appviewx

Release Notes

Version: 2024.3.0.0 (SaaS)

Copyright AppViewX, Inc.

Trademarks

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 v2024.3.0.0 (SaaS) Release Notes	Sep 2025

About this Guide

This release notes describe new features, enhancements, known and fixed issues, and known limitations in the software.

Intended Audience

- Customers onboarding AppViewX v2024.3.0.0.

Third-Party Software Acknowledgments

This section serves as a placeholder to document the third-party components referenced in this guide, along with their associated trademark information.

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 this release.

CERT+

- **Enhanced Flexibility in Network Scan Scheduling**

  Users can now manually initiate network scans at any time, even if a scan is already configured as a scheduled discovery. The scheduling interface has also been enhanced to support direct date/time input (along with the existing date picker), providing more flexibility and precision in configuring discovery schedules.

- **mTLS Detection in Network Scan Discovery**

  Network Scan Discovery now detects endpoints enforcing Mutual TLS (mTLS), flagging those requiring client certificates to help security teams identify and validate protected services.

- **Enable/Disable Control for Network Entries in Discovery**

  Administrators can now enable or disable individual network entries in scheduled discoveries. Only enabled networks are scanned; disabled ones are skipped and marked *network disabled.* A discovery fails if all networks are disabled but succeeds if at least one network is scanned, thus providing finer control over discovery scope and execution.

- **Enhanced Discovery Configuration with Report and Behavior Settings**

  The **Report Settings** under CERT+ > Certificate Discovery > Discovery Configuration have been expanded into a unified **Discovery Behavior & Report Settings** page.

  Administrators can now:
  - Enable or disable extended report modules such as mTLS checks, cipher suite analysis, CAA validation, and Heartbleed/Poodle vulnerability scans to optimize scan performance.
  - Control discovery execution by toggling key discovery, network connector sync, access controls for scheduled discoveries, and discovery history retention.

  This enhancement provides greater flexibility to reduce scan time, optimize resource usage, and align discovery operations with organizational governance policies.

- **Improved Inventory Hygiene for Archived Certificates**

  Certificate discovery now respects the *archived status* of certificates across all sources (CA, network scan, etc.). Certificates previously archived due to rotation, decommissioning, or expiration will be:

- Detected but retained as *Archived* during discovery.
- Excluded from the *active inventory*, preventing unintended reappearance.

This enhancement ensures cleaner inventory views, reduces noise, and maintains administrator intent during certificate lifecycle operations.

- **Azure Front Door and CDN Support**

  AppViewX now supports integration with Microsoft Azure Front Door, a high-performance, secure cloud CDN service.

  Microsoft Azure Front Door is a modern, high-performance, and secure cloud Content Delivery Network (CDN) that serves as the global entry point for your applications. It optimizes traffic by routing users to the nearest edge location for faster, more reliable access, while built-in caching, acceleration, and a Web Application Firewall (WAF) provide enhanced performance and protection—making it ideal for global websites and SaaS applications.

- **EST Standalone Server Enhancements**
  - **Intermediate CA Certificate Issuance via EST**

    Now supports issuing Intermediate CA certificates using the EST protocol, eliminating the need for API-based communication.

  - **Device Certificate Issuance and Key Generation**

    Enables key generation and certificate issuance for devices directly from the EST server or Mothership.

  - **Dedicated CSR Configuration Block:**

    Introduced a configurable block for device certificate CSR parameters, including Common Name (CN), locality, state, and more.

  - **Improved Certificate Storage**

    Device certificates are now stored in the same directory as Intermediate CA certificates for simplified management and access.

- AppViewX now supports certificate archival, allowing certificates that are no longer in use to be moved to an archival inventory. Archived certificates are excluded from discovery scans, helping maintain a cleaner and more focused active certificate inventory, while remaining accessible for legal, strategic, and operational purposes.

  Archival Options

- **Manual** from the Actions in the certificate inventory (with an option to specify the reason for certificate archival)
- **Auto-archival** as per the settings configured by an administrator user
- **Key features**
  - **Dedicated Archived Certificates Inventory:** An Archived Certificates inventory has been introduced within the existing inventory module. It supports the existing inventory functionalities including free-text search, pagination, grid display, data export, recovery, deletion, and user action logs.
  - **Auto-Archival Configuration:** From the **Archived Certificates** inventory, admin users can configure the following settings to enable automatic certificate archival. Certificate status values that will trigger auto-archival:
    - Expired
    - Renewed
    - Regenerated
    - Revoked

    Certificates with the above status values are moved into the archived certificates inventory (and not deleted or retained in the active certificate inventory). Duration after which a certificate a valid status value (for archival) will be auto-archived
  - **Certificate Recovery Configuration:** When restoring archived certificates, admin users can now define the following behaviors:
    - Choose whether the certificate is returned to its **monitored state** or its **original pre-archival state**.
    - Specify whether the certificate is placed in the **default certificate group** or the **original group** it belonged to before archival.
  - **Recovery of Archived Certificates:** Archived certificates can be recovered from the Archived Certificates inventory. The outcome of triggering a certificate recovery is based on the recovery configuration settings defined by the administrator user.
- **Support for URN Values in SAN Extension of X.509 Certificates**

  The Subject Alternative Name (SAN) extension of X.509 certificates now supports inclusion of Uniform Resource Name (URN) values. This is applicable only for Microsoft CA.

  A URN is a persistent, non-resolvable identifier that names a resource without indicating its location. This enhancement is targeted toward supporting identity schemes in environments where resource names are persistent and non-resolvable (for example, IoT devices, enterprise services with non-DNS identifiers).
- **Automated DNS TXT Record Creation for GlobalSign Domain SSL Certificates**

AppViewX now supports automated creation of DNS TXT records for Domain SSL certificates issued by GlobalSign CA.

As part of the current implementation of this feature, AppViewX integrates with the CloudFlare and Azure DNS providers to automate the complete lifecycle of DNS TXT records used for the CA challenge and response workflows, thus streamlining the domain validation step. The feature also provides automatic removal of DNS TXT records post successful certificate creation (for automatic challenge verification).

- A new **Automated Credential Rotation** job has been introduced to streamline the rotation of credentials used to access systems and devices integrated with AppViewX. This job can be triggered **on-demand** or scheduled to run at defined intervals, based on the credentials' TTL (Time to Live).

  Note:

  This feature currently supports only credentials used with the **AppRole** authentication method for accessing **HashiCorp Vault.**

- **New Certificate Authorities Report**

  A new report dashboard has been implemented to display the **total number of certificates issued**, categorized by **usage type** (Server, Client, Code Signing) and grouped by Certificate Authority (CA).

  This enhancement enables users to monitor certificate distribution more effectively across different CAs and usage types.

- **New Certificate Expiry - Inventory Report**

  A new report dashboard has been implemented to display the **total number of certificates nearing expiry**, categorized by **usage type** (Server, Client, Code Signing) and grouped by expiry period.

  This feature helps users monitor and manage upcoming certificate expirations more effectively across different usage types.

- **New Certificate Algorithm Report Dashboard**

  A new report dashboard has been implemented to display the **total number of certificates** based on:

  - Signature Algorithm
  - Hash Algorithm
  - Key Algorithm
  - Managed/Monitored status

The data is further categorized by **usage type** (Server, Client, Code Signing), enabling users to **monitor certificate distribution and algorithm usage** more effectively.

- **New Notification for Auto-Renewal and Auto-Regeneration Events**

  A new notification event has been introduced to send emails to certificate administrators when auto-renewal or auto-regeneration is triggered by the system. Notification settings can be enabled or disabled via a checkbox at:
  - The **Certificate Group** level
  - The **Individual Certificate** level (overrides group settings)

  This feature provides fine-grained control over which automated actions should trigger email alerts.

- Added support for an optional profile parameter EKU for DigiCert Server Certificate.
- Introduced F5 XC integration to support Certificate Lifecycle Management (CLM) for Distributed Apps.
- VMware vCenter integration added for Machine SSL and Signing Certificate CLM.
- Introduced FortiManager integration to enable Certificate Lifecycle Management (CLM) operations.
- Enabled access elevation support for HAProxy devices and an option to skip version validation.

DDI+

- **Advanced Reporting for IP Hygiene in DDI+**

  Introduced **Advanced Reporting** to compare IP address footprints across IPAM, ADC, Tanium, Wiz, Forward Networks, and CMDB. Provides grid-based compliance reports with filters, Excel export, custom workflows, and cross-source comparison.

- **Sync Settings Improvements for Infoblox**

  Enhanced Infoblox sync integrations in DDI+ with a new CIDR Exclusion List option. Customers can now configure excluded subnets on the *Settings* page to prevent large or problematic ranges from causing sync failures.

  Default exclusions: /4 and larger subnets are excluded by default.

  Resilient sync: Matching CIDRs are skipped (with clear logs) while valid data continues syncing.

  Improved reliability: Sync jobs remain robust and uninterrupted.

- **New Remediation Framework for IP Hygiene Automation**

  Introduced a Remediation Framework to automate IP hygiene across integrated sources (IPAM, ADCs, Tanium, Forward Networks, CMDB, and custom tools). Key capabilities include:

- **Remediation Reports:** Generate reports using customer-defined logic discrepancies (for example, unused IPs in IPAM with footprints in CMDB or Tanium).
- **Dynamic Field Mapping:** Map Reservation Name/Description dynamically from external sources (for example, CMDB Server Name, ADC Application Name).
- **Remediation Workflows:** Validate and bulk-push updates (such as IP reservations) to IPAM with full outcome tracking.
- **Action Auditing:** Detailed success/failure logs integrated into Adoption Reports.

This framework enhances automation, reduces manual effort, and ensures resilient IP hygiene enforcement.

- **Workflow Engine and Dashboard page for Domain Compliance Scan Engine**
  - Introduced a **DDI Compliance Scan Workflow Engine** with a dedicated dashboard to streamline and visualize domain-level compliance checks.
  - **Automated Scans:** Now powered by the AVX API, enabling automated initiation and scheduling of scans—eliminating the need for manual intervention.
- Enhanced the Domain, Zone, Subnet, and IP Inventory grids with advanced search and filtering to provide deeper DNS and IP intelligence.

KUBE+

- **Download CA Certificates to Secrets and ConfigMaps**

  Added support to download CA certificates directly into Kubernetes Secrets and ConfigMaps, enabling seamless integration with Kubernetes-based workloads.

- **Revoke Certificates from Certificate Inventory**

  A new option allows users to revoke certificates directly from the certificate inventory when revoking the corresponding Certificate CRD instance in Secure Apps.

- **Renew and Push Certificates to Kubernetes Secrets**

  Users can now renew certificates and push them directly to Kubernetes Secrets from the certificate inventory, streamlining certificate lifecycle operations within Kubernetes environments.

PKI+

- **CA Private Key Encryption:** CA private keys are now secured using AppViewX's standard multi-layered encryption process, aligning with best practices for key protection.
- **PQC OID Updates:** Integrated the latest NIST-published Object Identifiers (OIDs) for Post-Quantum Cryptography (PQC) algorithms into AppViewX PKI, ensuring compliance with evolving cryptographic standards.

SSH+

- **Push Private Key to CyberArk**

  Users can now securely push a private key to CyberArk by providing Safe Name, Username, Account Name, and Server Name.

  Once the private key is stored, it can be accessed and managed directly from CyberArk.

- **SSH Key Provisioning with Optional Vault Integration**

  SSH+ now supports provisioning SSH keys to target hosts through an intuitive, step-by-step wizard interface. Key capabilities include:
  - Support for multiple key types: Key Pair, Public Key, and Private Key
  - Optional integration with vault solutions
  - Guided configuration process

- **Improved SSH Host Inventory Interface with Windows Vendor Support**

  The SSH Host Inventory has been enhanced to support adding new hosts with a Windows vendor.

- **Key Compliance Group Configuration and Evaluation**

  The Key Compliance Group configuration has been enhanced to provide more granular control and visibility into key compliance status.

  Key updates include ability to select specific compliance risks for evaluation, including:
  - Weak Keys
  - Orphan Keys
  - Suspicious Keys
  - Shared User Keys
  - Shared Host Keys
  - Algorithm, bit length, and age

Compliance evaluation can now be triggered automatically every 30 mins. Compliance status is now visible in the **Key Inventory** view.

- **Delete & Rotate Key Process Replicated for Windows**

  The Delete and Rotate key processes, previously available for Linux systems, have now been replicated for Windows hosts. This functionality supports communication via SSH+ with Windows Gateway.

- **Provision Key Process Extended to Windows**

  The Provision Key process, previously supported on Linux, has been replicated for Windows hosts. This functionality supports communication via SSH+ with Windows Gateway.

- **Managed Device Discovery for SSH Host Inventory**
  - Enables discovery of hosts already managed within the SSH Host Inventory.
  - Retrieves lists of Linux and Windows managed hosts from the inventory.
  - Performs SSH key discovery separately for Linux and Windows devices on the selected hosts.
  - Includes robust error handling to gracefully manage issues such as database connection failures or inventory API timeouts.
- **Support for Windows Vendor in Fetch Keys Action**

  Added support for the Windows vendor in the Fetch Keys action within the Host Inventory.

- **Added Create SSH Key Feature for User Keys**

  Users can now generate SSH keys using supported bit lengths and algorithms as defined by policy. Additionally, they can assign tags during key creation for better organization and management.

- **Removed Access Request Feature**

  Users can no longer request access to hosts as this functionality has been deprecated.

- **Discovery of Unsupported OpenSSH Formats**

  The system now detects unsupported OpenSSH formats including ssh-dss, ssh-rsa with key size less than 2048 bits, Legacy PEM private key format, rsa-sha2-256/512, ssh-ed25519, and ecdsa-sha2.

- **Added Adoption Widget to SSH Dashboard**

  A new adoption widget has been introduced in the SSH dashboard, displaying key lifecycle events such as creation, rotation, deletion, and provisioning of SSH keys.

- **Revamped SSH Dashboards**

  The SSH dashboards have been updated with a new design, offering an improved look and enhanced detail for better usability and insights.

SIGN+

- **UI-Based Control for HSM Parallelism**

  Users can now enable or disable HSM parallelism directly from the **Sign Settings** section in the UI.

  This provides greater flexibility to balance **performance** and **security** based on specific operational requirements, allowing for optimized signing workflows tailored to different use cases.

- **Configurable Polling for Sequential HSM Signing**

  When HSM parallelism is disabled, users can now configure polling behavior and define **retry count** and **retry intervals** for status checks during the signing process from the UI.

  This ensures better control and adaptability in scenarios where sequential processing is required.

- **SIGN+ Utimaco HSM Device Signing Support**

  This feature provides the signing support for Utimaco HSM Devices for both Hash based and File based signing

- **Simplified User Onboarding & Access Management**

  A new model has been introduced to streamline user onboarding, access control, and service account visibility for SIGN+ users. Key capabilities include:

  - Role- and permission-based access managed via **Single Sign-On (SSO)**
  - Ability for administrators to create dedicated **user groups** for SIGN+ with predefined permissions
  - Automatic user provisioning through SSO using birthright access
  - Service account creation for API usage, since SSO credentials are not valid for API calls. Service accounts are securely isolated and visibility is configurable (for example, Self or All).

    These enhancements ensure secure, scalable, and seamless access to SIGN+ for both administrators and end-users.

- **ECC Certificate Mapping for HSM-Backed Signing**

  This feature enables users to map existing ECC certificates enrolled via HSMs to the AppViewX Platform, allowing them to be reused for signing operations within SIGN+.

- **Hash-Only Input Support for API-Based Signing**

Users can now perform signing operations by providing **hash-only inputs** via API.

- Accepts input in **hex** or **Base64** format
- No need for **ASN.1 encoding**, simplifying integration and usage

Platform

- **NLP-based Reports (Tech Preview)**

  Support to generate reports related to CERT+ via natural language.

- **mTLS Support for Helm-Based CC Deployments**

  mTLS is now supported in Helm-based CC installations. For enablement, contact the SRE team.

- **K3s Cluster Upgrade Support for Standalone CC**

  Standalone CC installations now support **K3s cluster upgrades** using the `avxctl upgrade k3s-cluster` command. This allows updates to the K3s platform and third-party images to address vulnerabilities and ensure version alignment.

- **Code Sign Validation for CC Artifacts**

  Code signature validation is now enforced during install and upgrade for the following CC components:
  - avx-mid-server-base
  - mid_server_gateway
  - mid_server_installer_dependencies
  - mid_server_platform_dependencies
  - mid_server_syslog
- **New CC Monitoring Metrics in Grafana**

  Introduced enhanced monitoring for CC metadata in Grafana, including metrics such as CC status, version, upgrade availability, component versions, and mTLS data—enabling improved visibility for SRE teams.

- **RBAC - Sub Delegation**

  RBAC Delegation provides a flexible and secure way to distribute RBAC-related administrative responsibilities across hierarchical user groups. This capability allows super admins to delegate permissions without losing control of core RBAC structures.

  Key Highlights

  - **Delegated Administration:** Super admins can enable delegation from the User Group Inventory (option visible only to super admins). Delegated admins gain authority to manage users, user groups, roles, and resources within their hierarchy.
  - **Hierarchical Permission Model:** Supports one level of delegation (super admin → level 1 admins). Access rights are determined by a user's position in the delegation tree, ensuring clear boundaries of responsibility.
  - **Scoped Control:** Delegated groups operate independently. Delegated admins cannot edit their own, peer-level, or upper-level groups, ensuring a secure chain of command.
  - **Ownership and Visibility:** Any new users, user groups, roles, or resources created by delegated admins are automatically visible to both the delegated admin and the super admin, but hidden from other users. Maintains ownership and delegation hierarchy for all entities, ensuring clear accountability.
  - **Shift from Classic RBAC:** When delegation is enabled, traditional RBAC user groups are disabled. Users outside delegated groups but with RBAC ACFs attempting to manage RBAC will see a UI error prompting them to contact the Admin.
  - **Controlled Mapping:** Limits user group association to lower-level entities during mapping.
  - **Mapping of Existing Groups:** Provides the option to map existing user groups under a chosen hierarchy, allowing smoother transitions into the delegation model.
- **Omada IDP Integration**

  AppViewX has exposed the two new SCIM endpoints to support Omada IDP integration: **scim/v2/ResourceTypes** and **scim/v2/Schemas** APIs. These APIs will fetch the details from the scimConfig collection in the database based on the config type.

- **Enforce User-Level Isolation for Internal Service Account Access**

  User-Level Isolation is now enforced for Internal Service Account access. A two-level ACF control (Access) is implemented with Self Account and All Accounts access privileges under Service Account ACF. Users with Self Account privilege can view only the service accounts they create, whereas users with All Account privileges can view all the service accounts that is available.

- Introduced two new report widgets in AppViewX Pages: **Crypto Score Chart** and **Multi-Line Chart.** These widgets use hook-based data retrieval, support Global Filters, and dynamically render charts based on configured hooks.
- Added Area Chart support in the chart configuration system, providing an additional visualization option for time-series data.
- Added Source Control integration for Git, Bitbucket, and Azure Repos in the SaaS version—previously available only in on-prem deployments.

Chapter 2: Enhancements

This section describes the enhancements in this release.

ADC+

- A new API has been introduced to retrieve device archives along with associated master key information for a specified device and group.
- Introduced real-time notifications to alert users immediately when a device's status changes.
- Introduced the ability to manage event source mappings within the AppViewX system, with a specific focus on the *Objects* event source.
- AppViewX now supports BeyondTrust credential integration for Citrix ADC devices.
- API support is provisioned for enable/disable operation of Application widget.

CERT+

- **Support for Managed Identity in Azure Resource Onboarding**

  AppViewX now supports Managed Identity as a credential type for onboarding Azure resources.

  Managed Identity is an Azure-generated identity that allows users to authenticate to Azure AD-protected services without needing credentials. An Azure-assigned identity is used for Azure AD authentication that fetches tokens automatically without storing credentials in AppViewX.

- **Lego Client Enhancements**

  The Lego client now supports **Let’s Encrypt** and integrates with the **AppViewX Plugin** enabling:

  - Seamless certificate management via AppViewX's enterprise-grade ACME solution
  - Plugin-based extensibility for custom logic
  - AppViewX-managed challenge updates and deletions
  - Support for record-based challenge validation

- **HTTP Support for CMP**

  The Certificate Management Protocol (CMP) is now extended to work with HTTP as well in the certificate lifecycle management platform. It enables certificate enrollment and revocation as defined in RFC 4210, ensuring compatibility with clients that use HTTP.

- **Default Enablement of Sectigo CA Support Across Protocols**

  Sectigo CA is now enabled by default for all supported certificate enrollment protocols:

  - ACME, SCEP, EST, and Intune
  - Additionally, the list of supported CAs for all protocols is now centrally managed using a common metadata configuration, ensuring consistency and easier control.
- **Distributed S3 Bucket Support for AWS Federated Account EC2 Onboarding**

  AWS EC2 cross-account onboarding now supports account-specific S3 buckets along with the centralized bucket approach. Account-specific S3 buckets improve efficiency and reduce operational risks such as access violations and single point of failure.
- **Expose API for creating and updating CA Policy in REST Palette**

  Enhanced support via API to create and update the CA policy via REST Palette.
- **Ability to view CERT Insights with multiple groups**

  Added the ability to select and view multiple certificate groups across all dashboards under the **Insights** page.

KUBE+

- Users can now download `appviewx-auth secret` when OAuth is selected during advanced onboarding.
- Users can now navigate across pages in KUBE+ using AVXpert.
- Support for date format preferences provided across all pages in KUBE+.

PKI+

- **Custom Template Deletion Behavior Updated**

  Custom templates can now be deleted; however, deleted templates will still appear on the last page of the **Templates** view for reference.
- **Template Activity Tracked in Audit Logs**

  All changes, deletions, or errors related to templates are now logged and accessible via the **Audit Logs**.
- **Custodian Email Field Added**

  A new field for the **Custodian's Email ID** has been introduced. It is auto-populated when a username is selected and is used to send approval links and notification messages directly to the custodian.
- **Enhanced M(N) Approval Flow with In-App Notifications**

Previously, the M(N) approval flow relied solely on email for communication and validation. With this enhancement:

- Users now receive **in-app notifications** that provide direct access to the approval screen.
- Notifications alert users when quorum is achieved or if approval validity has expired.
- This mechanism complements existing email alerts and can be configured in **PKI settings** to use email, in-app notifications, or both.

All actions and events related to approval notifications are now recorded in the **Audit Logs** for traceability.

Platform

- **Enhanced Prerequisite Checks for Smoother Onboarding**

  Additional prerequisite validations have been introduced to streamline the Cloud Connector (CC) onboarding process and reduce setup issues.

- **Critical Downtime Alerts for Cloud Connector**

  Cloud Connector downtime alerts have been upgraded in severity and are now marked as **Critical**, ensuring customers are promptly notified of service disruptions.

- **Security Updates: Library and Image Upgrades**
  - **Cloud Connector Libraries & Third-Party Components:** Upgraded core components including K3s, mirrored CoreDNS, and Helm binaries to their latest versions to address known vulnerabilities.
  - **Alpine Base Image:** Upgraded to the latest version in the CC container to fix vulnerabilities.
- **Improved CC Prerequisite and Firewall Error Handling**
  - During installation, Cloud Connector now detects active firewalls and prompts users to allow required ports.
  - All prerequisite error messages are consolidated and displayed together post-installation, ensuring better visibility and acknowledgment.
- **Improved Email Task Error Handling with Configurable Failure Behavior**

  Previously, if an invalid email address was specified in an email task, the task was marked as successful despite email delivery failure, with an error message only logged in the task logs.

  With this enhancement:

  - Email tasks will now be marked as *failed* if an error occurs while sending the email.
  - A new toggle key, `continueOnFailure`, has been introduced for email tasks.

  - *Enabled* by default to preserve existing behavior.
  - When *disabled*, any error (for example, invalid email address) will cause the task to fail.
- **JWT Token Authentication for REST Integration**

  A new authentication type, **JWT Token**, has been added under the REST integration type on the **Integration Vendor** page.

  - Enables secure execution of **Command Repository REST API** calls using JWT-based integrations.
  - Supports routing JWT-authenticated API calls through a configured proxy server.
- **Draft Request Global Variable Retrieval via API**

  In cases where a request is saved as a draft and contains **global variables**, these variables were previously not persisted in the `visualworkflow_request_inputoutput` collection until form submission.

  - The `visualworkflow-search-data` API has been enhanced to support this scenario.
  - It now accepts key-value pairs in the request payload, queries the relevant collection, and returns associated **request IDs**, even for draft requests.
- **Standardized Audit Log Format**

  A unified format for **audit logs** has been implemented across the platform to ensure consistency and improve log readability and traceability.
- **Strict Mode for Prevalidation and Postvalidation Palettes**

  By default, Prevalidation and Postvalidation palettes succeed even if there are device command or communication failures.

  To allow stricter validation:

  - A new flag, `enableStrictMode`, has been introduced.
  - When *enabled*, any such failure will cause the palette to be marked as *failed*.
  - Default is *disabled*, preserving current behavior.
- **API for Resource-Level RBAC Permissions in Form Tasks**

  A new API allows updating **RBAC permissions** for form tasks within a workflow at the resource level.

  - Requires **workflow request permissions** for invocation.
  - Supports bulk updates across multiple workflows.
  - Allows assigning or unassigning **Create**, **Review**, or **Submit** permissions to specific resources.
- **New API Gateway Profile for Internal REST Palette Usage**

  In alignment with EIS recommendations, a new **API Gateway profile** has been introduced specifically for APIs used within Visual Workflow. This profile is dedicated to the REST internal palette and enhances API visibility, monitoring, and ensures backward compatibility for existing integrations.

- **Improved Onboarding with Additional Prerequisite Checks**

  New prerequisite validations have been added to simplify and streamline the Cloud Connector (CC) installation process.

- **Critical Severity for CC Downtime Alerts**

  Cloud Connector downtime is now reported through Critical alerts, ensuring customers are promptly and clearly notified of service disruptions.

- **Security Enhancements: Library and Image Upgrades**
  - Updated core components including K3s, mirrored CoreDNS, and Helm binaries to their latest versions to address security vulnerabilities.
  - Upgraded the **Alpine base image** used in CC to the most recent version for improved security and stability.
- **Improved CC Prerequisite and Firewall Error Handling**
  - During installation, CC now detects if a firewall is enabled and prompts users to allow the required ports.
  - All prerequisite errors are now consolidated and displayed together at the end of the installation, improving visibility and user awareness.
- **User Profile Update Notification Policy Enabled by Default**

  AppViewX now enables the User Profile Update Notification policy by default. Users automatically receive alerts (via email and optional in-product notifications) whenever profile attributes such as email or phone number are updated. This ensures better visibility into sensitive user attribute changes without requiring manual log reviews.

- **CyberArk: Multi API Profile & String as Address Support**

  The CyberArk API integration has been enhanced to support multiple API profiles within AppViewX. Key updates include:
  - Ability to configure and manage multiple CyberArk API profiles.
  - Default profile names added to existing configurations and mapped to current settings.
  - A CyberArk API Profiles dropdown introduced in the CyberArk Layout page to select the appropriate profile.
  - Support for string values in the IP/FQDN Address field, enabling the use of logical names for CyberArk connectors.
  - Restriction to upload only .pfx files on the CyberArk API Profile page.
- **Help Info updates for PAM integrations: Form and API Settings**

Help info icons with relevant details has been added to the form fields for all PAM Integrations as follows:

- Add Credentials form - AppViewX, CyberArk, Thycotic, Hashicorp, BeyondTrust
- API Profile Settings form - CyberArk, Thycotic, Hashicorp, BeyondTrust

- **Replace admin user group with new user group with restricted permissions for scheduler service accounts**

  To improve security and enforce the principle of least privilege, the default **admin user group** and **admin role** previously assigned to scheduler service accounts have been replaced with a dedicated:

  - Scheduler User Group
  - Scheduler Role

  These new defaults grant restricted permissions tailored specifically to scheduler-related operations, eliminating unnecessary administrative access.

- **Ability to create and push Multi-Year License**

  AppViewX now supports the creation and management of **multi-year licenses**. Licenses can be generated with a validity period of **more than one year**, offering greater flexibility for long-term planning.

  To ensure control and compliance, an internal logic enforces a **maximum license duration of five years**.

- Enhanced a comprehensive UI component in the AppViewX Reports module that allows users to customize the visual appearance of grid charts. This feature provides granular control over header and row styling, including font sizes, text colors, and background colors.

Chapter 3: Bug Fixes

This section describes the bug fixes in this release.

CERT+

- **Linux Discovery:** Results are now limited to KDB certificates only when the KDB format is selected during onboarding.
- **IBM Client Discovery (Windows):** Fixed an issue where certificates could not be discovered if the certificate path contained spaces.
- **Imperva AWS Onboarding:** UI and functional issues on the onboarding page have been resolved.
- **Akamai CPS:** Corrected the **Push to Production Intent** behavior.
- **Access Control Enhanced for Discovered Certificates**

  Previously, unprivileged users could monitor or manage discovered certificates. This has been corrected: only users with read/write access to the relevant certificate group can now access these operations.

- **Improved Intune Challenge Validation Error Reporting & API Update**

  Intune Error Handling has been improved to capture and relay the exact error from the Azure portal back to the client machine, allowing for more precise troubleshooting.

  With Microsoft deprecating Azure AD Graph APIs, customers are now required to use Microsoft Graph API to ensure seamless Intune enrollment.

Platform

- **Task Logs Overlay Issue Resolved**

  Previously, clicking the **Maximize** button in task logs (Stage View) displayed a faded overlay on top of the expanded logs screen. This overlay issue has now been fixed.

- **Improved Error Messaging for Invalid Workflows**

  When an invalid workflow was enabled without validation and scheduled for execution, the system previously returned a generic error: *Service unavailable. Try after sometime.*

  This has been updated to return a specific error message, *Invalid Workflow*, clearly indicating the root cause.

- **Script Execution Unblocked After Invalid Form Submissions**

Previously, if a form submission had invalid field entries, subsequent execution of an associated script would fail due to lingering validation errors. This issue has been resolved; script execution now works independently of previous form validation states.

- **Workflow Import Error Handling Improved**

  Importing a helper script into a workflow could previously result in the entire request execution failing if there was an import error. This has now been fixed.

- **UI Alignment Fixed on Approve/Reject Page Accessed via Email**

  An alignment issue was observed on the page rendered after accessing the Approve/Reject action via an email link. This rendering issue has now been fixed to ensure proper UI alignment and consistent layout display.

- **Enforced Access Control for File Operations in Forms**

  In the **Form** task upload field, the UI enforces access control by preventing unauthorized users from performing file download or delete operations. Previously, these operations could still be executed via direct API calls, bypassing the UI restrictions.

  API-level resource-based authorization checks have now been implemented to align backend enforcement with UI restrictions. The API will validate that the requesting user has the necessary resource permissions on the associated request before allowing file download or deletion.

- **Deadlock Issue with Cloud Connector Status Update Resolved**

  Previously, an API call made after health persistence caused a deadlock with HSM, which prevented the Cloud Connector status from being updated. This has been resolved by replacing the API call with a direct method call.

- **Improved SNI Handling in API Calls**

  The system now uses the configured FQDN directly without resolving it to an IP, ensuring correct SNI processing during API communication.

- **Restriction of single user session in application**

  The **Force Logout** option is added to the Users page to immediately terminate the user's active sessions. However, the list of users available for force logout depends on the All/Self Account privilege in the Access ACF.

  Restriction of single user session in application will be enabled automatically for fresh installation.

- The certificate selection logic from the IDP metadata is updated to ensure reliable signature validation.
- The Apache Shiro vulnerability in the Cloud Connector is addressed by upgrading the Shiro-Ehcache to version 1.11.0.

Chapter 4: Known Issues

This section describes the known issues in this release.

ADC+

- If the AVI device name contains characters other than A–Z, a–z, 0–9, underscore (_), or dot (.), the external device backup will fail.

CERT+

- **GCP Load Balancer:** Certificates other than Global ALB are not discovered. Push and bind to other load balancers other than Global ALB are not working.
- The DigiCert Duplicate action is currently failing for one-step certificate approval, even though the certificate has already been manually approved and issued in the DigiCert CA portal.
- The movement of expired certificates to the Auto-Archival inventory gets stuck once the triggered cron job for certificate auto-archival reaches a threshold.
- Certificate enrollment fails for CSR generation as HSM for F5 device.
- For GlobalSign MSSL certificates, the uploaded certificate's validity is fixed at 365 days. Auto-regeneration is currently not supported, either via the UI or the exposed API.
- For SwissSign certificates, the Auto-Regenerate value for uploaded certificates is not being set based on the Group-level Auto-Regenerate toggle days.

Platform

- Email Subject Banner is missing from the Azure SSO certificate mail when SMTP is with Oauth API.
- When adding SMTP - Oauth with communication API, the **Hostname** and the **Port** fields are not mandatory.
- MFA enabled - When usergroup is not mapped for user, it is better to disable the resend OTP button on the MFA authentication page.

Chapter 5: Known Limitations

This section describes the known limitations in software in this release.

CERT+

- When migrating from any version earlier than **v2023.1.0 FP2** to **v2024.3.0**, a configuration sync for Azure settings must be manually triggered post-migration.

  Certificates manually pushed to the App Service cannot be discovered. Only certificates linked via Azure Key Vault are supported for discovery.
- During migration from **AppViewX v2020.3.0** to **v2024.3.0**, zones must be manually updated for Amazon Public CA.
- Following the Thames FP3 release, AWS customers using IAM Role Access (Credential Type) for onboarding must download the new CloudFormation template from the Cloud Addition page and update the trust relationship for the master role.
- Azure Managed Identity is supported only in SaaS deployments. It is not supported for Managed Kubernetes environments.
- Enrollment of certificates with CSR generation in FortiManager and Endpoint now supports auto-regeneration using the same CSR file name.

Platform

- Profile details such as **First Name, Last Name, and Email** are not updated when logging in with a RADIUS user.
- CyberArk API profile added with auth type - basic is not supported in credential page for fetching profile names