

# Software Vulnerability Manager (On-Premises Edition) Release Notes

May 2021

<b>Introduction</b> .....	<b>1</b>
<b>New Features and Enhancements</b> .....	<b>2</b>
Publish Patches to VMware Workspace ONE.....	2
SPS/ VPM QuickPatch .....	3
Support for Service Provider Initiated Single Sign-On .....	3
Integrate Azure SSO with SVM .....	3
Activity Log for Failed Login Attempts.....	4
Other Enhancements/Improvements .....	4
Binary Versions Changed.....	5
<b>Known Issues</b> .....	<b>5</b>
<b>Resolved Issues</b> .....	<b>5</b>
<b>Community Blogs</b> .....	<b>6</b>
<b>Product Feedback</b> .....	<b>6</b>
<b>Legal Information</b> .....	<b>6</b>

## 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:

- [Publish Patches to VMware Workspace ONE](#)
- [SPS/VPM QuickPatch](#)
- [Support for Service Provider Initiated Single Sign-On](#)
- [Integrate Azure SSO with SVM](#)
- [Activity Log for Failed Login Attempts](#)
- [Other Enhancements/Improvements](#)
- [Binary Versions Changed](#)



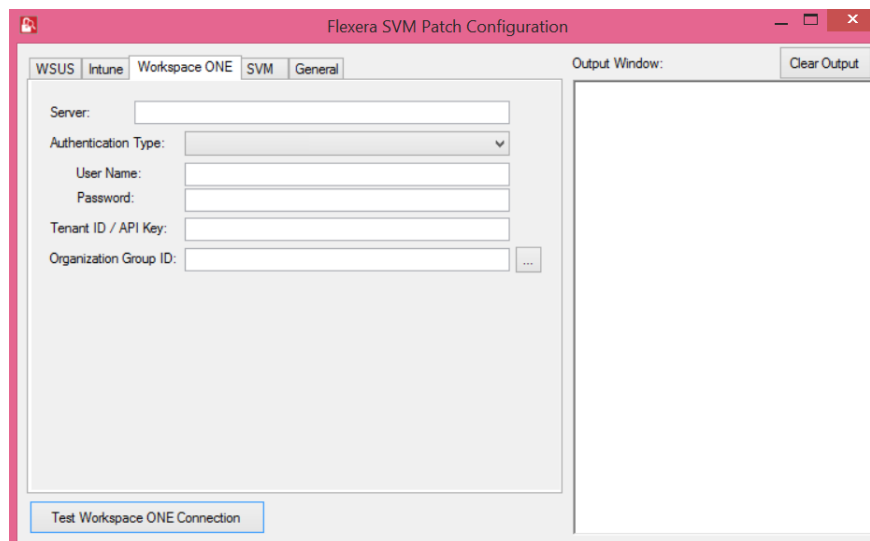
**Note** • To see the following new features and enhancements in your Software Vulnerability Manager (On-Premises Edition) interface, you must refresh your browser's cache (press Ctrl+F5).

## Publish Patches to VMware Workspace ONE

Software Vulnerability Manager can now publish SPS and VPM patches to VMware Workspace ONE.

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

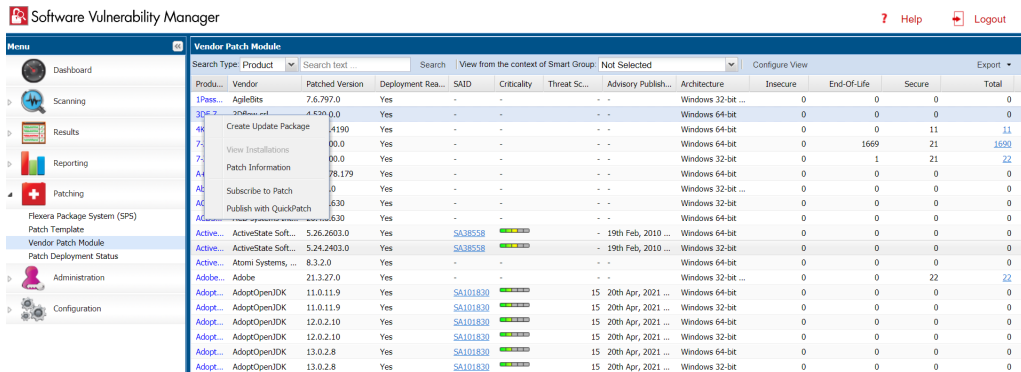
To publish patches to Workspace ONE, it will be necessary to configure patch daemon with valid Workspace ONE connection details.



Once the connection to Workspace ONE is configured, you can use either [Patch Automation](#) or Create Update Package wizard (ActiveX) to publish SPS and VPM patches to Workspace ONE.

# SPS/ VPM QuickPatch

This update of Software Vulnerability Manager introduces QuickPatch. This is a new and quick way for non-IE browsers to publish patches from SVM to an end-point management system with no dependency on ActiveX. QuickPatch publishes patches to end-point management system via Patch Daemon using defaults (no customizations).

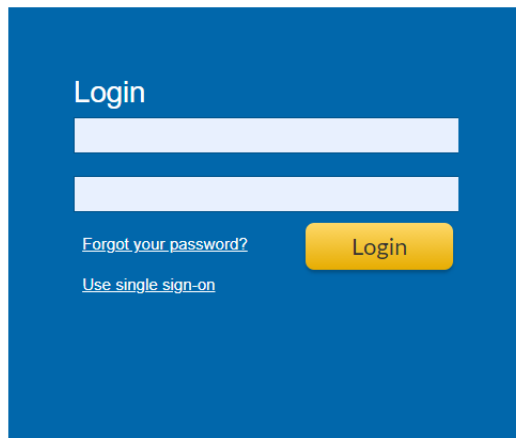


The screenshot shows the 'Vendor Patch Module' section of the Software Vulnerability Manager interface. It features a table with columns for Product, Vendor, Patched Version, Deployment Res., SAID, Criticality, Threat Sc., Advisory Publish..., Architecture, Insecure, End-Of-Life, Secure, and Total. The table lists various patches, including those for AgileBS, ActiveState Software, and AdoptOpenDK, with their respective versions and security metrics.

Product	Vendor	Patched Version	Deployment Res.	SAID	Criticality	Threat Sc.	Advisory Publish...	Architecture	Insecure	End-Of-Life	Secure	Total
1Pass...	AgileBS	7.6.797.0	Yes	-	-	-	-	Windows 32-bit ...	0	0	0	0
46	Create Update Package	4190	Yes	-	-	-	-	Windows 64-bit	0	0	11	11
71	View Installations	00.0	Yes	-	-	-	-	Windows 64-bit	0	1669	21	1690
71	Patch Information	00.0	Yes	-	-	-	-	Windows 32-bit	0	1	21	22
A4	Subscribe to Patch	78.179	Yes	-	-	-	-	Windows 64-bit	0	0	0	0
A6	Subscribe to Patch	0	Yes	-	-	-	-	Windows 32-bit ...	0	0	0	0
A6	Publish with QuickPatch	630	Yes	-	-	-	-	Windows 32-bit	0	0	0	0
A6	Publish with QuickPatch	630	Yes	-	-	-	-	Windows 64-bit	0	0	0	0
Active...	ActiveState Soft...	5.26.2603.0	Yes	SA38558	High	15	19th Feb, 2010 ...	Windows 64-bit	0	0	0	0
Active...	ActiveState Soft...	5.24.2403.0	Yes	SA38558	High	15	19th Feb, 2010 ...	Windows 32-bit	0	0	0	0
Active...	Atom Systems, ...	8.3.2.0	Yes	-	-	-	-	Windows 64-bit	0	0	0	0
Admin...	Adobe	21.3.27.0	Yes	-	-	-	-	Windows 32-bit ...	0	0	22	22
Adopt...	AdoptOpenDK	11.0.11.9	Yes	SA101830	High	15	20th Apr, 2021 ...	Windows 64-bit	0	0	0	0
Adopt...	AdoptOpenDK	11.0.11.9	Yes	SA101830	High	15	20th Apr, 2021 ...	Windows 32-bit	0	0	0	0
Adopt...	AdoptOpenDK	12.0.2.10	Yes	SA101830	High	15	20th Apr, 2021 ...	Windows 64-bit	0	0	0	0
Adopt...	AdoptOpenDK	12.0.2.10	Yes	SA101830	High	15	20th Apr, 2021 ...	Windows 32-bit	0	0	0	0
Adopt...	AdoptOpenDK	13.0.2.8	Yes	SA101830	High	15	20th Apr, 2021 ...	Windows 64-bit	0	0	0	0
Adopt...	AdoptOpenDK	13.0.2.8	Yes	SA101830	High	15	20th Apr, 2021 ...	Windows 32-bit	0	0	0	0

## Support for Service Provider Initiated Single Sign-On

Software Vulnerability Manager Cloud Edition can now initiate Single Sign-On via Identity Provider for authentication. You can click on Use single sign-on on the SVM login page and then provide your official email address to be automatically redirected to the configured Identity Provider to initiate login process.

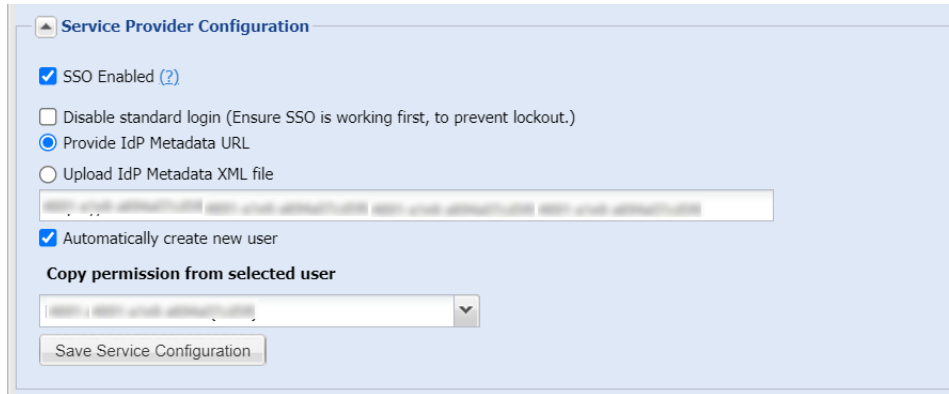


## Integrate Azure SSO with SVM

This feature will enable the users to authenticate with Identity Provider (IdP) like Azure within your organization.

To configure this feature go to **Configuration > Settings > Service Provider Configuration**.

**Single Sign-On** can be enabled from the **Configuration > Settings > Service Provider Configuration** page.



## Activity Log for Failed Login Attempts

All the failed login attempts will now be logged in the Activity Log.

Activity Name	Activity Status	User	Time	Activity Information	Host	Priority
User Login	Successful		11:44 5th May, 2021	Authentication by cached UID		High
User Login	Successful		11:44 5th May, 2021	Login (Software Vulnerability Manager)		Medium
User Login	Failed		11:43 5th May, 2021	Authentication by Password		High
User Login	Failed		11:43 5th May, 2021	Authentication by Password		High
User Logout	Successful		11:43 5th May, 2021	Logout (Software Vulnerability Manager)		Low
User Login	Successful		11:37 5th May, 2021	Authentication by cached UID		High
User Login	Successful		11:37 5th May, 2021	Login (Software Vulnerability Manager)		Medium
User Login	Successful		11:30 5th May, 2021	Login (Software Vulnerability Manager)		Medium
User Login	Successful		10:30 5th May, 2021	Login (Software Vulnerability Manager)		Medium
User Login	Successful		09:30 5th May, 2021	Login (Software Vulnerability Manager)		Medium
User Login	Successful		08:30 5th May, 2021	Login (Software Vulnerability Manager)		Medium
User Login	Successful		07:30 5th May, 2021	Login (Software Vulnerability Manager)		Medium
User Login	Successful		06:30 5th May, 2021	Login (Software Vulnerability Manager)		Medium
Report Sent	Successful		05:59 5th May, 2021	Report title: PDFCL_DaIReport - File Size : 0.45 MB		Medium
User Login	Successful		05:58 5th May, 2021	Authentication by cached UID		High
Report Sent	Successful		05:58 5th May, 2021	Report title: All Widgets - File Size : 143.41 MB		Medium
User Login	Successful		05:50 5th May, 2021	Authentication by cached UID		High
User Login	Successful		05:50 5th May, 2021	Login (Software Vulnerability Manager)		Medium
User Login	Successful		04:31 5th May, 2021	Login (Software Vulnerability Manager)		Medium
User Login	Successful		03:30 5th May, 2021	Login (Software Vulnerability Manager)		Medium

## Other Enhancements/Improvements

Following enhancements/improvements are added to SVM in this release:

- SVM-Intune Integration
  - SVM can now wrap multiple paths, used as detection rules for a package, into a single PowerShell Script and add it as a custom detection script, when a package is published to Microsoft Intune.
  - For few SVM packages, after the installation on an end point, the return code was not correctly sent back to Intune which resulted in incorrect deployment status of these packages in the Intune console. This issue is fixed now. Return code for all the packages are now sent back to Intune for accurate tracking of package deployment status.
- Patch Daemon
  - Clicking on Test SVM Connection button in the SVM Connection tab of Patch Daemon, to generate a new token, upon its expiration, required the Patch Daemon service to be restarted for the connection to be successful. Patch Daemon is now enhanced to be more robust to handle new tokens, without the need to restart the service.

## Binary Versions Changed

The following are the version of the binaries provided:

Binaries (ActiveX/Agent/Daemon) version: 7.6.1.15

Software Vulnerability Manager Client Toolkit: 5.0.XXX (download [SVM Client Toolkit](#)).

## Known Issues

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

Issue	Description
<b>IOJ-2191902</b>	Adobe Digital Editions 4.x showing wrong advisory mapping and criticality status in VPM view.
<b>IOJ-2177891</b>	<p>Some applications do not appear when not installed to their default location.</p> <ul style="list-style-type: none"><li>• 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. To avoid confusion and improper patching attempts, SVM intentionally scans for Java only in standard locations.</li><li>• If you would like to ensure known instances appear in scan results, you may choose to add a custom product in <b>Custom Scan Rules</b>.<ul style="list-style-type: none"><li>• Choose <b>Custom Scan Rules</b> from the <b>Filter Scan Results</b> node under the Scanning menu.</li><li>• Click <b>New Custom Scan Rule</b>.</li><li>• Enter the name and browse the file that you wish to have appear in scan results.</li></ul></li></ul>

## Resolved Issues

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

Issue	Description
<b>IOJ-2175914</b>	Error while publishing uninstall package using SVM Patch Daemon.

## 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.