



# AVX ONE Certificate Lifecycle Management (CLM): Seamless CA Switch Capability



## Entrust Distrust Incident Overview

Google announced Entrust SSL/TLS Certificates will be distrusted in Chrome browsers starting November 1, 2024. The decision by Google stems from Entrust's ongoing compliance issues and lack of progress in addressing reported incidents over the past 6 years. Newly issued Entrust Certificates after November 1, 2024 will be treated as invalid and untrusted, triggering security and privacy warnings that can lead to revenue loss and reputational damage. Although Certificates issued by Entrust before October 31, 2024 will remain trusted until their expiry date, Google advises replacing Entrust certificates before the deadline to avoid disruptions.

### Call to Action: *Crypto-Agility*

By implementing crypto-agility, including CA-agility, organizations can swiftly address CA distrust incidents and maintain resilience against evolving threats.

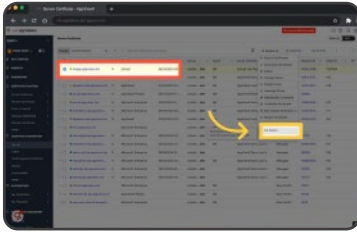
### Why Crypto-Agility is Essential

- Streamline CA/ Certificate Migrations and Reduce Risk
- Mitigate Outages and Disruptions
- Reduce Human Error and Boost Productivity

## Simplify CA Migrations and Enable Crypto-Agility with AVX ONE CLM

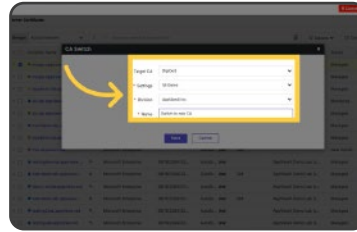
The AppViewX AVX ONE Certificate Lifecycle Management and PKI platform enables crypto-agility to make the CA and certificate migration process easy and efficient. Delivered as a SaaS solution, users can quickly employ the AVX ONE CLM "CA Switch" feature to switch CAs and migrate certificates in 5 simple steps.

### Step 1:



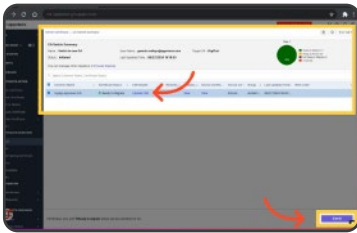
From your AppViewX AVX ONE CLM Certificate Inventory, select the discovered certificates issued by Entrust (or other distrusted CAs). Then select "CA Switch" from the Actions menu.

### Step 2:



Select a new CA of your choice

### Step 3:



Validate the certificate information and click submit

### Step 4:



Automate the replacement of Entrust certificates. AppViewX AVX ONE CLM handles everything from generating the CSR to requesting the certificates from a new CA and installing them on your servers and endpoints.



### Step 5:

Migration complete! The new certificates issued by a new CA will appear in your AppViewX AVX ONE CLM Certificate Inventory.

## Why Choose AppViewX AVX ONE CLM?

### Complete Visibility

- **Most Comprehensive Discovery, Inventory and Insights:** The AppViewX AVX ONE CLM Smart Discovery feature finds more certificates and mitigates untrusted certificate blind spots. Use the detect and response dashboards featuring Crypto Scoring and Google 90-Day readiness to reduce security weaknesses.
- **Single Pane of Glass:** Visibility and management for all certificates, issued from public or private CAs, across all of your endpoints.

### Continuous Control

- **Zero-Touch Policies:** Use policies to enforce the use of approved CAs, crypto-standards, validity periods and more to eliminate rogue and non-compliant certificates.
- **Granular Role-Based Access Control (RBAC):** Securely delegate tasks like CA migrations and other crypto policies across teams with granular RBAC.
- **Audit Trails:** User, certificate and key-related audit trails help track activities and simplify audits.
- **Superior Platform:** Critical core platform functionality including RBAC, approval workflows, intelligent notifications, reporting and a robust policy engine that cannot be built in house.

### Closed Loop Automation

- **Automate Your Way:** Automation that is out-of-the-box or custom, simple to advanced, zero touch or one click to fit your unique requirements.
- **Closed-Loop:** Unlike any other vendor, truly automate to the last mile. Robust integrations enable endpoint binding to ensure newly issued certificates are fully configured for use.
- **CA-Agnostic:** Automate certificate lifecycles across multiple public and/or private CAs, allowing you to maintain a multi-CA vendor strategy and CA-agility as best practice.
- **Crypto-Agility:** Fast, automated CA and certificate migration and replacement helps to ensure agility in the face of future disruptions like - 90-day TLS, Post-Quantum Cryptography or CA distrust incidents.
- **Workflow-First:** Powerful automation workflows (not just work-steps) that are integrated, customizable and support any number of CLM actions.
- **Agentless:** Benefit from automation that is powered by simple API connections instead of complex agents.
- **Self-Service:** Delegate CA migration tasks with oversight and across teams (DevOps, Cloud/Platform, NetOps, etc.) and customize self-service pages for ultimate ease of use.

AppViewX Inc.,

City Hall, 222 Broadway  
New York, NY 10038

info@appviewx.com  
www.appviewx.com

+1 (206) 207-7541  
+44 (0) 203-514-2226

©AppViewX, Inc. All Rights Reserved.