appviewx

Release Notes

Version: 2024.0.0 (MSP)

Copyright AppViewX, Inc.

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 the CentOS Project (www.centos.org).

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

Revision History

Revision	Description	Date
1.0	AppViewX v2024.0.0 (MSP) Release Notes.	November 2024

About this Guide

These release notes accompany AppViewX Release v2024.0.0 for the MSP Portal, ADC, CERT, PKI, SSH, KUBE, SIGN, DDI, Platform, and Visual Workflow modules. They describe new feature, enhancements, known and fixedissues, and known limitations in the software.

Intended Audience

- Customers who on-boards to AppViewX v2024.0.0.

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.
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 v2024.0.0 release.

MSP Portal

The following new features are included in AppViewX MSP Portal.

- Single Sign-On (SSO) is now supported for MSP users, enabling seamless access to their authorized tenants from the MSP Portal without requiring additional logins.
- A Demo Mode has been introduced in the MSP portal, allowing users to experience its functionality and value quickly using test data.

ADC

The following new features are included in AppViewX ADC.

- Nginx plus Version R30 and R31: Device Onboarding and Manage SLB objects with Certificate Life cycle Management.
- HAProxy Enterprise version onboarding support for Certificate Life cycle Management.
- Introduced an option to retry the Device Mid-Night sync to enhance reliability.
- **Note:**
  - As part of application upgrade, all F5 customers are expected to place the javax.xml.soap-api.jar as an additional dependency for the iControl.jar.

CERT

The following new feature is included in AppViewX CERT.

- The option for users to select the encryption algorithm when creating a PKCS #12 certificate has been enabled.

  Note: Allowed file formats <.p12> or <.pfx>.

- AppViewX introduced support for the Enterprise Application Service platform with the following features:
  - Onboarding Enterprise Application Services
  - Discovering certificates and profiles from Enterprise Application Services using on-demand discovery
  - Enabling automatic synchronization of the AppViewX inventory with the Azure cloud infrastructure.

- AppViewX introduced support for the APIM Service platform with the following features:
  - Onboarding APIM Services
  - Discovering certificates and profiles from APIM Services using on-demand discovery
  - Enabling automatic synchronization of the AppViewX inventory with the Azure cloud infrastructure.
- AppViewX introduces support for the App Registration Service platform with the following features:
  - Onboarding App Registration Services
  - Discovering certificates and profiles from App Registration Services using on-demand discovery
  - Enabling automatic synchronization of the AppViewX inventory with the Azure cloud infrastructure.
- The email notification feature has been enabled for certificate push and push & bind operations for enterprise applications from AppViewX.
- Added auto-enrollment support for DigiCert One certificate authority across ACME, EST, SCEP, MS Intune, and CMP protocols.
- Introduced the ability to clone agent settings for all auto-enrollment protocols.
- Enhanced ACME DNS functionality with additional options for DNS challenge validation alongside the existing flow:
  - Added option to manage TXT record addition in the DNS server through AppViewX.
  - Introduced the option to perform challenge validation using A records instead of TXT records.
  - Provided the option to bypass challenge validation for pre-validated domains.
  - Customers can now select their preferred Challenge Validation Type when "Challenge Type" is set to DNS.
  - Introduced support for custom attributes and certificate attributes in the EST client provided by AppViewX.
  - A new button, Push Type, has been added on IIS with the following options:
    - **Push Certificate**: This option pushes the certificate to the endpoint without binding it to any sites. The certificate will be pushed to the default web hosting certificate store for IIS.
    - **Push and Bind Certificate**: This option pushes the certificate and binds it to the respective site. It also allows the choice between updating existing site bindings or creating new bindings.

Note:

- As part of cloud connector (CC) upgrade, all F5 customers are expected to place the javax.xml.soap-api.jar as an additional dependency for the iControl.jar.
- The issue with displaying the correct connector status after certificate synchronization via discovery (both on-demand and scheduled) has been resolved for firewall and server vendors. Previously, the connector for the old certificate would incorrectly show an "in sync with device" status, even though the certificate was no longer present on the device. This has been

corrected, and the connector for the old certificate now accurately displays an "out of sync with device" status.

- In the configured application connector, the application will overwrite the key content of the key file specified in the selected profile.
- Added support for AIX OS version for successful certificate binding.
- Exported the Device Managed status details for servers.
- Exported Server Inventory for data modification and re-import without timeout for up to 5,000 devices.
- Introduced an upsert script to add multistack push intent in the database, enabling intent support within the product.

DDI

The following new feature is included in AppViewX DDI.

- Custom source support is introduced for the IP Intelligence feature, allowing the addition of any IP source to the system for more comprehensive IP searches and references. An inbuilt IP search engine is also introduced to improve search performance, providing faster and more efficient results for IP queries.

Platform

The following new features are included in AppViewX Platform.

- Retries ADC devcie config fetch for devices that are unresolved during the automatic midnight sync for ensuring continuous access and management of ADC devices even when initial attempts fail.
- Access control for User Interface tasks has been refined by introducing new levels: 'View,' 'Review,' and 'Review and Write.' Previously, users with 'Read' access could submit tasks, but now only users with 'Review' or higher access can submit tasks, while 'View' users are restricted to viewing tasks only.
- A Stepper (Wizard) Component has been implemented to break down complex configurations into a multi-step process, guiding the user through each step.
- The global filter component is added to reporting dashboards provides intuitive filtering options for multiple reports on a single page.
- A multi-step process utilizing the Stepper component has been introduced to streamline navigation to specific pages through internal links with page IDs. Key features include new buttons, page links, hook configuration, edit mode settings, global form updates, and validation methods.

PKI

The following new feature is included in AppViewX PKI.

- A new widget, **Certificate Usage (Yearly)**, has been introduced to display the yearly certificate count starting from the initialization date, showing the number of certificates issued each year from the reset date.

SIGN

The following new features are included in AppViewX SIGN.

- To improve user experience, a **None** option is added to the timestamping dropdown, allowing users to choose whether to include a timestamp when signing.
- The extension of support for signing document files such as PDFs and Microsoft Office, enables the use of AppViewX CSP with Mage for signing manifest files and the Set-AuthenticodeSignature PowerShell cmdlet for signing Authenticode files.
- From MS Office or Adobe Acrobat, when the SIGN managed code signing certificate is selected from Windows Certificate Store, the signing operation is routed through the AppViewX CSP Library to the SIGN Server.
- The AppViewX PKCS#11 Library is extended to integrate with Cosign for signing and verifying container images, SBOM and blob files. Installer changes include the commands in the README for signing the above file types using cosign.
- The extension of SIGN build artifacts using Script Commands enabled the integration of SIGN with Maven, Gradle, or Ant scripts for signing Java artifacts using the AppViewX PKCS#11 Provider.
- AppViewX SIGN is extended to sign ClickOnce manifest files using Visual Studio and integrate with InstallShield IDE for signing installer files in Windows.
- Added support for custom connector URL in SIGN package download.
- JSign 6.0 supports various file types for signing, including the newly added file types: psm1, psd1, vbe, and jse.

Chapter 2: Enhancements

This section describes the new features in AppViewX v2024.0.0 release.

CERT

The following enhancements are included in AppViewX CERT.

- In SCEP and MS Intune endpoint configuration, the Advanced Settings tab now defaults to enabling High Speed Transactions (set to Yes) and Duplicate Certificate Mitigation specifically for AppViewX PKIaaS CA.
- Added support for forced renewal in the EST client.
- In SCEP and MS Intune endpoint configuration, users can now select RA certificates from any group.
- Device Server Status Synchronization disabled by default and job will do only health check and manage the servers.
- Added HA proxy Enterprise version support for CERT operations.
- Enable commit for the pushed certificate into panorama and Palo Alto shared location.
- During the Apache push, if the app connector contains either a root or intermediate certificate, the content should be combined and placed into the corresponding discovered root or intermediate location.
- The JBoss Linux vendor private key file deletes after being pushed to a device with endpoint CSR generation.
- JBoss vendor relative paths are supported with legacy versions.
- AppViewX supports the following CLM actions for A10 v5.x:
  - Discovery
  - Push only
  - Push and bind.
- The tooltip text for application connectors discovered from Azure includes custom profile metadata. It now shows:
  - Vendor name
  - Tenant ID
  - Resource name
  - Azure service name
  - Device name This enhancement improves metadata readability.
- AppViewX supports Imperva SaaS integration, offering:
  - Certificate push
  - CSR generation.
- The Application Connector for the F5 vendor supports certificate/key file names up to 255 characters.
- Push operation and discovery are supported for A10 devices.

- An enhancement is made to the Upload Temp Path in the exported sheet to include entered details.
- The private key permission in the Cloud Connector is updated to **file owner read-only** and temporary directories created during push and discovery operations are deleted.

DDI

The following enhancement is included in AppViewX DDI.

- The IP search functionality has been optimized with refined algorithms for faster query execution, improved scalability to handle larger datasets, and enhanced accuracy to deliver more precise results and the user interface has been streamlined for better usability and navigation.

SIGN

The following enhancements are included in AppViewX SIGN.

- Dependent ACFs from other modules have been mapped to the SIGN ACF, ensuring automatic activation of related permissions when needed.
- Purging - permanently deletes Signing Inventory data while maintaining accurate license usage counts, reducing database memory overhead.
- HSM Performance Improvements > Fortanix - Introducing parallel signing functionality with Fortanix HSM to meet customer requirements for high-volume signing operations, ensuring enhanced throughput and optimized performance.

PKI

The following enhancement is included in AppViewX PKI.

- An optional parameter, Path Length Constraint, has been introduced for creating subordinate CAs from both PKIaaS root CA and external root CA. This parameter specifies the maximum number of subordinate CAs that can be created under the Issuing CA certificate with the defined Path Length Constraint value.

Platform

The following enhancements are included in AppViewX Platform.

- To address the issue of broken ACLs in reports, a new reports-based ACL feature was introduced. This enhancement ensures that users can access only the reports specifically assigned to them.
- Added custom filter support in grid component.
- Added widget type report support in Pages.

- The upload file API (visualworkflow-file-operation-upload) now supports a maximum download limit, allowing users to securely download files with a single-use link for enhanced security and control.
- IP search is enhanced and optimized.
- In addition to validating workflow input fields in the GUI, form-level regex validation is now performed on the server side to improve security.
- Users can upload .xml files using the generic file upload API.
- Entrust HSM support is enabled for SaaS environment
- As per the Web Content Accessibility Guidelines (WCAG) the Platform GUI is now enabled with keyboard based accessibility
- The license settings page is redesigned with the following changes:
  - A new "Freemium" tag and notification bar for each product.
  - The notification bar now includes a general upgrade option, and a deactivate button for freemium licenses.
  - Product expiry is now displayed in "number of days" format instead of a date.
  - The notification bar is moved to the bottom of the product card, with a generic bar providing upgrade options.
- IP whitelisting is enhanced based on multiple IP addresses too, enabling admins to set up policy for users logging in from public and private networks (by having SSL Inspection).
- In the SSO OIDC login settings, client secret will now be masked on the UI. The show client secret option will be shown only when the value is not masked and the authentication of "modify permission" is present.
- The user password policy is enhanced to allow setting a minimum character requirement for passwords. Currently, this is managed as a backend configuration, and if needed, the TAC team can assist with the setup.

Chapter 3: Bug Fixes

This section lists the fixed bugs in AppViewX v2024.0.0 release.

SIGN

The following bug is fixed in AppViewX SIGN.

- HSM Performance Improvements - Fortanix: Parallel signing functionality with Fortanix HSM was introduced to meet customer requirements for high-volume signing operations, ensuring enhanced throughput and optimized performance.
- The issue where signing through AppViewX SIGN tools using a Service Account was receiving an 'Invalid access token' error after the token expired beyond the configured expiration time in the platform's OAuth settings has been addressed. Now, when the token reaches its expiry, it is properly handled according to the platform's configuration, ensuring uninterrupted access without triggering errors due to token expiration.

Chapter 4: Known Issues

This section lists the known issues in AppViewX v2024.0.0 release.

CERT

The following known issue in AppViewX CERT.

- EC2 discovery status is marked as failed if the discovery process exceeds 20 minutes.
- Certificate push to Azure KeyVault secrets fails when using AES encryption.

Platform

The following known issue in AppViewX Platform.

- Infoblox IPAM sync may get stuck when processing batches with large subnets (for example, /8, /12, /16, /17, /18). Networks are divided into batches of 1000 for synchronization, but when larger subnets are included, the sync process hangs due to Health Probe failures caused by threads exceeding the execution time limit.

Chapter 5: Known Limitations

This section contains the known behaviors, system maximums, and limitations in software in AppViewX v2024.0.0 release.

ADC

The following known limitation is included in AppViewX ADC.

- After upgrading the cloud connecter (CC) to AppViewX v2024.0.0, the Syslog network policy must be updated manually.
- Amazon ELB device is not being managed in the SaaS environment due to a communication issue:
  - **Cloud Device Communication**: For cloud-based devices like Amazon and Akamai, communication occurs via the cloud data center (cloud-dc) in a SaaS environment. Configuring a proxy for these devices is unnecessary.
  - **Firewall Restrictions**: No firewall restrictions are applied to the URLs associated with these cloud devices.
  - **SaaS Device Addition**: When adding these devices in the SaaS environment, ensure the cloud-dc is selected as the data center, and no proxy is configured for the cloud-dc.

CERT

The following know limitations in AppViewX CERT.

- Manual updating of zones for Amazon Public CA is required during the migration from AppViewX v2020.3.0 to AppViewX v2024.0.0.
- In Google Cloud Platform (GCP), the following are the limitations:
  - Rollback functionality is not supported due to private key retrieval during backup is not feasible.
  - Auto-push encounters an error after certificate regeneration/renewal due to GCP's refusal of duplicate certificate names.
  - Certificate map and mapping entries refresh solely after a configuration synchronization is initiated.
  - Push and bind operations are not supported for regional load balancers if they already possess a classic certificate.
  - Push and bind operations are not supported for cross-region internal load balancers.
- To migrate to AppViewX v2024.0.0 from a version older than AppViewX v2023.1.0 FP2, a config sync must be triggered for Azure settings after the migration.
- Certificates that were directly pushed to the app service, api management cannot be discovered; only active certificates in custom domains and those linked via key vaults can be discovered.

- Cloud connector (CC) upgrade to AppViewX v24.0.0.0 is requried for AWS EC2 Linux on-demand discovery operation.
- The ACME DNS challenge validation feature functions correctly only when there is a single nameserver entry in the <resolv.conf> file.
- KDB use cases will fail for the supported vendors when the KDB toolkit version is less than 8.0.50.X and AES Encryption algorithm enabled in AppViewX Cisco ASA push usecase will not support when AES Encryption algorithm enabled in AppViewX IBM Websphere installed server (windows/Linux) should have Java Version 8 SR8 or above when AES Encryption algorithm enabled in AppViewX.

Platform

The following known limitations are included in AppViewX Platform.

- Implemented Report level permission for the users. Object level permissions will not work.
- Email reports is not supported for Global filter dashboard.

SSH

The following known limitation is included in AppViewX SSH.

- The following known limitations are included in AppViewX SSH:
  - Direct terminal access management to AWS hosts is currently not available. Bastion host setup is required and CC/vendors pod needs to be running on the bastion so that AppViewX can connect to the EC2 server via bastion.
  - File transfers and downloads from within the AppViewX terminal to the user client's machine or host machine via the browser is not supported.
  - Unmanaged client downloads do not include the necessary host CA that must be added to the user's client machine. Workaround: Users need to download the host CA and add it to the known host file of the client machine.
  - AppViewX SSH currently supports Cyberark and Thycotic as external credential providers.
  - Only the ECDSA256 algorithm is used for provisioning Host and User CA/SSH certificates, disregarding internal key policy settings.
  - Disabling toggles in Advanced Settings for global configurations does not remove the settings from hosts if already configured; it only prevents newly added hosts from being configured with these global settings.

- The rotate action for keys with associated SSH certificates does not rotate the associated certificates in hosts, therefore the rollback action is not supported for associated SSH certificates.
- The delete from endpoint action for keys with associated SSH certificates does not delete the associated certificates in hosts; therefore, the restore action is not supported for associated SSH certificates.