appviewx

Release Notes

Version: 2025.0.1.0 (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 v2025.0.1.0 (SaaS) Release Notes	Dec 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 v2025.0.1.0.

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.

Architecture

AppViewX now captures and logs failed or unauthorized EST requests that were previously dropped at the Gateway layer. The Gateway detects invalid certificates, missing credentials, or malformed EST paths and forwards these failure events securely to AppViewX. These events are now displayed under Audit Log tab, providing administrators improved visibility into rogue or unsuccessful EST access attempts.

Chapter 2: Enhancements

This section describes the enhancements in this release.

CERT+

- **Cloud Connector**
  - **Optimized K3s Upgrade and Cleanup for SHA Versions and Backups**

    Enhanced certificate management support is introduced for EST endpoints, including the ability to discover existing certificates, push new certificates, and bind certificates to EST endpoints after the push. These capabilities streamline certificate lifecycle operations and minimize manual configuration effort in EST endpoint management.
  - **Enhanced EST Endpoint Certificate Management**

    The system now removes older SHA versions and backups during the K3s cluster upgrade, reducing storage usage and ensuring a cleaner and more efficient environment.
  - **Enhanced Certificate Format Flexibility in Cloud Connector**

    Enhanced the Application Connector interface for Cloud Connector to support switching the certificate format from .jks to .pem, with an added configuration option to include Root and Intermediate certificates when applicable. When .pem is selected, a new checkbox will be enabled by default to allows users to optionally push Root and Intermediate certificates. This update provides greater flexibility for certificate deployment in Cloud Connector environments that rely on .pem formats.
  - **Expanded Scheduled Certificate Sync for Cloud Connector Devices**

    Expanded the scheduled certificate sync job to include Cloud Connector devices. The job sync now discovers and updates certificates for Cloud Connectors along with all other supported devices, while honoring the existing job enable/disable settings. This enhancement ensures consistent certificate synchronization across all device types and provides accurate, up-to-date visibility for automation, compliance, and reporting.
- **Audit Logging and Visibility for Unauthorized or Rogue Access Attempts to the EST Server**

  AppViewX now captures and displays audit logs for unauthorized or rogue access attempts to the EST Server. Previously, only valid EST client activity appeared under Certificate Logs and Audit Logs, while unauthorized access attempts were dropped at the Gateway and never recorded. With this enhancement, failed authentication events logged by the Gateway are forwarded to AppViewX, for visibility and security monitoring.

The system records key metadata—including source IP, timestamp, endpoint accessed, and failure reason—and presents these entries in the AppViewX Audit Log UI, clearly distinguishing them from successful events. This enables stronger auditing, threat detection, and operational transparency across the EST ecosystem.

- **Register IoT Device to Azure IoT hub**

  A new global setting, **Enable IoT Device Registration,** has been added to the Auto-Enrollment > EST Global Settings page. This feature enhances the EST auto-enrollment by introducing a centralized control for IoT Hub device registration. Enabling this global setting within individual EST configurations, allows administrators to enable/disable IoT device registration for each EST configuration and also link specific Azure IoT Hub account from the Integration Hub. After the successful EST enrollment, the certificate and the device details can now be automatically registered to the selected Azure IoT Hub account in the EST configuration settings.

- **mTLS Certificate Crypto Operations using HSM in EST Standalone Server**

  This enhancement extends the EST Standalone Server's PKCS#11-based HSM integration to support mTLS client authentication certificates. The server can now use an HSM-backed private key for mTLS authentication, ensuring that all key generation, storage, signing, and TLS handshake operations occur securely within the HSM.

  Key improvements include:
  - A configurable option to use HSM-managed private keys for mTLS client authentication, in addition to existing software key support.
  - Full hardware-backed protection for all mTLS cryptographic operations with the AppViewX EST endpoint.
  - Reuse of existing PKCS#11 session management to maintain consistency and reduce complexity.

  This enhancement strengthens security and compliance by ensuring the mTLS private key never leaves the HSM while maintaining seamless interoperability with the EST ecosystem.

- **mTLS Authentication enabled for EST Standalone Server during Device Registration**

  Added support for mTLS-based authentication to secure device registration communication between the EST Standalone Server and AppViewX.

  Enhancements include:

  - The EST Standalone Server now accepts configurable client certificates and private keys for authentication.
  - Administrators can specify trusted CA certificate(s) to validate the AppViewX server certificate.
  - The server securely loads and manages client credentials (certificates and private keys) from either the file system or an HSM, ensuring strong security and integrity.
- **Enhancement to WAEP Template Configuration**

  The enhancement introduces a configurable option in the WAEP certificate template settings that lets administrators choose which DNS entries to include in the SAN field.
- **Native SCIM Integration Support for Omada Identity Governance**

  This enhancement introduces native SCIM-based integration between AppViewX and the Omada Identity Governance platform to enable standardized and automated provisioning and deprovisioning of users and groups.

  The implementation uses GUIDs as the primary identifier for both Users and Groups to ensure consistency, scalability, and long-term compatibility. While newly provisioned entities will use GUID as the default ID, the system continues to support both GUID and loginName for backward compatibility.

SSH+

- Added support for mutual TLS (mTLS) to enforce certificate-based client authentication on the SSH Certificate Create API. The API now validates client certificates—checking issuer and expiry—against configured CA certificates, ensuring only trusted services can access the endpoint. mTLS settings and issuer certificates can be managed in the **SSH Advanced Settings** page.
- Enabled users to create and provision SSH certificates directly from the SSH inventory using an existing SSH CA (locally stored or HSM-backed). Users can generate and deploy an SSH certificate for a specific user and endpoint.
- Enhanced SSH CA management to support storing private keys in an Entrust HSM for newly created SSH CAs. This ensures secure custody of SSH CA key material, enforces cryptographic compliance, and prevents private keys from being stored in local storage.

Chapter 3: Bug Fixes

This section describes the bug fixes in this release.

CERT+

- Fixed an issue where scheduled discovery configurations for Microsoft Enterprise CA did not display the previously selected time range when editing the instance. This was caused by asynchronous data loading and has been resolved by introducing a delay to ensure dependent data loads correctly.
- Resolved an issue where certificates enrolled through WAEP were incorrectly marked as *Managed* instead of *Monitored*. All certificates issued through AEP protocols in AppViewX will now be maintained in the *Monitored* status.
- Intermittent failures in the Certificate Vulnerability job causing incorrect data population have been fixed. The failures were caused due to timeout limits imposed by the architecture. Modifications in the batch processing logic and dynamic backups have been introduced to mitigate the failures.

  Proxy support for vulnerability checks, however, remains unavailable.
- Fixed issues with adding custom attributes for the Sectigo CA caused by a mismatch between the CA name stored in the database (Comodo Certificate Manager) and the name used to retrieve attributes (Sectigo). A transform method has been introduced to map the names, ensuring that custom certificate attributes are now retrieved as expected.
- Issues with custom attributes not appearing in the certificate data exported from the server certificate inventory have been fixed. The export flow has been updated to ensure all custom attribute values are accurately included in the exported data.
- The issue with adding custom attributes for the Sectigo CA on the Certificate Attributes page has been resolved. The root cause was a mismatch between the certificate authority name stored in the database (Comodo Certificate Manager) and the name used to retrieve the custom attributes (Sectigo). A fix has been implemented to map the names correctly, ensuring that the custom attributes are now fetched successfully.
- Resolved an issue where the holistic view displayed an incorrect port number for the IIS connector when discovered through the Integrated Windows Gateway (IWG) agent.

PKI+

- Fixed issue with enrolling certificates using PKI.

Platform

- AppViewX resolved an issue where log messages containing JSON strings were causing malformed event payloads when sent to the Splunk API, leading to failures. The fix introduces proper JSON escaping and serialization before embedding log messages into the Splunk event payload. By encoding JSON content and escaping special characters, all event payloads now maintain valid structure, enabling successful ingestion and processing by the Splunk API without errors.

> **Note:**
>
> The Cloud Connector must be upgraded to the latest version for the fix to take effect.

Chapter 4: Known Issues

There are no known issues in this release.

Chapter 5: Known Limitations

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

SSH+

- Support is available only for generating RSA and EC CA key pairs in Entrust HSM.
- Support is also limited to signing and generating RSA/EC SSH certificates using RSA/EC CA certificates/key pairs stored in Entrust HSM.