appviewx

Release Notes

Version: 2024.1.3.0

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
1.5	AppViewX v2024.1.3.0 Release Notes.	April 2025
1.4	AppViewX v2024.1.2.1 Release Notes.	April 2025
1.3	AppViewX v2024.1.0.3 Release Notes.	April 2025
1.2	AppViewX v2024.1.0.2 Release Notes.	April 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 v2024.1.3.0 for the ADC+, CERT+, PKIaaS, Platform, SSH, and Visual workflow. They describe new features, enhancements, known fixed issues, and known limitations in the software.

Intended Audience

- Customers using AppViewX v2024.1.3.0

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.
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 AppViewX v2024.1.3.0 release.

ADC+

The following new feature is included in AppViewX PKIaaS.

- Support has been added for the new **AVI version v30**, ensuring compatibility with the latest updates and features.

CERT+

The following new features are included in AppViewX CERT+.

- Added support for managing extension-less trust certificates (PEM and JKS) on generic Linux systems to streamline certificate handling and secure SSL/TLS communication. This update removes file extension checks, adds permission handling, and enables bulk operations with structured JKS-to-PEM parsing. Extension-less discovery is limited to aggressive scan paths, while server/client certificates without extensions are still supported in the Truststore location.
- Introduced a global **Push to Firewall** setting for **Panorama** devices to streamline centralized certificate management.
- A new job has been added to the job scheduler to parse certificates that were either existing or migrated to AppViewX prior to version v2024.1.1.0. This job updates the certificate details to display the SID extension.
  - The job can be triggered once and **on-demand**.
  - To include the SID extension for your existing certificates, reach out to AppViewX's TAC team.
  - All **newly uploaded or discovered certificates** will automatically include the SID extension.
  - By default, the job is not included in the job scheduler. To display it in the scheduler and trigger execution, execute a database query on the cert_metadata collection with the help of AppViewX's TAC team.
- The certificate attribute system now supports the **Date** field type to allow specifying time-sensitive metadata for certificates at the time of certificate enrollment.
- A toggle button has been introduced on the certificate enrollment page to show or hide certificate attributes. This enhancement allows users to view only relevant fields, making certificate requests more intuitive and streamlined. By default, all existing attributes are set to visible for migrated entries.
- Bulk CSR updates and bulk approval for CA switch are now supported, enabling a more streamlined transition in the following scenarios:

  - From any CA to Microsoft CA (Enterprise or Standalone)
  - Between Microsoft CA types (Enterprise to Standalone).
- An option to exclude regenerated certificates (parent certificates) from the expiry report is now available, using the same toggle that allows exclusion of renewed certificates.
- Added support for an additional filter based on Group Display Name on the Expiry Alert page, enabling users to quickly identify and manage expiring certificates by specific groups for more efficient alert handling.
- Users can now customize report delivery periods and set **Custom Days** within a broader range, offering more control and better alignment with business requirements.
  - Users can now configure report delivery for any duration between **1 and 1999 days** under **Certificate Summary Report > Expiration > Custom Days**, providing greater flexibility to align with organizational reporting needs.
  - The enhanced **Custom Days** validation ensures more tailored reporting by accepting any positive number within the 1–1999 range.
  - This improvement applies to **Server**, **Client**, and **Code-Signing** certificates, enabling broader and more precise control across certificate types.
- Support has been added to allow users to view multiple selected filter values, making it easier to see all chosen groups or criteria. Additionally, users can now update filters, providing the flexibility to modify existing selections as needed.
- Users can now download the private key along with the client certificate, based on the selected **Download Key Access** role under **Client Certificate Actions**. By default, this option will be disabled to ensure enhanced security, giving users control while maintaining a secure environment.
- Support has been added to modify alert modes on **Expiry Alerts**, providing users with greater flexibility to customize how and when they receive expiration notifications.
- ACF support has been added for the "Demo Mode" under the **CERT+ module**, enabling customers to toggle the demo mode on or off based on their needs. This enhancement provides customers with the flexibility to control and restrict demo mode directly within the UI.
- Support has been added to pass the raw certificate content in the **certificate/discovery/upload API** payload, allowing users to upload certificates directly. To use this feature, ensure that the Cloud Connector (CC) is upgraded to the latest version: AppViewX v2024.1.3.0.
- Support has been added to trigger email notifications whenever a certificate with a private key is downloaded from the system.
- Added support for keypair generation and certificate enrollment at the Panorama template level, with push to PaloAlto Panorama template.

PKIaaS

The following new feature is included in AppViewX PKIaaS.

- Added support for new signature algorithms for CA creation, including RSA with SHA-384/512 and key sizes 2048, 3072, 4096, and EC P-521 with SHA-512. These enhancements offer improved cryptographic flexibility and security compliance.

KUBE+

The following new feature is included in AppViewX KUBE+.

- The AppViewX CSI Provider now supports a new combined type for certificates, where the certificate and key (certificate PEM + key PEM) are included in a single file. By Configuring keyWithCertPEM under additionalOutputFormats field in Cert CRD instance will enable this.

SSH

The following new features are included in AppViewX SSH.

- A new SSH Logs section has been added to the logs page to display entries generated by the SSH module. This section includes the following columns: Time, User, Device Name, Object Details, Source IP, AppViewX Node, Login Method, Comments, and Log Message. Additionally, an Access Control Feature (ACF) has been introduced to manage user visibility of the SSH Logs section.
- Added support for SSH log forwarding in the Platform's Observe and Logs section under Log Types. This allows secure forwarding of logs via SSH in both Syslog and CEF formats to a designated server.

Chapter 2: Enhancements

This section describes the new features in AppViewX v2024.1.3.0 release.

ADC+

The following enhancements are included in AppViewX ADC+.

- A new **Backup Pod** has been implemented for **F5 devices**, significantly improving system performance and reducing the load on subsystems and vendor pods. This enhancement ensures more efficient backups and better overall system stability.
- Introduced a retry mechanism for devices stuck in the In Progress status for X hours during the midnight config sync process.

CERT+

The following enhancements are included in AppViewX CERT+.

- To enhance certificate filtering for the **AppViewX-HydrantID integration**, AppViewX now enables filtering of **Certificate Authority discovery scan** results based on the following parameters:
  - **Certificate Types** (filter discovery results by certificate type)
  - **Created From** (filter discovery results by certificate creation date)
  - **Updated From** (filter discovery results by the most recent update date)

  This improvement allows customers to quickly narrow down discovery results, streamlining certificate management and improving efficiency.
- **Only for On-prem**: An IDnomic CA setting can now be onboarded with a RA-only configuration (replacing the previous CA + RA configuration). This CA setting will support discovery and all CLM actions using RA workflows without depending on any IDnomic CA endpoints.

  

  Note: Once the CA setting is onboarded, the configuration type (CA/RA) cannot be changed.

- The fix enables keypair generation at the Panorama template level and supports pushing enrolled certificates to Palo Alto Panorama, addressing the previously missing functionality. This enhancement streamlines the process, allowing customers to manage certificates more efficiently across their Panorama environments.
- Fields such as **Certificate Type**, **Certificate File Name**, and **Key File Name** are now exposed in the **Hooks Inventory**, giving customers greater visibility and control over certificate-related data. This enhancement simplifies tracking and improves management of certificates within automated workflows.

- Customers can now enter a password to seamlessly switch to the service account user during **SAP Web Dispatcher server onboarding**, simplifying the setup process and enhancing security control.
- Customers can now push certificates to **KDB** using the **GSKIT_64 toolkit**, enabling smoother integration and more efficient certificate management within secure IBM environments.
- Customers can now onboard **Windows Tomcat servers** with fully custom installation paths, even if the folder path does not contain "Tomcat" in its name. This enhancement offers greater flexibility for non-standard deployments and simplifies integration in diverse environments.
- AppViewX now supports fetching **AWS account credentials** directly from an integrated **CyberArk vault**, ensuring secure, up-to-date, and compliant credential management. By automating credential retrieval through CyberArk, this solution eliminates the need for manual handling, strengthens security, and aligns with enterprise access control policies.

  For AWS accounts onboarded using CyberArk-stored credentials, AppViewX enables:
  - **On-demand and scheduled cloud scans** for certificate discovery.
  - **Certificate lifecycle management actions** (push and bind) for supported AWS services.

  This enhancement streamlines operations while maintaining high standards of security and compliance.
- AppViewX now allows credentials for onboarding **Amazon CA** and **Amazon Private CA** settings to be securely fetched from an integrated **CyberArk vault**. This integration ensures credentials are always valid and current, enhancing security, eliminating manual credential handling, and ensuring compliance with enterprise access control policies.

  For Amazon CA and Amazon Private CA configurations onboarded using CyberArk-managed credentials, AppViewX supports:
  - On-demand and scheduled certificate discovery scans.
  - Discovery of Route53-enabled configurations.
  - Comprehensive **certificate lifecycle management actions**, including:
    - Certificate enrollment
    - Certificate renewal
    - Certificate regeneration
    - Certificate revocation.

  This capability streamlines certificate operations while maintaining high levels of security and governance.

Platform

The following enhancements are included in AppViewX Platform.

- Support has been added to hide out-of-the-box (OOB) user groups, offering customers the ability to customize their user interface for a more tailored and streamlined experience. To use this feature, db script has to be executed manually. For assistance with running the db script, contact the AppViewX's TAC team.
- **Only for SaaS**: The Cloud Connector (CC) upgrade process has been enhanced with a new pre-check mechanism that validates the K3s Kubernetes certificate before the upgrade begins. If the certificate is expired, users are immediately alerted with an error message and provided with the appropriate email distribution list to quickly request certificate renewal, minimizing upgrade disruptions.To further improve upgrade readiness, two additional pre-checks have been introduced:

  To further improve upgrade readiness, two additional pre-checks have been introduced:

  - Free Memory Check - Confirms that available memory exceeds 512MB
  - Disk Space Check - Confirms that at least 3GB of disk space is available

SSH

The following enhancements are included in AppViewX SSH.

- A dedicated **SSH tab** has been introduced in the **Logging module**, providing users with a clearer and more organized view of SSH-related logs for easier monitoring and analysis.
- SSH log forwarding is now supported through the existing log forwarding framework, enabling centralized monitoring and improved log management.

KUBE+

The following enhancement is included in AppViewX KUBE+.

- The secret created by Cert-Orchestrator currently includes tls.crt, tls.key, and ca.crt, which are used in various integrations such as OpenShift and AppViewX CSI Provider. With this update, a newline character (\n) is appended to the end of the tls.crt and ca.crt contents. This change ensures compatibility with OpenShift routes when attaching the secret directly.

DDI+

The following enhancements are included in AppViewX DDI+.

- Enhanced IP Search support now provides visibility for multiple VIPs associated with an IP and enables grouping of Pool members.
- Admins or configured users will now receive email notifications about sync failures, regardless of the vendor.

Chapter 3: Bug Fixes

This section lists the fixed bugs in the AppViewX v2024.1.3.0 release.

ADC+

The following bugs are fixed in AppViewX ADC+.

- The issue where **deleting a VIP via SDK** also triggered the deletion of the linked Server SSL Profile, due to shared associations with the **HTTPS monitor** and **Virtual Server**, has been fixed.
- When both **username** and **password** of a **GTM HTTPS monitor** were set to **None** via the SDK, the **username** was correctly cleared, but the **password** field displayed unexpected masked text. This issue has been fixed.
- The **connection count** displayed in the **Dashboard widgets** for pools and members was inconsistent. This issue has been resolved.
- The widgets were inaccurately reporting the **status of SLB pool members**, failing to reflect their actual state. This issue has been fixed.
- An issue where deleting a VIP via the SDK also triggered the deletion of the linked Server SSL Profile due to shared associations with the HTTPS monitor and Virtual Server has been fixed.
- When configuring both the username and password of a GTM HTTPS monitor to 'none' through the SDK, the username was correctly cleared, but the password field displayed unexpected masked text. This issue has now been fixed.
- The connection count in the widgets for pools and members was inconsistent in Dashboard. This issue has been fixed.
- The widgets are inaccurately reporting the status of SLB pool members, not reflecting their actual state.

CERT+

The following bugs are fixed in AppViewX CERT+.

- Users can now view all available ciphers, including **TLSv3 protocol ciphers at INSIGHTS**. To view all available ciphers including TLSv3 protocol ciphers, ensure that the Cloud Connector (CC) is upgraded to the latest version: AppViewX v2024.1.3.0.
- The Linux Server Discovery failure issue related to SSH connection and session re-creation errors has been fixed. Previously, intermittent failures occurred when existing connections were dropped or timed out by the server, leading to connection closures.

Platform

The following bugs are fixed in AppViewX Platform.

- The RADIUS user login authentication issue has been resolved. If you are using RADIUS external authentication, ensure that the Cloud Connector (CC) is upgraded to the latest version: AppViewX v2024.1.3.0.
- When users click the **AppViewX link** from an email, they are seamlessly directed to the requested page if their session is already active. This enhances convenience by eliminating the need to log in again, streamlining access and improving the user experience.

PKIaaS

The following bug is fixed in AppViewX PKIaaS.

- The issue where changing the region did not fetch the correct **Certificate Authorities (CAs)** on the first page load has been resolved, ensuring accurate and consistent data is displayed immediately.

Visual Workflow

The following bug is fixed in AppViewX Visual Workflow.

- The exceptions in the visualworkflow-request-logs API caused by attempts to access unavailable log data when restricted by the ACF setting has been handled through a validation logic in the API.

SSH

The following bugs are fixed in AppViewX SSH.

- Fixed an issue where details from the **known_hosts.old** file were incorrectly parsed during **SSH key discovery**.
- Resolved an issue where contents within the temporary working folder created by AppViewX were being discovered during **SSH key discovery**.
- Addressed an issue where key groups could be deleted even when **SSH keys** were associated with them.
- Fixed an issue where rediscovery of a completed scheduled discovery was causing an error.

KUBE+

The following bug is fixed in AppViewX KUBE+.

- An issue where the SDK failed to handle the **API** source during Kube+ enrollment has been fixed.

Chapter 4: Known Issues

This section lists the fixed bugs in AppViewX v2024.1.3.0 release.

CERT+

The following known issues are listed in AppViewX CERT+.

- In SAP ABAP Discovery, the certificates discovered are mapped to root inventory and due to that associated objects are not getting mapped.
- SAP ABAP discovery was failing with the unclear error message: **Certificate discovery failed for the device.**

Chapter 5: Known Limitations

This section lists the limitations in v2024.1.3.0 release.

CERT+

The following limitations are listed in AppViewX CERT+.

- **Only for On-prem**: Due to IDnomic API limitations, AppViewX is not notified when a certificate revocation request is declined. Hence, work orders for certificate revocation may still be shown as failing even if they are declined. This limitation will be addressed in the subsequent release versions.
- For the HydrantID CA, the certificate authority scan will discover only active certificates. To discover expired certificates, a rule must be created and applied at the time of triggering the certificate authority scan.