appviewx

Release Notes

Version: 2024.2.2.0 (On-prem)

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
1.0	AppViewX v2024.2.2.0 (On-prem) Release Notes.	July 2025

About this Guide

These release notes accompany AppViewX Release v2024.2.2.0 for the ADC+, CERT+, PKI+, and Pages modules. They describe new feature, enhancements, known and fixed issues, and known limitations in the software.

Intended Audience

- Customers who on-boards to AppViewX v2024.2.2.0.

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.

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 v2024.2.2.0 release.

ADC+

The following new feature is included in AppViewX ADC+.

- Introduced the ability to gracefully disable AVI GSLB Pool Members using the `graceful-timeout` setting, helping ensure smooth traffic transition and minimizing service disruption during maintenance or configuration changes.

CERT+

The following new features are included in AppViewX CERT+.

- Certificates can now be generated and filtered based on the presence or absence of the Security Identifier (SID). This feature is especially useful for identifying certificates tied to machine or user accounts and for compliance or audit reporting. The report is represented using a pie chart widget with interactive legends and chart elements, and can be exported as a .csv file.
- In compliance with recent updates from the CA/Browser Forum S/MIME Baseline Requirements, support has been extended for DigiCert-issued S/MIME certificates to now include the Given Name, Surname, or Pseudonym fields in the subject information during certificate enrollment.
- Enabling support for BlueCat Micetro DNS using ACME protocol clients such as Certbot and Win-ACME, with DNS challenge validation. This streamlines the issuance of certificates by leveraging existing DNS infrastructure to validate domain ownership automatically.
- For onboarding Microsoft Azure in AppViewX, AppViewX has now introduced support for configuring the Azure Government Cloud, which is a specialized cloud computing platform designed specifically for U.S. government agencies and their partners.

> **Note:** In the current implementation, the Azure Government Cloud configuration is supported only for the United States, to serve the U.S. government agencies and their partners with data residency, operations, and compliance as per the U.S. regulations.

- The Discovery Status email notification now includes the delta count of newly discovered certificates, enabling customers to quickly identify recent changes and take timely action.
- To simplify configuration and maintain consistency, Cipher Suite settings have been removed from **Insights** > **Risk & Crypto**. The feature now inherits settings from the General Cipher Settings section.
- ACL support has been added for Scheduled Discovery.

- Introduced an API to fetch devices identified during network scans, supporting integration and enhanced visibility into discovery results.
- Supported **Module Protection** mode of Entrust HSM to perform cryptographic operations like Private Key Generation, CSR Generation securely using the HSM module
- A new column named **Private Key in AppViewX** across all certificate categories (Server, Client, Code signing and Device), allowing users to quickly determine which certificates have their private keys securely stored in AppViewX.
- Users can now select the encryption algorithm when downloading certificates in PKCS#12 or PFX (.p12) format. While AES remains the default for enhanced security, 3DES can be chosen for compatibility with legacy systems.
- A **Clone** action has been added to the **Expiry Alert** configuration screen, enabling users to duplicate an existing configuration, edit it as needed, and save it as a new alert simplifying the setup of similar alert rules.
- AppViewX currently supports RSA key pair generation using HSM. With this enhancement, ECC (Elliptic Curve Cryptography) algorithm support will be enabled. Users can select the EC key type, which will activate the ECDSA curve option. Certificate enrollment and renew/regenerate actions using HSM with ECC will be supported for GlobalSign SSL and DigiCert CAs.
- Certificate validity (in days) is now available in Query Explorer, allowing users to easily track and filter certificates based on their remaining validity period for better lifecycle management.
- Support for certificates issued by SwissSign CA will include the product name in the Certificate Type field in the certificate inventory. Additionally, the Certificate Type can be used as a filter to generate custom reports based on the product name for certificates issued through SwissSign CA.
- Introduced an automation feature to automatically fetch and sync GlobalSign-managed domains with the AppViewX platform, reducing manual effort and ensuring your domain inventory stays up to date in real time.
- Support provided with API endpoint to assign certificate to certificate group and unassign certificate from certificate group.
- Support provided with API endpoint to update certificate attributes for a given certificates using ResourceID of the certificates.
- In a generic Linux setup, the private key is encrypted at the endpoint during creation and saved as an encrypted `.txt` file. During the push process, the key is decrypted. If the push is for a keystore type, the decrypted key is added to the appropriate keystore. If it is a PEM-type push, the decrypted key file is retained.
- Users can now update the system trust store in Linux Servers after pushing the certificate.
- PFX certificates pushed to Windows machines with server version 2016 or below will have the content encrypted with TripleDES algorithm by default.

- In WebLogic on Linux, certificate binding is supported for configurations that use the T3S protocol with the administration port enabled.
- The sample sheet export will now export a single sheet with multiple tabs for the corresponding vendors with only the applicable columns for the respective vendors.

> **Note:** This is applicable only for .xlsx type file export.

- In Apache Linux, users can now suppress email notifications for the website heartbeat file.
- API for accessing reports within Insights is now exposed, enabling seamless integration with external systems and enhanced automation of reporting workflows.

KUBE+

The following new features are included in AppViewX KUBE+.

- Added support to renew or regenerate certificates for existing Kube Secret connectors and push the updated certificates to the Kubernetes cluster through the Certificate Holistic View using App Connectors
- Added the ability to revoke certificates when revoking the Cert CRD Instance in the Secure Apps Inventory.

PKI+

The following new features are included in AppViewX PKI+.

- You can now explore PKI+ in read-only demo mode with sample data. This is disabled by default and can be enabled using the toggle button from the GUI.
- You can now configure AVX Native CA directly from the CA Inventory page on PKI+.

SSH+

The following new features are included in AppViewX SSH+.

- Customers can now manage HSM parallelism directly through the user interface. By navigating to the Sign Settings section, users can enable or disable HSM parallelism based on their specific performance and security needs. This configurable option enhances control and optimizes signing operations based on the use case.
- Customers can configure polling behavior for HSM-based signing operations when parallelism is disabled. Through the UI, users can define the retry count and the interval between retries to check

the signing status. This allows for greater control and adaptability in scenarios requiring sequential processing.
- Added an option to change the key group for keys in the User/Host Key Inventory, enabling easier organization and management.
- Added the ability to schedule or instantly discover SSH keys from hosts based on their host compliance group, ensuring all hosts within the group are automatically included in the discovery process.
- Added support for recursive scanning of dynamic users and custom directories. Users can specify a path using the `%u` tag to enable automated discovery across all user directories.
- The SSH_Key_Instance_Export workflow is now included by default with the product.

SIGN+

The following new features are included in AppViewX SIGN+.

- The HSM parallelism enablement through GUI provides customers with the flexibility to manage HSM parallelism directly through the user interface. By navigating to the Sign Settings section, users can easily enable or disable HSM parallelism based on their specific performance and security requirements. This configurable option enhances control and allows for better optimization of signing operations depending on the use case.
- The global level settings of polling configuration provides customers with the flexibility to configure polling behavior for HSM-based signing operations when parallelism is disabled. Through the GUI, users can define the retry count and the interval at which each retry should be triggered to check the status of the signing process. This ensures better control and adaptability in scenarios where sequential processing is required.

Chapter 2: Enhancements

This section describes the new features in AppViewX v2024.2.2.0 release.

CERT+

The following enhancements are included in AppViewX CERT+.

- Introduced two discovery modes, Optimized and Aggressive, for Sectigo CA in both On-Demand and Scheduled Scans. Optimized mode improves performance by fetching only new certificates, while Aggressive mode ensures complete inventory accuracy by downloading all certificates from the CA.
- Enhanced AppViewX to support Cisco ISE version 3.3.0.430 for Certificate Lifecycle Management (CLM), enabling seamless certificate operations on the latest ISE release.
- Apache Linux parsing support has been enabled with conf file containing virtual hosts with directives having no parameters
- Users can now perform bulk import of servers with SSH keys into AppViewX, simplifying large-scale onboarding and management.
- Added a chart configuration option that allows users to select the number of records displayed on a chart, offering better control over data visualization.

Platform

The following enhancement is included in AppViewX Platform.

- Added support to configure a report dashboard across multiple pages, enabling better organization and navigation of large data sets.

PKI+

The following enhancements are included in AppViewX PKI+.

- Once a custom template is used to issue at least one certificate, the following fields become non-editable: name, noRevAvail, extendedKeyUsage, baseKeyUsage, allowAuthorityKeyId, allowSubjectKeyId, subjectKeyHashBit, enableCrlDp, enableCaDefinedCrlDp, enableOcspDp, and enableCaDefinedOcspLi.
- The **Settings** page has been enhanced for better usability and control. The **Key Ceremony Admins** has been renamed to **Custodian Admins** for clearer role definition. In the **Certificate Inventory**, the "Issued Certificate Status" field is now labeled **Select Certificate Authorities**, and the list of issuer names displayed is based on RBAC permissions, ensuring users only see authorized CAs.

For users with the global setting previously set to **Managed**, all existing Certificate Authorities have been automatically transitioned to **Managed**, while any unselected CAs will default to **"Monitored"**, providing a more secure and streamlined CA management experience.

- The `otherName` extension in the SAN field now supports ASN.1 objects in addition to plain strings, enabling greater flexibility for advanced certificate use cases.

Chapter 3: Bug Fixes

This section describes the bug fixes in AppViewX v2024.2.2.0 release.

CERT+

The following bug fixes are included in AppViewX CERT+.

- The issue with the Certificate Manager role has been resolved by implementing a new approach that eliminates previous limitations. REST APIs are now used to accurately identify the file names of certificates and keys stored on the F5 device. The download process is automated using the JSCH (Java Secure Channel) library, replacing manual SCP command execution. This enhancement removes the need for node password input, streamlining operations and improving security.
- Resolved issues in the JKS file system push for Microsoft Server, both in the UI and backend, where the complete certificate chain was missing in the PrivateKeyEntry. This fix ensures successful deployments and improves certificate trust validation on the target server.
- The issue with the Canned Dashboard not updating has been resolved, ensuring real-time visibility and accurate monitoring of critical data.

Sign+

The following bug fixes are included in AppViewX Sign+.

- Resolved an intermittent issue in signing operations for HSM use cases caused by session timeouts observed in Thales GPN. This fix ensures more reliable and consistent signing performance.
- The issue with OpenSSL and SIGN+ on Ubuntu 24.04 has been resolved, ensuring seamless and secure functionality for your applications.

> **Note:** This fix requires either upgrading the existing SIGN+ package or installing the new SIGN + package of latest release version.

Reporting

The following bug fix is included in AppViewX Reporting.

- The issue with the Hook Count attribute not functioning correctly has been resolved, ensuring accurate tracking and improved reliability of hook operations.

Chapter 4: Known Issues

This section does not include known issues in the AppViewX v2024.2.2.0 release.

Chapter 5: Known Limitations

This section does not include known limitations in the AppViewX v2024.2.2.0 release.