appviewx

Release Notes

Version: 2024.3.1.0 (On-Prem)

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 v2024.3.1.0 (On-Prem) Release Notes	Sep 2025

About this Guide

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

Intended Audience

• Customers onboarding AppViewX v2024.3.1.0.

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

There are no new features in this release.

Chapter 2: Enhancements

This section describes the enhancements in this release.

Platform

- Improved CyberArk credential retrieval by removing the keystore dependency, enabling parallel fetching of credentials from CyberArk.
- **SCIM API Enhancements**
  - Enhanced SCIM APIs to support UUID as the user identifier for newly provisioned users, while maintaining backward compatibility for existing users using `loginName`.
  - All SCIM APIs now support the `application/scim+json` content type.
  - The `ServiceProviderConfig` API is now excluded from session-based authentication.

Chapter 3: Bug Fixes

This section describes the bug fixes in this release.

CERT+

- Users can now view and update certificate profiles under **CERT+ Administration.**
- After updating an expired password, users can now continue to manage all services associated with all child accounts of a multi-subscription Azure device.
- Domain auto-selection issues for enrollment and renewal of GlobalSign MSSL certificates have been fixed.
- Users can now see IIS Application connectors are in sync status after pushing and binding certificates using the **Update Site Binding** or **Create New Site Binding** options.
- Certificates that do not have the server or client authentication extended key usage can now also be bulk revoked from the inventory.
- Manually added application connectors will now inherit the **Push Automatically** flag from the certificate group settings, ensuring consistency and reduced manual effort.

Platform

Fixed issue where AWS accounts went from *Managed* to *Unresolved*.

SIGN+

Users can now install the SIGN+ package even when multiple certificates mapped to different policies share the same Common Name (CN). The installation process accurately identifies and retrieves all such certificates without conflict, ensuring seamless access and consistent policy enforcement despite CN duplication.

Note:

This functionality is supported for CSP; however, PKCS#11 treats the Common Name as a unique identifier and may not support this behavior.

SSH+

The **Delete keys from endpoints** action no longer blocks the deletion process if keys mapped to failed/unmanaged SSH+ Hosts are part of the deletion request.

Chapter 4: Known Issues

There are no known issues in this release.

Chapter 5: Known Limitations

There are no known limitations in this release.