

Software Vulnerability Manager (On-Premises Edition) Release Notes

December 2021

Introduction	1
New Features and Enhancements	2
Detect Log4j Vulnerable Files	2
SVM Patch Publisher	2
Assignment Group Support for VMWare Workspace ONE in SVM Patch Publisher.....	3
Windows Environment Variable Support for Scan Paths	3
New Settings for Java Assessment	4
Binary Versions Changed.....	4
Known Issues	5
Resolved Issues	5
Community Blogs	5
Product Feedback	5
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 (On-Premises Edition) includes the following new features and enhancements:

- [Detect Log4j Vulnerable Files](#)
- [SVM Patch Publisher](#)
- [Assignment Group Support for VMWare Workspace ONE in SVM Patch Publisher](#)
- [Windows Environment Variable Support for Scan Paths](#)
- [New Settings for Java Assessment](#)
- [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).

Detect Log4j Vulnerable Files

With this release, SVM adds enhancement to the host agent and the scanning logic to detect log4j files.

The **SVM Host Agent (v7.6.1.19)** now can detect the log4j jar files installed on a host machine. SVM will identify the version of the detected log4j file and categorize it as Secure, Insecure and EOL, to make you aware of vulnerable log4j versions in your environment.

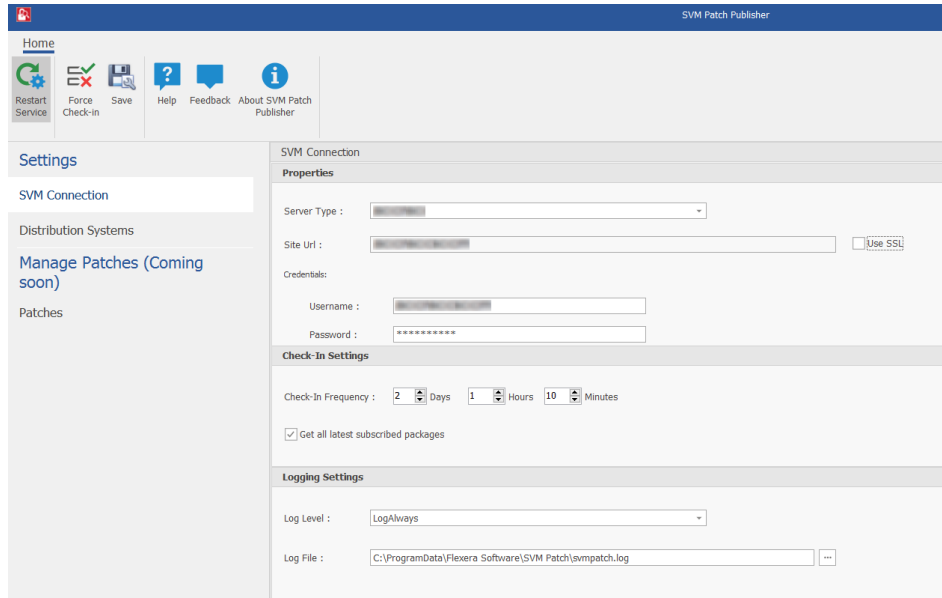
For more information, see [SVM December Update](#) release blog in our community.

SVM Patch Publisher

This release introduces a new tool - **SVM Patch Publisher**.

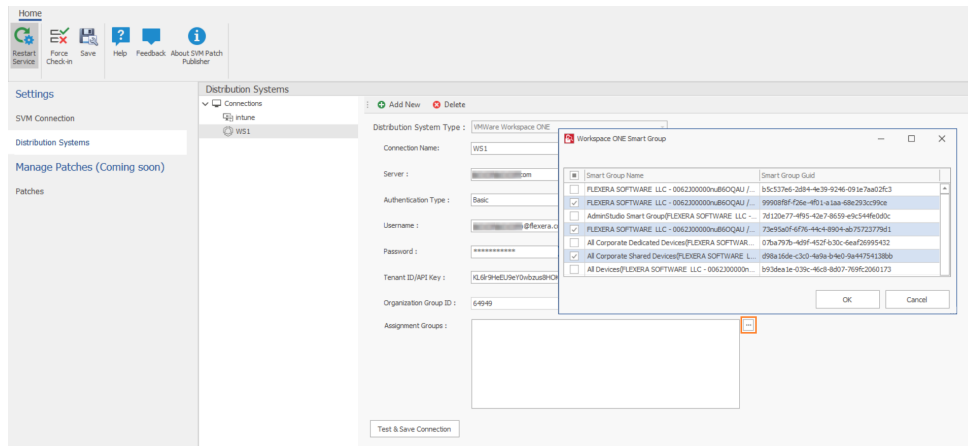
SVM Patch Publisher inherits its current functionalities from the **Patch Daemon**. **SVM Patch Publisher** enables you to configure connections to the SVM server and to the supported end point management systems. The tool polls SVM on a configured frequency to look for new patches resulting either from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

Upon installing the new tool, **SVM Patch Publisher** shortcut will be created on the desktop to launch the tool.



Assignment Group Support for VMWare Workspace ONE in SVM Patch Publisher

With this release, for Workspace ONE publishing, you can now choose a group or multiple groups and make assignments for end point deployments in the SVM Patch Publisher.

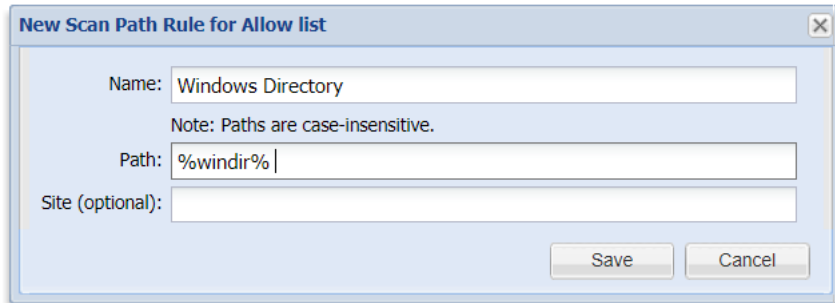


Windows Environment Variable Support for Scan Paths

You can now add environment variables to the Allow list and Block list in the Scan Paths view under Scanning menu. The environment variables will be resolved to the full path by the windows agent while scanning a host and will appropriately be either scanned or skipped.

For Example:

If **%windir%** is added to the Block list in the Scan Paths, then the agent will skip **C:\Windows** folder and its subfolders while scanning a host.



New Scan Path Rule for Allow list

Name: Windows Directory

Note: Paths are case-insensitive.

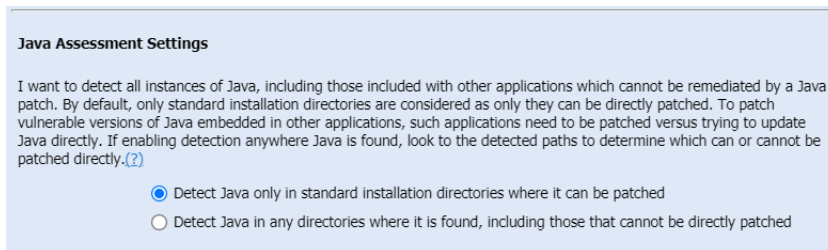
Path: %windir% |

Site (optional):

Save Cancel

New Settings for Java Assessment

A new setting for Java assessment is added to the **Settings** page under **Configuration** menu. This setting allows you to specify if you want to detect Java instances in the standard installation directories alone or in all the directories.



Java Assessment Settings

I want to detect all instances of Java, including those included with other applications which cannot be remediated by a Java patch. By default, only standard installation directories are considered as only they can be directly patched. To patch vulnerable versions of Java embedded in other applications, such applications need to be patched versus trying to update Java directly. If enabling detection anywhere Java is found, look to the detected paths to determine which can or cannot be patched directly.(?)

Detect Java only in standard installation directories where it can be patched

Detect Java in any directories where it is found, including those that cannot be directly patched

Binary Versions Changed

The following version of the binaries provided are:

- SVM ActiveX Plug-in v7.6.1.19
- Single Host Agent v7.6.1.19
- SVM Daemon v7.6.1.19
- SVM System Center Plugin v7.6.1.19
- SVM Patch Publisher v6.1.617 (to download, [click here](#))
- SVM On-Prem Client Toolkit v5.0.547 (to download, [click here](#))

Known Issues

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

Issue	Description
IOJ-2236858	Intune/ Workspace ONE customers upgrading to Patch Publisher 6.1.617 from Patch Daemon 5.0.547 or less needs to edit Patch Subscription to select the correct connection in Web interface.

Resolved Issues

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

Issue	Description
IOJ-2230820	Password expiration policies should not be enforced for SSO.
IOJ-2216881	VPM issue - incorrect product detected.
IOJ-2214678	Last Scan and Host column sorting in Smart Group is not working.

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.