appviewx

Release Notes

Version: 2022.1.0 FP3 (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_v2022.1.0 FP3 (On-Prem) 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.
- Customers who migrates from v2020.3.0 FP10 or FP11 to v2022.1.0 FP3.
- New customers who on-boards 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 (On-Prem).

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.
- 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
- AppViewX supports parsing, introduce keywords for advanced search in the Control Center, and provide backup and restore support for two primary objects in the GSLB module of the Citrix Vendor. These primary objects are GSLB Service Group and GSLB Service Group Member.
- 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 is 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+.

- 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

Install and Upgrade

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

- The introduction of Grafana dashboards allows for the monitoring of AppViewX performance, and it is possible to configure an Alert Manager to send email notifications upon reaching performance thresholds.
- For the purpose of troubleshooting, a new log collection tool has been implemented that efficiently gathers logs from all nodes without any interruption.
- An automatic remediation tool has been implemented to diagnose and resolve common issues without requiring manual intervention.

Platform

The following new features are included in AppViewX Platform.

- Multi-factor authentication is introduced to enhance security during authentication.

Security+

The following new features are included in AppViewX Security+.

- The option for vCMP host has been included in the F5 Firewall Device type.
- The certificate parsing now has a read-only access.

Chapter 2: Enhancements

This section lists the enhancements in AppViewX v2022.1.0 FP3 for the On-Prem module.

ADC+

The following enhancements are included in AppViewX ADC+.

Case/ Ticket Number	Description
ADC-12820	The Nginx vendor now has Logs and Alert settings enabled.
ADC-9597	Device and object backup support is now available for Nginx devices.
ADC-14629	NginxPlus objects now have two new statuses, namely "unhealthy" and "unavail"
ADC-15816	The support for state status drift is now enabled for Nginx devices.
ADC-15334	The support for device and object comparison is now expanded to include the Nginx vendor.
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-15590	The AppViewX product can monitor the count of objects, devices, and controllers added in the ADC, WAF, DNS, and Integration Inventory and display them on the License Metrics page of AppViewX.
ADC-7062	Support is now available to view AVI controllers and BigIQ nodes in the ADC Inventory.
ADC-17631	Pagination is introduced in backup group section.
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-26741 • CERT-32689	An enhancement has been made to cloud addition to support the addition of a Private CA (Standalone).

Case/Ticket Number	Description
CERT-24981 CERT-32688	IAM enhancements have been made to AppViewX, extending the support for certificate discovery and lifecycle management to AWS IAM services for Cross/Federated account types.
CERT-24626 CERT-32678	Support for certificate discovery and life cycle management has been extended to AWS CloudFront services for Cross/Federated account types.
CERT-24586	The ACM certificate now has an enhancement that allows it to be pushed with tags.
CERT-24596	AppViewX now offers extended support for certificate discovery and lifecycle management to the AWS Elastic Load Balancing (ELB) services for Cross/Federated account types. This allows users to efficiently manage their SSL/TLS certificates on ELB instances across multiple accounts using AppViewX's centralized interface.
CERT-25183	Extended support of certificate discovery and life cycle management to the AWS ACM services with Tag Attributes.
• CERT-25103 • CERT-34356	Vendor connectors and service connectors must be updated with their respective logo instead of using one logo for all cloud vendor and service types. Updates, modifications, and removals of fields are necessary for every service and vendor type.
CERT-25002	Support for on-demand discovery of cloud accounts is now enabled for both Standalone and Cross/Federated account types. This allows for more efficient and flexible cloud account management within AppViewX.
CERT-24261	Improved the logging functionality of the AppViewX User Console for all multi-cloud use cases (such as AWS, Azure, Google, etc.) to provide better visibility and monitoring.

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.

Security+

The following enhancements are included in AppViewX Security+.

Case/Ticket Number	Description
FIREWALL-958	CLM v7.0 now provides support for SSL certificates on FortiGate firewalls.
FIREWALL-1049	Device inventory now includes contexts to be displayed.
FIREWALL-1301	All vaults and credentials are now readily available in all consumption areas by default.

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 OOB and Custom Reports/Dashboards.

Install and Upgrade

The following enhancements are included in AppViewX Install and Upgrade.

- AppViewX now provides support for on-premises server deployment on RHEL 8.6 and 8.7 OS versions.
- AppViewX now supports TLS 1.3 and also allows for enforcing it for inbound connections (applicable only for on-premises deployments).
- MongoDB now meets CIS benchmark compliance.
- AppViewX now provides the ability to migrate the server from CentOS to either Ubuntu or RHEL operating system.
- The roll-back process has been made more stable.

Chapter 3: Bug Fixes

This section lists the fixed bugs in AppViewX v2022.1.0 FP3 (On-Prem).

There is no bug in this release.

Chapter 4: Known Issues

This section lists the known issues in AppViewX v2022.1.0 FP3 (On-Prem).

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.
- 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 (On-prem).

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.
- Actions for the front end object are not functioning properly.

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 and Install and Upgrade in AppViewX v2022.1.0 FP3 (On-Prem).

Install and Upgrade

The following security fix is included in AppViewX Install and Upgrade.

- Security issues have been mitigated through component upgrades.

Security Bulletin

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