appviewX

Release Notes

Version: 2020.3.0

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
1.4	Revised to update the New Features section.	November 2021
1.3	Revised to add limitation for ADC+.	July 2021
1.2	Revised to update the Fixed Issue section.	May 2021
1.1	Revised to update the Known Issue section.	April 2021
1.0	New Release of AppViewX v20.3.0	September 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: Introduction

AppViewX product contains the following modules: ADC+, CERT+, Platform, Security+, SSH+, and Workflow modules.

These release notes accompany AppViewX Release v2020.3.0 for the ADC+, CERT+, Platform, Security +, SSH+, and Workflow modules. They describe new feature, known limitation, and known and fixed problems in the software.

You can also find these release notes on the AppViewX Documentation webpage, located at https://adminguide.appviewx.com/release-notes-2.

Chapter 2: New Features

This section describes the new features in AppViewX v20.3.0 release for the ADC+, CERT+, Platform, Security+, SSH+, and Workflow modules.

ADC+

- **F5 Application State/Status Report APIs**
  - Application State/Status trend or fluctuation reports are built to fetch and decommission the virtuals servers or applications that are unused throughout a particular period.
  - AppViewX collects the State and Status of F5 Applications based on the following notifications,
    - Midnight Config Fetch
    - Device Addition
    - Manual Config Fetch
    - Syslog notification
    - Enable/Disable operation
  - These APIs fetch the status/status trend of an object. [supports a maximum of 100 flip counts by default which can be configured],
    - adc-object-state-trend-fetch
    - adc-object-status-trend-fetch
- **Automate Device Backup using Regex**
  - Ability to configure regex in the Backup group settings so that new devices discovered in AppViewX will be automatically added to the group for backup generation.
  - The backups can be generated on-demand or scheduled for a specific time frame.
  - AppViewX will notify the successful/failure backup generation.
- **Customize Action Comment Prompt**
  - Ability to provide customized placeholder in the dashboard.
  - Users can refer to the control center comments for details that are provided during action execution.
- **Multi-select Consistency**
  - Multi-selection on objects from the control center and dashboard are made consistent with a checkbox so that the user is aware of how to select objects and review the selected objects before executing actions.
- **Alert on In-progress Devices**

- AppViewX actively monitors the ADC devices that remain in In-progress for more than a specified interval (default is set to 2 hours which can be modified).
- The devices that match the criteria will be picked and raised as a critical device alert in the alerting module.
- To get notified about the device status, the user can configure email notification alerts in the alerts module.

- **Service Catalog for ADC Roles - MVP**
  - A self-service portal to access all service offerings for employees through a Single Pane of Glass.
  - ADC roles like Application Manager, Network Manager, and Admin are shipped with catalogs that can be set as a landing page by the Admin.
  - A provision to clone and customize the catalogs before publishing is also available.

CERT+

- **Manage Certificates from MS Servers Deployed in AWS (SSM Agent)**
  - Amazon AWS services, EC2 instances are now integrated with AppViewX (under cloud inventory) which identifies the windows instances deployed in the Amazon AWS cloud environment and manages the certificates within those server instances.
  - The regions scanned and the total count of windows instances discovered will be displayed in the cloud inventory.
  - Instance details and certificate discovery status will automatically be available in the server inventory.
- **Trust anchor push – IBM Client/Linux**
  - Ability to push trust certificates by navigating to the trust certificate holistic view and pushing them to the Linux device configured in AppViewX without the server certificates, from the new root and intermediate inventory.
- **Push only Server Certificate in PEM and DER Certificate Format**
  - Generic Linux connector which supports PEM and DER format during certificate push also supports the concatenation of the certificate.
  - By default, root and intermediate are concatenated with server certificates.
  - Provisions are now provided to select push preferences, such as Chain, Issuer and Server, and Server. Based on the user selection, push certificate triggers.
- **Application Connector for iLO**
  - Ability to add iLO in AppViewX to discover and bind certificates.
  - Once the iLO is successfully configured in AppViewX, users can enroll for a certificate from a third-party Certificate Authority by generating CSR in the end device.
  - On successful creation of the certificate, users can push the certificate into the iLO using the iLO application connector.
  - Ability to regenerate the certificate by replacing the expired certificate with the regenerated certificate.

- **REST Agent - Generic Linux**
  - Earlier, AppViewX used the SSH mode of communication to discover and push certificates to the Linux device.
  - Users have a provision to change the communication mode as REST Agent.
  - It is mandatory to deploy and run the REST Agent within the Linux device that helps to establish the communication to discover certificates.
  - On successful configuration of setting the communication mode as REST Agent, the certificates are discovered and managed in AppViewX.
- **Secure CSR and Private Key in the End Device - Apache [windows]/Tomcat [windows] Deployed in AWS Cloud Environment**
  - AppViewX can secure the CSR and private key in the Apache [windows]/Tomcat [windows] instance deployed within the Amazon AWS cloud environment by configuring the Apache/Tomcat instance in AppViewX.
  - Once the instance is successfully configured, the users can enroll for a certificate from a third-party certificate authority by generating the CSR within the Apache/Tomcat instance.
- **JBoss [Windows] - Version Configuration Removal from UI and Import**
  - AppViewX can fetch the versions automatically using the version fetch commands when the user specifies the JBoss version while configuring the device in AppViewX.
  - AppViewX supported JBoss server versions: GA 4.0.5, EAP 6.4, and EAP 7.0.
- **KDB Format Support - Generic Linux**
  - Users can configure the Linux device under the Generic Linux connector.
  - When you add a Generic Linux application connector to a certificate, users can create a KDB file, a KDB label, and push the certificate in KDB formats into the Linux Device.
- **FQDN and SUDO Support - Generic Linux**
  - AppViewX is accommodating FQDN while adding Linux devices under Generic Linux.
  - Users can either provide an IP address (or) FQDN to add the Linux device.
  - AppViewX resolves FQDN to its IP address and proceeds with certificate scanning.
  - When you add a Linux device, users can select the access elevation as ***Sudo***, which allows only the sudo users to proceed with certificate scanning.
- **UI Changes**
  - When you create a new certificate group, spaces and specials characters are allowed for the group name.
  - The add connector pop-up window is now available in full-screen and the option to minimize/maximize the screen is removed.
  - A detailed description has been added for each field under Policy, Certificate Authority, Discovery, and Group.

- Enhanced the usability of the Approve/Implement pop-up window in Certificate Authority and device workflow.
- In the holistic view, auto-refresh is triggered every 10 seconds.
- Access to select the server and client certificates from CA Switch through the CERT menu.
- Enhanced the CERT menu by introducing detailed sub-menus for discovery.
- Improved certificate bulk renew operation to trigger the renew immediately instead of waiting for the next scheduled job to pick the renew request.
- Improved the network scanning in the discovery module by introducing a new option called scanning intensity.

Install and Upgrade

- Transport Layer Security (TLS)
  - Secure Sockets Layer (SSL) is an encryption protocol intended to keep data secure in transit over a network. At present TLS v1.2 and TLS v1.3 are recommended. All other protocol versions are deprecated in 2018 by Apple, Google, Microsoft, and Mozilla. To disable deprecated TLS versions, new configuration parameter <ENABLE_LOWER_TLS> is added in <appviewx.conf> as part of the apply patch. This will provide options to either enable or disable TLS v1.0 or v1.1 communication between AppViewX and devices.
  - AppViewX recommends keeping the default value of the flag set to enable TLS v1.2 and enhance the infrastructure to support TLS v1.2 to be on the right security posture.

Platform

- **Logs in the SIEM Standard**
  - AppViewX has introduced a new toggle under Forwarding Settings for the user to toggle between log formats (SIEM and Syslog) for sending logs to an external server.
  - This SIEM tool stores, normalizes, aggregates, and applies analytics to that data to discover trends, detect threats, and enable organizations to investigate any alerts.
- **Notifying Number of Objects Selected using RegEx**
  - During the regex assignment, when the user clicks Add RegEx, the product will display a notification with the total number of objects selected at that given time.
  - It notifies that all the future objects will be assigned automatically. (A notification appears when the user hover over the Add RegEx button).
- **User Settings**

A new feature is introduced in the Authentication section under a new tab called User Settings.

- **Create a user on authorization failure (Toggle):** Users can enable this option in AppViewX if the user is authenticated but authorization fails.
- **Create a user with a unique email ID (Toggle):** Users can enable this option if there should be a unique email ID for all AppViewX users.
- **Session timeout (Text field with input in minutes):** Users can enter the idle web session timeout limit in minutes. The default value is 15 minutes.

- **Purging**

A new setting section called Purging is introduced under the General tab. There will be two tabs: Alerts/ Logging.

- **Alerts**
  - **Alert Purge Duration:** Enter the duration (in days) after the purging happens.
  - **Maximum Alerts Count:** Enter the maximum count of alerts that has to be maintained.

> **Note:** When the count value is set to 30,000 and the duration as 50 days:
> - **Count exceeds before the duration ends:** If there are 50,000 alerts received within 50 days, the latest 30,000 alerts will be stored and the rest will be purged.
> - **Duration reached before the count exceeds:** If the duration limit is reached (50 days) before the count limit (30,000), all alerts received during that period will be purged.

- **Logging**
  - **Logging Purge Duration:** User can enter the duration (in days) after the purging happens.
  - **Maximum Logging Count:** Users can enter the maximum count of logs that has to be maintained.

> **Note:** When the count value is set to 30,000 and the duration as 50 days:
> - **Count exceeds before the duration ends:** If there are 50,000 logs received within 50 days, the latest 30,000 logs will be stored and the rest will be purged.
> - **Duration reached before the count exceeds:** If the duration limit is reached (50 days) before the count limit (30,000), all logs received during that period will be purged.

- **Additional Setting in the SSO Configuration**

Under **Config** Information, the three fields were not editable for users in earlier versions of AppViewX. Now, the prefix for each field can be configured by the user.

Host: This is a text field that is repopulated with the current machine hostname that the product is running on. When this value is modified, it will be updated in the following fields with the mentioned suffix.

Entity ID: https://<VIP/WIP>/appviewx/ (Here VIP/WIP is the host).

Service URL: https://<VIP/WIP>/appviewx/ssoLogin (Here VIP/WIP is the host).

SLO URL: https://<VIP/WIP>/appviewx/logout (Here VIP/WIP is the editable host).

Note: When the user clicks the copy icon, the entire URL should be copied to the clipboard.

- **Changing the Password during First Time Login**
  - When the admin logs in the first time, a box appears that displays an option to change the password: **It is recommended to change your password before you continue using AppViewX**.
  - Once the password is changed or even if **Cancel** is clicked, the user will be redirected to the generic landing page for the consecutive login.
- **Pages Enhancement**
  - Earlier when the AppViewX logo is clicked it will display the version details.
  - Now the implementation is done in a way that when clicked, the landing page that the user has specified in User Preferences will be redirected to.
  - The version details are moved to a new location and will be displayed when the user clicks the three dots at the top right.
  - When the user sets a page built using the Page builder module as the landing page, there will be a small shutter icon that the user can use to hide or unhide the header bar on the landing page. This shutter icon will not be available if the user sets any other native page. For example: Dashboard as the landing page.
  - 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.

Security+

- **Revamp: Default Column Selections for Inventory and Control Center**

  The existing keywords are grouped based on their applicable search type Security/Nat/Route which makes the keyword identification better.

- **Policy Name Removal**
  - Removal Policy Name for all Vendor Device Addition Screens
  - Removal from Import Sheet
  - Removal from Reports
  - Removal from Control Centre

- Removal from all Implication Areas Like FW Rule Comparison, Config Drift, Traceroute, Goldenconfig, Backup-Restore, Risk Setting, CRUD Operations
- Complete Code Clean-Up For This Specific Field
- API Refinement.

- **Fortigate and FortiManager v6.2 Parsing**

  Vendor support is provided for the below product features,

  - Device Management
  - Control Center - NAT ROUTE and SECURITY support
  - Control Center - keyword Search
  - Dashboard Reports
  - Config Drift
  - Risk Setting
  - Golden Config Comparison
  - FW Rule Comparison
  - Trace Route
  - Backup and Restore.

Workflow

- **Visual Workflow (Service Orchestration and Automation Platform - SOAP)**
  - **Jenkins CI/CD Orchestration**
    - Integrated with Jenkins - Southbound and Northbound.
    - Integrated with Jenkins pipeline and orchestrating application services.
    - Jenkins CI/CD orchestration with AppViewX (VW) using OOB Jenkins tasks are triggered.
    - Pre-built (out of the box) tasks for triggering Jenkins job, pipelines, and authentication.
  - **DevOps - Ansible Tower Integration**
    - Integrated with Continuous Configuration Automation (CCA) - Ansible Tower.
    - Pre-built automation tasks are configured to integrate between AppViewX and Ansible Tower.
  - **GitHub Integration**
    - Integrated with GitHub.
    - Pre-built GitHub automation tasks are configured to integrate between AppViewX and GitHub.
    - Pre-built Git CLI automation tasks are configured to integrate between AppViewX and Git.
  - **GitLab Integration**
    - Integrated with GitLab.
    - Pre-built GitLab automation tasks are configured to integrate between AppViewX and GitLab.

- **Integration Platform as a Service (iPaaS)**

  A generic integration as a service (marketplace) is provided to enable faster integrations, automation through REST API, and SSH modes across multiple vendors.

- **REST API Task Enhancements**
  - **Enhanced REST API Authentication Mode Support**

    The following are types of authentication methods:

    - Basic Authentication
    - Bearer Token
    - API Key
    - Digest Authentication
    - AWS Signature
    - Akamai EdgeGrid.
  - **Inherit Integrations**

    REST API support to inherit from **Integration as a service** across one or more vendors.

- **Git (Source Control Integration)**

  DevOps Value Stream (CI/CD) Automation - GitOps

  Automate DevOps and SecOps Deployments with CI/CD Pipeline Integration

  - **Native source control integration with - GitHub, GitLab, BitBucket (cloud and on-premise)**
    - Low Code Platform to rapidly build and deploy applications from one or more pipelines.
    - Provision to integrate with Git.
    - Provision to pull and push workflows and tasks from the Git repository.
    - Provision to create and manage repositories on Git.
  - **GitOps Review**
    - Provision application and security services with GitOps review and compliance.
    - Any automated provisioning process can be committed and reviewed on Git for compliance checks.
    - Based on the configurations, AppViewX can receive an event and automatically provision and close the change management loop.
- **Pseudo form Enhancements**
  - Enhanced preview capabilities to display key workflow tasks in a form-based view (under Preview).
  - Schedule tasks, YAML, skype, email, command, API, and scripts.
- **CLI Command Task**
  - A new task called CLI Configure/Command Task (YAML Structure) is introduced.
  - Provision is provided to execute commands easily.

  - Provision to have command execution with in-built rules and rule criteria with event handling is provided.
  - Pre-built OOB command tasks across multiple vendors is available.
- **aPaaS - Redhat (OSE) Openshift container Integration**
  - Faster deployment cycles to get business applications to market.
  - Enables deployment of new digital products and services across the hybrid cloud for scalability.
  - Kubernetes container platform with full-stack automated operations to manage hybrid cloud and multi-cloud deployments is available.
  - Helps organizations move traditional application infrastructure and platforms from physical, virtual mediums to the cloud.
  - Native Service Orchestration and Integration of VW (SOAP) with Red Hat Openshift (a PaaS Platform) for application provisioning.
  - Automate set up of Openshift via Open Service Broker (OSB).
  - Secure DevOps PKI Orchestration with Opeshift and Visual workflow.
- **Archival and Restore of Automation Requests**
  - Provision to archive workflow requests by status, date/time.
  - Provision to restore (archived) workflow requests.
  - Provision to purge (archived) workflow requests.
- **Automation Collision**

  Automation collision validates duplicate configurations across workflow requests.

  - Pre-built cross workflow validation tasks to check for automation collision of configurations.
  - Automation collision tasks for F5.
  - Automation collision tasks for AVI.
  - Automation collision tasks for A10.
- **ADC/LBaaS Automation**
  - Pre-built modular tasks for F5-BIG IP automation across modules.
  - Pre-built solutions for F5-BIG IP app services automation across modules.
  - Pre-built modular tasks for AVI automation across modules.
  - Pre-built solutions for AVI SLB/GSLB automation.
  - Pre-built modular tasks for DNS automation across Infoblox and TCP Wave Bluecat.

Low Code Pages (Catalog)

- Enhanced UX and UI design of pages and page elements.
- Provision for single-page and tab layouts.
- Introduction of Tabs (horizontal and vertical) as a page element.
- Enhanced HTML widget with UI plugins (JQuery and Bootstrap) with pre-built HTML samples.

- Search widget: Introduction of search widget for application search, certificates search, and firewall policies.
- Enhanced landing page preferences with RBAC.
- Alert widget: Introduction of alert widget to track workflow status.
- OOB Catalogs: Pre-built OOB catalogs by persona (NetOps, SecOps)

Chapter 3: Known Limitations

This section contains the known limitations in AppViewX v20.3.0 release for the ADC+, CERT+, Platform, Security+, SSH+, and Workflow modules.

ADC+

- The devices that remain at In-progress, cannot be terminated due to technical challenges and can be notified to the user.
- The ADC reports in the Application monitoring tab, cannot be customized until they are abstracted.
- When multiple quick actions performed in the AppViewX's GUI for an object the actions are executed in random order and results in an undesired state. In this case, perform any of the following:
  - Perform the same action again to get the correct status in the desired state.
  - Check the status of the object and the previous action before performing another action on the same object.

Platform

- The RegEx feature is only applicable to ADC+.
- The SIEM feature is only applicable to CERT+.

CERT+

- **Manage Certificates from MS Servers Deployed in AWS (SSM Agent)**

  Microsoft server versions supported,

  - Microsoft Windows Server 2012 R2 Standard
  - Microsoft Windows Server 2016
  - Microsoft Windows Server 2008 R2.
- **Trust anchor push – IBM Client/Linux**

  Users cannot create a KDB file and push the certificate.
- **Push only Server Certificate in PEM and DER Certificate Format**
  - Users do not have provisions to concatenate root and server by eliminating the intermediate certificates.
  - Users must use the root/intermediate inventory to push the trust certificate into the end device.
- **Application Connector for iLO**
  - Discovers only the server certificate.
  - Supports only <.pem> format.

- **Secure CSR and Private Key in the End Device - Apache [windows]/Tomcat [windows] Deployed in AWS Cloud Environment**

  Only RSA bit type with bit length less than 4096 can be created.

Chapter 4: Known Issues

This section lists the known issues in AppViewX v20.3.0 release for the ADC+, CERT+, Platform, Security +, SSH+, and Workflow modules.

S/N	Description	Module
1	Cyberark integration - When fetch credential is triggered from CLI, it fails to decrypt the message (action inside the pod).	Platform
2	During the session timeout pop-up, the menu icon can be clicked, hence the page is redirected to IP: Port (web), and getting page not is found error is thrown.	Platform
3	When invalid IP and port are configured in log forwarding for UDP, the status in the database is shown as "config status": ok for forwarding the logs which is incorrect.	Platform
4	Alerts are not raised for license upload or activation failure - Improvement.	Platform
5	Super access resource with permission to all resources in AppViewX is modifiable.	Platform
6	In Audit, log-Action executed successfully log shows as an action performed in the standby device even though the action is performed in an inactive device.	ADC
7	In the Statistics settings page - After selecting the time interval and changing the vendor type, the selected time interval should be retained.	ADC
8	In Dashboard - Actions which is triggered via workflow is getting failed in the migration node.	ADC
9	A10 statistics collection fails when both VCs and vrrp is disabled in a standalone device.	ADC
10	State and Status of the objects updated via syslog is not taken for state and status drift API.	ADC
11	In Akamai - Action will not be performed for one data center to an object. A proper log must show for the action that cannot be performed.	ADC
12	Unable to modify credentials for devices that are added in the **Others** tab.	ADC
13	Migration_Single Device Deletion takes more than 20 seconds.	ADC

S/N	Description	Module
14	Script Execution: Status color is shown in RED even if the execution script is successful.	ADC
15	Search and export in the ADC page has different data.	ADC
16	Inconsistent F5 device Parsing Failure and Device status remains at In-Progress.	ADC
17	A threshold alert is not generated when the threshold alert and syslog alert are created with the same name.	ADC
18	Dashboard - AppView -> Create an Appwidget in a new user or a new deployment, undefined is thrown - intermittently.	ADC
19	When the user logins, the landing page is navigated to Published -> Inventory page in Page builder (Inconsistent).	Page Builder
20	Once a page is set as a landing page for the birthright role usergroup, it cannot be removed/overwritten with another page from the page builder.	Page Builder
21	Catalogs created by a user associated with the Birthright User Group doesn't get listed when it is shared with any other user.	Page Builder
22	Banner messages for different widgets In Pages based on the ACF of other modules is not relatable.	Page Builder
23	Gateway profile names are not displayed in the "status all" command.	Architecture
24	Tenant based <.js> files are not found in Kubernetes deployment.	Architecture
25	Need provision to raise alerts for free disk space, and memory usage of the appviewx running node.	Architecture
26	Not getting appviewx logs like free disk space, and memory usage of appviewx nodes in the logging and alerts module.	Architecture
27	In the Logging module "appviewx node" column hostname or IP is not mentioned and instead pod name is displayed.	Architecture
28	Discover AppViewX, Custom Discovery, GSLB, and SLB templates get failed.	AppVision

S/N	Description	Module
29	AppViewx Revoke is getting failed with the error "Crl update failed while getting crl holder encoded value."	CERT
30	REST agent-based device addition - Kube deployment model.	CERT
31	HSM based encryption - Dependency on Platform for device addition integration part.	CERT
32	ECDSA curve value is not shown in 'Inventory', 'Certificate Details Pop up', and the CA connector until the compliance check happens for those certificates when migrated from earlier versions of the product.	CERT
33	If there are 65,536 batches, it takes time to add and load in a table view.	CERT
34	On pushing an EC type certificate generated with endpoint source (KDB), to the same KDB in Linux server with the private key in device option, push is getting failed.	CERT
35	IBMClient (Linux): If the same cert is pushed to jks with different aliases, on discovery only one alias is discovered.	CERT
36	Nginx: On generating CSR in device with EC key type and bit length 224, cert is getting generated with 384-bit length.	CERT
37	Certificate Transparency reports response does not contain serial numbers due to change in the Google CT search response structure.	CERT
38	On submitting a parallel request continuously from EST, "Exception occurs while submitting CSR" is thrown.	CERT
39	Customer Difficulties in Server import - the user is unable to identify the Server import sheet missing headers.	CERT
40	High CPU on Mongo DB Node while creating a Certificate via Gateway.	CERT
41	Getting started section for CERT+ is now serving the purpose as expected.	CERT
42	Differences in IP range/Subnet discovery in the Kube environment compared with the normal environment because of bandwidth variations.	CERT
43	When triggering bulk renew for more than 2000 certificates, it is taking 9 seconds which should not take more than 5 seconds.	CERT

S/N	Description	Module
44	Performance time taken is high for count by issuer settings page when 20k+ CA certificates are available.	CERT
45	Due to the java upgrade from v1.8.222 to v1.8.262 Following EC curves are failing because of the java upgrade. ec431 Mapped Curve : c2tnb431r1t ec239 Mapped Curve : c2tnb239v2t ec193 Mapped Curve : sect193r2t ec409 Mapped Curve : sect409k1t ec192 Mapped Curve : secp192r1prime192v1t ec233 Mapped Curve : sect233k1t ec571 Mapped Curve : sect571r1B-571t ec192 Mapped Curve : brainpoolp192r1t ec283 Mapped Curve : sect283r1B-283t ec239 Mapped Curve : sect239k1t ec239 Mapped Curve : prime239v3t ec239 Mapped Curve : c2tnb239v1t ec224 Mapped Curve : secp224k1t ec320 Mapped Curve : brainpoolP320r1t ec233 Mapped Curve : sect233r1B-233t ec239 Mapped Curve : prime239v1t ec239 Mapped Curve : prime239v2t ec283 Mapped Curve : sect283k1t ec224 Mapped Curve : secp224r1P-224t ec384 Mapped Curve : brainpoolP384r1t	CERT

S/N	Description	Module
	ec512 Mapped Curve : brainpoolP512r1t ec193 Mapped Curve : sect193r1t ec191 Mapped Curve : c2tnb191v3t ec359 Mapped Curve : c2tnb359v1t ec224 Mapped Curve : brainpoolP224r1t ec239 Mapped Curve : c2tnb239v3t ec191 Mapped Curve : c2tnb191v3t ec256 Mapped Curve : brainpoolP256r1t	
46	When RGF flow is disabled, if the submitter rejects the form, both creator and reviewer can access the request.	VW
47	IE - request page-chart being displayed is very small.	VW
48	The grid shows different values apart from added values.	VW
49	VW: When the VW template is opened with disabled mode, enabled in another tab, the backend still accepts changes in the enabled template.	VW
50	VW Cancel a request does not work.	VW
51	After menu implementations, the work order status update for CA actions and also Push actions is taking nearly 15 seconds which affects the performance.	VW
52	Pseudo form in script and mail task.	VW
53	Imported VW tasks fail (randomly) until its simply open and saved.	VW
54	Not able to push a file from server to server.	VW
55	ITSM-Fails at Validate and Ansible Executor fails intermittently.	VW
56	Migration - DiffChecker Task Displays twice in UserInterface Menu.	VW
57	Newly allowed Special characters in roles/user/UserGroup/Resources impact over VW.	VW

S/N	Description	Module
58	Request Page -> All Request tab count does not show zero (0) when new user and (admin user for the first time) logins to the application	VW
59	Enable workflow API fails intermittently.	VW
60	Need to change gateway port hardcoded in collection update workflow.	VW
61	Command Task - Validator Check is required and Error Banner should throw an error if invalid config is given.	VW
62	Enable approval via email option fails.	VW
63	Request pages show improper count in all.	VW
64	Control Center Search - Auto suggestion to list Firewall devices for the keyword device is not working properly.	Security
65	WAF backup is not working in Kube deployment	Security
66	Templates to create/modify/delete Fortigate with multiple VDOMs are not working.	Security
67	Templates to create/modify/delete Fortigate and Fortimanager CNAT is not working.	Security
68	Firewall risk is not displayed in the control center.	Security
69	FirewallNB: CC: Rules which has IPv6 address do not bring values on CC search for some vendors.	Security

Chapter 5: Fixed Issues

This section lists the issues fixed in AppViewX v20.3.0 release for the ADC+, CERT+, Platform, Security +, SSH+, and Workflow modules.

S/No	Description	Module
1	After you create a certificate by uploading the CSR, if user tries to reissue the same with Upload CSR and rejects in the portal and again reissue by changing CSR as AppViewX by adding SAN, Reissue Retrieval does not work.	CERT
2	Unable to export filtered data from the inventory using the new menu export option.	CERT
3	In 12.4.2, the user was able to create a role with Connector actions enabled and No permissions given to Server and CodeSigning, after migration of the View Inventory for that role, the Server and Codesigning should be selected.	Platform
4	AVI under F5 (Vip under Vip) - AVI VSV Port Range matches with two different servers of F5 LTM pool member that is connections are missing.	ADC
5	Dashboard_ApplicationView_Clicking on view topology for the first time, it renders the dashboard page instead of the CC topology view.	ADC
6	Device gets failed - Role fetch gets failed when added with cyberark mode.	ADC
7	CC_Arp -> Enable/Disable comments are not set as mandatory.	ADC
8	Logging: No error logs get captured when the user acts on Unresolved/Failed device objects.	ADC
9	Syslog remote server (AppViewX Environment IP) is not removed from the device when the device deletes it from AppViewX.	ADC
10	In the 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
11	Traffic Grid: Status of Unresolved device objects is not shown in grey color.	ADC - Dashboard
12	In the Device Heatmap widget - the Device name is not getting populated in the device block.	ADC
13	VW Cancel a request does not work.	Visual Workflow

S/No	Description	Module
14	After you create certificates by uploading the CSR and when a user tries to reissue the same with Upload CSR and then rejects it in the portal and again Reissue by changing CSR as AppViewX and adding SAN, Reissue Retrieval does not work.	Cert+
15	Unable to export filtered data from the inventory using the new menu export option.	Cert+
16	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
17	ASA Hit count issue.	Security
18	Hit Count Mismatch.	Security
19	Vendor plugin is not starting up when HSM is enabled.	Install and Upgrade
20	External certificate lost on plugin upgrades	Install and Upgrade
21	MongoDB, vault backup, and restore issues	Install and Upgrade
22	If addons are not added under appviewx_kubernetes, prerequisite check should get failed during deployment	Install and Upgrade
23	Web socket issue	Install and Upgrade
24	Email approval is not working in visual workflow	Visual Workflow
25	Functionality to validate the appviewx.conf as a pre validation.	Install and Upgrade
26	Graceful shutdown of AppViewX cluster.	Install and Upgrade
27	Password less installation of AppViewX.	Install and Upgrade
28	Provided a static port for EST(30021) and SCEP(30022).	Install and Upgrade