management inside governed PKI environments

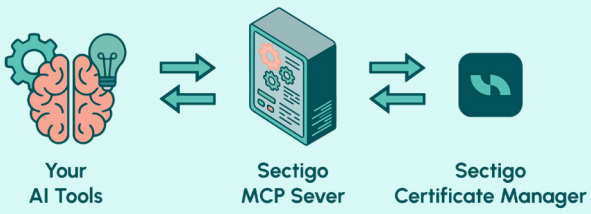
Non-human identities are now spreading across services, containers, APIs, and AI-driven processes. Each depends on certificates with its own lifecycle. As SSL/TLS validity moves toward 47 days, renewals shift from a scheduled task to a constant operational demand.

At the same time, many enterprises have already put AI agents to work across security and IT. What's still unresolved is how to give those agents-controlled access to certificate infrastructure without introducing authentication gaps, inconsistent controls, or fractured audit trails.

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 connects your AI agents to Sectigo Certificate Manager as the single, governed execution layer. Teams now can manage certificate tasks in plain language, using the AI tools they already rely on. No scripting, no interface switching, no custom connectors required.

What used to require manual effort now runs through your agents – finding expiring certificates, new issuances, renewals, revocations, check domain validation status, download certificates, and more. All of it is governed by SCM's existing framework, with consistent access controls, clear visibility, and a complete audit trail.

Get it done with one prompt, in simple words

The example below is one of many ways Sectigo MCP Server eliminates the manual steps between your team and their certificates.

	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."

What Sectigo MCP Server Enables

AI on your terms

Connect any MCP-compatible agent.

Ask-to-action made simple

Natural language prompts become governed certificate actions. No scripting required.

Certificate actions that enable workflows

Issue, renew, revoke, replace, approve, search, and report. Execution that goes well beyond read-only access.

Always within bounds

Permission-scoped tokens ensure AI agents act only within boundaries you have defined.

No infrastructure needed

Connect your preferred AI agent to Sectigo's fully hosted endpoint.

Every control stays intact

Keep SCM as the system of record throughout. Log every action, enforce every approval, and maintain every audit trail.

Common Use Cases

Stay ahead of high-frequency renewals

At shorter lifespans, renewal volume grows significantly. AI agents connected through the MCP Server can identify expiring certificates, initiate renewals, and confirm issuance automatically, reducing manual workload without bypassing approval controls.

Accelerate incident response

When a certificate-related incident occurs, speed matters. AI agents can query certificate status, trigger revocation, and initiate reissuance through natural language commands, compressing response time without requiring manual API navigation.

Streamline certificate discovery and reporting

AI agents can query SCM for certificate inventory, expiry windows, and coverage gaps across environments. Security teams get accurate, on-demand visibility without building custom reporting pipelines.

Integrate certificate operations into broader agentic workflows

For teams building agentic workflows that span infrastructure tasks, the MCP Server provides a stable, predictable interface for the certificate operations layer.

Reduce onboarding friction

New team members execute certificate tasks through natural language from day one. No platform training required, no manual navigation, and no waiting to become productive.

Sectigo advantage

Sectigo MCP Server is available and fully hosted globally, giving your teams a single governed endpoint that works wherever they operate.

Most MCP implementations for certificate management stop at surfacing information. Sectigo goes further. Your agents can take real action through SCM's existing Admin API, issuing, renewing, revoking, replacing, approving, and downloading certificates at enterprise scale.

Sectigo has always believed that the right infrastructure decision today should not become a liability tomorrow. Built on an open standard and connected to the platform your team already manages, Sectigo MCP Server is designed to grow with your AI strategy. As your capabilities evolve, your certificate operations infrastructure keeps pace.

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.