

Software Vulnerability Manager (Cloud Edition) Release Notes

March 2025

Introduction	1
New Features and Enhancements	2
Patch Publisher Enhancements	2
Hide Deployment Notifications in Workspace ONE	2
Updated Default URL for SVM Cloud Connection	2
Paginated Intune Groups	2
Software Vulnerability Manager User Interface Enhancements	3
Manage Assignments in Quick Patch.....	3
Paginated Intune Groups	3
Reference: Latest Binary Versions.....	3
Known Issues	4
Resolved Issues.....	4
Community Blogs	4
Product Feedback	5
Legal Information	6

Introduction

Flexera's Software Vulnerability Manager is a software vulnerability and patch management solution that facilitates a customized patch management process. It combines vulnerability and threat intelligence, end point assessment, and patch creation and publishing enable informed and rapid patch management.

Software Vulnerability Manager can assess software vulnerabilities for both Microsoft and non-Microsoft (third-party) product vulnerabilities covering Microsoft Windows, macOS, and Red Hat Enterprise Linux. The results of this assessment are connected to our vulnerability and threat intelligence to allow for effective prioritization. Finally, third party patches may be created and published to remediate endpoints using Microsoft® WSUS (often in conjunction with System Center Configuration Manager), via Microsoft® Intune, VMware® Workspace One, BigFix, or Tanium.

SVM Patch Publisher inherits its current functionalities from the Patch Daemon. SVM Patch Publisher enables you to configure connections to the SVM server and to the supported end point management systems. The tool polls SVM on a configured frequency to look for new patches resulting either from a manual publishing or Patch Automation to publish patches to the specified end point management system.

New Features and Enhancements

Software Vulnerability Manager (Cloud Edition) includes the following new features and enhancements:

- [Patch Publisher Enhancements](#)
- [Software Vulnerability Manager User Interface Enhancements](#)
- [Reference: Latest Binary Versions](#)

Patch Publisher Enhancements

The following improvements have been added to the SVM Patch Publisher.

- [Hide Deployment Notifications in Workspace ONE](#)
- [Updated Default URL for SVM Cloud Connection](#)
- [Paginated Intune Groups](#)

Hide Deployment Notifications in Workspace ONE

A new **Hide Notification** check box has been introduced when adding connections to Workspace ONE. This enhancement allows users to control the visibility of notifications, reducing unnecessary alerts, and ensuring a streamlined user experience.

Updated Default URL for SVM Cloud Connection

The Site URL for Patch Publisher connections has been updated from `csi7.secunia.com` to `svm.flexera.com` to improve consistency and user experience.

With this update:

- When selecting the **Cloud** option under **Server Type** in Patch Publisher, the Site URL will now be pre-populated as `svm.flexera.com`.
- Users can establish a successful connection to the new URL using both **Standard** and **SSO** authentication.

Paginated Intune Groups

In the **Intune Assignment Groups** dialog box, pagination has been enhanced with the addition of the **Next** and **Previous** buttons, improving navigation between pages.

- **Next Button**— Click to proceed to the next page.
- **Previous Button**— Click to return to the previous page.

Software Vulnerability Manager User Interface Enhancements

The following improvements have been added to the Intune publishing.

- [Manage Assignments in Quick Patch](#)
- [Paginated Intune Groups](#)

Manage Assignments in Quick Patch

The **Manage Assignments** panel has been introduced in QuickPatch, enhancing the management of endpoint deployments during Intune publishing. This new panel allows users to assign deployments within the endpoint management system.

In this panel, you can add the following assignments during endpoint deployments in Intune publishing:

- **Add Groups**— Assigns specific groups
- **Add All Devices**— Assigns all devices
- **Add All Users**— Assigns all users

These assignments can be applied to the **Required**, **Available**, and **Uninstall** sections.

Paginated Intune Groups

In the **Manage Assignments** option of **QuickPatch**, **Subscription**, and **Patch Deployment Status** pages, the **Intune Assignment Groups** dialog box now includes improved pagination with scrolling. As you scroll, the next set of data loads, improving usability and navigation.

Reference: Latest Binary Versions

The following is a list of the latest binary versions available in this release:

- SVM ActiveX Plug-in v7.6.0.29 (No change)
- Single Host Agent v7.6.0.29 (No change)
- SVM Daemon v7.6.0.29 (No change)
- SVM System Center Plugin v7.6.0.29 (No change)
- SVM Patch Publisher v7.25.1926 (To download this installer, [click here](#))

Refer “Enhancements and Resolved Issues” for changelog.

- SVM Cloud Client Toolkit v5.0.1926 (To download this installer, [click here](#))

This toolkit contains offline utilities such as the Multi-partition Reporting Tool, WSUS Management Tool (also available in SVM Patch Publisher), and Client Data Tool which add value to SVM. This toolkit does not include the Patch Daemon. This toolkit is for SVM Cloud edition only.



Note • On September 23, 2024, digital signing updates were released for SVM Patch Publisher (version 7.22.1546) and SVM Cloud Client Toolkit (version 5.0.1546).



Note • *Flexera SVM Patch Configuration* will be deprecated in the future; therefore, you are encouraged to migrate to the new SVM Patch Publisher tool.

Known Issues

The following table lists the known issues in Software Vulnerability Manager (Cloud Edition):

Issue	Description
IOK-1345425	In the SVM UI, the Deselect option is not available in the Add Groups pop-up for Intune connections.

Resolved Issues

The following table lists the customer issues that were resolved in this release of Software Vulnerability Manager (Cloud Edition):

Issue	Description
IOK-1337474	In Patch Publisher version 7.24, if only one WSUS connection is added as a distribution system and no groups are selected for deployment, the approval task encounters an “Object reference not set to an instance of an object” error.
IOK-1060172	The Client Data Tool returns an Invalid Token error when the password includes special characters.
IOK-1343745	For certain users, the minimum version for Firefox (x64) is not displaying correctly in the VPM subscription.

Community Blogs

Please subscribe to the latest posts about Software Vulnerability Manager by going to <https://community.flexera.com/t5/Software-Vulnerability/bg-p/SoftwareVulnerabilityManagementblog> and clicking **Subscribe**.

Please subscribe to the latest release announcements concerning Software Vulnerability Manager by going to <https://community.flexera.com/t5/Software-Vulnerability/bg-p/Software-Vulnerability-Release-blog> and clicking **Subscribe**.

Product Feedback

Have a suggestion for how we can improve this product? Please share your feedback with the product team by visiting the Software Vulnerability Manager Forum in the Flexera Community:

<https://community.flexera.com/t5/Software-Vulnerability/bd-p/SVM-Discussion>

Legal Information

Copyright Notice

Copyright © 2025 Flexera

This publication contains proprietary and confidential information and creative works owned by Flexera and its licensors, if any. Any use, copying, publication, distribution, display, modification, or transmission of such publication in whole or in part in any form or by any means without the prior express written permission of Flexera is strictly prohibited. Except where expressly provided by Flexera in writing, possession of this publication shall not be construed to confer any license or rights under any Flexera intellectual property rights, whether by estoppel, implication, or otherwise.

All copies of the technology and related information, if allowed by Flexera, must display this notice of copyright and ownership in full.

Intellectual Property

For a list of trademarks and patents that are owned by Flexera, see <https://www.flexera.com/legal/intellectual-property.html>. All other brand and product names mentioned in Flexera products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

Restricted Rights Legend

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.