appviewx

# Release Notes

**Version: 2025.0.0.0 (On-Prem)**

# Copyright AppViewX, Inc.



### Contact Information


AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

# Contents

# Preface

## Revision History

| Revision | Description | Date |
|---|---|---|
| 1.0 | AppViewX v2025.0.0.0 (On-prem) Release Notes | November 2025 |

## About this Guide

This release notes describe new features, enhancements, known and fixed issues, and known limitations in the software.

## Intended Audience

- Customers onboarding AppViewX v2025.0.0.0.

## Third-Party Software Acknowledgments

This section serves as a placeholder to document the third-party components referenced in this guide, along with their associated trademark information.

## Text Conventions

The following text conventions are used in this document:

| Convention | Description |
|---|---|
| **boldface** | Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary. |
| *italic* | Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values. |
| `codeblock` | Indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter. |

# Chapter 1: New Features

This section describes the new features in this release.

## ADC+

- **Share Multiple Dashboards To User Groups**

  AppViewX provides an option to share multiple dashboards to usergroups from the dashboards inventory.

- **Added Virtual Address to Dashboards / Application Widgets**

  Supports provided to monitor virtual-address from the application widget.

- The user can view the total object count of each group in the application widget.
- Added support to view the unused VIP/WideIP report in the default ADC dashboard, allowing administrators to identify unused entries based on their connection count.

## CERT+

- **Alerts about Failed Certificate Push**

  The certificate push failure alert is added as an event type under the configure alerts menu which allows configuring the alert types for selected device vendors across ADC, Server, MDM, Cloud, WAF and Firewall devices and certificate type with a custom alert message to be sent as part of the alert to the configured email address.

- **CA High Availability in SNOW CLM Settings**

  The Microsoft Enterprise CA setting addition is enhanced to update the deployment type to support adding the CA setting as a High Availability pair along with the existing Standalone type support. When the High Availability type is selected, the primary and secondary CAs can be fetched, configured and updated as per the respective CA configuration.

- **Retry/Retrigger Logic for Auto-Regenerate**

  When the certificate auto regenerate request fails for a given certificate, based on the DB configurations, the failed requests will be retriggered automatically in successive intervals instead of manual intervention.

- **CA Integrations**

AppViewX introduces a centralized platform for managing Domain Control Validation (DCV) across multiple Certificate Authorities (CAs). This enhancement delivers a unified framework for onboarding and managing domains, performing validations through both HTTP and DNS methods, and supporting manual (HTTP & DNS) and automated (DNS) renewal workflows. The repetitive validation processes are automated, significantly reducing manual effort and operational workload. It ensures domains remain continuously validated and trusted, supporting uninterrupted certificate issuance. It also provides a full validity of the DCV activities to maintain adherence to CA policies and internal compliance standards.

**Key Capabilities**:

- Unified Domain Inventory - Maintain a consolidated inventory of all domains managed across onboarded CAs, including DigiCert, Sectigo, GlobalSign MSSL, and GlobalSign Atlas.
- Domain Lifecycle Control - Enable administrators to add new domains, remove unused ones, and manage domain–CA trust relationships efficiently.
- New Domain Trust Management - Simplify domain onboarding and trust establishment for DCV without repetitive manual configurations.

**Visibility and Tracking**:

- DCV Status Monitoring - Monitor the real-time validation state of each domain, with status such as Pending, Active , In Progress, Expired, or Failed.
- Validation History - Maintain a detailed record of validation requests, revalidations, and renewal activities for each domain.
- Audit Trails - Capture all user and system actions for governance, troubleshooting, and compliance auditing.

**Flexible Validation Methods**:

- Multi-Method DCV Support - Support all major CA validation methods, including:
  - DNS TXT Records
  - DNS CNAME Records
  - HTTP File-Based Validation.
- DNS Vendor Integration - Integrate with leading DNS providers to automate DNS record creation and propagation checks, streamlining validation operations.

**Renewal Management**:

- Manual and Automated Renewal - Support both user-initiated (HTTP & DNS) and automated (DNS) revalidation workflows.
- Scheduled Renewals - Allow administrators to schedule domain renewals in advance of expiry, preventing service disruptions.
- Auto-Renewal Before Expiry - Automatically initiate renewal workflows before DCV validity expires to ensure ongoing compliance with CA requirements.

**Notifications and Alerts**:

- Proactive Alerts - Generate timely notifications for upcoming validations, expiry warnings, failed validations, and pending approvals.
- Multi-Channel Notifications - Deliver alerts through email and in-platform notifications, keeping administrators informed and reducing operational risk.

- **CRL validation - Improvisation**

  Previously, disabling the **CRL validation job** would turn off validation for all **Certificate Authorities (CAs)**. To improve flexibility, the CRL validation job has now been divided into two categories: **Public CRL Jobs** for certificates from centralized or public trust stores, and **Private CRL Jobs** for customer-added or tenant-specific certificates.

  This separation allows users to disable CRL validation for specific CAs that may be causing issues or failing validation. A **database script** is available to exclude problematic CAs from validation through a SWAT update. Additionally, an **exclusion list** can be maintained in the database to prevent customer-specific impact by defining which CAs are excluded from validation. Both public and private CRL jobs are **disabled by default** and, once enabled, run automatically **every 24 hours**.

- **Device Onboarding Group**
  - The Device Onboarding Group feature allows users to logically group devices that share similar onboarding parameters and automate configuration using defined rules. Each group can have rules that determine how devices are automatically assigned - based on criteria such as IP range, hostname pattern, operating system, or discovery source.
  - Within each Device Onboarding Group, administrators can predefine shared onboarding attributes like credential source (manual, PAM, or vault), certificate/key storage path, onboarding policy, and elevation method. This ensures consistent, policy-driven onboarding across environments.
  - By combining rule-based classification with reusable templates, the Device Onboarding Group feature reduces manual setup, speeds up large-scale onboarding, and enforces standardized onboarding practices across discovered devices.
- **Enhanced Device Onboarding in the Network Scan and Configuration Module**

  - The **Network Scan and Configuration** module now supports both automatic and manual device onboarding.
  - Users can select an **Onboarding Group** during configuration to automatically onboard discovered devices based on predefined rules, credentials, and configurations. They can also manually assign discovered devices to an Onboarding Group after the scan completes, providing more control and flexibility for environments that need validation or approval.
  - This enhancement ensures consistent policy enforcement while allowing users to choose between automated and supervised onboarding, improving both efficiency and governance.
- **Enhance Devices Tab in Discovery Status. Discovery**

  The Devices tab under Discovery Status now provides enhanced visibility into the auto-onboarding status of discovered devices. Users can view which devices were successfully onboarded automatically and take manual onboarding actions for those that were not. The grid enables users to select devices and initiate onboarding directly from the interface.

  > **Note:** Manual and auto-onboarding actions are supported only for vendors where a Device Onboarding Policy is defined.

- **Automated Device Onboarding via JSON in Policy Engine**

  This enhancement introduces JSON-based onboarding for multiple device types, enabling policy-driven automation and standardized configuration management.

  - **Master Template** - A master JSON template is delivered with the product during installation or upgrade. The template defines the JSON structures used to dynamically render UI components for policy creation.
  - **Policy Creation and Reuse** - Privileged users can create onboarding policies based on the master template. These policies can be reused across device groups to ensure consistent onboarding configurations.
  - **Automation and Integration** - Policies can be referenced in onboarding rules and applied to devices discovered during network scans. Matching devices are automatically onboarded based on predefined policy rules.

    > **Note:** Currently onboarding via JSON is supported only for Linux Server, Microsoft Server (MSServer, Exchange Service, Windows GW), IIS, MS SQL, F5 (ADC), Apache (Linux and Windows), Tomcat (Linux and Windows),and Nginx (Server).

- A new internal API has been introduced to validate device policy associations before performing delete or update operations.

- This release introduces a new internal API that validates device policy associations before performing delete or update operations. The API helps ensure that policies are not removed or modified while still linked to device groups or active devices.
- **Device Inventory ADC, Server changes**

  This enhancement adds two new columns to the ADC and Server Device Inventory tables to provide better visibility into device grouping and certificate details.

  - Onboarding Group - Displays the onboarding group assigned to each device. Groups are defined and managed through the Onboarding Groups page, where rules determine device assignments.
  - Summary - Provides a hyperlink that opens a detailed view of the certificates associated with the device.
- **Device Bulk Update from Policy Engine for the Associated Devices**

  When a device policy is updated, the changes are automatically applied to associated devices while respecting any local device-level updates as the preferred values. This support is available only for Linux Server, Microsoft Server (MSServer, Exchange Service, Windows GW), IIS, MS SQL, F5, Apache (Linux and Windows), Tomcat (Linux and Windows), and Nginx (Server).
- **Optimized Device Policy Updates**

  When an existing device policy is updated, the associated devices automatically receive only the **delta changes**, minimizing configuration overhead. The system also **preserves any local device-level updates** as the preferred values, ensuring efficiency while maintaining device-specific customizations.
- **Define Device Onboarding Policy with Configurable Stages**

  This feature introduces a stepper-based workflow for defining Device Onboarding Policies, enabling administrators to create consistent and governed onboarding processes. Administrators can define Device Onboarding Policies using an intuitive, guided stepper interface. The workflow supports:
  - Vendor Templates - Standardized onboarding configurations based on vendor-specific templates.
  - Pre/Post Onboarding Scripts - Automate preparatory and post-onboarding tasks.
  - Approvals - Incorporate approval steps to enforce governance and compliance.
  - Scheduling - Schedule onboarding operations for specific times or maintenance windows.
  - Notifications - Receive alerts on policy actions, approvals, and onboarding status.
- **Display Flag for Devices Updated from Policy Engine**

  This feature introduces a visible notification flag in Policy Engine to indicate when a device update has been triggered by the Policy Engine. Improves visibility and ensures administrators are aware of devices requiring a configuration fetch to apply the latest policy updates. The flag remains visible until one of the following actions completes successfully:

- Config fetch
- Manual update
- Nightly config fetch.

> **Note:** This behavior applies to all supported device types integrated with Policy Engine.

- **Enhance Certificate Groups with Policy and Auto-Reenrollment Options**

  This feature introduces new configuration options in Certificate Group Settings to define and automate certificate lifecycle management at the group level. Administrators can now configure Enrollment and Re-enrollment Policies directly within each certificate group. Added support for Auto-Reenrollment with a configurable expiry buffer to automatically renew certificates before expiration.

- **Device Summary Tab and Top Bar in Device-Specific View**

  Users can now access a device-level Summary Tab and Top Bar directly from the Device Inventory by clicking View, offering a consolidated, high-level overview of each device's key information. This enhancement improves visibility and efficiency by displaying device health, certificate posture, PQC readiness, and other critical attributes at a glance. It also unifies certificate status, risk indicators, PQC compliance, and device metadata in a single view, eliminating the need to navigate across multiple pages to gather device insights.

- **Integrate Certificate Enrollment with Policy Engine Workflow Engine**

  Users can now initiate certificate enrollment requests through the Policy Engine workflow engine, ensuring policy-driven, controlled, and auditable operations.Enrollment requests follow predefined policies, approval workflows, and validation checks configured by administrators. Provides a consistent and governed certificate lifecycle across the organization. Supports full auditability of enrollment actions for compliance and reporting purposes.

- **Update Certificate Validity for Next Renewal/Regeneration**

  Administrators can now update the validity period of a certificate prior to its next renewal or regeneration, enabling alignment with business requirements without re-enrollment or re-issuance. This provides administrators with flexibility to adjust certificate lifecycles on demand, reducing manual re-enrollment effort and ensuring certificates meet evolving business policies.

- **Workflow Engine Selection for Certificate Actions**

  Administrators can now select whether **Workflow Engine** or **Policy Engine** manages specific certificate actions, enabling a **phased transition** from legacy Workflow-based automation to the new Policy Engine framework.

- **Added New Reports in Insights**

  The **Operations** tab in **Insights** now includes additional **certificate lifecycle reports**, giving administrators greater visibility into automation coverage, renewal timelines, and push configurations.
  - **Auto Push Configured**: Displays the total number of certificates with auto-push enabled, along with a bar chart comparing Automated vs Non-Automated certificates.
  - **Renew Validity Report**: Presents a pie chart grouping certificates by validity remaining after renewal, categorized as **0–30 days**, **31–90 days**, **91–200 days**, **200–397 days**, and **397+ days**.

  These reports help administrators track renewal distribution and ensure compliance with CAB standards for reduced certificate validity periods.

- **Package a Default Re-Enrollment Policy**

  AppViewX now provides a system-generated Default Re-Enrollment Policy to ensure seamless certificate re-enrollment after migration to the new Policy Center framework.
  - Default Policy Availability - Automatically packaged and available immediately after upgrade.
  - Default Re-Enrolment Settings:
    - Certificate Validity: 200 days
    - Key Type: RSA
    - Key Size: 2048
    - Key/CSR Generation Location: AppViewX
  - Inherited Fields from Existing Certificates:
    - Issuing CA vendor, account, and Division (for Digicert)
    - Certificate type (Server, Client, and so on.)
    - Subject DN and SAN values.

    All certificates configured for re-enrolment post-upgrade are automatically mapped to the Default Re-Enrolment Policy.

    **Note:** Administrators cannot delete this policy in this release.

- **Introduced Re-Enroll Action for Certificates**

  A new **Re-Enroll** certificate action has been introduced to securely renew certificates with a new key while utilizing **CA renewal APIs**. This action always generates a fresh key and CSR, ensuring enhanced security without incurring additional billing or creating new certificate orders. It serves as a secure and consistent alternative to the existing **Renew** and **Regenerate** actions, aligning seamlessly with CA renewal workflows.

- **Enabled Event-Based Notifications in Policy Engine**

Business events are now emitted from **Policy Engine** to support **event-based notifications**, allowing real-time alerts and integrations based on specific policy actions or changes. This enhancement improves **visibility**, **automation**, and **response efficiency** across policy-driven workflows.

- **Improved Traceability for Certificate Enrollment and Actions**

  This enhancement improves traceability of certificate enrollment and related actions by refining how the **Policy Execution ID** is managed. The Policy Execution ID is now passed as a **payload parameter** instead of a certificate attribute during enrollment and is also stored in the **Certificate collection** for tracking and audit purposes. This update applies to all key **certificate lifecycle APIs**, ensuring consistent tracking of the **request source** across operations.

- **Master JSON Template for Certificate Authority Configuration**

  This enhancement introduces the ability to create a **master JSON template** in **Policy Engine** for configuring **Certificate Authorities (CAs)**. Administrators can define a **reusable template** to standardize configurations across multiple CA products and certificate types, including **vendor-specific fields** to meet diverse CA requirements. The master template can be leveraged during **Enrollment** and **Re-enrollment** processes, reducing repetitive manual setup and ensuring consistency.

  **Supported CAs:** Digicert, GlobalSign SSL, GlobalSign MSSL, Globalsign Atlas, Trustwave, Incommon, Sectigo, Google, Entrust MPKI, Ejbca, Digicert One, Let's Encrypt, CSC Global, AppViewX CA, FutureX, Hydrant ID, SwissSign, Amazon ACM, Amazon PCA, Microsoft Enterprise, Microsoft Standalone, AppViewX PKIaaS - GCP, AppViewX PKIaaS - Native CA, Godaddy CA, and Nexus.

- **Enhanced AppViewX ACME Client Download Options**

  AppViewX now allows users to **download the AppViewX ACME Client** from multiple locations, improving accessibility and usability for both administrators and end-users. The client can be downloaded from the **ACME Configuration page**, **Insights page**, and the **Agent and Download** section.

  - **Common Download Option** - A single, generic ACME client package compatible with all configurations is available through the **Download AppViewX ACME Client** button. Users can choose their **operating system (Windows or Linux)** before downloading. This option is ideal for administrators to distribute the client across the organization.
  - **Targeted Download Option** - Each ACME configuration entry includes a dedicated download option that provides a **pre-configured ACME client** mapped to the selected setting. Users can select their operating system and preview mapped agent details before downloading, ensuring quick setup with minimal configuration.

  AppViewX has also introduced AEP Agent ACL Enhancements for all the protocol Endpoints (EST, ACME, SCEP, MSIntune, CMP) in conjunction with this feature. AEP agents are now displayed based on the certificate group ACLs assigned to the logged-in user. If a user does not have access to a specific certificate group associated with an agent, that agent will be hidden from the user's AEP Agent Inventory. Consequently, users without the required group permissions will no longer be able to view or access agents linked to restricted certificate groups.

- **AppViewX ACME Client Enhancement for Automated Certificate Binding**

  The AppViewX ACME Client now supports automatic certificate binding to applications such as IIS, NGINX, Tomcat, and Apache immediately after certificate enrollment.

  - **End-to-end automation** - Automatically binds and updates certificates during enrollment and renewal.
  - **Application coverage** - Supports IIS, NGINX, Tomcat, and Apache.
  - **Logging and auditing** - Captures detailed logs of binding actions with automatic log rotation.
  - **Fail-safe operations** - Certificates remain intact even if binding fails, with detailed error logs recorded.
  - **Optimized performance** - Efficient binding minimizes impact on application availability.
  - **Backward compatibility** - Fully supports existing enrollment-only workflows.
  - **Flexible configuration** - Uses a JSON-based config file for easy setup and customization.
  - **Renewal enhancements** - Adds renewal hooks and a scheduler for automated lifecycle management.
  - **Certificate management** - Automatically backs up replaced certificates and keys as `.bak` files.
  - **Challenge handling** - Uses polling for challenge propagation to support the Enterprise Secure ACME AVX Plugin.
  - **Client behavior update** - Enables DNS propagation by default, removing the need for the `--dns.propagation-disable-ans` flag.

- **Update Certificate Validity for Next Renewal/Regeneration**

  This enhancement introduces the ability to modify the validity period of a certificate during its next renewal or regeneration. Users can define a new validity duration that overrides the default CA or template settings, offering flexibility to align with organizational security policies or short-lived certificate strategies.

  The selected validity period is automatically applied during the next renewal or key regeneration process, ensuring consistency across automation workflows and reducing manual intervention.

  > **Note:** The updated validity configuration applies only to future renewals or regenerations and does not alter the validity of the currently active certificate.

 

- A new Device Summary tab and top bar have been introduced in the device-specific view to provide a consolidated snapshot of device health and certificate status. The summary offers quick visibility into key metrics such as the total number of certificates associated with the device, expiring certificates, compliance status, and recent push or renewal activities.
- The new **Re-Enroll** action enables secure, policy-driven certificate re-enrollment by always generating a new key, ensuring better cryptographic hygiene and compliance with modern security standards. In this release, users can re-enroll certificates by generating a new key within AppViewX or by uploading a custom CSR, with future support planned for endpoint and HSM-based key generation. Governed by defined policies for approvals, notifications, and post-enrollment actions, this enhancement streamlines lifecycle management, reduces manual effort, enforces strong key rotation, and ensures end-to-end security during certificate renewal operations.
- **Package a Default Re-Enrolment Policy**

  A default Re-Enrollment Policy is now packaged with the product to accelerate setup and standardize certificate renewal operations. This built-in policy provides preconfigured settings for key generation, approval workflow, notifications, and post-enrollment actions, enabling immediate use without additional configuration. The default policy enforces new key generation during re-enrollment to align with security best practices and prevent key reuse.

  Administrators can clone or customize the default policy to align with organizational processes, allowing flexibility while maintaining a secure baseline for all re-enrollment activities.
- **Workflow Engine Selection for Certificate Actions**

  A new Settings Page has been introduced that allows administrators to configure the preferred workflow engine for certificate-related actions such as enrollment, re-enrollment and ACME. This enhancement provides flexibility for organizations to choose between AppViewX visual workflow engine or AppViewX Policy Engine workflow systems to manage approval chains, notifications, and automation sequences.

  The settings page offers a centralized configuration view, displaying all supported certificate actions and their assigned workflow engines. Administrators can modify these selections based on internal process requirements, ensuring consistency and compliance across the certificate lifecycle.
- **Enhance Certificate Groups with Policy and Auto-Reenrollment Options**

  Certificate Groups now support Policy Engine integration and auto-reenrollment configuration, enabling smarter, automated certificate lifecycle management. Administrators can associate specific enrollment or reenrollment policies with a certificate group to ensure consistent handling of approvals, key generation, and notifications across all group certificates. The new Auto-Reenrollment option allows certificates to renew automatically based on policy-defined triggers, minimizing manual effort and reducing the risk of certificate expiry.

 

- **Enhanced Operational Insights for Certificate Automation**

  Two new analytical reports have been added under **Insights** > **Operations** to enhance visibility into certificate automation and short-lived certificate readiness.
  - The Auto-Push Adoption Report shows a breakdown of endpoints with Auto-Push enabled vs. disabled, helping administrators assess automation coverage and identify areas requiring manual action.
  - The Renew Validity Report provides detailed visibility into certificate validity periods for upcoming renewals, enabling teams to monitor the adoption of shorter validity certificates and evaluate readiness for short-lived certificate management.

  Together, these reports deliver data-driven insights that help organizations measure automation maturity and optimize their certificate lifecycle strategies.
- **Policy-Driven Certificate Enrollment Integration**

  Certificate Enrollment is now integrated with the Policy Engine Workflow, enabling fully automated and policy-driven control over the enrollment process. Enrollment requests now follow configured workflows that define approvals, and notifications, ensuring consistent handling based on organizational policies such as CA selection, and key generation. This integration provides administrators with enhanced visibility, auditability, and flexibility in managing certificate enrollments across teams and business units.
- Introduced JWT token–based authentication secured with an Azure certificate for service-to-service communication. The system now uses certificate-based signing and validation of tokens, improving security and eliminating reliance on static client secrets.

## KUBE+

- In OpenShift, infrastructure certificate discovery can now be disabled based on a flag set during the Helm installation command, allowing administrators to control discovery behavior according to deployment requirements.
- Reduced the Healthy-to-Unhealthy flip time for clusters to ensure quicker and more accurate status updates in the KUBE+ Cluster Inventory.
- Improved the Connect Cluster installation command generation to provide better compatibility and usability for OpenShift clusters.

## Quantum Trust Hub

- **Post Quantum Cryptography (PQC) Readiness**

  AppViewX now enables organizations to evaluate the PQC readiness of their existing cryptographic landscape to identify quantum vulnerabilities, prioritize remediation efforts, and drive a seamless transition to a quantum-safe state. This is a major step towards ensuring cryptographic resilience in the era of quantum computing and the threats it introduces to existing cryptographic systems.

The first step to ensuring quantum resilience is crypto awareness; lack of visibility increases the risk of exposure to quantum disruption. AppViewX introduces the Quantum Trust Hub, a centralized console that offers end-to-end visibility into every cryptographic asset across your ecosystem, giving you a complete understanding of how and where cryptography is implemented, and how each component aligns with post-quantum security standards. The Quantum Trust Hub is equipped with:

- Dashboards that offer visibility into an organization’s cryptographic usage, the vulnerabilities and their corresponding severity levels, and the organization's overall progress towards PQC migration.
- Inventories that list all the cryptographic assets scanned for PQC-readiness and their quantum-safety status.
- Policies to define, manage, and enforce custom PQC policies to align with an organization’s individual security goals.

Key features of the Quantum Trust Hub:

- Discover, classify, and manage cryptographic assets via a comprehensive set of scans
- Review cryptographic analysis reports for quantum-related vulnerabilities.
- Measure PQC-readiness for post-quantum adoption.
- Review and prioritize recommendations for quantum-safe transition.

With v2025.0.0.0, Quantum Trust Hub has been introduced as a module within the AVX ONE CLM platform. Current customers can start with a free PQC readiness scan to assess their cryptographic readiness. The full-featured module is available with an additional license.

Contact us to talk to an AppViewX representative/request a demo on how you can start using the Quantum Trust Hub to kickstart your post-quantum readiness journey.

To refer to the documentation, see the Quantum Trust Hub Guide.

## SSH+

- **API for Downloading SSH User/Host Key(s)**

  Added API support for downloading SSH user and host keys, as well as certificates.

- **Restore & Rollback Keys in Windows**

  Added support for restore and rollback actions for keys on Windows hosts.

- **Dashboard - Compliance Trend Widget Changes**

 

Added two new widgets to the SSH Dashboard to enhance visibility: one for tracking the Compliance Trend and another for monitoring the Compliance Posture, providing better insight into SSH compliance status.

- **Delete key instance support for Missing Keys**

  Enhanced the delete key action to skip keys that are missing on hosts.

- **Recursive Scanning for User Directory Support for Windows and Linux**

  Added recursive and intensive scanning support for the default scan in host discovery.

- **Download SSH Key from Inventories**

  Added support in the SSH user/host key inventory to download keys and certificates through actions.

# Chapter 2: Enhancements

This section describes the enhancements in this release.

## SSH+

- **SSH Risk improvements**

  Improved SSH key risk categorization, including refinement of orphan risks into two categories: Misplaced and Rogue.

- **Display Compliance Details on Hover in SSH Keys Inventory**

  Added display of last compliance status update time and non-compliant parameter reason on hover in the Compliance Status column.

- **SSH - Export key Instance Changes**

  Updated export key instance behavior for partially managed hosts to prevent updating the successful scan time and marking keys as missing.

## CERT+

- **Enhanced Reporting for Short-Lived Certificates**

  AppViewX introduces Certificate Validation Reports for short-lived certificates, offering detailed insights into key lifecycle metrics. The former Google 90-Day Dashboard is now renamed Short-Lived Certificates, retaining all existing features while adding advanced reporting. The dashboard covers public certificates and includes data on inventory, renewals, re-enrollments, push status, expiry, and automation, providing complete visibility to identify discrepancies, automation gaps, and process inefficiencies in short-lived certificate management.

- **ACME Server Configuration Enhancements**

  AppViewX has introduced improvements that simplify and align ACME configuration with domain validation workflows, DNS challenge handling, and policy integrations to support Short Lived Certificates.

  - **Allowed Domain Names Migration:**
    - The Allowed Domain Names field has been moved from General Settings to CA Account Settings.
    - The field now auto-populates based on the selected CA and its configured DCV method.
    - If DCV is applicable for the selected CA, domain selection will be enforced accordingly.
    - If DCV is not applicable, a text input field will be available to enter multiple domain names manually.
  - **DNS Challenge Enhancements:**

 

    - When Challenge Type = DNS, two new fields have been added to select the DNS Vendor and corresponding Settings.
    - The Challenge Validation Type field has the following new values when Challenge Type is DNS - Automated DNS Validation, Automated DNS Validation (via AppViewX), and Enterprise secure challenge.
    - If a DNS Vendor integration already exists, settings will auto-populate automatically.
    - If not, a direct link to the Integration Hub is provided to configure a new vendor integration.
    - The following DNS vendors are supported in On-Prem and Saas - Akamai, Cloudflare, CSC, GoDaddy, Infoblox, Microsoft DNS (only On-Prem), Route 53, UltraDNS, and Azure.
- **IP/FQDN Field Update:**
  - The existing IP/FQDN field is updated from a text box to a dropdown menu.
  - Users can enter the load balancer details, if required.
  - The dropdown will display: For On-Prem Deployments - available On-Prem Node details.
- **Policy Engine Integration with ACME Protocol**

  AppViewX has introduced support for integrating Policy Engine with the ACME protocol to streamline certificate enrollment and re-enrollment processes. In General Settings, users can now choose between the traditional Workflow or Policy Engine option based on their operational requirements. The selected option determines the behavior and layout of the ACME Configuration page, as well as the corresponding Enrollment and Re-enrollment flows.

- **Dynamic Challenge Password Support for SCEP (JAMF Integration)**

  This enhancement adds dynamic challenge password support for the SCEP protocol when used with JAMF clients. By default, all clients will continue to support static challenge passwords. The Agent Settings Configuration Enhancements are as follows:
  - Introduced a new dropdown field, “Choose MDM Vendor,” allowing users to select the MDM from the available options: Generic SCEP, JAMF, and Addigy.
  - Added a **Challenge Type** field with radio button options:
    - Static: Supported for all MDM vendors and displays a text box to enter the static password.
    - Dynamic: Supported only for the JAMF MDM vendor and displays a dropdown with dynamic variable options.
  - Adds support for dynamic challenge password validation during certificate enrollment for JAMF clients.

 

## Platform - Visual Workflow

- A dedicated <appviewxInstallerDirectory>/sandboxLogs directory has been introduced for workflow script logs in on-prem environments, backed by a newly provisioned Persistent Volume and mounted in the python-executor container of the avx-python-sandbox and avx-python-sandbox-sync pods, replacing the earlier /appviewx/dependencies/logs mount. With this change, workflow and hook scripts are now restricted to logging only within the isolated sandboxLogs directory and can no longer access application logs.

# Chapter 3: Bug Fixes

This section describes the bug fixes in this release.

## CERT+

- **Sectigo certificate types**: Updated the fetch flow to remove leading and trailing spaces before storing data in the database.
- **Certificate inventory filters**: UI filter labels are now correctly mapped to backend expiry status labels, ensuring accurate data retrieval and export.
- **Expiry alert management**: Improved alert rename behavior so linked certificate attributes update correctly instead of creating duplicate entries; users can now remove attributes when linked alerts are deleted.
- **SAN parsing**: Enhanced decoding logic to detect and remove invalid characters (such as “#”) before saving SAN values to the database.
- **Configure Alert permissions**: Missing permissions added to ACF settings; the option now displays correctly in the UI based on user access.
- **Admin Settings tooltips**: Updated tooltip descriptions under CERT+ to clarify that changes apply to both **Job Scheduler** and **Certificate Profile** settings.
- **License upload**: Adjusted logic to prevent overwriting existing policy configurations during license upload.
- **Certificate attributes**: Fixed an issue where dynamically added certAttributes with stringified JSON values were misinterpreted as objects by the tooltip component.
- AppViewX has updated the status codes for the ACME new-nonce and new-account endpoints. The platform now correctly handles the two-step account creation process, which includes checking for an existing account and then creating a new one.

## Platform

- Resolved an issue where configurations could not be updated when a Palo Alto firewall device had secondary device details entered manually using the Manual Entry option. The fix removes ACL validation for secondary device configurations during the update process, allowing successful updates.
- Resolved the sorting issue for Request IDs on the Assigned Requests page.
- Fixed the visibility issue in form task tabular columns to ensure all columns remain visible, even when the table contains a large number of columns.

 

# Chapter 4: Known Issues

This section describes the known issues in this release.

### ADC+

- If the AVI device name contains characters other than A–Z, a–z, 0–9, underscore (_), or dot (.), the external device backup will fail.
- The F5 BIG-IP CVE Out-of-Band (OOB) workflow currently fails due to changes in external CVE data sources, which cause the existing implementation to malfunction.

### CERT+

- **GCP Load Balancer:** Certificates other than Global ALB are not discovered. Push and bind to other load balancers other than Global ALB are not working.
- The DigiCert Duplicate action is currently failing for one-step certificate approval, even though the certificate has already been manually approved and issued in the DigiCert CA portal.
- The movement of expired certificates to the Auto-Archival inventory gets stuck once the triggered cron job for certificate auto-archival reaches a threshold.
- Certificate enrollment fails for CSR generation as HSM for F5 device.
- For GlobalSign MSSL certificates, the uploaded certificate's validity is fixed at 365 days. Auto-regeneration is currently not supported, either via the UI or the exposed API.
- For SwissSign certificates, the Auto-Regenerate value for uploaded certificates is not being set based on the Group-level Auto-Regenerate toggle days.

# Chapter 5: Known Limitations

This section describes the known limitations in software in this release.

## CERT+

- **DCV Limitations for DNS Record Insertion**

  The DCV record insertion may fail if a previous DNS record operation fails in CSC Global. AppViewX uses the DDI SDK library for record insertion and cannot identify whether the failure results from an earlier DNS operation error. Additionally, if a duplicate DNS entry with the same key already exists in the UltraDNS portal, the record insertion fails. In such cases, the user must manually delete the existing record and then retry the operation.

- **DCV Limitations when Renewing an Expiring Domain**
  - **GlobalSign MSSL**
    - Due to the behavior of GlobalSign MSSL, domain re-validation is only allowed when the domain is active and has less than 90 days until expiry.
    - Unlike the MSSL GUI, which allows re-validation regardless of remaining validity, the GlobalSign MSSL API (v2.18) does not provide any re-validation endpoint.
    - Only vendor modifications are supported; to change the validation type, users must delete and re-add the domain.
    - The following renewal scenarios have not been validated due to API constraints:
      - Active domain expiring within 90 days – Vendor details can be modified, but the validation type cannot be changed.
      - Active domain with more than 90 days remaining – Re-validation or modification is not allowed.
      - Inactive domain (Pending Validation) – Vendor details can be updated, but the validation type cannot be changed.
      - Validation Failure – Vendor details can be updated, but the validation type cannot be changed.
  - **Sectigo**
    - Once a domain is submitted for validation (for example, validation is triggered), the validation type cannot be changed until the validation is completed or the domain is deleted.
    - The validation method field does not appear while validation is in progress.
  - **GlobalSign Atlas**
    - The validation method remains empty when the domain status is pending from the CA.
- **DCV Limitations for Sync Domain Functionality**
  - Invalid CA settings cause the Sync Domain function to fail for all associated certificate authorities except DigiCert, which continues syncing despite failed configurations.
  - Once the failed CA settings are corrected, all domain sync operations function as expected.