sectigo

DATASHEET

CA agnostic certificate lifecycle management

Keep your CAs. Consolidate the lifecycle.

Most enterprises run more than one certificate authority (CA). Public CAs secure websites and apps. Private CAs secure internal systems. Redundancy plans, regional needs and acquisitions add more. Each CA brings its own console, renewal process and blind spots.

Sectigo Certificate Manager (SCM) brings certificates from Sectigo and other public and private CAs into one inventory, one policy set and one automation model. SCM connects to DigiCert, GlobalSign, Microsoft CA (ADCS), AWS Private CA, Google Cloud CA Service and EJBCA, so your team can discover, issue, renew and revoke certificates in the same workflows, without changing CAs.



Built for shorter lifespans

Public TLS validity drops toward 47 days by 2029, and every renewal depends on a CA being trusted and available. SCM automates issuance and renewal across every connected CA using open standards, with no lock-in to a single vendor.

sectigo.com | Sectigo© 2026. | All rights reserved.

How it works?

The Sectigo CA Connector runs in your environment and links your existing CAs to SCM. One connector can serve several CAs, and several instances of each.

Public CAs

SCM connects to the public CAs you already use, such as DigiCert and GlobalSign. Your team can find, issue, renew and revoke their certificates in the same workflows as everything else, without changing CA relationships.

Private CAs

Private CAs anchor internal trust. Reissuing a private hierarchy is rarely realistic when roots are built into devices and applications. SCM manages certificates from Microsoft CA (ADCS), AWS Private CA, Google Cloud CA Service and EJBCA through each vendor's platform, with your hierarchy left intact. Sectigo Private CA is also available within SCM.

One lifecycle across every CA

Once your CAs are connected, you set issuance policy in SCM with any public or private CA as the source. SCM sends each request to the right CA, then manages every certificate in one place for installation, renewal, revocation and automation.

CA redundancy with Sectigo

One CA is a single point of failure.

Why it matters

Outages, mis-issuance, mass revocation and distrust can happen at any CA. When they do, the CA sets the timeline, and teams with only one CA have nowhere else to issue from. Shorter lifespans raise the stakes: with renewals every few months, even a short CA disruption can turn into expired certificates and service outages. A backup CA only helps if it's connected and managed before you need it.

Add Sectigo as a second CA and manage both in SCM. If your primary CA has an outage, distrust or mass revocation event, moving issuance becomes a policy change, not a migration.



Add a second public CA

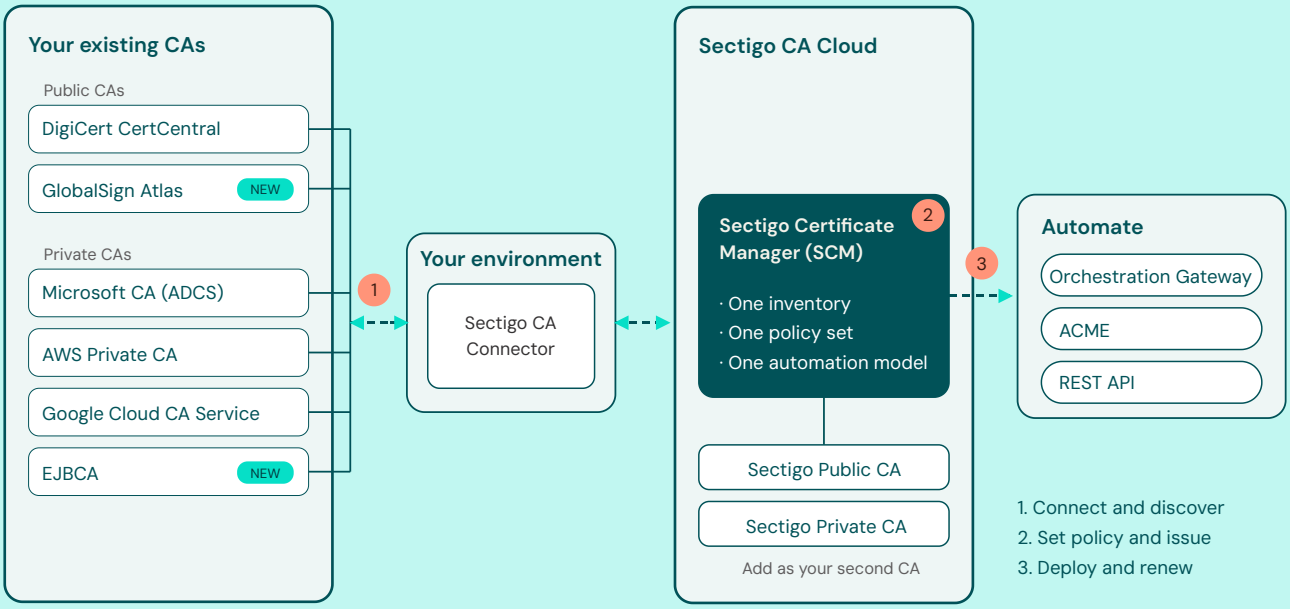
Pair DigiCert or GlobalSign with Sectigo public CA and switch issuance without rebuilding workflows.



Add a second private CA

Pair EJBCA or another private CA with Sectigo Private CA and shift workloads at your own pace.

One lifecycle across every CA you trust



Explore all supported Sectigo Certificate Manager integrations.

Technical documents: Understanding CA connectors

Key benefits of Sectigo Certificate Manager

Centralized control
A single pane of glass to manage both public and private certificates issued from Sectigo and other certificate authorities.

Rooted in trust
CA-grade governance, standards leadership through Sectigo's active role in the CA/Browser Forum, and built-in crypto agility and postquantum readiness.

No CA lock-in
Keep the CAs you trust, add Sectigo when you're ready, and shift issuance by policy. Consolidate tools, not CA relationships.

Zero-touch deployment
Automatically deploy and install certificates across your environment, with no manual steps.

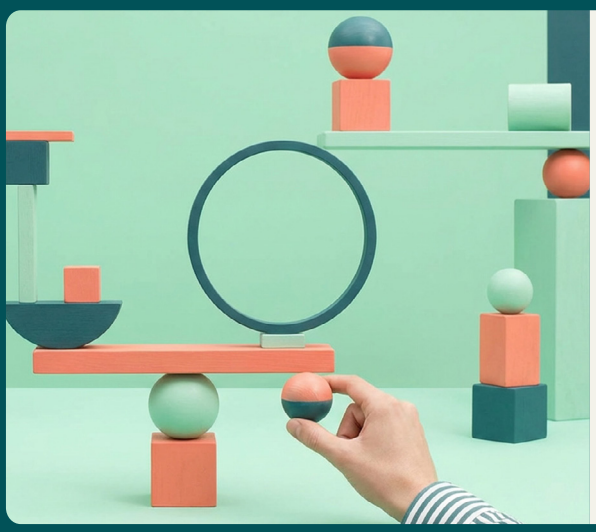
Certificate management in the cloud
Cloud-native efficiency means lower cost of deployment, faster threat discovery, automation, and perimeterless security across cloud and multi-cloud environments.

Enterprise integrations
Integrations with leading technology providers offer deployment flexibility and customizations to work within unique environments.

Dedicated support
Industry-leading customer support with white glove service from onboarding to continued account services.

CA reduncancy
A connected second CA keeps certificates issuing through an outage, distrust or mass revocation event.

sectigo.com | Sectigo© 2026. | All rights reserved.



CA redundancy with Sectigo

SCM manages public and private certificates from Sectigo and other CAs under one policy and audit trail. It's built for shorter lifespans, with no lock-in.

Talk to a Sectigo expert at sales@sectigo.com or explore SCM integrations.

About Sectigo

Sectigo is a leading provider of Certificate Lifecycle Management (CLM), helping organizations secure human and machine identities while reducing the hidden risks of modern digital trust. As certificate volumes grow and lifespans shrink, unmanaged certificates are becoming a source of outages, compliance exposure, and operational disruption. Sectigo uses Orchestrated Automation to deliver Simplicity at Scale through its cloud native CLM platform, bringing visibility, control, and lifecycle management together across complex environments. With more than 700,000 customers, including 65% of the Fortune 500, Sectigo is one of the largest and longest standing certificate authorities, with over 20 years of delivering unparalleled digital trust. For more information, visit www.sectigo.com or follow us on LinkedIn.

sectigo.com | Sectigo© 2026. | All rights reserved.