appviewx

Release Notes

Version: 2023.1.0 FP1 (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
1.0	AppViewX v2023.1.0 FP1 (On-Prem) Release Notes.	November 2023

About this Guide

These release notes accompany AppViewX Release v2023.1.0 FP1 for the ADC+, CERT+, PKI, SSH +, KUBE+, SIGN+, 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 FP1.

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 FP1 release.

CERT+

The following new features are included in AppViewX CERT+.

- For Entrust CA, AppViewX now allows you to enable/disable publishing certificate data content to Certificate Transparency (CT) Log server.
- CERT+ Demo mode (RBAC driven) allows user to experience the CERT+ offerings based on their RBAC permission. Users are allowed to view the forms, reports, inventory, and CLM actions.
- PaloAlto Version 11.0 is now supported, allowing users to include the purpose when performing a certificate push action.
- SSH Key integration: Passphrase support is enabled for all vendors when the credential type is SSH, users can enter the passphrase/password for private keys.

FIREWALL+

The following new features are included in AppViewX FIREWALL+.

- Parsing for CheckPoint SMS and FortiManager managed devices' Interfaces and Static Routes.
- Support for PaloAlto Version 11.
- Backup and Restore feature for PaloAlto and Fortigate Firewalls.
- Enabler for Panorama parsing.
- Support for parsing Fortigate Rule objects with API tokens.

KUBE+

Simplify SSL/TLS certificate management in Kubernetes using KUBE+. The KUBE+ introduces seamless automation for the lifecycle management of certificates, effortless integration with Kubernetes resources, and strong support for multiple Certificate Authorities (CAs). Secure your applications with ease and achieve crypto-agility through simplified PKI policies. Using KUBE+ ensure hassle-free certificate management for your clusters.

The following new features are included in AppViewX KUBE+.

- You can now download certificates and keys from the AppViewX certificate inventory to Kubernetes cluster secrets and Kubernetes pods.
- Keys are discovered alongside certificates from Kubernetes secrets.
- The CSR generation for certificate enrollment into pods and secrets can be accomplished now at the AppViewX end.

- If the secret already exists during certificate enrollment, it is possible to overwrite the secret's content with the newly enrolled certificate.
- Replicas, pod tainting, and health probes are introduced for the Cert-Orchestrator pod.
- Certificates that are auto-enrolled into secrets via the CLI, by directly applying YAML without generating it from the UI, will now be accessible in the Server Apps Inventory.
- Newly onboarded clusters can now be automatically managed by setting the **enable auto approval** to true in the cluster settings.

Platform

The following new features are included in AppViewX Platform.

- SCIM Support: Introduced a System for Cross-domain Identity Management (SCIM) support to enable seamless provisioning, synchronization, and de-provisioning of users and user groups from your Identity Provider to AppViewX.
- MS Sentinel Integration: Added an integration with MS Sentinel, enabling the forwarding of logs from AppViewX.
- Service Account Integration: You can now utilize Service Accounts from their own Authorization Server with AppViewX.

PKIaaS

The following new features are included in AppViewX PKIaaS.

- PKIaaS is now enabled with alert and monitoring for the following use cases:
  - GCP connectivity
  - Project availability
  - Credential validation
  - CA status.

SSH+

The following new features are included in AppViewX SSH+.

- Access Duration Customization: You can now specify access duration in either hours or days when requesting access to an infrastructure group, providing enhanced access management control.
- Enhanced SSH Certificate Discovery and Display: Boosted the SSH module to discover and display SSH certificates alongside SSH keys, offering a more comprehensive overview of your security credentials.
- Key Download for Unmanaged Client Access: You now have the capability to download keys for key-based access control, ensuring streamlined access management.

- Dynamic Access Flow Based on Access Mode: Introduced a dynamic access flow that adapts to either key or certificate-based access, based on the user's selected **Access Mode** during host addition.
- Simplified Host Certificate Rotation: You can effortlessly rotate host certificates directly from the host inventory, promoting secure host certificate management.
- SSH Certificate Revocation: A new revocation option has been introduced in the SSH User Key Inventory allowing users to revoke SSH certificates directly and thus enhancing security control.
- Choice Between 'Key' and 'Certificate' Access Modes: You can now choose **Key** and **Certificate** access modes during host addition, with the 'Certificate' option being pre-selected by default.
- Host Update with KRL File Location: Improved the host addition process to update the host with the Key Revocation List (KRL) file location, bolstering security, and revocation management.
- Renaming 'Jump Server' to 'Client': The term **Jump Server** is replaced with **Client** across the product for a more intuitive representation.
- Efficient Key Rotation and Deletion from Hosts with Multiple Keys: You can now easily rotate and delete keys from hosts with multiple keys through the user and host key age report.
- Enhanced Key Deletion Safeguards: Implemented measures to prevent the accidental deletion of host keys on endpoints with only one key, ensuring smoother and safer operations.

SIGN+

AppViewX has introduced SIGN+, an application designed to enhance code signing capabilities across a wide range of tools and DevOps pipelines. This release of SIGN+ provides you with a versatile and efficient code signing solution, enhancing your development and security processes.

The following new features are included in AppViewX SIGN+.

- Streamlined Code Signing: Simplify Code Signing Certificate enrollment and Certificate Lifecycle Management (CLM) operations.
- Configurable Signing Policies: Enjoy highly customizable signing policies tailored to your specific needs.
- Integration with AppViewX's CSP and PKCS#11: Seamlessly integrate with AppViewX's customized Cryptographic Service Provider (CSP) and PKCS#11 for enhanced security.
- Comprehensive Signing Inventory Management: Efficiently manage your code signing inventory with a full suite of tools and features.
- Multi-Tool Code Signing Support: Sign your code effortlessly using a variety of tools including SignTool, JSign, JarSigner, APKSigner, and Nuget.
- TSA Compatibility: Ensure compatibility with third-party Timestamp Authorities (TSA) for a wider range of options.

Visual Workflow

The following new features are included in AppViewX Visual Workflow.

- Integration of a new design for the service catalog.
- Enhancements to the UI/UX for VWFs.
- The ability to hide the Loop Palette in the workflow.
- Proxy support added to the Command Repository.

Chapter 2: Enhancements

This section describes the new features in AppViewX v2023.1.0 FP1 release.

Automation+

The following enhancements are included in AppViewX Automation+.

- The service catalog now features a fresh design and integrated forms. This update introduces a new catalog view and an enhanced request journey for VWFs.
- The UI/UX enhancements for VWFs include improved layout design for the service catalog on multiple pages. It also offers enhanced customization options for service catalog properties, including icons, titles, descriptions, colors, and fonts, with the ability to modify and show/hide them.
- To Hide the Loop Palette in the Workflow, you can configure the Hide option within the loop task properties. This option is initially disabled for the task, but you can enable it as required.

ADC+

The following enhancements are included in AppViewX ADC+.

- Enhanced FQDN support for WAF devices is now available.
- Introduced a drag-and-drop method for rearranging application and data center lists within the Traffic Grid Widget.
- Included a new **Alias Name** field within the Traffic Statistics Widget, allowing users to add custom names to the widget.
- Added support for onboarding WAF-supported vendor devices using FQDN.
- Implemented pagination for backup group devices and introduced device name search functionality.

CERT+

The following enhancements are included in AppViewX CERT+.

- With Entrust CA, AppViewX now allows you to refine the results of the CA Discovery Scan based on certificate type and certificate status.
- Self-signed certificates will now be categorized in the server/client certificate inventory, improving their differentiation from Root certificates. This change may potentially affect the license count.
- Certificate Enrollment with GlobalSign CA now includes the provision for domain-based validation.

PKI+

The following enhancements are included in AppViewX PKI+.

- Service Account Configuration Support: In this release, we've updated PKIaaS Initialization to seamlessly support provided service account configurations. This enhancement streamlines the onboarding process and ensures a smoother setup experience.
- CA Deletion Enhancement: PKIaaS now offers advanced CA deletion support. You can perform a CA hard delete, disregarding active issued certificates. This feature provides greater flexibility and control when managing your CAs.
- Complimentary CA Support: The introduction of complimentary CA support expands the options available to users and enhances the range of services within PKIaaS, making it even more versatile for your certificate management needs.

KUBE+

The following enhancements are included in AppViewX Kube+.

- Users now have the ability to define custom certificate file names and passwords for enrolling certificates into pods.
- A delete option has been introduced for all inventories in Kube+.

Chapter 3: Bug Fixes

This section lists the fixed bugs in AppViewX v2023.1.0 FP1 release.

There is no bug fix in this release.

Chapter 4: Known Issues

This section lists the known issues in AppViewX v2023.1.0 FP1 release.

KUBE+

The following know issues in AppViewX Kube+ .

- When pod certificates are auto-enrolled directly via CLI without generating YAML from the GUI, those certificates will not be available in the Secure Apps inventory.

Platform

The following know issues in AppViewX Platform.

- When making a request to the login API without including the username in the header, the displayed possible cause alongside the response message appears unnecessary. It should either provide meaningful information or be shown only when there are additional details regarding the error.
- The alignment of the theme header logo is incorrect when a custom header logo is not uploaded.
- With MFA enabled, it is advisable to disable the "Resend OTP" button on the authentication page when a user does not have a mapped user group.
- Encountering a 500 Internal Server Error (ISE) instead of the expected 401 Unauthorized status when authentication fails due to an invalid Authorization Basic token.
- Deletion or removal of the admin user group and admin role should be restricted and disallowed from both the tenant admin and general admin interfaces.

Chapter 5: Known Limitations

This section contains the known behaviors, system maximums, and limitations in software in AppViewX v2023.1.0 FP1 release.

KUBE+

The following known limitations are included in AppViewX KUBE+.

- Cache is retained in the certificate orchestrator for certificates that have already been uploaded. Consequently, if a certificate that was previously discovered is deleted in AppViewX, it will not be rediscovered.

  Workaround: To retrieve the certificate in AppViewX, you should delete the Secret Cache and restart the certificate orchestrator pod.

- You cannot overwrite certificates when enrolling them into a Secret that was created by downloading a Certificate (CertLoad CRD).

  Workaround: To enroll the certificate with the same Secret Name, delete the CertLoad Object associated with the Secret and then proceed with the enrollment.

SSH+

The following known limitations are included in AppViewX SSH+.

- Access requests using keys will not expire based on the provided access duration.
- If a certificate is discovered, and the Certificate Authority (CA) used to create it is not in the AppViewX SSH CA inventory, there will be no associated CA mapping after discovery.
- Access Type is not supported for CERT+ server inventory and AWS cloud account addition; they will default to certificate-based access.
- For discovered certificates with CAs not available in the AppViewX SSH CA inventory, certificate revocation action is not possible in the user key inventory.
- The remediation delete action for misconfigured host keys does not have a rollback feature, potentially leading to SSH connection failures in subsequent attempts.
- Unmanaged client access requests only support certificate-based access.

SIGN+

The following known limitations are included in AppViewX SIGN+.

- Requests are being triggered twice when requesting the signing of files using the Mage tool.