

Software Vulnerability Manager (Cloud Edition) Release Notes

December 2020

Introduction	1
New Features and Enhancements	2
Publish Patches to Microsoft Intune	2
Agent Caching of Scan Rules	3
Data API	3
Binary Versions Changed.....	3
Resolved Issues.....	4
Community Blogs	4
Product Feedback	4
Legal Information	5

Introduction

Flexera’s Software Vulnerability Manager (formerly called Software Vulnerability Manager 2019) is a vulnerability and patch management software solution that facilitates a customized patch management process. It combines vulnerability intelligence, vulnerability scanning, and patch creation with patch deployment tool Integration to enable targeted, reliable, and cost-efficient patch management.

Vulnerability and patch management are critical components of any security infrastructure because they enable proactive detection and remediation of vulnerabilities before they are actively exploited and your security compromised. With Software Vulnerability Manager, IT operations and security teams are empowered to prevent vulnerability threats from both Microsoft and non-Microsoft (third-party) product vulnerabilities, covering Microsoft Windows, macOS, and Red Hat Enterprise Linux.

Software Vulnerability Manager integrates seamlessly with Microsoft® WSUS and System Center Configuration Manager.

New Features and Enhancements

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

- [Publish Patches to Microsoft Intune](#)
- [Agent Caching of Scan Rules](#)
- [Data API](#)
- [Binary Versions Changed](#)



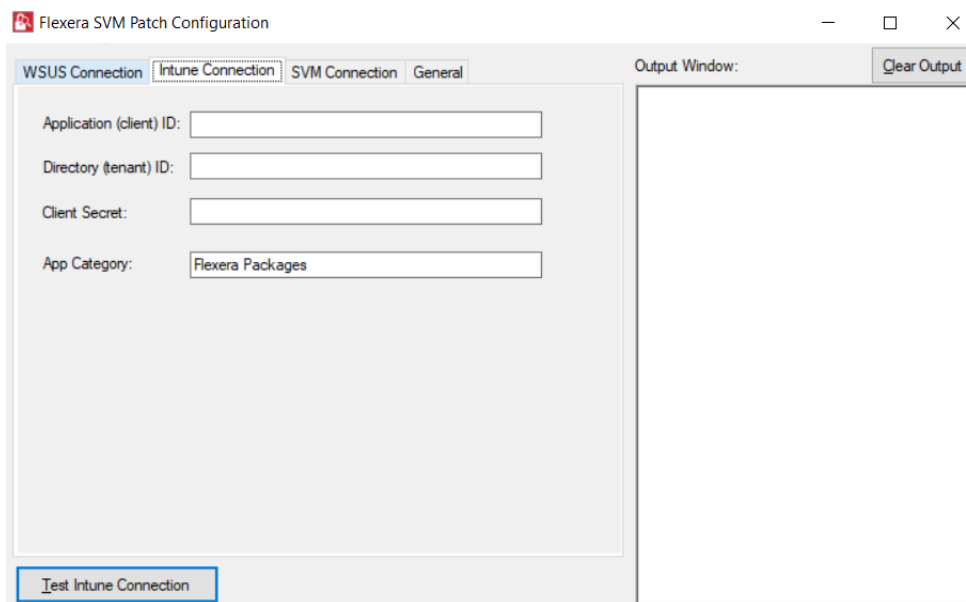
Note • To see the following new features and enhancements in your Software Vulnerability Manager (Cloud Edition) interface, you must refresh your browser's cache (press Ctrl+F5).

Publish Patches to Microsoft Intune

With this release, Software Vulnerability Manager (Cloud Edition) can now publish SPS/ VPM patches to Microsoft Intune.

This new capability requires a new version of patch daemon, released as a part of SVM Toolkit that can be downloaded at [SVMClientToolkitInstall.msi](#)

To publish patches to Intune, it will be necessary to configure patch daemon with valid Intune credentials and token.



The screenshot shows the 'Flexera SVM Patch Configuration' dialog box. It has four tabs: 'WSUS Connection', 'Intune Connection', 'SVM Connection', and 'General'. The 'Intune Connection' tab is selected. It contains four input fields: 'Application (client) ID:', 'Directory (tenant) ID:', 'Client Secret:', and 'App Category:'. The 'App Category' field has 'Flexera Packages' entered. To the right of the main configuration area is an 'Output Window' with a 'Clear Output' button. At the bottom left of the dialog is a 'Test Intune Connection' button.

Once this is setup, you can use either [Patch Automation](#) or ActiveX to publish SPS/ VPM patches to Intune.



Note • Patch daemon convert the patch to intunewin format before publishing.



Note • The Patch Daemon may be installed on any workstation or server. The prerequisites are:

- Windows 10 RSAT must be installed which can be obtained here <https://www.microsoft.com/en-us/download/details.aspx?id=45520>
- Windows 8.1 RSAT must be installed which can be obtained here <https://www.microsoft.com/en-us/download/details.aspx?id=39296&displaylang=en>
- Minimum version of .Net 4.7.2 must be installed.

Agent Caching of Scan Rules

New scan agents available with this release, will now cache scan rules. Agents servers will determine if the agent needs a new set of rules and will only push these rules if needed. This will result in decrease in the amount of network traffic generated by the scan agents which will be especially beneficial in very large environments. To take benefit of this enhancement, the current version of the scan agent in your environment should be upgraded to the new version of the agent - 7.6.0.15

Data API

With this release Software Vulnerability Manager (Cloud Edition) will support three new data APIs. These APIs have been provided to help download core set of assessment data that can be persisted in the local database. For more details on how to use these APIs, see [API Introduction](#).

The new Data APIs are as follows:

- **https://csi7.secunia.com/csi/api/?action=api&which=device&result_per_page=25&page=1**
This API provide details related to host and their last scanned date.
- **https://csi7.secunia.com/csi/api/?action=api&which=device_history&result_per_page=25&page=1**
This API provides summary security assessment data per host per date.
- **https://csi7.secunia.com/csi/api/?action=api&which=software_history&result_per_page=25&page=1**
This API provides security assessment data per host per date. The data will contain software products discovered on each host and their secure status for that day.

Binary Versions Changed

The following are the version of the binaries provided:

Binaries (ActiveX/Agent/Daemon) version: 7.6.0.15

Software Vulnerability Manager Client Toolkit: 4.0.XXX (download [SVM Client Toolkit](#)).

Resolved Issues

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

Issue	Description
IOJ-2160174	Fixed counts mismatch between row count and pagination count for Host Smart Groups.
IOJ-2149793	Fixed issue where scan agent was not scanning at a configured time in site configuration page.

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 © 2020 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.