appviewx

Release Notes

Version: 2023.1.0 FP2 (On-Prem)

Copyright AppViewX, Inc.

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).

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
1.2	AppViewX v2023.1.0 FP2 (On-Prem) Release Notes.	February 2024
1.1	AppViewX v2023.1.0 FP1 (On-Prem) Release Notes.	November 2023
1.0	AppViewX v2023.1.0 (On-Prem) Release Notes.	September 2023

About this Guide

These release notes accompany AppViewX Release v2023.1.0 FP2 for the ADC+, CERT+, PKI, SSH+, KUBE+, SIGN+, DDI+, Platform,Visual Workflow, and FIREWALL+ modules. They describe new feature, enhancements, known and fixedissues, and known limitations in the software.

Intended Audience

- New customers who on-boards to AppViewX v2023.1.0 FP2.

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 v2023.1.0 FP2 release.

ADC+

The following new features are included in AppViewX ADC+.

- Ability to onboard Array Networks of version 10.x into AppViewX inventory and manage the device effectively.
- Users can now import and export Host devices in the inventory for streamlined management.
- Introduction of a custom Model/Type column in the Inventory, providing details of the F5 and Rseries models.
- Support for Nginx new versions R28 and R29.
- Integration of ADC and Firewall Network Topology in ADC+ Application. ADC+ license now automatically includes five complimentary firewall nodes with firewall network mapping capabilities.
- Support for Citrix new version v14.x.

CERT+

The following new features are included in AppViewX CERT+.

- The AppViewX installation includes a set of predefined role-resource-user group configurations to help setup Role-Based Access Control (RBAC) configurations faster. Once logged in, users can map these configurations to corresponding users and make modifications or clones as needed.
- A **Select All** option is introduced for the discovered certificates inventory. This allows users to perform bulk update operations on all discovered certificates for actions such as Manage, Monitor, Ignore, and Exclude.
- The results of the certificate authority discovery scan for Microsoft Enterprise CA can now be filtered using the following discovery parameters:
  - Requester Name
  - Certificate Template
  - Common Name
  - Certificate Effective Date
  - Certificate Expiration Date.
- AppViewX supports discovering and managing certificates in Google Cloud Platform (GCP) environments. This implementation supports the following GCP services:
  - Certificate Manager
  - Load Balancer
  - Classic Certificates.

- AppViewX now supports CLM integration with GCP load balancers. This integration is primarily focused on GCP Certificate Manager and all types of GCP load balancers that support SSL termination. Key features of this integration include:
  - Resource discovery for onboarded GCP projects.
  - Certificate discovery from GCP LB and Certificate Manager.
  - Discovery, CA, and connector operations supported by CERT+.
  - Unbind and remove operations for certificates from the GCP LB / Cert Manager.
  - Platform scope such as audit logs and logs for all discovery and certificate management operations.
- CMP Protocol Implementation: AppViewX is now a standard-compliant CMP provider, capable of accepting requests in CMP/CRMF (RFC 4210/4211) format. It facilitates various CMP protocol request/response mechanisms for certificate retrieval and revocation.

Note: Cloud Connector upgrade is mandatory to access this feature.

- The MS Intune APIs now support HTTPS communication mode for auto-enrollment of certificates. To enable this setup, the app proxy must be enabled.

Note: Cloud Connector upgrade is mandatory to access this feature.

- The MS Intune AEP configuration page includes a "Proxy required" check box for challenge validation via proxy. When this check box is selected, the proxy configured for the corresponding data center will be utilized to connect with Azure AD for challenge validation.

Note: Cloud Connector upgrade is mandatory to access this feature.

- Using the ACME auto-enrollment protocol, you can now revoke certificates using requests signed either with the account key or the certificate private key.
- AppViewX now supports External Account Binding (EAB) in both static and dynamic modes. Configuration can be based on the AppViewX user group, where each user in the group receives a unique credential for account creation. The "External Account Binding" tab is accessible on the ACME configuration page to set up EAB details.
- AppViewX has tailored Posh-ACME to offer expanded functionality to customers beyond the capabilities of the existing Posh-ACME client, catering to diverse business and operational requirements. The enhanced features include:
  - Passing custom attributes from the client.
  - Passing certificate attributes from the client.
  - Passing additional CSR subject parameters such as Organization (O) and Organizational Unit (OU).

- Custom attributes can now be updated for newly created certificates generated via Enroll or Re-Enroll using the ACME clients (Win ACME & Cert Bot).
- AppViewX now features an Application connector for Akamai Certificate Provisioning System (CPS). With this integration:
  - Akamai CPS devices can be onboarded into AppViewX.
  - Users can discover and manage certificates from the Akamai CPS endpoint.
  - CSR generation can be performed at the Akamai CPS endpoint.
  - Certificates can be enrolled using AppViewX, and SSL certificates can be pushed for Akamai edge servers via Akamai CPS.
- Array Networks certificate lifecycle management (CLM) capabilities are integrated into AppViewX. This enables the onboarding of Array Networks ADC devices, offering a range of CLM actions such as device config sync, manual discovery, CSR generation both at AppViewX and at the endpoint, as well as push and bind functionalities.

DDI+

The following new features are included in AppViewX DDI+.

- Microsoft DNS integration
- CSC Registrar integration
- DDI+ now offers IP Hygiene functionality across IPAM and CMDB
- Advanced IP Search capabilities
- Firewall Integration and Correlation
- Domain and DNS Vulnerability Insights
- Extensible Attribute Support for DDI
- Ability to trigger custom workflows for Infoblox Config Sync
- Streamlined user journey for DDI Advanced settings during device addition
- IP Compliance ADC Violation report.

Install and Upgrade

The following new features are included in AppViewX Install and Upgrade.

- Support has been introduced for deploying AppViewX Server in the OpenShift Container platform.
- The RHEL 9 operating system is now supported for AppViewX Server deployment.
- Several components have been updated to their latest versions to address security issues.

KUBE+

The following new features are included in AppViewX KUBE+.

- In the Cluster Inventory, the following functionalities are added:
  - Introduction of a new onboarding mode called Easy On-boarding.
  - Default service and user groups named **kube-svc-account** and **Kube-UserGroup**, respectively, are associated with an Out-of-the-Box (OOB) role to facilitate smooth onboarding.
  - Authentication-less repository is implemented for Helm charts and Docker images, which are pushed to DockerHub for convenient access.
- API integration with the in-cluster component 'cert-orchestrator' deployed in the cluster now includes:
  - Enabling the Push action from KUBE+ UI for Issuer CA and Certificate enrollment YAML (CERT) to the destination cluster.
  - Enabling the Revoke action from KUBE+ UI for Issuer CA and Certificate enrollment YAML (CERT) to the destination cluster.

PKI+

The following new feature is included in AppViewX PKI+.

- Filter options are added to the CA Inventory and Custodian Inventory.

SSH+

The following new features are included in AppViewX SSH+.

- SSH Key Rotation and Deletion Remediation functionalities are now integrated with Visual Workflow, enhancing tracking and troubleshooting capabilities.
- Access request enhancements now allow users to request access for additional users or service accounts, expanding beyond self-access requests.
- Remediation and discovery algorithms are improved to incorporate Global Known_hosts and Authorized_keys. AppViewX now adheres to best practices by pushing rotated keys.
- Role-Based Access Control (Resources) integration with infra access and key groups provides comprehensive ACL support.
- Access Control Framework (ACF) for Access Management Modes (Terminal, Client, and Download) offers granular control over viewing restrictions.
- Users can now download Host CA Trust Certificates with Keys for **unmanaged clients** access mode.
- Security Alerts Analysis and Resolution in SAAS Environments focuses on addressing SaaS security issues and bugs.
- Enhanced Discovery Status now includes failure scenarios with intuitive UX, providing detailed failure information.
- Introduction of **Failed** and **Partially Accessible** status in Access Request Flows informs about provisioning failures.
- Terminal Support for AWS EC2 Linux Hosts via AppViewX Web Terminal is now available.

SIGN+

The following new features are included in AppViewX SIGN+.

- Users now have the option to select their preferred authentication method, which includes both the existing User-Based Authentication and the newly introduced OAuth-Based Authentication (OAuth 2.0).
- A new page called Sign Logs is implemented, providing a comprehensive range of information such as details of code signature creation and updates, digital certificates used in the signing process, timestamps of each operation, and the identity of the signatory.
- In the Policy Page Creation, a new field called **Test Policy** is introduced, allowing users to enable it for internal testing purposes without it being considered in the licensing process.
- Users can now easily select multiple policies while downloading the CSP/PKCS11 Package and perform signing operations using native fragmented signing tools.

Chapter 2: Enhancements

This section describes the new features in AppViewX v2023.1.0 FP2 release.

Automation

The following enhancements are included in AppViewX Automation.

- The Rest external Hook within the Hooks inventory and Form task Hooks now offers support for various authentication types, including:
  - Credential-based authentication
  - Integration as a service authentication
  - Bearer Token authentication
  - API Key authentication
  - AWS signature authentication
  - Akamai EdgeGrid authentication
  - OAuth 2.0 authentication.
- Provision to incorporate Akamai Edge Grid authentication support in the command repository, allowing routing of SAAS REST API for Akamai devices through the Cloud Connector (CC).
- Implementation of dedicated sandbox pods for script execution in on-premise deployment during FP2, enhancing security. The introduced python sandbox pods include:
  - avx-python-sandbox
  - avx-python-sandbox-sync
  - avx-python-sandbox-development
  - avx-python-sandbox-development-sync.
- A new configuration is introduced, enabling the API to filter results based on the user's Access Control Framework (ACF) permission in the current palette view request.
- The capability is added to include default vendor configurations for all integrated vendors in both the integration and DDI (DNS, DHCP, and IPAM) inventory.
- Microsoft and CSC vendors have been added to the integration hub and DDI (DNS, DHCP, and IPAM) inventory. Furthermore, support is extended to Config Sync and Delete Trigger Function for new Integration Hub Vendors such as Microsoft and CSC.

CERT+

The following enhancements are included in AppViewX CERT+.

- The expiry alerts feature is enhanced to allow:
  - Creation of alerts for CA certificates (previously limited to end certificates only).
  - Generation of tickets in ITSM tools (ServiceNow and JIRA) corresponding to the certificate expiry alerts.
- The certificate attribute values can be updated in bulk for server, client, code signing, and device certificates.

> **Note:** Before initiating a bulk update of certificate attributes, ensure that no updates are made to certificate attributes involved in an expiry alert.

- French language support is added for text fields in certificate discovery and custom reports.
- You can now upload a new CSR when renewing certificates issued by Microsoft and Entrust CAs, provided that the common name of the new certificate matches the existing one.
- Certificate discovery in Azure environments can now be initiated at multiple levels, including the settings level, subscription level, service level, and resource level, allowing for greater flexibility and granularity. Users can choose to initiate discovery for one or more subscriptions, resource types, or individual resources.
- Automatic synchronization (auto sync) with the AppViewX inventory is now enabled for Azure cloud environments. The synchronization can be scheduled at the setting level (as a midnight config sync) or at the service level.
- When adding connectors to push certificates into an Azure cloud environment in AppViewX v2023.1.0 FP2 and beyond, users can now:
  - Select the Azure service type to which the certificate will be pushed. Available service types include key vault, application gateway, and virtual machines.
  - For the application gateway service type, users can select the target profile to which the certificate will be pushed. Available target profiles include gateway SSL profile, gateway listener profile, and gateway back-end settings profile.

> **Note:**
> - After migrating to AppViewX v2023.1.0 FP2 and beyond, manually trigger a config fetch for all existing Azure accounts to ensure that all functionality enhancements are applied correctly. Delete all on-demand and scheduled discovery instances created for Azure and, post a successful config fetch, create a new discovery instance.
> - After migrating to AppViewX v2022.1.0 and beyond from any previous version, users must enter the data center details for each existing Azure account.

- All user activity, including cloud device addition, modification, deletion, manual discovery, connector actions, certificate enrollment, and more, in MultiCloud use cases is now tracked and logged as events. These logs can be utilized for debugging, monitoring, and security and auditing purposes.
- Idnomic CA auto enrollment, re-enrollment and revoke is now available with existing ACME, EST, SCEP, and MS Intune auto enrollment protocols.
- AppViewX has implemented standardization across fields for enrolling certificates and application connectors, along with support for managing Apache Linux servers without requiring access elevation:
  - **None** is added as one of the available Access Elevation options.
  - A single field is now used to store both file name and location, eliminating separate fields for CSR, private key, and certificates.
  - Several fields are removed in the App connector, including **Certificate directory**, **Key file directory**, **Intermediate and CA Certificate Directory**, and **Customize push location**. Additionally, field names are updated:
    - Certificate File Name to Certificate Location
    - Key File Name to Key Location
    - CA Name to Root Location
    - Intermediate File or Bundle Name to intermediate Location.
  - On the Enrollment page, the 'CSR Location' field is removed and the field names are updated:
    - CSR File Name to CSR File Location
    - Key File Name to Key File Location.
  - AppViewX now supports managing NginxPlus devices within the Nginx environment, including soft reload functionality, and also enables file parsing without requiring any extension.
  - AppViewX has introduced the option for "service restart" after any push or roll back operation performed on HAproxy servers. This feature is implemented based on customer selection.
  - When certificate keys are newly pushed into the Apache server, the file permissions for the owner are now set to read-only. Other users can not access to these keys.
- AppViewX has included the following certificate groups in the default certificate groups provided with the platform:
  - Private Certificates
  - Public Certificates.
- Bulk updates for certificate attribute values are now supported for server, client, code signing, and device certificates.

Note: Before you bulk update the certificate attribute values, review the attribute and expiry configuration mapping to prevent errors. For attributes that are included in expiry alert configurations, ensure that the updated value is of the same type and format as the original

value (for example, email ID attributes should be updated with a relevant email ID only and not any text value).

- As part of the Azure Gateway enhancements, support for V2 SKUs (Standard V2/WAF V2) is enabled, in addition to the existing support for V1 SKUs.
- Enhanced the Azure Application Gateway Services to enable CLM action for V2 gateways along with the V1 gateways. Users will now be able to discover SSL certificates, manage SSL certificates and perform CLM actions on both V1 and V2 gateways, with the azure account on-boarded with application gateway in AppViewX.

Platform

The following enhancements are included in AppViewX Platform.

- Enhanced Single Sign-On functionality now supports the encryption of SAML assertions.
- A new feature enables bulk export and import of user roles.
- Users can now opt to include or exclude the domain name in the username during synchronization from the Identity Provider.
- Added the option in the Password Policy to set Password Expiry for local user accounts.
- Introduced an option in the Password Policy to prevent users from reusing recent passwords.

SIGN+

The following enhancements are included in AppViewX SIGN+.

- AppViewX has implemented the Email notification toggle switch in the Signing Policy page, allowing users to enable notifications and updates to be sent out to specific users when a signing event occurs.
- Users now have the capability to download multiple levels of CA Certificate based on dynamic OS selection.
- AppViewX now supports ECC Key Based Signing (P-256, P-384, and P-521) when using the AppViewX PKCS#11 Provider with SIGN+.
- The following SIGN+ module's GUI is enhanced:
  - Automatic selection of a certificate in the dropdown menu when only one certificate is mapped to a signing policy, eliminating the need for user input.
  - Improved intelligence of IP range validation to ensure that the end IP is greater than the start IP.
  - Filtered policy list based on the chosen type (For example, File Based Policy and Hash Based Policy), displaying allowed file types for the selected policies.
  - During policy creation, only selected file types are allowed for upload in the Upload File feature.
- AppViewX has extended support for the existing SIGN+ installer to include Linux and MacOS platforms.

- The PKCS#11 Library is compiled for various Linux distributions and MacOS, broadening its usage across different Linux-based CICD Pipeline Servers and Client machines.
- AppViewX has upgraded to JSign 5.0 to support Pod Separation changes.
- SIGN+ is now accessible in the Managed Kubernetes setup.

Chapter 3: Bug Fixes

This section lists the fixed bugs in AppViewX v2023.1.0 FP2 release.

Automation

The following bugs are fixed in AppViewX Automation.

- Resolved the EIS issue with Broken ACL (11), addressing Design and Request related API.
- Resolved on-prem Remote Code Execution (RCE) related issue (30) through the implementation of dedicated Python sandbox pods for script execution.

ADC+

The following bugs are fixed in AppViewX ADC+.

- Resolved the issue with EIS - Broken ACL (8), addressing ACL restrictions for the delete and update API.
- The issue related to storing device backups for an extended duration is resolved.
- The issue related to ADC working sessions and F5 backup emails displaying 'NA' and 'Failure' despite the backups being visible in the GUI is resolved.
- Resolved issue with the incorrect reporting of Citrix VIP details using Query Explorer Hook.
- Resolved the object restore issue with sub-objects such as profile and monitor.
- Resolved a user-reported issue concerning the export of device information from the inventory when the device count exceeds 100.
- Support is provided to resolve the Internal server error in the Topology view in Control Center. Additionally, enhancements include the ability to perform traffic routing for v10 and v11 device GTM Pool objects, as well as the configuration option to set the number of Recursive VIP levels in the Topology view.
- Resolved the issue by adding fields in Query Explorer to expose the Self IP field of a device and list all the Dashboards for a user.
- Resolved an issue where the Device Backup Summary email incorrectly indicated **Success** for a failed backup instead of **Failure** when the email sending option with the Summary option was selected.
- Resolved the issue of needing SDK support to create VsVip in AVI devices. A fix has been provided to include the intent modify-vsvip-name for AVI. Additionally, the request to add a config fetch API in the internal REST palette has been addressed.

CERT+

The following bugs are fixed in AppViewX CERT+.

- The certificate renewal process is modified to incorporate case insensitivity for the certificate common name and DNS matching criteria. Previously, due to strict matching criteria applied to the Common Name field in the CSR parameters, certificate renewal requests failed due to discrepancies in the letter case. The case insensitivity adjustment will allow for a more flexible and error-tolerant renewal process.
- The compliance check for root and intermediate certificates now excludes the common name check. The compliance check is executed when the **Validate issuer and root certificate for compliance** feature is enabled in a CA policy.
- The issue of policy record count mismatch between the Policy Compliance Report and the Server Inventory Dashboard is resolved.

Chapter 4: Known Issues

This section lists the known issues in AppViewX v2023.1.0 FP2 release.

Automation

The following known issue in AppViewX Automation.

- The rollback work order will display the same work order ID as the original work order.

CERT+

The following known issues in AppViewX CERT+ .

- In Google Cloud Platform environments, not all discovered certificates are associated with groups.
- If the Google Cloud Platform (GCP) configuration synchronization fails for a specific project and service, users can trigger the configuration sync again for that project and service directly from the user interface (UI).

DDI+

The following known issues in AppViewX DDI+ .

- When extensible attributes are deleted, the corresponding key does not get removed from the domain inventory.
- When selecting the domain lifecycle breadcrumb while triggering any workflow under domain lifecycle, the automation side menu appears instead of the DDI+ Menu.
- The **In-Progress** status is not displayed during Infoblox config sync.

SSH+

The following known issues in AppViewX SSH+ .

- When ACF for the infrastructure access group is disabled, users can create a custom infrastructure access group using the **Type** and **Create** feature on the host addition pages. The user who creates the group can view or use the group only if the default or custom regex matches the group name.
- Access requests made using keys do not have an expiration based on the access duration provided. This means that client and unmanaged client-based access requests will continue to function without any expiration, regardless of the access duration specified.

Chapter 5: Known Limitations

This section contains the known behaviors, system maximums, and limitations in software in AppViewX v2023.1.0 FP2 release.

Automation

The following known limitations are included in AppViewX Automation.

- When executing a specific request, if pods are restarted, the Workflow Request remains in the in-progress state.
- Parallel execution of Child Workorders inside a loop is not supported.

CERT+

The following know limitations in AppViewX CERT+ .

- AppViewX does not support backup and rollback functionality as part of the Array networks CLM since the discovered private key is in the encrypted format.
- In Google Cloud Platform (GCP), the following are the limitations:
  - Pushing certificates to the Certificate Manager and binding them to Classic Load Balancers in the standard tier is not supported.Rollback functionality is not supported due to the inability to retrieve the private key during backup.Auto push after regeneration/renewal of certificates throws an error since GCP does not accept duplicate certificate names.
  - Certificate map and certificate mapping entries are refreshed only after a config sync is triggered.
  - Push and bind operations are not supported for regional load balancers if they already have a classic certificate associated with them.
  - Push and bind operations are not supported for cross-region internal load balancers.
- SHA224 is not supported by Signtool.
- SHA1 and SHA224 are not supported by Nuget tool.
- ECC Key Based Signing is not supported by Nuget tool.
- Hashing Algorithm/Timestamping URL cannot be specified in APK Signer.
- SHA-1 for jarsigner gives a warning as Warning: The SHA1withECDSA algorithm specified for the -sigalg option is considered a security risk and is disabled.
- SwissSign timestamp will not get verified in Signtool as Signtool uses authenticode verification by default.
- Signing PowerShell script files with Unicode characters using JSign fails on digital signature verification.
- HSM support for <.cat> file is not supported.

SSH+

The following known limitations are included in AppViewX SSH+.

- If a certificate is discovered and its corresponding Certificate Authority (CA) is not found in the AppViewX SSH CA inventory, then the CA name will not be mapped in the certificate. Additionally, such certificates cannot be renewed, revoked, or rotated within AppViewX.
- In CERT+ server inventory and AWS cloud account addition, Access Type is not supported and defaults to certificate-based access.
- The remediation delete action for mis-configured host keys lacks a rollback feature, which might lead to SSH connection failures in future attempts.