appviewx

Release Notes

Version: 2024.2.1.0 (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....iv
Revision History....iv
About this Guide....iv
Intended Audience....iv
Third-Party Software Acknowledgments....iv
Text Conventions....iv
Chapter 1. New Features....5
ADC+....5
CERT+....5
KUBE+....7
Platform....8
PKI+....8
SSH....8
Chapter 2. Enhancements....10
CERT+....10
PAGES....10
PKI+....10
Chapter 3. Bug Fixes....12
CERT+....12
PAGES....12
Chapter 4. Known Issues....13
Chapter 5. Known Limitations....14
CERT+....14

Preface

Revision History

Revision	Description	Date
1.0	AppViewX v2024.2.1.0 (On-prem) Release Notes.	June 2025

About this Guide

These release notes accompany AppViewX Release v2024.2.1.0 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 v2024.2.1.0.

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 v2024.2.1.0 release.

ADC+

The following new features are included in AppViewX ADC+.

- Enabelement of latest A10 V6 version support with all the standard features supported.
- Enabelement of latest AVI V31 version support with all the standard features supported.

CERT+

The following new features are included in AppViewX CERT+.

- AppViewX now offers end-to-end integration with Dell iDRAC using REST APIs, enabling the complete Certificate Lifecycle Management (CLM) workflow for iDRAC.
- AppViewX now supports HTTP validation over a custom port for ACME certificate issuance. Previously, validation was limited to port 80. With this enhancement, users can configure a custom port, ensuring compatibility with supported ACME Clients like Certbot, LEGO and allowing greater flexibility in deployment environments.
- Enhanced WAEP Enroll API to support default templates without OIDs, embed template metadata in certificates, enable dynamic CSR parsing, and add SID handling based on UI toggles.
- AppViewX now supports Cipher Suite Report customization through OOB workflow. Previously, ciphers strength can not be modified as per need, now users can configure a ciphers strength based on tls version in custom collection, and it will be used while generating the cipher suite report.
- AppViewX now supports email notifications for changes in discovery status. Users will receive alerts when a discovery job is completed, fails, or is partially successful. These notifications include key summary details such as the number of certificates newly discovered. This enhancement improves visibility and keeps certificate administrators informed in real time without requiring them to log in and check manually. Notifications are sent based on the discovery configuration and user or user-group preferences.
- A new API has been introduced that allows users to fetch the results of a certificate discovery execution using the discovery name as input. The response includes detailed metadata of all certificates discovered in that execution, such as Common Name, SANs, expiry, serial number, and more. It also provides summary metrics like the total number of certificates discovered. This API enables better automation, integration with reporting tools, and simplifies tracking and auditing of specific discovery runs.

- The Cipher Suite severity grouping used in the discovery summary reports is now managed through a unified configuration page under **CERT+** > **Administration** > **General Settings** > **Cipher Settings**. This update allows configurability in the report, ensuring consistency and ease of maintenance. Administrators can now define High, Medium, and Low priority cipher groups centrally, enabling better alignment with enterprise security policies.
- AppViewX now provides APIs to create, update and delete network entries used in certificate discovery scans. These APIs enable seamless integration with external systems for managing IP ranges and subnets designated for scanning. The new capability allows automation of network onboarding and maintenance, while also ensuring only enabled network entries are available during discovery configuration.
- AppViewX now supports APIs to programmatically trigger certificate discovery via Certificate Transparency (CT) logs and network-based scanning. These APIs allow users to initiate targeted scans using domain names (for CT logs), enabling integration with external systems, automation workflows, and DevSecOps pipelines. Each triggered scan is tracked with a unique name, and execution results are visible in the discovery inventory. This enhancement streamlines large-scale and event-driven discovery operations.
- TLS version details are now displayed alongside ciphers retrieved from servers after discovery, enhancing visibility and enabling accurate strength mapping.
- A new API is now available to export the mapping of ciphers to their corresponding TLS versions discovered during a specific certificate discovery execution. This API includes metadata such as discovery start and end time, and provides a structured format optimized for use with reporting tools like Power BI. It enables teams to analyze protocol-cipher usage trends, assess compliance, and integrate TLS configuration data into broader security dashboards and audits. Cipher report via api is supported for discoveries from - network, ip range and subnet and for discoveries only from current appviewx version 2024.2.1.0
- Support for multiple email address in group by introduced new field called "Alternative Email(s)" within the Certificate Group which will allow to add additional email addresses alongside the existing primary email
- AppViewX now supports within certificate group to select specific device category for Auto Push.
- AppViewX now supports CLM actions for the windows gateway client and server certificate.
- AppViewX Now supports Futurex CA addition , enrolment and regenerate.
- AppViewX now supports Endpoint CSR generation in iDRAC server and issue certificate from CA.
- AppViewX now supports onboarding Dell iDRAC server and discover all the certificates.
- AppViewX now supports onboarding Fortigate/FortiManager firewall devices with SSH port provided by the user and crud changes done.
- AppViewX now supports RBAC for Password vault addition for individual users.

- Blocked domain names field is introduced in the policy page. The user now has the ability to set up a blacklist for domains, similar to their existing setup in CA, where they prefer not to populate any values in the "Allowed Domains" list. The expectation is that all domain common names should be allowed by default, except for the explicitly blacklisted domains.
- The certificate download functionality by enabling strong encryption when private keys are included in the downloaded file. Introducing support for 7z (7-Zip) compression format as an optional mechanism to apply stronger encryption (for example, AES-256) compared to traditional ZIP-based exports.
- As part of international regulations, the maximum validity of SwissSign S/MIME certificates has been reduced from three to two years. This applies to the following products: SwissSign Personal S/MIME E-Mail ID Silver, SwissSign Pro S/MIME E-Mail ID Gold, SwissSign Pro S/MIME E-Mail ID Gold with Auth, and SwissSign Pro S/MIME E-Mail ID Gold RSASSA-PSS. Additionally, for Pro S/MIME E-Mail ID Gold certificates that include a name entry, the attributes **givenName** and **surname** or **pseudonym** must be provided separately in the request.
- Added support to restrict automatic renewal or regeneration of monitored certificates through configurable settings under **CERT+ > Administration > General Settings > Auto-Renewal** and **Auto-Regenerate Settings**, giving users greater control over certificate management actions.
- AppViewX now supports integration with Futurex Key Management and Encryption System (KMES), a FIPS 140-2 Level 3-certified key management solution offering robust cryptographic key lifecycle management. With this integration, Futurex KMES functions as a trusted Certificate Authority (CA) in AppViewX, enabling automated certificate issuance, regeneration, and improved PKI management with centralized control, high availability, and regulatory compliance.
  - Supports server, client, and code signing certificates
  - Enables CLM actions: enrollment, (auto) regeneration, and revocation checks via CRL/OCSP
  - Allows attribute inclusion during CLM actions and within inventory
  - Parses and stores root, intermediate, and signing CA certificates for chain formation
  - Supports importing externally issued certificates into inventory
  - Works with or without a proxy
  - Supports multi-credential authentication and optional client certificate
  - Provides real-time CA connectivity check upon configuration
  - Logs all certificate and key activities securely for auditing
  - Fetches and stores issuance policies and metadata
  - Maps issuance policy to signing CA, extension profile, root CA, approval group, validity, hash algorithm, and key length.

KUBE+

The following new feature is included in AppViewX KUBE+.

- CERT Group selection option has been moved from Kube Policy Central Cluster Policy page to Secure Apps enrollment form.
- Trigger certificate enrollment call from CERT Orchestrator whenever CERT CRD instance is edited.
- Introduced a flag to skip the deletion of the Secret when Cert CRD instance is deleted.
- PKIaaS Native CA is supported in KUBE+.

Platform

The following new feature is included in AppViewX Platform.

- Conditional Birthright Assignment is introduced toimprove Role-Based Access Control (RBAC) during user authentication via external loginThis feature aims to refine user access permissions and address the current issue of overly broadaccess granted through the automatic assignment of the birthright user group.

  To use this feature, dbscript has to be executed manually. For assistance with running the db script, contact the AppViewX'sTAC team.

PKI+

The following new feature is included in AppViewX PKI.

- The PKI inventory now displays all expired and valid certificates. The expired certificates can either be removed or renewed from the inventory to maintain a secure and up-to-date PKI system.

SSH

The following new feature is included in AppViewX SSH.

- The SSH_Key_Instance_Export workflow has been introduced to enable the export of all key instances from the user/host key inventory, allowing users to generate and receive reports instantly or on a scheduled basis via a configured email address. The workflow includes flexible filtering options such as missing or non-missing keys, host key status (Reachable, Unreachable, or Deleted), and key groups enabling users to tailor reports for specific auditing and management requirements.
- Advanced search support has been added for tags. Users can now access the Advanced Search section, where a dedicated Tags section is available. For each tag, users can specify a value to search for, and keys matching the specified tag values will be filtered accordingly.
- Audit log messages generated from user actions have been updated to include proper and necessary details.

- A new bulk tag update feature has been introduced, allowing users to efficiently update tag values for multiple keys using two methods:
  - **Group-based update**: Users can select a key group, choose specific keys within it, and assign a tag value to update all selected keys in one action.
  - **Template-based update**: Users can download a sample template, fill it with key fingerprints and desired tag values, and upload it to apply updates based on the provided fingerprints.

  This enhancement streamlines tag management, saving time and improving operational efficiency.
- Introduced APIs to streamline key and tag management, including endpoints for creating, listing, updating, and deleting tags, as well as for creating and modifying keys. These APIs enable seamless integration and automation of key lifecycle and tagging operations.
- Server import now supports the inclusion of the **Access Type** field for servers imported with **SSH Sync** enabled, allowing for more accurate configuration and improved access management during bulk imports.

Chapter 2: Enhancements

This section describes the new features in AppViewX v2024.2.1.0 release.

CERT+

The following enhancement is included in AppViewX CERT+.

- Enhanced Profile Sync API with performance optimizations and optional virtual server linkage to prevent timeouts on large F5 devices.
- The discovery summary has been enhanced to recognize and correctly categorize certificates using Post-Quantum Cryptography (PQC) key algorithms. Previously, PQC-based certificates were excluded from the results evaluation. With this update, certificates using PQC algorithms are now included and appropriately flagged. This enhancement ensures more accurate visibility into cryptographic strength and supports customers evaluating or adopting PQC readiness.
- To enhance usability and improve user understanding, informative tooltips have been added to all Discovery Reports in the Summary tab. Previously, the absence of contextual help made it difficult for users to interpret the purpose of each report. With this update, clear tooltips now provide guidance on the intent and relevance of each report, offering better clarity and improving the overall user experience.
- Enhanced the certificate search API to accepts multiple categories and returns matching certificates across those categories
- Added support for AVI 31 version across all CLM actions, allowing seamless certificate lifecycle management on AVI 31 devices for improved compatibility and operational efficiency.
- Added support for AVI 30 version across all CLM actions, enabling efficient and seamless certificate lifecycle management on AVI 30 devices for enhanced compatibility and control.
- Enhanced certificate parsing during discovery for Generic Linux to accurately handle certificates with a **TRUSTED** header and additional embedded data, ensuring more reliable and comprehensive certificate detection.

PAGES

The following enhancement is included in AppViewX PAGES.

- Consolidated landing page configuration for custom pages to simplify setup and provide a more streamlined, user-friendly experience in managing custom landing pages.

PKI+

The following enhancements are included in AppViewX PKI+.

- AppViewX allows to delete external subordinate CAs as well with custodian approval.
- Audit logs are available to track all changes or errors related to templates.

Chapter 3: Bug Fixes

This section describes the bug fixes in AppViewX v2024.2.1.0 release.

CERT+

The following bug fixes are included in AppViewX CERT+.

- An issue has been resolved where scheduled discovery jobs were being triggered immediately after any configuration update, even when the changes did not involve scheduling parameters. With this fix, scheduled discoveries now only execute according to their defined schedule, and updates to unrelated fields will no longer cause unintended runs. This ensures accurate scheduling behavior and prevents unexpected load on discovery infrastructure.
- Resolved the issue with Bulk Server Import using FQDN, ensuring smooth and reliable import of multiple servers for improved efficiency and reduced manual effort.

PAGES

The following bug fix is included in AppViewX PAGES.

- Improved the performance of Users & Groups rendering when using the Page Share function, ensuring faster load times and a smoother user experience.

Chapter 4: Known Issues

This section does not include known limitations in the AppViewX v2024.2.1.0. release.

Chapter 5: Known Limitations

This section contains the known behaviors, system maximums, and limitations in software in AppViewX v2024.2.1.0 release.

CERT+

The following known limitations are included in AppViewX CERT+.

- CSR generation in Dell iDRAC endpoint is getting failed with Organization field value containing comma special character
- When adding a Microsoft server integrated with the Windows Gateway Agent, the server's hostname must exactly match the hostname used in the Gateway URL . Any mismatch between the server hostname and the Gateway URL will cause push operations to fail.
- The AppViewX-Futurex integration currently does not support the following CLM actions due to API limitations:
  - Renew and auto-renew
  - Revoke.