appviewx

Release Notes

Version: v2024.1.2.0

Copyright AppViewX, Inc.

Trademarks

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
1.3	AppViewX v2024.1.2.0 Release Notes.	March 2025
1.2	AppViewX v2024.1.1.0 Release Notes.	March 2025
1.1	AppViewX v2024.1.0.1 Release Notes.	March 2025
1.0	AppViewX v2024.1.0.0 Release Notes.	March 2025

About this Guide

These release notes accompany AppViewX Release v2024.1.2.0 for the CERT+, Platform, PKIaaS. They describe new features, enhancements, known fixed issues, and known limitations in the software.

Intended Audience

- Customers using AppViewX v2024.1.2.0

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.

For example,

- This document includes software details developed by VMware, Inc. (www.vmware.com).

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.

Convention	Description
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 lists the new features in the AppViewX v2024.1.2.0 release.

AVXpert - TechPreview

The following new feature is included in AppViewX.

- Smart Search feature in AVXpert enhances search efficiency within the system. It interprets user queries intelligently and helps you find and filter any certificate you want simply by asking in natural language.
- Quick Navigation feature has been introduced in AVXpert which understands user queries and provide relevant route for the respective pages or actions within the system.

CERT+

The following new features are introduced in AppViewX CERT+.

- Optimized Apache Linux onboarding for smoother deployments by prioritizing profile certificates, providing greater control over non-profile discovery via Server Global settings, and enhancing configuration sync and discovery performance for improved efficiency.
- Trigger certificate discovery on the newly passive device in Palo Alto/Panorama only when its status transitions from Managed to Available during a High Availability (HA) failover, optimizing compute resource usage and licensing.
- The cron job's subsystem field in the avx_crontab collection will be updated from 'firewall' to 'general,' ensuring it runs regardless of license configuration. This update resolves an issue where Cert+ only customers were not triggering the scheduled midnight sync.
- Enabled CSR generation in HSM for GlobalSignAtlas CA for Server certificate enrollment.
- From Checkpoint HTTPS Inspection Policies are fetched and user should be able to perform push and bind operation to the Inspection policy rules.
- Support added for switching certificates between Microsoft Certificate Authorities (CA) with different settings in AppViewX. The switch functionality is now available for both Microsoft Enterprise CA (MSE) and Microsoft Standalone CA (MSS).
- A configurable option allows you to define the number of days before expired or revoked certificates transition to a 'monitored' state under the certificate history. Once the specified duration has passed, the system automatically updates the status. This applies to certificates in both revoked and expired states.
- A configurable option allows you to define the number of days before certificates transition to a 'monitored' state in the certificate history. Once the specified duration has passed since a certificate

was renewed, reissued, or regenerated, its status is automatically updated. This applies to all renewed, reissued, and regenerated certificates.

- An exposed API is now available to initiate the synchronization process for F5 device profiles, enabling seamless updates and improved management.

- In the Cert Inventory for Server, Client, Code Signing, and Device pages, status counts will be displayed with corresponding labels when users click on the filter summary:

  1. **Expiry in 1-10 days** (Previously 'Expiry in 10 days') – The certificate is set to expire within the next 10 days.
  2. **Expiry in 11-30 days** (Previously 'Expiry in 30 days') – The certificate is set to expire within 11 to 30 days.
  3. **Expiry in 31-90 days** (Previously 'Expiry in 90 days') – The certificate is set to expire within 31 to 90 days.
  4. **Expiry in 90+ days** (New Label) – The certificate is valid for more than 90 days.
  5. **Valid** – Includes all active certificates, excluding expired and revoked certificates.
  6. **Expired** – The certificate has expired.

- Introduced two new APIs for improved certificate management:

  1. **certificate/list API** – Retrieves the complete list of certificates in the inventory along with their associated application connector details.
  2. **certificategroup/list API** – Fetches the complete list of certificate groups.
- The Orphan Report Job Scheduler has been updated from running every 4 hours to a daily schedule at 12:45 AM.

Platform

The following new features are introduced in AppViewX Platform.

- Enhanced error messages for HSM actions to improve readability and clarity. These enriched failure messages are now also recorded in audit logs for better tracking and troubleshooting.
- New APIs have been introduced under the same API names but now utilize the POST HTTP method. These APIs are used to abort, resume, or pause workflow requests. The existing APIs that use the GET method will be marked as deprecated. New APIs with POST Method:
  - POST /visualworkflow-abort-request
  - POST /visualworkflow-pause-request
  - POST /visualworkflow-resume-request.
- **Introduced only for SaaS**: In MSP portal, the License menu has been added for ease of access for the MSP to view the license count and usage.

Chapter 2: Enhancements

This section lists the enhancements in the AppViewX v2024.1.2.0 release.

CERT+

The following enhancements are listed in AppViewX CERT+.

- Extended support for the subaccount level discovery of the sites.
- Support enabled to discover all the certificates from Primary Cisco ISE device.
- Enhanced the system to fetch Panorama template stacks and display them in the SSL Profiles list on the Add Application Connector page.
- Extended support for the subaccount level discovery of the sites in **Imperva Saas**.

PKIaaS

The following enhancement is listed in AppViewX PKIaaS.

Automatically synchronize the PKI+ OCSP signing certificate, ensuring seamless updates of the OCSP signing key in Redis during the OCSP generator job.

Chapter 3: Bug Fixes

This section lists the fixed bugs in the AppViewX v2024.1.2.0 release.

PKIaaS

The following bug is listed in AppViewX PKIaaS.

- After the renewal of the PKIaaS Native CA end certificate, the SKI and AKI values were previously set to None. This issue has been resolved, and the appropriate values are now populated.

Platform

The following bugs are listed in AppViewX Platform.

- Support for SID value fetch from ldap while enrolling EJBCA client certificates.

> **Note:** The CC upgrade to latest version "24.1.2.0" is required to this fix to work

- **Applicable only for SaaS**: The Thames regex pattern for the data center has been modified to disallow spaces. Additionally, 'CC' was added before AppViewX v2024.0.0.0, causing an error during cloud connector deletion. To resolve this, validation checks are already performed during creation and have been removed from the deletion process.
- To enhance security, sensitive fields in the `visualworkflow-integration-get-subcategory` API response are now masked for Northbound/API and Northbound/OpenShift vendor integrations.
- The field type of the Command Repo API response in the generate-commands-and-implement API has been updated to **Map** to ensure compatibility only with the Akamai vendor integration.

Chapter 4: Known Issues

This section does not include known issues in the AppViewX v2024.1.2.0 release.

Chapter 5: Known Limitations

This section lists known limitations in the AppViewX v2024.1.2.0 release.

CERT+

The following limitation is listed in AppViewX CERT+.

- When pushing a template stack in Panorama, all application connectors will be discovered if the templates belong to multiple template stacks.
- Users with a CERT-only license can add multiple firewall devices and perform CLM. However, this capability is restricted when ADC is enabled in combination, ensuring proper license compliance.