appviewX

Release Notes

Version: 2021.1.0

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

Preface

Revision History

Revision	Description	Date
1.0	AppViewX_v2021.1.0 Release Notes.	September 2021

About this Guide

AppViewX product contains the following modules: ADC+, CERT+, Google Cloud CAS, Platform, Visual Workflow, Smart Discovery, Security+, Page Discovery, and Report Engine.

These release notes accompany AppViewX Release v2021.1.0 for the ADC+, CERT+, Google Cloud CAS, Platform, Visual Workflow, Smart Discovery, Security+, Page Discovery, and Report Engine modules. They describe new feature, known limitation, and known and fixed problems 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 v2021.1.0 release for the ADC+, CERT+, Google Cloud CAS, Platform, Visual Workflow, Smart Discovery, Security+, Page Discovery, and Report Engine modules.

ADC+

- Added support for the Nginx Plus R22.
- Added support for Vendor Version abstraction to enable the latest F5 version.
- Ability to pin and customize pages for Application widget from the Pages as well.
- Ability to pin and customize pages for Heatmap widget from the Pages as well.
- Added support for BIG-IP F5 v16.
- Ability to add objects using regex for Application widget. This regex is used to dynamically update the Application widget with the objects that match the regex.
- Introduced simplified Left navigation panel for ADC+. The features of ADC are grouped under the following menu:
  - Traffic Management
  - Asset Management
  - Automation
  - Configuration Management
  - Logs and Alerts.
- Added API support to validate the last action status of an object.
- Added API support to validate the status of action executed on the actual device.
- Removed the reference of decommissioned BIG-IP devices from the Application.
- Widget Abstraction - Application Widget into Pages for customization.
- Widget Abstraction - Heat map widgets into Pages for customization.
- Soft delete for device config fetch.
- Provision to invoke a Light weight config fetch process on ADC devices on demand basis.
- Nginx plus - custom dashboard support and recursive topology completion.

ADC+ Automation

Added Catalog: F5 BIG-IP GTM:Create

- Create F5 GTM WideIp Workflow - User can use the workflow to create wideip object on the F5 devices managed in the Inventory.
- Create F5 GTM wideip with ServiceNow Workflow - User can use the workflow to create WideIp object on the F5 devices managed in the Inventory and Integrate the request in the Service Now.
- Create F5 GTM WideIP with Topology Workflow - User can use the workflow to create WideIp object with multiple pools on the F5 devices managed in the Inventory.
- Create F5 GTM WideIP with Topology Workflow - User can use the workflow to create WideIp object with Topology on the F5 devices managed in the Inventory.
- Create F5 GTM WideIP with Topology Workflow - User can use the workflow to create WideIp object with Topology on the F5 devices managed in the Inventory.
- Create F5 GTM WideIP with Topology and Partition Workflow - User can use the workflow to create WideIp object with Topology on the F5 in a Specifc Partition.

Added Catalog: F5 BIG-IP GTM:Modify

- Modify F5 GTM WideIp Workflow - User can use the workflow to Modify WideIp object's properties on the F5 devices managed in the Inventory.

Added Catalog: F5 BIG-IP GTM:Delete

- Delete F5 GTM WideIp Workflow - User can use the workflow to delete WideIp object on the F5 devices managed in the Inventory.

Added Catalog: F5 BIG-IP LTM:Create

- Create F5 LTM VIP Workflow - User can use the workflow to create VirtualServer object on the F5 devices managed in the Inventory.
- Create F5 LTM VIP with Service Now Workflow - User can use the workflow to create VirtualServer object on the F5 devices managed in the Inventory and Integrate the request in the Service Now.
- Create F5 LTM VIP with DNS Workflow - User can use the workflow to create VirtualServer object on the F5 devices managed in the Inventory and Integrate the request in the Infoblox (DNS) in **Appviewx Menu** > **Inventory** > **Devices** > **Others**.
- Create F5 LTM iRule Workflow - User can use the workflow to create Irules in the F5 devices managed in the Appviewx Inventory.
- Create F5 LTM VIP Basic Workflow - User can use the workflow to Create Virtual Server on the F5 devices Managed in Appviewx Inventory.

- Create F5 LTM VIP Advanced Workflow - User can use the workflow to Create Virtual Server,its additional properties on the F5 devices Managed in Appviewx Inventory.
- Create F5 LTM VIP with Partition Workflow - User can use the workflow to Create Virtual Server on the F5 devices in a specific Partition.
- Create F5 LTM Monitors Workflow - User can use the workflow to Create Monitor in a F5 device Managed in Appviewx Inventory.
- Create F5 LTM Monitors Workflow - Multiple Devices Workflow - User can use the workflow to Create Monitors in Multiple F5 Managed in Appviewx Inventory.
- Create F5 LTM Multiple VIP Workflow - User can use the workflow to Create Multiple VirtualServer on the F5 Managed in Appviewx Inventory.

Added Catalog: F5 BIG-IP LTM:Modify

- Modify F5 LTM VIP Advanced Workflow - User can use the workflow to Modify VirtualServer object's properties on the F5 devices managed in the Inventory.
- Enable and Disable F5 LTM Pool Members Workflow - User can use the workflow Enable/Disable Pool members associated the Virtual Server.
- Disable Unused F5 LTM VIP Workflow - User can use the workflow to get a report of Unused VirtualServers in F5 Managed in AppViewX Inventory and Disable the objects in the F5 device.
- Manage F5 LTM Pool members Workflow - User can use the workflow to change the properties of the pool member for a given VirtualServer. The workflow request can be Integrated with Service Now.
- Manage F5 LTM Data groups Workflow - User can use this workflow to Modify Existing datagroups and export datagroups from the F5 Device Managed in AppViewX Inventory.

Added Catalog: F5 BIG-IP LTM:Delete

- Get Unused LTM VIP and Delete Workflow - User can use the workflow to get unused virtual server on the F5 devices Managed in the inventory and delete.
- Delete F5 LTM VIP with Service Now Workflow - User can use the workflow to Delete VirtualServer object on the F5 devices managed in the Inventory and Integrate the request in the Service Now.
- Delete F5 LTM VIP Advanced Workflow - User can use the workflow to Delete Virtual server and its associated objects.
- Delete F5 LTM VIP Advanced Workflow - User can use the workflow to Delete Virtual server and its associated objects.

- Disable and Delete Unused F5 LTM VIP Workflow - User can use the workflow to get a report of Unused VirtualServers in F5 Managed in AppViewX Inventory and Delete the objects in the F5 device.
- Delete F5 LTM VIP Basic Workflow - User can use the workflow to delete VirtualServer object on the F5 devices managed in the Inventory.

Added Catalog: Reports

- F5-CPU and TMM Report Workflow - User can use the workflow to get CPU and TMM report of the F5 devices managed in the AppViewX Inventory.

Added Catalog: F5 BIG-IP Reports

- Get Unused LTM VIP and Notify Workflow - User can use the workflow to get a report of Unused VirtualServers in F5 Managed in Appviewx Inventory. Report can be sent to specific mail-Id. The Workflow will be in Disabled state by default. User can enable it.
- F5 LTM and GTM node Report Workflow - User can use the workflow to get a report listing the GTM node and LTM node details to specific Email-Id.
- F5 SSL Certificate expiry Report Workflow - User can use the workflow to get F5 LTM certificate expiry report to specific mail ID. Fetches certificates that are going to expire in 30, 60, or 90 days.

Added Catalog: F5 BIG-IP System:Compliance

- F5 BIG-IP Golden Config Compliance Workflow - User can use the workflow to run compliance check on Managed F5 devices and remediate the parameters that are non-compliant.
- Fetch F5 BIG-IP CVEs Workflow - User can use the workflow(Managed in Appviewx) to get CVE published in the site https://cve.mitre.org/.
- F5 BIG-IP CVE Reporting Workflow - The Visual workflow collects the report based on the CVE ID published and the affected F5 devices in the Inventory for the CVEs.

Added Catalog: F5 BIG-IP System:Software Upgrade

- Software upgrade on HA F5 devices Workflow - User can use the workflow to upgrade HA F5 (Managed in AppViewX) from one version to another version.
- Software upgrade on Standalone F5 devices Workflow:
  - User can use the workflow to upgrade Standalone F5 from one version to another version.
  - User has to move the ISO files Manually from their Computer to Appviewx Installed VM.

Added Catalog: Infoblox IPAM:Create

- Create Infoblox DNS records Advanced Workflow - User can use the workflow to Modify A, HOST, PTR,CNAME,TXT,MX records in Infoblox device Managed in AppViewX Inventory.

Added Catalog: Infoblox IPAM:Modify

- Modify Infoblox DNS record Advanced Workflow - User can use the workflow to Modify A, HOST, PTR,CNAME,TXT,MX records in Infoblox device Managed in AppViewX Inventory.
- Modify Infoblox DNS records Workflow - User can use the workflow to Modify A, HOST, PTR,CNAME,TXT,MX records in Infoblox device Managed in AppViewX Inventory. The workflow also fetches records based on app name.

Added Catalog: Infoblox IPAM:Delete

- Delete Infoblox DNS records Advanced Workflow - User can use the workflow to Delete A, HOST, PTR,CNAME,TXT,MX records in Infoblox device Managed in AppViewX Inventory.
- Delete Infoblox DNS records Workflow - User can use the workflow to Delete A, HOST, PTR,CNAME,TXT,MX records in Infoblox device Managed in AppViewX Inventory. The workflow also fetches records based on app name.

Added Catalog: Bluecat IPAM:Create

- Create Bluecat DNS records Workflow - User can use the workflow to Create A, HOST, PTR,CNAME,TXT,MX records in Bluecat device Managed in AppViewX Inventory.

Added Catalog: Bluecat IPAM: Modify

- Modify Bluecat DNS records Workflow - User can use the workflow to Modify A, HOST, PTR,CNAME,TXT,MX records in Bluecat device Managed in AppViewX Inventory.

Added Catalog: Bluecat IPAM:Delete

- Delete Bluecat DNS records Workflow - User can use the workflow to Delete A, HOST, PTR,CNAME,TXT,MX records in Bluecat device Managed in AppViewX Inventory.

Added Catalog: AVI GLSB:Create

- Create AVI GSLB service Workflow - Users can use the workflow to Create GSLB service.

Added Catalog: AVI GLSB:Modify

- ADC Modify AVI GSLB service Workflow - Users can use the workflow to Create Modify service.

Added Catalog: AVI GLSB:Delete

- ADC Delete AVI GSLB service Workflow - Users can use the workflow to Delete GSLB service.

Added Catalog: AVI SLB:Create

- ADC Create AVI SLB service Basic Workflow - Users can use the workflow to Create SLB (Virtual Service).

Added Catalog: AVI SLB:Modify

- ADC Modify AVI SLB service Advanced Workflow - Users can use the workflow to Modify SLB service (Virtual Service).

Added Catalog: AVI SLB:Delete

- ADC Delete AVI SLB service Workflow - Users can use the workflow to Delete SLB service(Virtual Service).

CERT+

- CLM and Certificate Discovery Support for Amazon Private CA.
- Policy revamp to include vendor specific details for each CA.
- Enhanced Key Usage (EKU) inclusion in Inventory filter.
- Display Subject Alternate Names (SAN) in connector and inventory.
- Custom CA integration for Istio using Kubernetes CSR.

CLMaaS

AppViewX now enables a cloud-based deployment for its flagship certificate lifecycle management product, CERT+.

AppViewX CERT+ is the next-gen certificate management suite that simplifies X.509 certificates and other crypto technologies across endpoints and environments by providing abstraction, standardization, and automation. It helps you gain visibility into and control over your entire PKI, making time-consuming administration and expensive outages a thing of the past. Private key protection and PKI self-service

come as standard, as does policy enforcement. CERT+ has integration with leading PKI, IAM, cybersecurity, and DevOps products, among others – making cross-environment functionality seamless, agile, and endlessly scalable.

Certificate Lifecycle Management

- Discover, create, renew, provision, revoke and manage SSL/TLS certificates in your environment.
- Automate your X.509 certificates and key lifecycles on application servers, ADCs, and endpoint devices.
- Leverage multi-vendor internal and external certificate authorities in your chain of trust.

Key features of this Solution Include

- Capability to perform smart certificate discovery from across datacenters and network segments.
- Integrate with multiple different Certificate Authorities to request certificates from a single interface.
- Ability to define Policies to enforce compliance.
- Enroll, Re-enroll, and Revoke certificates.
- Securely distribute newly enrolled certificates or renewed certificates to network devices and servers.
- Follow existing or improved business processes for managing certificates with automation.
- Single interface for enrollment protocols like SCEP, EST and ACME with choice of CAs to enroll certificates without making changes to PKI.
- Have agile PKI infra with minimum to no impact to PKI clients.
- Monitor Crypto infra security with out-of-box and customizable reporting.
- Enroll certificates for enterprise and IoT systems managed by MDM or EMMs.
- Migrate certificates between different Certificate Authorities.
- Manage certificates on network devices such as ADC, Firewalls, WAF along with network accessible servers.
- Discover and Manage certificates on cloud Key stores.
- Self-service Provisioning to Servers and Appliances:
  - AppViewX can publish self-service forms that end-users can use to request certificates that AppViewX will automatically provision on associated servers, devices, and appliances.

- Integration with DevOps tools:
  - AppViewX features native integrations with leading DevOps tools to carry out certificate operations in DevOps environments: Terraform and Ansible for deployment automation, Kubernetes and OpenShift for ingress certificate automation, Istio for service mesh security via mTLS, and so on.

CLMaaS New Features

- The CLMaaS (Certificate Lifecycle Management as a Software) deployment is facilitated by setting up a Cloud Connector Connectivity Service that routes communication securely between the AppViewX cloud and the tenant network.
- The Manage Cloud Connector certificates via AppViewX CERT+, acting as a proxy that securely transmits requests from AppViewX to the organization's critical enterprise infrastructure components.
- Currently, the cloud-based deployment is supported only for CERT+.
- CERT+ enables enterprises to automate their certificate lifecycle management to manage their internal and external PKI.
- The CLMaaS deployment supports the same features as the on-prem CERT+ deployment. To manage the Cloud Connector, the following features have been added:
  - Comprehensive inventory management interface that enables you to monitor and manage the Cloud Connectors lifecycle.
  - Ability to start, pause, and delete a Cloud Connector.
  - Runtime health analysis of the Cloud Connector.
  - Automatic and intelligent routing of traffic between Cloud Connectors.
  - Extensive data backup, retention, and restore capabilities.
  - Holistic view of the Cloud Connector to be able to push existing certificates to the Cloud Connector.
  - Authenticated access to the Cloud Connector by implementing Role-based Access Control (RBAC) for the Cloud Connector.
- To get started and work with the Cloud Connector, refer to CERT+ CLMaaS Deployment-Getting Started Guide and CERT+ CLMaaS Deployment-Cloud Connector User Guide.

Google Cloud Certificate Authority Service (CAS)

- **Certificate Lifecycle Management** - Certificates issued by CAS can be discovered and inventoried across a variety of endpoints. Renewals, revocations, self-service provisioning, enrollment, and monitoring operations can be performed from within the AppViewX platform.

Install and Upgrade

- Moved from Docker to Containerd.

Platform

- Cyberark support intergration in UI.
- Multiple OU support for AD integration.
- Saml enhancements with Sign AuthNrequest is enabled.

Page Builder

- You can now access the Pages module from the AppViewX menu directly.
- Page in Tabs mode now supports Tab reordering.
- Version control is now available in Pages.
- GUI for the Import Pages section has been updated to allow users to rename the Page and select the version of the Page they are importing.
- When sharing a Published page, you can now set the Landing page and also hide the AppViewX page header for selected user and user group.
- Application and Heat map widgets can now be pinned to your catalog pages.

Security+

- Cloudflare device addition in inventory only - No parsing.
- Bring in rule modify right click option for Checkpoint R88.
- Import Sheet mismatch about HA (Common for all Vendors).
- Configure Drift for Policy - Panorama.
- Device Backup, Compare, Restore and Rollback - Panorama.
- Auto SysLog Subscription - Panorama.
- Logging - Separate Firewall tab with Firewall Product logs.
- Source port and Destination port support for vendor Fortinet - Fortimanager.

Smart Discovery

- Automatic Device Discovery.
- Device Discovery with associated details of OS, Os Version, Device type (For example, Load Balancer, Server, and so on).
- Nmap Pre-packaged.
- Enhanced reporting with AppViewX current standard look and feel.
- Smart discovery available as an independent SKU.

Report Engine

- Device Name field is captured as part of DeviceBackupCount in connected platform.
- Additional values support are provided for between operator in QueryExplorer.

Visual workflow

- Provision to show/hide Request Logs.
- Option to have advanced code logger which can be validated in the UI.
- Integration improvements.
- Generate API with URL, payload and clear format.
- Support to enable Async script execution in script palette.
- Provision to support generic file upload and download.
- Store complete UI revamp.

Chapter 2: Known Issues

This section lists the known issues in AppViewX v2021.1.0 release for the ADC+, CERT+, Google Cloud CAS, Platform, Visual Workflow, Smart Discovery, Security+, Page Discovery, and Report Engine modules.

ADC+

- Topology Rendering takes 3.69s for Datacenter but connections are not established within time.
- Traffic Grid: Status of gwchild objects(where WideIP is NAPTR and gwchild is A Type) shown as gray color in widget.
- Dashboard: When user has only dashboard access, Creation of Dashboard with Heat Map Widget is failing with errors (Unauthorized access, read write permissions not available, and so on).
- Dashboard: HeatMap: **Logs** > **Pagination** is not working (Impacts: Alerts and iHealth section pagination).
- Dashboard: F5 > Server objects getting listed while creating widgets without any permission for the respective objects.
- AVI device module provision check is not handled.
- Dashboard: Akamai - View Topology for Server Level and Data Center Level is not providing any results and State for Property and Data Center Level is not displayed as in CC.
- Dashboard: Nginx Upstream View Topology is not working.
- Dashboard: When user has only dashboard access, Creation of Dashboard with Heat Map Widget is failing with errors (Unauthorized access, read write permissions not available, and so on).
- Dashboard: When user has only dashboard access, View Config shows unauthorized access.
- Syslog Port older entries are not getting deleted on AVI and Citrix devices.
- GTM Pool and PM,(objects with special character ( ), \ ) not displayed in CC (Dashboard) when searched with Pool/PM name.
- Threshold alert is not working when the threshold alert and syslog alert is created with same name.
- **Pages** > **Application View Widget** > **Widget Level Refresh** and **Object Level Refresh** are not happening and **Widget Level Refresh** button is not properly aligned.
- Application View: Invalid priority subgroup name showing in widget.
- Dashboard: Internal server error displayed when user performs set highest priority action on parent group.

- Get Class Management Widget Details (/dashboard-widget) API call is fetching application view widget details and also not throws proper response code for other widgets.
- User is allowed to delete restricted widgets.

ADC+ Automation

- Visual workflow relies on a Module "CommanRepo", to communicate with F5 device. Sometimes the commandRepo returns Empty response to the Visual Workflow , post communicating with device. This results in incorrect/Nodata data being shown in Visual Workflow.
- The CVE scan report do not includes modules AFM and ASM in F5.
- If the User provided Input - Record Name has space in it, the record will not be created in the Bluecat Device due to encoding issue.

CERT+

- Amazon PCA Discovery: Discover Button should not be enabled unless all available regions/s3 buckets are listed and, at least one of them is selected.
- Logs are not clear when Digicert certificate is Renewed without providing Order ID or Division details.
- Application IP passed in the response headers while cert report download - Application vulnerability.
- Filtering Certificates by Amazon CA also lists Amazon PCA in server inventory.
- While Regenerating Custom CA certificate, after changing the CA account the CSR parameters fields getting collapsed.
- While updating Certificate Attributes from inventory for the certificate without CA Connector, getting error as "null".
- Incorrect Error Message during Renewal from Inventory when user is not given permission to trigger workflow.
- The CSR Generation in Endpoint (Tomcat Linux) is failing if the CSR parameters contains space.
- AWS ACM-PCA Discovery: Unable to run Discovery for two Issuers from different regions in a single scan configuration.
- When the SaaS proxy is down in backend logs under the probable cause and remediation, need to add one more point stating that the "SaaS Proxy agent might not be running".
- Search functionality in job scheduler page does not return search results when given without key pair value.

- When user navigate to Alerts page from Holistic view on clicking View Alerts, after removing the search query and clicking enter the search query again retains.
- Discovery status is displayed as "Failed" though the discovery is successful when "Managed" status is selected for ACM cross account.
- Approve/Implement Actions not visible in the Renew process explorer page during Bulk Renew when Digicert certificate is Reissued instead of Renewed when approval required is enabled.
- Devices table getting resized during page navigation under certificate discovery.
- If AppViewX does not search with spaces, user should be shown with proper error message.
- Need to remove the line "Reusing ejbca locator from cache" from logs.
- Certificate validity period entries are displayed as "[object object]" if not added to CA policy before updating.
- Microsoft Enterprise Server Certificate - SAN other Name are not showing in the Certificate Content.
- Validation error message is providing java object level details.
- Certificate logs does not display both client and server under purpose/usage column.
- Error log correction for health API failure.
- On pushing an EC type certificate generated with endpoint source (KDB), to the same KDB in Linux Server with private key in device option, push is getting failed.
- Nginx: On generating csr in device with EC key type and bit length 224, cert is getting generated with 384 bit length.
- Secret key should be masked in the response on adding and updation of AWS device.
- Policy compliance report pie chart mouse hover data flickering intermittently.
- Count of SAN Names, 'ECDSA Curve' and 'HSM key handler Name' columns fails to export in the count by issuer and certificate summary report scheduled email.
- Certificate Transparency reports response does not contain serial number due to change in Google CT search response structure.
- Email configuration time for validation status report is to be given in GMT even though application time zone is IST.
- Revoked certificate under SSL scorecard being displayed as valid.
- Vulnerability widget not loading in SSL scoreboard report.
- GUI showing two loading bars when navigating to application connector via control center.

- After triggered Google CA discovery and refreshing the page, getting some error message related to Google CA unnecessarily.
- Programmable CA - GlobalSignMSSL CSR submission getting is failed with error "Request json or Python script contains error".

Platform

- Test query in LDAPs are not working when the configuration is not saved.
- SAML export metadata is not working when the IDP configuration and service provider information is added without save.
- Alerts are not raised for License upload or activation failure – Improvement.
- Super access resource with permission to all resources in AppViewX is modifiable.

Security+

- ControlCenter Search - Auto suggestion to list Firewall devices for the keyword device: is not working properly.
- Templates to create/modify/delete Fortigate with multiple VDOMs are not working.
- Templates to create/modify/delete Fortigate and Fortimanager CNAT is not working.
- FirewallNB: CC: Rules which has IPv6 address does not bring values on CC search for some vendors.
- FirewallNB: Count mismatch of some parameters in Optimization reports in Dashboard. CC counts for the same are perfect.

Visual Workflow

- Job scheduler weekly logic.

CLMaaS

- Login page takes up to 13 seconds to load full page during 10 concurrent users login.
- Strimzi pod restarts due to Out of memory.
- S3-Backup&Restore - Restore on different node -Kafka Communication throws ssl handshake error.
- Vulnerability API response x509 typecast issue in SSL scoreboard report.
- Logs have datacenter value as 'null' for general certificate reports when there is no option to choose DC value in GUI.

- SAAS: "cert-application-connector-findby-certificateid" API is taking 8.18 seconds for 10 users of load test.
- Managing Linux Servers on SAAS Env is not scaling due to Memory SLA for APIs.
- Backups folders are not gets deleted when uninstall is triggered.
- After did Cert push to cloud connector A another cloud connectors default certificate not showing the GUI.
- Resilience: CC is Paused from past 20 minutes even it is processing and SAAS Proxy is sending old request to same CC.
- Alerts are not raised if CPU and memory crossed 70 percentage of limit.
- OS gets corrupted on mounting the s3 bucket in /etc/fstab.
- After you click on edit app connector page for the cloud connector device that is added and click on save button "Invalid payload data" error banner is displayed.
- Resilience: When Kafka URL Node is down then CC became down also.
- [UX improvement] ::Upgrade config was confusing the user.
- While the CERT+ push we are not getting proper error message in GUI.
- Up and Running Cloud connector list is not displayed in App connector page.
- IDRAC (dell) device is getting unresolved.
- Observing upstream error in SaaS proxy log.
- Time taken to manage device in SaaS instance are comparatively higher than on prem nodes.
- In AppViewX, there will be both internal and external CRL and OCSP endpoints will be available and there is no data center option available to route request.
- ILO device addition failure.
- Improvement: Need validation for the Security token in the installation of cloud connector.
- CSR Generation in Weblogic Linux server with invalid CSR location has incorrect log message.

Chapter 3: Known Behaviors

This section contains the known behaviors, system maximums, and limitations in software in AppViewX v2021.1.0 for the CERT+, ADC+, DEVOPS, Platform, PKIaaS, SaaS, Security, SSH, Architecture, and Automation modules.

Install and Upgrade

- Upgrade is not supported from any versions.

ADC+

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.
- Citrix orphan GSLB Service parsing is not supported and Count differs from Device,Inventory,cc and Dashboard.
- (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.
- The Import option in the Dashboard does not support objects of different devices at a time.
- Actions cannot be configured or performed on an empty group.
- Actions can be customized for an object type and not for the individual objects.
- Filter button is not working in view action for external class.
- There is no auto suggest option when you configure an object.
- Import dashboard with more that one device objects is not supported.

Control Center

- Usage of logical operators between a primary and secondary keyword is not supported in Control center.
- No VIP under Wideip and Recursive Topology is supported for Haproxy,Nginx, and Bigiq.
- Status fetch is not happening for bigiq device.
- Object compare - Only for F5 objects.

- Parent disabled objects can be differentiated only based on the tool tip of state and status. State and Status color will not be changed.
- Action status fetch is failing during config fetch for GTM pool member objects created with cross partition.
- No orphan support for Amazon ELB Objects.

Device Management

- 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.
- CyberArk authentication is not supported for the A10 devices.
- Terminal Password should be updated in appviewx.property file.
- Proxy or Internet facility should be available for amazon device to get managed.
- AppViewX Group sync not supported for Citrix.
- Auto-detect and AppViewX Group sync not supported for A10 v2.0.
- CyberArk and AppViewX credentials are not supported for Akamai devices.
- A10 v2 server objects are not supported.
- Timestamp should be proper so that akamai device gets managed.
- The MongoDB supports parsing of the configuration file less than 16MB. The class files for the F5 device fails if it exceeds 16MB.
- The Big-IP system intermittently fails to authenticate the users with valid credentials. For detailed information, refer to Support.
- If there is an exclamatory mark (!) in the credential of a proxy setting, the connection will not be established.
- Configuration fetch can be triggered for devices in the ‘Queued’ or ‘Inprogress’ status after five minutes in FIFO basis.
- 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.
- The import and export of devices is not supported for Amazon ELB and Akamai.
- AVI devices can be managed only using a management IP address and the credentials provided must be a super-user.
- F5 v12 DNS records are not supported in the device management and Control center.

- NAT IP based device addition is not supported for Citrix devices.
- Orphan Objects are not supported for Citrix and Amazon ELB devices.
- If IP/FQDN/device name is already present in AppViewX, the device with the same details cannot be added to the Inventory.
- Cisco GSS is not supported.
- Configuring 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 more than 200 MB.
- 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.
  - 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 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.
  - 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.
- 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 write actions configurations can be defined in the Settings.

- Other Partition Objects are not parsed via syslog.
- State/Status updated for the LTM objects via F5 Rest call is not getting updated in Appviewx via syslog.
- Syslog that is subscribed with VIP IP in the current version will be subscribed with Node IP as host name after migrating to kube environment.
- After migrating to 20.3.0 kube based deployment, Syslog subscribed with VIP IP will change to Syslog subscription Node IP and port.

Backup and Restore

- For AVI, Device Backup fails when more than one tenant is present.
- The cross version device restore for F5 is not supported.
- The object restore is not supported for F5 v10 and AVI devices.
- During an object comparison, the modified lined will be highlighted in Yellow.
- 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 can be taken for Maximum Archive Size of upto 200MB.
- 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.

Statistics

- Apptag is removed,Hence the default dashboard reports(Top 10 VIP, Applciation Heatmap,Top 25 Applications and Number of objects report) for ADC will not be rendered.
- The ExplicitIP address is not supported for F5 v12 and V13 devices.
- The statistics generation (historic) for the objects in standby is not supported.
- Statistics will not be collected fro F5 wideip type SRV and NAPTR.
- The statistics are not supported for the AVI GSLB devices.
- Both Syslog and Threshold alerts creation together is not recommended. Any one alert should be created.
- Pools associated via iRule is not supported.

General

- When multiple quick actions are 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.
- On performing an action on BigIQ objects from AppViewX, the state/status change may not be reflected immediately in AppViewX due to delay in the action being reflected in the BigIQ device. This might require a manual refresh on objects from Control Center or Dashboard to get the state/status of the objects in AppViewX.
- Only the 1000 objects can be added to an Application Widget using regex. Once it reaches the limit of 1000 objects, a notification will be shown.

ADC+ Automation

- Software upgrade on HA F5 devices.
- Software upgrade on Standalone F5 devices.
- User has to move the ISO files Manually from their Computer to Appviewx Installed VM.
- Get Unused LTM VIP and Delete,Disable Unused F5 LTM VIP.
  - If the Discovered Number of Unused objects are more than 200, then workflow should be run only when load in appviewx is less.
- If the Discovered Number of Unused objects are more than 200, then workflow should be run only when load in appviewx is less.
- GTM and LTM workflow. All GTM, LTM workflow parses and writes objects only in "Common" Partition of the F5 Device workflow that have "Partition" in their Name , support all available partition in F5.
- AVI workflow does not support AVI v20.
- Visual workflow relies on a Module "CommanRepo", to communicate with F5 device. If the Devices is Managed using the option "FQDN", the CommandRepo module communication to F5 fails. Support for FQDN based communication is currently not available. Hence Visual Workflow do not work on F5 devices Managed using FQDN.

CERT+

- When user modifies service regions in AWS cross account, another entry is getting added in the table.
- Smart discovery occasionally fails with Error "Exceeded the Queue Retry Limit" while scanning 17k IPs with 256 IP's in batch.
- Communication is currently not checked while saving CA settings.
- Unable to generate CSR using generate CSR with the end point > **ADC** > **Citrix**.
- While regenerating an existing certificate, not able to find the requested certificate in ACM.
- In smart discovery differences observed in response for the same IP in the same node under two different instances.
- Assign/UnAssign group throws error "Error while processing API /certificate/discovery/instance seen to be throwing HTTP 500 in the scenarios where it should be HTTP 400.
- Filter by Compliance and Validity takes over 4 minutes to load when certificate count is more than 6 million.
- Unable to bind few certificates from appviewx to Amazon ELBs.
- AWS ACM push for specific key type fails for AppViewX CA.
- Higher processing time when adding/updating Opentrust CA setting with more than 20 certification management pofiles.
- SCEP Enrollment is not working with Certmonger Client "Error response is : Certificate is already revoked" error is seen when triggering revoke for suspended certificates.
- Resource not getting created if role sync is configured as "Now".
- When SCEP plugin deployed without EST plugin at AppViewX environment, the SCEP does not work.
- While opting for higher bit length (for example: 8192 and 7680) in manual certificate mode for re-enrollment, application goes to "Not-responding" state.
- No logs files generated during manual re-enrollment process as like autoenrollment [C:\Logs\SignIn].
- For all the failures on manual re-enrollment "The input is not a valid Base-64 string as it contains a non-base 64 character, more than two padding characters, or an illegal character among the padding characters" message is getting displayed.
- During re-enrollment, parent certificate properties like SAN, bit length and SHA are not reflected in child certificate.
- Push Agent - Status of the discovered certificates are not matching with the status mentioned in config file.

- On some environments only after upgrade, EC Curve value is not getting displayed in the certificate info.
- During user enrollment - on specifying dynamic CN and Computer name as "Yes", Certificate is submitted by the common name as "Users" instead of AD name.
- CA discovery is not supported for Entrust MPKI BETA CA.
- Certificate Transparency Check, Certificate validation check, Certificate CAA Record Check, Certificate Vulnerability Check jobs cannot be triggered from Job scheduler UI due to performance impact and will only run at specified cron intervals.
- Search functionality in job scheduler page does not return search results when given without key pair value.
- Certificate holistic page load might take up to 8 seconds to load when more than 10 concurrent users accessing application at the same time.

CLMaaS

The Cloud Connector excludes support for the following features:

- Certificate Lifecycle Management through Auto Enrolment Protocols
- Integration with Hardware Security Modules
- Configuring a Programmable Certificate Authority
- Log forwarding to external servers
- IDRAC and ILO Servers
- Integration with Thycotic Server
- Integration with MobileIron (Mobile Device Management)
- Certificate Lifecycle Management on the following devices:
  - ADC: F5 v0,v11 and v16 devices, A10 Devices
  - Firewall: Paloalto, Panorama, and Fortigate
  - SSM devices
  - WAF: Barracuda, Cloudflare, F5, and Imperva devices.
- Support for the following Certificate Authorities:
  - Global Sign CA
  - OpenTrust

- Custom VA
- AppViewX CA.

Platform

- Roles search with specific keyword in inventory is giving incorrect result.
- Only 10 objects can be assigned for ADC alert settings.
- Maximum 10 failed logging attempts can be added in settings.
- Re-ordering of servers is only for RADIUS and TACACS not for LDAP.
- Role-based Access Control (RBAC) - 50 rules are recommended.

Page Builder

- Catalogs created by an user associated with Birth right UG does not list when it is shared with other user.
- Once a page is set as landing page for birthright role user group, it cannot be removed/overwritten with another page from page builder.

Smart Discovery

- Scan results may vary due to different packets and connections being handled by different systems behind the device. For example The VERSION column is based on application-layer data, so it is possible that the connections were handled by different backend systems. OS detection results may vary based on network conditions.
- Smart discovery detects the back system with the help of TCP signature and during the scan. The TCP signature presented by the device might be different when communicated at different time. Nmap matches the TCP signature provided by the device during the scan, matches with the TCP signature in the database and presents the output. It may or may not be consistent with previous results.

Security+

General

- Add device - special characters support for device name.
- Device addition fails for some vendors with **Read Only** users.
- "When "" - "" is added to a device name in between from Libre office, the hyphen '-' is considered as a different character and error is shown in Device Import".

Web Application Firewall (WAF)

- Inactive policies of ASM can also be parsed.
- WAFNB: Token based authentication should be considered for Import, Export, Import Sample sheet, and Inventory GUI.
- WAF: CC: Sorting is not working in WAF CC.
- Resolving IP from FQDN is not completed for templates and it goes with the old flow.

Firewall

- AppViewX v11.4 to v12.3 migration is supported only for PaloAlto, Panorama, and Cisco.
- As the NB scheduler column of control center modified, required change must be implemented from the respective SB.
- AppViewX v11.4 to v12.3 migration, panorama rules are not migrated properly. Old copy of rules are also present after migration (inconsistent).
- Empty field validation missing for Password,Privilege password,Policy name and Credential name while importing device.
- Maximum characters validation missing for Username, Password, Credential name and Privilege password while importing device.
- In Firewall, while importing devices validations are not thrown for password field when it is empty.
- Wildcard object type parsing in FMG and Juniper.
- Firewall NB: Rule Comparison: Once the rules are selected and compared, user should be able to shuffle the comparison like referred rules to reference rule and vice versa.
- FirewallSB: FortiManager: IPv4 Local In Policy and IPv6 Local In Policy parsing is not supported.
- FirewallNB: RuleComparison: While Comparing two rules with same name and same policy name, second rule cannot be selected as pop-up is loaded considering the policy name as a unique value.
- FirewallNB: RuleComparison: Negate values are not considered as Negate in comparison.
- FirewallNB: RuleComparison: When 2 rules have same name and different configuration or different name and same configuration, it shows as "difference" in compare page.
- FirewallDashboard: OptimizationReports: Shadowed rules should also have information of base rules (rule which was used to compare).
- FirewallDashboard: UnusedObjectsReport: Rule redirection from unused objects table.
- To revert the existing expert mode for CKP devices.

- R75: rule with only "any" also coming for duplicate address object in optimization report.
- SB_Checkpoint: Hitcount value is not shown for rules with no name.
- Firewall: Rule Comparison: Rules which has Recursive group objects cannot be used in Rule comparison.
- In Backup and restore tab , the tab should be changed to drop down.
- Firewall:On modification of the devices with credential list as cyberark, then the list of credentials is snot being displayed in drop down.
- SB_Checkpoint: Hitcount value is not shown for Inline layer rules.
- Port search works only for Fortigate, Cisco and Juniper vendors.
- TCP, UDP, and SCTP values to be added for Cisco vendors. SourcePort search does not work for some vendors. Ports in service groups cannot be searched for some vendors.
- IPv6 compliance check will not work. The FQDN check is not completed.
- After migration, for already added device either config fetch should happen or compliance settings has to be saved so that the report will be generated.
- Resolving IP from FQDN is not done for templates and it goes with the old flow.

Workflows

- User should not able to modify or delete existing mapped source, destination, and service objects.
- User should not able to delete rule associated with objects.
- Policy creation in Firewall and Policy via templates should be allowed based on R or R/W permission for the device/security Policies.
- "Any" cannot be given for Source, Destination and Service objects from templates in CKP R77.
- User should not able to modify or delete existing mapped source, destination, and service objects in CKPR77.
- User should not able to delete rule associated with objects in Fortigate and Fortimanager.
- "Any" cannot be given for Source, Destination and Service objects from templates in CKP R77.
- No warning message thrown if device is not available at inventory.

Chapter 4: Fixed Issues

This section lists the issues fixed in AppViewX v2021.1.0 release for the ADC+, CERT+, Google Cloud CAS, Platform, Visual Workflow, Smart Discovery, Security+, Page Discovery, and Report Engine modules.

ADC+

- In Audit log-Action executed successfully log shows as action performed in standby device even though the action is performed in active device.
- In Statistics settings page- After selecting the time interval and changing the vendor type. The selected time interval should be retained.
- In Dashboard-Actions triggered via workflow is getting failed in migration node.
- A10 statistics collection fails when both VCS and VRRP are disabled in a standalone device.
- State and Status of the objects updated via syslog is not taken for state and status drift API.
- In Akamai- Action will not be performed when there is only one datacenter for a object,Proper log should be shown for the action that cannot be performed.
- Migration_Single Device Deletion takes more than 20 seconds.
- Script Execution : Status color shown as RED even if execution script gets success.
- Observing slowness over the application during restore option.

CERT+

- AppViewX CA certificate revocation fails due to path change in Kubernetes deployment.
- IBMClient (Linux) : If same cert is pushed to jks with different aliases, on discovery only one alias is discovered.
- Performance time taken is high for Count by issuer settings page when 20k+ CA certificates are available.

Platform

- Cyberarc integration not supported.
- While getting session timeout pop-up, able to click on the menu's, hence page is redirected to IP:Port (web) and getting page not found error.

Page Builder

- Banner messages for different widgets In Pages based on the ACF of other modules is not relatable.
- GUI: When the user(associated with a custom related page as landing page) logins , landing page is navigated to **Published** > **Inventory** page in Page builder (Inconsistent).

Visual Workflow

- VW Cancel a request does not work.
- Psudeo form in script and mail task.
- Not able to push file from server to server.
- Migration - DiffChecker Task Displays twice in UserInterface menu.
- Newly allowed Special characters in roles/user/UserGroup/Resources impact over VW.
- Request Page - All Request tab count does not show zero (0) when new user and (except admin user for first time) logins to the application.
- Need to change gateway port hard coded in collection up gate workflow.
- Command Task - Validator Check is required and Error Banner should throw if invalid config is given.
- Enable approval via email option fails.
- Request pages shows improper count in all.