appviewx

Release Notes

Version: 2024.1.0.0 (SaaS)

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 v2024.1.0.0 (SaaS) Release Notes.	February 2025

About this Guide

These release notes accompany AppViewX Release v2024.1.0.0 for the ADC+, CERT+, PKI+, KUBE+, SIGN+, Platform, and Visual Workflow modules. They describe new feature, enhancements, known and fixed issues, and known limitations in the software.

Intended Audience

- Customers who on-boards to AppViewX v2024.1.0.0.

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 v2024.1.0.0 release.

ADC+

The following new features are included in AppViewX ADC+.

- Administrators now have control over dashboard auto-refresh with a global setting and Access Control Framework (ACF). This allows them to enable or disable auto-refresh at the platform level while ensuring only authorized users can configure it for specific dashboards. This feature optimizes performance and prevents unnecessary system load caused by frequent refresh actions.
- Administrators can now set a minimum configurable interval for live traffic statistics collection across all user widgets in ADC+. By defining a global minimum interval in general settings, admins can control real-time data collection frequency, ensuring optimized performance and resource efficiency.
- AppViewX now supports Cloudflare integration, enabling centralized management of Cloudflare accounts, automated discovery of Load Balancers, Pools, and Endpoints, and application-centric visibility across multi-cloud environments. Customers can efficiently monitor, troubleshoot, and manage traffic for disaster recovery (DR) with actions like enabling/disabling Load Balancers, Pools, and Endpoints, updating traffic policies, and viewing logs and alerts. Blue/Green swing, Canary deployments, and Global Server Load Balancing (GSLB) automation enhance business continuity, security, and operational efficiency.

AVXpert - TechPreview

The following new feature is included in AppViewX.

- AppViewX users can now access product documentation using AVXpert in Natural Language. This feature can be switched on by RBAC controls.

CERT+

The following new features are included in AppViewX CERT+.

- The Filtered Cert Sync feature in Device Management for customized certificate discovery during configuration fetch, improving accuracy and efficiency in identifying and managing certificates.
- Enhanced security and operational efficiency by enabling **sudo access** for all actions performed by WebLogic on Linux, ensuring seamless execution of administrative tasks while maintaining controlled privilege escalation.

- Support for Imperva WAF (SaaS) discovery has been added, enabling the application connector to link to the certificate associated with the Imperva domain. This enhances the ability to seamlessly integrate and manage Imperva WAF configurations.
- Customers can now create PEM files with the entire certificate chain, allowing them to download a PEM bundle that contains all the trust certificates in a single file for easier management and deployment.
- The current option for downloading a PEM file with truststore combines the certificate, intermediate and root into a ZIP file. The ask is to provide an option to download a PEM file with truststore as a single text file containing the certificate, intermediate and root certs. This could be implemented by adding a "File Type" option with ZIP or Text when a user enables the "Download Truststore Certificates" option on a PEM file.
- AppViewX now supports F5 ASM v16 and v17 management through the WAF module, enabling seamless control of F5 ASM devices and security policy parsing. This enhancement improves visibility, security management, and operational efficiency for web application protection.
- AppViewX now supports SSH key authentication from Thycotic PAM for devices in servers, enhancing security and simplifying access management through seamless integration.
- Users can now configure the Windows Gateway Agent to communicate over HTTPS in addition to HTTP, enhancing security for Windows server access.
- Azure VM onboarding now supports Windows-based VMs in addition to Linux-based VMs. Like Linux servers, once Microsoft Server devices are onboarded, users must update VM credentials in the server inventory to enable certificate lifecycle management.
- In EST, during MTLS authentication, the server now performs a revocation check on the client authentication certificate. If the certificate is expired, the request is aborted, ensuring enhanced security and compliance.
- New issuer names have been added to Sectigo CA (Comodo Certificate Manager). During discovery, certificates from these issuers will now be classified as Sectigo CA certificates for improved identification and management.
- The following certificate group management features will be available after v2024.1.0.0 due to dependencies on additional API exposure from other teams: create, retrieve, update, and delete certificate groups; assign certificate groups to CA policies; and configure certificate groups for existing resources. Additionally, AppViewX introduces an API to configure devices for an existing resource.
- Seamless Cloud Connector deployment on AKS and GKE, ensuring full functionality without issues. This enhancement provides greater flexibility while maintaining compatibility with existing on-prem, EKS, and OpenShift installations without disruption.
- Enhanced scalability for Cloud Connector with autoscaling based on CPU and memory usage, ensuring optimal performance. Users can configure custom metrics as needed and deploy multiple pod replicas using ReplicaSets without conflicts. Updated Kubernetes manifests now include ReplicaSet configurations for seamless deployment and reliability.

- Enhanced RBAC for Cloud Connector Data Centers enables business units to control access to multiple Cloud Connectors securely. This ensures that each unit can manage and restrict CC usage to its respective owners, improving security and operational efficiency.
- Cloud Connector installation now supports Rocky Linux, offering seamless deployment with the same design as RHEL environments. Users can leverage Rocky Linux without requiring any specific changes, ensuring flexibility and ease of adoption.
- With the help of Cloudflare and Azure Integration HUB, now user can automate the Let's Encrypt CA enrollment using DNS challenge type and also the manual option will be available.
- AppViewX now supports a multi-subscription model for Microsoft Azure, enabling seamless bulk subscription onboarding for Azure accounts. The feature has been further enhanced to allow bulk onboarding of selected subscriptions, giving users greater flexibility and control over their cloud environment. Customers can now onboard only the required subscriptions, improving efficiency, security, and compliance while optimizing resource management.

Install and Upgrade

The following new feature is included in AppViewX Install and Upgrade.

- A new interactive UI has been introduced to simplify and enhance user experience for Fresh Installation, Upgrade, Data Restore, Log Collection, Auto Remediation, Patch Application, and Configuration Comparison. This intuitive interface streamlines deployment, troubleshooting, and maintenance tasks, ensuring greater efficiency, accuracy, and ease of use for administrators.

Kube+

The following new features are included in AppViewX Kube+.

- The KUBE+ CA Certificate Expiry Alert now supports filtering by Cluster Name, Namespace, and Common Name, enabling faster issue resolution. The report also includes certificate type, cluster name, namespace, and leaf count for improved visibility and compliance.
- The EKS add-on deployment process now allows overwriting the cluster name in the secret YAML file and assigning a unique service account per cluster (*clustername-svc-account*). A new link on the Connect Cluster page opens a detailed view with cluster name and vendor information, along with a **Download Credentials** button for retrieving the *secret.yaml* file. Additionally, the *secret.yaml* file now includes **CLUSTER_NAME** and **VENDOR_NAME** keys, enhancing configuration and management during add-on deployments.
- Agentless discovery enables cluster identification and management without requiring agent installation or configuration. It streamlines EKS cluster discovery using user-defined cloud devices and child

account selection. Kubernetes objects like Secrets, ConfigMaps, and Nodes are automatically managed in the certificate inventory, offering the same features and support as agent-based clusters.
- New advanced certificate options allow users to select a custom certificate deployment mode for greater flexibility and control.
- The PKI+ Dashboard for Kube+ offers valuable insights into Kubernetes certificates managed through Kube+, enabling customers to monitor, manage, and ensure the security of their certificates more effectively.

Platform

The following new features are included in AppViewX Platform.

- AppViewX previously retrieved credentials from a statically hardcoded backend path. To enhance flexibility and security, an option now allows specifying alternative paths for accessing secrets. This enables organizations to customize secret storage, enhance compliance, and strengthen access control in alignment with their security policies.
- The **Credential Store ACF** has been introduced in the **Resources** > **Access Control** page, providing enhanced control over credential access. For migrated users, the default permission will be set to `.*`, ensuring a seamless transition while allowing administrators to refine access permissions as needed.
- SSK key-based authentication has been enabled as part of Thycotic integration, enhancing security and access control for credential management. This provides a more secure and efficient authentication mechanism for seamless integration.
- Client secret notification can now be enabled in Service Accounts, allowing proactive alerts for client secret expiry. Notifications will be sent 90, 60, 30, 7, and 1 day(s) before expiry, and 1 day after, ensuring timely renewals and uninterrupted access. Additionally, the Client Secret Validity (in days) field has been moved from **OAuth settings** to **Service Accounts** for better accessibility and management.
- AppViewX now supports handling multiple accounts with identical usernames but different credentials, ensuring seamless authentication and access management. This enhancement allows users to securely manage multiple accounts without conflicts.
- The **DisplayName** field has been introduced in **User Groups**, allowing for clearer identification and improved user management. This enhancement helps streamline group organization and enhances usability.
- Email communication via Graph API has been introduced for the SMTP OAuth authentication type, enabling seamless email integration. Additionally, the **Hostname** and **Port** fields must be filled with values, even though they are not required for API communication.
- A secure HTTPS URL can now be configured with CORS enabled to display custom content in the login banner. This feature allows organizations to provide personalized messages, security notices, or compliance information while ensuring secure and controlled content delivery.

- The Access Level ACF under Logs and Alerts enhances visibility control for Observer and Explorer roles with All, Group, and Self access options. During migration, non-admin users default to Group-level access, which can be modified as needed. This ensures better access management, security, and streamlined log monitoring.
- System account is replaced with a dedicated service account.

PKI+

The following new feature is included in AppViewX PKI+.

- After creating a PKI CA, a link will be available for each CA, allowing users to navigate directly to its holistic view in the PKI CA Inventory for easier management and tracking.

SIGN+

The following new features are included in AppViewX SIGN+.

- AppViewX has streamlined HSM account onboarding in the SIGN+ module to enhance efficiency. The new 'Create HSM' option on the 'Get Started' page enables users to quickly initiate HSM account creation by selecting a data center, reducing setup time and simplifying the process.
- A streamlined and efficient installer upgrade process that ensures a seamless model for package installation, package upgrades, and the downloading of updated client certificates.
- The vendor-type check for Fortanix has been removed, enabling parallel processing for all HSM vendors, including Thales and Utimaco. This enhancement improves performance, reduces processing time, and ensures a more efficient and seamless experience for customers using different HSM vendors.
- The Signing Inventory system in SIGN+ has been enhanced with advanced filtering and export functionalities, allowing users to efficiently filter data, revisit statuses, and export relevant information for improved usability and workflow management.
- Predefined roles have been introduced in SIGN+ to simplify user management, enhance security, and ensure users have access only to the necessary resources and functions. This improvement enhances operational efficiency, reduces administrative overhead, and strengthens security compliance for customers.
- The enhanced AppViewX PKCS#11 Library now supports OpenSSL integration, offering customers improved handling of the MatchedCert struct, a more efficient C_FindObjects function, and detailed signing commands in the README after running the SIGN+ Installer. These improvements streamline integration, increase efficiency, and simplify setup for a seamless OpenSSL experience.
- SIGN+ now supports Entrust HSM with an enhanced session handling logic, offering both parallel and non-parallel approaches for signing files and hashes. This improvement benefits customers by

ensuring more efficient and flexible session management, optimizing performance for both large-scale and standard signing operations.

- The setup and validation of the CI/CD pipeline flow for the integration of SIGN+ with the AWS DevOps pipeline ensure seamless automation of build, test, and deployment processes. This integration enhances efficiency, reduces manual intervention, and accelerates delivery cycles, providing customers with faster and more reliable updates and deployments.
- Swagger has been implemented for all SIGN+ APIs, with request and response data collected via Postman. The Swagger UI, accessible from the AVX UI, provides an interactive view of the API structure. This ensures up-to-date documentation, simplifying API exploration for both internal teams and external users.

Visual Workflow

The following new features are included in AppViewX Visual Workflow.

- Support has been provided to sort internal REST APIs in ascending order based on their API names.
- Support has been provided to resize the table columns of a tabular field by dragging in the form task of the request stage view.
- Currently, in the form task of a request, hooks can only be triggered automatically when the fields are within the same form group. We are now extending support to allow hooks to be triggered automatically even when the fields are in different form groups.
- The AVX::ESCAPE command escapes any non-alphanumeric characters (letters or digits). It returns a new string where unsafe characters are prefixed with a backslash (\), ensuring they are treated as literal characters rather than part of a shell command.
- AppViewX now supports custom OIDs and extensions in certificate profile templates for AppViewX CA and AppViewX PKIaaS CA certificates. Once enrolled, certificates using these templates display custom OID and extension details, enhancing flexibility, control, and compliance.
- AppViewX now supports certificate duplication for server certificates issued by **DigiCert CA**, simplifying certificate management and reducing manual efforts. This feature enables quick replication of existing certificates, ensuring faster deployments and minimal downtime.

  Supported CA certificate types include:
  - Secure Site OV, EV, EV SSL, and EV Multi-Domain SSL
  - Basic OV, EV, Multi-Domain SSL, and Wildcard
  - EV SSL and EV Multi-Domain
  - GeoTrust TrueBusiness ID EV and OV
  - Thawte SSL Webserver EV and OV
  - Private Multi-Domain SSL, Private SSL Wildcard, and Private SSL OV

- AppViewX has introduced the workflowType parameter for the Renew Certificate in Async Mode and Renew Certificate in Sync Mode APIs. This enhancement provides greater control over workflow execution, allowing users to streamline and customize certificate renewal processes based on their operational needs.
- AppViewX now offers a CRL and OCSP Required toggle under Vendor-Specific Details for Custom CA certificate enrollment. This feature allows users to control the inclusion of CRL and OCSP settings based on predefined conditions, ensuring flexibility, compliance, and improved certificate lifecycle management.

Chapter 2: Enhancements

This section describes the new features in AppViewX v2024.1.0.0 release.

CERT+

The following enhancements are included in AppViewX CERT+.

- Sudo access has been enabled for WebLogic Linux, streamlining key operations such as configuration fetch, discovery, backup, push, bind, and rollback. This improvement enhances operational efficiency, simplifies management tasks, and ensures smoother execution of critical processes for customers.
- Validation has been added for the serverPath, installationDirectoryPath, adminConsoleCredentials, and installationConfigPath fields, ensuring they match a specified regex pattern. This improves data integrity, reduces errors, and enhances the security and reliability of the configuration process for customers.
- An enhancement has been made to support custom DNS nameservers for ACME Challenge validations. As a result, a Cloud Connector upgrade is required for users utilizing the ACME DNS Challenge or Enterprise Challenge methods, ensuring compatibility and improved functionality.
- Enhancements have been made to the AppViewX Terraform Provider, now available in the new version v1.0.1, offering improved features and functionality for better integration and management.
- The nm-cloud-setup.service and nm-cloud-setup.timer prerequisites have been included for RHEL, ensuring smoother setup and improved system compatibility.
- Support for a Cloud Connector status checking script has been added, allowing users to easily monitor and ensure the health and connectivity of their Cloud Connector.
- HTTPS has been enabled for the Integrated Gateway, enhancing security by encrypting data transmission and ensuring safe, secure communication.
- Provision has been added for updating repository and chart URLs for Helm, offering greater flexibility and control in managing Helm deployments and configurations.
- For certificate expiry alerts sent over email, you can now choose from multiple email templates to determine the format and structure of the email content.
- Custom DNS Nameserver support has been added for ACME Challenge validations, enhancing flexibility and control. A **CC Upgrade** is required for users utilizing the ACME DNS Challenge or Enterprise Challenge method to ensure seamless compatibility.
- The AppViewX Terraform Provider has been enhanced and released as **v1.0.1**, offering improved functionality and better integration for infrastructure automation.
- Security enhancements include special character encoding in APIs, DOM Purify for UI sanitization, and RBAC enforcement across all APIs. Session-less API requests are blocked, and sensitive data like

usernames and passwords are no longer passed in URLs or exposed in API responses. Additionally, Expiry Alert Email Template is now integrated with the platform for seamless notifications.

- In Entrust CA configuration, the Username and Password fields have been renamed to API Username and API Key for better clarity and alignment with authentication standards.
- The tooltip for the **Name** field in CA switch details (for both server and client) has been updated to provide clearer context and guidance.
- The **Timezone** field has been added to discovery APIs for scheduled discovery scans, ensuring accurate time-based execution across different regions.
- Certificate ownership and permission customization for push-to-device actions is now supported on Generic Linux, providing greater control over file permissions.
- PEM file permissions were retained during push operations, ensuring consistency, while the private key was set to 600 permissions by default for enhanced security.
- Case-insensitive scan support is now enabled for Linux vendors, allowing customers to discover certificate types in uppercase, improving flexibility and accuracy in certificate management.
- The Group selection dropdown now includes a searchable field, making it easier to quickly find and select groups across various actions, including Enroll and CLM, Group Settings, CSR Generation, Certificate Upload, Bulk Updates, and Auto Enrollment (EST, ACME, SCEP, SCEP MS Intune). This enhancement improves efficiency and user experience by reducing manual scrolling and selection time.
- The DigiCert Discovery API is enhanced to update vendor-specific details, including Renewal Message, Notes, and Additional Email, along with existing certificate attributes. This improvement ensures better tracking and management of certificates with enriched metadata.
- CA settings fields are now exposed in the Query Explorer and available in Hooks Inventory, enabling better visibility, customization, and automation for certificate management.
- Support for additional GoDaddy certificate types has been added, including UCC_WILDCARD_OV_SSL and UCC_WILDCARD_DV_SSL under Server Certificates, and OV_DS under Code Signing, enhancing certificate management flexibility.
- The Cloud Connector (CC) installation now includes an enhanced pre-requisite check that validates the inactivity of the following Network Manager services:
  - nm-cloud-setup.service
  - nm-cloud-setup.timer

  This ensures a smoother installation process for RHEL OS users by preventing conflicts with these services.
- AppViewX has introduced a monitoring script to ensure seamless Cloud Connector (CC) operations. This script proactively checks CC health, ensuring uninterrupted patch updates. It verifies resources, services, and CC communication to maintain optimal performance and reliability.
- Integrated gateway is now supported with HTTPs using winRM.

- AppViewX now supports using a customer’s internal repository URL for Helm-based Cloud Connector installation. Before configuring the internal repository, customers can first pull the AppViewX Helm and Docker images into their repository. Once done, they can specify their internal repository URL while adding the Cloud Connector through the Helm installation model. Additionally, the Helm-based installation script will automatically populate the internal repository URLs during configuration.
- The Integrated Gateway now features a Microsoft CA prerequisite check to ensure seamless CA connectivity. This enhancement validates essential requirements, including Windows Gateway reachability, user credential authentication, WinRM service status and configuration, and CA discovery, ensuring a smooth and reliable integration process.
- AppViewX now supports username with domain/username format for device authentication in the Integrated Gateway.

Platform

The following enhancements are included in AppViewX Platform.

- The default password history limit has been increased from 5 to 10, preventing users from reusing their last 10 passwords for enhanced security.
- Parallel execution, currently available for Fortanix HSM, is being optimized and extended to support all HSMs, improving performance and efficiency. This enhancement will automate the process, eliminating manual configurations and ensuring seamless execution across all supported HSMs.
- The minimum password length is now 12 characters for enhanced security. After upgrading to v2024.1.0.0, users with shorter passwords get a 7-day grace period with daily login screen reminders and email notifications. After the grace period, password updates will be mandatory at login.
- The User Group now supports a Group Display Name, similar to Certificate Group, enhancing clarity and ease of identification.
- Enhanced security for KMS access by replacing hardcoded credentials with a secure authentication mechanism, ensuring better protection and compliance.
- An out-of-band (OOB) provisioning workflow is now available to securely migrate customers' KMS keys from old accounts to new accounts, ensuring a smooth and secure transition.
- The MSP Partner Portal now features updated product links, ensuring access to the latest versions. The Resource Hub page has also been enhanced to include all available product resources. Clicking a product link will now open the relevant resources in a popup for a seamless user experience.
- CERT+ Insights data from tenants is now accessible directly on the Insights dashboard of the MSP portal, providing centralized visibility and streamlined monitoring.
- Improved Tenant and Cluster Management Inventory with a streamlined view—fewer columns for better readability. The first column now features clickable links to view details in a pop-up, complete with color-coded status indicators and copy icons for key parameters. Action icons and functions are

now available in a dropdown, allowing users to select tenants or clusters and perform specific actions efficiently.

- Enhanced tenant deletion process in the MSP portal for better control and security. The 'Delete' action is now available for tenants in Active, Expired, Failed, or Trial states. Deletion requests require approval from designated Level-1 (L1) and Level-2 (L2) approvers, configurable via the new 'Delete Tenant Approval Settings' page. Once a tenant is deleted, its MongoDB backup is retained in AWS S3 for 30 days before permanent removal.

PKI+

The following enhancements are included in AppViewX PKI+.

- Introduced Post-Quantum Cryptography (PQC) capabilities, updating or replacing current algorithms (for example, RSA and ECC) with PQC algorithms to ensure the infrastructure remains secure in the era of quantum computing.

  You can now leverage AppViewX's own Certificate Authority (CA), **AppViewX PKIaaS Native CA**, for PKI initialization, enabling them to take advantage of PQC benefits. The following new modules have been introduced in **PKI+** to enhance functionality and security:

  - **PKI dashboard**: The following widgets are displayed on the **End entity certificate count by CA** tab:
    - **Certificates by Templates**: This widget displays all the certificates created via the various templates.
    - **Certificates by CAs**: This widget displays all the certificates created via the various CAs. By default, all the CAs are selected.
    - **Certificate Issuance Trend**: This widget displays all the certificates based on their issuance trend such as daily, weekly, monthly, yearly, and custom.
    - **CA Hierarchy**: This widget displays the number of CA hierarchies. Click View to display the CA hierarchies created and the certificates under each of the CAs listed along with their count.
  - **Template**: AppViewX provides templates for you to select or customize your own for creating CA and end certificates, allowing you to tailor your cryptographic infrastructure to meet your organization's specific needs. This customization enhances security and ensures preparedness for future quantum threats.
  - **Issue Certificate**: You can issue any certificate by uploading any uploaded CSR from the CAs available in PKIaaS.
  - **CRL**: A default CRL service is now provided with a customizable CRL Distribution Point (CRL DP) that can be embedded into certificates via templates. The CRL Scheduler allows configuration of CRL

issuance frequency and expiry. Additionally, manual CRL publishing is available with options to set a custom expiry time and timezone.

> **Note:** Custom CRLDP and OCSP routing through the Cloud Connector are supported exclusively with the latest version, ensuring enhanced functionality and compatibility.

- Customers can now define the path length based on their use cases, as the previous 3-level hierarchy restriction has been removed.

Pages

The following enhancement is included in AppViewX Pages.

- Enhanced widget properties and styles for better usability and a more intuitive user experience.

Kube+

The following enhancements are included in AppViewX Kube+.

- Cert-Orchestrator now supports automatic ClientSecret renewal, using the existing ClientID and ClientSecret. The new ClientSecret is securely stored and used for all future authentications with AppViewX, ensuring seamless and secure access management.
- Supports certificate enrollment and discovery for OpenShift Routes and certificate discovery for ConfigMaps, ensuring better visibility and management.
- Users can now exclude namespaces during the discovery of Secrets, ConfigMaps, and OpenShift Routes by configuring a Namespaces Regex list in cluster policies. Policies can apply to multiple clusters, with exclusions displayed on the View Cluster and Modify Cluster pages. Users can also selectively include namespaces from the exclusion list if needed.

SIGN+

The following enhancements are included in AppViewX SIGN+.

- Performance has been enhanced by caching certificate information, reducing the need to query the database with each request. This improvement speeds up access, resulting in faster response times and a more efficient experience for customers.
- The setup and validation of the CI/CD pipeline flow for integrating SIGN+ with GitHub Actions have been enhanced, ensuring smoother automation of build, test, and deployment processes. This improvement boosts efficiency, accelerates delivery cycles, and provides customers with faster and more reliable updates.

- API payload changes have been exposed to improve user understanding, accompanied by updates to the API documentation. This ensures clearer guidance for users, making integration and usage of the API more straightforward and efficient.
- The validation for the number of polls and polling interval has been set to ranges of 1-20 and 10-300000, respectively. Additionally, the info message has been updated to reflect the millisecond change, ensuring clearer guidance and helping customers configure these settings more accurately for improved performance and efficiency.
- The deletion of signing policies has been enhanced to prevent removal if a signing operation is associated with it. This ensures that signing policies cannot be deleted, preserving the signing record in the signing inventory and maintaining data integrity for customers.
- To resolve inconsistencies in SIGN+ logs, a comprehensive solution has been proposed to review and refine Sign Logs and Audit Logs. This ensures accurate tracking of critical actions, such as signing events, authentication attempts, and configuration updates, with detailed information like timestamps, user IDs, outcomes, and metadata, providing customers with reliable and transparent log data for improved monitoring and auditing.
- The CI/CD pipeline flow for SIGN+ integration with Atlassian Bamboo Actions has been set up and validated. It involves configuring a Bamboo repository, installing the SIGN+ package in the runner environment, and creating a pipeline to build the artifact, trigger signing, and verify the signature. This streamlined process ensures efficient signing and artifact validation for customers.
- Fields to accept and return TSA responses in bytes have been introduced, along with logic for communicating with the timestamping server in the code-signing pod. A new DB script for proxy communication with the server has also been added, streamlining the timestamping process.
- Enhanced functionality to improve user experience by removing the 'Press enter' prompt for exiting in Sign+_installer and implementing retry logic for up to three attempts in case of a Gateway timeout issue, ensuring smoother operation and minimizing disruptions.
- By removing the 'Fortanix' vendor check, parallel processing is enabled for all HSM vendors, including Thales and Utimaco. Data export now processes in chunks for faster performance, and the installer upgrade returns only DLL versions, improving API speed and reducing upgrade times.
- The 'Download Signed Files' API now supports multiple sign IDs, allows up to 25 files per download, and removes UI restrictions. Files are bundled into a zip for faster, more efficient downloads.
- The fix dynamically applies proxy settings for routing to the Cloud Connector (CC) and automatically switches to the next available proxy if one fails, ensuring uninterrupted service.
- SIGN+ SIEM Alerting Capability ensures the availability of application logs for critical business use cases across AppViewX, providing enhanced monitoring and quicker issue detection for improved security and reliability.
- AppViewX SIGN+ offers two authentication modes: Basic Authentication and OAuth-based Authentication using Service Accounts. The Service Account mode relies on clientID and clientSecrets,

which have a set validity period. Currently, if a client secret expires, there's no automated method to regenerate it, potentially blocking the signing process until the new secrets are applied.
- Pkcs11Mode enables installation in Non-Administrator mode, installing only necessary PKCS11 libraries and certificates. It copies DLL files to the User AppData folder, generates the AVXPKCS11.cfg file with the correct path, and includes only required PKCS11 commands.
- Support for multiple downloads of signed files has been added, allowing users to efficiently download multiple files at once, saving time and improving workflow productivity.
- Utimaco HSM support for SIGN+ has been added, enabling seamless integration with Utimaco hardware security modules for enhanced security and improved signing capabilities.
- Enhanced proxy handling for Cloud Connector (CC) to ensure seamless connectivity. The system now dynamically fetches configured proxy settings and applies them to routing calls. If multiple proxies are set, it automatically switches to the next available proxy in case of failure, ensuring uninterrupted operation.

Visual Workflow

The following enhancement is included in AppViewX Visual Workflow.

- Proxy support for Akamai in Rest tasks ensures secure and seamless communication, enabling reliable access and performance while maintaining network security and compliance.
- Support for resuming in the retry palette after a pause in visual workflow requests enhances workflow efficiency, allowing for seamless continuation of tasks without disruption and improving overall process control.
- Exposing the API visualworkflow-update-resource-permission for the CERT use case ensures smoother integration, enabling more efficient resource management and enhanced security for CERT operations.
- Support for regular expressions in requests from Quick Settings based on resources enhances flexibility and precision, making it easier to filter and manage data efficiently.
- Disabling search functionality when a filter is applied in the request inventory improves focus and ensures more accurate results by preventing conflicting search actions.
- CyberArk support for ServiceNow integration enhances security by streamlining user access management, ensuring seamless and secure workflows between the two platforms.
- Support for ACL validation in the update-resource-permission functionality ensures better access control and compliance, providing greater security by validating permissions before updates are applied.
- A provision has been made to enable proxy support for Akamai Edge Grid authentication in the REST external task. When executing the REST exernal task using the Akamai Edge Grid authentication, the "Use Proxy" field must be enabled. This ensures that the specified API is routed through the configured proxy.

- The sorting of internat REST APIs has been been applied to the following endpoints: Rest internal task, Hook internal task, Form task hook internal task, Diff-Checker task, Create hook internal rest. A search field has aso been provided to locate the APIs quickly.
- In the form task of the request, hooks can now be be executed by and auto-trigger even if the fields are in different form groups.
- In tabular table of the form task, a resize option has been provided for the table columns. The resize option is availabe in the Tabular field and in the Preview of tabular field in form task of Request Stage view.
- A new API, visualworkflow-update-workflow-resource-permission, enables users to update resource permissions for Request and UI palette ACL permissions. Users can assign or unassign permissions based on the API payload, ensuring flexible access control. Permission updates are allowed only if the user has workflow request permissions, enhancing security and governance.
- RBAC now includes a ‘Show Request Log’ option to restrict access to logs in visual workflow requests, applying exclusively to Service Tasks (UI tasks remain unchanged). By default, this permission is enabled for all existing roles. In the activity log for Service Tasks, only ‘Task initiated’ and ‘Task completed’ entries are displayed, while logs remain hidden during request execution, enhancing security and access control.
- Support for AppViewX, BeyondTrust, CyberArk, Thycotic Secret, and HashiCorp credential types is now available for Basic and Credential authentication within REST tasks, hooks, and integration vendors, enhancing flexibility and security in authentication management.
- OAuth authentication now supports Password and Client Credentials grant types for executing the Command Repo REST API via Integration Hub. Additionally, users can now specify the scope in the OAuth credential type, enhancing security and access control.
- Special character support has been added to tasks, settings, dynamic authorization, and global variables in the visual workflow, enhancing flexibility and usability.
- The AVX::ESCAPE function ensures secure handling of user and third-party inputs by escaping non-alphanumeric characters when processed by an OS shell. It scans each character in the input string, prefixing unsafe characters with a backslash (\) to prevent unintended command execution, enhancing security and system integrity.

Chapter 3: Bug Fixes

This section lists the fixed bugs in AppViewX v2024.1.0.0 release.

CERT+

The following bugs are fixed in AppViewX CERT+.

- The issue related to minimal sudo access certification for Gateway use cases has been fixed, ensuring proper access control and security while maintaining the necessary permissions for smooth operation.
- In the expiry alerts description for ServiceNow, line breaks will now be retained as added, ensuring that the formatting is preserved for clearer and more organized alerts.
- Introduced Interactive and Network mode in windows gateway agent. Interactive mode will be default mode. After changing it to Network mode, user doesn't needed to be added in allow logon policy and windows gateway agent will be able to communicate to the end server.
- With Network mode enabled in the Windows Gateway Agent, users can manage Windows servers without requiring credentials to be added to the allow logon policy on the agent machine. However, the user must still have local admin privileges on the target server.
- Fixed an issue where a certificate store containing certificates with the strong password protection option enabled could not be parsed. With the latest Windows Gateway Agent, such certificates will now be successfully parsed.
- To prevent missed certificate regenerations, a 10-day threshold from the desired regeneration date has been implemented. If a certificate is not regenerated on the scheduled day, it will automatically be picked up in the next job run within the threshold period, ensuring continuity and reducing manual intervention.
- Enhanced REST communication from CC by enabling UTF-8 encoding by default. This ensures seamless handling of special characters, such as French characters in Sectigo custom attributes, across both SaaS and on-premise setups. Users can validate this by submitting a certificate creation request with such attributes.
- When the user add/modify the Microsoft IIS server with password vault identity name containing regex/ special characters, the modify page is blank and it is fixed and it should display all the fields
- When the user push the certificate with root and intermediate certs, the pushed certificate in the keyvault does not contain chain, it is fixed and it should see the complete certificate path
- When parsing the application registration services response from the device, if the fetch app registrations api returns only one page of data from the device, the issue occurs. It's fixed now and it should discover all the certificates after successful parsing
- The issue with mapping certificates to another connector has been resolved. For certificates generated on the endpoint:

  - The **vendor** and **category** fields will be auto-populated.
  - Only **profiles related to the specific endpoint device** will be displayed.
  - The **private key on the device** will be selected automatically, with its **location pre-filled** for seamless certificate management.
- Resolved an issue where **Apache configuration fetch** did not retrieve any virtual hosts when configured with **sudo access elevation**, ensuring seamless discovery and management of virtual host configurations.

Platform

The following bug is fixed in AppViewX Platform.

- Enhanced security by removing the API key from the OIDC form, reducing exposure to sensitive credentials and ensuring a more secure authentication process.

PKI+

The following bugs are fixed in AppViewX PKI+.

- Resolved an issue where DN details were reversed during CSR generation through AppViewX. Now, CSR generation behaves consistently across both AppViewX and HSM, ensuring accuracy and reliability.
- When the AppViewX PKIaaS CA connector is added to a certificate, the key specifications (key type, bit length, and hash function) are derived from the existing certificate to which the PKIaaS connector is applied.

SIGN+

The following bug is fixed in AppViewX SIGN+.

- The issue with signing via compute URL connection type not working in Managed Kubernetes has been fixed, ensuring reliable signing functionality in these environments.

Visual Workflow

The following bugs are fixed in AppViewX Visual Workflow.

- Support for assigning resources with the highest priority in Workflow Studio has been added, enabling more efficient resource allocation and ensuring critical tasks are prioritized for optimal workflow performance.
- Users can now add Infoblox server details even if the URL is invalid, providing greater flexibility and preventing workflow interruptions while ensuring the server configuration process continues smoothly.
- When sensitive fields are provided as input (REST API, Hooks) to the visualworkflow-get-task-details API, they will be masked in the response to prevent their exposure.
- In the request inventory datatable, the search feature has be optimised to include both the keyword entered in the search field and the filters that are applied by selecting the categories.
- The issue in the Workflow Search Textbox has been fixed, improving search accuracy and ensuring a smoother user experience when filtering workflows.
- The issue with dynamic user group authorization not working in provisioning has been fixed, ensuring seamless and accurate user group access management during provisioning.
- Users can now enter input by clicking on form fields in the Add Variable form within the script task and Global variables can now be retrieved when pressing Ctrl+G in the script editor upon opening the script task for the first time.
- The issue of credentials being disclosed in plaintext in the visualworkflow-get-task-details has been fixed, enhancing security by ensuring sensitive information is properly protected.
- Users can now configure a regex in Workflow Quick Settings under 'Workflow Request' to control access to workflow execution. This ensures precise permission management by matching ACL resource names, enhancing security and flexibility.

Chapter 4: Known Issues

This section lists the fixed bugs in AppViewX v2024.1.0.0 release.

ADC+

The following known issues are listed in AppViewX ADC+.

- The restore process for F5 WAF devices may fail; a fix is planned for an upcoming release to ensure reliability.
- WAF functionalities remain **unchanged** for **device onboarding** and **backup restore**.

CERT+

The following known issues are listed in AppViewX CERT+.

- AWS Cloud ACL permissions are not saving correctly on the Resource page.
- The AWS IAM App Connector turns red after config sync when a regenerated certificate is pushed.
- OVA - SSH server pod enters CrashLoopBackOff status if the user ID is 1001.

Platform

The following known issues are listed in AppViewX ADC+.

- The email subject banner is missing from Azure SSO Certificate emails when using SMTP with OAuth API.
- When configuring SMTP with OAuth using the communication API, the hostname and port fields are now optional.
- For MFA-enabled setups, if a user is not mapped to a user group, the Resend OTP button will be disabled on the MFA authentication page to enhance security and prevent unnecessary OTP requests.
- The logo in emails appears distorted when using the default template, especially when the sender and receiver are on different platforms, such as Microsoft to Gmail.
- MK8s - SMTP test connection check does not occur when enabling MFA.

Chapter 5: Known Limitations

This section contains the known behaviors, system maximums, and limitations in software in AppViewX v2024.1.0.0 release.

ADC+

The following known limitations are included in AppViewX ADC+.

- WAF functionalities are restricted in the following areas:
  - Control Center
  - Dashboard
  - WAF Policy Resource ACL.
- ADC OOB AVI workflows are not supported in the SaaS environment.

CERT+

The following known limitations are included in AppViewX CERT+.

- In Google Cloud Platform (GCP), the following limitations apply:
  - Rollback functionality is unsupported due to challenges with private key retrieval during backup.
  - Auto-push errors occur after certificate regeneration/renewal because GCP rejects duplicate certificate names.
  - Certificate map and mapping entries refresh only after initiating a configuration synchronization.
  - Push and bind operations are unsupported for cross-region internal load balancers.
  - Push to Classic Application Load Balancer premium tier, Classic proxy Network Load Balancer premium tier, and Global external proxy Network Load Balancer via Certificate Manager is not supported.
- To migrate to v2024.1.0.0 from a version older than v2023.1.0 FP2, a configuration sync must be triggered for Azure settings post-migration.
- Certificates directly pushed to the app service cannot be discovered; only certificates linked through key vaults are discoverable.
- Manual updating of zones for Amazon Public CA is required during the migration from AppViewX v2020.3.0 to v2024.1.0 to ensure proper configuration and functionality.
- The PDF report download from the Validation Status Server widget is not supported when the record count exceeds 2,000.
- The PQC Algorithm Report calculation may be inaccurate, leading to discrepancies in the Crypto Score, Signature Algorithm Strength, and Hash Algorithm Strength widgets under Insights > Risk & Crypto Dashboard.

- Known Limitations in Helm Model CC:
  - **HSM Vendor Support** – HSM vendors requiring binary installation are not supported.
  - **mTLS Support** – Currently unavailable for mothership communication.
  - **F5 Vendor Functionalities** – Features requiring iControl JARs are not supported, impacting:
    - Certificate discovery
    - ADC functionalities

> **Note:** If customers allow mounting external volumes, support may be possible.

  - **IoT Use Cases** – Cluster policies may block externally accessible ports (NodePorts).
    - **Workaround:** IoT ports will be exposed using a LoadBalancer instead of NodePorts.
  - **Reverse SSH Access** – Any functionality (e.g., A10) requiring reverse SSH access from device machines to the Cloud Connector will be impacted.
  - **Cluster-Wide Policies** – Any policies affecting network communication or LoadBalancer creation must be allowed by the cluster administrator to ensure proper Cloud Connector functionality.
  - **Repo Auth Token Requirement** – For **MK8S installation**, a repository authentication token must be added in the **saas-proxy deployment**.
  - **Custom RBAC Permissions** – If a user utilizes custom resource permissions, any newly added Cloud Connector will require **manual addition** of the corresponding **data center (DC) permission** within the resource.
- Microsoft servers from Azure can only be managed via the Windows Gateway. The Integrated Gateway flow is not supported.
- A Cloud Connector (CC) upgrade is mandatory to enable **EJBCA CA REST-based discovery**, ensuring seamless certificate discovery and management.

Platform

The following known limitations are included in AppViewX Platform.

- Observe & Explore Logs: Excel export is limited to 100 records.
- SMTP email functionality with the default template is supported from Hudson FP3 onward. To use this feature, CC must be upgraded to v2023.0.0 FP3 or later.