Software Vulnerability Manager (Cloud Edition) Release Notes

June 2022

Introduction

Flexera's Software Vulnerability Manager is a software vulnerability and patch management solution that facilitates a customized patch management process. It combines vulnerability and threat intelligence, end point assessment, and patch creation and publishing enable an informed and rapid patch management.

Software Vulnerability Manager can assess software vulnerabilities for both Microsoft and non-Microsoft (third-party) product vulnerabilities covering Microsoft Windows, macOS, and Red Hat Enterprise Linux. The results of this assessment are connected to our vulnerability and threat intelligence to allow for effective prioritization. Finally, third party patches may be created and published to remediate endpoints using Microsoft® WSUS (often in conjunction with System Center Configuration Manager), via Microsoft® Intune or VMware® Workspace One.

New Features and Enhancements

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

- Enhanced SVM Patch Publisher
- Host Deletion Settings

- Improved Content of Smart Groups Notification
- Binary Versions

***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).*

Enhanced SVM Patch Publisher

SVM Patch Publisher is enhanced with the following new features:

- Create and Publish Flexera Package System (SPS) and Vendor Patch Module (VPM) Patches
- Support for BigFix Unified Endpoint Management System

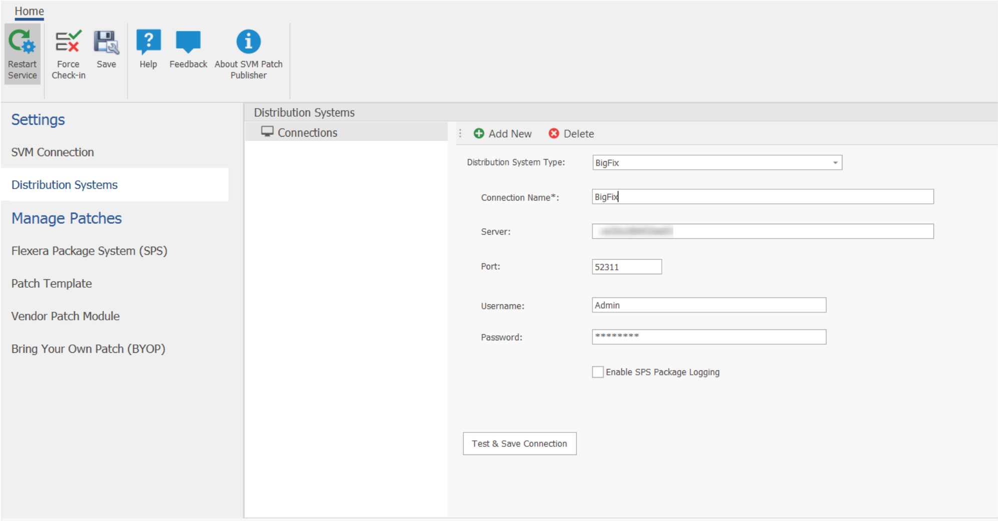
Create and Publish Flexera Package System (SPS) and Vendor Patch Module (VPM) Patches

The Manage Patches view is enabled in this update with the following menu:

- **Flexera Package System (SPS)—**View, create and publish SPS patches to the configured endpoint management systems like WSUS/ConfigMgr, Intune etc.
- **Patch Template—**View the templates created for patch automation.
- **Vendor Patch Module—**View, create and publish VPM patches to the configured endpoint management systems like WSUS/ConfigMgr, Intune etc.
- **Bring Your Own Patch (BYOP)—**Identify applications that not covered by SPS and VPM patch catalogs to bring your own patch.

Support for BigFix Unified Endpoint Management System

Configure and publish SPS and VPM patches to BigFix Unified Endpoint Management System.



Distribution System Type: BigFix

Connection Name*: BigFix

Server: [redacted]

Port: 52311

Username: Admin

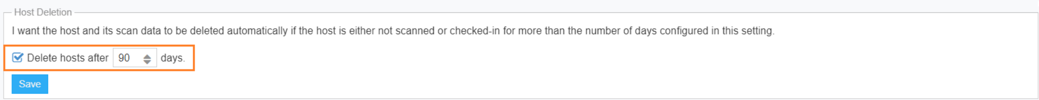
Password: ********

□ Enable SPS Package Logging

Once the connection to BigFix is configured, you can use either Patch Automation or ActiveX to publish SPS and VPM patches to the specified end point management system (BigFix).

Host Deletion Settings

A new setting to delete hosts and their scan data for which the last scanned/check-in time is greater than the specified number of days.


Host Deletion

I want the host and its scan data to be deleted automatically if the host is either not scanned or checked-in for more than the number of days configured in this setting.

☑ Delete hosts after 90 days.

Improved Content of Smart Groups Notification

With this update, you will see more detailed information in smart group notification email. If any advisory changes for advisory smart group, details such as creation date, criticality, CVSS score will be included in the email notification.

Binary Versions

The following version of the binaries provided are:

- SVM ActiveX Plug-in v7.6.0.19 (no change)
- Single Host Agent v7.6.0.19 (no change)
- SVM Daemon v7.6.0.19 (no change)
- SVM System Center Plugin v7.6.0.19 (no change)
- SVM Patch Publisher v7.0.727 (to download, click here)
- SVM Cloud Client Toolkit v5.0.561 (to download, click here) (no change)

This toolkit contains offline utilities such as the Multi-partition Reporting Tool, WSUS Management Tool and Client Data Tool which add value to SVM. This toolkit does not consist of Patch Daemon. This toolkit is for SVM Cloud edition only.

Patch Daemon will be deprecated in the future; therefore, you are encouraged to migrate to the new SVM Patch Publisher tool.

- SVM On-Prem Client Toolkit v5.0.547 (to download, click here) (no change)

  This toolkit contains Patch Daemon and offline utilities such as the Multi-partition Reporting Tool, WSUS Management Tool and Client Data Tool which add value to SVM.

Known Issues

The following table lists the known issues in Software Vulnerability Manager (Cloud Edition):

Issue	Description
IOK-704176	When connection to Intune is established for the first time with an App Category, publishing of SPS and VPM patches to this Intune connection will fail. Please follow the below steps for the workaround: ● Delete the configured App Category and save the Intune connection. ● Publish at least one patch to the Intune connection without App Category. ● Reconfigure the Intune connection with the App Category. Now all patch publishes to Intune should work.
IOK-706287	The selections made in the Configure View dialog will not be applied to Flexera Package System (SPS) view until the Patch Publisher is closed and relaunched.

Resolved Issues

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

Issue	Description
IOJ-2217368	Smart group notifications not working g for certain Advisory configuration.
IOJ-2250444	Enhanced Intune Assignment Groups to display all data in SVM Patch Publisher.
IOK-704747	Changed API “action=get_host_scan_info” from “POST” to “GET” to support PowerShell API. For more information, see List Scan Result for Each Host.

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 © 2022 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.