appviewx

Release Notes

Version: 2023.1.0 FP3 (On-Prem)

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.....iv

Chapter 1. New Features.....6

Chapter 2. Enhancements.....14

Chapter 3. Bug Fixes.....21

Chapter 4. Known Issues.....22

Chapter 5. Known Limitations.....24

Preface

Revision History

Revision	Description	Date
1.4	AppViewX v2023.1.0 FP3 (On-Prem) Release Notes, updated the CERT Bug section.	June 2024
1.3	AppViewX v2023.1.0 FP3 (On-Prem) Release Notes.	June 2024
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

• Customers who on-boards to AppViewX v2023.1.0 FP3.

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.
Convention	**Description**
`codeblock`	Indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Convention	Description
`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 FP3 release.

ADC+

> **Note:** As part of application upgrade, all F5 customers are expected to place the axis.jar as an additional dependency for the iControl.jar.

The following new features are included in AppViewX ADC+.

BIG-IP Distributed Cloud (XC) Basic Integration: Enables customers to deploy and operate their applications in a cloud-native environment, whether on their network, in a data center, or across multi-cloud (pure SaaS/hybrid) setups. This offer includes:

- **Integration and Management**:
  - AppViewX can integrate with F5 XC Services.
  - Centralized management of distributed applications and DNS management.
  - Automated discovery of HTTP, TCP, and DNS load balancers from the services.
- **Application Visibility and Troubleshooting**:
  - App-centric visibility of applications across cloud services.
  - Monitor and troubleshoot application issues through the Control Center (CC) and Database (DB).
- **Application Provisioning and Certificate Management**
  - Provision HTTP/TCP applications with custom certificate creation.
  - **Supports pure SaaS** - Remote Execution (RE) for the management of applications on the cloud.
  - **Supports hybrid SaaS** - Combined Execution (CE) for the management of applications on both cloud and on-premises environments.

F5 Velos Controller/Partition Management: ADC+ now offers support for the following:

- **Inventory and Service Discovery**:
  - Centralized management of F5 BIG-IP Velos Controllers, Partitions, and Tenants.
  - Automated discovery of tenants and high availability (HA) configurations from hosts.
- **Configuration Management and Compliance**:
  - Automated configuration backup and recovery.
  - Automated configuration compliance and vulnerability detection.
- **Application Visibility and Insights**:
  - Application-centric visibility across multi-vendor infrastructure.
  - Monitoring and troubleshooting of application issues.

- **Traffic Management**:
  - Dynamic traffic management and routing of application traffic for disaster recovery (DR).
  - Business continuity through Blue/Green swing and Canary deployment.
- **Self-Service and Automation**: Application provisioning for load balancing (LB) and global server load balancing (GSLB).

Netscaler to F5 Migration: Facilitating a shift in application delivery infrastructure for business continuity and migration from Netscaler to F5. Traditionally, this has been a manual and time-consuming process, but now it is automated through AppViewX. The key functionalities are:

- **Automated Configuration Migration**: Migrate configurations from Netscaler to F5 BIG-IP.
- **Supported Versions**: Netscaler v11 & above to F5 BIG-IP 12 & above (including rSeries and Velos).
- **Modules**: GSLB and SLB.
- **Migration Methods**:
  - Migration of standard SLB & GSLB Netscaler configurations to F5 via CLI.
  - Migration of basic SLB Netscaler configurations to F5 via AS3.
- **Migration Process**:
  - **Review Migration**: Evaluate the migration percentage, supported vs. unsupported parameters, and review changes before proceeding.
  - **Go-Live and Application Readiness**: Ensure application traffic cutover and obtain sign-off from application owners for the final go-live.

Unused Closed Loop Decommissioning: The unused object monitoring and closed-loop decommission enhancements ensure efficient resource management by identifying and removing unused objects, thereby reducing potential configuration errors. The key features include:

- **Automated Monitoring and Decommissioning** - Disabled objects are monitored for a user-specified time interval before deletion.
- **One App Dashboard Integration** - Includes reports covering WiP and VIP objects with decommissioning options.
- **Closed-Loop Remediation** - Multiple objects can be decommissioned simultaneously via the dashboard.
- **Database and Device Synchronization** - Decommissioned objects are removed from the AppViewX database, and devices are configured to reflect the latest data.

Multi HA Software Upgrade: The Multiple HA Pairs (Parallel Software Upgrades) via Controller Workflow enables efficient and streamlined upgrades for multiple HA devices simultaneously, reducing downtime and ensuring a seamless transition to the latest software versions. The key features include:

- **Controller Workflow**: Upgrade up to 6 HA device pairs in parallel, enhancing efficiency and minimizing upgrade time.
- **Out of the Box (OOB) Solutions**
  - Automates the F5 BIG-IP upgrade process from version 11.x to the latest, specifically tailored for HA pairs.
  - Includes image transfer, installation, and device reboot processes.
  - Ensures all necessary pre-upgrade and post-upgrade checks are performed for a smooth and error-free transition. Seamless Integration.
- The workflow is designed to integrate seamlessly with existing AppViewX infrastructure, providing a reliable and efficient upgrade process.

> **Note:** Each request will have a two-to-five minutes delay before firing. A typical HA upgrade takes approximately 1.5 hours to complete.

ADC+ Freemium Support: ADC+ Freemium support allows customers to seamlessly experience the value from cross-products and improves cross-sell opportunities. Key features include:

- **Activation Flexibility**: ADC+ Freemium plan can be activated on top of any product line.
- **Availability**: Applicable to all SaaS production customers.
- **Feature Access**: All SaaS-supported ADC features will be available for use with a usage restriction of 10 ADC nodes.
- **Onboarding Experience**: Users will be provided with a quick onboarding experience to get started.
- **LB Sync Enablement**:
  - Cert production customers with existing ADC devices can enable LB sync for a maximum of 10 ADC nodes upon Freemium enablement.
  - LB sync allows AppViewX to manage the end-to-end configuration of an ADC device.
- **Upgrade Path**: The Freemium plan can be upgraded to a production license from the product.

CERT+

> **Note:** As part of application upgrade, all F5 customers are expected to place the axis.jar as an additional dependency for the iControl.jar.

The following new features are included in AppViewX CERT+.

Support for CSC Global CA

- Onboard the CSC Global CA in AppViewX.
- Discover CSC Global CA certificates using on-demand and scheduled discovery types
- Filter results of the certificate authority scan for CSC Global CA using the following discovery parameters:
  - Certificate status
  - Certificate types
  - Certificate effective date
  - Certificate expiration date.
- You can select a combination of discovery parameters, but you can only choose one parameter from either the certificate effective date or the certificate expiration date.
- Perform the Enroll, Renew, Revoke, and Reissue CLM actions for CSC Global CA certificates.

Introduced the Insights Menu

- AppViewX has now introduced the Insights menu. The INSIGHTS menu provides comprehensive information and analytics on the overall certificate summary, operations, risk and crypto, and the Google 90-Day report, delivered through the CERT+ infrastructure.

- **Insights > Summary**: The Insights Summary report presents a concise overview of the Inventory Snapshot, Crypto Score, Certificates Expiry, and Certificates by type and issuing CAs managed within AppViewX.

- **Insights > Operations**: The Insights Summary report presents a concise overview of the Operations Snapshot, Certs based on Scan, Crypto Score Trend, Managed Status, Crypto Score Trend, CLM Action Trend, Auto Renewals, and Auto Enrollment Trend managed within AppViewX.
- **Insights > Risk and Crypto**: The insights Risk and Crypto report presents a concise overview of the Crypto Score, Non-standard certificates, managed within AppViewX. It helps administrators monitor and maintain the security posture of certificates throughout their life cycle, identifying potential vulnerabilities or weaknesses that may need to be addressed.
- **Insights > Google 90 Day**: The Google 90-day certificate refers to Secure Sockets Layer (SSL) certificates issued by Certificate Authorities (CAs) in accordance with Google's guidelines on certificate validity periods. This dashboard displays the reports related to certificate scores, server certificate age, issuers, key algorithms, and key lengths, adhering to the guidelines set by Google for 90-day SSL certificates.

Integrated the Microsoft Exchange server as a Service

- Options and flexibility to select services as either MSServer or Microsoft Exchange server.
- Support for existing data by using MSService as the default service.

- If no services are selected, the implementation will default to MSServer. Thus, during configuration fetching and discovery, certificates will be discovered from MSServer.
- Addition of a profile connector for the Exchange server.
- Discovery of certificates from the configured services.
- CSR generation from endpoint, Push, and Bind workflows are enabled from AppViewX for MSExchange.
- Certificate push and bind support for POP, IMAP, SMTP, and IIS services.
- A new "Service Names" column has been added to the Imported Server File. The expected service names are MSServer and ExchangeServer (comma-separated values if both are entered).

Introduced the following support for IoT

- The ACME protocol now includes functionality for Suspend and Activate actions.
- The winacme client is enhanced to support custom attributes, certificate attributes, and additional CSR subject parameters.
- Newly enrolled certificates via auto-enrollment protocols will now be automatically added to the monitored status within the AppViewX inventory.
- Support for SwissSign CA has been added to ACME, EST, SCEP, CMP, and MS Intune protocols.
- Support for EST on macOS clients.

Introduced the following support for Multi-Cloud:

- Support for onboarding of new service "App Services " and discovery of certificate and profiles from it .
- Support for ondemand certificate discovery from App Services.
- Support for auto sync options for the added Azure Devices and their services.

- Expired/revoked certificates can now be moved to the **Monitored**state (from the **Managed** state). After renewal/reissue/regenerate, old certificates can be moved to the **Monitored** state (from the **Managed** state).
- For DigiCert CA, the division assigned to a certificate can now be displayed in the certificate. By default, the division is not displayed. It can be enabled for display manually.

AppViewX introduces support for the SwissSign MPKI CA with the following capabilities:

- Onboard the SwissSign MPKI CA in AppViewX.
- Discover SwissSign MPKI certificates using on-demand and scheduled discovery types.
- Perform the following CLM actions for SwissSign MPKI certificates:
  - Enroll
  - Revoke

  - Generate CSR
  - Upload certificates
- Access alerts and audit logs for SwissSign MPKI certificates.

DDI+

The following new features are included in AppViewX DDI+.

- Introduced the Application Topology Menu, allowing you to search for application FQDNs and gain visibility into the application's network infrastructure, including DNS, load balancers, firewall NAT rules, and pool members.
- Added Bluecat DDI+ integration with support for IP compliance, ServiceNow integration, and DNS management.
- Enhanced Firewall Correlation support for DDI+ with Checkpoint and PaloAlto.
- Added AVI and Citrix vendor support for ADC-DDI correlation.
- Implemented Cloudflare DNS Integration for DNS management and automation.

KUBE+

The following new feature is included in AppViewX KUBE+.

- **Auto Deploy PKI Policy**: Rule-driven cluster onboarding to automatically enforce PKI policy on clusters.
- **Offboard Policy**: Enables administrators to remove or offboard all metadata related to the cluster and associated settings in both the cluster and AppViewX when the cluster is deleted. This ensures a thorough and clean removal process, maintaining data integrity and security by eliminating residual configuration and metadata.
- **Dynamic Group Updates**: Enables the automatic deletion of groups in the Certificate Inventory when the corresponding namespaces are deleted at the cluster end. This ensures that the inventory remains up-to-date and free of obsolete groups, streamlining certificate management and maintaining organizational clarity.
- **All Certificates Inventory**: Enables administrators to view and manage certificates across cloud, containers, and on-premises environments from a single console. By clicking the "All Certificate" option, users can access a consolidated view of all certificates, simplifying management and oversight.
- **Beta Support for SSL Certificate Remediation**: Introduces beta support for SSL certificate remediation for certificates discovered from Kubernetes. Users can now switch the Certificate Authority (CA) or renew certificates based on their expiry dates, enhancing security and ensuring timely certificate updates.

Platform

The following new feature is included in AppViewX platform.

- AppViewX now supports Entrust Hardware Security Module (HSM) for enhanced cryptographic operations and key management.

SSH+

The following new features are included in AppViewX SSH+.

- Introduced the Access Control Lists (ACL) for hosts using the app infra groups: Hosts are now manageable resources with read/write permissions through the Platform's ACL page.
- Restoration of Deleted Keys: Keys deleted from endpoints can be restored from the new **Recently Deleted Inventory** within a 30-day period.
- Automated Removal of Public Keys for Expired Key-Based Access: A cron job is now triggered to remove the public key of expired access requests from endpoints.
- Automated Renewal of Host Certificates: A cron job is now triggered to rotate host certificates before their configured expiry date in the key policy under Host Certificate Auto Rotate Settings.
- Revocation of Access Requests: Access Requests can now be approved, rejected, and revoked from the new Access Request Hub page.
- Revocation of Access for Hosts Removed from Infra Access Groups: When a host is transferred from one group to another, active access requests from the old group are revoked for only that host.
- Backup & Rollback of Rotated Keys: Added ability to backup keys before rotation, enabling users to roll back to the old key from the key inventory.

SIGN+

The following new features are included in AppViewX SIGN+.

- SIGN+ now allows you to upload a code signing certificate either as PFX/PKCS#12, as a private key, or by mapping to an existing HSM. This feature enables users to use an existing Code Signing Certificate, import it into the Certificate Inventory, and later map it to policy and perform signing functions.

- The onboarding journey for SIGN+ is tailored to meet the specific configuration needs of the customer:
  - The onboarding journey begins from the **GET STARTED** page.
  - After completing the onboarding process, you can perform modify and signing operations with the existing flow. The onboarding journey can be accessed anytime from the **GETTING STARTED** page.
- The TimeStamping Authority (TSA) server, usually provided by a third party, is now an independent, deployable service running on a dedicated HTTPS server. This service is hosted with a valid SSL

certificate, and the certificate for signing timestamp responses will be obtained from a trusted Certificate Authority (CA) or issued through a Private CA where applicable.

- Customers with access to products other than SIGN+ can now apply for a Freemium role. This role grants all permissions of the SIGN+ module, allowing users to explore its functionalities. Freemium resources also have access to dependent modules for RBAC to support the product's privileges.

Chapter 2: Enhancements

This section describes the new features in AppViewX v2023.1.0 FP3 release.

Automation

The following enhancements are included in AppViewX Automation.

- Email customization options is introduced in the email task by integrating the email templates available under Platform > System Administration > Themes and Personalization > Email.
- Support for authentication using credential store is provided for Basic Auth and Credential Auth types. This support extends to integration vendors, ServiceNow tasks, Hook REST external, Form Associate Script REST external, External REST palette, and Command Repo REST calls authenticated using integration.

CERT+

The following enhancements are included in AppViewX CERT+.

- The discovery parameters for filtering Microsoft Enterprise CA certificate discovery now incorporate a Time Range option. When this filter is active, the Certificate Effective Date and Certificate Expiration Date discovery parameters become disabled.
- Expired or revoked certificates are now capable of transitioning from the Managed state to the Monitored state.
- Following renewal, reissue, or regeneration, old certificates can transition from the Managed state to the Monitored state.
- Improved the certificate type arrangement during certificate pushing to a Panorama PaloAlto Firewall device. The certificate type field has been reorganized, with the default value now set to PKCS12 <.p12>. If no private key is available, only PEM <.pem> will be displayed.
- AppViewX is improved the onboarding process for HAProxy and certificate push with the following enhancements:
  - After binding the certificate to the HAProxy server's config file, three service actions such as None, Reload, and Restart are added to the dropdown list on the add/edit application connector page.
  - A database script has been enabled (to be executed in the backend by the AppViewX SRE team) to customize the order of certificate and key contents in the .pem file. This allows the private key content to be placed at the beginning or end of the <.pem> file.
- AppViewX has implemented standardized fields for adding Tomcat Linux servers and certificate push as outlined below:

- For Tomcat Linux server addition:
  - The "Use Existing Configuration" field on the add/edit application connector page is now enabled by default.
- For certificate type PEM:
  - The fields "Server certificate location" and "Server certificate name" are merged into a single field called "Certificate Location.
  - The fields "Private key location" and "Key name" are merged into a single field called "Key Location.
  - The fields "Root location" and "CA certificate name" are merged into a single field called "Root Location.
  - The fields "Intermediate certificate location" and "Intermediate certificate name" are merged into a single field called "Intermediate Location.
- Tomcat ADManager and Self Service Plus are integrated into Windows Tomcat, enabling CLM operations for both ADManager and AD Self Service. Push, Bind & Rollback actions have now been enabled for <.p12> and <.pfx> certificate types.
- In existing JBoss/Wildfly Linux and JBoss Windows versions, the "Use Existing Configuration" option is now enhanced and set to default in the following scenarios:
  - Discovery: After the discovery process and certificate on-boarding into the certificate inventory.
  - Push: On the add application connector screen, within the Certificate Details section.

  If the "Use Existing Configuration" option is not selected, the fields "KeyStore Location", "Password", and "Alias Name" will be displayed.
- Enhanced to perform CLM actions with the PKCS <*.p12> certificate on the JBoss (Windows and Linux) device. This includes pushing the certificate to the device, binding it, and being able to discover and rollback within the AppViewX interface. This feature is NOT supported for JBoss v6.4 and older versions.
- Support for Wildfly (Windows and Linux) version 31.x has been added. JBoss Elytron (Windows and Linux) now facilitates device management with the recommended standalone.xml configuration.
- The private key is now encrypted during CSR generation at the endpoint for Tomcat, WebLogic,and JBoss WildFly on both Windows and Linux. Following CSR generation at the endpoint, only the encrypted private key is saved in a text file, while the plain text file containing the private key is deleted.
- EST version 1.4 is now available, featuring:
  - Support for an Uninstall script.
  - Option to enable/disable manual enrollment flow.
  - Ability to control allowed domains in the Subject Alternative Name (SAN).
- Introduced the Certificate Manager option enabled based on the type of load balancers in the application connector page.
- Support for certificate push to secrets in Keyvaults.

- Support for certificate discovery from Secrets.
- Microsoft CA, Microsoft PC, and Microsoft Server now support Gateway Credential as a credential type.
- The Restart option is now available for Apache on Windows.
- For Microsoft CA, you can now select one or multiple discovery parameters to filter the results during an optimized discovery scan.

CERT+ licensing now offers two models:

- **Certificate-based count (introduced in v2023.1.0 FP3):** The license count is based on the number of certificates in the inventory.
- **Certificate instance-based count (existing):** The license count is derived from the number of connectors associated with a certificate.
- You can choose the certificate licensing model when requesting a license.

- Optimized certificate discovery scan is now supported for DigiCert CA. This optimized scan type allows you to filter discovery results by selecting one or multiple discovery parameters.
- When certificates are exported in the CSV and XLS formats, the **Valid From** and **Valid To** columns now also include the certificate expiration time along with the certificate expiration date.
- Before upgrading a cloud connector version, you have the ability to view the current and to-be-upgraded version numbers, as well as the checksum of the binaries that will be uploaded as part of the upgrade process. This information is presented in the dialog box for upgrade confirmation.

  Additionally, you can download the tarballs to conduct vulnerability scans before proceeding with the upgrade. Checksum files are included and downloaded along with the tarballs.
- Starting with v2023.1.0 FP3, support for the tech preview of the integrated gateway functionality has been expanded to include Apache (Windows) and Tomcat (Windows) devices. Recommendations for utilizing the integrated gateway functionality:
  - Hostnames employed in the integrated gateway should be resolvable in the cloud connector.
  - The use of Fully Qualified Domain Names (FQDN) is preferred.
- Notifications concerning version upgrades for cloud connectors, upgrade statuses (including initiation, success/failure scenarios, and so on.), and cloud connector downtime are now available through two channels:
  - Displayed in the Notifications Center.
  - Emailed to the admin user for convenient tracking and awareness.

- Strting with v2023.1.0 FP3, the certificate and key files for the AppViewX Cloud Connector will no longer be stored on the mothership. Instead, before each cloud connector upgrade, the certificates and keys will be generated directly on the cloud connector.

  While this change will not impact the upgrading process from an existing installed version to the latest version of the cloud connector, it should be noted that fresh installations of older versions will no longer be supported.

KUBE+

The following new feature is included in AppViewX KUBE+.

- **Cluster PKI**:
  - Removed the one-to-one dependencies between clusters/namespaces and the "Issuer CA" created in the Issuer CA inventory.
  - Introduced a template-based approach for onboarding Issuer CA and associating it with the cluster.
- **Cluster Policy**:
  - Default out-of-the-box cluster policies applicable both cluster-wide and for specific namespaces. These default policies can be modified and reused.
  - Provides an improved method for using and managing policies, allowing for seamless association of clusters and namespaces to specific policies.
- **Cluster PKI**:
  - Removed the one-to-one dependencies between clusters/namespaces and the "Issuer CA" created in the Issuer CA inventory.
  - Introduced a template-based approach for onboarding Issuer CA and associating it with the cluster.
- **Holistic View Redirection**: Certificates enrolled in Secure Apps can now be redirected to the certificate holistic view by clicking on the common name.
- **KUBE+ Insights**: Improved KUBE+ Insights by providing detailed information on certificate expiries, enrolled certificates, discovered certificates, and certificates set to auto-renewals.

PKI+

The following enhancements are included in AppViewX PKI+.

- Starting from v2023.1.0 FP3, certificates enrolled through the AppViewX PKI CA will be initially in the monitored state. Users can modify the certificate status by navigating to PKI > Settings and selecting the desired option under "Issued Certificate Status" in the CERT Inventory.

Platform

The following enhancement is included in AppViewX Platform.

- A new configuration option, 'Max Session Timeout', is introduced in Platform > Access Management > Authentication Settings. This setting ensures that sessions are forcefully logged out after a specified maximum duration, regardless of user activity. This measure enhances security by preventing malicious users from keeping sessions indefinitely active.
- A new option, Auto Create Service Account, has been introduced in the external service account configuration to control the service accounts auto creation from external Identity Provider. When enabled, this option will automatically creates service accounts in AppViewX upon the first login attempt. If disabled, service accounts must be manually created in AppViewX using the Client ID from the identity provider.
- Enhanced the validation process for service accounts from external identity providers (IDPs). The audience name is now mandatory in the external service account configuration. After upgrading, you must reconfigure your external service accounts to include the audience name for them to continue working properly. Please note, there is no impact on service accounts created locally in AppViewX.
- Introduced new customization options in AppViewX, allowing you to personalize the appearance of emails sent from the platform. You can now customize the logo, signature, and footer in all outgoing emails to align with your organization's branding standards. To achieve this, customize the default email template available under Platform > System Administration > Themes and Personalization > Email.
- Enhancements are made to display the current and to-be-upgraded version numbers, along with the checksum of the binaries to be uploaded during the upgrade process. This information is presented in the dialog box for upgrade confirmation before initiating the cloud connector version upgrade.

  Additionally, users have the option to download the tarballs to conduct vulnerability scans before proceeding with the upgrade. Checksum files are downloaded alongside the tarballs to facilitate this process.
- Notifications concerning version upgrades for cloud connectors, upgrade statuses (including initiation, success/failure scenarios, and so on.), and cloud connector downtime are now accessible through two channels:
  - Notifications Center: Users can view these notifications within the Notifications Center interface.
  - Email: Admin users will receive these notifications via email for convenient tracking and awareness.

SSH+

The following enhancements are included in AppViewX SSH+.

- The Host Certificates Expiry Widget is added to the dashboard.
- Enhanced the search functionality and group filter in the key inventory.
- Access request functionality is enhanced through the use of Principals for Certificate-Based Access:
  - Requester names are now incorporated as principals in certificates during access requests.
  - Allowed principals can be removed from the host inventory.
- The option to enable Advanced Key Provisioning Control is now available on the Settings page.
- The key discovery enhancements are implemented to enhance performance.

SIGN+

The following enhancements are included in AppViewX SIGN+.

- The synchronous signing process for file-based and hash-based operations has been enhanced, specifically for HSM-based certificates. The status indicators have been updated from "FAILED" and "SIGNED" to "INPROGRESS," "SIGNED," and "FAILED" for signed requests. Additionally, the signing policy creation now includes Polling Interval Settings. The signing status can be viewed in the Signing Inventory, improving the signing process with enhanced status monitoring and sequential processing of each signing request.
- Enhancements are made to extend the functionalities of the AppViewX CSP and PKCS11 Providers with client tools in the SIGN+ Package:
  - Users can now provide the password as a command-line argument, bypassing the password prompt and overwriting previous installation prompts.
  - Support for XMLSecTool is provided, with commands to be used and automatically generated in the README file.
  - The log file rotation mechanism has been enhanced to generate a log file for each day of the week. If the same day occurs in the subsequent week, the previous log file gets overwritten.
- The AppViewX PKCS11 provider is now compatible with the following Linux distributions:
  - Debian 12.5
  - Amazon Linux 2023.
- SIGN+ offers the option to adjust the visibility of signing requests, allowing users to choose between two options:
  - View All the Signed Requests by all the Users
  - Viewing the Signed Requests by Logged In User.
- The existing APIs in the SIGN+ module have been optimized by streamlining the retrieval of crucial information through publicly exposed APIs:

  - The "code-signing-get-policy," "code-signing-get-added-keys-for-policy," and "code-signing-get-added-meta-info-for-policy" APIs are enhanced to simplify the acquisition of policy details, signing key details, and associated meta information specific to a policy.
  - A dedicated Code Signing Certificate Retrieval API (code-signing-generate-hash) is introduced to enhance user-friendly certificate retrieval for validation purposes.
  - The "Upload and Sign" API is enhanced to restrict accepted signature formats to raw signatures, excluding PKCS#7, XML, JWT, and CBOR formats.
- SIGN+ is enhanced the code signing APIs to display the accurate status of signing requests in the Signing Inventory of the AppViewX nodes. The status of the signing request in AppViewX nodes now aligns with the status in the signing tool once the polling is complete.
- The AppViewX PKCS11 provider, traditionally used for Certificate Based Signing in native fragmented signing tools such as Jarsigner, JSign, APKSigner, and XMLSecTool, has now been enhanced to support Key Based Signing.

Chapter 3: Bug Fixes

This section lists the fixed bugs in AppViewX v2023.1.0 FP3 release.

ADC+

The following bug is fixed in AppViewX ADC+.

- Fixed the F5 GTM Priority Change Issue.
- Resolved inaccuracies in object count display for Citrix ADC in the database.
- AppViewX now closes open sessions on BIG-IP.
- Fixed communication errors during midnight configuration fetch, ensuring devices are correctly resolved.
- Fixed discovery issues with standby F5 nodes during onboarding in SingleNode-OnPrem deployment.
- Restored functionality of the Topology view.
- Corrected status mismatch of ADC objects in the dashboard.
- Fixed display of incorrect subnet IP in VLAN when VLAN is changed for Self IP.

CERT+

The following bug is fixed in AppViewX CERT+.

- Issues in enrolling GlobalSign certificates by uploading CSR are resolved.
- The issue where cloud connector-related alerts were not appearing in the audit logs, and status change logs for cloud connectors were not being displayed, has been resolved. Now, these logs are correctly reflected in the audit logs.
- All certificate attributes and custom attributes are now incorporated into the Server Certificates Report, Client Certificates Report, and Code Signing Certificates Report.
- The issue with the command repository returning a 401 unauthorized error for Akamai CPS GET calls has been resolved.
- The issue of passwords being printed in logs has been resolved. Credentials and fetch configuration now function correctly when the server is added as a Windows Server device, ensuring enhanced security and seamless operations.

SSH+

The following bug is fixed in AppViewX SSH+.

- The issue regarding the automatic removal of public keys for expired key-based access is resolved.

Chapter 4: Known Issues

This section lists the known issues in AppViewX v2023.1.0 FP3 release.

Automation+

The following known issue in AppViewX Automation+.

- The Routers and Switches tab in the device inventory may not be visible to some Automation+ customers due to new license changes introduced in AppViewX. Customers needing this feature for visual workflow solutions can contact AppViewX technical support, who will assist in enabling the feature. AppViewX plans to restore the Routers and Switches tab to its default state in the next major release.

CERT+

The following known issue in AppViewX CERT+.

- The Renew Certificate with Servicenow workflow's email content has invalid text message for success scenario.
- Application slowness due to Expiry report cron job on tenant having 4000 KUBE+ groups.
- Custom attribute values are not being included in export files (both CSV and XLS formats)..
- Microsoft Enterprise CA Discovery: The Certificate Expiration Date and Certificate Effective Date range filters are not yielding accurate results based on the specified criteria.
- Migration Issue: After downloading the sample server import sheet and editing it with valid details, the import process fails.
- Google CA: When using the "Renew" action with "Use Existing CSR", the CSR parameters are being updated if they are modified.
- CSC Global : Certificate enrolment failed with some allowed special character.
- Rollback function failed in Windows tomcat with use existing configuration and private key in device enabled.
- Crypto Score is not displaying properly in trend charts when it's below 1 in the Crypto Score Trend.
- Categories with low certificate counts are not visible in the doughnut charts in Insights. To view one category, all other categories need to be unselected.
- Data display in the bar chart is not proper in the Certificates by Issuing CAs widget when a large number of CAs are present.
- Certificates based on Scan Type are not getting updated in the Insights dashboard after the migration.

- The server certificate count in the Certificates Expiry widget on the Insights Summary page is different from the Server Inventory Expiry counts.
- Certificate ACF needs to be updated for migrated roles.

DDI+

The following known issues in AppViewX DDI+.

- Audit logs for the Bluecat vendor have not been implemented.
- There is application slowness when the system has two million ADC objects and two million DDI records.

Install and Upgrade

The following known issue in AppViewX Install and Upgrade.

- The scheduled execution of the 'appviewx_infra_cert_vw' workflow fails because of outdated scripts stored in the database.

SSH+

The following known issues in AppViewX SSH+.

- Host management process fails when switching from login type "identity key" to other credential types.
- When AWS SSH discovery fails during AWS EC2 onboarding, discovery status is not marked as failed.
- Reconnect action for AppViewX terminal indefinitely loads until timeout.
- Host count is not updated properly in infra access group inventory page during host dissociation from an infra access group.
- User is unable to perform rotate action successfully if key has host association details of deleted hosts.
- When user performs Host key rotation, the older host key is not deleted from the device
- Only 100 records will be shown to select in the component in Infra access group create/update, Host compliance group create/update & in managed scan.
- User is able to add infra access group via the dynamic type feature in host/discovery page even though Create infra access group ACF is disabled
- When user moves host from one group to another, certificate will be revoked & KRL will be updated in the moved host but trusted user CA belonging to old group will not be removed.

Chapter 5: Known Limitations

This section contains the known behaviors, system maximums, and limitations in software in AppViewX v2023.1.0 FP3 release.

ADC+

The following known limitations are included in AppViewX ADC+.

- Auto-detection of peers when adding controller devices with management IPs is not supported due to limitations with F5 communication protocols. Controllers can only be added using the floating IP.

CERT+

The following know limitations in AppViewX CERT+ .

- For CSC Global certificates discovered from the CA, certificate renewal and reissue does not support the use of existing CSR details.
- The CSC Global CA, currently, does not support the following CLM actions:
  - Regenerate
  - Reinstate
  - Suspend
  - Revoke.
- For certificate enrollment using the CSC Global CA, only the following methods of CSR generation are supported:
  - AppViewX
  - Upload CSR
  - Support for CSR generation via HSM and endpoint will be introduced in the upcoming releases.
- Upon onboarding or importing the MS Exchange Server for certificate management and discovery in AppViewX, the following limitations are present:
  - MS Exchange Server accepts DNS SAN value only. If multiple SAN values are specified at the time of CSR generation at Endpoint, Appviewx will consume the DNS value, ignore the rest and create the CSR.
  - When pushing certificates with Services as POP or IMAP, the MS Exchange server automatically maps the SMTP service.
  - Backup and Rollback CLM actions are not supported.
  - RSA is the only supported keytype with bit lengths 1024, 2048, 4096. The CSR generation at Endpoint will fail for keytypes other than RSA.
  - Service restart is only supported for IIS Service.

  - Windows Gateway and the Exchange server have to be configured on different machines.
  - Discovery of Root and Intermediate certificates with the export command is not possible.
- Certificate discovery for devices and CAs that include the integrated gateway functionality will be done in batches of 500 certificates.
- Only certificates enrolled through auto-enrollment protocols after the FP3 patch will be assigned a monitored status. Certificates already enrolled will maintain their managed status. Moreover, renewed certificates that were previously enrolled and managed will also retain their managed status, instead of being switched to a monitored status.
- Manual updating of zones for Amazon Public CA is required during the migration from AppViewX v2020.3.0 to v2023.1.0 FP3.
- 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.
- For SwissSign MPKI certificates, AppViewX does not include support for the CLM actions:
  - Renew
  - Reissue
  - Regenerate
  - Reinstate
  - Suspend.
- The ED25519 algorithm is not currently supported by Bouncy Castle.
- To migrate to v2023.1.0 FP3 from a version older than 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 cannot be discovered; only active certificates in custom domains and those linked via key vaults can be discovered.

PKI+

The following known limitation is included in AppViewX PKI+.

- For migrated tenants, certificates previously enrolled through the AppViewX PKI CA will remain unchanged. However, preferences specified by the user on the PKI Settings Page, under the "Issued Certificate Status in CERT Inventory" option, will apply to newly enrolled certificates.

SSH+

The following known limitations are included in AppViewX SSH+.

- 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.