appviewx

Release Notes

Version: 2022.1.0 FP3 (SaaS)

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_v2022.1.0 FP3 (SaaS) Release Notes.	April 2023

About this Guide

This release document accompanies AppViewX v2022.1.0 Fix Pack 3 (FP3) releases. All the customer requests such as feature requests, enhancements, bug fixes, Stories, known issues, and known behaviors are handled via monthly maintenance release called as fix pack (FP). All the below listed tickets are regressed and packaged as part of the FP3 release.

Intended Audience

- Customers who migrates from AppViewX v2022.1.0 FP2 to AppViewX v2022.1.0 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.
`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

Additional features and functionality have been added to enhance the functionality of AppViewX v2022.1.0 FP3 application. These new features are incorporated to improve the overall performance of the application. In this section, you can find a list of the new features that have been introduced in the AppViewX v2022.1.0 FP3 (SaaS).

ADC+

The following new features are included in AppViewX ADC+.

- The ability to manage high availability Nginx devices in the ADC device inventory, including both active-standby and active-active configurations.
- Nginx Plus LB comes with pre-shipped out-of-the-box automation solutions for creating, modifying, and deleting LB servers. These solutions have also been integrated with IPAM and ITSM to provide seamless functionality.
- A comprehensive automation solution is developed for modifying, deleting, and creating Citrix SLB and GSLB virtual servers, as well as their corresponding bind objects.
- An automation solution is developed to facilitate the creation of Citrix SLB and GSLB virtual servers. The solution also enables the association of services, service groups, and other relevant objects with these virtual servers.
- An automation solution is implemented for the creation, modification, and deletion of context switch virtual servers in Citrix. This solution also allows for the association of LB virtual servers with the context switch virtual server.
- Support provided for restoring the Citrix HA devices.
- Parsing support for the Citrix vendor covers a select range of secondary objects, which comprises SSL Cipher Group, SSL Cert Key Pair, SSL Policy Label, SSL Policy, SSL Action, SLB Profile, Policy Label, Policy, Action, and Monitor.

  The Control Center (CC) now features new keywords for advanced search in the Citrix vendor. These keywords, which have been recently introduced, include SSL Cipher Group, SSL Cert Key Pair, SSL Policy, SLB Profile, Policy, and Monitor.
- Support given for object backup and object restore for few secondary objects in the Citrix vendor. Secondary objects includes: SSL Cipher Group, SSL Policy Label, SSL Policy, SLB Profile, Policy Label, Policy, Action, Monitor
- The ability to comprehensively manage and execute actions on the Citrix Cluster nodes.

- AppViewX supports backup, restore, and comparison of devices and objects configuration for the Citrix cluster nodes.
- Support provided for two actions related to the SLB Virtual Server object type in the Citrix vendor, which are **viewing persistence records** and **clearing persistence records**.
- AppViewX now offers support for the latest version, v22.x, of the AVI Vendor. With this support, AppViewX can manage AVI Version 22.x in the ADC Device Inventory, and all the supported functionalities will operate seamlessly in AVI Version 22.x.
- The ADC Product Demo mode iis activated to assist partners, customers, field teams, and prospects in showcasing or demonstrating the value of the ADC Product. By enabling the ADC Product Demo mode, it eliminates the need to incorporate live data.
- • AppViewX now supports the latest version, v17.x, of the F5 Vendor. This support enables AppViewX to manage F5 Version 17.x in the ADC Device Inventory, with all the supported functionalities working seamlessly in F5 Version 17.x.
  - Ability to manage F5 "GTM modules" Device in the ADC Device Inventory with read only user. For example, user with AUDITOR Role.
    - F5 "GTM Only" Device management with Auditor role is supported only for the F5 versions 13 and above.
    - OOB Workflows for the device added with read only user. For example, user with AUDITOR Role fails.
  - The "Cipher Group" and "Cipher Rules" LTM objects of an F5 device can now be consumed from AppViewX via Control Center Search

CERT+

The following new features are included in AppViewX CERT+.

- AppViewX provides support for performing the following actions with GlobalSign Atlas CA:
  - CA policy integration.
  - CA setting integration
  - Rabbit MQ Linux Server v3.9
  - CLM actions such as reissue and revoke
  - CA Switch
  - Certificate Enrollment
  - CA discovery functionality.

- AppViewX supports for delta discovery for Apache Linux servers. This support enables configuration fetch and midnight config sync.
- AppViewX supports for pushing certificates to all Palo Alto Firewalls via the Panorama platform.
- AppViewX supports to include Checkpoint Firewall device version 80.40, with full CLM functionality support.
- AppViewX supports to include Fortigate Firewall device version 7.0, with complete CLM functionality support.
- Certificate discovery based on Certificate Transparency (CT) log scan: Positioning of button menu, behavior on click, form design, inventory, and summary.
- Included an additional column to the Inventory for the PKIaaS: WAEP requirement

PKIaaS

The following new features are included in AppViewX PKIaaS.

- AppViewX PKIaaS provides support for the following features:
  - Retrieve the Global Catalog Server details
  - LDAP base
  - AD Template data via CC
  - Duplicate selected Template
  - Publish created Template to AD.
- Introduced the template auto-fetch feature:
  - CC detail auto fetch ,Global Catalog Server IP,LDAP base and validation of AD inputs.
  - Auto fetch List of Template name, OID, Validity and Renewal period.
  - Allow selection of existing templates.
  - Based on selection pull the details of selected templates and parse values to auto-populate in the form.
  - Template configuration and CA mapping.
  - Fault tolerance.
- The duplication of templates and the download of executable batch files are introduced.
- Synchronization of Windows templates with the AppViewX WAEP GUI.
- Prevention of revocation and deletion of OCSP certificate.

- Improving the left menu and user experience for dashboard view.
  - CA Insights
  - Issued Certificates Summary
  - WAEP Summary
  - License Usage.

Platform

The following new features are included in AppViewX Platform.

- With the new Master encryption setting, you have the capability to encrypt all of your secure materials in AppViewX using HSM.
- Multi-factor authentication is introduced to enhance security during authentication.

Security+

The following new features are included in AppViewX Security+.

- An option is added for vCMP host and vCMP guest.

Chapter 2: Enhancements

This section lists the enhancements in AppViewX v2022.1.0 FP3 (SaaS).

ADC+

The following enhancements are included in AppViewX ADC+.

Case/Ticket Number	Description
ADC-14255	Ability to add and manage A10 devices in a SaaS setup and perform traffic management/self serving activities on the discovered Apps via Control center of Dashboard.
ADC-14219	Ability to add and manage AVI devices in a SaaS setup and perform configuration management.
ADC-13609	Ability to add and manage A10 devices in a SaaS setup.
ADC-13602	Ability to add and manage Citrix devices in a SaaS setup.
ADC-12344	Ability to add and manage F5 devices in a SaaS setup and perform configuration management.
ADC-15993	Studio Rules enablement in SaaS.
ADC-14523	Ability to add and manage Citrix devices in a SaaS setup and perform configuration management.
• ADC-14516 • ADC-14263 • ADC-14233	Ability to add and manage A10 devices in a SaaS setup and perform configuration management. **Note:** The following points are the limitations of this enhanced feature: • The restoration of the Citrix GSLB service group is having an impact on the SGMs and servers. • If a child object is deleted, the restoration of the A10 object will fail. • The A10 HA device restoration is successful, but SLB objects are not restored.

Case/Ticket Number	Description
ADC-14226	Ability to add and manage Citrix devices in a SaaS setup and perform traffic management/self serving activities on discovered Apps via Control center of Dashboard.
ADC-17075	Validation for F5 v17 in saas.
ADC-17072	Supporting object compare support for Citrix objects from control center and object compare page.
ADC-17649	RBAC standardization based on new UX themes.
ADC-15590	AppViewX is now able to keep track of objects, devices and controllers count that is added in the ADC, WAF, DNS and Integration Inventory and showcase in the License Metrics page of AppViewX.
ADC-7062	Support given to see AVI controllers and BigIQ nodes in the ADC Inventory.
ADC-17631	Pagination is introduced in Backup Group section.
ADC-12820	Logs and Alert settings enabled for Nginx vendor.
ADC-9597	Support given for Device and Object Backup of Nginx devices.
ADC-13204	Ability to manage High availability Nginx devices in ADC device inventory.
ADC-14629	Two new state status introduces for Nginx objects.
ADC-15816	Support for state status drift now enabled for Nginx device.
ADC-15334	Support for Device and object compare is now extended for Nginx device.
ADC-16913	Ability to customize object actions from control center and dashboard. (OOB workflow shipped to create snow ticket for tracking and email notification).
ADC-17772	Support for SFTP BIG-IP ISO files during software upgrade on Standalone and HA F5 device.
ADC-14754	Enabling Bluecat workflows in aligned with SaaS.
ADC-14498	AppViewX supports for parsing system-related information from the Citrix device.

CERT+

The following enhancements are included in AppViewX CERT+.

Case/Ticket Number	Description
CERT-24586	ACM (AWS Certificate Manager) has been enhanced to enable the pushing of ACM certificates with Tags.
CERT-24596	Improvements have been made to AWS ELB (Elastic Load Balancer) in both standalone and cross accounts type.
CERT-25183	Enhancements have been made to AWS ACM in both standalone and cross accounts type.
CERT-25002	The cloud discovery has been improved to cover standalone, cross, and federated accounts type.
CERT-24261	The UI logging and terminal log have been enhanced.
CERT-26741 CERT-32689	The cloud addition functionality has been improved to support Private CA (Standalone) environments.
CERT-24626 CERT-32678	Extended support of certificate discovery and life cycle management to the AWS CloudFront services for Cross/Federated account type.
CERT-25103 CERT-34356	The logo for Cloud Connector and the form fields have been modified for all cloud vendors and service types.
CERT-24981 CERT-32688	The AWS IAM services for Cross/Federated account type now have an extended support for certificate discovery and life cycle management, as part of the IAM Enhancements.

Platform

The following enhancements are included in AppViewX Platform.

- To enhance the user experience, the roles tree structure has been updated in accordance with the new product UX.
- The license page now offers the capability to assign separate expiration dates to different products, resulting in improved visibility.
- For each metric, the license page now offers more comprehensive metrics information.
- A license expiry notification setting has been incorporated into the license page, enabling you to receive email alerts regarding your license's impending expiration or when it is about to surpass the usage limit.

- A new setting has been added under Platform for tracking usage data, giving you the option to enable or disable product usage data tracking.
- You can now extend your trial seamlessly with the new "Extend Trial" option
- The "Terms and Services" agreement will now be displayed upon first login to the product. User can read and accept the terms and conditions.

Security+

The following enhancements are included in AppViewX Security+.

Case/Ticket Number	Description
FIREWALL-958	The support for FortiGate firewall SSL certificates for version 7.0.
FIREWALL-1301	Support for Thycotic and Hashicorp vaults to add firewall devices.

Reporting

The following enhancements are included in AppViewX Reporting.

Case/Ticket Number	Description
REPORT-1252	The Reporting Engine now supports CSV and XLSX formats for both Out-Of-The-Box (OOB) and Custom Reports/Dashboards.

Chapter 3: Bug Fixes

This section lists the fixed bugs in AppViewX v2022.1.0 FP3 (SaaS).

There is no bug in this release.

Chapter 4: Known Issues

This section lists the known issues in AppViewX v2022.1.0 FP3 (SaaS).

ADC+

Known issues of AppViewX ADC+ are as follows:

- When a user has limited ACF, the demo mode may break.
- If a user only has permission to access Device Inventory, the ADC+ menu option may not be visible.
- Even if an action passes in the next retry, a failure during FP3 SAAS action is still logged in the audit log.
- The implementation of cross device object rollback for Citrix needs functional discussion.
- For Citrix, attributes like 'Weight', 'LB Method', and 'Persistence' are not updated via status fetch but only through Config fetch.
- Object restore lists objects without ACL permissions.
- Demo Mode ACF enablement is not enabled for all ADC Default Roles in the Common category.
- Certain SLB profile types that exist in primary objects but not in 'System -> profiles' are not parsed.
- Topology view of GTM V server cannot be viewed in CC > GTM Vserver.
- New menu ACF is unclear from an end user perspective.

CERT+

Known issues of AppViewX CERT+ are as follows:

- Vulnerability score card Dashboard needs to be disabled.
- The update of the Certificate Authority connection alert fails on the Certificate Alerts page.
- An SMTP connection error occurs when attempting to assign or unassign a group for email transfer ownership.
- The unassign process takes a long time to complete and hangs when attempting to unassign the group.
- The private key discovery feature does not work correctly for the Fortigate device.
- When FIPS mode is enabled in Fortanix HSM, both CSR generation and certificate enrollment processes are failing.

Chapter 5: Known Limitations

This section contains the known behaviors, system maximums, and limitations in software in AppViewX v2022.1.0 FP3 (SaaS).

ADC+

Known limitations of AppViewX ADC+ are as follows:

- AVI: SLB Objects state and status are not updated if the parent object is disabled.
- Control Center: Some Policies don't expand SLB actions, and when SSL Policies have Default SSL actions linked, SSL action is not expanded in SSL Policies Configuration.
- F5: LTM pool and LTM irule class object restore are not functioning correctly.
- F5: Object Restore is not working as expected and has an impact on object roll-back.

CERT+

Known limitations of AppViewX CERT+ are as follows:

- Migration of AWS standalone devices is now supported for versions v2020.1.0, v2020.2.0, and v2020.3.0 through v2020.3.0 FP7 of CERT+
- Migration of AWS devices is not supported for versions such as v2012.X.X, v2019.X.X, and v2021.X.X of CERT+. It is advisable to delete all AWS devices, both standalone and cross accounts, before migration from these unsupported versions. After migration to v2022.1.0 is complete, the devices can be added back.
- AppViewX recommends to delete the following before migration, if you are migrating from v2020.1.X, v2020.2.X, and v2020.3.X to v2022.1.X.
  - All the Amazon CA settings.
  - Any of the EC2 instances that is added manually from the Server inventory.

Note:

- Do not delete the auto discovered from the cloud accounts.
- For more details, refer CERT+ User Guide.

- The batches in CT log discovery for the "google.com" domain are inappropriate and out of order.
- Due to account limitations, it is not possible to validate the Organizational SSL, Alpha SSL, and Extended SSL in GlobalSign SSL.

- The renew operation fails for the GlobalSign MSSL CA discovered certificates that are close to expiration.
- Revoking the uploaded certificate for Hashicorp Vault CA fails.
- AppViewX recommends users to trigger update zones manually for each AWS public CA settings after it has migrated from v2022.1.0 FP2 to v2022.1.0 FP3

Platform

Known limitations of AppViewX Platform are as follows:

- For migrated tenant the license information of licensed metrics are not grouped.

Chapter 6: Security

This section lists the Security Bulletin in AppViewX v2022.1.0 FP3 (SaaS).

For more details about security bulletin, refer Security Bulletin Guide.