appviewx

AVX ONE Certificate Lifecycle Management (CLM): Smart Discovery

Automated Certificate Discovery to achieve complete certificate visibility and mitigate the risk of certificate-related outages, vulnerabilities, and compliance violations

Overview

Digital certificates are fundamental to securing and maintaining the availability of all digital assets in an organization. Through authentication and encryption, they help establish digital trust vital for all internet communications and transactions. However, without complete visibility and effective management, these certificates can become a source of significant risk, exposing organizations to downtime, unauthorized access, and data breaches.

Today's complex IT infrastructures operate with a large number of certificates used to secure a wide variety of public and private trust machine (non-human) identity management use cases. These certificates continue to proliferate rapidly across cloud, edge, and containerized environments. Being aware of how many certificates there are, who owns them, and where they are located is crucial to managing certificates effectively, eliminating security blindspots, and tackling disruptions, such as CA compromises/ distrust incidents, Google's 90-day certificate proposal, and post-quantum cryptography.

Challenges - Certificate Discovery and Visibility

Discovering and maintaining visibility into all certificates in the infrastructure is a significant challenge organizations face, particularly when relying on spreadsheets and point solutions for certificate lifecycle management. While CA-provided tools can assist in discovering and managing certificates issued by a specific CA, they fall short in holistically discovering and managing certificates acquired from all sources (public and private CAs) or deployed across multiple endpoints (servers, mobile devices, laptops, etc.). Without CA-agnostic discovery and centralized visibility, PKI, InfoSec, and cross-functional teams are forced to operate in silos, facing constant dilemmas.

- How do you manage certificates issued by multiple public/private CAs?
- Do you have a single source of truth for all certificates or do you use multiple tools (i.e. spreadsheets, CA-provided tools, etc.)?
- Where do you look when there is a certificate-related outage?
- How quickly can you detect and remediate a certificate-related outage or security incidents?
- How do you know which certificates are tied to which applications, services, and devices?
- How do you track certificates that are about to expire?
- How do you detect and monitor certificates that are self-signed or use weak crypto standards?

Large organizations often have several departments across multiple geographies, with each team requesting certificates based on individual requirements. This leads to many certificates going unmanaged or rogue in remote locations across complex hybrid multi-cloud environments. For instance, developers frequently create self-signed certificates for testing purposes, which when not tracked, can end up in production, exposing systems to vulnerabilities and security breaches. However, lack of discovery and visibility makes tracking self-signed certificates a logistical nightmare. Eventually, these certificates become gateways for malicious actors to gain access to the network. Also, while discovering certificates across the enterprise infrastructure is a struggle in itself, certificates that reside on devices outside the network perimeter, such as edge and IoT devices mostly go undocumented.

Another challenge is the discovery of temporary certificates from third-party software used for initial testing. These certificates must be replaced before going into production. However, due to process oversights, these temporary certificates can end up in an organization's infrastructure without the knowledge of the PKI and security teams. Additionally, application owners might deploy certificates, including from unapproved CAs without informing PKI administrators, leading to certificates going unnoticed.

Unknown, unmanaged, and non-compliant digital certificates pose significant security risks and operational challenges. Certificate sprawl, fragmented visibility, and poor control over these certificates can lead to unexpected expirations causing outages, unauthorized access, data breaches, and system vulnerabilities, undermining the overall security posture of an organization. They can also complicate audits and compliance, potentially resulting in costly fines and reputational damage.

How AVX ONE CLM Helps Build Awareness and Greater Visibility of Your Certificate Ecosystem

AppViewX AVX ONE CLM is a ready-to-consume, scalable certificate lifecycle management (CLM) solution that automates all certificate processes end-to-end. It enables you to discover, inventory, monitor, and automate the complete lifecycle for all public and private trust certificates, through a central management console. AppViewX brings together visibility, automation, and control across on-premises, multi-cloud, hybrid cloud, IoT, and containerized environments to simplify certificate lifecycle management, improve efficiency, build crypto-agility, and ensure continuous compliance.

AVX ONE CLM - Smart Discovery

As mentioned earlier, establishing complete visibility of the entire certificate inventory is critical to preventing certificate-related issues and risks. The first step towards achieving visibility is to discover all certificates installed in your infrastructure.

AVX ONE CLM offers **Smart Discovery** to automatically discover certificates across your hybrid multi-cloud environments. Automated discovery helps locate and document all certificates used within your organization, giving you comprehensive visibility to take immediate action, eliminating the risk of unknown, rogue, and non-compliant certificates.

AVX ONE CLM Smart Discovery provides various scanning methods to help discover public and private trust certificates on machines, devices, workloads, applications, cloud services and more. These scans can be run on demand or at scheduled intervals to continually discover new certificates. Flexible **discovery schedules** help in running automated discovery at fixed off hours or during low traffic hours as per the organizational standards.

The various scanning methods offered by AVX ONE CLM Smart Discovery include:

1. Public Certificate Discovery/CT Log Scan

This scan allows you to discover certificates from publicly accessible Certificate transparency (CT) logs, helping to detect public TLS certificates, including rogue or unauthorized certificates.

2. Cloud Discovery/Cloud Account Scan

This scan allows you to discover certificates from managed cloud instances and services, such as AWS, Azure, and GCP. Proper authentication and authorization is required to access the internal certificate store and all the resources using the certificates.

3. Public/Private CA Scan

AVX ONE CLM offers out-of-the-box integration with prominent certificate authorities to help discover certificates based on CAs. You can onboard both your public and private CAs to AppViewX and run a CA scan to fetch certificates from all CA accounts.

4. Managed Devices Scan

Not all certificates are exposed to a port on the network. In such cases, you can run this scan to discover certificates from the device certificate stores. Certificates are discovered by scanning the configuration of network devices (such as load balancers, firewalls, and web servers) using the device's authentication credentials.

5. External Tool Scan

AVX ONE CLM integrates with third-party security scanning tools like Rapid7 and Qualys to allow you to import certificates. This eliminates the need for running multiple scanners for certificate discovery.

6. Network Scan

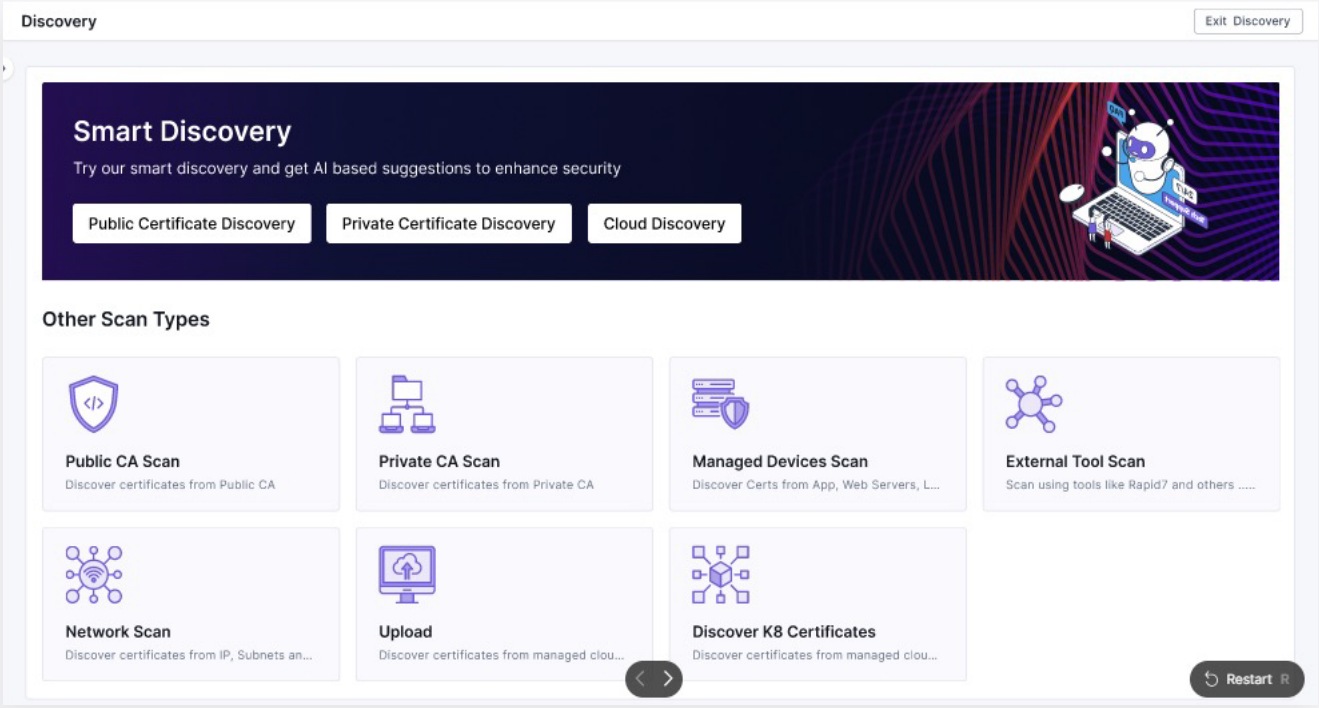
This is a non-authenticated scan that allows you to discover certificates from IP, subnets, and URLs. The scan helps identify certificates residing on various IP-Port combinations within the network along with the devices or applications associated with each certificate. Additionally, the scan can discover even the OS associated with the IPs provided. This scan is customizable, allowing total pause-resume control for optimal network utilization.

7. Certificate Upload

AVX ONE CLM also supports direct certificate uploads. You can simply bulk upload your certificates as necessary.

8. Kubernetes Certificate Scan

This scan allows you to discover certificates easily from your Kubernetes clusters and environments by deploying AVX ONE CLM for Kubernetes.



To ensure that certificate discovery does not impact network performance and operations, AVX ONE CLM Smart Discovery provides two unique features:

- **Scanning Intensity Control:** Allows you to manage the intensity of the discovery scan, so you run a full discovery scan at a stretch without overwhelming your network. By adjusting the scanning intensity, you can alleviate network pressure and maintain smooth performance.

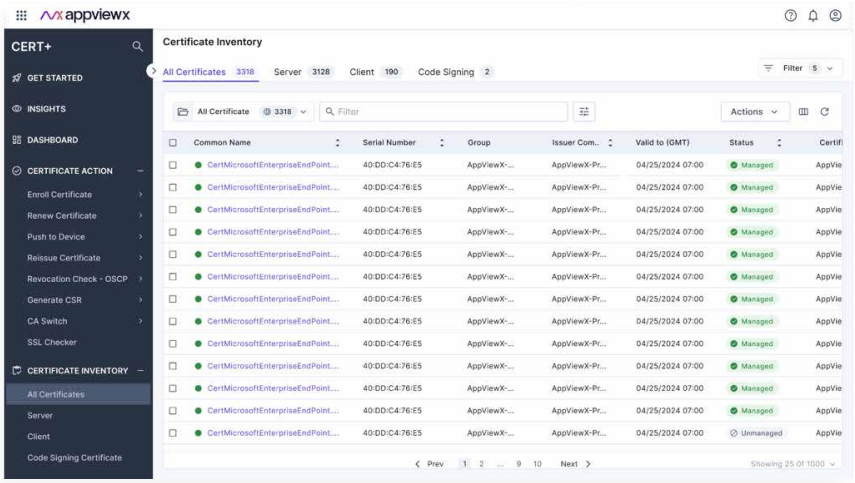
- **Sequential Batching:** Allows you to run discovery scans in smaller, manageable batches to ensure optimal performance.

To further enable you with greater control over certificate discovery, AVX ONE CLM Smart Discovery provides **Discovery Rules**. These settings allow you to define what certificates can be discovered, giving you better control and saving a lot of time.

For example, PKI Administrators can select any of the following parameters for a filtered and fast certificate discovery:

- Exclude/include expired certificates
- Exclude/include certain templates
- Exclude/include various certificate parameters

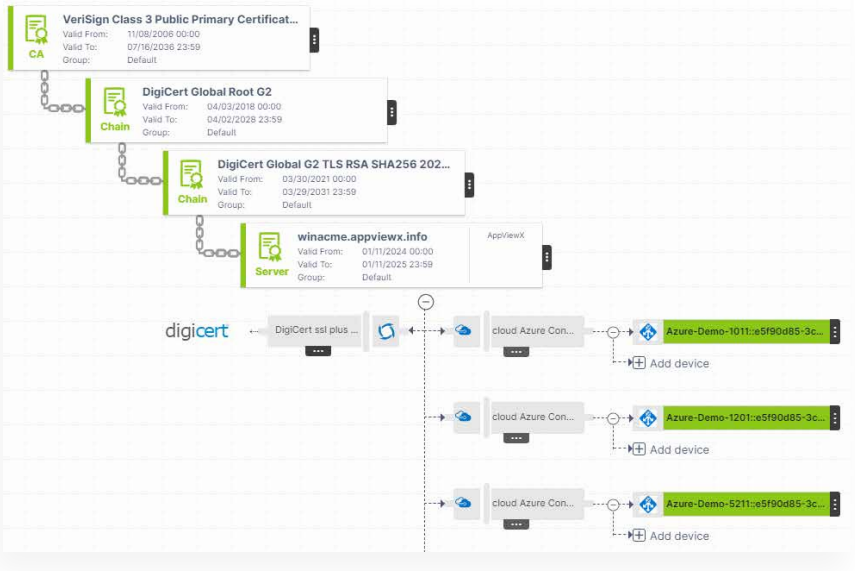
AVX ONE CLM – Certificate Inventory, Complete Visibility, and Chain of Trust View



After discovering the certificates, AVX ONE CLM helps build centralized visibility by populating all discovered certificates across both private and public CAs in a single central inventory. This inventory serves as **a single source of truth for all certificates** after discovery, providing essential certificate information, such as the location, owner, chain of trust, associated applications, crypto standards, and expiry dates.

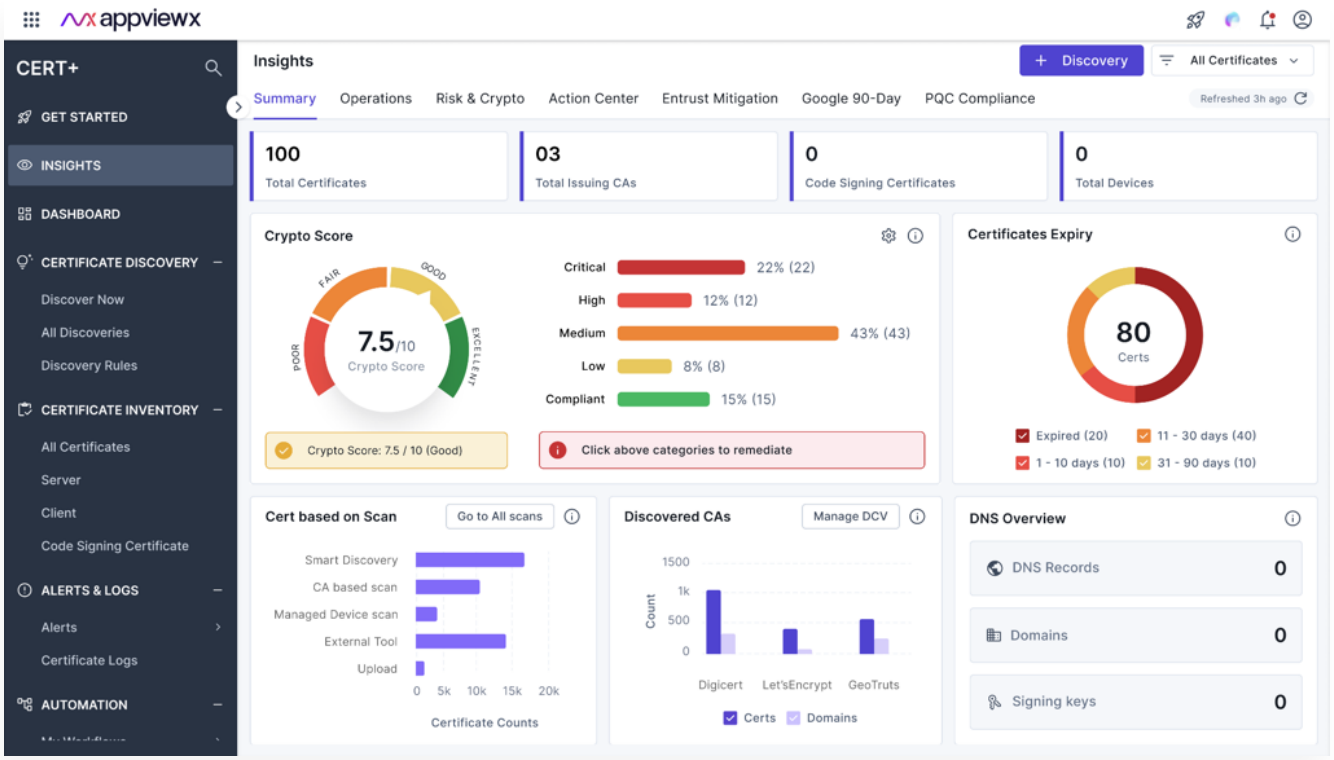
You can customize the inventory to display over fifty different columns of certificate-related details and metadata based on your need for granular visibility. You can also segment certificates into groups, such as server, client, code signing, and device certificates to simplify renewals and revocations.

In the certificate inventory, AVX ONE CLM also offers **a holistic view of the Chain of Trust**. Clicking on a certificate will take you to this unique view that offers actionable visualization of the complete certificate chain of trust as well as where the certificate is deployed. You can even renew, revoke, and provision certificates to new endpoints in this view.



AVX ONE CLM – Insights

AVX ONE CLM also offers Insights, a suite of **actionable graphical dashboards** designed to help you analyze and understand your organization's crypto health, enabling data-driven decision-making. These powerful dashboards provide an overall Crypto Score, a Google 90-day Score to assist with 90-day TLS certificate preparation, and a PQC Score to gauge post-quantum cryptography readiness. You can simply click on any of the widgets within the Insights dashboard to drill down and take appropriate action.



AVX ONE CLM – Alerting

To ensure timely renewals, approvals, or escalations, AVX ONE CLM offers a detailed and persistent expiry notification mechanism, catering to different use cases. You can utilize these built-in, customizable alerts to notify PKI Administrators about connectivity between AppViewX and a CA and certificate owners about upcoming certificate expirations or any failed CLM actions like renewal/revocation. Customization enables you to define the frequency and dates/time for alerts and the email subject, body, and the address of the expiry notification. These alerts can be delivered via emails for manual actions or via simple network management protocol (SNMP) traps for automation and integration with ITSM and SIEM solutions.

AVX ONE CLM - Reporting

AVX ONE CLM features intelligent reporting capabilities to help keep up with industry standards and ensure continuous compliance. As soon as the discovery is complete and certificates are added to the inventory, **pre-defined and categorized** reports are generated providing a high-level view of expiring certificates, compliance, and more.

You can **build your own reports (BYOR)** based on any custom attribute or certificate metadata, such as reports for specific teams or applications or groups. Custom reports help PKI administrators or certificate owners systematically and efficiently track their certificates. You can also create multiple reports and tag them to a single dashboard for a holistic view of all reports in one place.

Centralized inventory, contextual dashboards, and intelligent reporting helps monitor certificates for expiry and vulnerabilities and remediate issues proactively, mitigating the risk of outages, security breaches, and compliance violations.

Flexible Consumption Models

AVX ONE CLM can either be consumed as a service or deployed in the enterprise network. Irrespective of how the solution is consumed, the features and benefits remain the same and are available from one centralized console.

SaaS – Operated by AppViewX

Available as a service, AVX ONE CLM is fully managed and updated by AppViewX. Customers can directly set up an account, instantly start using it and realizing value to solve certificate management challenges.

On-Prem and Hosted Deployment

The CLM automation capabilities of AVX ONE CLM can also be deployed within a customer's environment in hypervisor-based VMs, private clouds, or public clouds using AWS, GCP, Microsoft Azure, and others.

Achieve Visibility, Automation, and Control of Your Digital Certificates with AVX ONE CLM

It is impossible to manage and protect what you can't see. Achieve greater visibility of digital certificates across your entire IT infrastructure with AVX ONE CLM Smart Discovery and ensure all your certificates are valid and compliant at all times. Automate certificate lifecycle management end-to-end, from issuance to provisioning and revocation, to minimize human error and boost operational efficiency. Enforce PKI policies and governance to maintain control and protect your applications, workloads, services, devices, and machines from certificate-related outages and security risks.

Security simplified with AppViewX

AppViewX is trusted by the world's leading global organizations to ensure application availability, security and compliance with centralized visibility and control of public key infrastructure (PKI) and application delivery services across complex hybrid multi-cloud environments. The AppViewX Platform enables self-service automation and orchestration for NetOps, DevOps, SecOps and application teams to quickly and easily translate business requirements into automation workflows that improve agility, harden security, enforce compliance, eliminate errors, and reduce cost.

Make visibility the cornerstone of your protection mechanism.

https://www.appviewx.com/live-demo/

AppViewX Inc.,

City Hall, 222 Broadway
New York, NY 10038

info@appviewx.com
www.appviewx.com

+1 (206) 207-7541
+1 (212) 951 1146