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

- Single Sign-On (SSO)
- External Package Signing for Software Vulnerability Manager Client Toolkit
- Disable Report Options Based on Report Format
- Added CVSS Score to the CSV Reports
- Search Advisory by SAID
- Binary Versions

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).*

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 your organization.

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

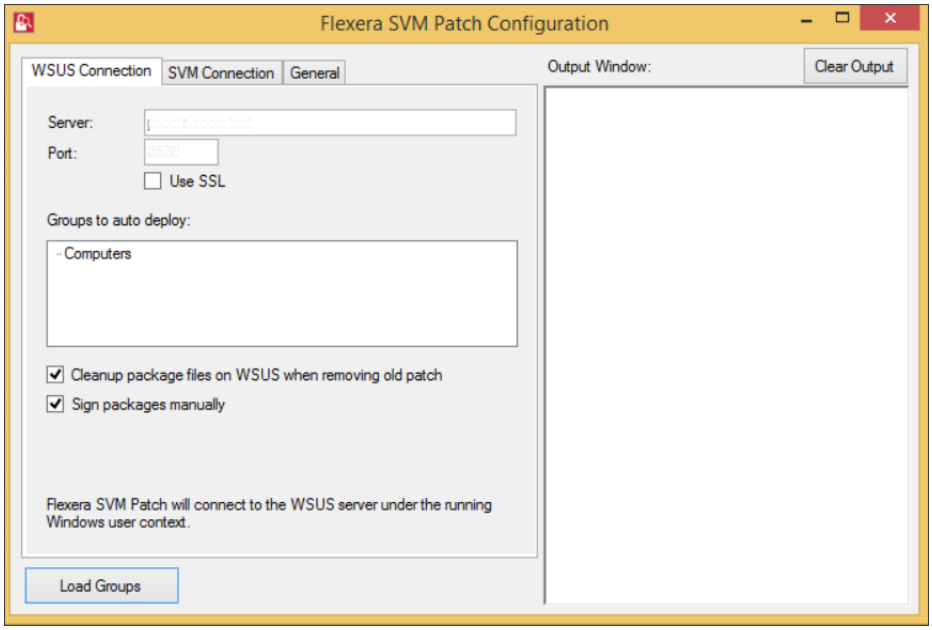
Single Sign-On can be enabled from the **Configuration > Settings** page.

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.

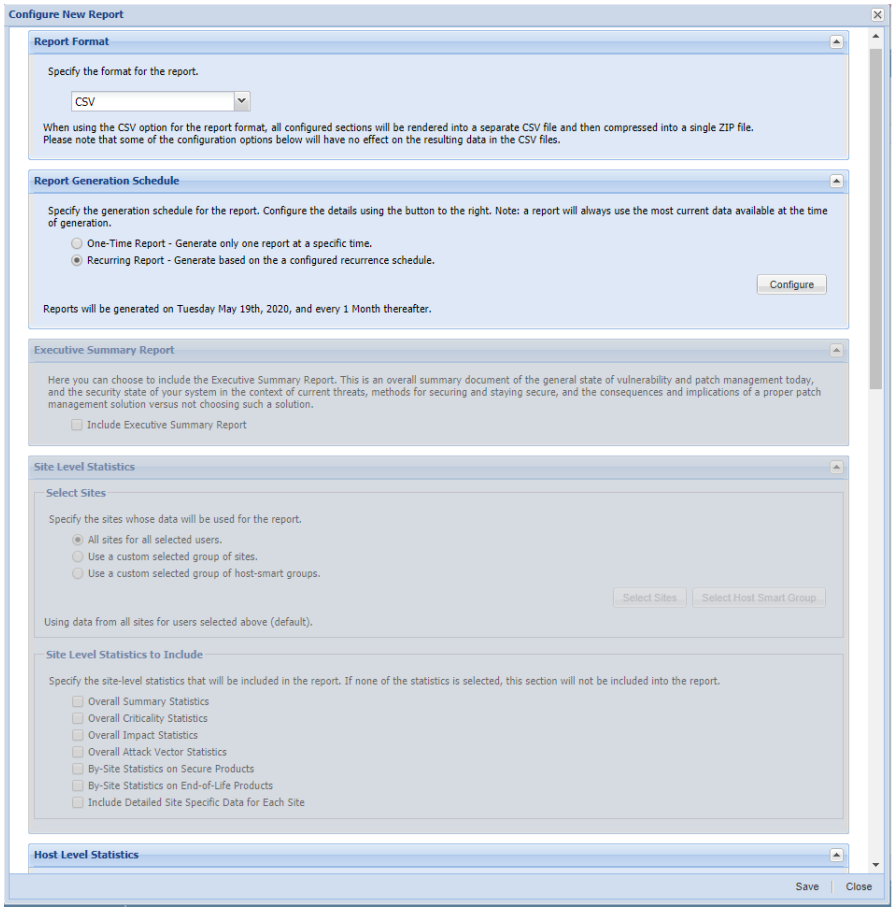
In Software Vulnerability Manager Client Toolkit, select **Sign package manually** option.



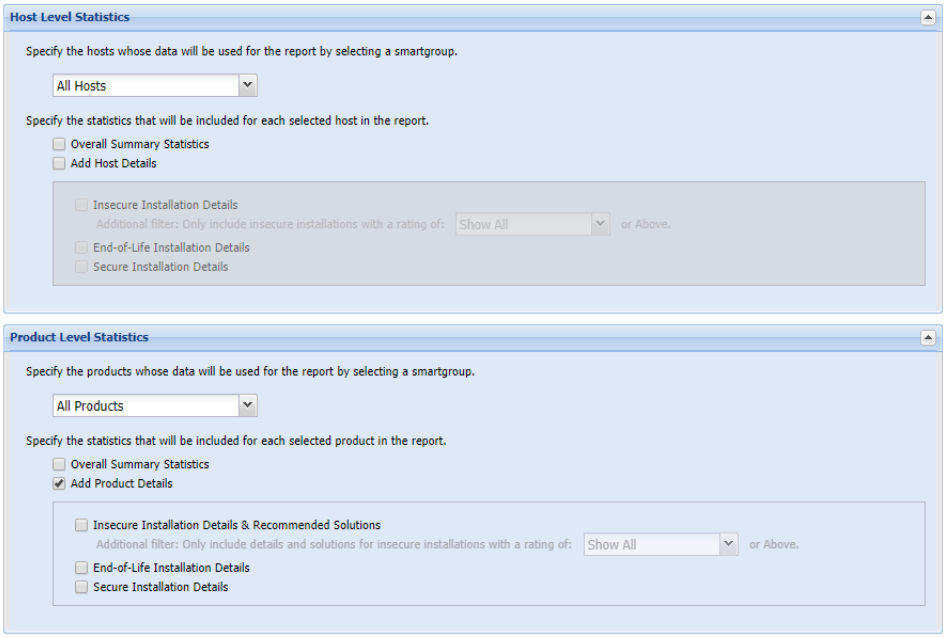
For detail on performing the Manual package Signing, see External package signing for Software Vulnerability Manager Client Toolkit.

Disable Report Options Based on Report Format

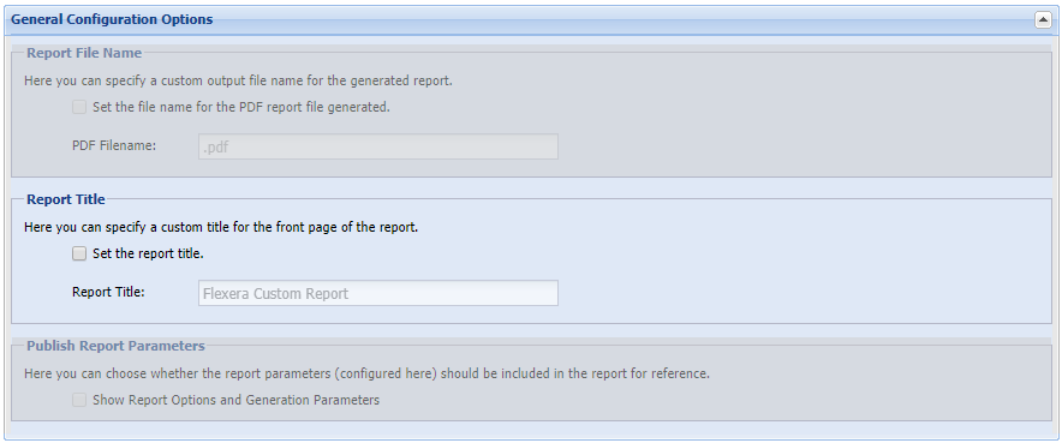
With this new enhancement, **Executive Summary Report**, **Site Level Statistics**, and **Overall Summary Statistics** check box for both **Host Level Statistics** and **Product Level Statistics** are disabled when you select report format as CSV.



Insecure Installation Details for both **Host Level Statistics** and **Product Level Statistics** are enabled only when you select **Add Product Details** and **Add Host Details** respectively.

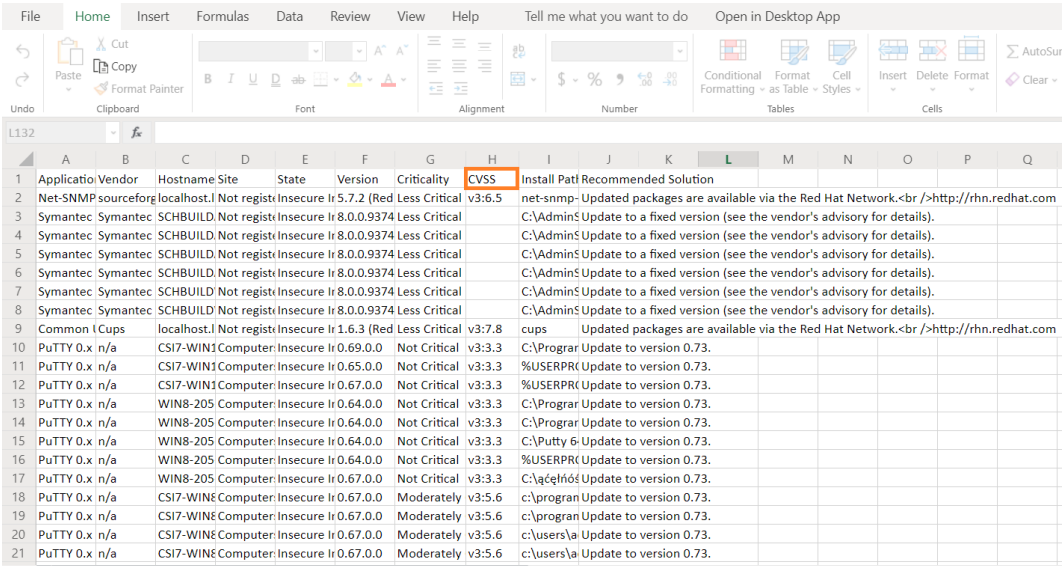


The **PDF Filename** tab and the **Publish Report Parameters** sections are disabled when you set **Report Format** to **CSV**.



Added CVSS Score to the CSV Reports

With this new enhancement, a new CVSS column has been added to the CSV Reports.



	A	B	C	D	E	F	G	H	I	J
1	Applicatio	Vendor	Hostname	Site	State	Version	Criticality	CVSS	Install Path	Recommended Solution
2	Net-SNMP	sourceforg	localhost.l	Not regist	Insecure Ir	5.7.2 (Red	Less Critical	v3:6.5	net-snmp-	Updated packages are available via the Red Hat Network. http://rhn.redhat.com
3	Symantec	Symantec	SCHBUILD	Not regist	Insecure Ir	8.0.0.9374	Less Critical		C:\Admin$	Update to a fixed version (see the vendor's advisory for details).
4	Symantec	Symantec	SCHBUILD	Not regist	Insecure Ir	8.0.0.9374	Less Critical		C:\Admin$	Update to a fixed version (see the vendor's advisory for details).
5	Symantec	Symantec	SCHBUILD	Not regist	Insecure Ir	8.0.0.9374	Less Critical		C:\Admin$	Update to a fixed version (see the vendor's advisory for details).
6	Symantec	Symantec	SCHBUILD	Not regist	Insecure Ir	8.0.0.9374	Less Critical		C:\Admin$	Update to a fixed version (see the vendor's advisory for details).
7	Symantec	Symantec	SCHBUILD	Not regist	Insecure Ir	8.0.0.9374	Less Critical		C:\Admin$	Update to a fixed version (see the vendor's advisory for details).
8	Symantec	Symantec	SCHBUILD	Not regist	Insecure Ir	8.0.0.9374	Less Critical		C:\Admin$	Update to a fixed version (see the vendor's advisory for details).
9	Common U	Cups	localhost.l	Not regist	Insecure Ir	1.6.3 (Red	Less Critical	v3:7.8	cups	Updated packages are available via the Red Hat Network. http://rhn.redhat.com
10	PuTTY 0.x	n/a	CSI7-WIN1	Computer	Insecure Ir	0.69.0.0	Not Critical	v3:3.3	C:\Prograr	Update to version 0.73.
11	PuTTY 0.x	n/a	CSI7-WIN1	Computer	Insecure Ir	0.65.0.0	Not Critical	v3:3.3	%USERPR(	Update to version 0.73.
12	PuTTY 0.x	n/a	CSI7-WIN1	Computer	Insecure Ir	0.67.0.0	Not Critical	v3:3.3	%USERPR(	Update to version 0.73.
13	PuTTY 0.x	n/a	WIN8-205	Computer	Insecure Ir	0.64.0.0	Not Critical	v3:3.3	C:\Prograr	Update to version 0.73.
14	PuTTY 0.x	n/a	WIN8-205	Computer	Insecure Ir	0.64.0.0	Not Critical	v3:3.3	C:\Prograr	Update to version 0.73.
15	PuTTY 0.x	n/a	WIN8-205	Computer	Insecure Ir	0.64.0.0	Not Critical	v3:3.3	C:\Putty 6	Update to version 0.73.
16	PuTTY 0.x	n/a	WIN8-205	Computer	Insecure Ir	0.64.0.0	Not Critical	v3:3.3	%USERPR(	Update to version 0.73.
17	PuTTY 0.x	n/a	WIN8-205	Computer	Insecure Ir	0.67.0.0	Not Critical	v3:3.3	C:\ąćęłńóś	Update to version 0.73.
18	PuTTY 0.x	n/a	CSI7-WIN8	Computer	Insecure Ir	0.67.0.0	Moderately	v3:5.6	c:\progran	Update to version 0.73.
19	PuTTY 0.x	n/a	CSI7-WIN8	Computer	Insecure Ir	0.67.0.0	Moderately	v3:5.6	c:\progran	Update to version 0.73.
20	PuTTY 0.x	n/a	CSI7-WIN8	Computer	Insecure Ir	0.67.0.0	Moderately	v3:5.6	c:\users\a	Update to version 0.73.
21	PuTTY 0.x	n/a	CSI7-WIN8	Computer	Insecure Ir	0.67.0.0	Moderately	v3:5.6	c:\users\a	Update to version 0.73.

Search Advisory by SAID

With this new enhancement, you can search Advisory either by **CVE**, **SAID**, or **Description**.

Binary Versions

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

Binaries version: 7.6.1.13

Resolved Issues

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

Issue	Description
IOJ-2125934	Renamed White/Black List Feature to Allow list/Block list.
IOJ-1865237	The smart group drop-down is removed for Criticality Overview - Threat Profile of Vulnerabilities dashboard.
IOJ-2129915	LDAPS password enhancement requests.

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.