appviewx

Release Notes

Version: 2024.2.4.0 (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 v2024.2.4.0 (On-Prem) Release Notes	Sep 2025

About this Guide

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

Intended Audience

- Customers onboarding AppViewX v2024.2.4.0.

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

There are no new features in this release.

Chapter 2: Enhancements

This section describes the enhancements in this release.

CERT+

- **Change in EKU Policy for DigiCert CA Server Certificates**

  Effective October 1, 2025, DigiCert CA server certificates will include only server authentication in the **Extended Key Usage (EKU)** field. Dual authentication will no longer be supported.

  As a temporary provision until May 1, 2026, DigiCert CA will continue to allow dual authentication. Customers who need to continue enrolling server certificates with dual EKU can contact the AppViewX SRE team at saashelp@appviewx.com.

  > **Note:**
  >
  > It is strongly recommended to transition away from using server certificates for dual authentication to align with current industry best practices.

- **Support for ECC in HydrantID CA Certificate Enrollment**

  Certificate enrollment workflows through HydrantID CA in AppViewX now support the **Elliptic Curve Cryptography (ECC)** algorithm. ECC offers stronger security, lower computational overhead, and aligns with modern PKI best practices.

  With this enhancement, customers can now:
  - Request and issue certificates using ECC algorithms
  - Configure ECC key lengths to meet security and compliance requirements

  To enable the ECC algorithm for certificate enrollment, modify your custom HydrantID CA policy to select the desired ECC bit length-key pair combination(s) and the corresponding ECDSA curve values.

Chapter 3: Bug Fixes

This section describes the bug fixes in this release.

CERT+

- **Resolved Issues with DNS field in Amazon Private CA Certificate Enrollment**

  The DNS field now correctly displays and auto-populates with the **Common Name** when DNS is selected as a Subject Alternative Name (SAN). Previously, the field was hidden and failed to auto-populate.

- **Improved Handling of Unavailable Certificates in CA Connector**

  Users will now receive a success response even when certificates do not have CA connector, ensuring smoother workflow execution and improved error handling.

- **Resolved Issue with Certificate Search after Enrollment or Renewal**

  Previously, when a user enrolled a new certificate or renewed/regenerated an existing one, the certificate appeared in the inventory. However, searching by common name failed new and renewed certificates to appear in search results due to reset keywords and search tokens after push/bind operations.

  Now users can push/bind a certificate to any device and on doing a free-text search in the inventory, the certificates will appear as expected.

Chapter 4: Known Issues

There are no known issues in this release.

Chapter 5: Known Limitations

There are no known limitations in this release.