Software Vulnerability Manager (Cloud Edition) Release Notes

August 2020

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:

- Single Sign-On (SSO)
- External package signing for Software Vulnerability Manager Client Toolkit
- 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).*

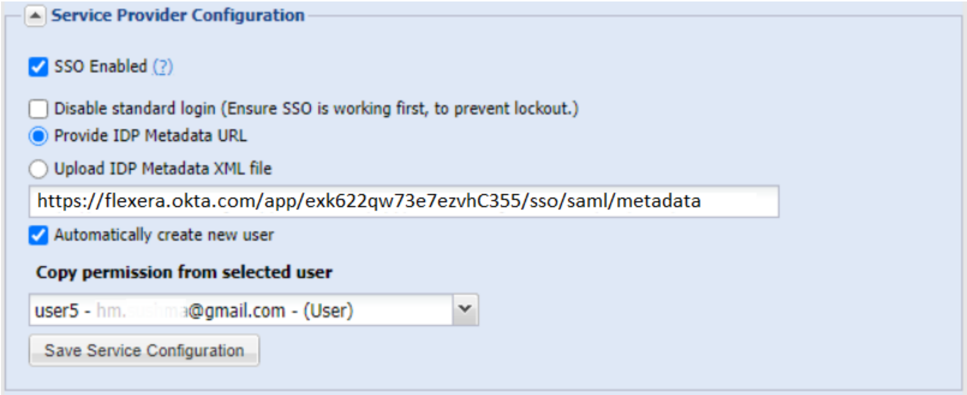
Single Sign-On (SSO)

With this release, Software Vulnerability Manager can now support Single Sign On (SAML2 protocol).

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

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

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



☑ SSO Enabled (?)

☐ Disable standard login (Ensure SSO is working first, to prevent lockout.)

● Provide IDP Metadata URL

○ Upload IDP Metadata XML file

https://flexera.okta.com/app/exk622qw73e7ezvhC355/sso/saml/metadata

☑ Automatically create new user

Copy permission from selected user

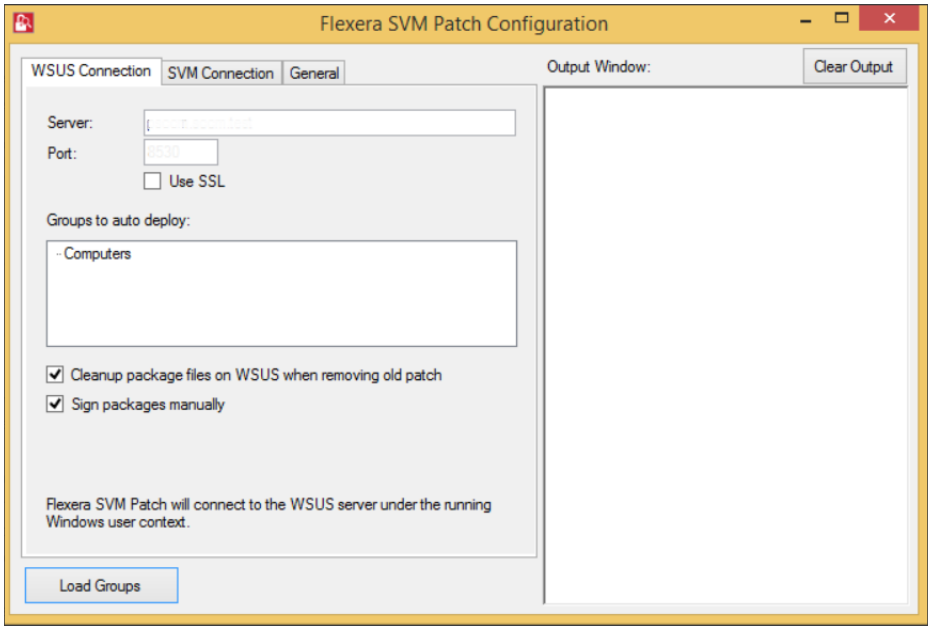
user5 - hm.[redacted]a@gmail.com - (User)

For more details, see Configure Single Sign-On (SSO).

External package signing for Software Vulnerability Manager Client Toolkit

Using Manual Signatures (also known as External Signatures) allows separating the privilege of Windows Server Update Services (WSUS) administration from the privilege to mark a package as trusted for deployment. With automatic signatures (typically, but not always, using a self-signed certificate), the WSUS administrator has full access to a digital certificate and private key that is trusted by all the machines within the organization. With Manual signatures, WSUS, and thus the WSUS administrator, does not require access to the private key.

In Patch daemon, select **Sign package manually** option.



Flexera SVM Patch Configuration

Server: pscom.scom.test
Port: 8530
□ Use SSL

Groups to auto deploy:

- Computers

☑ Cleanup package files on WSUS when removing old patch
☑ Sign packages manually

Flexera SVM Patch will connect to the WSUS server under the running Windows user context.

For detail on performing the Manual package Signing, see External package signing for Software Vulnerability Manager Client Toolkit.

Binary Versions Changed

The following are the new version of the binaries provided for this release:

Binaries (ActiveX/Agent/Daemon) version: 7.6.0.13

Software Vulnerability Manager Client Toolkit: 3.0.241 (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-2125934	Renamed White/Black List Feature to Allow list/Block list.

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

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.