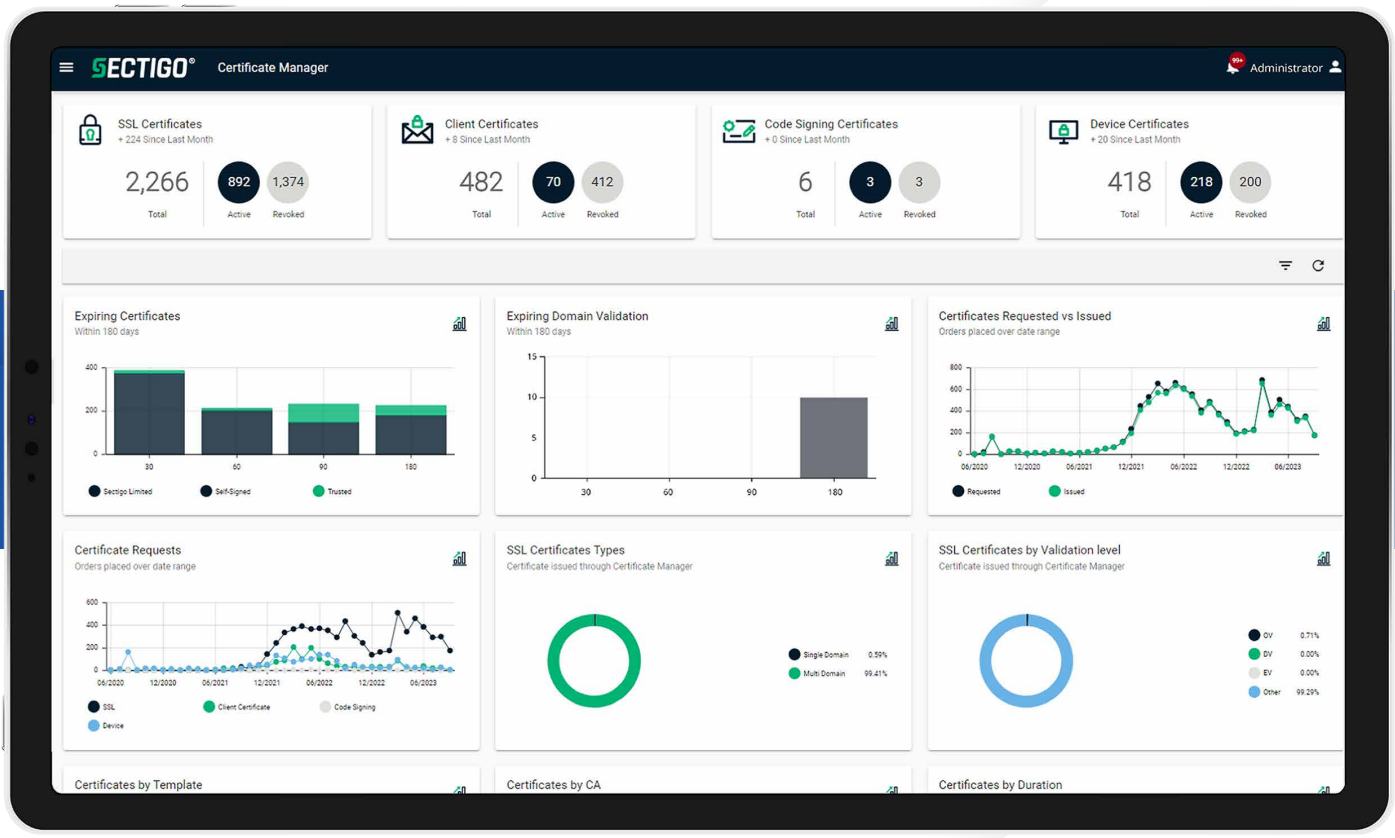
SECTIGO® | CERTIFICATE MANAGER

Datasheet

Sectigo Certificate Discovery



SECTIGO®

Why Discovery Matters

Many organizations struggle with incomplete visibility into their certificate environments, leading to outages, compliance risks, and operational inefficiencies. Discovery helps eliminate these issues by uncovering:

- **Rogue or unauthorized certificates** issued outside approved processes, often by shadow IT or unmanaged private CAs.
- **Certificates hidden in team silos,** especially within DevOps pipelines, where short-lived certs may be spun up without oversight.
- **Scattered storage locations** across hybrid and multi-cloud environments, making centralized management nearly impossible.
- **Expired or soon-to-expire certificates** that can cause downtime, security alerts, or failed audits.
- **Unknown or forgotten certificates** left behind from previous systems, migrations, or decommissioned services.
- **Weak or outdated cryptographic configurations** such as deprecated algorithms or insufficient key lengths
- **Certificates with unclear usage** or attached to dormant services, contributing to bloat and audit gaps

By addressing these pain points, certificate discovery lays the foundation for secure, efficient certificate lifecycle management.

SECTIGO®

In addition to providing a comprehensive understanding of the digital landscape, certificate discovery offers a few key advantages:

Full visibility

An overwhelming 97 percent of organizations claim that partial visibility due to increased certificate volumes and expanded use cases is a key risk . Effective discoveries should inventory every digital certificate to eliminate blind spots, and provides centralized visibility across all environments, including certificates issued by third-party CAs and those stored in Microsoft Active Directory.

Outage prevention

Discovery reveals which certificates are nearing expiration, driving proactive renewal strategies that are also supported via CLM automation. Automated renewal reduces the risk of costly expirations or outages, and automation provides users with real-time alerts of their certificate inventory.

Stronger security posture

Visibility elevates security posture by highlighting otherwise hidden weak points involving rogue certificates, outdated algorithms, or other cryptographic concerns. Discovery also supports crypto-agility by ensuring every certificate is known, current, and quickly replaceable as requirements evolve.

Improved compliance

Certificate discovery provides clear proof of strong data encryption and identity verification, and produces an audit trail, verifying close adherence to strict regulatory standards. Automated scanning and documentation help enforce policy-driven CLM for audits, governance, and internal risk controls.

How it Works

Sectigo's comprehensive discovery solutions center around four key capabilities. These are defined by relationships to the cloud, external or internal focus, reliance on agents, and specific integrations. Capabilities include:

Cloud discovery

Helps discover and manage certificates from Azure Key Vault, AWS Certificate Manager, and GCP Certificate Manager. It pulls certificates directly into SCM, giving you centralized oversight without the need for manual exports.

External certificates (agentless)

Address public-facing servers without direct agent installation. External certificate discovery provides a straightforward approach to scanning certificates. This leverages the TLS (Transport Layer Security) handshake to collect certificate details without requiring an agent or internal access.

Internal certificates (network agent)

Install an agent within the local environment to scan endpoints and discover internal certificates. Sectigo reaches out via the network agent and then creates a TLS handshake. The certificate is returned to the Sectigo platform, where it can be inventoried.

Internal certificates (MS agent)

Sectigo Certificate Manager (SCM) runs on a Windows system and connects to Active Directory to retrieve certificates published to the Active Directory and issued by your Microsoft CA. Those certificates are then pulled into SCM for centralized visibility and tracking. This also enables assignment of certificates to specific teams, departments, or organizations, simplifying management across complex environments.

SECTIGO®

Following a complete scan, examine both previously and newly discovered certificates. After a complete scan, all discovered certificates, internal and external, are clearly identified and organized within the SCM portal. Displayed in a single, intuitive view, Sectigo shows where each certificate was found, its expiration date, and other key metadata such as common name, certificate profile and renewal status.

Sectigo's Features and Solutions

In addition to providing a comprehensive understanding of the digital landscape, certificate discovery offers a few key advantages:

Continuous scanning

Periodic scans can be configured to ensure proactive monitoring so that all certificates are identified, tracked, and assessed to prevent expirations and other issues. Sectigo Discovery scales effortlessly across enterprises, regardless of certificate volume or issuing CA.

Instant alerts

With Sectigo, detected misconfigurations or expirations prompt email, Teams, or Slack alerts, facilitating a quick response that can prevent costly downtime or breaches and integrating seamlessly with existing workflows.

Intuitive dashboard

Promising centralized visibility, Sectigo's easy-to-navigate dashboard provides a helpful overview of all discovered certificates and clarifies essential details in a highly visual and accessible manner.

Enhanced search and filtering

Sectigo's search mechanisms allow users to filter based on important certificate attributes. Filtering features help you manage certificates with ease, allowing you to quickly find certificates by issuer, expiration date, configuration status, and more.

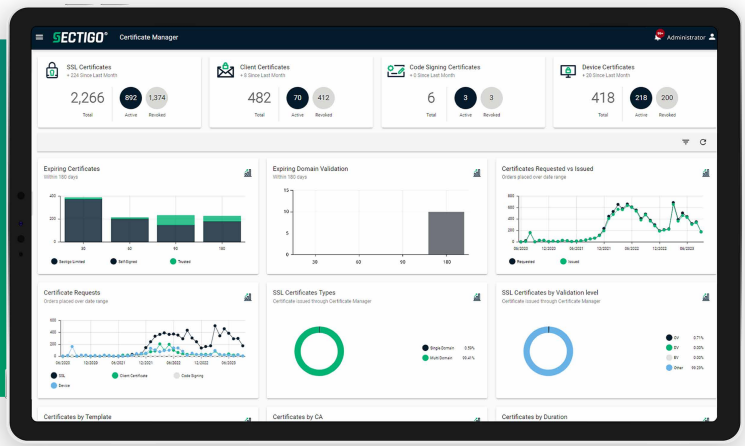
Certificate discovery reporting

Sectigo Discovery reports help to reveal overall compliance and security posture, supporting audits, risk assessments, and internal governance planning, to ensure organizations stay in line with standards like NIST 2.0, PCI DSS, GDPR, HIPAA, and more.

Get Started with Certificate Discovery

Ready to expand certificate visibility and get on the path to reliable certificate management?

Book a Demo to see it in action



About Sectigo

Sectigo is a leading provider of digital certificates and Certificate Lifecycle Management solutions – establishing a strong foundation of digital trust for companies of all sizes. Sectigo's universal CLM platform is CA agnostic and automates the lifecycles of both public and private digital certificates, regardless of origin, within a single platform. With over 20 years of experience, Sectigo's heritage as a Certificate Authority is uniquely positioned to provide over 700,000 customers the confidence they need in an increasingly challenging cybersecurity landscape.

For more information, visit www.sectigo.com.

SECTIGO®