appviewX

Release Notes

Version: 2020.1.0

Copyright AppViewX, Inc.

Trademarks

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_v2020.1.0 Release Notes.	February 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

- Ability to add and manage F5 v15 devices with self-servicing capabilities. LTM and BIG-IP DNS objects are now supported. You can perform actions like enable, disable, order, priority, LB mode, ratio change, and others in the Control Center and Dashboard.
- F5 devices can now be managed using the Cert Manager along with the Admin role.
- Ability to add and manage AVI v18 devices with self-servicing capabilities. SLB and GSLB objects are now supported. You can perform actions like enable, disable, graceful disable, priority, LB mode, ratio change, and others in the Control Center and Dashboard.
- Ability to add and manage Citrix v13 devices with self-servicing capabilities. SLB and GSLB objects are now supported. You can perform actions like enable, disable, LB mode, ratio change, and others in the Control Center and Dashboard.
- Ability to add and manage Nginx Plus R18,19 devices with self-servicing capabilities. SLB objects are now supported and you can perform actions like enable, disable from the Control Center.
- Ability to view the state **(Active, Standby, Offline)** for devices in the Device Heat Map widget and sort the device blocks accordingly.
- An option to enable admin visibility for all dashboards created by AppViewX users has been added to the Settings module. When a user is deleted, the respective dashboards will now be retained and visible to the admin.
- Manage a BIG IP device using the Certificate Manager role for Cert discovery. AppViewX will skip LTM/BIG-IP DNS parsing if the role is identified as a Cert Manager and it will manage the device for certificate discovery.
- An out-of-the-box workflow that generates a report of Top N-talkers to the selected BIG-IP Virtual server has been introduced. The AVR module must be enabled on the BIG IP device to generate this report.
- Out-of-the-box standard workflows have been added to automate BIG-IP application services.
  - Create/Modify/Delete Virtual Server on BIG-IP with DDI and ITSM Integration.
  - Software upgrade on Standalone and HA BIG-IP devices.
- Out-of-the-box workflows have been added for Application Service automation using AS3 (Declarative API) that delivers faster and easier application deployment.
  - Create or Modify Application Service on BIG-IP using AS3.
  - Delete Application Service on BIG-IP using AS3.
  - Fetch Application Service from BIG-IP using AS3.
- Out-of-the-box standard workflows have been added to automate NGNIX Plus application services.
  - Create/Modify/Delete the Virtual Server on NGNIX Plus with DDI and ITSM Integration.

Certificate

- While creating a discovery instance, the user will be able to discover only the required TLS version certificates using the **TLS version(s)** multi-selection dropdown box available in the **Discover By** section.
- The user can apply the access control rule for newly discovered certificates using the **Use Access Control Rule** available in the After Discover section.
  - This option will be editable only when the ‘Move Certificate to Inventory with Status’ is marked either as Managed or Monitored.
  - If this option is enabled, the certificate group selected in the access control rule will be applied.
- The option to change the polling request job scheduler is included to configure the frequency of the polling request with the CA until AppViewX receives the successful response from CA.
- For EST, the following types of authentications have been included:
  - Only Certificate TLS
  - Certificate TLS with HTTP as a fallback
  - Both Certificate TLS and HTTP
- For EST, URL support is available as the default URL
- You can now find and execute the keytool command for Weblogic and Websphere.
- Service Account support has been included for WebSphere.
  - During device addition, the service account details will be collected for managing the account by parsing the objects and discovering the certificates.
  - Push, bind and rollback operations for certificates will now be done only in the service account.
- Temporary Push Location is an optional field that has been included for Websphere during the device addition process. During certificate push operation, if a certificate has to be pushed to the customized temporary location before to the destined object, the user has to fill the temporary push location value in this field.
- In the **Auto Enrollment** section, the option to configure MS Intune integration with AppViewX has been added. The user can now enroll certificates, with any external CA that configured in the SCEP MS Intune form.
- AppViewX supports libEST for certificate enrollment and re-enrollment process.
- AppviewX now discovers certificates from the Apache TOMCAT server through SSH and Rest agent communication. Going forward, TOMCAT can communicate through SSM and discover certificates from Amazon AWS.
- Terraform provider has been added for new certificate requests
  - The AppViewX Terraform provider is used for creating new certificates through the AppViewX CERT+ platform and download it.
  - Users can install the provider in the Terraform instance and request a new certificate for the specific Certificate Authority settings configured in the CERT+ platform.

  - The provider consists of several input files based on Certificate Authorities where the user just provides the common name and requests the certificate.
  - Users can define other CSR parameters specific to the CA by configuring the CA policy in the CERT+ platform and as well as in a policy JSON from the Terraform.
  - The created certificates can be downloaded in the Terraform environment in a user-defined directory and a specified file format for future DevOps process.
- Automated Certificate Enrollment in the Hashicorp Vault has been introduced.
  - The vault enables you to deal with a whole Public Key Infrastructure (PKI) to guarantee secure correspondence among various applications.
  - The vault has a PKI engine that can store certificates, keys and the CSR. With this secret engine, services can get certificates without going through the usual manual process of generating a private key and CSR, submitting to a CA, and waiting for the verification and signing process to complete.
  - AppViewX has a vault PKI plugin which can be installed on the environment where the vault is running. At the time of plugin installation, users can set the AppViewX endpoint and the CA from which the certificate has to be requested for enrollment.
  - Users can run the common vault PKI certificate commands to enroll new certificates and have the certificates stored in the vault PKI engine.
- Gemalto DPOD HSM integration has been introduced.
  - On-Demand SafeNet Data Protection is a cloud-based platform providing a wide range of cloud HSM and key management services.
  - AppViewX now supports integration with the On-Demand SafeNet Data Protection in the cloud.
  - Users can add the HSM to AppViewX by installing the HSM client on the AppViewX environment. Adding the HSM to AppViewX supports the functionality for generating private keys on the HSM at the time of CSR generation for any Certificate Authority from the AppViewX CERT+ platform.

Security

- Control Center search has been enhanced.
  - Users can search using the source and destination ports (Only For Juniper, Cisco, and Fortigate).
  - Users can search for rules with/without schedulers.
  - Users can search for rules that do not match NAT rules.
  - Users can search for rules having matching nat rules.
  - Users can search for Firewall rules based on the vendor.
- FQDN support for all Firewall and WAF vendors has been introduced.
  - Users can now use FQDN to add a new vendor device and access various capabilities for the AppViewX managed devices.
- Golden configuration has been introduced in Firewall Rules.

  - Users can now customize/standardize the golden configuration (standard template) which would be evaluated across Firewall security rules. Using that rule users can perform the compliance validation that helps to generate the compliance reports.
- Export security & NAT rules from the Control Center.
  - Users can now be able to export the firewall, security, route, and NAT rules from the Control Center.
  - Users can now export reports from the dashboard in .pdf and .xlsx format.

Platform

- The user onboarding UX/UI experience has been simplified using a wizard flow where users can setup Authentication, User groups, Roles, and Resources.
- This respective wizard flow can be accessed through the Quick Configure option in the existing Authentication, User groups, Roles, and Resources screen.
- Users will now be able to set up LDAP, TACACS, RADIUS, SAML authentication details, and priority order as part of the wizard flow.
- The user will be able to add user groups into AppViewX by pulling specific user groups from the Active Directory to AppViewX. This can be performed based on specific patterns/keywords/codes, internal user groups for RADIUS/TACACS/SAML and support Bulk Export/Import options to onboard user groups in the same wizard flow.
- The role creation process is simplified with pre-built ADC, Certificate, Security, and Automation user roles.
- The custom role creation process is simplified by providing information against each ACF (Access Control Function) that explains the significance of the functionality.
- Users can now assign a pre-shipped role/custom role created to the onboarded user groups as part of the Roles stage in the wizard flow.
- Dynamic rule-based resource tagging of newly discovered ADC objects, Certificates based on Query using object/Certificate fields available within AppViewX has been added.
- Dynamic rule-based resource tagging of newly discovered ADC objects, Certificates using a script to tag based on data available with external tools (SNOW, Other CMDB, etc.) has been introduced.
- Rule templates are pre-shipped to ease the dynamic tagging of resources.
- Dynamically created resources can be assigned to the user dynamically by mapping the respective rule to the required user groups as part of the **Rules in Use** inventory in the wizard flow.
- Creation/Management of RBAC rules can also be done from the Studio module.

SSH

- DZDO porting change has been introduced.
- Replacing **Sudo** (Superuser Do) in all Linux commands used by SSH+ to 'Dzdo' (The program uses Role-Based access rights for zones stored in the Active Directory).
- HMAC support has been added.
- Users can now manage devices with the HMAC-256 Algorithm an HMAC-256 (Hash-Based Message Authentication Code).
- **Cloud Tech Card** has been introduced.
- The AWS support that was compromised with the previous version of AppViewX has been fixed in this release.

Reports

- A feedback icon will be displayed at the bottom right and the top-right corner throughout AppViewX. The user can submit feedback for the corresponding module by clicking this icon. You can view the user feedback by downloading the user survey and feedback report from the Reports store. (This option can also be disabled in the Settings section).
- You can now send multiple reports/entire dashboards created using reports to one or multiple users from the Inventory. You can also schedule the reports to be sent at a particular date/time. All the scheduled jobs can be monitored in the **Scheduled Jobs** section to abort, pause or modify it.
- You can now enable/disable the custom collections to be accessible to reports using the query builder.

Workflow

- The **Generate API** icon in the Settings has now been added to the command bar. You can now generate APIs and download the Ansible files by clicking this icon.
- The option to Enable/Disable the **Ansible Executor** has now been added to the YAML editor.
- In the **Field Builder**, a new field type to download the file has been added. You can now download the file from any external URL or a file path.
- In forms, under the **Resources & Settings** section, you can customize the buttons by renaming them for all UI related tasks. For other tasks, it will be available in the Customize Tasks section.

Chapter 2: Fixed Issues

Bug ID	Description	Module
131193	Error in sending an email when there is a mismatch in the unique attributes configured	Automation +
131252	Cloned sub-flow added in the cart is not updated with the configured changes	Automation +
130894	Syslogs are not supported for Fortigate 5.6 and above	Security+
131379	FN: Reports: Unable to remove scheduled time from the inventory after the completion of the reports scheduler	Reports
131632	FN: Reports: Unable to update the last refreshed time when the user clicks the live refresh icon	Reports
131263	LDAP user group - Unable to view the assigned user group in the user group popup screen	Platform
131667	Group change through assign/unassign is successful, so the group change in the edit connector should be freezed	CERT+
130547	Entrust CA does not provide **pending** status in certificate enrollment and hence, auto-approval should be enabled in CA portal	CERT+
131202	When on-demand revocation check call is triggered, CRL logs should contain the certificate authority name	CERT+
131338	Mobileiron rollback is failing when the row count exceeds 50 in device GUI [Update from device side]	CERT+
131355	Websphere: The mapping of the application connectors is improper for certificates discovered from profiles in management scope.	CERT+
131357	Weblogic: The mapping of the application connectors is improper for certificates discovered from profiles in the management scope.	CERT+
131384	Orphan report loads for 50K application connector and does not load when it exceeds 70K certificates.	CERT+
131424	When alias name in certificates gets mismatched, there may be an error in the server profile for Websphere devices.	CERT+

Bug ID	Description	Module
131501	When a user doesn't have access to default group and clicking **Unassign** option from Holistic view, it throws an error "User doesn't have permission to this group" but gets unassigned successfully	CERT+
131211	MQServer - rollback for create label is not working as expected	Rapid SB
131317	CA certificates are not getting pushed to MQServer without a label in all cases - Create KDB, Create a label	Rapid SB
131691	No support for RADWARE	ADC
112869	CC_Infraview_Column based filter_RangeSlider initial values are not maintained correctly in UI by default	ADC
131377	ApplicationView: Getting **500 InternalServerError** when the user restricts actions only in the parent group and performs action by selecting objects of different levels of groups.	ADC
131417	AVI - For an object which has down status, a red pattern should be shown	ADC
127728	Device Inventory - Switch and Router - Cannot add a device with Credential List	Switches
127092	AppViewX 12.4 VW - Every task in VW takes almost 1.5 or 2 minutes to complete	VW
129732	Unable to manage Fortigate devices	Security+
130853	Unable to send emails	Platform
130617	Access log rollover does not occur	Installation
131733	Migration_Backup Download icon for an individual file is not available for migrated backups	ADC

Chapter 3: Known Issues

Bug ID	Category	Subject	Possible Fix Date
133646	Deployment	During the restart of the components, the Start log's file size becomes large	20th Feb 2020
133605	ADC	Resource name with % special character is not supported in ADC object ACL	3rd March 2020
133597	Platform	When a new role with Full ACF permission is added and the Save button is clicked all the suboptions expect ACF "general" gets selected.	2020.2
133546	ADC	The device which has **Read** permission from the Control Center and when the restore function is enabled, the device with **Read** permission needs to restrict the restore function	31st March 2020
133489	Cert+	Performance time taken is high for Count by issuer settings page when 20k+ CA certificates are available.	2020.3
133480	Cert+	On denying the pending request in entrust CA portal, the certificate status is not getting updated in certificate holistic view	31st March 2020
133404	Platform	No proper field validation for resource and certificate group name field in RBAC rule configuration page	2020.2
133373	Visual Workflow	Request Fails due to "Review task" failover link + UI status	2020.2
133361	ADC	VIP Under Wide IP Structure is not rendered for IPV6 RD Objects in F5.	15th, March 2020
132935	ADC	AVI under F5 (Vip under Vip)- AVI VSV Port Range matches with 2 different servers of F5 LTM pool member means connections are missing	2020.2
132910	Visual Workflow	Special character " * " in subflow cannot be dragged to workspace	2020.2

Bug ID	Category	Subject	Possible Fix Date
132909	Platform	While creating the same name in Proxy settings, a Log Forwarding Internal Server Error is thrown	2020.2
132732	ADC	Citrix Server actions are not performed and an exception is thrown. Audit logs should be covered for this failure scenario	15th, March 2020
132630	Rapid SB Connectors	MQServer >> On pushing a certificate without a key, the server certificate is pushed in the PEM format	28th, February 2020
132008	Rapid SB Connectors	MQServer - Endpoint CSR generation fails for EC Key Type	28th, February 2020
131898	Rapid SB Connectors	On pushing certificate to Linux with DER, PKCS7 types, server, intermediate and root certificates are pushed in PEM format.	28th, February 2020
131542	Platform	In SMTP page, after disabling the Authorization required and trying **Test** option, it displays an error message "This field is mandatory" across username and password in the Authorization required field	3rd, March 2020
131358	Visual Workflow	New user folder cannot be renamed with a special character	2020.2
129239	ADC	Dashboard_ApplicationView_Clicking on view topology for the first time renders the dashboard page instead of the CC topology view	3rd, March 2020
128752	Platform	Threshold alert is not generated when the threshold alert and Syslog alert is created with the same name.	2020.2
126977	ADC	iHealth is not generated - F5 Login Portal is in progress for more than 4 hours if case.no has been provided	2020.2
113720	Visual Workflow	When RGF flow is disabled and if the submitter rejects the form, both the creator and the reviewer can access the request	2020.2

Bug ID	Category	Subject	Possible Fix Date
133654	ADC	Unable to perform an action for LTM - Node of FQDN type action	31st, March 2020
133682	ADC	Statistics are not getting collected for IPV6 type service group member	2020.2
133681	ADC	The search of Orphan GTM Pool Member displays "No result found".	2020.2
133778	ADC	F5V15-ClassManagement_ExternalClassUpload throws 500 internal server error - intermittently	2020.2
133786	ADC	View Actions(which should be navigated to the second page) are not working from Open in new window	2020.2

Chapter 4: Limitations

ADC

- In device management,
  - If you want the FDQN devices to be managed using CyberArk credentials then it is recommended that the FQDN devices are added with a trailing dot in the CyberArk vault.
  - CyberArk authentication is not supported for the A10 devices.
  - CyberArk and AppViewX credentials are not supported for Akamai devices.
  - If the IP/FQDN/device name is already present in AppViewX, the device with the same details cannot be added to the Inventory.
  - Configuration fetch can be triggered for devices in the ‘Queued’ or ‘In progress’ status after five minutes on a FIFO basis.
  - If there is an exclamatory mark (!) in the credential of a proxy setting, the connection will not be established.
  - The Big-IP system intermittently fails to authenticate the users with valid credentials. For detailed information, refer to the following link: https://support.f5.com/csp/article/K15285.
- The MongoDB supports parsing of the configuration file less than 16MB. The class files for the F5 device fails if it exceeds 16MB.
- F5 v12 DNS records are not supported in the device management and control center.
- In F5 devices, the external class files that have more than 1,20,000 records will not be parsed.
- F5 devices can be managed using the Admin and Cert Manager role only.
- AVI devices can be managed only using a management IP address and the credentials provided must be a super-user.
- Actions are not supported on AVI IPv6 objects.
- The recursive topology view for AVI and Nginx Plus SLB objects are not supported.
- NAT IP based device addition is not supported for Citrix devices.
  - GSLB Server actions are not supported for Citrix devices.
- Orphan Objects are not supported for Citrix and Amazon ELB devices.
- Cisco GSS is not supported.
- The import and export of devices are not supported by Amazon ELB and Akamai.
- A10 v2 server objects are not supported.
- Configuring the DNS name in the display name format cannot be reordered.
- 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.
  - iHealth QKView download cannot be handled for file sizes of more than 200 MB.

- The python scripts must contain SHEBANG in the python installed directory to run them in the script execution widget.
- Updating the object configuration change based on SYSLOG has the following limitations:
  - In the case of an object state change, if the hostname matches with more than one device name, the respective Syslog will be ignored.
  - Syslog under the 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 through syslogs will be processed until the device config fetch is complete.
  - 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.
  - Syslog based configuration updates are not supported for other partition Cirix objects.
  - For A10 devices, if the Syslog is subscribed using a logstash hostname, it should not be more than 29 characters.
  - Any modification in the device boot location recommends Config fetch to receive SYSLOG(s).
  - SYSLOG 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.
- The usage of logical operators between a primary and secondary keyword is not supported in the Control Center.
- The AVI pool-group is not supported in the Control Center and Dashboard modules.
- Trap from the A10, AVI, and Citrix devices will not be available in the AppViewX alerts module.
- The read actions from AppViewX will be redirected to the respective devices. However, the object writes action configurations that can be defined in the settings.
- In Backup and restore,
  - For AVI, Device Backup fails when more than one tenant is present.
  - The cross version device restores for F5 is not supported.
  - The object restore is not supported for F5 v10 and AVI devices.
  - During object comparison, if the selected objects (with the same name) are available in multiple partitions, then the comparison will be performed on a random configuration.
  - The object/environment comparison is available only for the F5 devices. However, it is not supported for the F5 objects GTM pool member, GTM virtual server, LTM pool member, child Wide IP, records, interfaces, VLAN, self IPs, SNAT translation list, and traffic group.
- The Import option in the Dashboard – Application widget does not support objects of different devices at a time.

- In the Application View widget,
  - Actions cannot be configured or performed on an empty group.
  - Actions can be customized for an object type and not for the individual objects.
  - There is no auto-suggest option when you configure an object.
  - (For application widgets only) To handle the device flip and monitor the active objects seamlessly, an option Show only active is available in the dashboard settings.
- In the Traffic Statistics widget,
  - The tooltip will not be displayed if statistics for any of the parameter is not collected.
  - The explicit IP address is not supported for F5 v12 and V13 devices.
  - If the Traffic Statistics widget has been monitored for more than two hours in the Mozilla Firefox browser, it 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 have been reset.
  - The DAY filter in the TOP 10 VIP(s) by Connection and Top 25 Application Connection widgets represents the data for the 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 by the AVI GSLB devices.
  - Statistics will not be collected for F5 WideIP type SRV and NAPTR.

Platform

- This dynamic resource tagging is available only for newly discovered ADC objects and certificates.
- Objects/Certificates and respective permissions that are a part of the existing resources will not be updated/changed.
- All the existing User groups, Roles, and Resources screen functionalities will function as normal and the data will be in sync with the wizard flow screens.
- The migration of data tagging with existing resources to an RBAC rule is not supported as part of this phase. Users need to create new rules to perform dynamic tagging of resources.
- When the user is trying to provide access for General settings in the Role-Authorized functions page, AppViewX will select all settings, but it appears that only certain settings are selected.

Certificate

- With AppViewX EST client,
  - Only certificate enrollment and re-enrollment actions are supported.
  - Only one certificate can be requested for enrolment and re-enrollment at a time by the end machine.
  - The only certificate with the TLS authentication type is supported.

  - HTTP auth basic and digest are supported only in curl.
  - ‘anyauth’ is not supported in AppViewX.
  - MAC - EST client script has to be executed manually.
  - Linux - The execution of the EST client script can be automated using crontab.
- In Authentication Mode for ‘Certificate TLS with HTTP as fallback’ option, the client certificate is mandatory in the client request.
- Cloud devices added before 2019.4.0 have to be manually deleted and re-added to AppViewX.
- For MDM integration with AppViewX through SCEP, only certificate enrolment is currently supported.