appviewX

Release Notes

Version: 2020.2.0

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

Preface

Revision History

Revision	Description	Date
1.0	AppViewX_v2020.2.0 Release Notes.	May 2020

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

The following new features are introduced in respective modules in this release:

ADC+

- The State/Status updates of F5 objects v11 to 15 are processed on a real-time basis (which was earlier handled on a 5 mins interval) through Syslog notifications. With this, the Control center/Dashboard modules will reflect the real-time state/status for effective monitoring.
- AppViewX can process only the Syslogs that have the complete FQDN of the F5 device in it as the Host Names might be the same across multiple Load balancers.
- A Standardised API has been exposed to get the Application Widget details.
- The API will accept Dashboard and Widget names as input and return the objects and its details configured within the widget.
- The object IDs can be used to perform Bulk/Individual actions on the objects. Refer <link the standardised API guide> for payload details.

CERT+

- **Trust Store Management**
  - Provision for the root and the intermediate certificates from the trust store inventories has been added.
    - Currently, MQServer on Linux and Windows is the supported vendor.
  - **Trust_Store_Certificates** is the new dashboard that is used to track the expiry status of the root and intermediate certificates as separate widgets: Intermediate Certificates Expiry Status and Root Certificates Expiry Status.
    - A new status: **Expiry in 120 days** has been introduced for both root and intermediate certificates.
- **GoDaddy Native Support**
  - GoDaddy Programmable CA connector has been converted to native support.
  - Code signing certificate enrollment with ‘DNS’ SAN has been supported.
- More than one server device with the same IP address can be managed in the Server inventory. The same IP address is used to manage the server devices across the vendors.
- **UI Changes**
  - When you hover the burger in the global menu the CERT+ menu will be displayed.
  - When CERT+ is clicked, a new way of showing the Certificate features have been introduced.
  - The new style has the following features:

    - The static menu on the left side.
    - The static menu can be expanded/collapsed and can be shrunk.
    - The search feature is available to search the menus on the list.
- **CERT+ ACF Changes**
  - Due to changes in the **CERT+** menu, the following ACFs has been changed:
    - Job Scheduler ACF has been removed.
    - Admin Settings is the new ACF that's introduced. By enabling this ACF the following menus can be accessed:
      - Job Scheduler
      - Certificate Attributes
      - Email Settings
      - Expired Certificates
      - History of Certificates
      - Certificate Profile
    - "Application Settings" is renamed to "Application".
    - "CA Settings" is renamed to "Certificate Authority".
- Sectigo CA

  An option to reissue has been introduced for Sectigo CA client certificates.

  - Similar to server certificates: submit, approve, and implement stages are being introduced for client certificates in a holistic view.
  - **Short-lived Certificates**

  To support Sertigo's short-lived server certificates, AppViewX helps the user to create certificates with 'validity in days' representation.

- ECDSA Curve
  - The user can provide **ECDSA Curve** while enrolling for a server or a client certificate in AppViewX which helps server authorities issue certificates for the provided ECDSA curve.
  - It is also added in the compliance check and for all the CAs in the certificate policy.
- Monitor CRL Job

  A 5-minute monitor job runs to check the certificate's revocation status by downloading the CRL points from the corresponding certificate authorities.

- Custom OCSP (Online Certificate Status Protocol) Job

  Users can configure scheduled OCSP Job to check the certificate's revocation status of all the certificates in the inventory.

Security+

- **SaaS Implementation for Security+ (WAF and Firewall)**
- SaaS has been implemented for Security+ (WAF and Firewall) with the expectation that all South Bound APIs will connect to the device using common connectors provided by Framework with either REST or SSH.
- The Framework provided separate REST and SSH connectors to communicate with the device and get the response.
- Earlier in AppViewX, the Southbound APIs of vendors that use REST APIs were not using the common connector provided by Framework, instead, it had its Rest interface to communicate and get the response.
- Currently, the vendors are using REST APIs where our REST interface in South Bound will be removed, and hereafter it will be using Rest Common connector provided by Framework.
- Our Southbound API will give the required inputs like API, Payload, Request type, etc. to the Framework REST connector which in turn communicates to the device and gives back the response to Southbound.
- The Vendors to be Changed: F5- AFM, Checkpoint, Palo Alto, Panorama, FortiManager, and WAF- F5 ASM.
- **Identifying the Device (primary and Secondary) Information**
  - Earlier, AppViewX used to consider manually added devices in inventory as Active irrespective of its original HA status and the configuration would be fetched.
  - Currently, AppViewX gets the HA-Pair status from the devices and based on the status which if currently Active, it fetches the configuration of the Active device whereas the Passive device goes to Standby state.
- **Control Center Export Enhancement**
  - The ability for a User to export Security, Route & NAT rules from Control Center in a Comma-separated-values file.
  - Policy/NAT/Route count information is now displayed in the device inventory, and when clicked it gets redirected from the device inventory page to the CC rule.
  - New keywords have been added for displaying the Control Center Search Revamp 2.0. The keywords are Source Zone, Destination Zone, Rules with hit counts, Rules without hit counts, Compliance, and Optimization.
- **Standardized API Implementation for Security+ (Firewall, WAF, Proxy)**

  The following APIs will be validated for proper request type, error codes, and sample payload request for the response in Swagger: firewall-device, firewall-get-devices-by-filter, firewall-cc-objectchildren-

compare, firewall-cc-objectchildren-search, firewall-controlcenter-search, firewall-policy-config, WAF-device, waf-get-devices-by-filter.

- The issue whereF5 had blocked the SFTP session for the remote users to address security vulnerabilities is fixed by changing the logic to try with SFTP first and if it fails, SCP will be used.

Platform

- **ForgeRock SSO Support**

  Users can now login to the product through SSO (Single Sign-On) supported by ForgeRock Identity Management.

- **Birthright Role for External Authentication**
- When the Admin enables the Birthright role feature, all new users who log into the product will be provided with a predefined set of customizable functions.
- When this Birthright role is enabled, the admin can create and assign a dedicated user group with predefined roles and resources and set it as the Birthright role.
- Whenever a new user logs in he will be mapped with the roles and resources specified in that particular user group.
- **Provision to Upload Custom Logos for Login and Header Page**

  Customers can upload different logos in the login and header page to match their branding requirements.

- **Notifying Users when User Groups are not Associated with Roles or Resources**
- Admins who associate User Groups to Roles and Resources sometimes skip/forget to associate User Groups to a user.
- To tackle this, an alert icon has been added to the User Group inventory to notify if that particular group is not associated with a role, resource, or both.
- **SAML Only Authentication**

  When the user logs into the product using an IDP (Identity Provider), the authentication will be done using SAML (Security Assertion Markup Language) protocol.

- **License to be Uploaded in .zip file Format**
- In AppViewX, the license is generally uploaded in the text file format. Since its a .txt file, transit across Windows and Linux OS adds or removes carriage return.
- Due to this issue, there are issues while trying to decrypt the license file and this displays an error.
- To tackle this, we will accept the license file in the .zip format.
- Hostname Removed from the Login Page UI.

- Exposing the hostname can be lead to vulnerabilities or exploitation.
- From this release, the hostname will be removed from the Login Page UI and the HTML markup.

SSH+

- New architecture changes are imported in the SSH Connector.
- As part of SCP integration from the architectural team, we have exposed the following to support SCP operations. The feature will be part of the 20.2.0 version connector-ssh-plugin. Underlying it uses jsch:0.1.55 to create and execute the SCP command in the server.
- The controller call in the backup-restore-web-handler has been removed.
- Checkmarx vulnerability has been removed. A new scan will be done to check for other vulnerabilities.

Workflow

- Easy workflow design (BYOW) Build Your Oen workflow using vendor APIs, command library.
- Enhanced workflow UX design with I/O mapping, Task info, and Tagging.
- Automatic form generation from REST API, script, and YAML.
- Automatic task generation: Convert vendor API’s into automatable tasks dynamically.
- Rapid Northbound network service Orchestration with Ansible, REST API, and Terraform.
- Inbuilt vendor API tasks, and utilities for the easy network, Business Process automation.
- New Product Line: Self-service catalog with branding.

Reporting

- **Dynamic Scheduling based on Threshold Limit**
  - The certificate dashboard will be loaded based on the configured threshold limit.
  - The reporting framework will have the provision to configure the threshold in terms of certificate count.
  - The user has to click on the live refresh button to get the live data on demand.
  - The dynamic scheduling has to be configured at the report level.
- For Users with RBAC, a provision has been added to change the color code for ‘specific’ data in the reports. Providing the color code is optional and not mandatory. There are three types of color configuration:
  - By default, color code mapping will be done based on the reporting module standard.
  - Color configuration at the query builder/API/script level.
  - Manual Color Code Mapping: In Reports, color code can be selected/modified using the settings option available in the Report Engine.

Chapter 2: Fixed Issues

Bug ID	Description	Module
133646	Logs are not being rotated for appviewx component's start log	Deployment
133605	Resource name with % special character is not supported in ADC object ACL	ADC
133597	When a new role with Full ACF permission is added and the Save button is clicked all the suboptions expect ACF "general" gets selected.	Platform
133546	When both the device which has Read permission from the Control Center and the Restore function is enabled, the device with Read permission needs to restrict the restore function	ADC
133480	On denying the pending request in the entrust CA portal, the certificate status does not get updated in the certificate holistic view.	Cert+
133404	No proper field validation for resource and certificate group name field in the RBAC rule configuration page.	Platform
133373	Request Fails due to "Review task" failover link + UI status	Visual Workflow
133361	VIP Under Wide IP Structure is not rendered for IPV6 RD Objects in F5.	ADC
132910	Special character " * " in subflow cannot be dragged to the workspace.	Visual Workflow
132909	While creating the same name in Proxy settings a Log forwarding Internal Server Error is thrown.	Platform
132732	Citrix Server actions are not performed and an exception is thrown. Audit logs should be covered for this failure scenario.	ADC
132630	MQServer -> On pushing a certificate without a key, the server certificate is pushed in the PEM format.	Rapid SB Connectors
132008	MQServer - Endpoint CSR generation fails for EC Key Type.	Rapid SB Connectors
131898	On pushing certificate to Linux with DER, PKCS7 types, server, intermediate and root certificates are pushed in PEM format.	Rapid SB Connectors

Bug ID	Description	Module
131542	In the SMTP page, after disabling the Authorization required and trying the Test option, it displays an error message "This field is mandatory" across username and password in the Authorization required field.	Platform
131358	New user folder cannot be renamed with a special character.	Visual Workflow
133492	RBAC: While creating a rule with the "Object Type" (ADC) query, it displays the raw object code (For example, a10vs, vs, lpm) in the query builder popup.	Reporting
126977	iHealth is not generated - F5 Login Portal is in progress for more than 4 hours if the CaseNo has been provided.	ADC
133654	Unable to perform an action for LTM - Node of Fqdn type _Action.	ADC
133682	Statistics do not get collected for IPV6 type service group member.	ADC
133681	Search of Orphan GTM Pool Member displays "No result found".	ADC
133778	F5V15-ClassManagement_ExternalClassUpload throws 500 internal server error - intermittenly.	ADC
133786	View Actions (which should be navigated to the second page) are not working from the Open tab In New Window.	ADC
133646	Logs are not being rotated for appviewx component's start log	Deployment
133605	Resource name with % special character is not supported in ADC object ACL	ADC
133597	When a new role with Full ACF permission is added and the Save button is clicked all the suboptions expect ACF "general" gets selected.	Platform
133546	When both the device which has Read permission from the Control Center and the Restore function is enabled, the device with Read permission needs to restrict the restore function	ADC
133480	On denying the pending request in Entrust CA portal, the certificate status does not get updated in the certificate holistic view.	Cert+
133404	No proper field validation for resource and certificate group name field in the RBAC rule configuration page.	Platform

Bug ID	Description	Module
133373	Request Fails due to "Review task" failover link + UI status	Visual Workflow
133361	VIP Under Wide IP Structure is not rendered for IPV6 RD Objects in F5.	ADC
132910	Special character " * " in subflow cannot be dragged to the workspace.	Visual Workflow
132909	While creating the same name in Proxy settings a Log forwarding Internal Server Error is thrown.	Platform
132732	Citrix Server actions are not performed and an exception is thrown. Audit logs should be covered for this failure scenario.	ADC
132630	MQServer -> On pushing a certificate without a key, the server certificate is pushed in the PEM format.	Rapid SB Connectors

Chapter 3: Known Issues

Bug ID	Description	Module
132935	AVI under F5 (Vip under Vip)- AVI VSV Port Range matches with 2 different servers of F5 LTM pool member i.e. connections are missing.	ADC
129239	Dashboard_ApplicationView_Clicking on view topology for the first time renders the dashboard page instead of the CC topology view.	ADC
128752	Threshold alert is not generated when the threshold alert and syslog alert are created with the same name.	ADC
113720	When RGF flow is disabled, and if the submitter rejects the form; both the creator and the reviewer can access the request.	Visual Workflow
136066	Logging: No error logs get captured when the user performs an action on Unresolved/Failed device objects.	ADC
136747	Certificate Transparency reports and response does not contain serial number due to change in the Google CT search response structure.	Cert+
136732	ASA Hit count issue.	Security
136731	Hit Count Mismatch.	Security
136719	After Creating DigiCert SSL plus certificates by uploading the CSR and when we try to reissue the same with Upload CSR and then reject it in the portal and again Reissue by changing CSR as AppViewX and adding SAN, Reissue Retrieval gets stuck.	Cert+
136703	Traffic Grid: Status of Unresolved device objects is not shown in grey color.	ADC-Dashboard
136695	Syslog remote server (AppViewX Environment IP) is not removed from the device when the device deletes it from AppViewX.	ADC
134286	Snapshots taken during the upgrade are not shown in the inventory post-upgrade.	Installation
133924	In Control center- During the batch process, few batches get failed and as a result, the state and status of the objects in the failed batch will be shown as none and status unavailable.	ADC-Control Center

Bug ID	Description	Module
136603	Unable to export filtered data from the inventory using the new menu export option.	Cert+
136613	In 12.4.2, the user was able to create a role with Connector actions enabled and No permissions are given to Server and CodeSigning, after migration of the View Inventory for that role, the Server, and Codesigning should be selected.	Platform
136490	VW Cancel a request does not work.	Visual Workflow
136468	Migration_Issue_ECDSA curve editable in the Edit_Connector operation.	Cert+
136331	In Device Heatmap widget- Device name is not getting populated in the device block.	ADC
131580	No Alert raised for the License upload or activation failure.	Platform
135681	IBMClient (Linux): If the same cert is pushed to jks with different aliases, on discovery only one alias is discovered.	Cert+
132602	FirewallNB: Import: Devices with Expert/Privilege password cannot be Imported using Credential List as it expects a value in the Expert password field in the Import sheet.	Security
136831	ECDSA curve value will not be shown in 'Inventory' and 'Certificate Details Pop up' until the compliance check happens for those certificates when migrated from earlier versions of the product.	Cert+
136831	The ECDSA curve field will be editable in the Edit CA Connector operation until the compliance check happens for those certificates when migrated from earlier versions of the product.	Cert+
136796	Device gets failed - Role fetch gets failed when added with cyberark mode.	ADC
136805	Dashboard-AppView->Create an Appwidget in a new user or a new deployment, undefined is thrown - intermittently.	ADC
136806	CC_Arp->Enable/Disable comments are not set as mandatory.	ADC

Chapter 4: Limitations

ADC+

- AppViewX can process only the Syslogs that have the complete FQDN of the F5 device in it as the Host Names might be the same across multiple load balancers.
- The F5 GTM object Syslog messages do not contain Record type information hence the state/status updates cannot be supported for objects with the same name and different record types.
- Disabling the F5 GTM pool will also change the state of its members as ‘Disabled_By_Parent’. In such a case, the syslogs are being sent only for the changes on Parent objects, hence the state of children objects cannot be updated in AppViewX.
- AppViewX alerts cannot be raised in case of State/Status changes through Syslogs as session information is not included in the Syslogs from Logstash.

CERT+

- During the provisioning of MQServer on both Linux and Windows, Refresh QManager has to be manually performed directly in the device or by using a script.
- All the bit length and key type details supported in AppViewX are available. Only the relevant values for GoDaddy is applicable to enroll the certificate and perform any other CA actions. All the other values can be non-selected in the AppViewX policy.
- The code signing certificate is the only MVP in this release.
- Device certificates inventory will share the same ACF as for Server certificates inventory.
- For the Bulk download of client certificates, the “Download Certificate” in “Client certificate actions” is applicable.

SEC+

AppViewX Sec+ only supports Hit Count Search applicable for 100 records.

Reporting

- The Color code is not applicable for Trend chart, Line chart, Metric Chart, and Grid Chart.
- In Stackedbar the color code is not applicable if the field is a date field.