



Release Notes

Version: 2024.0.2.0

Copyright AppViewX, Inc.

Copyright © 2024 AppViewX, Inc. All Rights Reserved.

This document may not be copied, disclosed, transferred, or modified without the prior written consent of AppViewX, Inc. While all content is believed to be correct at the time of publication, it is provided as general-purpose information. The content is subject to change without notice and is provided “as is” and with no expressed or implied warranties whatsoever, including, but not limited to, a warranty for accuracy made by AppViewX. The software described in this document is provided under written license only, contains valuable trade secrets and proprietary information, and is protected by the copyright laws of the United States and other countries. Unauthorized use of software or its documentation can result in civil damages and criminal prosecution.

Trademarks

The trademarks, logos, and service marks displayed in this manual are the property of AppViewX or other third parties. Users are not permitted to use these marks without the prior written consent of AppViewX or such third party which may own the mark.

External Reference Links

This product includes software developed by Red Hat, Inc. (www.redhat.com).

This product includes software developed by VMware, Inc. (www.vmware.com).

All other trademarks mentioned in this document are the property of their respective owners.

Contact Information

AppViewX, Inc.

222 Broadway, FL 19

New York, NY 10038

Email: info@appviewx.com

Web: www.appviewx.com

Contents

Preface.....	iv
Chapter 1. New Features.....	5
Chapter 2. Enhancements.....	7
Chapter 3. Bug Fixes.....	9
Chapter 4. Known Issues.....	11
Chapter 5. Known Limitations.....	12

Preface

Revision History

Revision	Description	Date
1.3	AppViewX v2024.0.2.0 Release Notes.	November 2024
1.2	AppViewX v2024.0.1.1 Release Notes.	November 2024
1.1	AppViewX v2024.0.1.0 Release Notes.	October 2024
1.0	AppViewX v2024.0.0 Release Notes.	October 2024

About this Guide

These release notes accompany AppViewX Release v2024.0.2.0 for the CERT+, PKI+, KUBE+, Platform, and Automation modules. They describe new features, enhancements, known fixed issues, and known limitations in the software.

Intended Audience

- Customers using AppViewX v2024.0.2.0

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.
<i>italic</i>	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
<code>codeblock</code>	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 the AppViewX v2024.0.2.0 release.

CERT+

The following new features are included in AppViewX CERT+.

- Enabled sudo access elevation support for WebLogic Linux and JBoss Linux CLM use cases. This feature facilitates the parsing of configuration files on WebLogic Linux and JBoss Linux servers, providing a secure and efficient method for non-root users with restricted access rights to retrieve and parse configuration data.
- Enabled automatic switching to a service account on Apache, Tomcat, and WebLogic Linux, ensuring all commands run under the service account. File transfer workflows use a shared folder for secure transfers to target directories.
- Introduced an option to push Microsoft Server PEM certificates as a bundle, with a custom push feature in the UI to enable pushing certificates either as a chain or as individual files. Options include **Issuer and Server** (default) and **Chain**. Added support for defining certificate order (for example: Server, Root, and Intermediate) through a script update, with the default set to 'server:inter:root.'
- Added a vendor-specific field, **Expiry Emails**, to the **HydrantID** enrollment form. This field can be updated during enrollment and is also discoverable during certificate discovery. The value is included in the response of the **GET Certificate** API call.
- Introduced additional vendor-specific fields for DigiCert CA such as **Additional Email**, **Renewal Message**, and **Notes**. These fields can be populated during certificate enrollment and are sent to DigiCert to update the corresponding order details. Any changes to these fields trigger updates to DigiCert to ensure synchronization.

KUBE+

The following new features are included in AppViewX KUBE+.

- Enabled certificate enrollment for OpenShift routes with KUBE integration, supporting certificate issuance and discovery for OpenShift environments.
- Enabled certificate enrollment into custom keys within secrets, supporting CA-bundled and chained formats. Introduced certificate orchestrator for managing enrollment of certificates, keys, and CA certificates into secrets with custom key configurations.

IoT+

The following new feature is included in AppViewX IoT+.

- AppViewX introduces its own certificate authority, offering seamless integration with industry-standard auto-enrollment protocols for streamlined and automated certificate management. Supported protocols include EST, ACME, SCEP, MS Intune, CMP, and WAEP.

Chapter 2: Enhancements

This section describes the enhancements in the AppViewX v2024.0.2.0 release.

CERT+

The following enhancements are included in AppViewX CERT+.

- Enabled the ability to create certificates with AppViewX and use **Upload CSR** as a CSR generation option during renewal. For Sectigo renewals, added support for CSR generation options (**AppViewX** and **Upload CSR**) and parameters including **Validity**, **Hash Function**, and additional **SANs**.
- Enabled URL discovery with proxy for Cloud-DC, removing nmap for port checks. For other DCs, OpenSSL and proxy chains fetch certificates, with proxy settings stored in the network connector database.
- Enhanced SSL validation check job support with proxy, featuring updated cipher retrieval, routing by proxy and IP range, external reports using network connector settings, removal of multi-threading, data retention during job triggers, and an audit log for job start and end times.
- Enhanced SSL checker and SSL validation report for improved accuracy and efficiency, providing better insights into SSL configurations, faster detection of issues, and more detailed reports to streamline troubleshooting and ensure secure connections.

PKI+

The following enhancements are included in AppViewX PKI+.

- Introduced Post-Quantum Cryptography (PQC) capabilities, updating or replacing current algorithms (for example, RSA and ECC) with PQC algorithms to ensure the infrastructure remains secure in the era of quantum computing.

You can now leverage AppViewX's own Certificate Authority (CA), **AppViewX PKIaaS Native CA**, for PKI initialization, enabling them to take advantage of PQC benefits. The following new features are introduced in PKI:

- **PKI dashboard:** The following widgets are displayed on the **End entity certificate count by CA** tab:
 - **Certificates by Templates:** This widget displays all the certificates created via the various templates.
 - **Certificates by CAs:** This widget displays all the certificates created via the various CAs. By default, all the CAs are selected.

- **Certificate Issuance Trend:** This widget displays all the certificates based on their issuance trend such as daily, weekly, monthly, yearly, and custom.
- **CA Hierarchy:** This widget displays the number of CA hierarchies. Click View to display the CA hierarchies created and the certificates under each of the CAs listed along with their count.
- **Template:** AppViewX provides templates for you to select or customize your own for creating CA and end certificates, allowing you to tailor your cryptographic infrastructure to meet your organization's specific needs. This customization enhances security and ensures preparedness for future quantum threats.
- **Issue Certificate:** You can issue any certificate by uploading any uploaded CSR from the CAs available in PKIaaS.
- **CRL:** A default CRL service is now provided with a customizable CRL Distribution Point (CRL DP) that can be embedded into certificates via templates. The CRL Scheduler allows configuration of CRL issuance frequency and expiry. Additionally, manual CRL publishing is available with options to set a custom expiry time and timezone.



Note: Custom CRLDP and OCSP routing through the Cloud Connector are supported exclusively with the latest version, ensuring enhanced functionality and compatibility.

Chapter 3: Bug Fixes

This section lists the fixed bugs in the AppViewX v2024.0.2.0 release.

CERT+

The following bugs are fixed in AppViewX CERT.

- Fixed an issue with Apache configuration parsing using sudo access elevation, improving parsing of Virtual Host files on Linux servers. This fix ensures secure and efficient access for non-root users, eliminating the need for the downloadFile method from the SSH connector.
- Fixed an issue where WebLogic Linux devices were transitioning to an unresolved status after uploading a valid SSH key file without a password. This resolution ensures smoother device management, improving stability and reliability for users managing WebLogic Linux environments.
- Fixed an issue where the domain could not be retrieved for DigiCert using cert-fetch-custom-attribute. If no custom attributes are enabled at the CA end, the fix ensures the retrieval of other required fields, improving the reliability of the attribute-fetch process.
- Fixed an issue with the validityPeriods under CA Settings for DigiCert CA, where validityInDays was shown as null instead of an empty array. Now, during certificate policy fetch, if validity in days or years is not provided, it will display an empty array, ensuring more accurate and consistent data presentation.
- Fixed an issue where the next execution time of the scheduled network scan was not properly aligned with the set schedule (Date and Day). The certificate schedule discovery now includes a timezone option, allowing customers to set their preferred timezone for more accurate scheduling.
- Fixed an issue where Monday was automatically selected when scheduling a weekly job. The default Monday selection has been removed from the Certificate Validation Check modal, allowing for more flexible scheduling.
- The issue with the Push to Device feature and discovery on the secondary device has been resolved. Push and bind operations to profiles are now successful, enabling smoother certificate management. You can now achieve your desired outcome of pushing the certificate directly to the device, enhancing efficiency and satisfaction.
- The issue causing commit failures on the PaloAlto Firewall has been resolved. Now, when you push a certificate, both the push and commit operations work seamlessly, ensuring a smoother and more reliable certificate deployment process.

Platform (Automation)

The following bugs are fixed in AppViewX Platform Automation.

- The ability to add or update the regex library has been enhanced to ensure that any changes made are automatically synchronized across all nodes and pods in the environment.
- Fixed an issue where emails could not be sent to roles via the Email task in the Email Palette. The fix ensures that emails are now successfully sent based on the assigned role.
- Resolved an issue where the Workflow Regex Library used in-memory caching for server-side regex validation to reduce frequent database calls. To address data inconsistency concerns, the in-memory cache implementation has been removed, ensuring accurate and consistent regex validation.
- The logic has been revamped to prevent a Role User's email from being overwritten by a User Group's email. The Email Palette's **To** field now correctly uses the user's email ID based on their assigned role.

Platform (SaaS - Cloud Connector)

The following bugs are fixed in AppViewX Platform (SaaS - Cloud Connector).

- The issue triggering rare OOM scenarios due to TLS protocol configuration has been resolved. TLS has been re-enabled, restoring the previous secure connection setup and ensuring stable system operation. This update ensures consistent cloud connector connectivity and status persistence, preventing the intermittent disruptions previously observed.
- The mTLS CC upgrade issue, where the `/download-installer` API was incorrectly included in Cloudflare, has been resolved. This fix ensures that the Curl command used to download the latest image works correctly for tenants with mTLS enabled, preventing download failures during CC upgrades.
- To reduce the number of decryption requests to the vault, a cache has been introduced to store the installation key, enhancing performance and reducing overhead during installation processes.

Chapter 4: Known Issues

This section lists the known issues in the AppViewX v2024.0.2.0 release.

CERT+

The following known issues in AppViewX CERT+.

- On Windows Tomcat, rollback fails when the **Use Existing Configuration** and **Private Key in Device** option is enabled.
- Proxy Cloud Connector support is not available for the SSL validation report.

Chapter 5: Known Limitations

This section contains the known limitations in the AppViewX v2024.0.2.0 release.

There is no known limitation in this release.