

Software Vulnerability Manager (On-Premises Edition) Release Notes

July 2021

Introduction	1
New Features and Enhancements	1
Assignment Group Support for Intune in SVM Patch Configuration	2
New Software Vulnerability Manager Client Data Tool.....	2
Binary Versions Changed.....	3
Known Issues	4
Resolved Issues	4
Community Blogs	5
Product Feedback	5
Legal Information	5

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 an 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 or VMware® Workspace One.

New Features and Enhancements

Software Vulnerability Manager (On-Premises Edition) includes the following new features and enhancements:

- [Assignment Group Support for Intune in SVM Patch Configuration](#)
- [New Software Vulnerability Manager Client Data Tool](#)

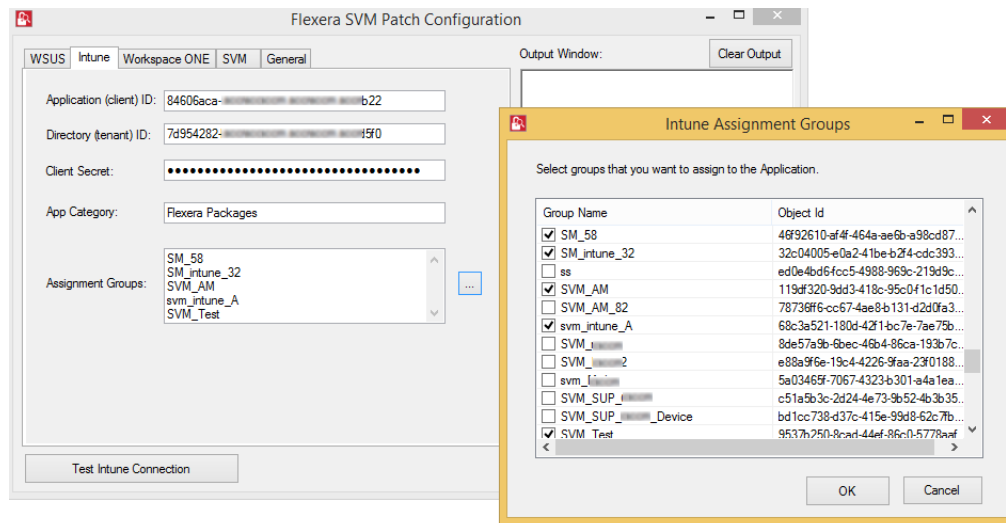
- [Binary Versions Changed](#)



Note • To see the following new features and enhancements in your Software Vulnerability Manager (On-Premises Edition) interface, you must refresh your browser's cache (press Ctrl+F5).

Assignment Group Support for Intune in SVM Patch Configuration

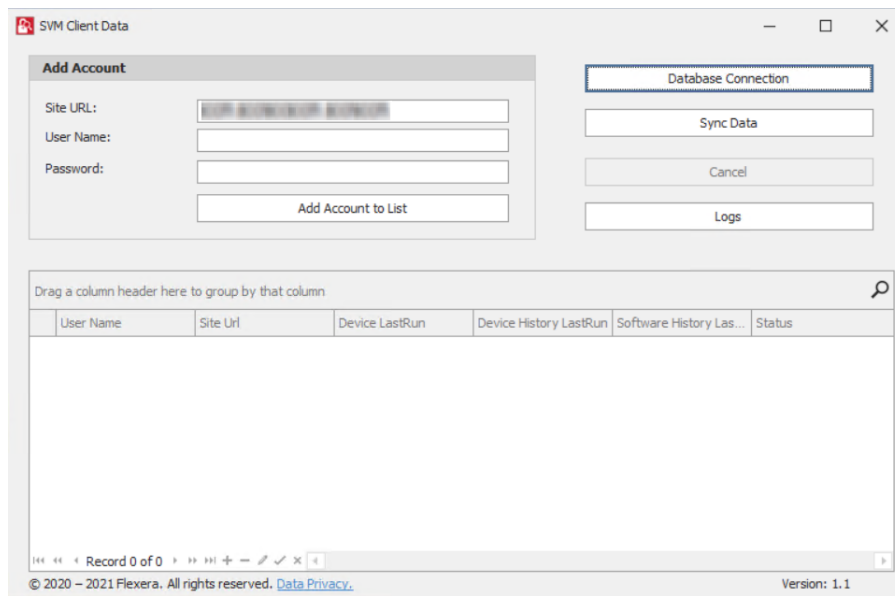
With this release, for Intune publishing, you can now choose a group or multiple groups and make assignments for endpoint deployments in the SVM Patch Configuration (Patch Daemon).



For more information, see [Assignment Group](#).

New Software Vulnerability Manager Client Data Tool

A new tool - SVM Client Data is added to the SVM Client Toolkit. Upon installing the new version of SVM Client Toolkit, a shortcut for SVM Client Data will be created on the desktop. This will allow you to store your SVM data in a Microsoft SQL database to keep for as long as you wish.



Alongside the SVM Client Data Tool, Power BI templates have been included. These templates provide a starting point for customizing data trend reports. Power BI is a part of Microsoft's power platform. To customize the included template, download Power BI Desktop (<https://powerbi.microsoft.com/en-us/downloads/>).

Binary Versions Changed

The following version of the binaries provided are:

SVM ActiveX Plug-in v7.6.1.15 (no change)


Single Host Agent v7.6.1.15 (no change)

SVM Daemon v7.6.1.15 (no change)

SVM Client Toolkit Installer v5.0.414 (download [SVM Client Toolkit](#)).

Known Issues

The following table lists the known issues in Software Vulnerability Manager (On-Premises Edition):

Issue	Description
IOJ-2177891	<p>Applications that are installed to a location other than their default location may not appear.</p> <p>Java is often included with other applications. When vulnerable, the application that installed Java should be patched. Deploying a Java patch will only update/install Java to its standard location and will not patch the instance shipped with a third-party product.</p> <p>To avoid confusion and improper patching attempts, SVM intentionally scans for Java only in standard locations. If you would like to ensure known instances appear in scan results, you may choose to add a custom product in Custom Scan Rules.</p>  <hr/> <p>To add a custom product in Custom Scan Rules:</p> <ol style="list-style-type: none">1. Choose Custom Scan Rules from the Filter Scan Results node under the Scanning menu.2. Click New Custom Scan Rule.3. Enter the name and browse to the file that you wish to have appear in scan results.

Resolved Issues

The following table lists the customer issues that were resolved in Software Vulnerability Manager (On-Premises Edition):

Issue	Description
IOJ-2191902	Adobe Digital Editions 4.x showing wrong advisory mapping and criticality status at VPM view.
IOJ-2190077	SVM agent deployment via Intune shows Failed status in Endpoint.
IOJ-2184148	Mark End Of Life for products without version rule. For more information, see article .
IOJ-2206211	Mark Adobe Fireworks CS6 status as End Of Life.
IOJ-2203198	Upgrade jQuery library to v3.6 to mitigate reported vulnerabilities.

Community Blogs

Please subscribe to latest news on Software Vulnerability Manager by going to <https://community.flexera.com/t5/Software-Vulnerability/bg-p/SoftwareVulnerabilityManagementblog> and clicking on 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 © 2021 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.