appviewx

Release Notes

Version: 2022.1.0

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

Copyright AppViewX, Inc. ii

Copyright © 2022 AppViewX, Inc. All Rights Reserved. ii

Trademarks. ii

External Reference Links. ii

Contact Information. ii

Preface. iv

Revision History. iv

About this Guide. iv

Text Conventions. iv

Chapter 1. New Features. 5

ADC+. 5

CERT+. 6

PKIaaS. 7

Platform. 8

Chapter 2. Fixed Issues. 9

Platform. 9

Chapter 3. Known Issues. 10

ADC+. 10

CERT+. 10

Platform. 12

PKIaaS. 13

Visual Workflow. 13

Chapter 4. Fixed Issues. 14

ADC+. 14

Multicloud. 19

Preface

Revision History

Revision	Description	Date
1.0	AppViewX_v2022.1.0 Release Notes.	June 2022

About this Guide

AppViewX SaaS release is focused towards ADC+, CERT+, Platform, and PKIaaS. This includes management of certificate on-prem and cloud endpoints from AWS. They describe new features, fixed issues, known issues, and limitations in the software.

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 v2022.1.0 release.

ADC+

- User can select the device for statistic collection by giving option Device/Group in settings.
- Provision to Select the timeline for Traffic Statistics widget- 'Day' as the default data in Traffic statistics based on setting.
- Default heatmap polls device every 60 seconds by default as part of stability.
- AVI vendor abstraction and version support available.
- Default auto refresh settings is changed from 1 minute to 5 minutes in dashboard as part of stability.
- In Dashboard > Stability, disable the refresh button to avoid frequent status calls.
- Select all VIPs and take actions features are disabled for users.
- Nginx plus vendor abstraction and version support (R23,R24,R25) is available.
- A10 V5 Vendor Version is supported.
- Introduced F5, AVI, and A10 keywords in control center for a refined search.
- The Data center is supported for Akamai and AWS Vendor.
- As part of dashoard stability, the objects that can be added in Dashboard Application View widget is restricted.
- Toggle button for object backup is introduced to switch off heavy operations in Backup and Restore. Object backup enabled will do a object backup. By default this settings will be disabled.
- As part of statistics stability, upgraded the elastic component jar from v5.x to v7.x version.
- Nginxplus device addition with FQDN, SSH port, and Sudo user are supported in Device Inventory for Nginx supported vendor.
- Self Servicing action drain is supported in control Center and Dashboard for the Nginx vendor supported objects.
- In Nginx plus, all state files will be downloaded and parsed irrespective of file format in that device.
- Stale entries cleanup from Application View Widget and Traffic Statistics Widget in the Dashboard module when the devices/objects are decommissioned from AppViewX.
- AppViewX allows the user to bookmarking/saving of Device Backups in the backup and restore page, So that the user will not lose any backup.

- Reduce the Config Fetch Time on ADC Device Management in the ADC Device Inventory by skipping LTM and GTM object parsing for Certificate Use cases with a on demand property.

  Supported ADC Vendors:

  - Nginx
  - A10
  - AVI
  - F5
  - HAProxy.
- Pre-defined SLB and GSLB templates have been introduced to help configure, manage and monitor SLB and GSLB Applications in the Application View Widgets effortlessly. This helps the App Teams to self-serve Application services & Traffic seamlessly. For eg: Data center/Device based instant App Visibility
- Summary email of device backup will be generated based on the setting during the backup group creation. It gives detailed information about the device details, archive files, and status of the backup.
- Node Password dependency was removed for HAProxy device addition in device management.
- Device communication Stability (From AppViewX to Vendor Device): Optimization in Object Status fetch calls to reduce device loads.

CERT+

- Clients for ACME protocol for Windows and Linux operating systems to bring automatic certificate enrollment capability to the devices for device identity or application certificates.
- Ability to completely automate certificate lifecycle management across all AWS accounts of a large enterprise:
  - Discover all AWS accounts
  - Discover the AWS services being used in the discovered accounts
  - Discover the certificates installed/stored in the services
  - Policy based access control over the discovered services and certificates
  - Lifecycle actions for the discovered certificates
  - Periodic re-discovery of accounts, services, and certificates to keep the inventory updated.
- Support for following additional CAs for certificate lifecycle actions:

  - Entrust MPKI
  - DigiCert MPKI
  - GlobalSignMSSL
  - Nexus CA
  - Amazon Private CA.
- Support for following additional devices/application for certificate lifecycle actions:
  - Panorama & Palo Alto v10
  - SAP Web Dispatcher and ABAP
  - AVI Vantage v21
  - VMWare NSX.
- ACME protocol support for auto-enrollment for following additional CAs:
  - Amazon Private CA
  - DigiCert MPKI.
- Ability to generate Private Key and CSR on Fortanix HSM.
- Ability to define exclusion list for IP Address that need not be scanned for Certificate Discovery.
- Inclusion of built-in workflows in Automation for orchestrating various complex use cases of certification lifecycle management.

PKIaaS

- Ability to offer managed private CA hierarchy without investing resources, time and effort into PKI. Following is available via AppViewX console:
  - Ability to enroll and manage PKI custodians
  - Ability to spin and manage root CA and sub-CAs
  - Virtual key ceremony (M of N approval) for all CA management actions
  - Ability to setup OCSP responder for PKIaaS CAs.
- Ability to auto enroll machine and user certificates from PKIaaS CA for Microsoft Windows domain joined entities [Windows AEP].
- Ability to auto enroll machine or application certificates from PKIaaS CA for any device via ACME, EST, and SCEP protocols

Platform

Security

- Service Account is introduced with oAuth Client Credentials support to access AppViewX APIs from external tools securely.
- Enforced all users to change the password on first login to secure the user credentials.
- RCE introduced in studio rules script bypass.

Integrations

- OpenID Connect (OIDC) protocol is supported for integrating IAM solutions with AppViewX.
- HSM PKCS#11 interface is supported to integrate HSM devices with AppViewX quickly in a standard way.
- Splunk HTTP Event Collector (HEC) is supported for forwarding audit logs from AppViewX to Splunk (Cloud Version).
- Hashicorp Vault is supported to integrate with AppViewX.

Logs

- The log forwarding supports onprem splunk with UDP and TCP protocols.

License

- License usage dashboard is introduced to track the usage of License.
- SaaS - License trial expiry alert and user notification is introduced.
- Soft stop and 1000 certificate limits are allowed for trial license users.
- Access to CLMaaS post trial period but within the data retention period 30 days.

SMTP

- Data center supports the SMTP on settings page.

Chapter 2: Fixed Issues

This section contains the fixed Issues in AppViewX v2022.1.0 release.

Platform

- When you trigger any API (for example, add role) using oauth tokens and if the tokens are expired or invalid then proper error code should get displayed.
- The first name in the tenant user profile is captured from email and it restricts the personal information update due to the special character.
- SaaS Multitenancy - In **Accounts** > **Usergroups** assigned users for group shows the user admin while checking the admin user group even if the admin user is removed in multi tenancy
- SaaS Multitenancy - Session expiry pop up is not displayed.
- ACF tree is missing for tenant management - Multinode Setup.
- HSM device addition is inconsistent when there are two CC with same DC.
- Script "avx_crontab_avx_crontab_21_1_0_0" is failing with an error "Rotate encryption key cron changing script failed"
- The License Provisioning fails for CUSTOM plan for newly added SAAS tenants.

Chapter 3: Known Issues

This section contains the known Issues in AppViewX v2022.1.0 release.

ADC+

- Class Management Widget: When there are multiple devices in roll back, single/multiple device selection does not trigger roll back and throws 500 error message for the api - adc-dashboard-widget-class-management-rollback-action.
- Insight statistics VipTrafficDetailsAggregation fails for the large scale environment
- User must retain the provision to keep the additional <config.> while using Modify LTM Application services workflow.

CERT+

- CSR generation on AVI loadbalancer version 21 is known to fail.
- Certificate discovery for AVI loadbalancer version 18 and 20 is known to fail.
- Generic and AppViewX WinACME client continues with enrollment request even if the initial connection fails.
- AppViewX enforces 100 seconds timeout on synchronous APIs.
- AppViewX can recognize and associate issuer certificates from Private PKI such as Microsoft ADCS only after CA setting is added. If the issuer certificate is onboarded before CA setting is configured AppViewX fails to recognize the certificate’s association with the CA.
- AppViewX fails to mark a failed certificate association to a SAP ABAP endpoint when an incorrect profile push is performed.
- Support for certificate management on Azure virtual machines is not available.
- Below listed certificate authorities (CAs) are not supported:
  - GlobalSign SSL
  - Trustwave
  - Let's Encrypt
  - Renew Certificate and Revoke Certificate features are not supported for Amazon Public CA.
- SMIME Certificates are not supported for all vendors (except Digicert).
- Below listed endpoint ADC devices are not supported:

  - F5 v10.0 and F5 v11.0
  - A10 v2.7.2
  - Push to Device feature is not supported for A10 SLBs
  - Generating CSR and Private Key in the end device feature is not supported for the Citrix Netscaler device.
  - Push to Device feature is not supported for the endpoint AVI devices.
  - Generating CSR and Private Key in the end device feature is not supported for the AVI v21.X device.
- Below listed endpoint server devices are not supported:
  - Apache Linux v2.4.10, Apache Linux v2.4.33, Tomcat Linux v7.0.65, and Tomcat Linux v8.5.29 (deployed in AWS)
  - Oracle iPlanet
  - IBM WebSphere Linux v8.5.5.3
  - HP iLO
  - Dell iDRAC
  - Cisco UCS.
  - Cisco Call Manager
  - SAP Endpoints of ABAP
  - Web Dispatcher
- Push to Device feature is not supported in the endpoint firewalls.
- Endpoint Arbor network is not supported.
- In F5, the certificate manager role related operations are not supported.
- The CSR and Private Key generation is not supported on a Citrix Netscaler loadbalancer.
- In Certificate Discovery section, the root certificate is not being discovered from DigiCert MPKI CA.
- In Certificate Enrollment section, unable to validate other profiles such as User, Device, or Organization due to error message for DigiCert MPKI CA.
- In Client Certificate Enrollment section, the DigiCert MPKI CA displays all the SAN fields that are configured in the policy section.
- In Certificate Discovery section for the DigiCert MPKI CA, the discovery is getting success when multiple seat IDs provided along with invalid seat ID and no error message appears for the invalid seat ID.

- In GlobalSignMSSL account, the renew option support is available only for the Organization SSL due to account limitation.
- In Client Certificate Enrolment section, the DigiCert MPKI CA is being failed by sending directory_name value in SAN.
- The GlobalSignMSSL CA does not support for the Cloud and Extended SSL due to account limitation.
- For GlobalSignMSSL CA, the Global IP address does not work due to account limitation.
- The OPENTRUST CA discovery is not supported.
- Email notification on Certificate ownership transfer is not supported.
- You can not validate the DigiCert Revoke with double approval enabled in Portal, as the Certificate Revoke Request V1 workflow was added in Store and unable to rename the workflow to the default certificate_revoke_request.
- Revoke certificate action fails for the DigiCert MPKI account.
- The CA switch does not happen from other CAs to Amazon Public CA and Amazon Private CA.
- The SCEP MS Intune challenge verification fails when the cloud connector is not connected with the MS Intune server.

Platform

- Unable to download the CC installation tar package, often getting Network error.
- User addition is successful with invalid usergroup association and also value showing in the assigned group column.
- Check boxes missing from the rules store page – Inconsistent
- In CSV mail attachment, profiles are retrieved in the list form instead of comma separated.
- SaaS: Rule Page is not displayed properly in Mac OS at Chrome.
- Multi-Tenant: Error banner message is not displayed when user performs user search action with invalid LDAP host.
- License report dashboard header is hidden even if it has sufficient space in the widget.
- Log forwarding is not working when there are two CC with same Data center.

PKIaaS

- CAs and custodians are immediately deleted from the back-end if user deletes the CA/Custodian in the PKIaaS console.
- Two Classifications of subject alternative names - Generic SAN [DNS and Email] and Customized SAN [SPN and UPN]. These two SANs cannot coexist together.
- Windows AEP runs as an user who is logged in, if the user logs out the application will exit. The suggested work around to avoid the disconnection using the "NSSM" utility to register the windows AEP as a service.
- Smart card logon EKU is not supported by AppViewX.

Visual Workflow

- Import workflow takes more than expected time.
- Variables added inside the task variable section is not getting saved.

Chapter 4: Fixed Issues

This section contains the fixed Issues in AppViewX v2022.1.0 release.

ADC+

Field	Description
Dashboard	In F5 devices, the external class files that have more than 1, 20,000 records will not be parsed. The python scripts must contain SHEBANG in the python installed directory to run them in the script execution widget.
Dashboard	The Citrix orphan GSLB Service parsing is not supported and count differs from the Device, Inventory, CC, and Dashboard.
Dashboard	(Only for application widgets) To handle the device flip and monitor the active objects seamlessly, the **Show only active** option is available in the dashboard settings.
Dashboard	The Import option in the Dashboard does not support objects of different devices at a time.
Dashboard	Actions cannot be configured or performed on an empty group.
Dashboard	Actions can be customized for an object type and not for the individual objects.
Control Center	The VIP feature does not support under Wideip and Recursive Topology for Haproxy, Nginx, and Bigiq.
Control Center	Object compare: Only for F5 objects, the parent disabled objects can be differentiated based on the tool tip state and status. The State and Status color will not be changed.
Control Center	No orphan support for Amazon ELB Objects.

Field	Description
Device Inventory	If you want the FDQN devices to be managed using CyberArk credentials then ensure that the FQDN devices are added with a trailing dot in the CyberArk vault.
Device Inventory	The CyberArk authentication is not supported for the A10 devices.
Device Inventory	CyberArk and AppViewX credentials are not supported for Akamai devices.
Device Inventory	The A10 v2 server objects are not supported.
Device Inventory	Timestamp should be in sync between the server and AppViewX for the Akamai device to get managed.
Device Inventory	The MongoDB supports by parsing the configuration file less than 16MB. The class files for the F5 device fails if it exceeds 16MB.
Device Inventory	If there is an exclamatory mark (!) in the credential of a proxy setting, the connection will not be established.
Device Inventory	Configuration fetch can be triggered for devices in the**Queued** or **Inprogress** status after five minutes in FIFO basis.
Device Inventory	If config fetch is triggered for the HA devices, the secondary device will be triggered after the config fetch is completed for the primary device.
Device Inventory	The import and export of devices are not supported for Amazon ELB and Akamai.
Device Inventory	AVI devices can be managed only using a management IP address and the credentials provider must be a super-user.
Device Inventory	F5 v12 DNS records are not supported in the device management and Control center.

Field	Description
Device Inventory	The NAT IP based device addition is not supported for Citrix devices.
Device Inventory	Orphan Objects are not supported for Citrix and Amazon ELB devices.
Device Inventory	If IP/FQDN/device name is already present in AppViewX, the device with the same details cannot be added to the Inventory.
Device Inventory	The Cisco GSS is not supported.
Device Inventory	Configuring DNS name in the display name format cannot be reordered.
Device Inventory	Generating an iHealth report through device inventory has the following limitations: • The iHealth report generated in the reports column displays only the latest archive. • If an iHealth report generation is in **Queued** or **In-progress** status, another iHealth report can be triggered only after 30 minutes. • The iHealth QKView download cannot be handled for file sizes more than 200 MB.
Device Inventory	Updating the object configuration change based on SYSLOG has the following limitations: • In the case of an object state change, if the host name matches with more than one device name, respective SYSLOG will be ignored. • The SYSLOGS under logging module will not contain the device name. • Any configuration changes to the iRule class files, policy, and partition list will trigger a device config fetch. No other changes received via SYSLOGS will be processed until the device config fetch is complete.

Field	Description
	• If any AVI device is subscribed/unsubscribed in the cluster, then all the available devices in the cluster will be updated respectively. • The Syslogs cannot be received from the Citrix devices when subscribed using the logstash hostname. • For A10 devices, if the Syslog is subscribed using logstash hostname, it should not be more than 29 characters. • Any modification in the device boot location recommends Config fetch to receive SYSLOG(s). • SYSLOGS from Kafka cannot be processed for AVI devices as the logs received contains the hostname of the device. • A manual subscription is required to receive the Syslogs from the A10 devices.
Backup & Restore	The cross version device restore for F5 is not supported.
Backup & Restore	The object restore is not supported for F5 v10 and AVI devices.
Backup & Restore	During an object comparison, the modified lined will be highlighted in Yellow.
Backup & Restore	During object comparison, if the selected objects (with the same name) are available in the multiple partitions, then the comparison will be performed on a random configuration.
Backup & Restore	Backup can be taken for Maximum Archive Size of upto 200MB.
Statistics	The tool tip will not be displayed if statistics for any of the parameter is not collected.

Field	Description
	The ExplicitIP address is not supported for F5 v12 and V13 devices.
	If the Traffic Statistics widget is monitored for more than two hours in the Mozilla Firefox browser, will cause 1 core CPU usage and the browser becomes unresponsive.
	In the DNS success rate widget, the percentage might drop to zero if the statistics has been reset.
	The DAY filter in the TOP 10 VIP(s) by Connection and Top 25 Application Connection widgets represents the data for last 24 hours based on the server time.
	In the Application Bandwidth and Traffic Statistics Summary widgets, the selection application must contain the F5 and Citrix SLB(s). If any other SLB has been encountered the value will be set to zero.
	The statistics generation (historic) for the objects in standby is not supported.
	The statistics are not supported for the AVI GSLB devices.
	The statistics will not be collected fro F5 wideip type SRV and NAPTR.
	Since the F5 device shows bandwidth usage as a cumulative value, the statistics collected for the first time cannot imply correct bandwidth percentage in device heat map. However, the statistics collected further will show the correct bandwidth utilization percentage.
	Pools associated via iRule is not supported.
	Application Bandwidth report is not supported for Citrix Devices.

Field	Description
	.
	Application Bandwidth calculation when VIPs are from different devices is not supported. .

Multicloud

- AWS cloud device service unavailable error appears.
- AWS accounts with Multiple IAM role names and then Cert Sync Staus is In-progress shows as Indefinitely.
- AppViewX CA issued Cert push to key vault fails.