



Software Vulnerability Manager (On-Premises Edition)

User Guide

Legal Information

Book Name: Software Vulnerability Manager (On-Premises Edition) User Guide
Part Number: SVMOPPE-MARCH2020-UG00
Product Release Date: March 2020

Copyright Notice

Copyright © 2020 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.

Contents

- 1 Software Vulnerability Manager On-Premises Edition Help Library 9**
 - Product Support Resources 13**
 - Contact Us..... 14**
- 2 Introduction 15**
 - The Scan Process – How Does it Work? 15**
 - Software Vulnerability Manager Software Vulnerability Management Life Cycle 16**
 - System Requirements 17**
 - Permissions..... 18
 - Software Vulnerability Manager Console and WSUS Compatibility..... 18
 - Software Vulnerability Manager with Scanning and Patching Capabilities 20
 - System Architecture Overview 21**
- 3 Getting Started with Software Vulnerability Manager On-Premises Edition 23**
 - Install Your Software Vulnerability Manager On-Premises Edition Environment 23**
 - Opening a Support Case 24**
 - Download and Install the Software Vulnerability Manager Plug-in 24**
 - Download and Install the Software Vulnerability Manager Daemon 25**
 - Configuring SCCM to Report Windows Update Information 27**
 - Download and Install the Software Vulnerability Manager System Center Plug-in..... 29**
 - Download and Install the Software Vulnerability Manager Client ToolKit 29**
 - Flexera SVM Patch Configuration..... 31
 - Flexera WSUS Management Tool..... 34
 - [Patching Information 34](#)
 - [Configuration 37](#)
 - Join Flexera’s Customer Community 38**
- 4 The Dashboard 39**

5	Agent Administrative Privileges and Data Collection	41
	Agent Administrative Privileges	41
	Agent Data Collection	42
6	Scanning	45
	Agent-Based Scan – Requirements for Windows	46
	Agent-Based Scan – Requirements for Mac OS X	47
	Agent-Based Scan – Requirements for Red Hat Enterprise Linux (RHEL)	47
	Remote/Agent-less Scan – Requirements (Windows)	48
	Remote Scanning Via Software Vulnerability Manager (Agent-less Scan)	49
	Quick Scan	49
	Scan Groups	50
	Scan Progress	51
	System Center Inventory Import	51
	System Center Import Schedules (Requires the Software Vulnerability Manager Daemon)	53
	Remote Scanning Via Agents	53
	Software Vulnerability Manager Agent Command Line Options	54
	Help	54
	Version	54
	Install	54
	Install the Agent via SCCM	55
	Uninstall	56
	Modify Settings	57
	Controlling the Service	57
	Scanning from the Command Line	57
	Randomizing the Agent Scan Schedule	57
	Agent Configuration Options	58
	Network Appliance Agents	63
	Network Appliance Groups	63
	Download Network Agent	63
	Scanning Via Local Agents	64
	Scan Types	65
	Single Host Agents	65
	Download Local Agent	66
	Run Scan from System Center Configuration Manager (SCCM)	68
	Scanning Mac OS X	72
	Download the Software Vulnerability Manager Agent for Apple Mac OS X	72
	Prepare Your Mac	73
	Install the Mac Agent	74
	Scanning Red Hat Enterprise Linux (RHEL)	75
	Installing the Software Vulnerability Manager Agent for Red Hat Linux	75
	Filter Scan Results	76
	Scan Paths	76
	Custom Scan Rules	77

Completed Scans	77
7 Results	81
Sites	81
Smart Groups	81
Host Smart Groups	83
Overview and Configuration	83
Configured Host Smart Groups	84
Filter Host Smart Groups on missing Microsoft Knowledge Base (KB) articles	84
Product Smart Groups	86
Overview and Configuration	86
Last Scan Date for Product Smart Groups	86
Configured Product Smart Groups	87
Advisory Smart Groups	87
Overview and Configuration	88
View/Edit Smart Group Configuration	88
Configured Advisory Smart Groups	89
View All Advisories	89
8 Reporting	91
Report Configuration	91
Smart Group Notifications	93
Database Access	94
Database Console	94
Database Cleanup	95
Scheduled Exports	95
9 Patching	97
Flexera Package System (SPS)	97
Flexera SPS Page Features	98
Product display criteria for SPS	98
Language selection for SPS	99
Patch update searches by Common Vulnerabilities and Exposures (CVE)	99
Advisory Published date	100
SPS Concepts and Terminology	100
What does a SPS package consist of?	100
Applicability Rules	101
SPS Package	101
Execution Flow Script	102
Files	102
Creating a Patch with the Flexera Package System (SPS)	102
Create an Update Package	103
Create an Uninstall Package	103
Create a Custom Package	104

The SPS Package Creation Wizard	104
Step 1 of 4: Package Configuration	105
Step 2 of 4: Package Contents	106
Step 3 of 4: Applicability Criteria - Paths	107
Importing Bulk File Paths in the SPS Package Creation Wizard.	108
Step 4 of 4: Applicability Criteria - Rules	110
Vendor Patch Module	111
Vendor Patch Module Page Features	111
Product display criteria for Vendor Patch Module	112
Patch update searches by Common Vulnerabilities and Exposures	114
Advisory Published date in Vendor Patch Module	114
Threat Score in Vendor Patch Module	114
Creating a Patch with the Vendor Patch Module	115
Create an Update Package	115
View Installations	115
Patch Information	116
Package Creation Wizard in Vendor Patch Module	117
Step 1 of 4: Package Configuration	117
Step 2 of 4: Package Contents	118
Step 3 of 4: Applicability Criteria - Paths	119
Step 4 of 4: Applicability Criteria - Rules	120
Automating Patch Deployment	122
Subscribe to Package	122
Edit Subscription	124
Agent Deployment	124
Add Proxy Settings	125
WSUS/System Center	125
Available	126
Deployment	126
Creating the WSUS-CSI GPO Manually	127
Deploying the Update Package Using WSUS	131
Deploying the Update Package Using System Center	132
Patch Configuration	132
External Package Signing	132
WSUS/System Center	133
Step 1 – Connection Status	134
Step 2 - Certificate Status	135
Step 3 – Group Policy Status	137
Setting Up Clients to Access WSUS	138
Third-Party Integration	138
Create and Publish the Package	139
Patch Template	139
Patch Automation	144
10 Administration	149

Roles	149
User Management	151
Create a New Administrator	151
Create a New User	151
Active Directory (Requires the Software Vulnerability Manager Plug-in)	153
IP Access Management (Requires the Software Vulnerability Manager Plug-in)	153
Password Policy Configuration	154
11 Configuration	157
Settings	157
Scan Threads	158
Live Updates	158
Collect Network Information	158
Zombie File Settings	159
Check for Missing Microsoft Security Update Settings	159
Flexera Software Package System (SPS) Timestamp	159
Mask paths that show user names	160
Configure Agent's status polling	160
Default Recipient Settings	160
Windows Update Settings	161
Log Messages	162
Activity Log	162
Suggest Software	163
Security	163
Change Password	163
Password Recovery Settings	164
A Appendix A - Software Vulnerability Manager Partition Management	165
Introduction	165
Partition Management	165
Overview	166
Permissions	167
Host and User Licenses	167
Create a New Partition Administrator	167
Grant User Access to all Completed Scans and Single Host Agent Entries	169
B Appendix B - About Secunia Advisories	171
CVSS (Common Vulnerability Scoring System)	171
CVE References	172
Where (Attack Vector)	172
Criticality (Severity Rating)	172
Impact (Consequence)	173

C	Appendix C - CSV Export File Cross-References	175
	Host Smart Group	176
	Advisory Smart Group	176
	Product Smart Group	177
	Scan Result	177
	Completed Scan	178
	Scheduled Exports	178
	Single Host Agent	179
	Smart Group Notifications	179
	User Management	180
D	Appendix D - Threat Intelligence	181
	Evidence of Exploitation	182
	Criteria for the Threat Score Calculation	182
	Threat Score Calculation - Examples	183
	Threat Intelligence Data for Operations and Security	186
	Threat Score Locations	186
	Dashboard Threat Score	186
	Completed Scan Page Threat Score	187
	All Advisory Popup Threat Score	187
	All Installation Popup Threat Score	188
	Advisory Summary Threat Score	189
	Host Smart Group Threat Score	190
	Product Smart Group Threat Score	191
	Smart Group Criteria Threat Score	191
	All Advisory Threat Score	192
	All Advisory Smart Group Criteria Threat Score	192
	Zero Day Advisory Threat Score	193
	Flexera Package System (SPS) List Threat Score	194

Software Vulnerability Manager On-Premises Edition Help Library

Flexera's Software Vulnerability Manager 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 it enables 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, Mac OS, and Red Hat Enterprise Linux.

Software Vulnerability Manager integrates seamlessly with Microsoft WSUS and System Center Configuration Manager.

Table 1-1 • Software Vulnerability Manager On-Premises Edition Help Library

Topic	Content
Introduction	Provides an overview of Software Vulnerability Manager: <ul style="list-style-type: none">• The Scan Process – How Does it Work?• Software Vulnerability Manager Software Vulnerability Management Life Cycle• System Requirements

Table 1-1 • Software Vulnerability Manager On-Premises Edition Help Library (cont.)

Topic	Content
Getting Started with Software Vulnerability Manager On-Premises Edition	<p>Provides details of how to perform the following tasks:</p> <ul style="list-style-type: none"> ● Install Your Software Vulnerability Manager On-Premises Edition Environment ● Opening a Support Case ● Download and Install the Software Vulnerability Manager Plug-in ● Download and Install the Software Vulnerability Manager Daemon ● Configuring SCCM to Report Windows Update Information ● Download and Install the Software Vulnerability Manager System Center Plug-in ● Download and Install the Software Vulnerability Manager Client ToolKit ● Join Flexera's Customer Community
The Dashboard	<p>Provides an overview of your hosts with the help of various “portlets”. Portlets are a collection of components that graphically display key data and allow you to create profiles which can display a unique combination of portlets.</p>
Agent Administrative Privileges and Data Collection	<p>Provides details on the following:</p> <ul style="list-style-type: none"> ● Agent Administrative Privileges ● Agent Data Collection

Table 1-1 • Software Vulnerability Manager On-Premises Edition Help Library (cont.)

Topic	Content
Scanning	<p>Provides details on the following:</p> <ul style="list-style-type: none"> ● Agent-Based Scan – Requirements for Windows ● Agent-Based Scan – Requirements for Mac OS X ● Agent-Based Scan – Requirements for Red Hat Enterprise Linux (RHEL) ● Remote/Agent-less Scan – Requirements (Windows) ● Remote Scanning Via Software Vulnerability Manager (Agent-less Scan) ● System Center Inventory Import ● Remote Scanning Via Agents ● Software Vulnerability Manager Agent Command Line Options ● Network Appliance Agents ● Scanning Via Local Agents ● Run Scan from System Center Configuration Manager (SCCM) ● Scanning Mac OS X ● Scanning Red Hat Enterprise Linux (RHEL) ● Filter Scan Results ● Completed Scans
Results	<p>Provides details on the following:</p> <ul style="list-style-type: none"> ● Sites ● Smart Groups ● Host Smart Groups ● Product Smart Groups ● Advisory Smart Groups
Reporting	<p>Provides details on the following:</p> <ul style="list-style-type: none"> ● Report Configuration ● Smart Group Notifications ● Database Access ● Scheduled Exports

Table 1-1 • Software Vulnerability Manager On-Premises Edition Help Library (cont.)

Topic	Content
Patching	<p>Provides details on the following:</p> <ul style="list-style-type: none"> • Flexera Package System (SPS) • Creating a Patch with the Flexera Package System (SPS) • The SPS Package Creation Wizard • Vendor Patch Module • Agent Deployment • WSUS/System Center • Creating the WSUS-CSI GPO Manually • Deploying the Update Package Using WSUS • Deploying the Update Package Using System Center • Patch Configuration • Patch Template • Patch Automation
Administration	<p>Provides details on the following:</p> <ul style="list-style-type: none"> • Roles • User Management • Active Directory (Requires the Software Vulnerability Manager Plug-in) • IP Access Management (Requires the Software Vulnerability Manager Plug-in) • Password Policy Configuration
Configuration	<p>Provides details on the following:</p> <ul style="list-style-type: none"> • Settings • Log Messages • Activity Log • Suggest Software • Security
Appendix A - Software Vulnerability Manager Partition Management	<p>Provides an Introduction and details of Partition Management.</p>

Table 1-1 • Software Vulnerability Manager On-Premises Edition Help Library (cont.)

Topic	Content
Appendix B - About Secunia Advisories	Explains Secunia Advisory terminology for: <ul style="list-style-type: none"> ● CVSS (Common Vulnerability Scoring System) ● CVE References ● Where (Attack Vector) ● Criticality (Severity Rating) ● Impact (Consequence)
Appendix C - CSV Export File Cross-References	When you export data from the Software Vulnerability Manager user interface to a CSV file, some values may differ. Each data set in this appendix includes a cross-reference table to explain the different values between the user interface and CSV file.
Appendix D - Threat Intelligence	Threat Intelligence Module augments Software Vulnerability Manager's vulnerability intelligence with a Threat Score that provides the ultimate prioritization tool for your busy desktop operations teams. This module requires purchase by the user.

Product Support Resources

The following resources are available to assist you with using this product:

- [Flexera Product Documentation](#)
- [Flexera Community](#)
- [Flexera Learning Center](#)
- [Flexera Support](#)

Flexera Product Documentation

You can find documentation for all Flexera products on the [Flexera Product Documentation](#) site:

<https://docs.flexera.com>

Flexera Community

On the [Flexera Community](#) site, you can quickly find answers to your questions by searching content from other customers, product experts, and thought leaders. You can also post questions on discussion forums for experts to answer. For each of Flexera's product solutions, you can access forums, blog posts, and knowledge base articles.

<https://community.flexera.com>

Flexera Learning Center

Flexera offers a variety of training courses—both instructor-led and online—to help you understand how to quickly get the most out of your Flexera products. The Flexera Learning Center offers free, self-guided, online training classes. You can also choose to participate in structured classroom training delivered as public classes. You can find a complete list of both online content and public instructor-led training in the Learning Center.

<https://learn.flexera.com>

Flexera Support

For customers who have purchased a maintenance contract for their product(s), you can submit a support case or check the status of an existing case by making selections on the **Get Support** menu of the Flexera Community.

<https://community.flexera.com>

Contact Us

Flexera is headquartered in Itasca, Illinois, and has offices worldwide. To contact us or to learn more about our products, visit our website at:

<http://www.flexera.com>

You can also follow us on social media:

- [Twitter](#)
- [Facebook](#)
- [LinkedIn](#)
- [YouTube](#)
- [Instagram](#)

Introduction

This chapter introduces the following topics:

- [The Scan Process – How Does it Work?](#)
- [Software Vulnerability Manager Software Vulnerability Management Life Cycle](#)
- [System Requirements](#)
- [System Architecture Overview](#)

The Scan Process – How Does it Work?

The first step in scanning a system is to collect specific metadata from primarily .EXE, .DLL, and .OCX files on the system being scanned. Metadata is generic non-sensitive text strings embedded in the binary files from the vendors of the products. This data is collected and then sent to our Secure Data Processing Cloud where it is processed and parsed.

The data is then matched against our File Signatures, which are rules that match the raw metadata to an actual product installation.

Part of this matching process also results in an exact version being extracted from the metadata. This means that after the initial parsing Software Vulnerability Manager knows exactly which products are on the system and their exact version – a precise inventory of software on the system.

The inventory of software is then compared against the unique Secunia Advisory and Vulnerability Database, which contains the most accurate and current Vulnerability Intelligence available.

The result is a precise inventory of products, their versions, the security state of each, along with a direct reference to any corresponding Secunia Advisory detailing the exact vulnerabilities and their Secunia assessed criticality and impact.

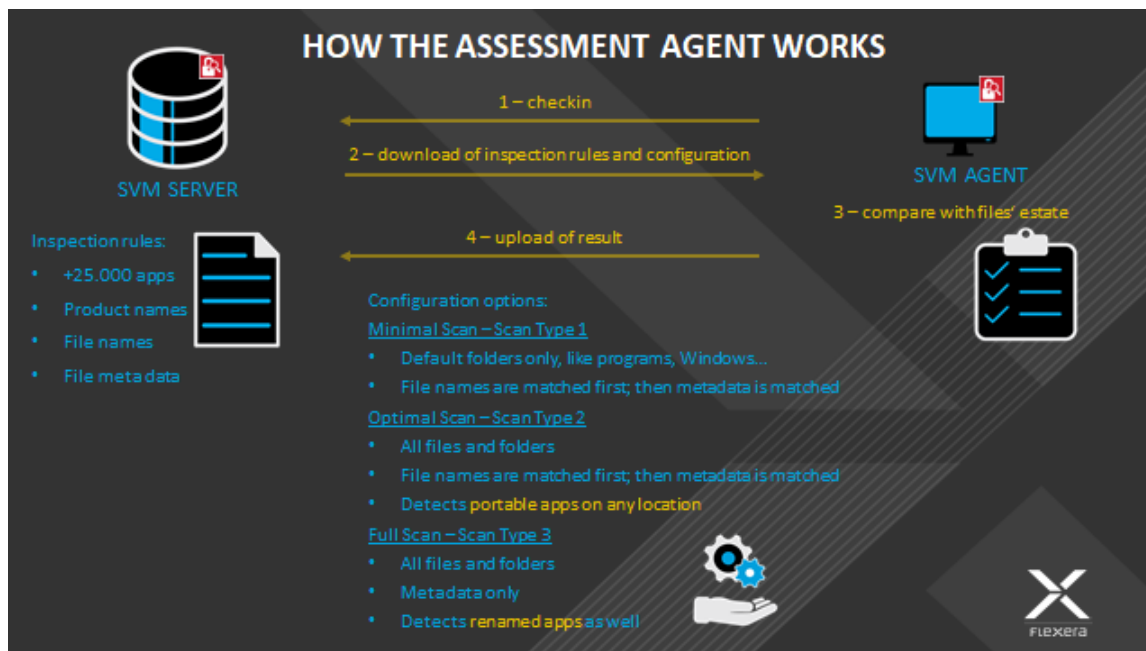
Since the scan process works by looking at the actual files on the system being scanned, the result is extremely reliable as a product cannot be installed on a system without the actual files required being present.

This in turn means that Software Vulnerability Manager rarely identifies false-positives and you can immediately use the results from Software Vulnerability Manager without doing additional data mining.

Software Vulnerability Manager is flexible and scalable when it comes to scanning a corporate network and you can choose to use Agent, Agent-less, or a combination of both scanning methods in the same environment.

For further information about the different Software Vulnerability Manager scanning approaches, see [Scanning](#).

The graphic below summarizes how the Software Vulnerability Manager Agent works and compares the three scan types.

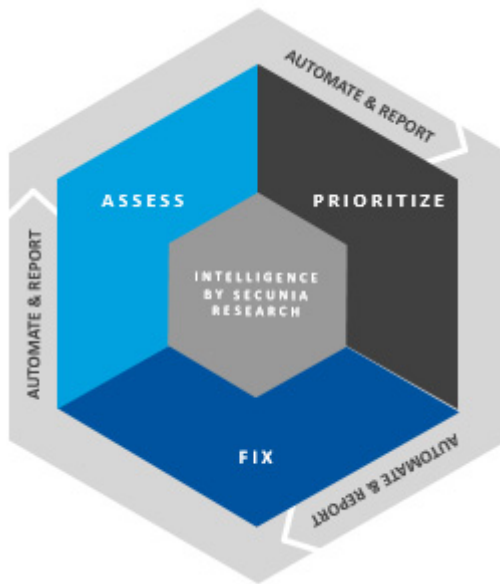


Software Vulnerability Manager Software Vulnerability Management Life Cycle

Software vulnerability management is a critical component of any security infrastructure because it enables proactive detection and remediation of security vulnerabilities.

A process to identify vulnerable products, including products not authorized in an organization's environment, paired with effective patch management is an absolute must to reduce the window of exposure and eliminate the root cause of a potential compromise.


Software Vulnerability Manager automates all steps of the software vulnerability management life cycle, allowing organizations to strengthen the security of their networks.



System Requirements

To use the Software Vulnerability Manager console, your system should meet the following requirements:

Table 2-1 • Software Vulnerability Manager (On-Premises Edition) System Requirements

Requirement	Description
Monitor Resolution	Minimum resolution of 1280 x 1024
Browser	Internet Explorer 11 or higher  Note • Scan results can also be viewed from other browsers.
Internet Connection	Internet connection capable of connecting to <code>http(s)://csi_server_name/</code> .
Sites to Whitelist	You are required to white-list the following sites: <ul style="list-style-type: none"> The <code>http(s)://csi_server_name/</code> should be white-listed in the Firewall/Proxy configuration. https://sync.secunia.com should be white-listed for SSL inspection as the CSI server doesn't trust the packages that are not signed by our server.
Cookie Settings	The following cookie settings are required: <ul style="list-style-type: none"> First-party cookie settings at least to prompt (in Internet Explorer) Allow session cookies
PDF	A PDF reader is required.

Before starting Software Vulnerability Manager, the following should also be present:

- [Permissions](#)
- [Software Vulnerability Manager Console and WSUS Compatibility](#)
- [Software Vulnerability Manager with Scanning and Patching Capabilities](#)

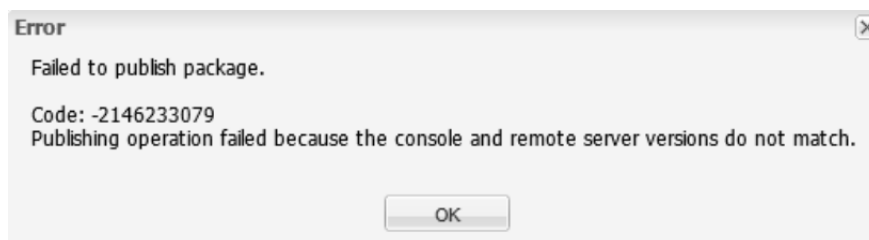
Permissions

The following permissions should be present:

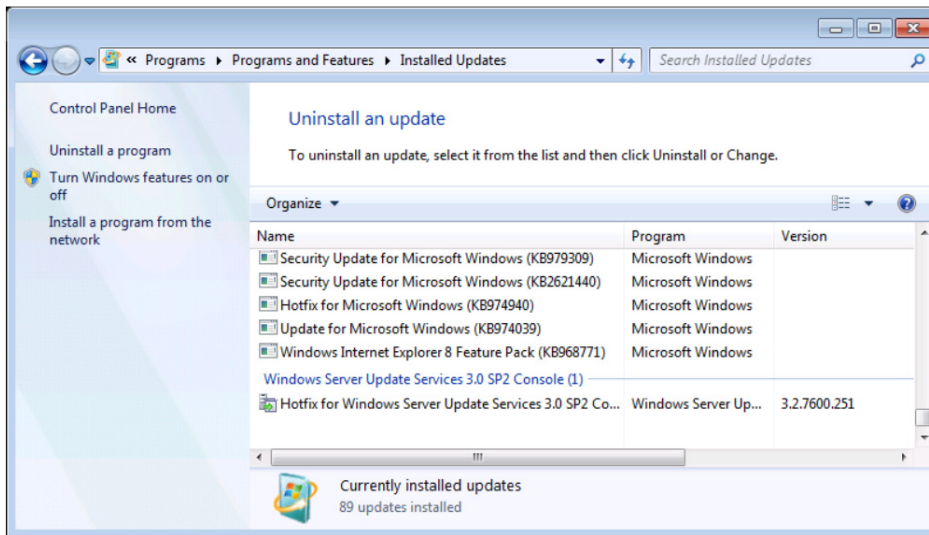
- Connect and Select permissions to the user (or service account) at the SQL Server Host of your System Center database. See [Download and Install the Software Vulnerability Manager Daemon](#).
- WSUS Administrator Group privileges (located locally on your WSUS Server)
- (Optional) Domain Administrator privileges for Group Policy Object creation - however the Group Policy Object can be created manually. This is a one-time configuration so the rights are not required on a permanent basis.

Software Vulnerability Manager Console and WSUS Compatibility

When the WSUS Server and Software Vulnerability Manager are installed on different machines, they must be on the same patch level for the WSUS Administrator Console API on the Software Vulnerability Manager console plug-in host to work. If they are not on the same patch level, the Software Vulnerability Manager console plug-in host will not publish packages to the WSUS server, and you will receive the following error message:



You should ensure that the same KB articles are installed on both the WSUS Sever and the Software Vulnerability Manager console plug-in host. To find the WSUS updates that have been installed, navigate to **Programs and Features (Add/Remove Programs)** in the bottom of the list of Installed Updates.



To ensure compatibility between the WSUS server and Software Vulnerability Manager, perform the following steps.



Task

To ensure compatibility between the WSUS Server and Software Vulnerability Manager:

1. Consider the Windows Server and WSUS version compatibility options:

Windows Server Version	WSUS Version
2008	3.0
2012	4.0
2012 R2	6.3 (9600.16384).
2016	4.0

2. The Software Vulnerability Manager plug-in host must be installed on an operating system that is able to run the appropriate version of the WSUS Administrative Console. The plug-in host uses WSUS API calls to publish patch updates. The API calls will not work unless the Software Vulnerability Manager plug-in host is on the same or similar version to the WSUS host. See the table below to ensure compatibility:

WSUS Version	Windows OS Version
3.0	7
4.0	8
6.3	8.1
4.0	10



Note • To ensure no version mismatch or OS version issues, directly install the Software Vulnerability Manager Console on the WSUS Server, which should already have the appropriate WSUS Administrative Console installed.

3. Install the Microsoft System Center 2012 Configuration Manager (SC2012) plug-ins on the same machine as follows:

Windows OS Version	Windows Server Version
7	2008
8	2012
8.1	2012 r2
10	2016

Software Vulnerability Manager with Scanning and Patching Capabilities

To successfully scan and create updates, the following should be present when using Software Vulnerability Manager.



Task

To scan and create updates:

1. Internet Explorer 11 or higher with Software Vulnerability Manager Plug-in installed (in order for Software Vulnerability Manager to connect to WSUS and to create packages successfully, Internet Explorer must be run as administrator in most cases - right-click and select **Run as administrator**).
2. In Internet Explorer **Tools > Internet options > Advanced**, ensure **Use TLS 1.1** and **Use TLS 1.2** are selected.
3. WSUS Administration Console matching your WSUS server's version.
4. Visual C++ Redistributable for Visual Studio 2012.
5. Microsoft .NET Framework runtime 4 or later.
6. If the WSUS Self-Signed Certificate is going to be used, and the user wishes to provision the certificate through the **Patching > WSUS/System Center > Deployment** function, Remote Registry service must be enabled on the clients.
7. Select the target hosts where the certificate is to be installed (CTRL+ mouse click for multiple selection), right-click and select **Verify and Install Certificate**.

Running Patching

To run patching on Windows 8.1 and Server 2012 R2, perform the following steps.



Task

To successfully run patching on Windows 8.1 and Server 2012 R2:

1. On the Windows Server machine, from the Server Manager, go to **Add Roles & Features > Features**.
2. Select the Appropriate Installation Type (Role-Based & Feature Based as opposed to Remote Desktop Services Installation).
3. Select the local server as the Destination Server for the installation.
4. Click **Next** to bypass the Server Roles menu and go to the Features menu.
5. Within the Features menu, scroll down the list and find the Remote Server Administration Tools (RSAT).

6. Expand the RSAT feature menu and locate the Role Administration Tools list of features.
7. Expand the list and find Windows Server Update Services Tools.
8. Enable this feature and all additional sub-features listed underneath it (API and PowerShell cmdlets and User Interface Management Console).
9. Proceed to the end of the Add Roles & Features Wizard by clicking **Next** and then **Install**.
10. Restart Windows and launch Software Vulnerability Manager from a web browser (for example Internet Explorer).

System Architecture Overview

The following screenshots provide a visual overview of the Software Vulnerability Manager system architecture.

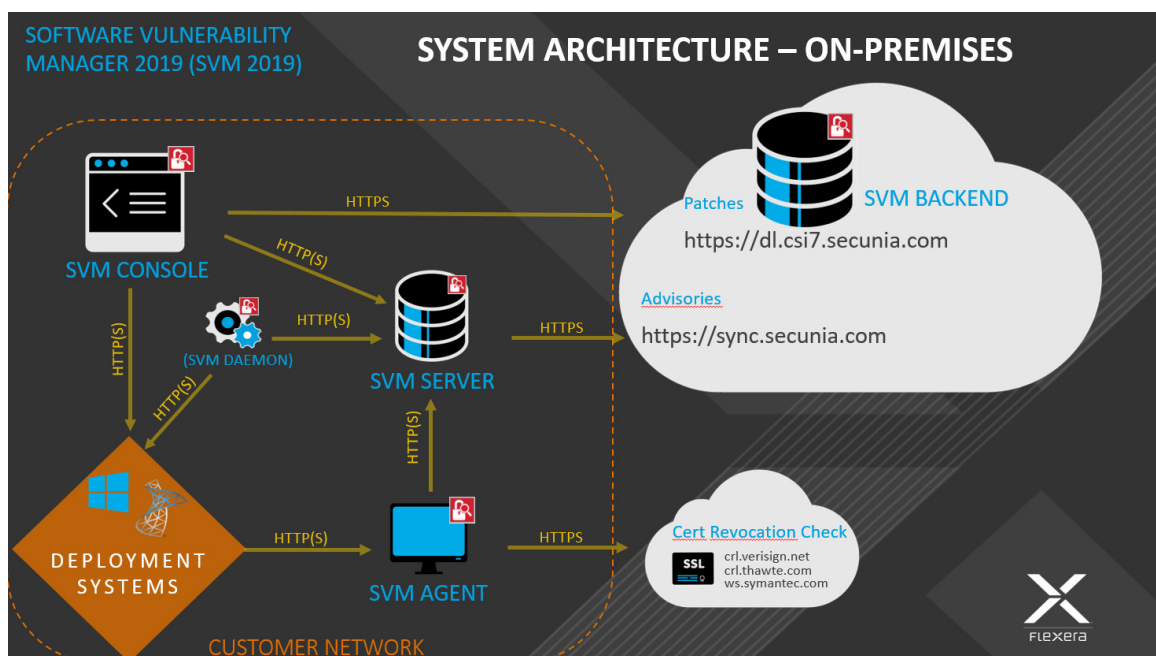


Figure 2-1: Software Vulnerability Manager System Architecture - On-Premises

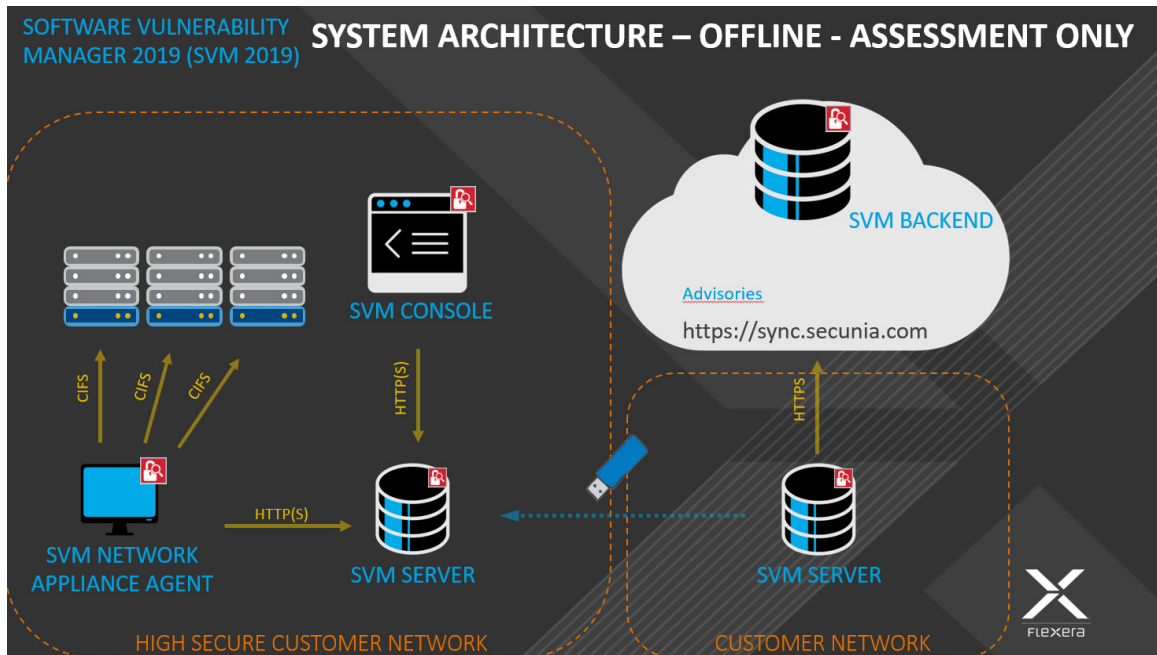


Figure 2-2: Software Vulnerability Manager System Architecture - Offline - Assessment Only

Getting Started with Software Vulnerability Manager On-Premises Edition

This section walks you through the steps for getting started with Software Vulnerability Manager On-Premises Edition:

- [Install Your Software Vulnerability Manager On-Premises Edition Environment](#)
- [Opening a Support Case](#)
- [Download and Install the Software Vulnerability Manager Plug-in](#)
- [Download and Install the Software Vulnerability Manager Daemon](#)
- [Configuring SCCM to Report Windows Update Information](#)
- [Download and Install the Software Vulnerability Manager System Center Plug-in](#)
- [Download and Install the Software Vulnerability Manager Client ToolKit](#)
- [Join Flexera's Customer Community](#)

Install Your Software Vulnerability Manager On-Premises Edition Environment



Task

To install your Software Vulnerability Manager On-Premises environment:

1. Open a support ticket with Flexera through our Customer Community at <https://community.flexera.com>.
2. Your support contact will then grant you access to download the RPM at <https://ca.secunia.com/download/>.
3. To login the first time to the Software Vulnerability Manager via `http(s)://csi_server_name/`, use the following user name and password:
 - **User name:** default
 - **Password:** flexera

4. Change your user name and password. The new password must contain a minimum of eight characters, or comply with the criteria defined in your custom [Password Policy Configuration](#).



Tip • Once you have changed your password, please set up your [Password Policy Configuration](#), so that you can recover the Root Admin password without having to open a support case to have the password reset.



Important • For security purposes, Software Vulnerability Manager has a session timeout that will log you off after 2 hours of inactivity.

Opening a Support Case

If you have any questions or concerns regarding your Software Vulnerability Manager On-Premises' account, please open a support case by logging in to our Customer Community at <https://community.flexera.com>, and then selecting **Get Support > Open New Case** from the menu at the top of the screen.



Note • You are required to login to the Flexera Community before the **Open New Case** option will be displayed.

Download and Install the Software Vulnerability Manager Plug-in

The first time you login to Software Vulnerability Manager, click the link on the bottom of the page and follow the on-screen instructions to download and install the Software Vulnerability Manager Plug-in to enable scanning and patching. Please note that the Plug-in is only compatible with Internet Explorer version 11 or higher.

Software Vulnerability Manager Plug-in is installed locally and must be installed on the machine you are running the Software Vulnerability Manager console from. Once the Software Vulnerability Manager Plug-in has been installed the download link is removed from the page.



Task

If Internet Explorer is blocking the ActiveX Plug-in, follow the steps below to allow it to load:

1. Open Internet Explorer's Internet options.
2. Go to the Security tab.
3. Select Trusted Sites.
4. Add your server's IP or hostname to the Trusted Sites.
5. Go back to the **Security** tab and click Custom level.
6. Scroll down to **Initialize and script ActiveX controls not marked as safe for scripting** and change the setting from **Disable** to Prompt or Enable.

Download and Install the Software Vulnerability Manager Daemon

The Software Vulnerability Manager Daemon is a stand-alone executable that executes various schedules configured in the Software Vulnerability Manager console. It runs as a background service with no user interaction. You can download the Daemon from `http(s)://csi_server_name/daemon`.

The Daemon integrates a number of local data sources in your network with the Flexera Cloud. It should be deployed to a node in the network that has high availability (for example, the server running the System Center or SQL server).

Once deployed, the Daemon will regularly scan the following data sources, based on the configuration created in Software Vulnerability Manager:

- Active Directory
- Microsoft System Center Configuration Manager (“System Center”) Imports
- Scheduled Exports
- WSUS State Change



Important • As the Daemon is connecting directly to the Flexera and System Center database servers unattended, Software Vulnerability Manager’s System Center Inventory Import page should be configured to include System Center SQL Host, SQL Port and SQL Database connection details prior to the installation of the Daemon to enable the latter to start executing unattended schedules correctly and on time.

To be able to pass authentication at the SQL server during an unattended scheduled Import, the Daemon has to be installed and configured with a user account that has been specifically assigned with Connect/Select permissions at the SQL Server Management Studio software prior to the installation of the Daemon.

When scheduled imports require it, the Daemon connects directly to the System Center database. This may block upgrades of System Center. Before upgrading System Center, make sure to stop the Daemon service, and start it again after the upgrade to System Center is complete.

The Daemon should only be deployed once to avoid two instances competing to retrieve the schedules.

The user or service account that runs the Daemon must have:

- Run-as Service privileges
- Write permission on the location where the exports should be placed and log file written for scheduled CSV file output and log file creation
- Member of local WSUS group “WSUS Administrators”
- LDAP query privileges
- SQL DataReader privileges
- System Center Configuration Manager Read only Analyst privileges

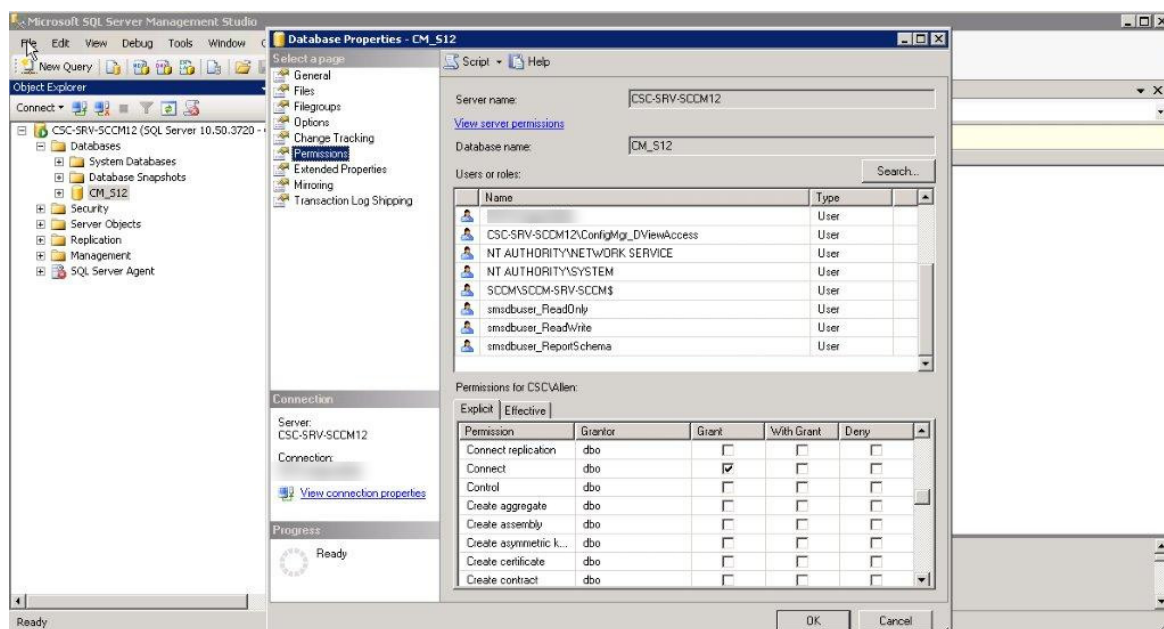
Assigning Connect and Select Permissions to the User

To assign Connect and Select permissions to the user (or service account) that will be used to run the Daemon service, perform the following steps.

**Task**

To assign Connect and Select permissions to the user (or service account) that will be used to run the Daemon service:

1. Open SQL Server Management Studio software at the SQL Server Host.
2. Expand Databases and find the name of your System Center database.
3. Right-click the database name and select Properties.
4. Enter the Permissions section from the left-hand side menu.
5. Find the account that will be used to install the Daemon and click on it.
6. While highlighted, review the Explicit permissions of the account below and find and select the Connect and Select check boxes.
7. Save the configuration and exit the SQL Server Management Studio.



Installing the Daemon

To install the Daemon, perform the following steps.



Important • To run the Daemon service successfully note the following:

- SVM Daemon does not require elevated permissions to run once the service has been setup, but it requires that the installation of it is performed by an account that is at least Local Administrator on the machine where the service is to be installed.
- The Daemon's service account must not be restricted by a GPO configuration the ability to logon to the server selected for installation of the Daemon. Such domain policy will prevent the Daemon to run as a service and would therefore prevent it to perform intended functionality.



Task

To install the Daemon:

1. Double-click the Daemon installer icon and follow the wizard instructions.
2. Accept the End User License Agreement and click Next.
3. Enter the Daemon Proxy Settings (host name, port, user name and password), if required. The values in populated fields are fetched from the current user's Internet Explorer proxy settings. Click Next.
4. Enter the User Name and Password of your Software Vulnerability Manager account and click Install.



Important • The Daemon executes scheduled tasks configured in Software Vulnerability Manager. Therefore, the Software Vulnerability Manager user account used during the Daemon installation must be the same one that set up the scheduled tasks in Software Vulnerability Manager. It can be a user account or an administrator account in Software Vulnerability Manager.

5. Enter the credentials for the user account (or service account) that was setup beforehand to grant access for the Daemon to the SQL Server Host. The user name must be entered in the <username>@<AD domain> format. Click Next.
6. Click Finish to close the Daemon setup.

For reference, the Daemon now outputs reports to a user-configured path. This path is set when the Daemon is installed and there is a page in the installer to configure the path. The file created at that path gets the data and time appended to its name, so for example, if the user sets the name to all_hosts.csv in Software Vulnerability Manager, then the resulting file will actually be named all_hosts_2016-03-10_13-00_01.csv, or whatever the date and time were when the file was created.

Also note that, from Daemon version 2.0.0.6 onwards, if the user leaves the path empty when installing the Daemon, then exporting reports won't work at all. To fix this later, the user will have to reinstall the Daemon and set the path in the installer.

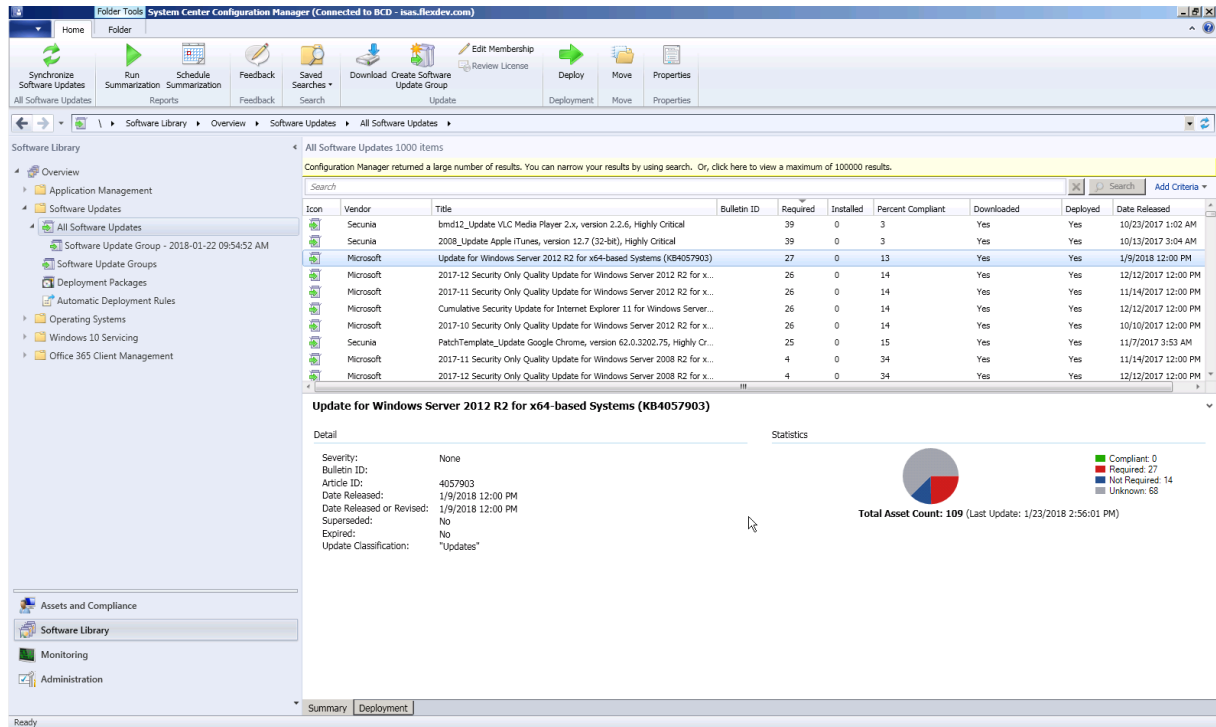
The Daemon uses the System Center SQL Database Settings that are specified in the Configure dialog. If those settings haven't yet been specified when the Daemon has been run then it will check for them again in 10 minutes and every 10 minutes afterwards until it gets them.

The Daemon checks with Flexera every 10 minutes to download new schedules or fetch changes to existing schedules as long as it is not in the process of processing scans and the results are displayed in the Software Vulnerability Manager [Completed Scans](#) page.

Configuring SCCM to Report Windows Update Information

If you are using System Center Configuration Manager (SCCM) to push Windows updates pulled from Windows Server Update Services (WSUS), make sure you DO NOT configure the Specify Intranet MS Update Location (GPO).

You will know Windows updates are being pulled by looking here in SCCM:



You want to make sure that the Windows updates have the following results:

- “Yes” is displayed in the **Download** column.
- “Yes” is displayed in the **Deployed** column.
- The pie chart shows that some machines require the Windows update.

To verify the SCCM database has the Windows updates you need, run this query:

```
SELECT v_Update_ComplianceStatusAll.ResourceID, Client_Version0, Distinguished_Name0, Name0,
Netbios_Name0, BulletinID, ArticleID, Title
FROM v_r_system
inner join v_Update_ComplianceStatusAll ON
v_Update_ComplianceStatusAll.ResourceID=v_r_system.resourceid
inner join v_UpdateInfo ON v_UpdateInfo.CI_ID=v_Update_ComplianceStatusAll.CI_ID
AND v_Update_ComplianceStatusAll.Status IN (2, 3)
```

You should then get the following result:

	ResourceID	Client_Version0	Distinguished_Name0	Name0	Netbios_Name0	BulletinID	ArticleID	Title
1	16777333	5.00.8498.1008	CN=SVM-ISAS-WIN7,CN=Comp...	SVM-ISAS-WIN7	SVM-ISAS-WIN7			Update Foxit Reader 7.x, version 8.x, Highly Critical
2	16777337	5.00.8498.1008	CN=SVM-ISAS-WIN10,CN=Com...	SVM-ISAS-WIN10	SVM-ISAS-WIN10		3125217	Update for Windows 10 for x64-based Systems (KB3125217)
3	16777337	5.00.8498.1008	CN=SVM-ISAS-WIN10,CN=Com...	SVM-ISAS-WIN10	SVM-ISAS-WIN10		3173427	Update for Windows 10 for x64-based Systems (KB3173427)
4	16777333	5.00.8498.1008	CN=SVM-ISAS-WIN7,CN=Comp...	SVM-ISAS-WIN7	SVM-ISAS-WIN7			Update 7-zip, version 16.x, Highly Critical
5	16777333	5.00.8498.1008	CN=SVM-ISAS-WIN7,CN=Comp...	SVM-ISAS-WIN7	SVM-ISAS-WIN7			2008R2_Update Oracle Java JDK 1.7.x / 7.x, version 8.x, Highly Critical

Download and Install the Software Vulnerability Manager System Center Plug-in

The System Center Plug-in should be installed on the same machine that the System Center Configuration Manager console is installed. You can use the Plug-in on the System Center Configuration Manager Server or on a client machine where the console is installed.

Download the installer from `http(s)://csi_server_name/sc2012/x64`.

Double-click the installer icon and follow the wizard instructions.

Launch the System Center Configuration Manager console. The Plug-in can be found under the Software Library > Flexera Software folder.

Login with your Software Vulnerability Manager Account credentials (User name/Password).

Your machine should have access to `http(s)://csi_server_name/`.

Download and Install the Software Vulnerability Manager Client ToolKit

To ease patch automation and WSUS management you must download and install **Software Vulnerability Manager Client ToolKit**. To download this tool kit, [click here](#).

On successful installation of Software Vulnerability Manager Client ToolKit, below tools will get installed and their respective shortcuts will be created in your desktop.

- [Flexera SVM Patch Configuration](#)
- [Flexera WSUS Management Tool](#)



Important • You must install **Software Vulnerability Manager Patch Client ToolKit** to utilize the Vendor Patch Module - Automation, see [Automating Patch Deployment](#).

Prerequisites

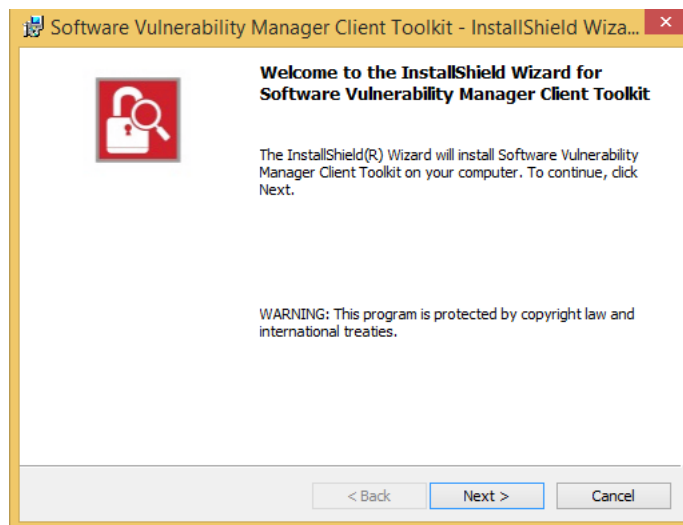
The below prerequisites are required:

- .Net Framework 4.6.1 or above.
- OS Requirements:
 - Install Software Vulnerability Manager Client ToolKit in Windows Server 2012 or Windows 8, for Windows 2012 WSUS.
 - Install Software Vulnerability Manager Client ToolKit in Windows Server 2016 or Windows 10, for Windows 2016 WSUS.
- Install both the Software Vulnerability Manager Client ToolKit and WSUS in the same domain.

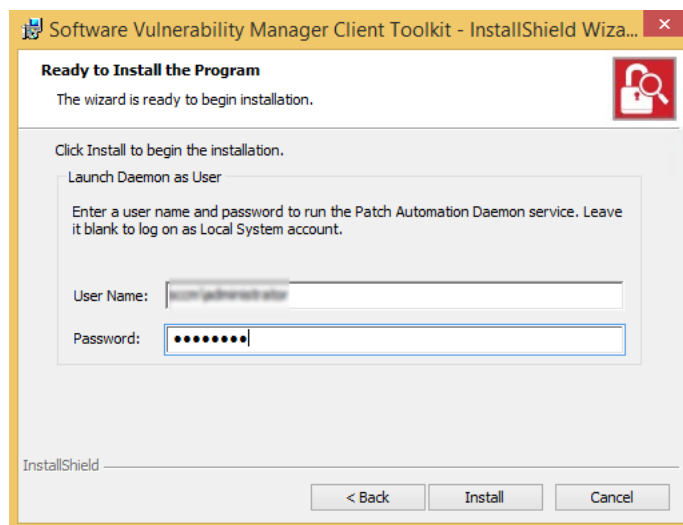
**Task**

To download and install the tool kit follow the below steps

1. Download the Software Vulnerability Manager Patch Configuration Tool from the [SVM Tool Kit](#). Save it in your desired folder path.
2. Double click the set up file, welcome wizard appears. Click **Next**.



3. You will be prompted to enter your system credentials. Click **Install**.



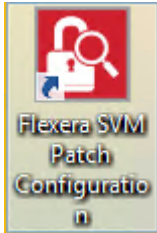
Tip • On successful installation, one shortcut for **Flexera Software Vulnerability Manager Patch Configuration** and one shortcut for **Flexera WSUS Management Tool** will get created in your desktop.

4. On successful installation, click Finish. **Flexera SVM Patch Configuration** windows pane appears, see [Flexera SVM Patch Configuration](#).

Flexera SVM Patch Configuration

Flexera Software Vulnerability Manager Patch Configuration integrates Software Vulnerability Manager application with the configured WSUS server to achieve the automation for subscribed packages.

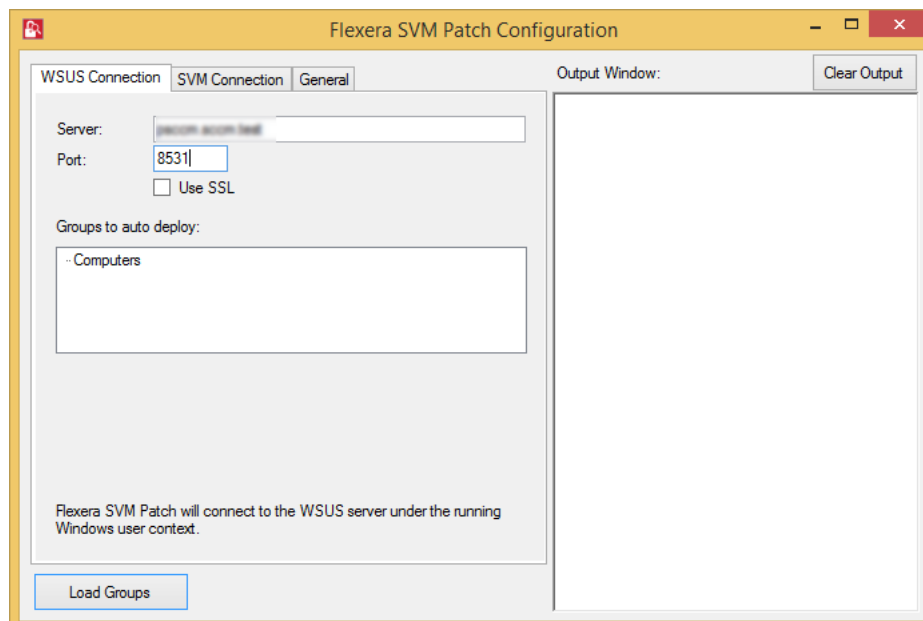
On successful installation of Software Vulnerability Manager Client ToolKit, a shortcut with a name **Flexera SVM Patch Configuration** will get created.



Task

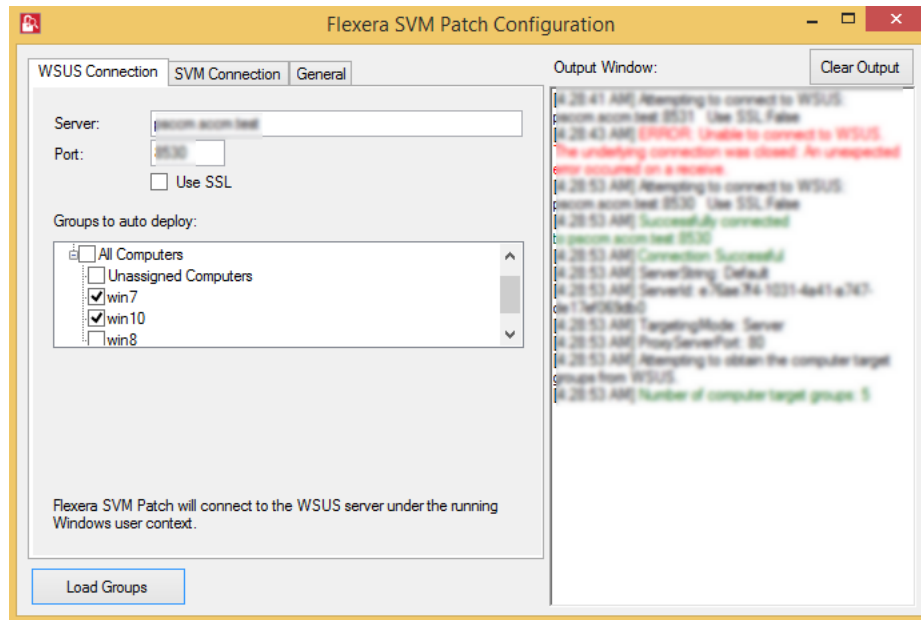
To use Flexera Software Vulnerability Manager Patch Configuration follow the below steps:

1. Double click on the shortcut created on your desktop, **Flexera SVM Patch Configuration** windows pane appears.
2. It consist of three tabs:
 - WSUS Connection tab
 - SVM Connection tab
 - General tab

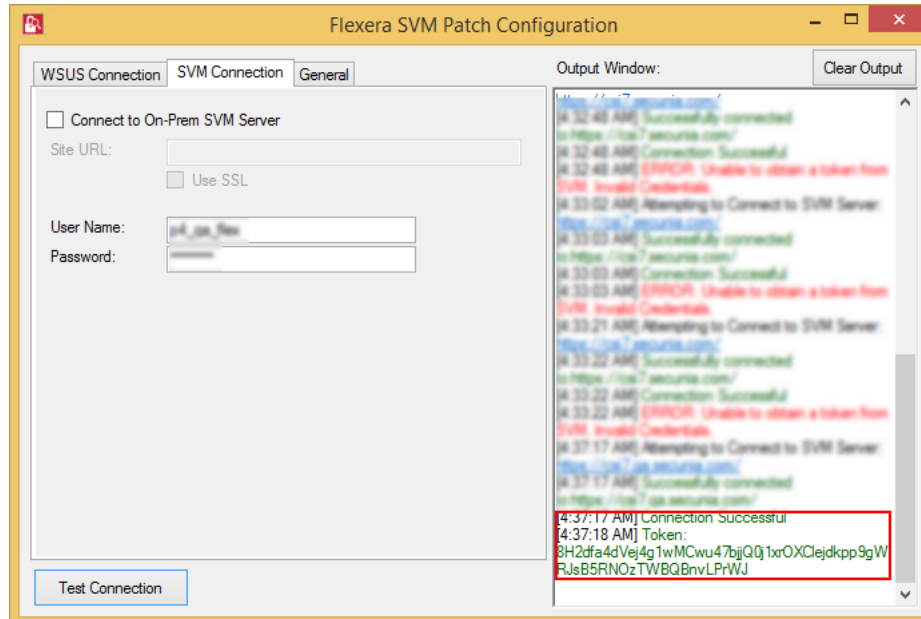


3. In **WSUS Connection** tab, enter the WSUS server details and the port number, click **Load Groups**.
4. In **Groups to auto deploy**, you can see the list of computer groups configured in WSUS Server.

5. Select the computer groups which you wanted to deploy the packages. To know more about a package publishing, see [Automating Patch Deployment](#).

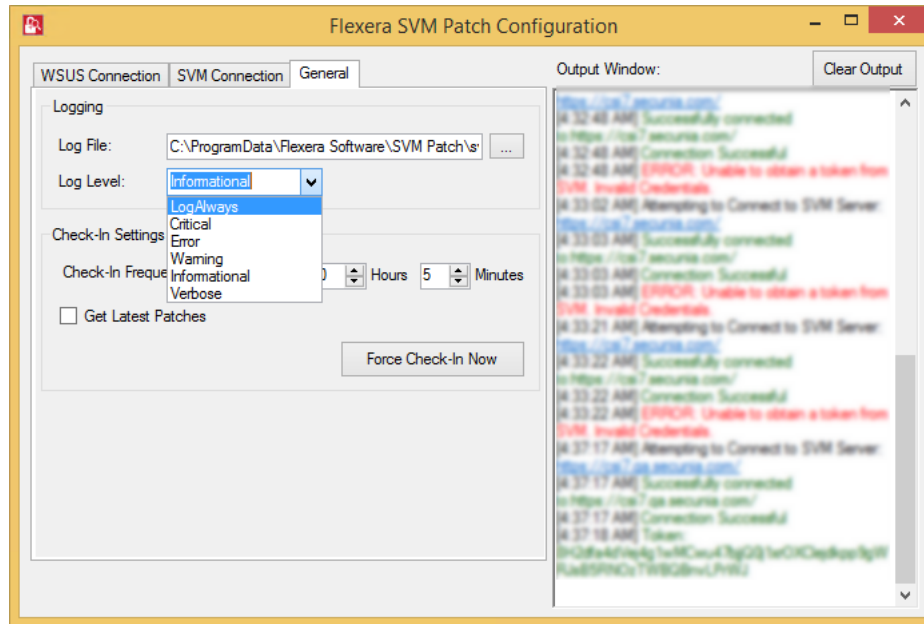


6. In SVM Connection tab, you will be prompted to enter your Software Vulnerability Manager Cloud credentials.
7. Click **Test Connection** button, on successful connection you will receive a Token in the Output Window.

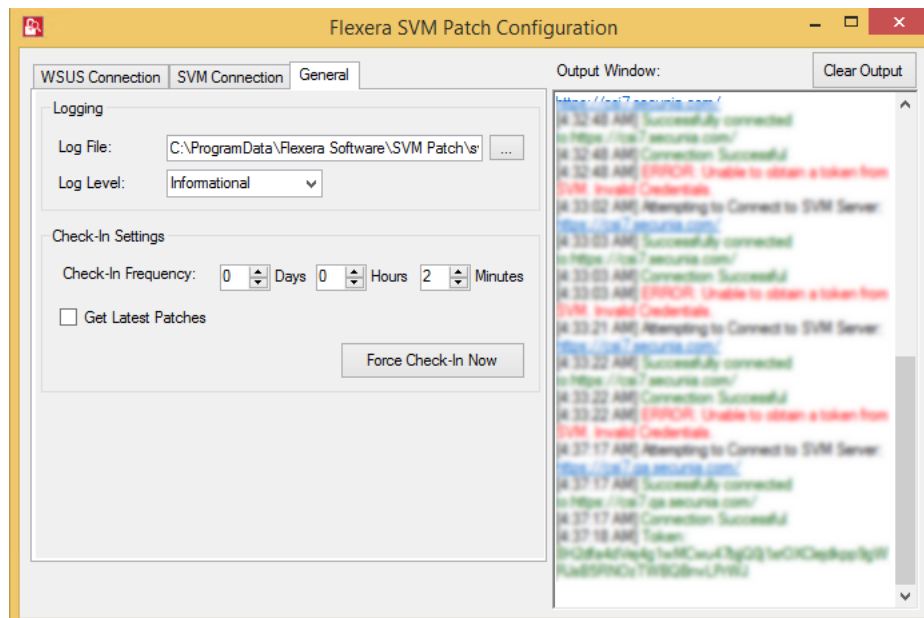


8. In the General tab, you can edit the folder path to save the action logs of this Tool. By default, the folder path will be **C:\ProgramData\Flexera Software\SVM Patch\svmpatch.log**.
9. You can set any one of the below preferences to save the log files:
 - LogAlways

- Critical
- Error
- Warning
- Informational
- Verbose



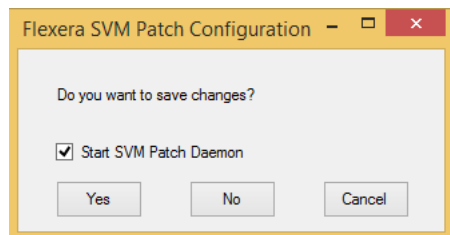
10. In **Check-In Settings**, you can set the frequencies to pull the relevant packages from the server.





Note • Force Check-In Now button can be used to pull relevant packages immediately.

11. To run the services, click close button. You will be prompted to enable **Start SVM Patch Daemon** in the closing window.



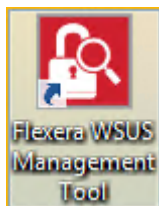
Flexera WSUS Management Tool

Flexera WSUS Management Tool allows you to manage the packages and configuration settings of WSUS.

On successful installation of Software Vulnerability Manager Patch Configuration Tool, along with the Software Vulnerability Manager Patch Configuration Tool shortcut, one shortcut for **Flexera WSUS Management Tool** will get created in your desktop.

It consist of two tabs:

- [Patching Information](#)
- [Configuration](#)



Patching Information

Patching Information tab prompts you to connect to the WSUS server to view the packages, based on the selected filter option, either 3rd party, Microsoft updates, or both. It also allows you to approve, delete, decline the selected patches and select a computer groups where you want to deploy these approved patches, at the set deadline.

It consist of three sections:

- Filter Update List
- Group Approvals
- Set Approval Deadline

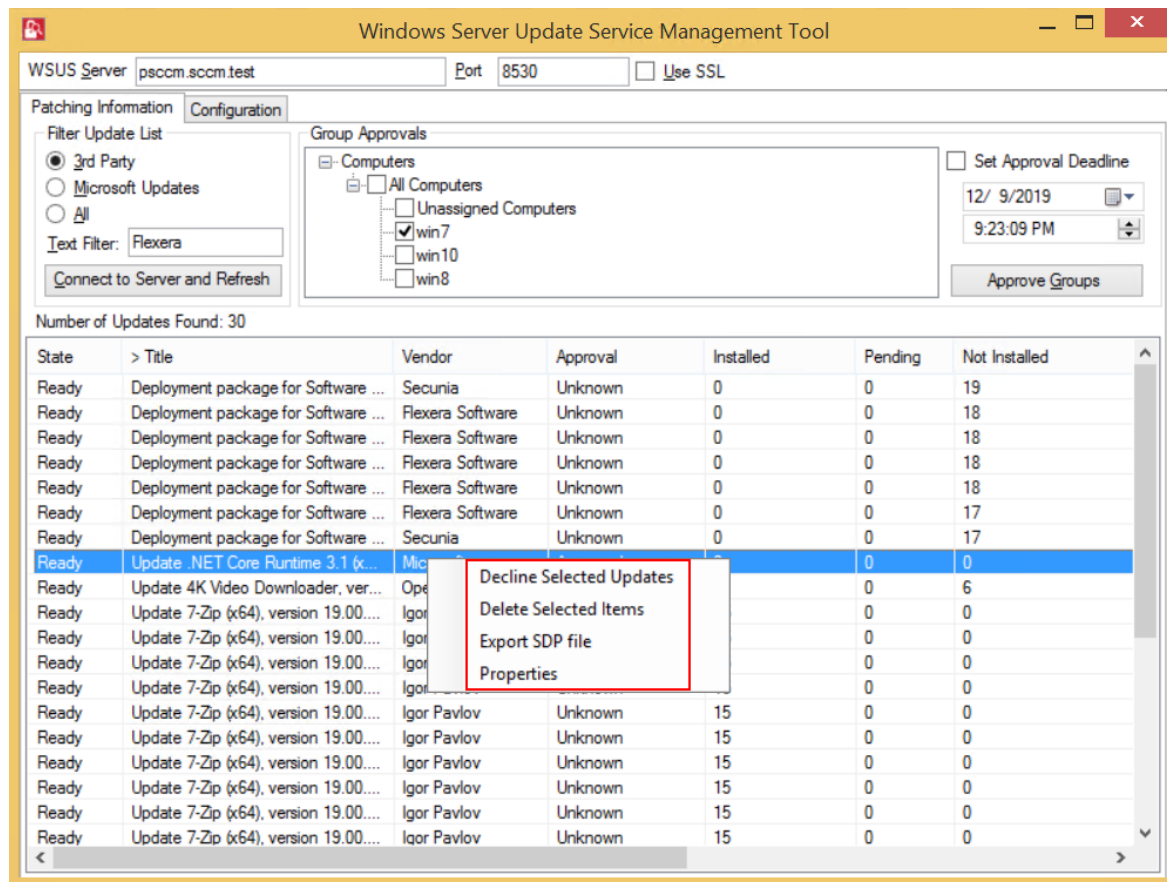


Task

To use WSUS Management Tool follow the below steps:

1. Double click on the shortcut **Flexera WSUS Management Tool** in your desktop, **Windows Server Update Service Management Tool** home page opens.

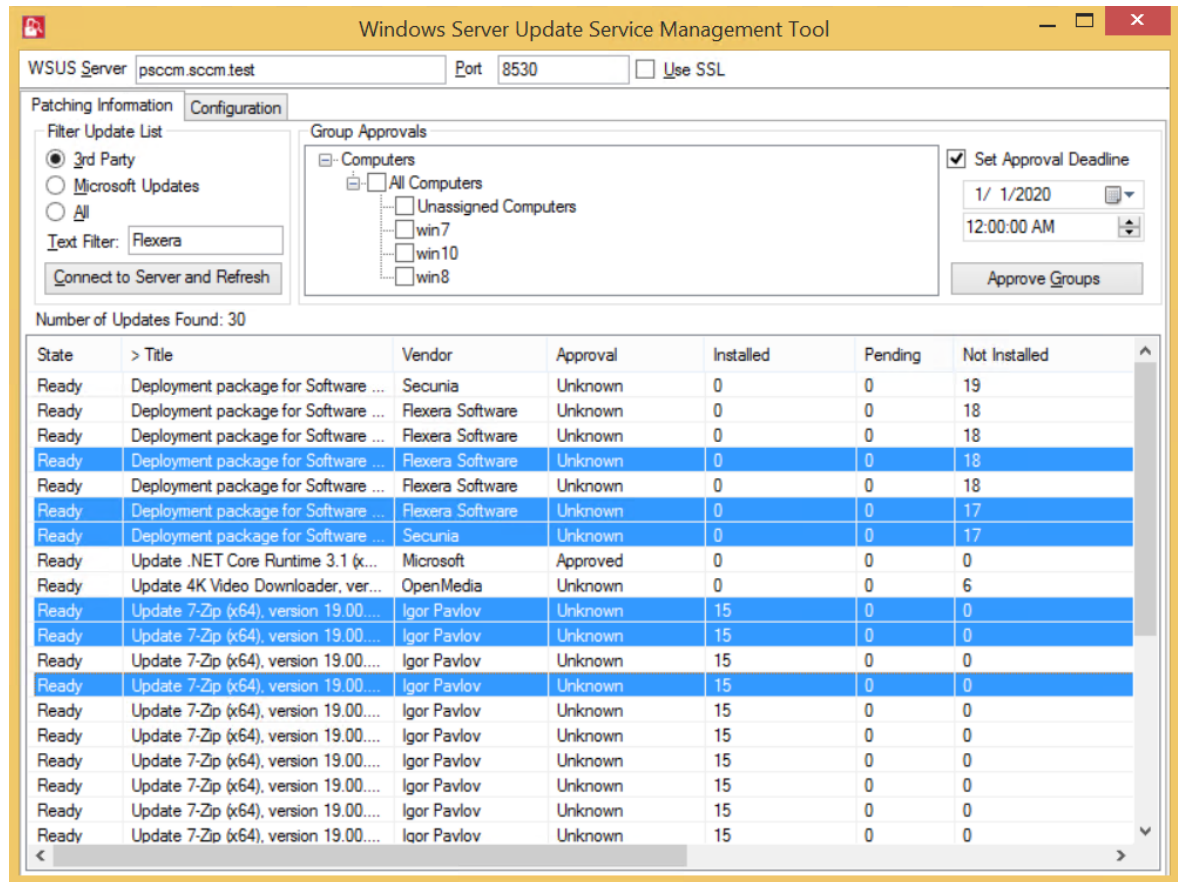
2. In the **Filter Update List**, you can either select 3rd Party Patches, Microsoft Updates, and All. You can enter the patch name or vendor name in the **Text Filter** box to fetch a quick patch list.
3. Click **Connect to Server and Refresh**, list of patches based on the selected **Filter Update List** appears.
4. Right click on a patch, you can perform a below function:
 - Decline Selected Updates
 - Delete Selected Items
 - Export SDP file
 - Properties
5. In **Group Approval** section, you can select a desired computer groups from the WSUS server.



6. Select the **Set Approval Deadline**, you can set the date and time to deploy the approved patches.



Tip • WSUS management tool allows you to Approve, Decline, and Delete multiple patches at the same time.

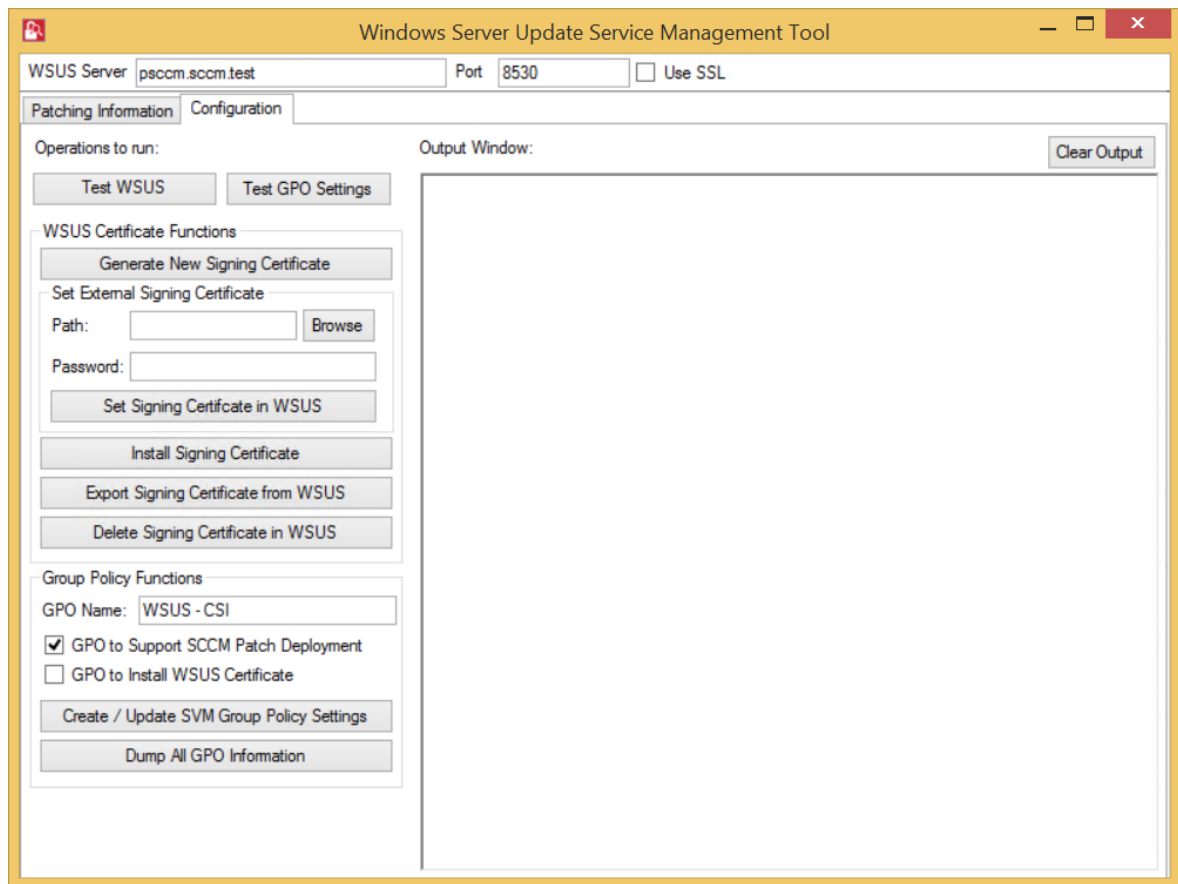


7. To approve the selected patches, click **Approve Groups**. You can see the **Approved** status from the **Approval** Column.

Configuration

In Configuration tab, you can perform the below WSUS configuration actions:

- Test WSUS
- Test GPO Settings
- Generate New Signing Certificate
- Install Signing Certificate
- Export Signing Certificate from WSUS
- Delete Signing Certificate in WSUS
- Create / Update SVM Group Policy Settings
- Dump All GPO Informations



Join Flexera's Customer Community

Join Flexera's Customer Community - the place to go for case management, knowledge base articles, and product forums. A community of customers is waiting to meet you! To get started:

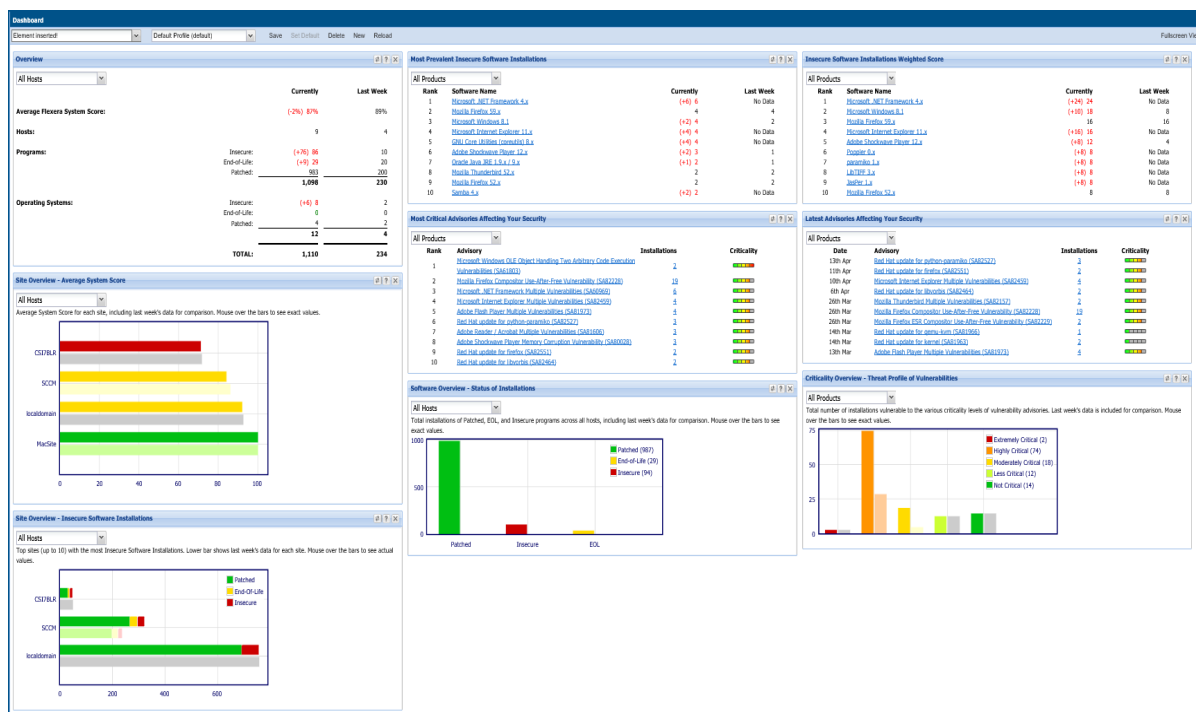
- Visit our Customer Community (<https://community.flexera.com>) and create an account. We extend case management privileges to two individuals per organization. Your organization's administrative contact (many times an individual in procurement or finance) has the ability to assign case management privileges.
- Visit our product forums! It's a great way to exchange best practices and tips and tricks with other customers like you!

4


The Dashboard

The Dashboard provides an overview of your hosts with the help of various “portlets”. Portlets are a collection of components that graphically display key data and allow you to create profiles which can display a unique combination of portlets.

The first time you login to the Software Vulnerability Manager console the Dashboard page will only display the Overview portlet. Select the Dashboard elements you want to view from the drop-down list on the upper left of the page. You can then either save the profile or, if you have created several profiles, set it as the default profile. You can also delete, add a new profile or reload the current profile view.





Tip • Click  in any portlet to refresh the data displayed. You can further filter the data in portlets that allow Smart Group selection.



Tip • Click  in any portlet for more detailed information on the data displayed.



Note • You can only load one unique portlet at a time.



Tip • You can toggle between Full-screen and Standard views.

Agent Administrative Privileges and Data Collection

The Software Vulnerability Manager On-Premises Edition requires an Agent to be installed on your server to scan your environment for vulnerabilities. Installing the Software Vulnerability Manager Agent file `csia.exe` requires administrative privileges. When scanning your environment, the Agent collects data from each device that is scanned.

The following sections provide further details:

- [Agent Administrative Privileges](#)
- [Agent Data Collection](#)

Agent Administrative Privileges

The Software Vulnerability Manager Agent requires administrative or root privileges for the following functionality:

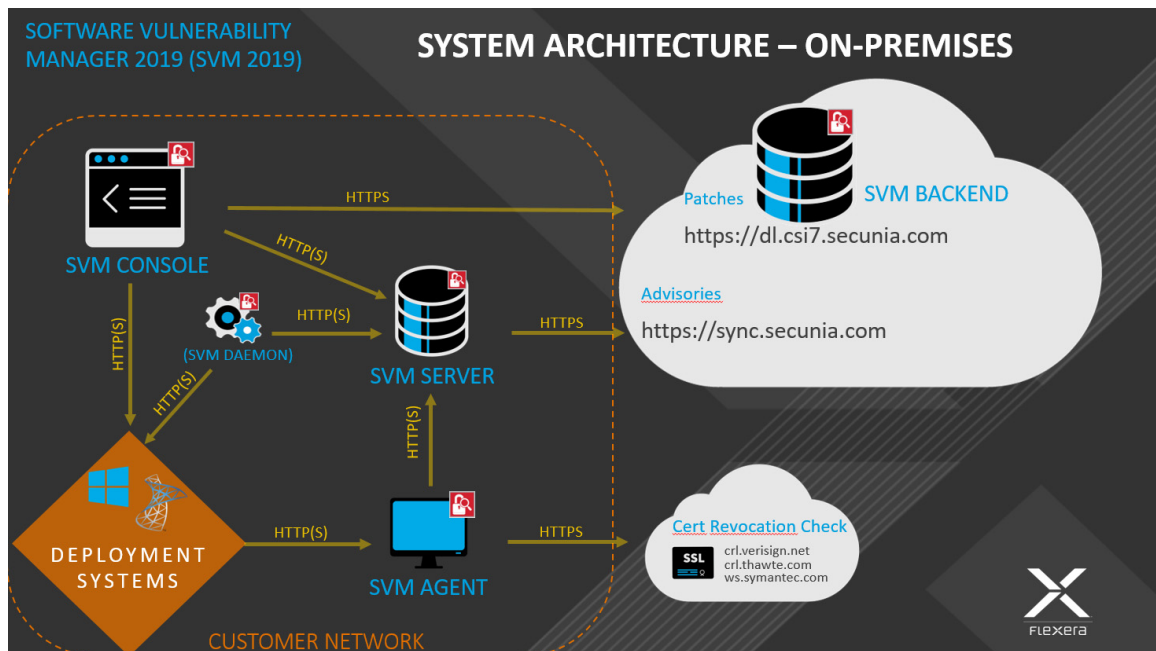
- Install or uninstall the service
- Update configuration data stored in per-machine locations (Examples: MachineGUID (written once); last scan time (updated each scan))
- Scan the entire hard drive for vulnerable software (non-administrative users cannot read other users' local files)



Note • *At this time, it is not feasible to skip parts of this functionality when installing the Agent without administrative or root privileges.*

The Software Vulnerability Manager Agent requires network connectivity (HTTP/HTTPS) to <your SVM2018 on-prem server host name>.

See the diagram below for an overview of the Software Vulnerability Manager On-Premises System Architecture.



Agent Data Collection

After scanning your environment, the Software Vulnerability Manager Agent collects the following data, which is summarized into a single POST to <your CSI on-prem server host name>. The Agent collects data from Windows, Red Hat Enterprise Linux (RHEL) and Mac OS X operating systems. The data collected varies by operating system as described below.

All Operating Systems

- Machine name
- MachineGUID (generated by Flexera)
- System type (architecture / operating system)
- IP address
- MAC address
- Time (GMT, local)

Windows

- Distinguished name
- List of security Knowledge Base articles installed or pending, source thereof
- List of vulnerable and unrecognized applications from the File System scan:
 - Sends only:
 - File path

- File size
- Metadata from the Portable Executable (PE) header to recognize known software (Examples: timestamp, machine architecture)
- Metadata from the Version Block to recognize known software (Examples: product name, product version, company name, original file name, internal name, file version, comments, file description, legal copyright, legal trademarks, private build, special build)
- Files collected are filtered by scan rules or type
- Locations of well-known system folders (Example: C:\Program Files)
- List of drives discovered or scanned
- Processing time and other profiling measures

Red Hat Enterprise Linux (RHEL)

- List of installed Red Hat Package Managers (RPMs) from rpm
- List of packages with security updates using the Yellowdog Updater Modified (YUM) tool

Mac OS X

- List of applications from the File System scan of .plist sends only:
 - File path
 - Metadata from the plist used to recognize known software (Examples: author; description; CFBundle: display name, identifier, short version string, version, executable, get info string, name, package type; NSHumanReadableCopyright)
- List of operating system updates queried from the system

6

Scanning

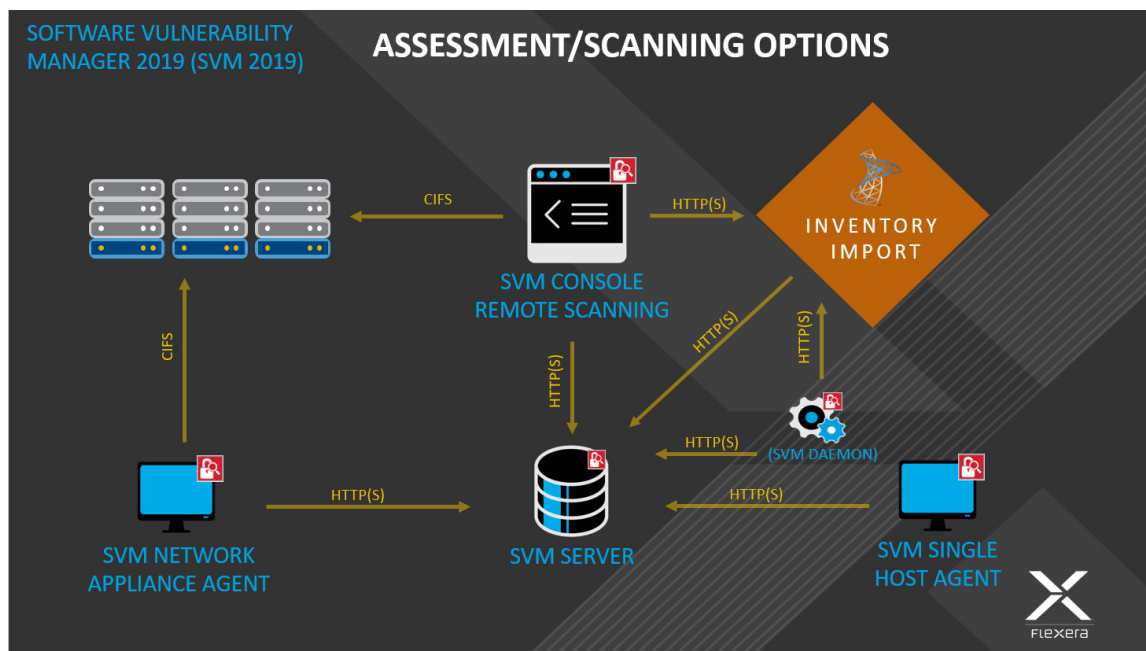
Software Vulnerability Manager allows scanning of target hosts using the following approaches:

- Single Host Agent-based scans are conducted by the Software Vulnerability Manager Agent that can be installed in different modes: Single Host mode, Network Appliance mode, or Command Line mode.
- Alternatively, you can scan the target hosts by launching a scan from the system where the Software Vulnerability Manager console is running. By using this approach, no software is installed in the target hosts. The scanning is performed using standard operating system services. This scan is also referred to as a “remote scan”.

The various types of scan are listed and shown below:

- [Agent-Based Scan – Requirements for Windows](#)
- [Agent-Based Scan – Requirements for Mac OS X](#)
- [Agent-Based Scan – Requirements for Red Hat Enterprise Linux \(RHEL\)](#)
- [Remote/Agent-less Scan – Requirements \(Windows\)](#)
- [Remote Scanning Via Software Vulnerability Manager \(Agent-less Scan\)](#)
- [Remote Scanning Via Agents](#)
- [Scanning Via Local Agents](#)
- [Run Scan from System Center Configuration Manager \(SCCM\)](#)
- [Scanning Mac OS X](#)
- [Scanning Red Hat Enterprise Linux \(RHEL\)](#)

Below is a visual overview of the Software Vulnerability Manager scanning options:



Note • If the WSUS Self-Signed Certificate will be used to sign the update packages created by Software Vulnerability Manager, you can use a different certificate as an alternative.



Important • Administrators must ensure that Software Vulnerability Manager, and its scanning Agent respectively, have access to all necessary system and online resources which allow the application to run as intended. The address `http(s)://csi_server_name/` should be white-listed in the Firewall/Proxy configuration to ensure that the client system is allowed access to these online resources.

Agent-Based Scan – Requirements for Windows

The flexibility offered by Software Vulnerability Manager ensures that it can be easily adapted to your environment.

If you choose to scan using the installable Agent (Agent-based scans), as described in [Single Host Agents](#), the following requirements should be present in the target hosts:

- Administrative privileges (to install the Software Vulnerability Manager Agent – `csia.exe`)
- Microsoft Windows Server 2008 R2, 2012, 2012 R2, 2016
- Microsoft Windows Operating System 7 Service Pack 1, 8.1, 10
- Network Connection – SSL 443/TCP to `http(s)://csi_server_name/`.
- Windows Update Agent 2.0 or later

Agent-Based Scan – Requirements for Mac OS X

The following requirements should be met before installing the Single Host Agent on an Intel-based Mac OS X machine:

- Supported Systems:
 - 10.8 Mountain Lion
 - 10.9 Mavericks
 - 10.10 Yosemite
 - 10.11 El Capitan
 - 10.12 Sierra
 - 10.13 High Sierra
 - 10.14 Mojave
- Administrator privileges at minimum ('root' privileges required for the installation)
- Network Connection – SSL 443/TCP to `http(s)://csi_server_name/`.
- The user installing the Agent must have 'execute' permissions on the file (`chmod +x`).

Agent-Based Scan – Requirements for Red Hat Enterprise Linux (RHEL)



Note • The csia agent for RHEL is architecture independent (that is, it works for 32- and 64-bit).

To install the Single Host Agent on a Red Hat Enterprise Linux (RHEL) machine, the user:

- Must be a member of the sudoer group.
- Must have write access to the `/etc/csia` folder to save configuration data.
- Must have a RHEL machine that supports the following operating systems:
 - RHEL 6: requires bash, gzip, sed, gawk, procps, coreutils, glibc(x86-32), libcurl(x86-32), libconfig(x86-32), libuuid(x86-32), yum, yum-security
 - RHEL 7: requires: bash, sed, gawk, procps, coreutils, glibc(x86-32), libcurl(x86-32), libconfig(x86-32), libuuid(x86-32), yum

For further RHEL agent installation information, see [Installing the Software Vulnerability Manager Agent for Red Hat Linux](#).



Note • It may be possible to install the scan Agent on RHEL operating systems and configurations other than those described above. However, these have not been tested and are not supported by Flexera.

Remote/Agent-less Scan – Requirements (Windows)

If you prefer to scan without installing the Software Vulnerability Manager Agent (Agent-less scans), the following requirements should be present in the target hosts:

- Ports 139/TCP and 445/TCP open inbound (on hosts)
- File sharing enabled on hosts
- Easy/simple file sharing **disabled**
- Windows Update Agent 2.0 or later

Required Windows services started on hosts:

- Workstation service
- Server service
- Remote Registry service (by default is disabled on Win7/Vista)
- COM+ services (COM+ System Application: Set to Automatic)

In order for a Remote/Agent-less scan to succeed, the user executing the scan – whether that's the user running the Software Vulnerability Manager console or the user for the service running the network appliance – must have **local administrative privileges** on the scanned hosts.

When performing Remote/Agent-less scans, the result may be displayed as **Partial** in the Completed Scans page. This is caused by the Windows Firewall default settings that block the RPC dynamic ports.

On the host, in Windows Firewall, the user should create an inbound rule to allow inbound traffic for all products that use RPC dynamic ports.



Task

To create the rule:

1. From Windows **Control Panel (View by Category) > System and Security > Windows Firewall**, select **Advanced settings**.
2. Select **Inbound Rules** in the **Windows Firewall with Advanced Security on Local Computer** pane and then select **New Rule** in the **Actions** pane.
3. The New Inbound Rule wizard opens
4. Select **Custom rule** and click **Next**.
5. Select **All programs** and click **Next**.
6. In the Protocol and Ports window:
7. From the **Protocol type:** drop-down list, select **TCP**.
8. From the **Local port:** drop-down list, select **RPC Dynamic Ports**.
9. Click **Next** until the Profile window appears.
10. Clear **Private** and **Public**, select **Domain** and click **Next**.

11. Give the rule a name, for example: **Software Vulnerability Manager**.

12. Click **Finish**.

Once you have created the rule, use the Software Vulnerability Manager console to perform a remote scan of the PC. The host will connect to Windows Update and the scan status should be displayed as **Success** in the Completed Scans page.

Remote Scanning Via Software Vulnerability Manager (Agent-less Scan)

These scans are performed in an Agent-less manner and the credentials used by Software Vulnerability Manager to authenticate on the target hosts will be the same as those of the user that launched the Software Vulnerability Manager console.

This section describes the features for this Agent-Less Scan:

- [Quick Scan](#)
- [Scan Groups](#)
- [Scan Progress](#)



Important • Please consider the system requirements for the Scan Groups/Agent-less scans, described in [Remote/Agent-less Scan – Requirements \(Windows\)](#).

Quick Scan

Use this page to conduct quick, on-demand, scans from your Software Vulnerability Manager console against remote hosts on your network or your local PC. Enter the scan type and IP address range for the hosts you wish to scan in the **Enter hosts to scan** screen and click **Scan Hosts**.

For local host scanning, click **Include this computer in scan**.

Enter hosts to scan

Scan Type

☒ Type 2: All Paths (Recommended)

☐ Type 1: Default Paths

IP Range

From:

To:

IP Addresses or Computer names

Scan this computer (localhost)

☒ Include this computer in scan

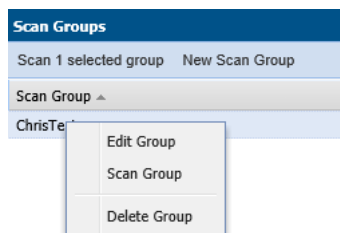
Scan 1 Host

To make sure that you are able to remote scan the target host, please ensure that all the system requirements for the remote scan are in place.

The progress can be seen under [Scan Progress](#).

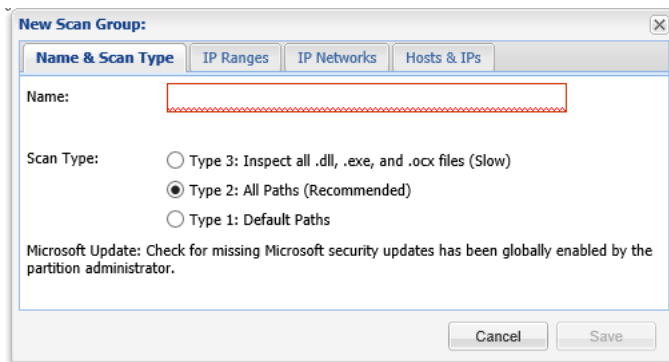
Scan Groups

This page displays a list of Scan Groups you have created. To start a scan, right-click the group name and select **Scan Group**.



If you are scanning remote hosts, your current login credentials, or the ones you supplied via “Run as...” will be used to authenticate against the remote hosts when conducting the scan.

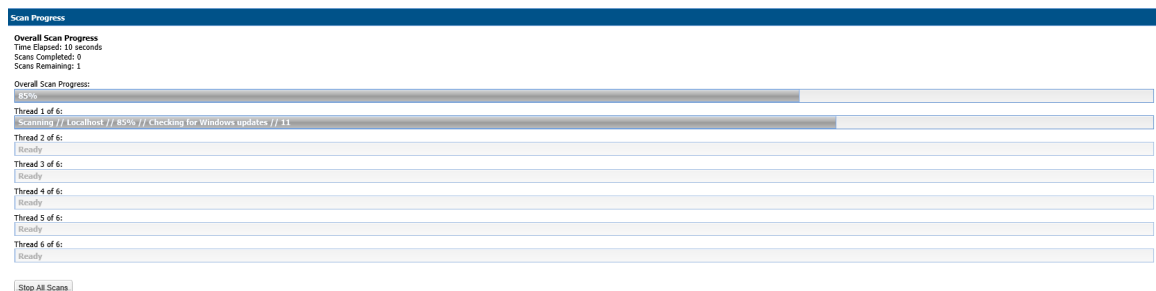
Click **New Scan Group** to create and configure a group of hosts to be scanned.



After navigating through the different tabs: **Name & Scan Type**, **IP Ranges**, **IP Networks** and **Hosts & IPs**, click **Save** to create the scan group.

Scan Progress

Use this page to track the scans being conducted. You can also configure the number of simultaneous scan threads (the default value is set to 5) as described in [Settings](#).



System Center Inventory Import

Scan results are obtained from the data collected by the System Center software inventory agent, which avoids the need to install the Software Vulnerability Manager Agent on each client.

To set up an import schedule, see [System Center Import Schedules \(Requires the Software Vulnerability Manager Daemon\)](#).

System Center integration requires the following prerequisites:

- **Setting up authentication**—The user running the Software Vulnerability Manager console must have access to the database containing the data of the System Center. For System Center Configuration Manager the database is named CM_<site_code> and for System Center Configuration Manager 2007 it is named SMS_<site_code>. To add permissions, open SQL Server Management Studio, right-click the appropriate database, navigate to permissions and add Connect and Select.
- **Setting up the software inventory agent**—Assuming that the System Center site has been set up, open the System Center console and ensure that the System Center client (agent) is installed on the hosts to be scanned. In System Center Configuration Manager, go to Devices and right-click Install client. Then go to Administration > Client Settings > Properties > Software Inventory. To configure the broadest possible pattern, select File Detail: full and add the

patterns *.dll, *.exe, *.ocx. Do not exclude the Windows directory. Less data will be generated by specifying a narrower pattern, however, the quality of the scan result will suffer.

- **Increasing the software inventory file size**—In addition, you might want to consider increasing the software inventory file size from the default of 5 MB to 12 MB. To accomplish this, change the following registry key on the System Center Server:

HKLM\Software\Microsoft\SMS\Components\SMS_SOFTWARE_INVENTORY_PROCESSOR\Max File Size

Click Configure System Center. In the Software Vulnerability Manager System Center Configuration page, enter the System Center Server Name. Select the Use System Center Collection Name as Site name for imported hosts check box to use the Collection name as a host's Site name during Collection import and click Save.

Software Vulnerability Manager System Center Configuration

System Center SQL Database Settings

Choose automatic to get the SQL connection data from System Center server or specify your own connection data with manual option.

☒ Automatic

System Center Server Name:

☐ Manual

System Center Import Settings

Choose whether or not to automatically create a Site name from the System Center Collection Name and assign it to imported hosts.

☒ Use System Center Collection Name as Site name for imported hosts

Save

If you select Manual, enter the SQL Host, SQL Port and SQL Database connection data and click Save.

Software Vulnerability Manager System Center Configuration

System Center SQL Database Settings

Choose automatic to get the SQL connection data from System Center server or specify your own connection data with manual option.

☐ Automatic

☒ Manual

SQL Host:

SQL Port:

SQL Database:

System Center Import Settings

Choose whether or not to automatically create a Site name from the System Center Collection Name and assign it to imported hosts.

☒ Use System Center Collection Name as Site name for imported hosts

Save

In the System Center Inventory Import page, click Import Selected Collections or Import All Collections.



Important • The scan result is based on the data collected by the software inventory agent, which may not be of the same quality as that of the Software Vulnerability Manager Agent (csia). This means that there could be discrepancies between a

scan performed by the System Center integration and the csia. It may also result in some products not being detected correctly. For higher quality scan results Flexera recommends using the csia.

System Center Import Schedules (Requires the Software Vulnerability Manager Daemon)

To create a new System Center import schedule, perform the following steps.



Task

To create a new System Center Import Schedule:

1. Click New System Center Import Schedule and enter:
 - The Schedule Name.
 - The Next Run date and time.
 - The Frequency (Hourly, Daily, Weekly or Monthly) that the import will be performed or select the One-Time Import check box.

2. Click Add Collections and enter the Collections to include in the Import Schedule.
3. Right-click an Import Schedule in the grid to edit or delete the schedule.

Remote Scanning Via Agents

You can use Network Appliance Agents for scanning one or more networks at scheduled intervals without having to install the Software Vulnerability Manager Agent in every single target host.

With the csia.exe installed in Network Appliance mode, you will have the ability to schedule remote scans.

The hosts to be scanned can be identified by an IP-range, IP-network or Host-name.

The Software Vulnerability Manager console allows you to easily manage the scans being performed by the Network Appliance Agent.



Important • Please consider the system requirements for the Scan Groups/Agent-based scans, described in [Agent-Based Scan – Requirements for Windows](#) and [Agent-Based Scan – Requirements for Mac OS X](#).

Software Vulnerability Manager Agent Command Line Options

You can use the following command line options for the Software Vulnerability Manager Agent.

- [Help](#)
- [Version](#)
- [Install](#)
- [Uninstall](#)
- [Modify Settings](#)
- [Controlling the Service](#)
- [Scanning from the Command Line](#)
- [Randomizing the Agent Scan Schedule](#)
- [Agent Configuration Options](#)

Help

Run the Software Vulnerability Manager Agent to get instructions and a list of command line options (ignores all other command line options, prints instructions and exits immediately). Also prints version as with -V. Exclusive:

```
csia.exe -h
```

Version

Print the version number of the Software Vulnerability Manager Agent on the command line (exclusive):

```
csia.exe -V
```

Install

Install the Software Vulnerability Manager Agent from the command line, with configuration options. Installs as current user, prompts for password, settings saved to HKCU:

```
csia.exe -i <config options>
```

Install the Software Vulnerability Manager Agent from the command line to run as LocalSystem, with configuration options. Saves settings to HKLM:

```
csia.exe -i -L <config options>
```

Install the Software Vulnerability Manager Agent from the command line to run as <user>, with configuration options. Prompts for password and saves settings to HKEY_<user>:

```
csia.exe -i -R <user> <config options>
```

Install the Software Vulnerability Manager Agent from the command line to run as <user>, with <password> with configuration options. Saves settings to HKEY_<user>:

```
csia.exe -i -R <user>:<password> <config options>
```

Install the Software Vulnerability Manager Agent from the command line but not write anything to the registry (also works with -R and -L):

```
csia.exe -i -N
```

If you need to install the Software Vulnerability Manager agent for multiple partitions, you can download one agent from the CSI server and add the agent to a preconfigured Microsoft System Center Configuration Manager (SCCM) package. For details see [Install the Agent via SCCM](#).

Install the Agent via SCCM

In an environment with multiple partitions, you can download one Software Vulnerability Manager agent from the CSI server and add the agent to a preconfigured Microsoft System Center Configuration Manager (SCCM) package. The preconfigured SCCM package must first implement the registry keys necessary to identify the Software Vulnerability Manager agent and the relevant partition where the Software Vulnerability Manager agent should deliver the scan result. Then the SCCM package installs the Software Vulnerability Manager agent.

The end result is to have several SCCM packages that are all preconfigured to create the appropriate registry keys and only require an “unidentified” agent, which is downloaded directly from the CSI server. When agents need to be upgraded, only one Software Vulnerability Manager agent must be downloaded to replace the existing agent file in the SCCM package.



Important • The following instructions will only work with the Software Vulnerability Manager On-Premises version 7.5.1.12-1 and above versions.



Task

Install the Agent via SCCM:

1. Create the registry keys required to identify the Software Vulnerability Manager Agent and the related Partition using one of the below registry locations, depending on the OS architecture (32/64 bit):
 - (32bit OS) HKEY_LOCAL_MACHINE\SOFTWARE\Secunia\CSI Agent
 - (64bit OS) HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Secunia\CSI Agent
2. Name the four required registry keys, which are all String Values, as follows:
 - CSIAHost
 - CSIAPort
 - CSIAToken
 - CSIAUser

These values are available in the Software Vulnerability Manager Console, and any user can acquire the values for these four registry keys.

- The registry keys can be configured by adding installation switches to a command-line installation:

Set the Server host name	--host <host name>
Set the Server port	--port <port number>
Set the Software Vulnerability Manager token	--token <token>
Set the Software Vulnerability Manager user ID	--userid <userid>

- In the Software Vulnerability Manager console under **Scanning > Single Host Agents > Download Agent**, download the agent. On the same page there is a button named **Email Settings**. Click this button, and an email will be sent to the email address specified in the related Software Vulnerability Manager user profile.
- Copy the “unstamped” agent file from the CSI server /usr/local/Secunia/csi/binaries/csia/win/csia.exe (do not rename the file) to the preferred installation location on the host (Default location is C:\Program Files (x86)\Flexera\CSI Agent\csia.exe).
- Install the csia.exe via the command line: Start cmd with run-as-admin.
- Access the folder location where the csia.exe is located and run the command: csia.exe -i username@domain:password -d install.log -v -skip-wait
- Open Regedit to locate the new Software Vulnerability Manager Agent folder.

Uninstall

Uninstall the Software Vulnerability Manager Agent service, remove all settings and delete the key from the registry where the service reads them from:

```
csia.exe -r
```



Note • The -L and -R options are irrelevant when uninstalling.

If the service is installed but cannot be removed, then the registry settings aren't removed.

If the service is not installed, does nothing.

If the registry settings cannot be removed, a warning is given and the service is removed regardless.

To uninstall the Software Vulnerability Manager Agent service, while leaving the registry settings intact:

```
csia.exe -r -N
```

To remove the service, if installed, and delete the \Software\Secunia\Software Vulnerability Manager Agent registry key from everywhere in the registry (exclusive):

```
csia.exe --delete-all-settings
```


Modify Settings

Save command line setting to the registry, so the service will use it. The settings are saved to the location based on where installed the Software Vulnerability Manager Agent reads the settings from. If no Agent is installed, or the settings cannot be saved to the correct location, nothing is saved, an error is printed and the command aborts:

```
csia.exe -S <config option>
```

Controlling the Service

Starts the service if it is not running (exclusive):

```
csia.exe --start  
csia.exe --restart
```

Stops the service if it is running (exclusive):

```
csia.exe --stop
```

Scanning from the Command Line

Run the Software Vulnerability Manager Agent with immediate command line scan, with options. Ignores registry settings and server settings:

```
csia.exe -c <config options>
```

Run the Software Vulnerability Manager Agent locally in service mode as current user, reading options from command line, registry and server, with command line options taking precedence, then server options, then registry options. To stop the service once it is running, press CTRL+C:

```
csia.exe -fg <config options>
```

If possible, run the Software Vulnerability Manager Agent locally in service mode as a different user with -L and -R. This will read options in exactly the same way as a service, with the exception of <config options> on the command line override which, unlike a service, has no command line:

```
csia.exe -fg -L <config options>  
csia.exe -fg -R <user> <config options>
```

Order of precedence:

- Settings given on command line take precedence but, when running as a service, there is no command line.
- Settings from server take precedence over settings read from registry.

Randomizing the Agent Scan Schedule

Set up a random scan schedule to stagger the scanning of multiple machines within a system. This command line applies to all platforms.

```
csia.exe -c -si <scan interval upper limit>
```

“si” represents scan interval, and the scan interval’s upper limit can be set up by the number of minutes.

For example, `csia.exe -c -si 20` would mean that the scanning agent will start scanning after a delay of random minutes, which could be from 1 to 20 minutes.

Agent Configuration Options

The following table lists the Agent configuration options.

Table 6-1 • Agent Configuration Options

Configuration Option	Description
Program Options:	
<code>-A/--network-appliance</code>	Run in Network Appliance mode.
<code>-c/--cli</code>	Run software inspection from the command line using command-line settings and server-supplied settings. Exit codes returned: 0 - SUCCESS 1 - SERVER BUSY 2 - OPERATION FAILED 3 - SERVICE FAILED
<code>-d <path> --debug <path></code>	Write diagnostic information to the specified file.
<code>--getfileinfo <path></code>	Directory for output file
<code>-h/--help</code>	Display this message and exit.
<code>-n/--checkin-interval <interval></code>	Set the check-in interval for the service. This setting is in the format INTEGER followed by M/H/D representing minutes, hours, or days. Example: 10M for a 10-minute interval or 2H for a two-hour interval
<code>-o/--outdir <path></code>	Directory for output file
<code>-oc/--output-csv <file></code>	Output inspection results to a CSV file.
<code>-ox/--output-xml <file></code>	Output inspection results to an XML file.
<code>-si/--scantime_interval <minutes></code>	Set a random range to delay running software inspection. 0 means no random range, or 1-60 minutes.
<code>--skip-wait/--skipwait</code>	Skip the initial 10 minute wait before the first check in.
<code>-v --verbose</code>	Display or log additional diagnostic information.

Table 6-1 • Agent Configuration Options (cont.)

Configuration Option	Description
-V/--version	Display program version information and exit. Use this option when you want to check the version of the agent.
Customer Area Option:	
-g/--group <group>	Create host as a member of <group> in your Software Vulnerability Manager Account (defaults to domain or langroup if unspecified).
Mac Agent Option:	
--delete-all-settings	Deletes all information, including Globally Unique Identifiers (GUID), from the system to ensure it is clean to accommodate a new installation.
Network Settings:	
-D --direct-connection	Bypass proxy, use direct connection.
--forcehttps	Force HTTPS, regardless of port. When this option is not specified, we default HTTPS on port 443 and HTTP on other ports. This option is for debugging purposes.
--ignore-ca	Ignore unknown certificate authority.
--ignore-cn	Ignore invalid Common Name in cert.
--ignore-crl	Ignore Certificate Revocation list.
--pac-url <url>	Proxy Autoconfig url
--request-timeout <minutes>	Sets a timeout on network connections. Set for 1-10 minutes or use 0 for no timeout. Use this option to increase the timeout period of HTTP requests to prevent the timeout error when the server does not respond in 2 minutes.
-U <user:pass> --proxy-user <user:pass>	Set proxy credentials (saved in encrypted form).
--use-network-winhttp	Enable WinHttp network stack. Use WinHTTP when you want the agent to control the behaviors of the HTTP Internet protocol. We default WinHTTP to force using TLS 1.2. Also, the command line options for proxy such as -x, -U, and -D are designed to work in conjunction with WinHTTP. This option is for debugging purposes.

Table 6-1 • Agent Configuration Options (cont.)

Configuration Option	Description
--use-network-wininet	Enable WinInet network stack (default). Use WinInet when you want to control the behaviors of HTTP Internet protocol using the Internet Options. Since WinInet does not have services support, the agent running as a service ignores this option. This option is for debugging purposes.
-x <proxy:port> --proxy <proxy:port>	Set proxy.
Proxy Options:	
-D/--direct-connection	Force direct connection, overriding default internet proxy settings.
--pac-url <URL>	Specify the URL of the Proxy Auto Configuration file (.pac/.dat).
-U/--proxy-user <user[:pass]>	Specify Proxy authentication.
-x/--proxy <host[:port]>	Use HTTP proxy on given port.
Scan Options:	
--check-wmi	Use WMI to get Windows updates. Use this option to query Windows updates on SCCM using WMI in addition to a query using Windows Update Agent. This option could be used to see if the SCCM client on the device/host can be used for reporting missing KBs.
-t/--type	Software Inspection Type: 1, 2 (default), or 3. 1: Inspect applications in default locations only. 2: Inspect applications in non-default locations. 3: Inspect all .dll, .exe, and .ocx files. For details, see Scan Types .
-w/--no-os-update/--no-win-update	Do not connect to Windows Update.
--wua-proxy <0,1 or host[:port]>	Configure proxy settings for Windows Update. 0: Use the default setting. 1: Use the proxy configured with -x/--proxy. <host[:port]> Manually set the proxy host and port.

Table 6-1 • Agent Configuration Options (cont.)

Configuration Option	Description
Scan settings that server can override:	
-g <group> --group <group>	Group name for association
-n <minutes>M --checkin-interval <minutes>M -n <hours>H --checkin-interval <hours>H	Set Check-in interval.
-w --no-win-update --no-os-update	Disable windows update check.
Security Options:	
--ignore-ca	Ignore Unknown SSL Certificate Authority (CA).
--ignore-crl	Ignore SSL Certificate Revocation Check.
--ignore-cn	Ignore Invalid SSL Certificate Common Name (CN).
Server Options:	
--userid <userid>	Set the Software Vulnerability Manager access user ID.
--token <token>	Set the Software Vulnerability Manager access token.
--host <hostname>	Set the Server hostname.
--port <port>	Set the Server port.
Service Options:	
--delete-all-settings	Delete all settings related to this program from the registry. Deletes these settings from all registry keys.
--dry-run/--dryrun	Run up to the point of scanning without writing any changes and then exit (useful to log the configuration). Use this option to examine if the agent is able to run and communicate with the server. It will exit before scanning and won't make any changes to the system. You can use this option along with -c.
-i/--install	Install service.
-L/--localsystem	Run the service as the LocalSystem user.

Table 6-1 • Agent Configuration Options (cont.)

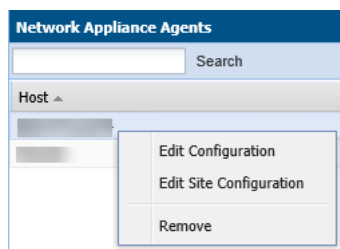
Configuration Option	Description
--manual	When installing, set service to only be started manually, rather than automatically
-N/--no-registry-write	When installing, do not write any settings to registry. When removing, do not delete settings from registry.
-p/--copy <dest>	Before installing, copy executable file to <dest> and install the service to run from <dest>.
-r/--remove	Remove service.
-R/--runas <user[:pass]>	Specify the user the service should run as. For a domain user type "user@domain" or "domain\user"
-S/--only-save-settings	Only save settings from the command line to registry, as the relevant user. Does not run, install or remove. Use this option when you want to modify the agent registry settings after the agent is installed. You need to restart the agent service to make the changes effective. This option could be used to edit the server options like userid/token/host/port stored in the registry. This setting is the opposite of "-N" options. If -N is used, no registry setting will be edited.
Service Recovery Settings:	
--service-failure-actions <actions>	Failure actions and their delay time (in milliseconds), separated by / (forward slash) – e.g., run/5000/reboot/800. Valid actions are <run restart reboot>. (Must be used in conjunction with the --service-failure-reset option)
--service-failure-command <command line>	Command line to be run on failure.
--service-failure-flag	Changes the failure actions flag setting of a service. If this setting is not specified, the Service Control Manager (SCM) enables configured failure actions on the service only if the service process terminates with the service in a state other than SERVICE_STOPPED. If this setting is specified, the SCM enables configured failure actions on the service if the service enters the SERVICE_STOPPED state with a Win32 exit code other than 0 in addition to the service process termination as above. This setting is ignored if the service does not have any failure actions configured.
--service-failure-reboot <message>	Message broadcast before rebooting on failure.

Table 6-1 • Agent Configuration Options (cont.)

Configuration Option	Description
--service-failure-reset <period>	Length of period of no failures (in seconds) after which to reset the failure count to 0 (may be INFINITE). (Must be used in conjunction with --service-failure-actions)

Network Appliance Agents

Use this page to view a list of the hosts which have Network Appliance Agents installed. Right-click a host to configure the Network Appliance Agent installed on that host.



To scan using a Network Appliance Agent you must:

- Install the Agent in Network Appliance mode
- Create a Network Appliance Scan Group

A schedule links the above to perform scans of the group at set intervals.

To create a target group to be scanned by a Network Appliance agent, see [Network Appliance Groups](#).

To download the network agent, see [Download Network Agent](#).

Network Appliance Groups

Use this page to create a target group that will be scanned by a Network Appliance Agent. Click **New Group** to create a new target group that will be remotely scanned by one of the Network Appliance Agents previously installed.

Download Network Agent

Use this page to download the `csia.exe` file as well as read an explanation on how to install the Network Appliance Agent.



Important • Ensure that the Agent file `csia.exe` is available in the system that will host the Agent in Network Appliance mode.

Example

If you want to scan three different networks (for example Germany, United States, and United Kingdom) without having to install the Agent in Single Host mode, then you can install three instances of csia.exe in Network Appliance mode, one on each network.

Afterwards you will be able to scan all the hosts on the three locations at scheduled intervals by creating the appropriate scan groups in **Network Appliance Groups** and assigning each group to its respective and previously installed Network Appliance Agent.

Result

15 minutes after installing a csia.exe in Network Appliance mode, the Network Appliance Agent will appear in **Scanning > Remote Scanning Via Agents > Network Appliance Agents**.

To specify the target host to be scanned by the Network Appliance Agent, please configure the scan group in **Scanning > Remote Scanning Via Agents > Network Appliance Groups**.

Install the Network Appliance Agent from the command prompt using:

```
>csia.exe -A -i
```

It is essential that the csia.exe is installed with the correct credentials.

The user installing the Network Appliance Agent must have administrator rights to all the target hosts that will be scanned by the Network Appliance Agent.

Example of an installation:

```
C:\Documents and Settings\Administrator>cd "%Program Files%\Secunia\CSI"
C:\Program Files\Secunia\CSI>csia.exe -A -i
Enter password for user 'Administrator':
Starting 'Secunia CSI Agent' service
'Secunia CSI Agent' service started
'Secunia CSI Agent' successfully installed
C:\Program Files\Secunia\CSI>
```

Scanning Via Local Agents

Software Vulnerability Manager provides different scan approaches, enabling you to select the one that best suits your environment. The Agent-based deployment is more robust and flexible for segmented networks or networks with mobile clients (for example, laptops). Once installed, the Agent will run silently in the background.

This is the recommended scanning approach due to its flexibility, usage convenience, and performance.



Important • Please consider the system requirements for the Scan Groups/Agent-based scans, described in [Agent-Based Scan – Requirements for Windows](#) and [Agent-Based Scan – Requirements for Mac OS X](#).


[The Scan Process – How Does it Work?](#) graphic references three [Scan Types](#) that are compared below.

To scan using the Agent installed in Single Host mode, see [Single Host Agents](#).

To download the local agent, see [Download Local Agent](#).

Scan Types

Table 6-2 • Scan Types

Scan Type	Folders Searched	File Name Match	Applications Detected
Minimal Scan - Scan Type 1	Default folders only Example: Program Files	File names are matched first; then metadata is matched Example: c:\Program Files\Mozilla Firefox\Firefox.exe	Known applications in predefined locations on a host
Optimal Scan - Scan Type 2 	All files and folders	File names are matched first; then metadata is matched Example: c:\Custom Mozilla Firefox Folder\Firefox.exe	Known applications in any location ("portable applications") on a host
Full Scan - Scan Type 3	All files and folders	Metadata only Example: c:\Custom Mozilla Firefox Folder\myFirefox.exe	Renamed applications that match a pattern detected in the first two scan types such as .exe, .dll, and .ocx in any location on a host

Note • Scan Type 2 is the default scan type.

Single Host Agents

Use this page to manage configurations and schedule scans for the hosts where the Agent is installed as a service in Single Host mode.

Double-click a host to manage the configuration of the selected Agent and change its settings (Inspection type, Check-in frequency, Days between scans).

Right-click a host name and select **Edit Site Configuration** to manage the configuration for all the hosts in that Site.



Important • When selecting options under **Edit Site Configuration**, note that:

- Any edits to the scan schedule will come into affect only after the currently scheduled scan has completed. Each agent could potentially have a scan scheduled at different times. Therefore, any new scan configuration edit will affect the scan schedule at various times.
- Any edits made to the **Agent Check-In Frequency** option or selecting the **Schedule Next Scan** option **Scan host as soon as possible** will come into effect only after an agent has checked in as per the previously set scan frequency.

- The scan configuration settings set on the Software Vulnerability Manager website are not automatically transmitted to the agents. The agents have to connect to the Software Vulnerability Manager website as per their prior scheduled **Agent Check-In Frequency** before the agents become aware of the new scan configuration edits.

The hosts scanned with the csia.exe will be grouped by Site. By default the domain name will be used as a Site name.

To change a Site name, please refer to [Sites](#). You can also specify a Site name when installing the Agent, by using the **-g** parameter or by specifying a Site name in the additional parameters when creating the Agent deployment package described in [Agent Deployment](#).

Download Local Agent

Use this page to download the signed and unsigned Agents (csia.exe) as well as read an explanation on how to install the Agent in Single Host mode. For the signed Agents you shall download the token file csia_token.ini.

The following unsigned Agents are available:

- Download Agents with Token
 - Microsoft Windows (ver. 7.6.0.10)
 - Macintosh OS X - 64bit (ver. 7.6.0.10)
 - Macintosh OS X - 32bit (ver. 7.6.0.7)
 - Red Hat Linux 7.x (ver. 7.6.0.10)
 - Red Hat Linux 6.x (ver. 7.6.0.10)

The following Signed Agents are available:

- Download Signed Agents without Token
 - Microsoft Windows (ver. 7.6.0.10)
 - Macintosh OS X - 64bit (ver. 7.6.0.10)



Important • Note the following for Signed Agents:

- To install signed agent for Windows, download [csia_token.ini](#) and place it in the same folder where agent is saved.
- To install signed agent for MacOS, see [Prepare Your Mac](#).

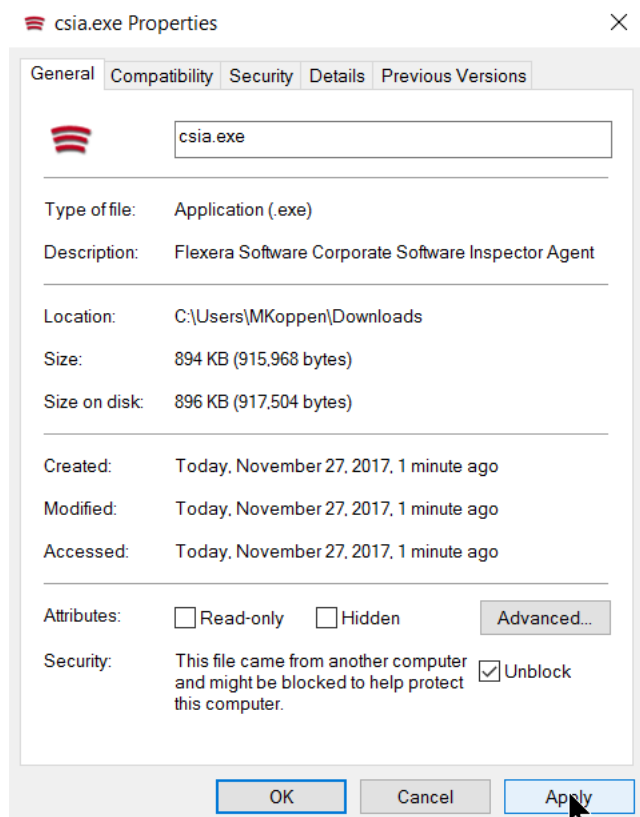
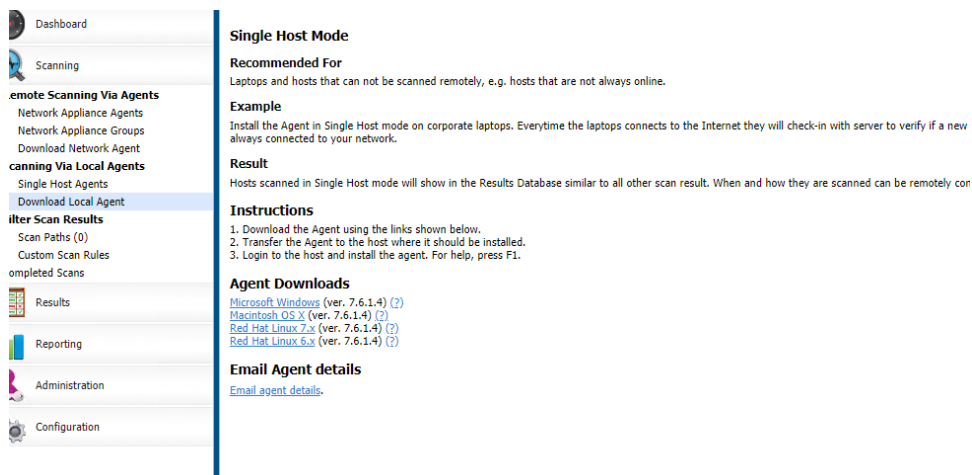
If your intention is to deploy the Software Vulnerability Manager Agent through WSUS/System Center please refer to [Agent Deployment](#) for further information.



Important • Ensure that the Agent (csia.exe) is available in a local folder on the target PC before installing.

Example

Install the csia.exe (Agent) in Single Host mode; download the Agent from the Software Vulnerability Manager console under Scanning > Scanning via Local Agents > Download Local Agent.



Note • Make sure to right click on the .exe in the deployment share to “Unblock” it. Click **Apply** > **OK**.

Once the Agent is installed, every time, for example, the laptop goes online (Internet connection) it will verify if a new scan should be conducted.

After scanning, the result will be displayed in **Scanning > Completed Scans** in the Software Vulnerability Manager console.



Important • When the Agent is installed a unique identifier is generated so that each Agent has its own unique ID. For this reason, the Agent should not be included in OS images. Doing so will result in having several instances of the same Agent and in the inability to correlate the scan results with the scanned hosts.

Result

Hosts scanned with the Agent in Single Host mode will be displayed in **Results > Host Smart Groups**.

When and how the hosts are scanned can be controlled from the Software Vulnerability Manager console under **Single Host Agents**. Right-click a host name and select **Edit Configuration** to change the Agent settings.

Install the Agent from the command prompt with Local Admin account using:

```
csia.exe -i -L
```

Example of an installation:

```
C:\Documents and Settings\Administrator>cd "%Program Files%\Secunia\CSI"
C:\Program Files\Secunia\CSI>csia.exe -i -L
Starting 'Secunia CSI Agent' service
'Secunia CSI Agent' service started
'Secunia CSI Agent' successfully installed
C:\Program Files\Secunia\CSI>
```

By using the **-L** parameter, the Agent will be installed as a service running under the LocalService user account. For further information, refer to:

<http://msdn.microsoft.com/en-us/library/windows/desktop/ms684190%28v=vs.85%29.aspx>

If you are a member of a domain and you do not use the **-L** switch, the service will be installed under the user account performing this action, granting the 'logon as a service' privilege.

However, this privilege is usually removed in the next GPO background refresh since domain policies will not allow it. As a consequence, the Agent will stop working after the privilege has been removed.

Refer to [Agent Deployment](#) to deploy the csia.exe through WSUS/System Center for further information of how to deploy the csia.exe via Group Policy.



Important • The csia.exe file is a customized executable, unique and private for your Software Vulnerability Manager account. This means that the csia.exe automatically links all scan results to your Software Vulnerability Manager account.

Once the Agent is installed it will automatically scan after ten minutes. You can also initiate an on demand scan by executing **csia.exe -c**.

Run Scan from System Center Configuration Manager (SCCM)

The Software Vulnerability Manager Agent does not have to be installed on the local host to do a scan. You can create a traditional package in SCCM and run the scan on a weekly basis. To do this, you first need to be able to connect to <your CSI on-prem server host name>.



Task

To run the Software Vulnerability Manager Agent inside an SCCM package:

1. Download the latest Software Vulnerability Manager Agent as per [Download Local Agent](#).
2. Launch the ConfigMgr console. Select **Software Library > Application Management > Packages**.
3. From the ribbon, click **Create Package**.
4. Complete the package information and click **Next**.

Create Package and Program Wizard

Package

Package

Program Type

- Standard Program
- Requirements
- Summary
- Progress
- Completion

Specify information about this package

Enter a name and other details for the new package. To take full advantage of new features that include the Application Catalog, use an application instead.

Name: Flexera CSI Scan Package

Description:

Manufacturer: Flexera

Language: ENG Version: 7.5.0.11

☒ This package contains source files

Source folder: \\scm16\Source\Packages\CSI_Agent [Browse...](#)

< Previous Next > Summary Cancel

5. On the **Program Type** page, ensure **Standard Program** is selected and click **Next**.
6. On the **Standard Program** page, configure the following settings and click **Next**.
 - Name: **CSI Scan**
 - Command Line: `csia.exe -c -v -d c:\windows\temp\csiscan.log` (creates a scan log file up to 16 MB in size)
 - Run: **Hidden**
 - Program can run: **Whether or not a user is logged on**

Create Package and Program Wizard

Standard Program

Specify information about this standard program

Package
Program Type
Standard Program
Requirements
Summary
Progress
Completion

Name: CSI Scan

Command line: csia.exe -c -v -d c:\windows\temp\csiscan.log Browse...

Startup folder:

Run: Hidden

Program can run: Whether or not a user is logged on

Run mode: Run with administrative rights

☐ Allow users to view and interact with the program installation

Drive mode: Runs with UNC name

☐ Reconnect to distribution point at log on

< Previous Next > Summary Cancel

7. On the **Requirements** page, complete the requirements as shown below and click **Next**.

Create Package and Program Wizard

Requirements

Specify the requirements for this standard program

Package
Program Type
Standard Program
Requirements
Summary
Progress
Completion

☐ Run another program first

Package: Browse...

Program:

☐ Always run this program first

Platform requirements

☒ This program can run on any platform

☐ This program can run only on specified platforms

☐ All Windows RT

☐ All Windows RT 8.1

☐ All Windows 10 (32-bit)

☐ All Windows 10 (64-bit)

☐ All Windows 7 (64-bit)

☐ All Windows 8 (64-bit)

☐ All Windows 8.1 (64-bit)

☐ Windows Embedded 8 Industry (64-bit)

☐ Windows Embedded 8 Standard (64-bit)

☐ Windows Embedded 8.1 Industry (64-bit)

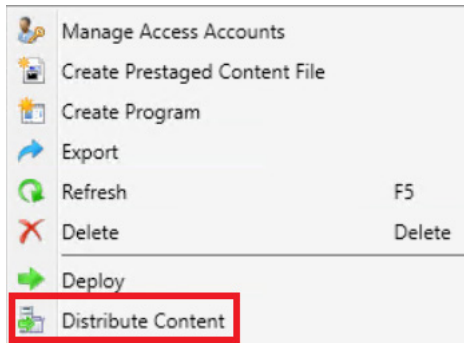
Estimated disk space: 2 MB

Maximum allowed run time (minutes): 60

< Previous Next > Summary Cancel

8. Finish the wizard.

9. Distribute the package to all Distribution Points or groups using the **Distribute Content** feature.



Task *To create the initial scan and the weekly reoccurring scan:*

1. Select the Package and click **Deploy** on the ribbon.
2. On the **General** page, select the target collection and click **Next**.
3. On the **Content** page, verify that the content is distributed and click **Next**.
4. On the **Deployment Settings** page, ensure the purpose is Required and click **Next**.
5. On the **Scheduling** page, in the Assignment schedule click **New**. Schedule a scan for as soon as possible and create a weekly scanning schedule. Also configure the Rerun behavior deployment to **Always rerun program**.

Deploy Software Wizard

Scheduling

General
Content
Deployment Settings
Scheduling
User Experience
Distribution Points
Summary
Progress
Completion

Specify the schedule for this deployment

This program will be available as soon as it has been distributed to the content servers unless it is scheduled for a later time below. For required applications, specify the assignment schedule.

☐ Schedule when this deployment will become available:
11/17/2017 10:01 AM UTC

☐ Schedule when this deployment will expire:
11/17/2017 10:01 AM UTC

Assignment schedule: New... Edit... Delete

As soon as possible
Occurs every 1 weeks on Friday effective 11/17/2017 10:02 AM

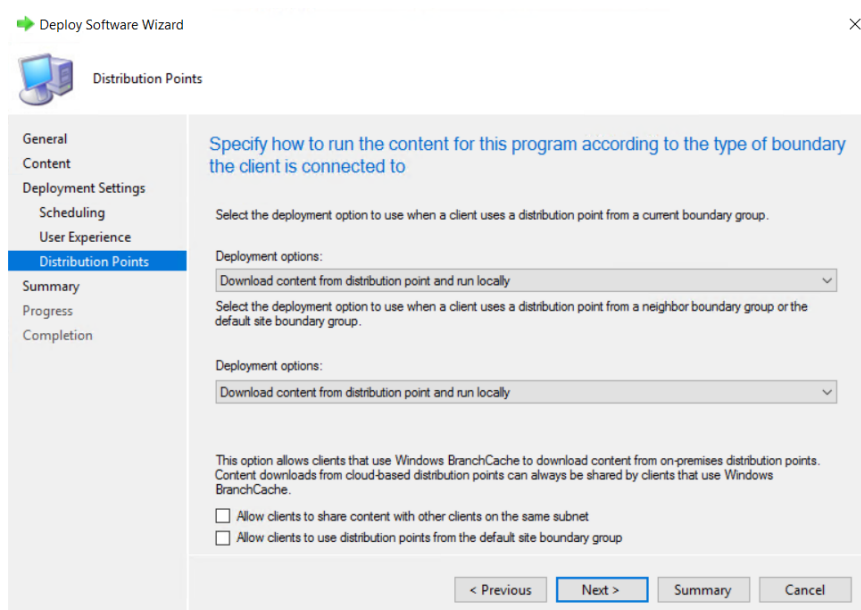
Rerun behavior: Always rerun program

< Previous Next > Summary Cancel



Tip • For larger environments, it is recommended to spread out the execution schedule of the scan package to avoid spikes of network traffic.

6. On the user **Experience** page, click **Next**.
7. On the user **Distribution Points** page, select **Download content**, and click **Next**.



8. Finish the wizard.

You can now monitor the scanning results from the Software Vulnerability Manager console.

Scanning Mac OS X

To scan Apple Mac OS X machines, you need to deploy the Single Host Agent locally on the target system.

The installation can only be done under the Mac Terminal, as the Agent will be installed as a daemon (service) under the LocalSystem account.

Installation of Local Services on Mac OS X systems requires root privileges. The 'root' account is disabled by default on Mac systems; therefore you need to enable it to proceed.

Before scanning Mac OS X machines, please see the following sections:

- [Download the Software Vulnerability Manager Agent for Apple Mac OS X](#)
- [Prepare Your Mac](#)
- [Install the Mac Agent](#)

Download the Software Vulnerability Manager Agent for Apple Mac OS X

The Software Vulnerability Manager Agent for Mac OS X (csia) is a small, simple, customizable and extremely powerful Software Vulnerability Manager scan engine that offers a fully featured command line interface (CLI) to the Software Vulnerability Manager scanning functionality.

This allows you to run Software Vulnerability Manager scans directly from the command line, or to launch scans by using the Software Vulnerability Manager console.

You can download the Agent binary under **Scanning > Scanning via Local Agents > Download Local Agents**.



Important • Ensure that the Agent is always available in a local folder on the target host.

Prepare Your Mac

Installation of daemons (services) on Mac OS X systems requires **root account** privileges. This means that root account should always be used when installing the Software Vulnerability Manager Agent.

You can switch to your local root account by using the command “**su root**” in your Mac Terminal. You will be prompted to provide the password for the root account.

```
bash-3.2$ su root
Password:
```

Provide the password for “**root**” if you know it. If you are not certain about the password, you may want to try entering ‘**toor**’, which is the default password for the root account, or you may also try with the current password of your Administrator account. Both ways may work, but if the account is disabled on the system, none of the passwords would work.



Important • The Terminal window will not display the password you typed in. Once you have entered the password correctly, press **ENTER** and wait for confirmation.

If you do not know the password for the root account, or the latter is currently disabled, you can perform the following actions to enable the account and set a new password:

- Open **Terminal**
- Type **sudo passwd root**
- Provide a new password

For more details on how to enable root account on Mac OS X systems, please refer to:

<http://support.apple.com/kb/ht1528>



Important • If you cannot enable the ‘**root**’ account on the Mac, or you prefer to not use it directly, you can alternatively use the “**sudo**” switch before each command associated with Agent activities. For example: “**sudo ./csia -i -L**” can be used to install the Agent on the system.

Once you are ready with setting/logging the root account you are one step away from installing the Agent.

When you download the Agent on a Mac system, normally the file is being set with limited file permissions on the system. You must check whether the file is allowed execution on the system by using the ‘**ls -l**’ command which will list the file and will show its file permissions.

```
-rwxr-xr-x 1 csc staff 803460 May 30 11:04 csia
-rwxr-xr-x@ 1 csc staff 803460 Jun 11 13:04 csia_csc50
```

In case the permissions do not include execute rights (the 'x' character) for any user, you should set them for the root account by using the **chmod +x** command.

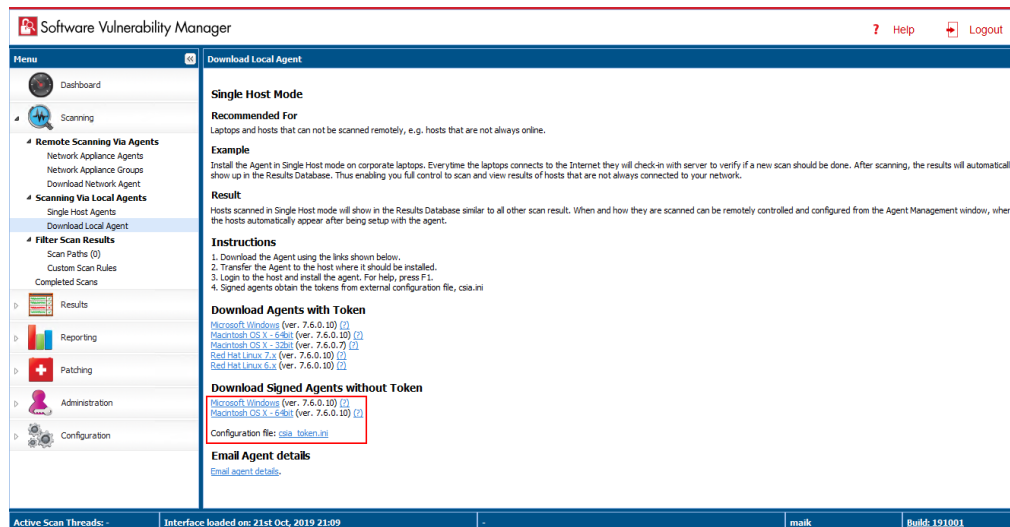
```
chmod +x csia
```

(If you are not using the root account, add **sudo** before **chmod**)



Note • For MacOS Catalina and Mojave note the following:

- In **Scanning > Scanning Via Local Agents > Download Local Agent**, download the disk image and *csia_token.ini*.



- Double-click the downloaded disk image to view the *csia* executable file.
- Drag & drop the *csia* executable file and *csia_token.ini* to your desired location to install the Mac agent.

Install the Mac Agent

The traditional way of installing the Software Vulnerability Manager Agent is as a daemon (similar to local service in Windows) as it will operate under the Mac OS X LocalSystem account.



Task

Install the binary by using the Mac Terminal services as follows:

1. Open **Terminal**:
 - `sudo su`
 - Pass: (Administrator password)
 - whoami (should be root)
2. Browse to the directory where you have placed the *csia* binary file:
 - `chmod +x csia`
 - Type the following command to install the Agent: `sudo ./csia -i`

```
CSC-Mac:Downloads csc$ sudo ./csia -i
[01/20 13:40:49.294] Initializing Flexera Software Corporate Software Inspector Agent 7.5.1.3
[01/20 13:40:49.311] GUID : F34D6E90-AFC4-401C-A687-4D3CAC380643
[01/20 13:40:49.318] 'com.secunia.csia' service started
[01/20 13:40:49.318] 'Corporate Software Inspector Agent' successfully installed
[01/20 13:40:49.318] Corporate Software Inspector Agent 7.5.1.3 shutting down
CSC-Mac:Downloads csc$
```

The Agent shows in the Software Vulnerability Manager console approximately 15 minutes after the installation.

Use the “-h” switch to see a full list of parameters supported by the Agent.

Scanning Red Hat Enterprise Linux (RHEL)

Red Hat Enterprise Linux (RHEL) 6 and 7 are the only operating systems officially supported by Flexera for the Software Vulnerability Manager RHEL scan Agent. It may be possible to install the scan Agent on operating systems and configurations other than those described. However, these have not been tested and are not supported by Flexera.

The scan Agent for RHEL uses the inventory which is already present (RPM) and displays this in the Software Vulnerability Manager after being processed by Flexera Detection/Version Rules. To download the Software Vulnerability Manager Agent for Red Hat Linux, go to **Scanning > Scanning via Local Agents > Download Local Agents**. For further information, see [Installing the Software Vulnerability Manager Agent for Red Hat Linux](#).

Installing the Software Vulnerability Manager Agent for Red Hat Linux



Note • This is a sample reference implementation that you can use to help guide your setup.

To install the Software Vulnerability Manager Agent for Red Hat Linux:

The RHEL 6 Agent requires: bash, gzip, sed, gawk, procs, coreutils, glibc(x86-32), libcurl(x86-32), libconfig(x86-32), libuuid(x86-32), yum, yum-security

The RHEL 7 Agent requires: bash, sed, gawk, procs, coreutils, glibc(x86-32), libcurl(x86-32), libconfig(x86-32), libuuid(x86-32), yum

Login as root at the RHEL machine and install/update the package (the same command line option works for both cases):

```
su root
yum localinstall --nogpgcheck <path>/csia_linux-7.x.x.xx-x.noarch.rpm
```

Specifying proxy settings for the scanner (recommended method):

You can update the proxy setting to override the environment variables:

Update the proxy setting in the configuration file /etc/csia/csia.conf

Login as root and restart the scanner service:

```
su root
service com.secunia.csia restart (RHEL 6)
```

OR

```
systemctl restart com.secunia.csia.service (RHEL 7)
```

Specifying the LAN Group of the machine:

This setting will be overridden if the DNS domain name of the machine is publicly available (check with the 'dnsdomainname' command).

Update the LanGroup setting in the configuration file `/etc/csia/csia.conf`.

Login as root and restart the scanner service:

```
su root  
service com.secunia.csia restart (RHEL 6)
```

OR

```
systemctl restart com.secunia.csia.service (RHEL 7)
```

Immediately update the RHEL Agent configuration:

If you have set the Agent check-in time to, for example, 1 day, it will be 1 day until the RHEL Agent picks up any configuration changes. If you want the RHEL Agent to immediately adapt to configuration changes, you can use the commands below to accomplish this by simply restarting the Agent service.

Login as root and restart the scanner service:

```
su root  
service com.secunia.csia restart (RHEL 6)
```

OR

```
systemctl restart com.secunia.csia.service (RHEL 7)
```

Uninstalling:

Login as root and uninstall the scanner RPM package:

```
su root  
rpm -e csia_linux
```

Filter Scan Results

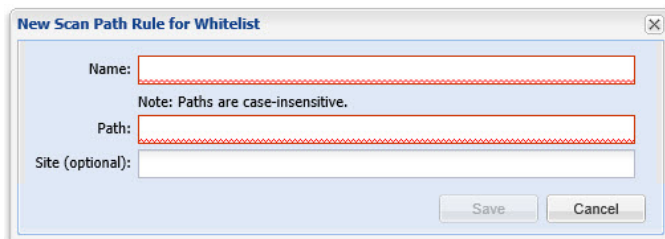
Software Vulnerability Manager has the following scan features to restrict the locations inspected by the scan and to create and maintain custom rules for scanning customer created programs, drivers, and plug-ins.

- [Scan Paths](#)
- [Custom Scan Rules](#)

Scan Paths

Use this feature to create either a Whitelist or Blacklist of paths/locations to restrict the locations inspected by the Software Vulnerability Manager scan.

Click **Add Whitelist Rule** or **Add Blacklist Rule** and enter the **Name**, **Path** and **Site (optional)** details.



Important • This feature is not applicable to RHEL.

If using the Whitelist, all the locations white-listed will be inspected by the scanner and any other locations are excluded from Software Vulnerability Manager inspections.

If using the Blacklist, all the locations/paths black-listed will be ignored and any other paths are inspected by the Software Vulnerability Manager scan.



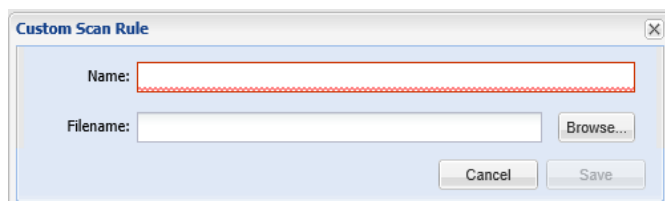
Important • Use this feature with **caution**. By using the Scan Path Rules some of your paths will be excluded from the scan and Software Vulnerability Manager will not alert you towards excluded insecure products, even if they potentially expose your hosts to security threats.



Important • It is not possible to simultaneously use both a Blacklist and a Whitelist.

Custom Scan Rules

Use the Custom Scan Rules page to create and maintain custom rules for scanning customer created programs, drivers, and plug-ins. Click **New Custom Scan Rule** and enter a **Name** for the rule and the **Filename** to scan. Click **Browse** to search for the file you want to add to the rule.



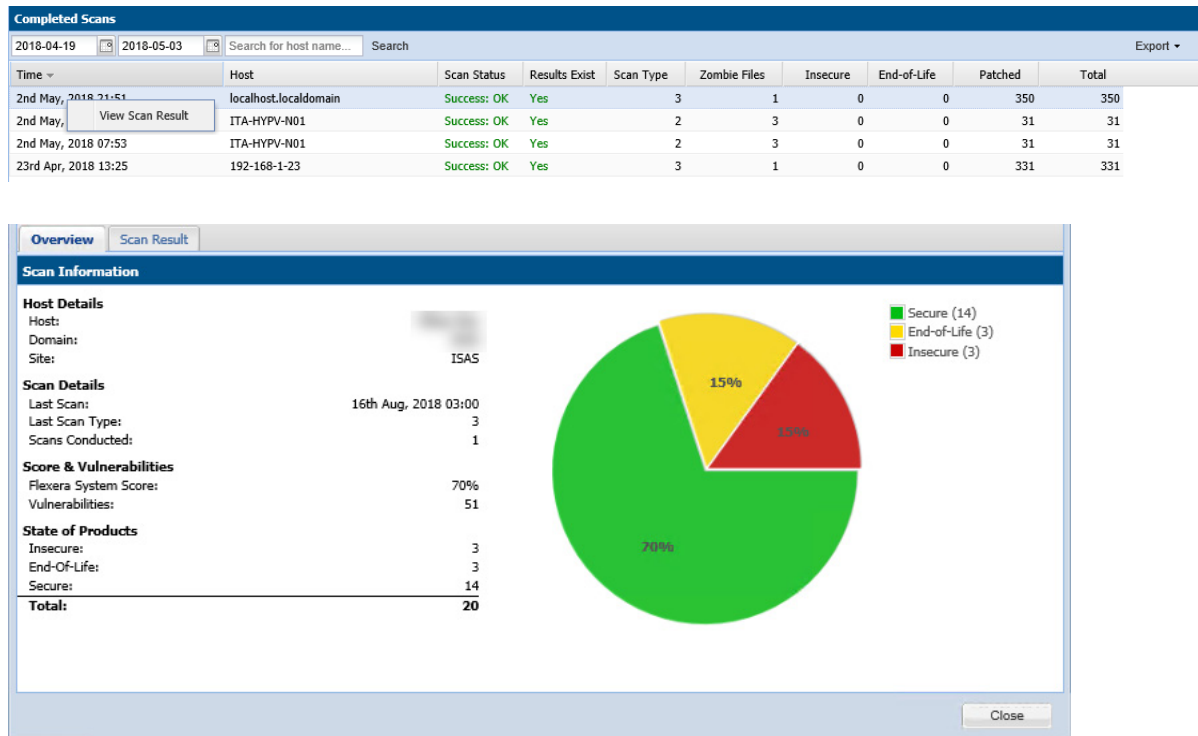
Right-click a rule in the grid to edit or delete the rule.



Important • The file to be scanned must contain valid File Version Information.

Completed Scans

Use this page to view a summary of the scans conducted. Double-click an entry for further details or right-click and select **View Scan Result**.



Scan Status:

Success

The scan was completed successfully.

Partial

The Software Vulnerability Manager scans consists of two parts; the first part is the scan of third-party applications, the second part is collecting information about Microsoft patching status from the Windows Update Agent (WUA).

If the Software Vulnerability Manager scan engine is not able to obtain the required information from the WUA, the scan result will be **Partial**. Check the setting that controls the behavior of the WUA when a scan is completed (refer to [Settings](#) for further information).

Failed

Software Vulnerability Manager was not able to connect to the remote target to perform the scan. Refer to [Remote/Agent-less Scan – Requirements \(Windows\)](#) for further information.

Possible Reasons for Scan Status

After you complete a scan, you will see a **Completed Scans** page. This page includes a **Scan Status** column. The following table explains the possible reasons for the Scan Status.

Table 6-3 • Possible Reasons for Scan Status

Scan Status	Possible Reasons
Success: OK	Scan executed successfully.
Partial Success	Scan executed with partial success.
Partial: Windows Update Failed	<p>The scan was partially successful. An error occurred during the Windows update check due to possibly one or all of the following reasons:</p> <ol style="list-style-type: none"> 1. It appears that the RPC service is not running or that the Host is firewalled to disallow access to the RPC service. 2. You do not appear to have specified the correct login credentials to perform Windows Update checks on the Host. 3. Check that the Windows Update service is running on the Host and that you use the correct administrative login credentials. <p>NOTE: This means that certain Microsoft products for this Host are listed with a potential incorrect security state.</p>
Failure	Scan failed.
Failed: License Limit Reached	<p>You have reached the limit of your CSI License Key. To resolve this issue:</p> <ol style="list-style-type: none"> 1. Please make sure that you have removed all retired machines from your CSI console using the database cleanup tool. 2. You may need to purchase more host licenses. Please contact sales@flexera.com for more licenses.
Failed: No Connection	Could not connect to Host. Check that the Host is not blocked by a firewall.
Failed: Resolving Host	Could not resolve Host. Please verify that you typed the host name correctly.
Failed: Access Denied	The scan failed. Please verify that you are using the correct administrative login credentials for the Host.
Failed: Error Connecting	Check that you have sufficient privileges to access the Host. Check that the Host is not blocked by a firewall.
Failed: Partial Success	<p>The scan started, but it could not be completed due to possibly one or all of the following reasons:</p> <ol style="list-style-type: none"> 1. Please verify that you are using the correct administrative login credentials for the Host. 2. 'Easy File Sharing' is disabled on the Host. 3. The Host is not blocked by a firewall.
Failed: No Data Retrieved	The scan started, but it could not be completed. Please verify that you are using the correct administrative login credentials for the Host. 'Easy File Sharing' is disabled on the Host. The Host is not blocked by a firewall.

Table 6-3 • (cont.)Possible Reasons for Scan Status

Scan Status	Possible Reasons
Failed: IP/AD Restrictions	The user who installed the agent on the specific machine is not allowed to scan a machine with that IP address.
Failed: Communications Error	There has been a communications error between the agent and the Host. This could be a temporary issue, so rescanning may resolve this issue.

7

Results

After scanning your system, you can use the following options to view your scan results:

- [Sites](#)
- [Smart Groups](#)
- [Host Smart Groups](#)
- [Product Smart Groups](#)
- [Advisory Smart Groups](#)

Sites

Use this page to view the Sites maintained within your account. You can double-click a Site name to see all the hosts grouped under that Site name.

Right-click a Site to view its Hosts or delete the Site.

Scanned hosts will be grouped in a Site with the same name as the domain they log on to.



Important • Switching to Active Directory will remove your current Sites structure (your existing data will be backed up).

Smart Groups

Smart Groups are the medium by which a Software Vulnerability Manager user views scan results. You are able to see the hosts, products, and associated advisories that are available to you, based on your view of the network as configured by your administrator. Furthermore, you are able to create custom filtered views of each of these using a variety of predefined criteria. The **All Hosts**, **All Products**, and **All Advisory** default Smart Groups are created by Flexera, and cannot be edited or deleted. They represent an unfiltered view for their respective content. Use the filters when creating additional Smart

Groups to effectively customize the data you are most interested in, and want to see, create reports on, receive alerts and notifications about, and see dashboard portlet data on. Smart Groups are the basis by which most data in Software Vulnerability Manager is viewed, and can be used effectively to optimize your workflow.



Note • Smart Groups are generated periodically, and the data you see is only as current as the last time the Smart Group was compiled. At any time you can queue the recompilation of a Smart Group to get the most current data.

Within the Smart Group grids, you can double-click to view/edit an existing group's configuration. Alternatively, right-click a Smart Group to view, edit, compile or delete the group.

Select a Smart Group and click **Queue For Compilation** to update the data and notifications for the group. The group will usually update within minutes.

Click **Create New Smart Group** to configure a new Smart Group. Click **+** and **-** to add or remove criteria.

Click **Templates**, where available, to open the Smart Group Example Use Cases page. Select an appropriate use case and click **Use Template** to populate the Smart Group Overview and Configuration page, which you can then edit to match your specific requirements.

Configure New Smart Group

Smart Group Name:

Description:

Business Impact:

Contains advisories that match of the following criteria:

Criteria

is

Customize Columns

An Advisory Smart Group's contents grid will always show the Secunia Advisory ID and Description for each entry. Use this form to control which additional columns are shown in the grid view. Mouseover a checkbox for the column description.

☒ Select All ☐ Select Custom

☒ Criticality ☒ Zero-Day ☒ Advisory Published ☒ Vulnerabilities ☒ Solution Status ☒ CVSS Base Score ☒ Attack Vector ☒ Impact ☒ Installations ☒ Products ☒ Hosts



Important • If you edit a configured Smart Group, all existing log files and notifications for the Smart Group will be deleted. New logs will be created after your changes have been saved.



Important • Content can be available in multiple Smart Groups at the same time. For example, if you have a Smart Group showing all insecure products and another showing all products from Adobe, then if a host has an Adobe product installed that is insecure, this will be displayed in both Smart Groups. Also note that when you first run a scan you won't see the hosts in All Hosts, or any reports, until the Smart Group is compiled.

Host Smart Groups

This section describes how to:

- View existing configured Host Smart Groups (see [Overview and Configuration](#))
- Configure new Host Smart Groups (see [Configured Host Smart Groups](#))
- Cross-Reference Host Smart Group Values - User Interface Versus CSV File (see)
- [Filter Host Smart Groups on missing Microsoft Knowledge Base \(KB\) articles](#)

Overview and Configuration

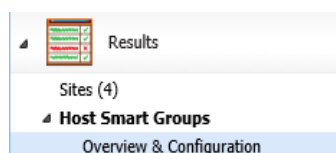
This page describes how to view existing configure Host Smart Groups and to configure new Host Smart Groups.



Task

To view the existing configured Host Smart Groups and configure new Smart Groups:

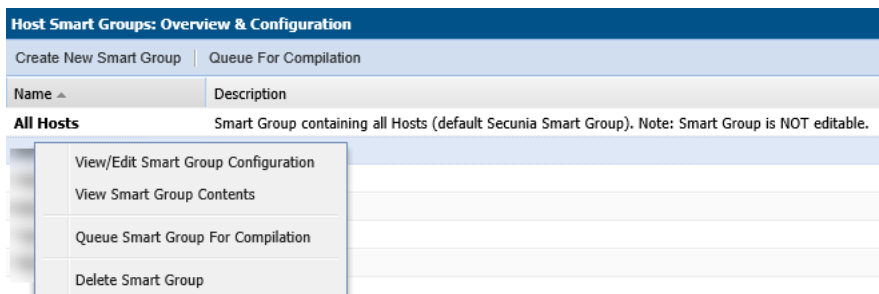
1. Navigate to Host Smart Groups Overview & Configuration.



2. Right-click an item in the grid to view, edit, compile or delete the Smart Group.
3. When the View/Edit Smart Group menu appears, make the needed changes to the Smart Group.



Note • All Hosts is the default Smart Group and cannot be edited or deleted.



Configured Host Smart Groups

Use this page to view the information for each Host Smart Group you created. Right-click an item in the grid to view the scan result or delete the selected host.

Smart Group: "All Hosts" - Last Compiled: 2018-04-18 14:55:19									
Host	System Score	Last Scan	Insecure	End-Of-Life	Patched	Total	Site Name	Scan Engine	Software Platform
QA_WINB1A	95%	5th Apr, 2018 07:08	8	7	78	93	SCOM	CSI 7.6.1.2	CSI Windows
QA_WINB1B		5th Apr, 2018 07:10	2	8	80	90	SCOM	CSI 7.6.1.2	CSI Windows
Mac		10th Apr, 2018 01:02	0	0	7	7	MacSite	Mac Agent 7.6.1.2	CSI Mac

Filter Host Smart Groups on missing Microsoft Knowledge Base (KB) articles

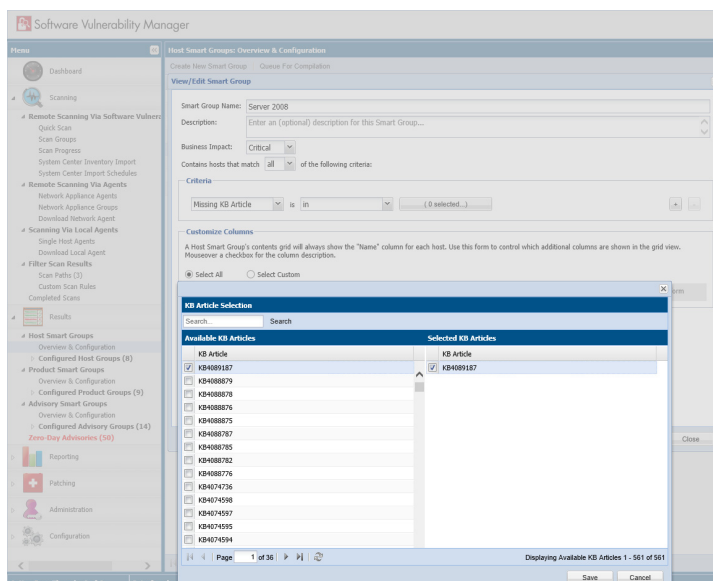
One option for filtering Host Smart Group information is by Microsoft KB articles to create a report of hosts that are missing one or several specific KB articles. This filtering can be used for new or existing Host Smart Groups.



Task

To create a new Host Smart Group for missing Microsoft KB articles:

1. Navigate to **Host Smart Groups Overview & Configuration**.
2. In the **Criteria** field, select the **Missing KB Article** and the appropriate **in** or **Not in** option.
3. In the **KB Article Selection**, search for the available KB articles.
4. Place a check mark in front of the appropriate KB article to include in the Host Smart Group and click **Save**.



Important • The following conditions affect the availability of selecting and listing missing Microsoft KB's.

- The selection of a particular KB in the **Available KB Articles** field is based on whether the PC's in the partition currently have a list of missing KB's.
- When a new KB is released, it will appear using the **in** criteria filter after the scan is completed. To include future KB's, use the **Not in** filter and choose the oldest **Available KB Articles** list.
- Only machines with missing KB's will be listed in the new host smart group. If a machine does not have any missing KB's, then the KB will not be listed in either the **in** or **Not in** filter.



Task

To create a report of missing Microsoft KB articles:

1. Navigate to the **Completed Scans** view.
2. Click **Export** to save the report as a CSV file.

Overview									
Scan Result									
Patch Information									
Patches Available									
Export									
<input type="checkbox"/> Patched <input checked="" type="checkbox"/> End-Of-Life <input checked="" type="checkbox"/> Insecure									
Name	Version	State	SAID	Criticality	CVSS Base Score	Issued	Vulnerabilities	Missing MS KB	
1Password 4.x	4.1.0.523	Insecure	SA73742		V2: 1.7	538 days ago	1		
7-zip 16.x	16.4.0.0	End-Of-Life	SA82839		V2: 10	6 days ago	1		
Adobe Flash Player 28.x	28.0.0.161 (IE)	End-Of-Life	SA82501		V2: 10	27 days ago	6		
Adobe Flash Player 28.x	28.0.0.161 (IE)	End-Of-Life	SA82501		V2: 10	27 days ago	6		
Cygwin 2.x	2.0.4	Insecure	SA76592		V2: 6.8	374 days ago	1		
Cygwin 2.x	2.0.4	Insecure	SA76592		V2: 6.8	374 days ago	1		
Microsoft Edge	11.0.14393.2007	Insecure	SA82473		V2: 10	27 days ago	10	4093119	
Microsoft Internet Explorer 11.x	11.0.14393.2007	Insecure	SA82459		V2: 10	27 days ago	13	4093119	
Microsoft Internet Explorer 11.x	11.0.14393.2007	Insecure	SA82459		V2: 10	27 days ago	13	4093119	
Microsoft Windows 10	Windows 10 Ent...	Insecure	SA82455		V2: 10	27 days ago	6	4093110,4093119	
Mozilla Firefox 57.x	57.0.4.6577	End-Of-Life	SA82228		V2: 10	42 days ago	1		
Node.js 4.x	4.4.3.0	Insecure	SA82116		V2: 7.8	46 days ago	1		
Node.js 6.x	6.4.0.0	Insecure	SA80411		V2: 6.4	150 days ago	1		
Oracle Java JRE 1.9.x / 9.x	9.0.0.0	End-Of-Life	-	-	-	-	-		
Pale Moon 27.x	27.5.1.6489	Insecure	SA80229		V2: 5	159 days ago	2		
Python 2.7.x	2.7.13150.1013	Insecure	SA77878		V2: 10	301 days ago	10		
Python 3.x	3.6.2150.1013	Insecure	SA80113		V2: 4.3	168 days ago	1		
Symantec Endpoint Protection...	14.0.2349.100	Insecure	SA79902		V2: 1.7	181 days ago	2		
Symantec Endpoint Protection...	14.0.2349.100	Insecure	SA79902		V2: 1.7	181 days ago	2		
Symantec Endpoint Protection...	14.0.2349.100	Insecure	SA79902		V2: 1.7	181 days ago	2		

Product Smart Groups

This section describes how to:

- View existing configured Product Smart Groups (see [Overview and Configuration](#))
- Configure new Product Smart Groups (see [Configured Product Smart Groups](#))

Overview and Configuration

Use this page to view the existing configured Product Smart Groups and to configure new Smart Groups. Right-click an item in the grid to view, edit, compile or delete the Smart Group. To filter Product Smart Groups by the Last Scan Date, see [Last Scan Date for Product Smart Groups](#).

All Products is the default Smart Group and cannot be edited or deleted.

The other default Smart Groups for End-Of-Life Products, Insecure Products, and Patched Products have been pre-created for you by Flexera. You can right-click to view, edit, compile or delete these Smart Groups.

Product Smart Groups: Overview & Configuration	
Create New Smart Group	Queue For Compilation
Name	Description
All Products	Smart Group containing all Products (default Flexera Smart Group). Note: Smart Group is NOT editable.
End-Of-Life Products	Smart Group containing End-Of-Life Products (default Flexera Smart Group).
Insecure Products	Smart Group containing Insecure Products (default Flexera Smart Group).
Patched Products	Smart Group containing Patched Products (default Flexera Smart Group).

View/Edit Smart Group Configuration

View Smart Group Contents

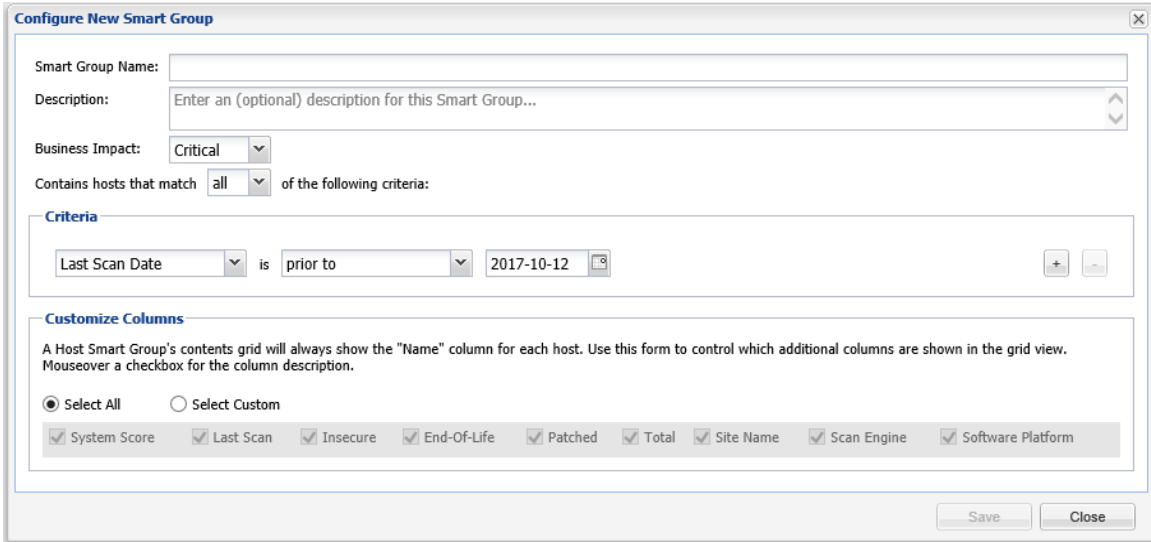
Queue Smart Group For Compilation

Delete Smart Group

Last Scan Date for Product Smart Groups

Product Smart Groups can be filtered by **Last Scan Date**. This filter option lists products that were detected within a specified time interval using one of the following Last Scan Date options: exactly, prior to, after, older than, and within last.

For example: if machine1 was scanned on 12 October 2017 and a product was detected, then the product will be a result when searched using a Last Scan Date greater than 11 October 2017.



Configure New Smart Group

Smart Group Name:

Description:

Business Impact: Critical

Contains hosts that match all of the following criteria:

Criteria

Last Scan Date is prior to 2017-10-12

Customize Columns

A Host Smart Group's contents grid will always show the "Name" column for each host. Use this form to control which additional columns are shown in the grid view. Mouseover a checkbox for the column description.

☒ Select All ☐ Select Custom

☒ System Score ☒ Last Scan ☒ Insecure ☒ End-Of-Life ☒ Patched ☒ Total ☒ Site Name ☒ Scan Engine ☒ Software Platform

Save Close

Configured Product Smart Groups

Use this page to view the information for each Product Smart Group you created. Right-click an item in the grid to display the installation details.

Smart Group: "All Products" - Last Compiled: 2018-04-18 14:55:19

Showing All Platforms

Product Name	Patch Version	SAID	Advisory Descrip...	Criticality
7-zip 16.x	-	-	-	-
accountsservice	-	-	-	-
acpid 1.x	-	-	-	-
Adobe Flash Player 14.x	29.x (NPAPI)	SA81973	Adobe Flash Pla...	5
Adobe Flash Player 26.x	29.x (IE)	SA81973	Adobe Flash Pla...	5
Adobe Flash Player 29.x	29.0.0.113 (NPA...	-	-	-
Adobe Flash Player 9.x	29.x (ActiveX)	SA81973	Adobe Flash Pla...	5

End-of-Life (EOL) products will not include Secunia Advisory IDs (SAID), as Flexera does not assign vulnerabilities to EOL products.

Smart Group: "End-Of-Life Products" - Last Compiled: 2018-07-23 10:00:27

Menu

Product Name	Patch Version	SAID	Advisory Descrip...	Criticality	CVSS Base Score	Vendor	Insecure	End-Of-Life
7-zip 16.x	18.x	-	-	-	-	-	0	5
Adobe Acrobat Reader 4.x	18.x (Continuous)	-	-	-	-	Adobe Systems	0	1
Adobe Flash Player 14.x	30.x (NPAPI)	-	-	-	-	Adobe Systems	0	1
Adobe Flash Player 23.x	30.x (IE)	-	-	-	-	Adobe Systems	0	2
Adobe Flash Player 25.x	30.x (NPAPI)	-	-	-	-	Adobe Systems	0	4
Adobe Flash Player 27.x	30.x (IE)	-	-	-	-	Adobe Systems	0	8
Adobe Flash Player 28.x	30.x (IE)	-	-	-	-	Adobe Systems	0	2
Adobe Flash Player 29.x	30.x (IE)	-	-	-	-	Adobe Systems	0	10
Adobe Flash Player 9.x	30.x (ActiveX)	-	-	-	-	Adobe Systems	0	1
Adobe Reader XI 11.x	18.x (Continuous)	-	-	-	-	Adobe Systems	0	5

Advisory Smart Groups

This section describes how to:

- View existing configured Advisory Smart Groups (see [Overview and Configuration](#))
- Configure new Advisory Smart Groups (see [Configured Advisory Smart Groups](#))

Overview and Configuration

Use this page to view the existing configured Advisory Smart Groups and to configure new Smart Groups. Right-click an item in the grid to view, edit, compile or delete the Smart Group.

All Advisories is the default Smart Group and cannot be edited or deleted.

For further details, see [View/Edit Smart Group Configuration](#).

Zero-Day Advisories reference a vulnerability that is actively exploited prior to its disclosure. These advisories can be filtered by **Advisories that Affected You** and **All Advisories**.

Menu		Zero-Day Advisories						
Dashboard		Scope of Data: <input checked="" type="radio"/> Advisories that Affected You <input type="radio"/> All Advisories						
Scanning		Zero-Day SAID	Advisory Description	Criticality	Advisory Published	Vulnerability	Affected Installations	Export
Results		SA79397	Microsoft Multiple Products Memory Corruption Vulnerability		10th Oct, 2017	1	1	
Sites (4)		SA78994	Microsoft .NET Framework Code Execution Vulnerability		12th Sep, 2017	1	15	
Host Smart Groups		SA76703	Microsoft Office Multiple Products Multiple Vulnerabilities		9th May, 2017	6	1	
Overview & Configuration		SA76672	Microsoft Internet Explorer Multiple Vulnerabilities		9th May, 2017	6	10	
Configured Host Groups (1)		SA76271	Microsoft Office Multiple Vulnerabilities		10th Apr, 2017	8	2	
All Hosts (9)		SA76226	Microsoft Internet Explorer Multiple Vulnerabilities		11th Apr, 2017	3	10	
Product Smart Groups		SA75547	Microsoft Internet Explorer Multiple Vulnerabilities		24th Feb, 2017	12	10	
Overview & Configuration		SA73948	Mozilla Firefox / Firefox ESR SVG Animation Use-After-Free Vulnerability		30th Nov, 2016	1	1	
Configured Product Groups (4)		SA72985	Microsoft Multiple Products RTF Memory Corruption Vulnerability		11th Oct, 2016	1	1	
All Products (474)		SA72977	Microsoft Products Multiple Vulnerabilities		11th Oct, 2016	8	26	
End-Of-Life Products (14)		SA72953	Microsoft Internet Explorer Multiple Vulnerabilities		11th Oct, 2016	10	10	
Insecure Products (48)		SA72380	Microsoft Internet Explorer Multiple Vulnerabilities		13th Sep, 2016	10	10	
Patched Products (41)		SA70398	Microsoft Internet Explorer Multiple Vulnerabilities		10th May, 2016	5	10	
Advisory Smart Groups		SA69989	Microsoft Windows Privilege Escalation and Pool Corruption Multiple Vulnerabilities		12th Apr, 2016	4	5	
Overview & Configuration		SA67695	Microsoft Windows Multiple Privilege Escalation Vulnerabilities		8th Dec, 2015	4	5	
Configured Advisory Groups (2)		SA67666	Microsoft Office Multiple Products Multiple Vulnerabilities		8th Dec, 2015	6	1	
Zero-Day Advisories (33)		SA66378	Microsoft Office Multiple Products Multiple Vulnerabilities		8th Sep, 2015	7	2	

View/Edit Smart Group Configuration

For each Smart Group, you can create or edit the advisory criteria using the Zero-Day Status and Advisory Published criteria. Both criteria include dates, which are created using the Coordinated Universal Time (UTC). Therefore, the local zone date of the user could be different from the zone the advisory data was saved in, which may lead to a difference in advisory lists.

In the **View/Edit Smart Group** menu, you can filter results by date for the following criteria: Advisory Published, Last Scan Date, and Secunia Advisory ID (SAID) Creation Date. This filtering by date creates a list of all Advisories published on that date.

View/Edit Smart Group

Smart Group Name: April

Description: Enter an (optional) description for this Smart Group...

Business Impact: Critical

Contains advisories that match all of the following criteria:

Criteria

Advisory Published is after 2015-04-01

Advisory Published is prior to 2015-07-10

Customize Columns

An Advisory Smart Group's contents grid will always show the Secunia Advisory ID and Description for each entry. Use this form to control which additional columns are shown in the grid view. Hoverover a checkbox for the column description.

Select All

Select Custom

☒ Criticality
 ☒ Zero-Day
 ☒ Advisory Published
 ☒ Vulnerabilities
 ☒ Solution Status
 ☒ CVSS Base Score
 ☒ Attack Vector
 ☒ Impact
 ☒ Installations
 ☒ Products
 ☒ Hosts

Save Close

88

SVMOP- MARCH2020-UG00 Software Vulnerability Manager (On-Premises Edition) User Guide

Configured Advisory Smart Groups

Use this page to view the information for each Advisory Smart Group you created. Click a Secunia Advisory ID (**SAID**) in the grid to display the details. For further details, see [View All Advisories](#).

Smart Group: "All Advisories" - Last Compiled: 2018-04-18 14:55:20		
SAID	Advisory Description	Criticality
SA81973	Adobe Flash Player Multiple Vulnerabilities	
SA81606	Adobe Reader / Acrobat Multiple Vulnerabili...	
SA80028	Adobe Shockwave Player Memory Corruptio...	
SA79744	Apache OpenOffice Multiple Vulnerabilities	

View All Advisories

Under the **Configured Advisory Group** view is a listing of All Advisories. For each advisory, you can click the corresponding number listed in the **Installations**, **Products**, and **Hosts** columns. After clicking the number in the **Installations** column, you will see a list of affected installations per host.

Smart Group: "All Advisories" - Last Compiled: 2018-05-03 0:33:19												
SAID	Advisory Description	Criticality	Zero-Day	Advisory Published	Vulnerability	Solution Status	CVSS Base Score	CVSS2 Base Score	CVSS3 Base Score	Attack Vector	Impact	Export
SA75828	WinSCP Protocol Handler Command Line Sw...		No	14th Sep, 2007	1	-	-	0	0	-	undefined	1 1 1
SA75725	Python "purple_markup_unescape_entity(7"		No	10th Mar, 2017	1	-	-	0	0	-	undefined	1 1 1
SA78029	Mozilla Firefox Multiple Vulnerabilities		No	9th Aug, 2017	28	Unpatched	V2: 10	10	0	From Remote	undefined, Security Bypass, Cro	1 1 1
SA78329 Affected Installations												
Product												
Version												
Host												
Mozilla Firefox 54.x												
54.0.1.6388												
Page 1 of 1												
Displaying Installations Affected By Advisory 1 - 1 of 1												
Close												

The All Advisories list affecting a product shows all current and past advisories that affect a product. Note that the Secunia Advisory ID number (SAID) listed under the **SAID** column could be related to different platforms.

Smart Group: "All Advisories" - Last Compiled: 2018-05-03 0:33:19												
SAID	Advisory Description	Criticality	Zero-Day	Advisory Published	Vulnerability	Solution Status	CVSS Base Score	CVSS2 Base Score	CVSS3 Base Score	Attack Vector	Impact	Export
SA75732	1Password Process Authentication Security...		No	15th Nov, 2016	1	Vendor Patched	V2: 10	10	0	From Remote	Denial of Service	1 1 1
SA75836	7-zip FPS and VOP File Handling Type Value...		No	10th May, 2016	2	Unpatched	V2: 10	10	0	From Remote	Denial of Service	1 1 1
SA80839	7-zip Memory Corruption Vulnerability		No	1st May, 2018	1	Vendor Patched	V2: 10	10	0	From Remote	Denial of Service	1 1 1
SA78208	Adobe Acrobat / Reader X2 Desktop Multiple...		No	11th Apr, 2017	47	-	-	-	-	-	-	1 1 1
SA78480	Adobe Flash Player / AIR Multiple Code Exe...		Yes	10th May, 2016	30	Vendor Patched	V2: 10	10	0	From Remote	System Access	1 1 1
SA78480 Affected Products												
Product												
Adobe AIR 3.x												
Adobe AIR 3.1.x												
View from the context of Smart Group: All Products												
Overview												
Installations												
All Advisories												
SAID	Advisory	Criticality	Advisory Publish.	Solution Status	Attack Vector	Zero Day	CVSS Base Score	CVSS2 Base Score	CVSS3 Base Score	Attack Vector	Impact	Export
SA55262	Adobe		2014-01-14	Unpatched	From remote	No	V2: 5	5	0	From Remote	Denial of Service	1
SA55049	Adobe		2013-12-10	Vendor Patched	From remote	No	V2: 10	10	0	From Remote	Denial of Service	2
SA55272	Adobe		2013-11-12	Vendor Patched	From remote	No	V2: 10	10	0	From Remote	Denial of Service	2
SA55592	Adobe		2013-09-10	Vendor Patched	From remote	No	V2: 10	10	0	From Remote	Denial of Service	4
SA55325	Adobe		2013-07-09	Vendor Patched	From remote	No	V2: 10	10	0	From Remote	Denial of Service	3
SA55251	Adobe		2013-06-11	Vendor Patched	From remote	No	V2: 10	10	0	From Remote	Denial of Service	1
SA55318	Adobe		2013-05-15	Vendor Patched	From remote	No	V2: 10	10	0	From Remote	Denial of Service	13
SA55251	Adobe		2013-04-09	Vendor Patched	From remote	No	V2: 10	10	0	From Remote	Denial of Service	4
SA55296	Adobe		2013-03-12	Vendor Patched	From remote	No	V2: 10	10	0	From Remote	Denial of Service	4
SA55166	Adobe		2013-02-12	Vendor Patched	From remote	No	V2: 10	10	0	From Remote	Denial of Service	17
SA55273	Adobe		2013-01-08	Vendor Patched	From remote	No	V2: 10	10	0	From Remote	Denial of Service	1
SA55166	Adobe		2012-12-12	Vendor Patched	From remote	No	V2: 10	10	0	From Remote	Denial of Service	3
SA55123	Adobe		2012-11-07	Vendor Patched	From remote	No	V2: 10	10	0	From Remote	Denial of Service	7
SA55176	Adobe		2012-10-09	Vendor Patched	From remote	No	V2: 10	10	0	From Remote	Denial of Service	29
Page 1 of 2												
Displaying advisories 1 - 15 of 18												
Close												

8

Reporting

This chapter describes the following Software Vulnerability Manager reporting features:

- [Report Configuration](#)
- [Smart Group Notifications](#)
- [Database Access](#)
- [Scheduled Exports](#)

Report Configuration

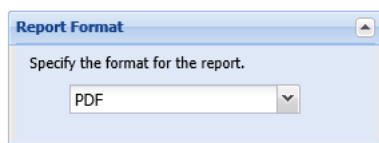
Use this page to view a list of reports that have been configured and scheduled for generation. You can configure a new report by clicking **Generate New Report** or right-click an existing report to view, edit or delete it. The Software Vulnerability Manager reporting capabilities allow the user to schedule and fully customize the intended report.



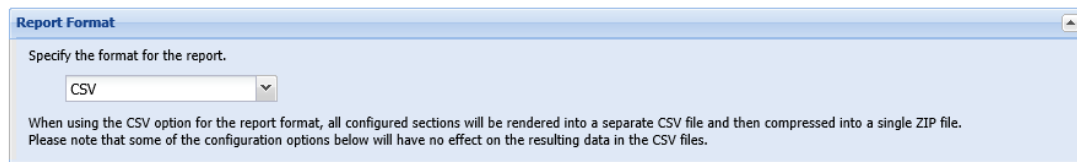
Task

To configure a report:

1. Choose between PDF and CSV as the format for the report.



2. When using the CSV option for the report format, all configured sections will be rendered into a separate CSV file and then compressed into a single ZIP file. Please note that some of the configuration options below will have no effect on the resulting data in the CSV files (CSV reports are Host Level Statistics and Product Level Statistics).



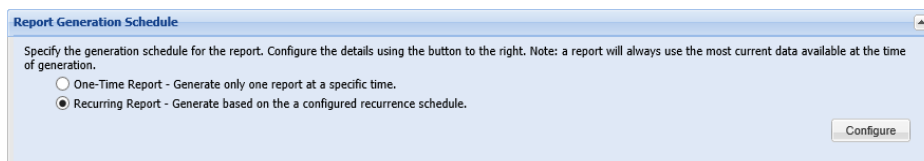
Report Format

Specify the format for the report.

CSV

When using the CSV option for the report format, all configured sections will be rendered into a separate CSV file and then compressed into a single ZIP file. Please note that some of the configuration options below will have no effect on the resulting data in the CSV files.

3. Choose between a One-time only report or a recurring one (daily, weekly, monthly) and click **Configure** to select the report distribution date or frequency schedule.



Report Generation Schedule

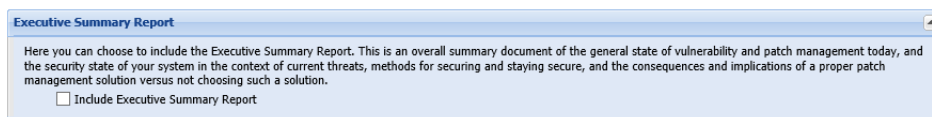
Specify the generation schedule for the report. Configure the details using the button to the right. Note: a report will always use the most current data available at the time of generation.

☐ One-Time Report - Generate only one report at a specific time.

☒ Recurring Report - Generate based on the a configured recurrence schedule.

Configure

4. Choose to include the Executive Summary Report which provides an overall summary with the general state of vulnerability and patch management.

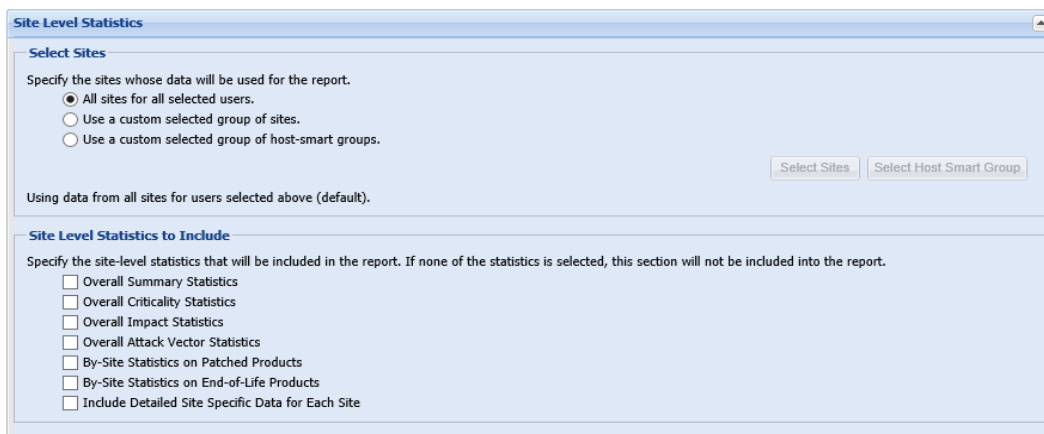


Executive Summary Report

Here you can choose to include the Executive Summary Report. This is an overall summary document of the general state of vulnerability and patch management today, and the security state of your system in the context of current threats, methods for securing and staying secure, and the consequences and implications of a proper patch management solution versus not choosing such a solution.

☐ Include Executive Summary Report

5. Choose which sites should be included together with which statistics to include.



Site Level Statistics

Select Sites

Specify the sites whose data will be used for the report.

☒ All sites for all selected users.

☐ Use a custom selected group of sites.

☐ Use a custom selected group of host-smart groups.

Select Sites Select Host Smart Group

Using data from all sites for users selected above (default).

Site Level Statistics to Include

Specify the site-level statistics that will be included in the report. If none of the statistics is selected, this section will not be included into the report.

☐ Overall Summary Statistics

☐ Overall Criticality Statistics

☐ Overall Impact Statistics

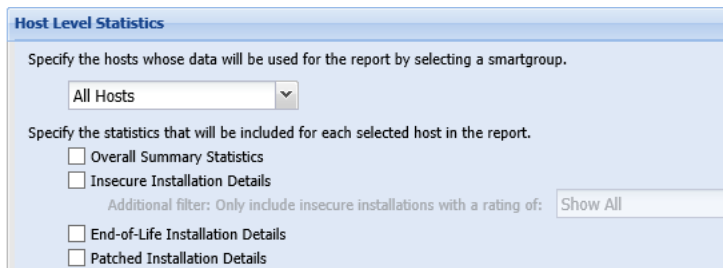
☐ Overall Attack Vector Statistics

☐ By-Site Statistics on Patched Products

☐ By-Site Statistics on End-of-Life Products

☐ Include Detailed Site Specific Data for Each Site

6. Choose a Host Smart Group to be included together with which statistics to include.



Host Level Statistics

Specify the hosts whose data will be used for the report by selecting a smartgroup.

All Hosts

Specify the statistics that will be included for each selected host in the report.

☐ Overall Summary Statistics

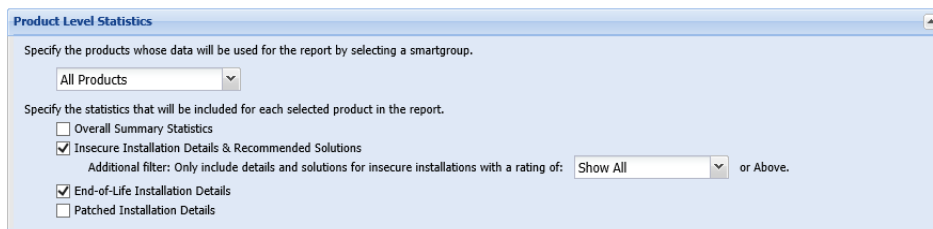
☐ Insecure Installation Details

Additional filter: Only include insecure installations with a rating of: Show All

☐ End-of-Life Installation Details

☐ Patched Installation Details

7. Choose a Product Smart Group to be included together with which statistics to include.



Product Level Statistics

Specify the products whose data will be used for the report by selecting a smartgroup.

All Products

Specify the statistics that will be included for each selected product in the report.

☐ Overall Summary Statistics

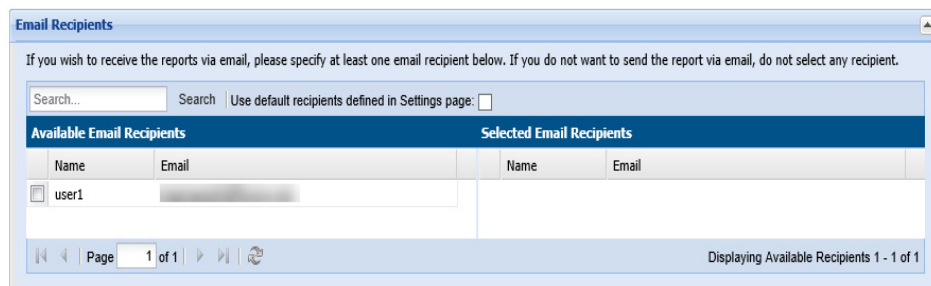
☒ Insecure Installation Details & Recommended Solutions

Additional filter: Only include details and solutions for insecure installations with a rating of: Show All or Above.

☒ End-of-Life Installation Details

☐ Patched Installation Details

- Choose the email address of the person(s) receiving the report or, if you do not want to send the report via email, do not select any recipients.



Email Recipients

If you wish to receive the reports via email, please specify at least one email recipient below. If you do not want to send the report via email, do not select any recipient.

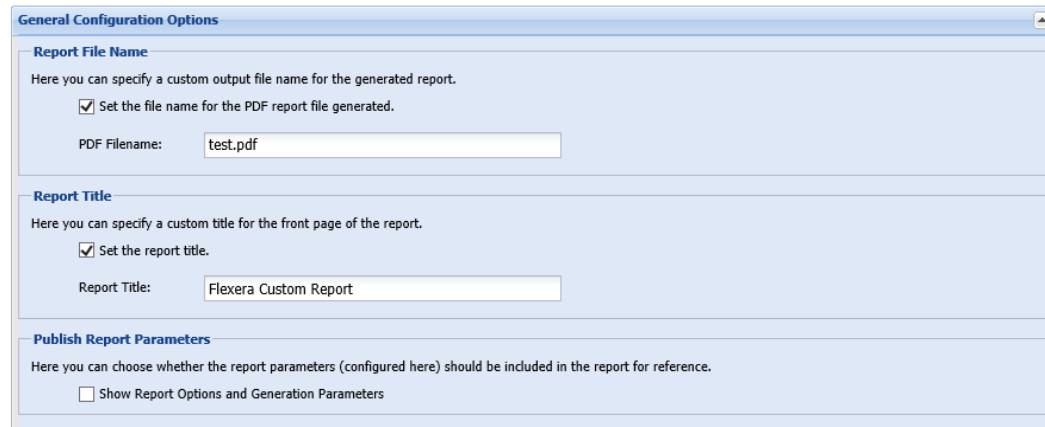
Search... Search Use default recipients defined in Settings page: ☐

Available Email Recipients		Selected Email Recipients	
Name	Email	Name	Email
<input checked="" type="checkbox"/> user1			

Page 1 of 1

Displaying Available Recipients 1 - 1 of 1

- Choose the name for the PDF file, set the report title, and specify if you would like to include the report parameters in the report itself. All the reports available through this feature are provided in a PDF format and will be emailed to the defined email addresses in accordance with the schedule and recurrence specified. Once generated, a report can also be downloaded directly from the main page.



General Configuration Options

Report File Name

Here you can specify a custom output file name for the generated report.

☒ Set the file name for the PDF report file generated.

PDF Filename: test.pdf

Report Title

Here you can specify a custom title for the front page of the report.

☒ Set the report title.

Report Title: Flexera Custom Report

Publish Report Parameters

Here you can choose whether the report parameters (configured here) should be included in the report for reference.

☐ Show Report Options and Generation Parameters



Important • The emails containing the PDF reports will be sent by your configured mail server. The mail server must be configured before users receive the PDF reports.

Smart Group Notifications

Use this page to create and configure reminders, notifications, and alerts for a Smart Group based on the current state or changes to a group.

Click **Configure New Notification**, enter the required information and then click **Save**.

Configure New Notification

Notification Details

Name & Applicability

You must give this notification a name (or short description) to be used when receiving alerts. Here you will also select the Smart Group for which the notification will apply.

Name: Smart Group:

Alerting Conditions

Choose the conditions under which you will receive an Alert.

ALERT me when the

How often should this notification rule run? Period is based on when the rule is saved/modified:

☐ NOTIFY me (email only) when the alert conditions are NOT met. I.e., leave unchecked for a 'no news is good news' policy.

Recipients Selection

Select email recipients:

Search ☐ Use default recipients defined in Settings page:

Available Email Recipients		Selected Email Recipients	
Name	Email	Name	Email
<input type="checkbox"/> user1			

Page 1 of 1

Displaying Available Recipients 1 - 1 of 1

Save Close

Database Access

- To access Flexera's SQL database, see [Database Console](#).
- To delete hosts from your Software Vulnerability Manager account by configuring rules that check for certain criteria, see [Database Cleanup](#).

Database Console

Use this page to access Flexera's SQL database. You can access the content of each table by selecting the table name in the **Tables** pane. Expand the table name to view the objects and data types within that table.

To create an SQL query, right-click a table and select **Show Data** to automatically create a **SELECT * FROM** table query from the specific table. You can also right-click a table and select **Schedule Query** to create [Scheduled Exports](#) for the table and save the output to a CSV file.

The **Details** and **Results** panes display the status of the query.

The screenshot shows the Database Console interface. On the left, a tree view lists various tables under the 'base_csi_smartgroup' folder. The 'Details' pane on the right shows a query executed at 16:11:23 with a status of 'Success'. The query is 'SELECT * FROM base_csi_smartgroup_products_1_3;'. Below this, the 'Results' pane displays a table with 10 columns: csi_device_soft..., nsi_device_id, software_inspec..., product_id, soft_type, insecure, eol, patched, custom_id, and an 'Export' button. The table contains 5 rows of data.

csi_device_soft...	nsi_device_id	software_inspec...	product_id	soft_type	insecure	eol	patched	custom_id
1231	2	21	37734	2	0	1	0	
1232	2	21	37734	2	0	1	0	
1241	2	21	42778	2	0	1	0	
1267	2	21	58445	2	0	1	0	
1282	2	21	60072	2	0	1	0	

Database Cleanup

Use this page to delete hosts from your Software Vulnerability Manager account by configuring rules that check for certain criteria.

You can use this page, for example, to delete all the hosts that have not been scanned for more than 15 days.

Click **Add Rule**, enter the required information and click **Save**.

The 'New Rule' dialog box is shown. It has fields for 'Action' (Delete Host), 'Name' (15 Days Rule), and 'Criterion' (Last Scan Time). There is a dropdown for 'More than' with the value '15' and a unit dropdown set to 'Days'. A 'Save' button is visible at the bottom right.

The rules can be based on **Last Scan Time**, **Last Check-in Time** or for Host that have been **Never Scanned**. Once a rule has been configured you can see which **Affected Hosts** meet the criteria defined in the rule and will be deleted from your Software Vulnerability Manager account.

Once you have checked the hosts to be deleted you can choose to run the rule. Right-click the rule name and select **Execute Rule**.

The screenshot shows the 'Database Cleanup' page with a table of rules. The table has columns for 'Name' and 'Action'. A right-click context menu is open over the '15 Days Rule' entry, showing 'Execute Rule' and 'Delete Rule' options.

Database Cleanup	
Rules	
Add Rule	
Name	Action
15 Days Rule	Execute Rule Delete Rule

Scheduled Exports

Use this page to view, edit or delete automated data extraction schedules.

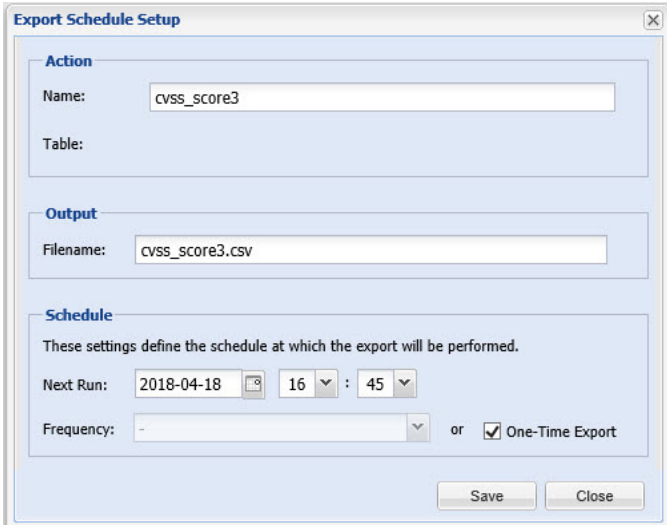


Important • To schedule exports you must first download and install the Software Vulnerability Manager Daemon from <https://secuniaresearch.flexerasoftware.com/support/download/>.

Right-click a table in the Database Console and select **Schedule Query**. You can configure the file by hiding columns in the grids prior to export.

In the Export Schedule Setup screen, enter:

- The **Name** of the scheduled export.
- The **Filename** that you want to save the CSV file as.
- The **Next Run** date and time.
- The **Frequency** (Hourly, Daily, Weekly or Monthly) that the export will be performed or select the **One-Time Export** check box.



The image shows a screenshot of the 'Export Schedule Setup' dialog box. It has three main sections: 'Action', 'Output', and 'Schedule'. In the 'Action' section, the 'Name' field is set to 'cvss_score3' and the 'Table' field is empty. In the 'Output' section, the 'Filename' field is set to 'cvss_score3.csv'. In the 'Schedule' section, there is a note: 'These settings define the schedule at which the export will be performed.' The 'Next Run' is set to '2018-04-18' with a calendar icon, followed by a time picker showing '16' and '45'. The 'Frequency' is set to '-' with a dropdown arrow. There is a checkbox for 'One-Time Export' which is checked. At the bottom right are 'Save' and 'Close' buttons.

Right-click a Scheduled Export in the grid to edit or delete the export.

9

Patching

After scanning your system and analyzing the appropriate vulnerabilities to patch, the next step is to patch your system. The following topics describe how to configure and deploy Software Vulnerability Manager's patching function.

- [Flexera Package System \(SPS\)](#)
- [Creating a Patch with the Flexera Package System \(SPS\)](#)
- [The SPS Package Creation Wizard](#)
- [Vendor Patch Module](#)
- [Agent Deployment](#)
- [WSUS/System Center](#)
- [Creating the WSUS-CSI GPO Manually](#)
- [Deploying the Update Package Using WSUS](#)
- [Deploying the Update Package Using System Center](#)
- [Patch Configuration](#)
- [Patch Template](#)
- [Patch Automation](#)

Flexera Package System (SPS)

This section provides further information regarding:

- [Flexera SPS Page Features](#)
- [SPS Concepts and Terminology](#)

Flexera SPS Page Features

The **Flexera Package System (SPS)** page displays a list of products for which Software Vulnerability Manager can automatically create an Update/Uninstall package. Right-click any of the listed products to view the available options.

Flexera Package System (SPS)												
Search View from the context of Smart Groups All Products Configure View New Custom Package Export												
Product	Vendor	Patched Version	Architecture	SAID	Criticality	Detected	Insecure	End-Of-Life	Patched	Total	Hosts	Uninstallable
7-zip		18.x	Windows64-bit	SA82839		1 day, 4 hours a...	0	2	0	2	2	No
7-zip 9.x		18.x	Windows32-bit	SA82839		5 months ago	0	2	0	2	2	No
Calibre 2.x		3.x	Windows64-bit	SA81916		36 days ago	0	2	0	2	2	No
eMule Plus 1.x		1.2.5.0	Windows32-bit	SA34799		36 days ago	1	0	0	1	1	Yes
FileZilla 3.x		3.21.0	Windows32-bit	SA72252		5 months ago	1	0	0	1	1	Yes
Adobe Acrobat DC 15.x	Adobe Systems	2015.006.30413 (Cl...	Windows32-bit	SA81606		3 months ago	1	0	0	1	1	No
Adobe Acrobat Reader DC	Adobe Systems	18.x (Continuous)	Windows32-bit	SA81606		36 days ago	5	14	0	19	19	No
Adobe Acrobat Reader DC 15.x	Adobe Systems	2015.006.30413 (Cl...	Windows32-bit	SA81606		3 months ago	1	0	0	1	1	No
Adobe Flash Player	Adobe Systems	29.x (ActiveX)	Windows32-bit	SA82501		36 days ago	0	3	0	3	3	No
Adobe Flash Player	Adobe Systems	29.0.0.140 (NPAPI)	Windows32-bit	SA82501		35 days ago	10	4	0	14	14	No
Adobe Shockwave Player 12.x	Adobe Systems	12.3.1.201	Windows32-bit	SA80028		36 days ago	11	0	0	11	11	No
Apple iTunes	Apple	12.7.4	Windows32-bit	SA82742		36 days ago	5	0	0	5	5	No
Google Chrome	Google	66.x	Windows64-bit	SA82905		35 days ago	1	8	0	9	9	No
Google Chrome	Google	66.x	Windows32-bit	SA82905		36 days ago	0	13	0	13	13	No
GTK 2.x	Kernel.org	2.14.2	Windows64-bit	SA79072		4 months ago	2	0	0	2	1	No
Mozilla Firefox	Mozilla Foundation	59.0.2	Windows64-bit	SA82228		36 days ago	4	3	0	7	7	Yes
Mozilla Firefox	Mozilla Foundation	59.0.2	Windows32-bit	SA82228		35 days ago	12	24	0	36	33	Yes
Mozilla SeaMonkey 1.1.x	Mozilla Foundation	2.x	Windows32-bit	SA81634		36 days ago	0	1	0	1	1	Yes
Mozilla Thunderbird 52.x	Mozilla Foundation	52.7	Windows32-bit	SA82157		36 days ago	15	0	0	15	15	No
Oracle Java JDK	Oracle Corporation	8u171	Windows64-bit	SA82703		36 days ago	7	1	0	8	8	No
Oracle Java JDK	Oracle Corporation	8u171	Windows32-bit	SA82703		36 days ago	6	1	0	7	7	No
Oracle Java JRE	Oracle Corporation	8u171	Windows32-bit	SA82703		36 days ago	6	1	0	7	7	No
Oracle Java JRE 1.8.x / 8.x	Oracle Corporation	8u171	Windows64-bit	SA82703		1 day, 4 hours a...	8	0	0	8	8	No
LibreOffice 5.x	The Document Found...	5.4.6	Windows32-bit	SA82719		36 days ago	1	0	0	1	1	No
VLC Media Player 2.x	VidoolAN	2.2.7	Windows64-bit	SA80098		6 months ago	3	0	0	3	3	No
VLC Media Player 2.x	VidoolAN	2.2.7	Windows32-bit	SA80098		36 days ago	5	0	0	5	5	No

The **Flexera Package System (SPS)** features include:

- Product display criteria for SPS
- Language selection for SPS
- Patch update searches by Common Vulnerabilities and Exposures (CVE)
- Advisory Published date

Product display criteria for SPS

Click Configure View to select the criteria that will be used to display the products in this view.

Configure View

You can customize the view of the products displayed using the following configurable options:

☒ Group products where patched version and architecture are identical

☒ Display only End-of-Life or Insecure products

☒ Display only products for which silent update packages can be created automatically

☐ Hide Microsoft products

☐ Highlight products for which update packages have been created

Note: The Software Vulnerability Manager should not be used for creating patches for Microsoft products. The updates should come from Microsoft.

Apply Cancel

When the Group products where patched version and architecture are identical check box is selected, the SPS page rows will be grouped by the product, architecture, and the patch required to update them to a secure version.

If a row represents two or more product versions that require the same update, then the Product column will not show the product version. For example, if Firefox 32.x and Firefox 37.x both require updating to patched version 40.x, then the Product column will display “Firefox” only.

This means that if, for example, four products previously required the same update, rather than listing them four times they will be listed once. This allows you to create fewer packages to target the same number of installations.

Product	Vendor	Patched Version	Architecture	SAID	Criticality	Detected	Insecure	End-Of-Life	Patched	Total	Hosts	Uninstallable
7-zip		18.x	Windows64-bit	SA82839		1 day, 4 hours a...	0	2	0	2	2	No
7-zip 6.x		18.x	Windows32-bit	SA82839		5 months ago	0	2	0	2	2	No
Calibre 2.x		3.x	Windows64-bit	SA81916		36 days ago	0	2	0	2	2	No
eHole Plus 1.x		1.2.5.0	Windows32-bit	SA34729		36 days ago	1	0	0	1	1	Yes
FileZilla 3.x		3.21.0	Windows32-bit	SA77252		5 months ago	1	0	0	1	1	Yes
Adobe Acrobat DC 15.x	Adobe Systems	2015.006.30413 (Cl...	Windows32-bit /...	SA81606		3 months ago	1	0	0	1	1	No
Adobe Acrobat Reader DC	Adobe Systems	18.x (Continuous)	Windows32-bit /...	SA81606		36 days ago	5	14	0	19	19	No
Adobe Acrobat Reader DC 15.x	Adobe Systems	2015.006.30413 (Cl...	Windows32-bit /...	SA81606		3 months ago	1	0	0	1	1	No
Adobe Flash Player	Adobe Systems	29.x (Active)	Windows32-bit /...	SA82501		36 days ago	0	3	0	3	3	No
Adobe Flash Player	Adobe Systems	29.0.0.140 (NPAPI)	Windows32-bit /...	SA82501		35 days ago	10	4	0	14	14	No
Adobe Shockwave Player 12.x	Adobe Systems	12.3.1.201	Windows32-bit /...	SA80028		36 days ago	11	0	0	11	11	No
Apple iTunes	Apple	12.7.4	Windows32-bit	SA82942		36 days ago	5	0	0	5	5	No
Google Chrome	Google	66.x	Windows64-bit	SA82905		35 days ago	1	8	0	9	9	No
Google Chrome	Google	66.x	Windows32-bit	SA82905		36 days ago	0	13	0	13	13	No
GTK 2.x	Kernel.org	2.14.2	Windows64-bit	SA79072		4 months ago	2	0	0	2	1	No
Mozilla Firefox	Mozilla Foundation	59.0.2	Windows64-bit	SA82228		36 days ago	4	3	0	7	7	Yes
Mozilla Firefox	Mozilla Foundation	59.0.2	Windows32-bit	SA82228		35 days ago	12	24	0	36	33	Yes
Mozilla SeaMonkey 1.1.x	Mozilla Foundation	2.x	Windows32-bit /...	SA81634		36 days ago	0	1	0	1	1	Yes
Mozilla Thunderbird 52.x	Mozilla Foundation	52.7	Windows32-bit /...	SA82157		36 days ago	15	0	0	15	15	No
Oracle Java JDK	Oracle Corporation	8u171	Windows64-bit	SA82703		36 days ago	7	1	0	8	8	No
Oracle Java JDK	Oracle Corporation	8u171	Windows32-bit	SA82703		36 days ago	6	1	0	7	7	No
Oracle Java JRE	Oracle Corporation	8u171	Windows32-bit	SA82703		36 days ago	6	1	0	7	7	No
Oracle Java JRE 1.8.x / 8.x	Oracle Corporation	8u171	Windows64-bit	SA82703		1 day, 4 hours a...	8	0	0	8	8	No
LibreOffice 5.x	The Document Foun...	5.4.6	Windows32-bit	SA82713		36 days ago	1	0	0	1	1	No
VLC Media Player 2.x	Videolan	2.2.7	Windows64-bit	SA80908		6 months ago	3	0	0	3	3	No
VLC Media Player 2.x	Videolan	2.2.7	Windows32-bit	SA80908		36 days ago	5	0	0	5	5	No



Note • An SPS package created when the Group products where patched version and architecture are identical check box is selected (grouped mode) can cover multiple product rows that are displayed when the check box is not selected (ungrouped mode). Consequently this can lead to a discrepancy when determining whether an update for the product already exists if you are switching between the grouped and ungrouped modes. For example, if you create an update for a product in grouped mode, the update may not be accurately detected when using the ungrouped mode. For this reason it is recommended to only use the grouped mode when creating updates.

Language selection for SPS

You can target specific languages and approve packages before they are published. The package configuration, based on the product family, is retained for future use.

Patch update searches by Common Vulnerabilities and Exposures (CVE)

In the **Flexera Package System (SPS) Search Type** field, you can search patch updates by CVE, which are referenced in Secunia Advisories. The CVE results help identify affected hosts, advisories, and patches across entire organizations.

Product	Vendor	Patched Version	Architecture	SAID	Criticality	Detected	Advisory Publ...	Insecure	End-Of-Life	Secure	Total	Hosts	Uninstallable
LibreOffice 5.x	The Document Foun...	5.4.6	Windows32-bit	SA82713		36 days ago	19th Apr, 2018	1	0	0	1	1	No

Advisory Published date

The **Advisory Published** date is listed in the **Flexera Package System (SPS)** grouped and ungrouped views. This date provides a quick reference for the latest patching information.



Note • In the Flexera Package System (SPS) ungrouped view which lists each product version separately, there will be no Secunia Advisory IDs (SAID) listed for End-of-Life (EOL) products. Therefore, the Advisory Published date will be blank for EOL products.

Product	Vendor	Patched Version	Architecture	SAID	Criticality	Detected	Advisory Published	Insecure	End-Of-Life	Secure	Total	Hosts
Product: Oracle Java JRE 1.8.x / 8.x (1 Item)	Oracle Corporation	Bu171	Windows64-bit	SA82703	CRITICAL	2 days ago	18th Apr, 2018	3	0	0	3	3
Product: Oracle Java JDK 1.8.x / 8.x (1 Item)	Oracle Corporation	Bu171	Windows64-bit	SA82703	CRITICAL	2 days ago	18th Apr, 2018	3	0	0	3	3
Product: VLC Media Player 2.x (1 Item)	VideoLAN	2.2.7	Windows32-bit	SA80908	CRITICAL	35 days ago	17th Nov, 2017	2	0	0	2	1

Figure 9-1: Flexera Package System (SPS) ungrouped view

Product	Vendor	Patched Version	Architecture	SAID	Criticality	Detected	Advisory Publ.	Insecure	End-Of-Life	Secure	Total	Hosts
eHule 0.x	eHule	0.47.2.66	Windows32-bit	SA16239	CRITICAL	20 days ago	27th Jul, 2005	1	0	0	1	1
FileZilla 3.x		3.21.0	Windows32-bit	SA72252	CRITICAL	20 days ago	25th Aug, 2016	1	0	0	1	1
VLC Media Player 2.x	VideoLAN	2.2.7	Windows32-bit	SA80908	CRITICAL	20 days ago	17th Nov, 2017	2	0	0	2	1
Calibre 2.x		3.x	Windows32-bit	SA81916	CRITICAL	20 days ago	9th Mar, 2018	0	1	0	1	1
Apple iTunes 12.x	Apple	12.7.4 (32-bit)	Windows32-bit / 64-bit	SA82442	CRITICAL	20 days ago	30th Mar, 2018	1	0	0	1	1
Oracle Java JDK 1.8.x / 8.x	Oracle Corporation	Bu171	Windows64-bit	SA82703	CRITICAL	2 days ago	18th Apr, 2018	3	0	0	3	3
Oracle Java JRE 1.8.x / 8.x	Oracle Corporation	Bu171	Windows64-bit	SA82703	CRITICAL	2 days ago	18th Apr, 2018	3	0	0	3	3
7-zip 16.x		18.x	Windows64-bit	SA82829	CRITICAL	3 days ago	1st May, 2018	0	1	0	1	1
7-zip 9.x		18.x	Windows32-bit	SA82829	CRITICAL	20 days ago	1st May, 2018	0	1	0	1	1
Adobe Flash Player 27.x	Adobe Systems	29.x (ActiveX)	Windows32-bit / 64-bit	SA82386	CRITICAL	20 days ago	8th May, 2018	0	1	0	1	1
Adobe Flash Player 27.x	Adobe Systems	29.x (NPAPI)	Windows32-bit / 64-bit	SA82386	CRITICAL	20 days ago	8th May, 2018	0	1	0	1	1
Mozilla Firefox	Mozilla Foundation	60.x	Windows64-bit	SA83099	CRITICAL	12 days ago	9th May, 2018	0	2	0	2	2
Mozilla Firefox 55.x	Mozilla Foundation	60.x	Windows32-bit	SA83099	CRITICAL	20 days ago	9th May, 2018	0	1	0	1	1
Google Chrome	Google	66.0.3359.170	Windows64-bit	SA83981	CRITICAL	3 days ago	11th May, 2018	1	1	0	2	2
Google Chrome 65.x	Google	66.x	Windows32-bit	SA83981	CRITICAL	20 days ago	11th May, 2018	0	1	0	1	1
Adobe Acrobat Reader 2017 17.x	Adobe Systems	2017.011.30080	Windows32-bit / 64-bit	SA82959	CRITICAL	20 days ago	14th May, 2018	1	0	0	1	1
Adobe Acrobat Reader DC 15.x	Adobe Systems	2015.006.30418 (Cl...	Windows32-bit / 64-bit	SA82959	CRITICAL	3 days ago	14th May, 2018	1	0	0	1	1
Adobe Acrobat DC 15.x	Adobe Systems	2015.006.30418 (Cl...	Windows32-bit / 64-bit	SA82959	CRITICAL	3 days ago	14th May, 2018	1	0	0	1	1

Figure 9-2: Flexera Package System (SPS) grouped view

SPS Concepts and Terminology

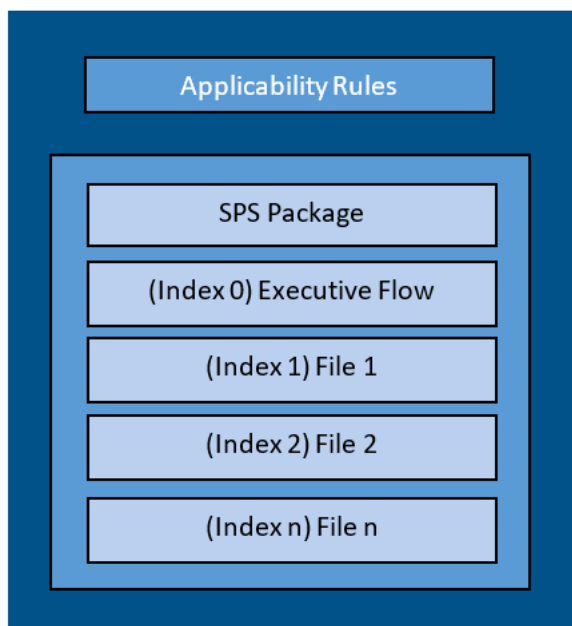
Software Vulnerability Manager users should become familiar with the concepts and terminology described in this section.

- What does a SPS package consist of?
- Applicability Rules
- SPS Package
- Execution Flow Script
- Files

What does a SPS package consist of?

The package consists of two parts; applicability rules and SPS package. The applicability rules are used by WSUS to only execute the package on computers that are applicable for the selected package.

The SPS package consists of the payload that is then executed on the computer.



The following sections explain in greater detail all the components that make a SPS package.

Applicability Rules

The applicability rules are rules used to decide whether or not a package should be offered to a client. These rules are as follows:

IsInstallableApplicabilityRule – Obtains the rules for determining whether or not this item is installable on a given computer. It generally consists of paths and version information of relevant files.

IsInstalledApplicabilityRule – Obtains the rules for determining whether or not this item is already installed on a given computer. It generally consists of keys and value information of relevant registry keys.

IsSupersededApplicabilityRule – Obtains or sets the rules for determining whether or not this item is superseded by another update on a given computer. It generally consists of paths and version information of relevant files.

SPS Package

The SPS package must always consist of at least one file that is placed at index “0”, this is the execution flow script, and any additional files will be numbered accordingly in ascending order. The execution flow script is either JScript (JavaScript), VBScript or Powershell script; by default a JavaScript example is provided in the SPS Package Creation Wizard.

The script will be automatically extracted from the SPS package and executed. Based on the execution flow more files can then be extracted and executed from the SPS package, referenced by their index order.



Important • When using Powershell Scripting as the execution controlling script of the package, you must ensure that Microsoft Visual C++ 2012 Redistributable (x86) is installed on the target hosts you are deploying the update package to.

Execution Flow Script

This execution flow script is always executed. This is the file with index 0, and as such it will always be the first to run.

In the execution flow script you can define any other files to be extracted and executed. The default execution flow template that is provided in the SPS Package Creation Wizard will extract the first file supplied in the package with the specified silent parameters (usually this is the patch file provided by the vendor). Any other files added to the package will NOT be extracted or executed when using the example script.

If you create your own execution flow, no user interaction is available. To make your execution flow totally unattended, use log files accordingly for easy troubleshooting.

Files

The SPS package supports additional files besides the execution flow script. The added files will have array indices from 1 to n where the first file will have index 1, and the additional files are numbered in ascending order.

Creating a Patch with the Flexera Package System (SPS)

The Flexera Package System (SPS) page displays a list of products that you can create updates for.

Click **Configure View** to customize the list and limit the types of products shown, as well as highlight products for which packages have or have not been created.

If highlighted, products for which SPS packages exist will be shown in green.

A product will be displayed in blue if the vendor provides unattended/silent installation parameters for its patches. Any product listed in blue is available to have an update created in a simple 3 step process.

Some products are presented in gray because the vendor of the product does not provide silent installation parameters. If you choose to patch one these products, you must provide (import) the **.MSI/.MSP/.EXE** file together with the parameters for the unattended installation. Software Vulnerability Manager will then repackage and publish the update through the standard workflow. Packages cannot be automatically created by Software Vulnerability Manager for these products.

If you wish to create a new custom package that does not necessarily patch an existing product, for example to deploy new software, you can click **New Custom Package**. In this case you should provide the files/installer that will be executed on the target client together with the execution flow script.

With Software Vulnerability Manager, you are able to create three different kinds of packages. Right-click a product and select one of the available options:

- [Create an Update Package](#)
- [Create an Uninstall Package](#)
- [Create a Custom Package](#)

For the Update and Uninstall packages a default execution flow script is provided in the SPS Package Creation Wizard ([Step 2 of 4: Package Contents](#)), which will fulfill most of the common needs.

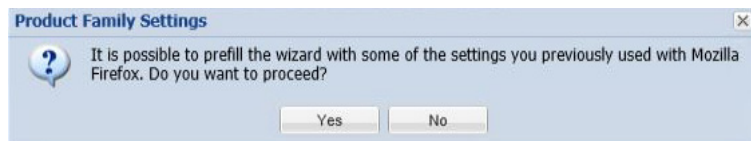
The execution flow script for an Update package can also be customized for additional functionality. You can also configure your patching package SPS Installer Parameters using dynamic check box options (where applicable) based on product functionality, including:

- Remove End User License Agreement
- Disable Automatic Updates
- Silent Install
- Update to lowest secure version
- No reboot necessary
- Cumulative updates in one package
- Set Security Level
- Remove system tray icon
- Restrict Java Applications
- Uninstall Prior to Installing
- Prevent Installation of Certain Components
- Prevent Collection of Anonymous Usage Statistics
- Remove Desktop Shortcut

Create an Update Package

A Product will be displayed in blue if the vendor provides unattended/silent installation parameters for its patches. Any Product listed in blue is available to have an update created in a three-step process. Right-click or double-click one of these Products and select **Create Update Package** to start the SPS Package Creation Wizard.

Software Vulnerability Manager retains Product Family Settings that you previously used. Click **Yes** to prefill the SPS Package Creation Wizard with the available settings.



Create an Uninstall Package

Any Products that are listed as **Yes** in the **Uninstallable** column are available to have an uninstall package created in a four-step process exactly as the update packages in blue.

Flexera Package System (SPS)												
Product	Vendor	Patched Version	Architecture	SAID	Criticality	Detected	Insecure	End-Of-Life	Patched	Total	Hosts	Uninstallable
7-zip		18.x	Windows64-bit	SA82839		1 day, 4 hours a...	0	2	0	2	2	No
7-zip 64		18.x	Windows32-bit	SA82839		5 months ago	0	2	0	2	2	No
Adobe Acrobat DC 15.x	Adobe Systems	2015.006.30413 (Cl...	Windows32-bit /	SA81606		3 months ago	1	0	0	1	1	No
Adobe Acrobat Reader DC	Adobe Systems	18.x (Continuous)	Windows32-bit /	SA81606		36 days ago	5	14	0	19	19	No
Adobe Acrobat Reader DC 15.x	Adobe Systems	2015.006.30413 (Cl...	Windows32-bit /	SA81606		3 months ago	1	0	0	1	1	No
Adobe Flash Player	Adobe Systems	29.0.0.140 (NPAPI)	Windows32-bit /	SA82591		35 days ago	10	4	0	14	14	No
Adobe Flash Player	Adobe Systems	29.x (ActiveX)	Windows32-bit /	SA82591		36 days ago	0	3	0	3	3	No
Adobe Shockwave Player 12.x	Adobe Systems	12.3.1.201	Windows32-bit /	SA80928		36 days ago	11	0	0	11	11	No
Apple iTunes	Apple	12.7.4	Windows32-bit	SA82242		36 days ago	5	0	0	5	5	No
Calibre 2.x		3.x	Windows64-bit	SA81316		36 days ago	0	2	0	2	2	No
eMule Plus 1.x		1.2.5.0	Windows32-bit	SA34799		36 days ago	1	0	0	1	1	No
FileZilla 3.x		3.21.0	Windows32-bit	SA72252		5 months ago	1	0	0	1	1	Yes
Git 2.x	Kernel.org	2.14.2	Windows64-bit	SA72072		4 months ago	2	0	0	2	1	No
Google Chrome	Google	66.x	Windows64-bit	SA82905		35 days ago	1	8	0	9	9	No
Google Chrome	Google	66.x	Windows32-bit	SA82905		36 days ago	0	13	0	13	13	No
LibreOffice 5.x	The Document Foun...	5.4.6	Windows32-bit	SA82719		36 days ago	1	0	0	1	1	No
Mozilla Firefox	Mozilla Foundation	59.0.2	Windows64-bit	SA82228		36 days ago	4	3	0	7	7	Yes
Mozilla Firefox	Mozilla Foundation	59.0.2	Windows32-bit	SA82228		35 days ago	12	24	0	36	33	Yes
Mozilla SeaMonkey 1.1.x	Mozilla Foundation	2.x	Windows32-bit /	SA81634		36 days ago	0	1	0	1	1	Yes
Mozilla Thunderbird 52.x	Mozilla Foundation	52.7	Windows32-bit /	SA82152		36 days ago	15	0	0	15	15	No
Oracle Java JDK	Oracle Corporation	8u171	Windows64-bit	SA82703		36 days ago	7	1	0	8	8	No
Oracle Java JDK	Oracle Corporation	8u171	Windows32-bit	SA82703		36 days ago	6	1	0	7	7	No
Oracle Java JRE	Oracle Corporation	8u171	Windows32-bit	SA82703		36 days ago	6	1	0	7	7	No
Oracle Java JRE 1.8.x / 8.x	Oracle Corporation	8u171	Windows64-bit	SA82703		1 day, 4 hours a...	8	0	0	8	8	No
VLC Media Player 2.x	VideoLAN	2.2.7	Windows64-bit	SA80928		6 months ago	3	0	0	3	3	No
VLC Media Player 2.x	VideoLAN	2.2.7	Windows32-bit	SA80928		36 days ago	5	0	0	5	5	No

For Products listed as **No** in the **Uninstallable** column you must customize the execution flow script to successfully uninstall the product. This can be done by starting the SPS Package Creation Wizard and selecting the **Edit Package Content** check box in Step 1.

If you have an SPS XML template you can import it by clicking **Import Package** in the first step of the wizard. Once this is completed, all the fields in the wizard will be automatically populated, including the execution flow script.

Special attention should be given to the files mentioned in the execution flow script. These files can be files originally provided by the SPS template creator or they can be dynamically downloaded.



Important • You should only import SPS packages if you trust the author of the package and the source from where you downloaded/obtained the package.

Create a Custom Package

Software Vulnerability Manager allows creating custom packages that can be deployed through WSUS/System Center. By creating a custom package you can do a wide range of actions; everything from updating and uninstalling third-party applications to handling complex execution flows with multiple files.

The creation of a custom package can be done in two different ways. Either:

- Right-click a product and choose **Create Custom Package**. By doing this the product applicability rules will be included in the package; this will mean that the Custom Package will only be applicable for computers with the selected product installed.
- OR
- Click **New Custom Package** to start the SPS Package Creation Wizard. In this case no applicability rules will limit the installation base.

Independently of the chosen approach, in both cases the SPS Package Creation Wizard will be initiated.

The SPS Package Creation Wizard

Creating an SPS Package involves a four-step process:

- **Step 1 of 4: Package Configuration**

- [Step 2 of 4: Package Contents](#)
- [Step 3 of 4: Applicability Criteria - Paths](#)
- [Step 4 of 4: Applicability Criteria - Rules](#)

Step 1 of 4: Package Configuration

In Step 1 no action is required if the selected product was in blue. You should only check **Edit Package Content (Optional)** if the product was in gray or there is a need to customize the update patch by selecting a different file(s) and/or defining a different execution flow script.

Step 1 of 4: Package Configuration

Use this form to set the name and description of the SPS package, or edit the properties of an existing one. In the following steps you will configure the package contents and parameters before creating and publishing the package, or exporting it as an XML formatted file.

Import XML (Optional)

You can start by importing an existing SPS Package File. This will populate all of the wizard data fields with the package data, which you can then view and/or edit.

NOTE: You should only import packages if you trust the author of the package and the source from where you downloaded / retrieved the SPS package.

Package Name

The package will be created with the following name. Choose a new name if desired.

Name:

Description (Optional)

Here you can give a description of the package. For example, what it does, the contents, usage, etc.

Description:

Reference Id (Optional)

Here you can assign an Id to this package if desired.

Reference Id:

SPS Installer Parameters (Optional)

Here you can configure optional parameters you want to pass to the installer. This set of options is unique to this product. Some parameters have warning message associated that should be read and understood before moving forward

Configure Package Behavior: ☒ Default (?)

☐ Disable checking for running Chrome processes (?)

☐ Kill any running Chrome processes (?)

Select Installer: ☒ Install Enterprise version

☐ Install Stable version

Edit Package Content (Optional)

If you choose to edit the package contents, in the next Step of the wizard you will have the option to view/edit the package contents. If not, you will be directed immediately to Step 3.

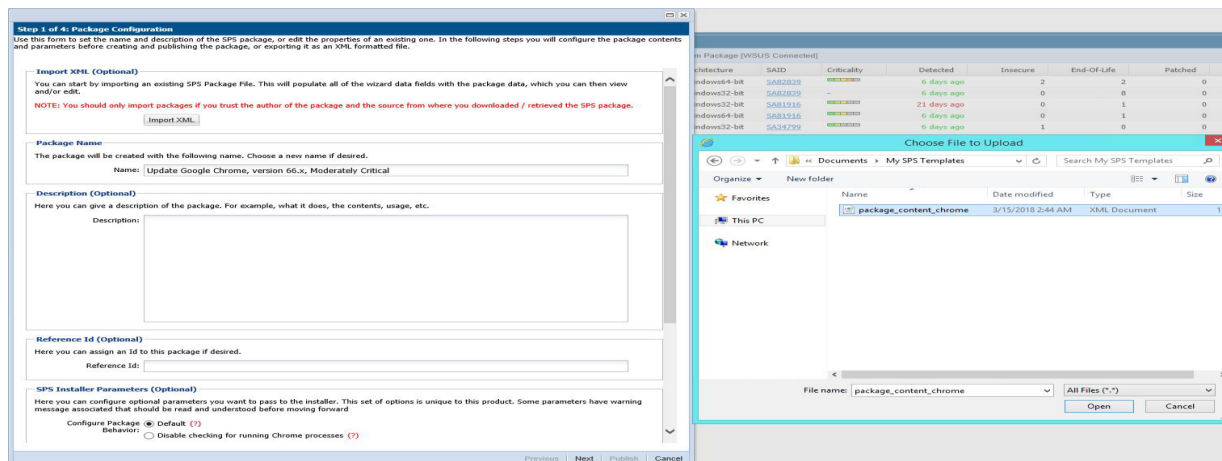
☐ Edit Package Content

Vendor & Product Naming

☐

Previous | Next | Publish | Cancel

The **Import Package** feature allows you to import a SPS template in XML format that will automatically populate all the fields of the SPS Package Creation Wizard. This feature will be especially relevant when creating custom updates or when creating update packages for the products in gray.



In Step 4 of the wizard you will also have the option to export the XML template for the package being created.

After clicking **Next**, and if **Edit Package Content (Optional)** was not selected, you will go directly to [Step 3 of 4: Applicability Criteria - Paths](#).

Step 2 of 4: Package Contents

Step 2 becomes available when **Edit Package Content** is selected in Step 1. The first section of Step 2 is the Execution Script where you select **JScript (Javascript)**, **VBScript** or **Powershell Script** and then review or create a customized execution flow.

You are also able to change the files that are included in the SPS package, which can either be local files or links to be dynamically downloaded upon publishing of the package.

To test a newly created execution flow together with the added files click **Create SPS File**. A SPS.exe file is created that can be executed locally prior to being published into the WSUS server.

This SPS.exe file will include the execution flow script and the files to be included, but not the applicability rules.

Step 2 of 4: Package Contents

Here you configure the package contents, including the execution script included, and the files included.

Execution Script

View/Edit the execution flow and script type for this SPS package.

Script Type: JScript (Javascript)

Execution Flow:

```

var Title = "Update Google Chrome, version 66.x, Moderately Critical";
var GUID = "1535ed8d-b052-45ab-8665-9544a8ee7e7d";
var silentParams = "/S";
var optionalParams = " /business";

// The following four variables have been embedded by the CSI at the
// start of this script
// var GUID = "";
// var Title = "";
// var silentParams = "";
// var optionalParams = "";

var ret = 1;
function main() {
    if ( !GUID ) {
        server.logMessage( "No GUID supplied for package " + Title );
        return 1;
    }
}

```

Files To Include

Configure the files to include in this package. The grid below shows the files that are currently scheduled to be included, and if they will be downloaded dynamically (i.e., in the case of URLs) or if they are local files. You can add additional files via the 'Add File' button, as well as choose from additional language packages available via the 'Show Localised Files' button. To remove a files, right-click and select 'Remove'.

File(s) to include in the package	Status
http://dl.secunia.com/SPS/GoogleChrome_66.0.3359.139_64-bit_SPS.exe	To Be Dynamically Downloaded

Add Local File

Add Download Link

Add Localisation (Language) File

Create SPS File

You also have the option of creating an SPS File from this package, should you wish to.

Create SPS File

Previous

Next

Publish

Cancel

Step 3 of 4: Applicability Criteria - Paths

In Step 3 you should select the paths/locations to which this package should be applied. These are usually populated by Software Vulnerability Manager based on the scans previously conducted.

Please be advised to only choose paths that are valid to avoid any update loops. You can also use paths with CSIDL and KNOWNFOLDERID if you select the **Show Advanced Options** check box. These variables should be used with their decimal value.

Step 3 of 4: Applicability Criteria - Paths

Here you can define the path-based applicability rules for this package. Below you will find any relevant paths already found or configured for the package. You can deselect paths in the grid or add paths as needed via the "Add Path" button. Check the "Advanced Options" box to enable additional options in the "Add Path" dialog and to show advanced options in the grid.

☐ Show Advanced Options

Add Path

Always Install Option
The purpose of this option is to allow installations of new software. For custom packages which are not updates to existing installations, you can bypass the "isInstallable" WSUS rule which will ignore all system paths when deciding if this package can be applied. Note - this will not bypass the rules for checking if something is already installed, or is superseded by a more recent version.

☐ Mark Package as "Always Installable"

Minimum Version Option
The purpose of this option is to allow for updating of older products. Normally one updates a product to its secure version within the same major version. You can alter this behaviour by specifying a custom minimum version. Note: the version you enter must also be supported by the installer itself - you cannot enter arbitrary values here.

Minimum Version:

Path	Information
<input checked="" type="checkbox"/> C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	1

Previous | Next | Publish | Cancel

For packages that should not have any paths for applicability, select the **Mark Package as "Always Installable"** check box to ignore all paths. Paths for App-V and Mac OS X are filtered out since they are not supported for patching.

Use the **Minimum Version Option** to update older products. Normally, a product is updated to its secure version within the same major version. You can alter this behavior by specifying a custom minimum version. Note: the version you enter must also be supported by the installer itself - you cannot enter arbitrary values here.

Importing Bulk File Paths in the SPS Package Creation Wizard

To help with situations where you wish to include specific file paths for scanning software, you can now import multiple file paths by providing a CSV file during Step 3 of the patch/template creation process (CSIL-9630).

On the **Step 3 of 4: Applicability Criteria - Paths** panel, click **Add Path** to open the **Import Path Applicability Rules for Package** dialog box, and select a local CSV file which contains file paths.

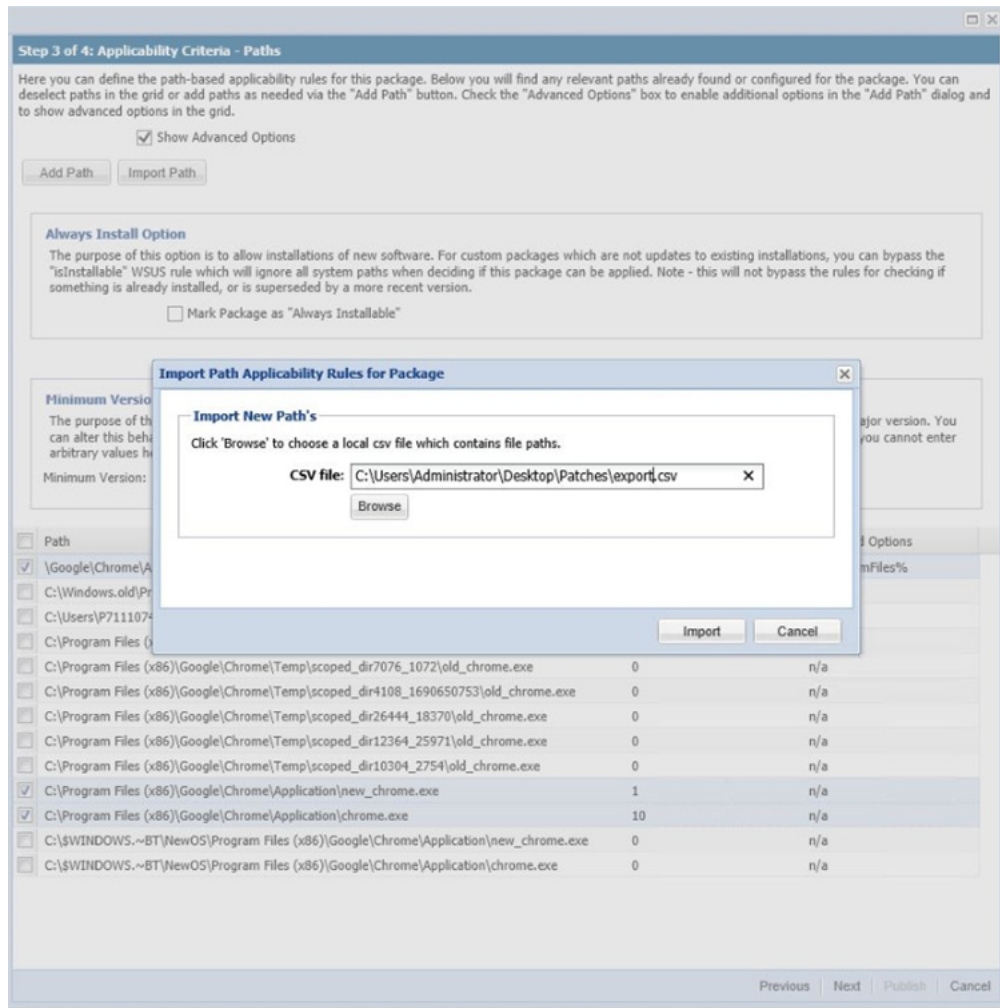


Figure 9-3: Import Path Applicability Rules for Package Dialog Box

This enables you to target specific file paths or to include file paths discovered in other partitions in order to create a single patch for deployment that covers all desired file paths.

CSV File Format

When creating a CSV file for import, file paths entered in the following formats are acceptable:

C:\Users\Administrator\AppData\Local\Temp\Acme\acinstall\tools\acmeinstall\tools\7z.exe
C:\Program Files\Acme\tools\7z.exe
%ProgramFiles%\Acme\tools\7z.exe



Note • The CSV file does not need to have comma-separated values, but just a list. You don't have to use quotes when there are spaces in a file path. The CSV file can essentially be a text list with just one column. As a single column list of values, simply provide one file path per line (no header row or additional columns should be included).

Step 4 of 4: Applicability Criteria - Rules

In Step 4 you should specify if you want to limit the package to 32-bit or 64-bit systems or computers with specific operating system languages. The patch file to be deployed will be automatically downloaded in the background by the Software Vulnerability Manager console. Once this is completed the Software Vulnerability Manager console will repackage and publish the update package into the WSUS/System Center.

The WSUS option will be unavailable if the WSUS Connection is not established.

To export the package select **File System (Export)** and click **Publish**.

Step 4 of 4: Applicability Criteria - Rules

Here you configure the applicability rules for the package.

System Applicability

Configure the system type(s) the package will be applied to.

Apply Package To: ☐ 32-bit Systems Only ☒ 64-bit Systems Only ☐ Both 32-bit and 64-bit Systems

Special Rule

The following special rule is available to configure:

☐ Reboot is required after package has been installed.

Language Settings

Configure package applicability rules based on language:

☐ Only make package applicable to computers with one of the selected languages.

Select Languages: Language

- Arabic
- Chinese (Hong Kong SAR)
- Chinese - (Simplified)
- Chinese - (Traditional)
- Czech
- Danish

Export Patch Script

Before publishing XML patch script to your file system, you have the option to configure XML file. Note: As you might wish to share this package, for example via the community forum, you can choose to not include the package files as binary and the applicability paths from Step 3, as your paths may contain private user data.

☐ Do not include Step 3 Applicability Paths in XML File.

☐ Do not include package file(s) as binary in XML File.

Patch Template (Optional)

Save as template

Template Name: Enter Template Name...

Publish Options

Select option for publishing Flexera package

Publish package using: ☒ WSUS ☐ Altiris ☐ Export Patch Script ☐ Save Template

Previous | Next | Publish | Cancel

If a reboot is required after the package has been installed this can also be configured in the second part of this step as well as checking if Java is running.

To configure your package to only be applicable for certain languages of the operating system, select **Only make package applicable to computers with one of the selected languages** and select the relevant language.

In this step you are also able to export the package that you have already configured to be used for future reference. You have the option to include or exclude Step 3 applicability paths and the installer as binary.

The two options (**Do not include Step 3 Applicability Paths in XML File** and **Do not include the package file(s) as binary in XML File**) are taken into consideration only when exporting the package to the **File System (Export)**, otherwise the selection will be disregarded.

Vendor Patch Module

Vendor Patch Module represents the largest set of patch data on the market today. It is designed to integrate several hundred out of the box patches for prioritization and publishing within SVM. Additionally, it exposes details which helps you to be aware what patches exist, and to provide as much detail as possible to make bringing your own patch to SVM easier. These additional entries are typically missing something like the actual setup file (because the vendor does not make it publicly available) or because we don't have default applicability criteria (but can leverage assessment results for your environment).



Tip • To know more about the Vendor Patch Module, [click here](#).

This section provides further information regarding:

- Vendor Patch Module Page Features
- Creating a Patch with the Vendor Patch Module
- Package Creation Wizard in Vendor Patch Module
- Automating Patch Deployment



Important • Vendor Patch Module is an optional feature and must be purchased separately:

- For pricing and availability, please contact your sales representative or contact us online at: <https://www.flexera.com/about-us/contact-us.html>
- If the feature is not purchased, you can view the list of available patches but cannot use them.

Vendor Patch Module Page Features

The **Vendor Patch Module** page displays a list of products for which Software Vulnerability Manager can automatically create an Update/Uninstall package. Right-click any of the listed products to view the available options.

Vendor Patch Schedule																	Export	
Search Type	Product	Search out	View from the context of Smart Group	Not Detected	Configure View													
Product	Vendor	Patched Version	Deployment Ready	SAD	Criticality	Threat Score	Advisory Published	Architecture	Insecure	End-Of-File	Secure	Total	Hosts	Updated On	Download	File Size		
CompuSecure Update for Inter...	Microsoft	3124275	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 64-bit	0	0	0	0	0	0 2nd May, 2019	Download	4273 MB		
CompuSecure Update for Inter...	Microsoft	3124275	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 32-bit	0	0	0	0	0	0 2nd May, 2019	Download	2042 MB		
CompuSecure Update for Inter...	Microsoft	3124275	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 64-bit	0	0	0	0	0	0 2nd May, 2019	Download	3856 MB		
CompuSecure Update for Inter...	Microsoft	4047206	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 64-bit	2	0	0	2	51	0 2nd May, 2019	Download	5231 MB		
CompuSecure Update for Inter...	Microsoft	4047206	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 64-bit	0	0	0	0	0	0 2nd May, 2019	Download	5258 MB		
CompuSecure Update for Inter...	Microsoft	4047206	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 32-bit	0	0	0	0	0	0 2nd May, 2019	Download	2849 MB		
CompuSecure Update for Inter...	Microsoft	4047206	No	SAD9921	<div><div></div></div>		99 13th May, 2019 17:00	Windows 64-bit	0	0	0	0	0	0 2nd May, 2019	Download	5441 MB		
CompuSecure Update for Inter...	Microsoft	4047206	No	SAD9921	<div><div></div></div>		99 13th May, 2019 17:00	Windows 32-bit	0	0	0	0	0	0 2nd May, 2019	Download	2919 MB		
CompuSecure Update for Inter...	Microsoft	4047206	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 64-bit	0	0	0	0	0	0 2nd May, 2019	Download	5248 MB		
CompuSecure Update for Inter...	Microsoft	4047206	No	SAD9921	<div><div></div></div>		99 13th May, 2019 17:00	Windows 64-bit	0	0	0	0	0	0 2nd May, 2019	Download	5441 MB		
CompuSecure Update for Inter...	Microsoft	3124275	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 64-bit	0	0	0	0	0	0 2nd May, 2019	Download	15 MB		
CompuSecure Update for Inter...	Microsoft	3124275	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 32-bit	0	0	0	0	0	0 2nd May, 2019	Download	8 MB		
CompuSecure Update for Inter...	Microsoft	3124275	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 64-bit	0	0	0	0	0	0 2nd May, 2019	Download	2271 MB		
CompuSecure Update for Inter...	Microsoft	3124275	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 32-bit	0	0	0	0	0	0 2nd May, 2019	Download	1221 MB		
CompuSecure Update for Inter...	Microsoft	3124275	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 64-bit	0	0	0	0	0	0 2nd May, 2019	Download	2106 MB		
CompuSecure Update for Inter...	Microsoft	3124275	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 32-bit	0	0	0	0	0	0 2nd May, 2019	Download	1077 MB		
CompuSecure Update for Inter...	Microsoft	3124275	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 64-bit	0	0	0	0	0	0 2nd May, 2019	Download	2271 MB		
CompuSecure Update for Inter...	Microsoft	3124275	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 64-bit	0	0	0	0	0	0 2nd May, 2019	Download	2953 MB		
CompuSecure Update for Inter...	Microsoft	3124275	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 32-bit	0	0	0	0	0	0 2nd May, 2019	Download	1448 MB		
CompuSecure Update for Inter...	Microsoft	3124275	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 64-bit	0	0	0	0	0	0 2nd May, 2019	Download	2953 MB		
CompuSecure Update for Inter...	Microsoft	4047206	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 64-bit	0	0	0	0	0	0 2nd May, 2019	Download	2531 MB		
CompuSecure Update for Inter...	Microsoft	4047206	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 32-bit	0	0	0	0	0	0 2nd May, 2019	Download	127 MB		
Internet Explorer 11 for Windows 7...	Microsoft	11.0.9600.16428	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 64-bit	0	0	0	0	0	0 2nd May, 2019	Download	5322 MB		
Internet Explorer 11 for Windows 7...	Microsoft	11.0.9600.16428	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 32-bit	0	0	0	0	0	0 2nd May, 2019	Download	2634 MB		
Internet Explorer 9 for Windows 7 (E...	Microsoft	9.0.8116.16421	No	SAD9922	<div><div></div></div>		99 13th May, 2019 17:00	Windows 32-bit	94	0	12	106	106	2nd Jun, 2019	Download	1728 MB		
Opera (x64)	Opera Software ASA	62.0.3131.72	No	SAD9922	<div><div></div></div>		67 24th Apr, 2014 17:00	Windows 64-bit	0	0	0	0	0	0 12th Jul, 2019	Download	5521 MB		
Opera (x86)	Opera Software ASA	62.0.3131.72	Yes	SAD98125	<div><div></div></div>		67 24th Apr, 2014 17:00	Windows 32-bit	0	0	0	0	0	0 12th Jul, 2019	Download	5248 MB		
Opera for Mac	Opera Software ASA	62.0.3131.66	No	SAD9922	<div><div></div></div>		67 24th Apr, 2014 17:00	Mac Intel 64-bit	0	0	0	0	0	0 12th Jul, 2019	Download	7230 MB		
Novell View Desktop (x64)	Novell	2.0.0.67	Yes	SAD3262	<div><div></div></div>		64 23rd Feb, 2015 16:00	Windows 64-bit	0	0	0	0	0	0 2nd May, 2019	Download	1542 MB		
Novell View Desktop (x86)	Novell	2.0.0.67	Yes	SAD3262	<div><div></div></div>		64 23rd Feb, 2015 16:00	Windows 32-bit	0	0	0	0	0	0 2nd May, 2019	Download	1542 MB		
Fusion	VMware	11.0.1.16436589	No	SAD9108	<div><div></div></div>		62 16th Nov, 2017 16:00	Mac Intel 64-bit	0	0	0	0	2	1 10th Jun, 2019	Download	49521 MB		
WinRAR (x64)	Rabab	5.71.0.0	No	SAD4251	<div><div></div></div>		58 12th Feb, 2019 16:00	Windows 64-bit	0	0	0	0	0	0 27th Jun, 2019	Download	24 MB		
WinRAR (x86)	Rabab	57.11.0	No	SAD4251	<div><div></div></div>		58 12th Feb, 2019 16:00	Windows 32-bit	0	0	0	0	0	0 2nd May, 2019	Download	24 MB		
Microsoft Visual Studio 9 Service Pack 1	Microsoft	9.0.2	No	SAD5627	<div><div></div></div>		57 13th Aug, 2012 17:00	Windows 32-bit	0	2	0	2	2	2 May, 2019	Download	3479 MB		
Security Essentials (x64) (x64)	Microsoft	4.10.0.59.0	No	SAD4212	<div><div></div></div>		50 5th Apr, 2018 17:00	Windows 64-bit	0	0	0	0	5	5 2nd May, 2019	Download	1437 MB		
Security Essentials (x64) (x86)	Microsoft	4.10.0.59.0	No	SAD4212	<div><div></div></div>		50 5th Apr, 2018 17:00	Windows 32-bit	0	0	0	0	0	0 2nd May, 2019	Download	1166 MB		
Safe	Apple	15.0.15.2	Yes	SAD9922	<div><div></div></div>		23 13th May, 2019 17:00	Windows 64-bit	128	0	0	128	82	20th May, 2019	Download	3671 MB		
Acrobat 10.1.15 Pro and Standard up...	Adobe	10.1.16.0	No	SAD8905	<div><div></div></div>		50 13th May, 2019 17:00	Windows 32-bit	1	1	2	5	4	4 May, 2019	Download	1061 MB		
Acrobat 10.1.23 Pro and Standard up...	Adobe	11.0.21.0	No	SAD8905	<div><div></div></div>		19 13th May, 2019 17:00	Windows 32-bit	1	1	2	5	4	4 May, 2019	Download	2470 MB		

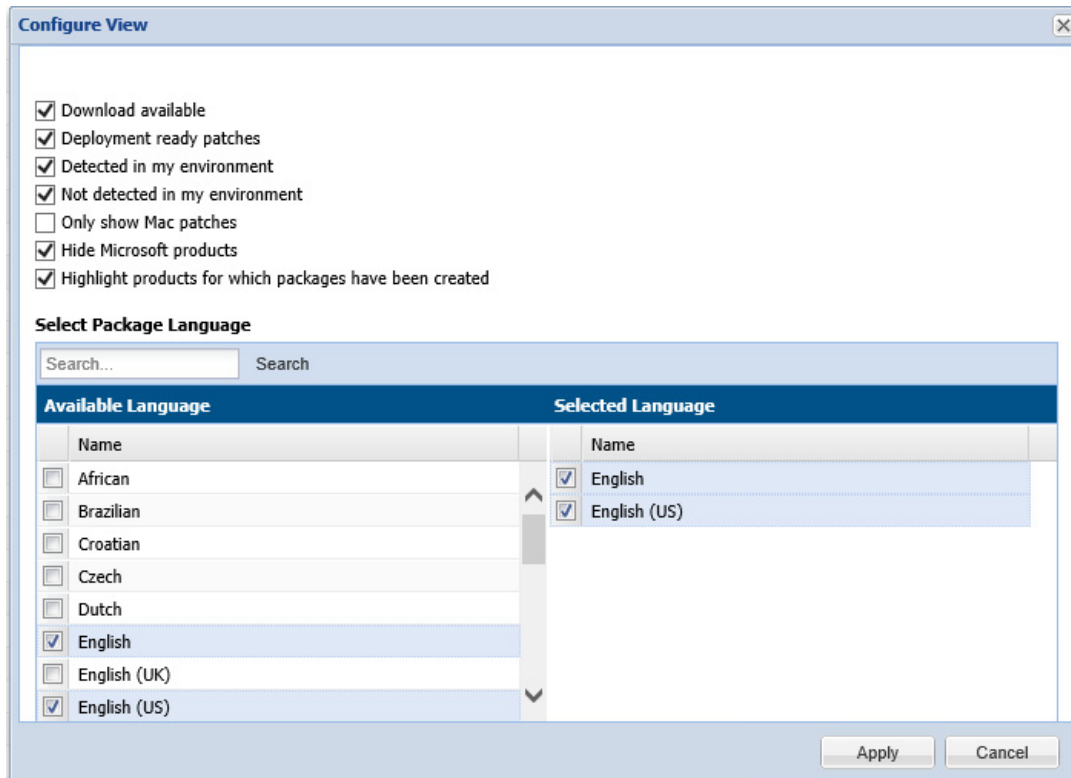
The **Vendor Patch Module** features include:

- Product display criteria for Vendor Patch Module
- Patch update searches by Common Vulnerabilities and Exposures
- Advisory Published date in Vendor Patch Module
- Threat Score in Vendor Patch Module

Product display criteria for Vendor Patch Module

Click Configure View to select the below criteria that will be used to display the products in this view:

- **Download available** - Displays a list of patches available to download
- **Deployment ready patches** - Displays a list of deployable out of the box patches which have no missing details. These patches are highlighted in **Blue** color in the products list and have a high rate of success in mass deployment.
- **Detected in my environment** - Displays a list of patches available for applications which are already installed in the user environment
- **Not detected in my environment** - Displays a list of patches available for other applications which are not deployed in the user environment
- **Only show Mac patches** - Displays a list of patches for MAC OS, You can easily download them for deployment in your Mac management solution of choice.
- **Hide Microsoft products** - Hides a list of products with the vendor name Microsoft.
- **Highlight products for which packages have been created** - Displays a list of products in Green color for which packages have been created successfully.



Note • MSP packages are currently **Not deployment** ready, but deployment is possible depending on the environment that these packages are ready to be deployed as is.

Select Package Language

You can target specific languages and approve packages before they are published. The **Configure View** settings in the Vendor Patch Module can be retained for future use.

By default, the following package language is selected:

- English
- English (UK)
- English (US)
- English GB
- English US
- Multi

You are also able to change the default selected language and select new package languages.

Patch update searches by Common Vulnerabilities and Exposures

In the **Vendor Patch Module Search Type** field, you can search a patch updates by CVE, which are referenced in Secunia Advisories. The CVE results help identify affected hosts, advisories, and patches across the entire organizations when appropriate Smartgroup filters are chosen.

Vendor Patch Module													
Search Type:	CVE	0084	Search	View from the context of Smart Group: Not Selected				Configure View					
Product	Vendor	Patched Version	Deployment Rea...	SAID	Criticality	Threat Sc...	Advisory Publish...	Architecture	Insecure	End-Of-Life	Secure	Total	Hosts
NET...	Microsoft	4.6.01590.00	Yes	SAB89273			13th May, 2019...	Windows 32-bit...	398	0	239	637	258
2nd May, 2019... Download													

Advisory Published date in Vendor Patch Module

The **Advisory Published** date is listed in the **Vendor Patch Module** provides a quick reference for the latest patching information.

Vendor Patch Module													
Search Type:	Product	Search text	Search	View from the context of Smart Group: Not Selected				Configure View					
Product	Vendor	Patched Version	Deployment Rea...	SAID	Criticality	Threat Score	Advisory Published	Architecture	Insecure	End-Of-Life	Secure	Total	Hosts
Safari	Apple	5.34.57.2	Yes	SAB89060		23	13th May, 2019 17:00	Windows 32-bit...	0	128	0	128	92
Acrobat 11.0.23 Pro and...	Adobe	11.0.23.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	1	1	2	4	4
Acrobat DC Pro and Sta...	Adobe	17.11.30142.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	1	1	2	4	4
Acrobat DC Pro and Sta...	Adobe	15.006.30497.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	1	1	2	4	4
Acrobat DC Pro and Sta...	Adobe	19.012.20034.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	2	35	1	38	38
Acrobat Reader 2017 Cl...	Adobe	17.11.30142.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	1	0	2	3	3
Reader 11.0.23 update ...	Adobe	11.0.23.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader 11.0.23 update ...	Adobe	11.0.23.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader DC (English)	Adobe	15.007.20033.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	2	35	8	45	45
Reader DC Classic Track...	Adobe	15.006.30497.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	2	35	8	45	45
Reader DC update - All I...	Adobe	19.012.20034.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	2	35	8	45	45
Reader DC update - Mul...	Adobe	19.012.20034.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	2	35	8	45	45
Reader X (English)	Adobe	10.1.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (Brazilian)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (Croatian)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (Czech)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (Dutch)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (English)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (Finnish)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (French)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (German)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (Hungarian)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (Polish)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (Romanian)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (Russian)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (Slovak)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63

Threat Score in Vendor Patch Module

The **Threat Score** provides the Threat Score information for the out of the box patches listed in the **Vendor Patch Module**.



Note • Threat Score is available only for users with Threat Intelligence Module

Vendor Patch Module													
Search Type:	Product	Search text	Search	View from the context of Smart Group: Not Selected				Configure View					
Product	Vendor	Patched Version	Deployment Rea...	SAID	Criticality	Threat Score	Advisory Published	Architecture	Insecure	End-Of-Life	Secure	Total	Hosts
Safari	Apple	5.34.57.2	Yes	SAB89060		23	13th May, 2019 17:00	Windows 32-bit...	0	128	0	128	92
Acrobat 11.0.23 Pro and...	Adobe	11.0.23.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	1	1	2	4	4
Acrobat DC Pro and Sta...	Adobe	17.11.30142.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	1	1	2	4	4
Acrobat DC Pro and Sta...	Adobe	15.006.30497.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	1	1	2	4	4
Acrobat DC Pro and Sta...	Adobe	19.012.20034.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	2	35	1	38	38
Acrobat Reader 2017 Cl...	Adobe	17.11.30142.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	1	0	2	3	3
Reader 11.0.23 update ...	Adobe	11.0.23.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader 11.0.23 update ...	Adobe	11.0.23.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader DC (English)	Adobe	15.007.20033.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	2	35	8	45	45
Reader DC Classic Track...	Adobe	15.006.30497.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	2	35	8	45	45
Reader DC update - All I...	Adobe	19.012.20034.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	2	35	8	45	45
Reader DC update - Mul...	Adobe	19.012.20034.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	2	35	8	45	45
Reader X (English)	Adobe	10.1.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (Brazilian)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (Croatian)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (Czech)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (Dutch)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (English)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (Finnish)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (French)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (German)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (Hungarian)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (Polish)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (Romanian)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (Russian)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63
Reader X (Slovak)	Adobe	11.0.0.0	Yes	SAB89005		19	13th May, 2019 17:00	Windows 32-bit...	60	1	2	63	63

Creating a Patch with the Vendor Patch Module

The Vendor Patch Module page displays a list of products that you can create updates for.

Click Configure View to customize the list and limit the types of products shown in the list as per your requirements.

A product will be displayed in blue if the vendor provides unattended/silent installation parameters for its patches. Any product listed in blue is available to have an update created in a simple 3 step process.

Some products are presented in gray because the vendor of the product does not provide setup files to deploy, Packages cannot be automatically created by Software Vulnerability Manager for these products.

With Vendor Patch Module you can update a package. Right-click a product you can see the following options:

- [Create an Update Package](#)
- [View Installations](#)
- [Patch Information](#)

To Update packages a default execution flow script is provided in the ([Step 2 of 4: Package Contents](#)), which will fulfill most of the common needs.



Important • The color code for the Vendor Patch Module products list is as follows:

- **Blue color patches** - Out of the box patches are ready to deploy with no missing details, so no extra details needed to deploy these patches.
- **Black color patches** - Patches that are missing some information, but are available to download. To create a patch, any missing details must be provided.
- **Gray color patches** - Patches that are missing some information including the vendor setup files. To create a patch, the vendor setup must be provided along with any missing details.
- **Green color patches** - Patches for which packages have already been created.

Create an Update Package

A Product will be displayed in blue if the vendor provides unattended/silent installation parameters for its patches. Any Product listed in blue is available to have an update created in a 3 step process. Right-click one of these Products and select Create Update Package to start the Package Creation Wizard.

To **Create Update Package** using 3 step process, see [Package Creation Wizard in Vendor Patch Module](#)



Note • You can not **Create Update Package** for MAC OS patches.

View Installations

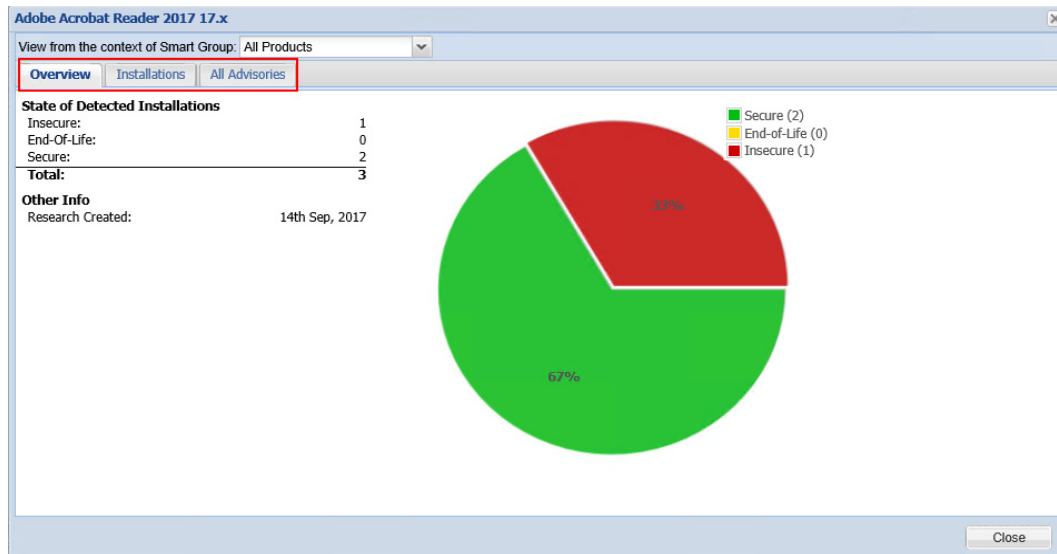
To display the installation details of a product in the Vendor Patch Module, Right-click one of a product and select **View Installations** to open the wizard,

The **View Installations** wizard provides the following details:

Overview - Provides the details of **State of Detected Installations** with a pie chart representation.

Installations - Provides the list of Host machines where product is installed.

All Advisories - Provides the list of Secunia Advisory ID and its criticality details.

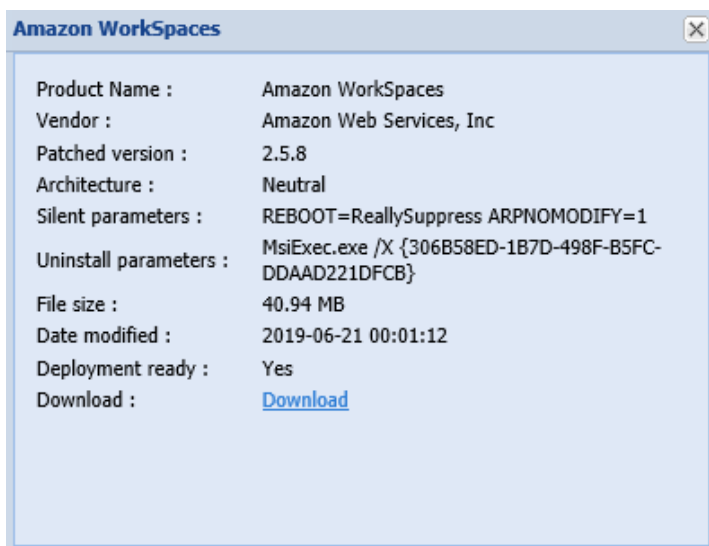


Patch Information

To know the details about any patch in the Vendor Patch Module, Right-click and select Patch Information.

Patch Information provides the following details of a selected patch:

- Product Name
- Vendor
- Patched Version
- Architecture
- Uninstall Parameters (If required)
- File Size in MB
- Date Modified
- Deployment ready status
- Download link



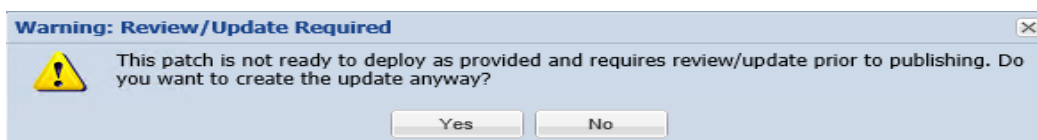
Package Creation Wizard in Vendor Patch Module

The following steps explain how to create update Package:

- [Step 1 of 4: Package Configuration](#)
- [Step 2 of 4: Package Contents](#)
- [Step 3 of 4: Applicability Criteria - Paths](#)
- [Step 4 of 4: Applicability Criteria - Rules](#)

Step 1 of 4: Package Configuration

In Step 1, if the selected product was in **Black** and **Gray** you will get a Warning message. click **Yes** to initiate the **Package Configuration** wizard.



In the Package Configuration wizard, click **Next**.

Step 1 of 4: Package Configuration

Use this form to set the name and description of the VPM package, or edit the properties of an existing one. In the following steps you will configure the package contents and parameters before creating and publishing the package.

Package Name

The package will be created with the following name. Choose a new name if desired.

Name:

Description (Optional)

Here you can give a description of the package. For example, what it does, the contents, usage, etc.

Description:

Reference Id (Optional)

Here you can assign an Id to this package if desired.

Reference Id:

Vendor & Product Naming

Choose this option to overcome limitations in the number of categories that can be published in the SCCM. This will set the vendor attribute of the package to *Flexera* and strip the product version from the product name.

☐ Use Flexera Custom Naming

Step 2 of 4: Package Contents

Step 2 provides the following package details:

- Silent Parameter
- Files to Include
 - Add Local File
 - Add Download Link

Step 2 of 4: Package Contents

Here you configure the package contents, including the silent parameters, and the files included.

Silent Parameters

Here you can provide silent parameters for the package

Silent Parameters: REBOOT=ReallySuppress ARPNO MODIFY=1

Files To Include

Configure the files to include in this package. The grid below shows the files that are currently scheduled to be included, and if they will be downloaded dynamically (i.e., in the case of URLs) or if they are local files. You can add additional files via the 'Add File' button, as well as choose from additional language packages available via the 'Show Localised Files' button. To remove a file, right-click and select 'Remove'.

File(s) to include in the package	Status
Amazon+WorkSpaces.msi	To Be Dynamically Downloaded

Add Local File Add Download Link

Previous Next Publish Cancel

You are also able to change the files that are included in the update package, which can either be local files or links to be dynamically downloaded upon publishing of the package.

Click **Next** to open the **Applicability Criteria - Paths** wizard.



Note • Note the Following:

- If the selected product was **Blue** and **Black** in color, you can see the file(s) to include in the package.
- If the selected product was **Gray** in color, you need to add the file(s) or download link manually.

Step 3 of 4: Applicability Criteria - Paths

In Step 3 you should select the paths/locations to which this package should be applied. These are usually populated by Software Vulnerability Manager based on the scans previously conducted.

Please be advised to only choose paths that are valid to avoid any update loops. You can also use paths with CSIDL and KNOWNFOLDERID if you select the Show Advanced Options check box. These variables should be used with their decimal value.

Step 3 of 4: Applicability Criteria - Paths

Here you can define the path-based applicability rules for this package. Below you will find any relevant paths already found or configured for the package. You can deselect paths in the grid or add paths as needed via the "Add Path" button. Check the "Advanced Options" box to enable additional options in the "Add Path" dialog and to show advanced options in the grid.

☒ Show Advanced Options

Always Install Option

The purpose of this option is to allow installations of new software. For custom packages which are not updates to existing installations, you can bypass the "isInstallable" WSUS rule which will ignore all system paths when deciding if this package can be applied. Note - this will not bypass the rules for checking if something is already installed, or is superseded by a more recent version.

☐ Mark Package as "Always Installable"

Minimum Version Option

The purpose of this option is to allow for updating of older products. Normally one updates a product to its secure version within the same major version. You can alter this behaviour by specifying a custom minimum version. Note: the version you enter must also be supported by the installer itself - you cannot enter arbitrary values here.

Minimum Version:

<input type="checkbox"/> Path	Information	Advanced Options
<input checked="" type="checkbox"/> \Amazon Web Services, Inc\Amazon WorkSpaces\workspaces.exe	Default Install Path	%ProgramFiles(x86)%

For packages (except .msi and .msp) that do not have any paths for applicability, select the Mark Package as “Always Installable” check box to ignore all paths. Paths for App-V and Mac OS X are filtered out since they are not supported for patching.

Use the Minimum Version Option to update older products. Normally, a product is updated to its secure version within the same major version. You can alter this behavior by specifying a custom minimum version.

Click **Next** to open the **Applicability Criteria - Rules** wizard.



Note • The minimum version you enter must also be supported by the installer itself - you cannot enter arbitrary values here.

Step 4 of 4: Applicability Criteria - Rules

In Step 4 you should specify if you want to limit the package to 32-bit or 64-bit systems or computers with specific operating system languages. The patch file to be deployed will be automatically downloaded in the background by the Software Vulnerability Manager console. Once this is completed the Software Vulnerability Manager console will publish the update package into the WSUS/System Center.

The WSUS option will be unavailable if the WSUS Connection is not established.

To export the package select Cabinet File (Export) and click Publish.

Step 4 of 4: Applicability Criteria - Rules

Here you configure the applicability rules for the package.

Configure the system type(s) the package will be applied to.

Apply Package To: ☐ 32-bit Systems Only
☒ 64-bit Systems Only
☐ Both 32-bit and 64-bit Systems

Language Settings

Configure package applicability rules based on language:

☐ Only make package applicable to computers with one of the selected languages.

Select Languages:

- Language
- Chinese - (Simplified)
- Chinese - (Traditional)
- Czech
- Danish
- Dutch
- English

Publish Options

Select option for publishing Flexera package

Publish package using: ☐ WSUS
☐ Altiris
☒ Cabinet File (Export)

Previous | Next | **Publish** | Cancel

To configure your package to only applicable for certain languages of the operating system, select Only make package applicable to computers with one of the selected languages and select the relevant language.

After deployment, you can see the patches for which packages have been successfully created are highlighted in **Green** color in the **Vendor Patch Module** products list. See [Product display criteria for Vendor Patch Module](#).

Software Vulnerability Manager

Dashboard

Scanning

Results

Reporting

Patching

Playerra Package System (SPS)

Patch Template

Agent Deployment

Vendor Patch Module

VSUS / System Center

Available

Deployment

Configuration

External Package Signing

VSUS / System Center (Connected)

Altiris Configuration

Administration

Configuration

Vendor Patch Module

Search Type: Product Search text: Search View from the context of Smart Group: Not Selected Configure View

Product	Vendor	Patched Version	Deployment Reason	SAID	Criticality	Threat Score	Advisory Publics.	Architecture	Insecure	End-Of-Life	Secure	Total	Hosts	Updated On	Download
DVDShtylr (x86)	Alex Thring	3.1.0.0	Yes	-	-	-	-	Windows 32-bit	0	0	0	0	0	12th Jul, 2019 1...	Download
Algoodeo	Algoxy	2.1.0.0	No	-	-	-	-	Windows 32-bit	0	0	0	0	0	2nd May, 2019 0...	Download
Altaro Hyper-V Backup	Altaro	4.1.43.0	No	-	-	-	-	Windows 32-bit	0	0	0	0	0	7th May, 2019 2...	Download
Kindle	Amazon	1.26.0.55076	Yes	SA74634	2	10th Jan, 2017...	-	Windows 32-bit	0	0	0	0	0	12th May, 2019...	Download
Amazon WorkSpaces	Amazon Web Services, I...	2.5.8.0	Yes	-	-	-	-	Windows 32-bit	0	0	0	0	0	20th Jun, 2019 1...	Download
Anaconda 3 (x64)	Anaconda Inc.	5.1.0.0	No	-	-	-	-	Windows 64-bit	0	0	0	0	0	2nd May, 2019 0...	Download
Anaconda 3 (x86)	Anaconda Inc.	5.1.0.0	Yes	-	-	-	-	Windows 32-bit	0	0	0	0	0	11th Jul, 2019 1...	Download
PDFsam Basic	Andrea Vaccondio	4.0.3.0	No	-	-	-	-	Windows 32-bit	0	0	0	0	0	30th May, 2019...	Download
Android Studio	Android	3.4.2.0	No	-	-	-	-	Windows 32-bit	0	0	0	0	0	10th Jul, 2019 1...	Download
Android Studio for Mac	Android	3.4.2.0	No	-	-	-	-	Mac Intel 64-bit	0	0	0	0	0	10th Jul, 2019 1...	Download
HeadSQL	Ansar Becker	9.3.0.4984	No	-	-	-	-	Windows 32-bit	0	0	1	1	1	2nd May, 2019 0...	Download
AnyCAD Viewer 2011	AnyCAD Solution	2.0.1.0	Yes	-	-	-	-	Windows 32-bit	0	0	0	0	0	2nd May, 2019 0...	Download
AnyDesk	AnyDesk Software GmbH	5.2.2.0	Yes	-	-	-	-	Windows 32-bit	0	0	0	0	0	13th Jul, 2019 1...	Download
AnyDesk for Mac	AnyDesk Software GmbH	4.3.0.0	No	-	-	-	-	Mac Intel 32-bit	0	0	0	0	0	15th Jul, 2019 1...	Download
Any DWG to PDF Converter	AnyDWG Software Inc.	2015.0.0.0	No	-	-	-	-	Windows 32-bit	0	0	0	0	0	2nd May, 2019 0...	Download
NetBeans IDE (x64)	Apache	11.0.0.0	No	-	-	-	-	Windows 64-bit	0	0	0	0	0	2nd May, 2019 0...	Download
NetBeans IDE (x86)	Apache	11.0.0.0	No	-	-	-	-	Windows 32-bit	0	0	0	0	0	2nd May, 2019 0...	Download
OpenOffice (English UK)	Apache	4.1.6.0	Yes	SA87068	2	15th Jan, 2019...	Windows 32-bit	0	1	1	2	2	2	25th Jun, 2019 1...	Download
OpenOffice (English US)	Apache	4.1.6.0	Yes	SA87068	2	15th Jan, 2019...	Windows 32-bit	0	1	1	2	2	2	25th Jun, 2019 1...	Download
OpenOffice (English US)	Apache	3.4.1.0	Yes	SA87068	2	15th Jan, 2019...	Windows 32-bit	0	1	1	2	2	2	2nd Jul, 2019 17...	Download
Tomcat	Apache	9.0.22.0	No	SA33326	-	3rd Jun, 2009...	Windows 32-bit	0	0	0	0	0	0	19th Jul, 2019 1...	Download
Tomcat	Apache	7.0.94.0	No	SA33326	-	3rd Jun, 2009...	Windows 32-bit	0	0	0	0	0	0	2nd May, 2019 0...	Download
Tomcat	Apache	8.5.43.0	No	SA33326	-	3rd Jun, 2009...	Windows 32-bit	0	0	0	0	0	0	10th Jul, 2019 1...	Download
ArtServer Universal (x64)	App Dynamic	5.5.7.0	Yes	-	-	-	-	Windows 64-bit	0	0	0	0	0	4th Jul, 2019 17...	Download
ArtServer Universal (x86)	App Dynamic	5.5.7.0	Yes	-	-	-	-	Windows 32-bit	0	0	0	0	0	4th Jul, 2019 17...	Download
Free AppDeploy Repackager	Free AppDeploy	1.2.5.0	Yes	-	-	-	-	Windows 32-bit	0	0	0	0	0	2nd May, 2019 0...	Download
Application Support (x64)	Apple	7.6.0.0	Yes	SA33216	-	25th Apr, 2013...	Windows 64-bit	0	0	0	0	0	0	24th Jul, 2019 1...	Download
Application Support (x86)	Apple	7.6.0.0	Yes	SA33216	-	25th Apr, 2013...	Windows 32-bit	0	0	0	0	0	0	24th Jul, 2019 1...	Download
iCloud (x64)	Apple	7.13.0.14	No	-	-	-	-	Windows 64-bit	0	0	0	0	0	24th Jul, 2019 1...	Download
iCloud (x86)	Apple	7.13.0.14	Yes	-	-	-	-	Windows 32-bit	0	0	0	0	0	24th Jul, 2019 1...	Download

Automating Patch Deployment

In Vendor Patch Module, new option [Subscribe to Package](#) has been added to right click menu which helps user to automate deployment of patches.

Subscribed packages will be deployed automatically to configured WSUS using a new tool called **Software Vulnerability Manager Client ToolKit**, see [Download and Install the Software Vulnerability Manager Client ToolKit](#).

To use this option, navigate to **Patching >> Vendor Patch Module**. List of patches appears.

You can know a patch whether it is already subscribed and its status in the **Subscribed** and **Subscription Status** column.

Right click on a patch which you want to subscribe, select the below option:

- [Subscribe to Package](#)
- [Edit Subscription](#)



Note • Install **Software Vulnerability Manager Client ToolKit** to utilize the Vendor Patch Module - Automation.

Vendor Patch Module											
Search Type: Product	Search text	Search	View from the context of Smart Group: Not Selected		Configure View						
Product	Vendor	Patched Version	Deploy...	SAID	Criticality	Threat Sc...	Advisory Publish...	Architecture	Insecu...	Subscribed	Subscription Started
1Password	AgileBits	7.3.712.0	Yes	-	-	-	-	Windows 32-bit ...	0	Yes	8th Dec, 2019 17:05
4K Video Downloader	OpenMedia	4.10.1.3240	Yes	-	-	-	-	Windows 64-bit ...	0	Yes	8th Dec, 2019 17:05
4K Video Downloader for Mac	OpenMedia	4.10.0.3230	No	-	-	-	-	Mac Intel 64-bit	0	No	
SKPlayer (x64)	DearMob Inc.	6.1.0.0	No	-	-	-	-	Windows 64-bit	0	No	
SKPlayer (x86)	DearMob Inc.	6.1.0.0	No	-	-	-	-	Windows 32-bit	0	No	
SKPlayer for Mac	DearMob Inc.	6.1.0.0	No	-	-	-	-	Mac Intel 64-bit	0	No	
7-Zip (x64)	7-Zip	19.00.00.0	Yes	-	-	-	-	Windows 64-bit	1	No	
7-Zip (x86)	7-Zip	19.00.00.0	Yes	-	-	-	-	Windows 32-bit	0	No	
ABBYY FineReader	ABBYY	15.0.1496.0	No	-	-	-	-	Windows 64-bit	0	No	
ABBYY FineReader	ABBYY	15.0.1496.0	No	-	-	-	-	Windows 32-bit	0	No	
Accumulated hotfix 1 for Auto...	Autodesk Inc.	21.0.52.0.4	No	SA908...		-	27th Aug, 2019 ...	Windows 64-bit	0	No	
Accumulated hotfix 1 for Auto...	Autodesk Inc.	21.0.52.0.4	No	SA908...		-	27th Aug, 2019 ...	Windows 64-bit	0	No	
Accumulated hotfix 1 for Auto...	Autodesk Inc.	21.0.107.0.19	No	SA908...		-	27th Aug, 2019 ...	Windows 32-bit	0	No	
ACDSee (32-bit)	ACD systems Internati...	20.4.0.630	Yes	-	-	-	-	Windows 32-bit	0	Yes	20th Nov, 2019 15:21
ACDSee (64-bit)	ACD systems Internati...	20.4.0.630	No	-	-	-	-	Windows 64-bit	0	No	
Acrobat 10.1.16 Pro and St...	Adobe	10.1.16.0	No	SA890...		12	15th Oct, 2019 ...	Windows 32-bit ...	0	No	
Acrobat 11.0.23 Pro and St...	Adobe	11.0.23.0	No	SA890...		12	15th Oct, 2019 ...	Windows 32-bit ...	0	No	
Acrobat DC Pro and Standa...	Adobe	17.11.30152.0	No	SA890...		12	15th Oct, 2019 ...	Windows 32-bit ...	0	No	
Acrobat DC Pro and Standa...	Adobe	15.006.30505.0	No	SA890...		12	15th Oct, 2019 ...	Windows 32-bit ...	0	No	
Acrobat DC Pro and Standa...	Adobe	19.021.20056.0	No	SA890...		12	15th Oct, 2019 ...	Windows 32-bit ...	3	No	
Acrobat Reader 2017 Classi...	Adobe	17.008.30051.0	No	SA890...		12	15th Oct, 2019 ...	Windows 32-bit ...	0	No	
Acrobat Reader 2017 Classi...	Adobe	17.11.30152.0	No	SA890...		12	15th Oct, 2019 ...	Windows 32-bit ...	0	No	
ActivDriver x64	Promethean Ltd	5.16.7.0	No	-	-	-	-	Windows 64-bit	0	No	
ActivDriver x86	Promethean Ltd	5.16.7.0	No	-	-	-	-	Windows 32-bit	0	No	

Subscribe to Package

Subscribe to package option provides interface to define the threshold for automation. It helps you to set the below preferences, based on your requirements.

Either one of the below preferences can be defined:

- **Always publish a new patch when a new version is available** - Publishes when new version of the patch is available.
- **Only publish a new patch when any of the following are true:** Publishes when any one of the defined preferences are met. To know more about the below preferences, see [Appendix B - About Secunia Advisories](#).

- **SAID CVSS3 score is greater than**
- **Criticality is greater than**
 - Extremely Critical
 - Highly Critical
 - Moderately Critical
 - Less Critical
 - Not Critical
- **Threat score is greater than**
- **Patched version greater than** - By default current version of a patch will be displayed

Either one of these option must be selected to define the deployment schedule based on the above preferences:

- **Trigger subscription rule above now for the current version** - Publishes the package right away
- **Trigger subscription rule above next time a new version is available** - Start publishes the package when newer version is available



Task

To automate a patch deployment do the below following:

1. Right click a product or multiple products, select **Subscribe to Package** option. **Configure Subscription** wizard appears.

2. Choose your preferences and select your deployment schedule. Click **Save**.



Note • To unsubscribe the subscription, see [Edit Subscription](#).

Edit Subscription

If the package is already subscribed as explained in [Subscribe to Package](#), you can right click and select **Edit Subscription** to edit the configured preferences. To unsubscribe the subscription, click **Unsubscribe** button.

Configure Subscription - 1Password

Subscription started on 13th Jan, 2020 05:05

☒ Always publish a new patch when a new version is available
☐ Only publish a new patch when any of the following are true:

SAID CVSS3 score is greater than

Criticality is greater than

Threat score is greater than

Patched version greater than

☐ Trigger subscription rule above now for the current version
☒ Trigger subscription rule above next time a new version is available

Package configuration

☒ Use Flexera custom naming

Unsubscribe Save Cancel

Agent Deployment

If you choose to scan the target host by using the Software Vulnerability Manager Agent in Single Host mode (recommended), you can easily distribute and install the Agent by deploying it through WSUS/System Center.

Click **Create CSI Agent Package** under **Agent Deployment** to start the Software Vulnerability Manager Agent Package wizard.

Agent Deployment

Agent Summary

Below is a summary of the Software Vulnerability Manager Agents currently installed in the network.

NOTE: The statistics are based on scan results thus may be out of synchronisation with your WSUS/System Center server if a scan has not been recently performed.

Overall Agent Statistics

Total Number of Hosts:	65
Number of Hosts with an Agent Installed:	36
Number of Hosts without an Agent Installed:	29

Version Statistics for Installed Agents

Hosts with the Newest Agent Installed ($\geq 7.6.0.2$):	2
Hosts with an Older Agent Installed ($\geq 7.0.0.0$ and $< 7.6.0.2$):	34
Hosts with an Outdated Agent Installed ($< 7.0.0.0$):	0

Deploy the Software Vulnerability Manager Agent through your Microsoft WSUS/System Center Server

Click "Create Software Vulnerability Manager Agent Package" to start the Software Vulnerability Manager Agent Package wizard.

Create Software Vulnerability Manager Agent Package

The Software Vulnerability Manager Agent Package can be created and managed just like any other SPS package. You can also [Add Proxy Settings](#).

Add Proxy Settings

You can add proxy settings to the installation script in the SPS wizard when creating the agent deployment package. In [Step 2 of 4: Package Contents](#), modify the variables in the Execution Flow field.

Step 2 of 4: Package Contents
Here you configure the package contents, including the execution script included, and the files included.

Execution Script
View/Edit the execution flow and script type for this SPS package.

Script Type: **JScript (Javascript)**

Execution Flow:

```
// The following variables can be optionally modified and will be
// used accordingly
var proxyUsername = ""; // NOTE: If proxyUsername is entered you must enter
runAsUsername and runAsPassword as well
var proxyPassword = ""; // NOTE: If proxyPassword is entered you must enter
runAsUsername and runAsPassword as well
var proxyHost = "";
var proxyPort = "";
var runAsUsername = ""; // If a domain is used please use: user@domain
var runAsPassword = "";
var siteName = "";

function main() {
    if ( !GUID ) {
        server.logMessage( "No GUID supplied for package " + Title );
    }
}
```

Files To Include
Configure the files to include in this package. The grid below shows the files that are currently scheduled to be included, and if they will be downloaded dynamically (i.e., in the case of URLs) or if they are local files. You can add additional files via the 'Add File' button, as well as choose from additional language packages available via the 'Show Localised Files' button. To remove a file, right-click and select 'Remove'.

File(s) to include in the package	Status
http://dl.secunia.com/SPS/GoogleChrome_66.0.3359.139_64-bit_SPS.exe	To Be Dynamically Downloaded

Add Local File Add Download Link Add Localisation (Language) File

Create SPS File
You also have the option of creating an SPS File from this package, should you wish to.

Create SPS File

Previous Next Publish Cancel

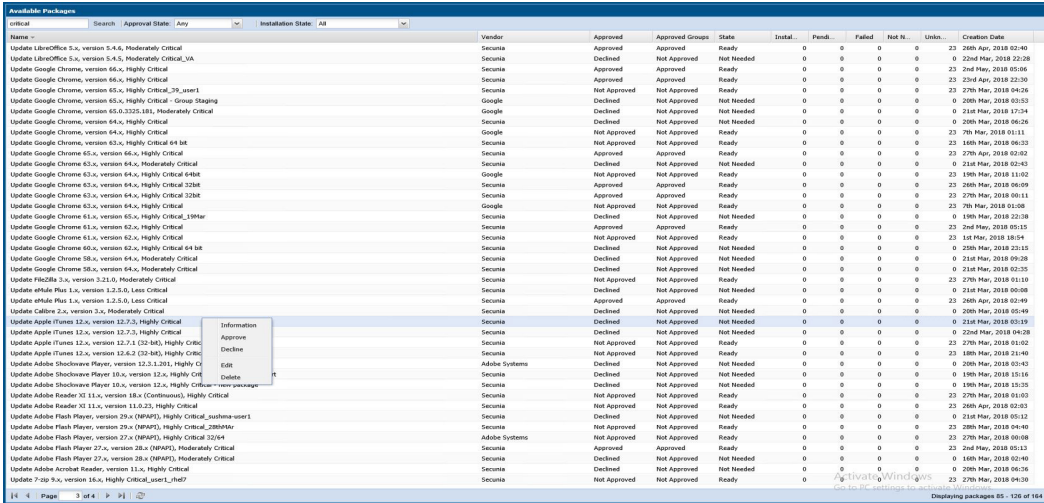
WSUS/System Center

The following sections describe the WSUS/System Center:

- [Available](#)
- [Deployment](#)

Available

Right-click a package for more options such as **Approve**, **Decline** or **Delete** or double-click a package to display additional status details.



Name	Search	Approval State	Any	Installation State	All	Vendor	Approved	Approved Groups	Status	Instal.	Pend.	Failed	Not H.	Unin.	Creation Date
Update LibreOffice 5.x, version 5.4.6, Moderately Critical						Secunia	Approved	Approved	Ready	0	0	0	0	0	23 26th Apr, 2018 02:40
Update LibreOffice 5.x, version 5.4.6, Moderately Critical, VA						Secunia	Declined	Not Approved	Not Needed	0	0	0	0	0	22nd Mar, 2018 22:28
Update Google Chrome, version 66.0, Highly Critical						Secunia	Approved	Approved	Ready	0	0	0	0	0	23 2nd Mar, 2018 05:06
Update Google Chrome, version 66.0, Highly Critical						Secunia	Approved	Approved	Ready	0	0	0	0	0	23 2nd Mar, 2018 22:39
Update Google Chrome, version 65.x, Highly Critical, 39_user1						Secunia	Not Approved	Not Approved	Ready	0	0	0	0	0	23 27th Mar, 2018 04:26
Update Google Chrome, version 65.x, Highly Critical - Group Staging						Google	Declined	Not Approved	Not Needed	0	0	0	0	0	0 29th Mar, 2018 03:53
Update Google Chrome, version 65.0.3325.181, Moderately Critical						Google	Declined	Not Approved	Not Needed	0	0	0	0	0	0 21st Mar, 2018 17:34
Update Google Chrome, version 64.x, Highly Critical						Secunia	Declined	Not Approved	Not Needed	0	0	0	0	0	0 29th Mar, 2018 06:26
Update Google Chrome, version 64.x, Highly Critical						Secunia	Declined	Not Approved	Ready	0	0	0	0	0	23 7th Mar, 2018 01:11
Update Google Chrome, version 63.x, Highly Critical 64 bit						Google	Not Approved	Not Approved	Ready	0	0	0	0	0	23 16th Mar, 2018 06:23
Update Google Chrome 65.x, version 64.x, Highly Critical						Secunia	Approved	Approved	Ready	0	0	0	0	0	23 27th Apr, 2018 02:02
Update Google Chrome 65.x, version 64.x, Highly Critical						Secunia	Declined	Not Approved	Not Needed	0	0	0	0	0	0 21st Mar, 2018 02:42
Update Google Chrome 65.x, version 64.x, Highly Critical 64bit						Google	Not Approved	Not Approved	Ready	0	0	0	0	0	23 19th Mar, 2018 11:02
Update Google Chrome 65.x, version 64.x, Highly Critical 32bit						Secunia	Approved	Approved	Ready	0	0	0	0	0	23 26th Mar, 2018 06:09
Update Google Chrome 65.x, version 64.x, Highly Critical 32bit						Secunia	Approved	Approved	Ready	0	0	0	0	0	23 27th Mar, 2018 06:11
Update Google Chrome 65.x, version 64.x, Highly Critical						Google	Not Approved	Not Approved	Ready	0	0	0	0	0	23 7th Mar, 2018 01:08
Update Google Chrome 61.x, version 65.x, Highly Critical, 189Mar						Secunia	Declined	Not Approved	Not Needed	0	0	0	0	0	0 19th Mar, 2018 22:38
Update Google Chrome 61.x, version 62.x, Highly Critical						Secunia	Approved	Approved	Ready	0	0	0	0	0	23 2nd Mar, 2018 05:15
Update Google Chrome 61.x, version 62.x, Highly Critical						Secunia	Not Approved	Not Approved	Ready	0	0	0	0	0	23 1st Mar, 2018 18:54
Update Google Chrome 65.x, version 62.x, Highly Critical 64 bit						Secunia	Declined	Not Approved	Not Needed	0	0	0	0	0	0 25th Mar, 2018 23:15
Update Google Chrome 58.x, version 64.x, Moderately Critical						Secunia	Declined	Not Approved	Not Needed	0	0	0	0	0	0 21st Mar, 2018 09:38
Update Google Chrome 58.x, version 64.x, Moderately Critical						Secunia	Declined	Not Approved	Not Needed	0	0	0	0	0	0 21st Mar, 2018 02:35
Update Firefox 3.x, version 3.21.0, Moderately Critical						Secunia	Not Approved	Not Approved	Ready	0	0	0	0	0	23 27th Mar, 2018 01:10
Update eHub Plus 1.x, version 1.2.5.0, Less Critical						Secunia	Declined	Not Approved	Not Needed	0	0	0	0	0	0 21st Mar, 2018 06:08
Update eHub Plus 1.x, version 1.2.5.0, Less Critical						Secunia	Approved	Approved	Ready	0	0	0	0	0	23 26th Apr, 2018 02:49
Update Calloria 2.x, version 3.x, Moderately Critical						Secunia	Declined	Not Approved	Not Needed	0	0	0	0	0	0 20th Mar, 2018 05:49
Update Apple iTunes 12.x, version 12.7.3, Highly Critical						Secunia	Declined	Not Approved	Not Needed	0	0	0	0	0	0 21st Mar, 2018 02:19
Update Apple iTunes 12.x, version 12.7.3, Highly Critical						Secunia	Declined	Not Approved	Not Needed	0	0	0	0	0	0 22nd Mar, 2018 04:28
Update Apple iTunes 12.x, version 12.7.1 (32-bit), Highly Critic						Secunia	Not Approved	Not Approved	Ready	0	0	0	0	0	23 27th Mar, 2018 01:02
Update Apple iTunes 12.x, version 12.6.2 (32-bit), Highly Critic						Secunia	Not Approved	Not Approved	Ready	0	0	0	0	0	23 18th Mar, 2018 21:46
Update Adobe Shockwave Player, version 12.0.3.201, Highly Cr						Adobe Systems	Declined	Not Approved	Not Needed	0	0	0	0	0	0 20th Mar, 2018 03:43
Update Adobe Shockwave Player 10.x, version 12.x, Highly Cr						Secunia	Declined	Not Approved	Not Needed	0	0	0	0	0	0 19th Mar, 2018 15:16
Update Adobe Shockwave Player 10.x, version 12.x, Highly Cr						Secunia	Declined	Not Approved	Not Needed	0	0	0	0	0	0 19th Mar, 2018 15:25
Update Adobe Reader XI 11.x, version 18.x (Continuous), Highly Critical						Secunia	Not Approved	Not Approved	Ready	0	0	0	0	0	23 27th Mar, 2018 01:03
Update Adobe Reader XI 11.x, version 11.0.23, Highly Critical						Secunia	Not Approved	Not Approved	Ready	0	0	0	0	0	23 26th Apr, 2018 02:03
Update Adobe Flash Player, version 29.x (PPAPI), Highly Critical, 389Mar						Secunia	Declined	Not Approved	Not Needed	0	0	0	0	0	0 21st Mar, 2018 05:12
Update Adobe Flash Player, version 29.x (PPAPI), Highly Critical, 389Mar						Secunia	Not Approved	Not Approved	Ready	0	0	0	0	0	23 28th Mar, 2018 04:40
Update Adobe Flash Player, version 27.x (PPAPI), Highly Critical 32bit						Adobe Systems	Not Approved	Not Approved	Ready	0	0	0	0	0	23 27th Mar, 2018 06:08
Update Adobe Flash Player 27.x, version 28.x (PPAPI), Moderately Critical						Secunia	Approved	Approved	Ready	0	0	0	0	0	23 2nd Mar, 2018 05:13
Update Adobe Flash Player 27.x, version 28.x (PPAPI), Moderately Critical						Secunia	Declined	Not Approved	Not Needed	0	0	0	0	0	0 16th Mar, 2018 02:40
Update Adobe Acrobat Reader, version 11.x, Highly Critical						Secunia	Declined	Not Approved	Not Needed	0	0	0	0	0	0 29th Mar, 2018 06:26
Update 7-zip 1.x, version 16.x, Highly Critical, user1, chet						Secunia	Not Approved	Not Approved	Ready	0	0	0	0	0	23 27th Mar, 2018 04:36



Important • Once the updates have been published into the WSUS, the same rules previously configured for the Microsoft updates will apply to the updates created by Software Vulnerability Manager. If the updates automatically appear with the Approved status, this means that this setting is being inherited from the WSUS.

Deployment

Use this page to view a host's information collected from the WSUS Server. Use the **Installation State** drop-down list to filter the hosts being displayed.

Right-click a host and select **Information** to view additional details such as: **Scan Result**, **Patch Information**, **Patches Available** and **Overview**.

You can also right-click a host listed in this view and select **Verify and Install Certificate** to install the required certificate created or imported in [Step 2 - Certificate Status](#).

Usually the certificate is installed through a GPO as described in [Step 3 – Group Policy Status](#).

In order for Software Vulnerability Manager to connect to WSUS and to create packages successfully, Internet Explorer must be run **As Administrator** in most cases (right-click and select Run as administrator). Also note that the Remote Registry must be enabled on hosts for which you intend to install the certificate using the Software Vulnerability Manager GUI. The remote registry is not needed if distributing the certificate through GPO.

The WSUS Self-Signed Certificate can also be installed through a manually created Group Policy.

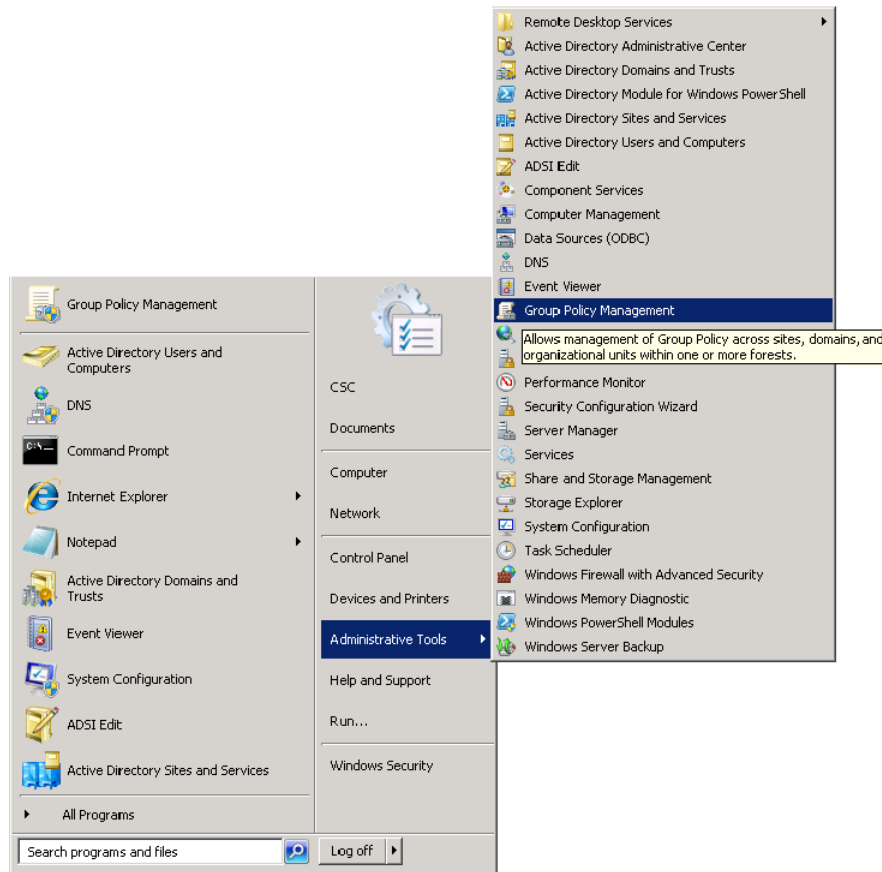
Creating the WSUS-CSI GPO Manually



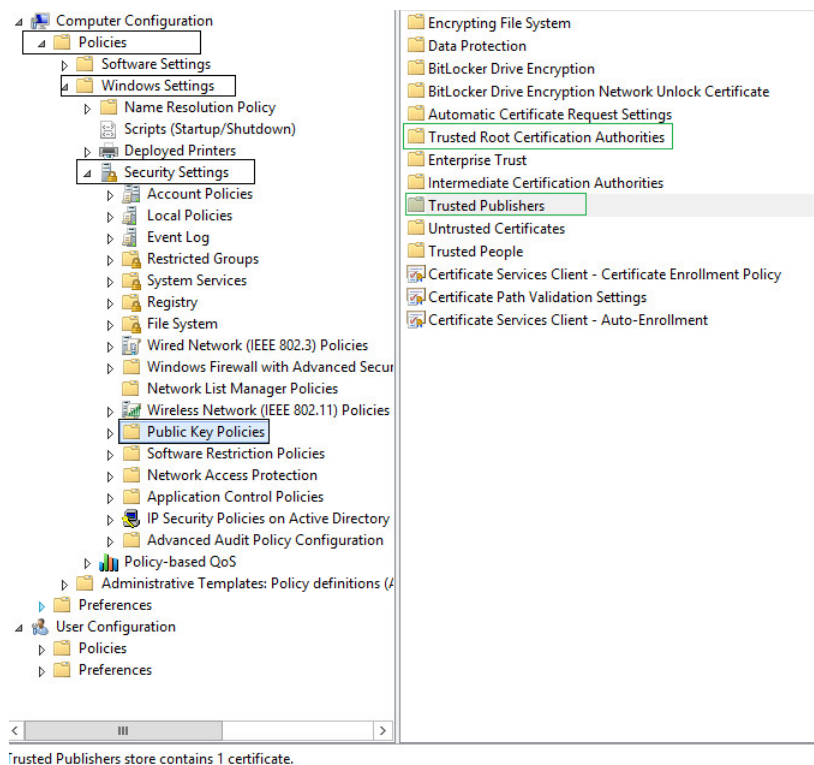
Task

To create the WSUS-CSI GPO manually:

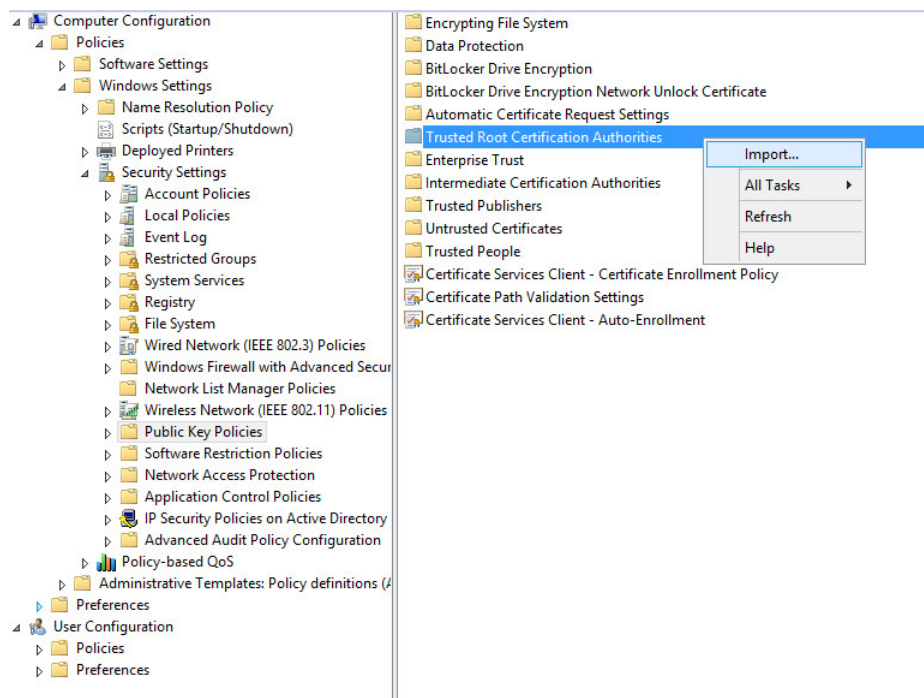
1. Export the WSUS Self-Signed Certificate.
2. On the Domain Controller, click **Start > Administrative Tools > Group Policy Management**. Right-click your Domain name and select **Create a GPO in this domain, and Link it here**. Alternatively you can edit an existing GPO.



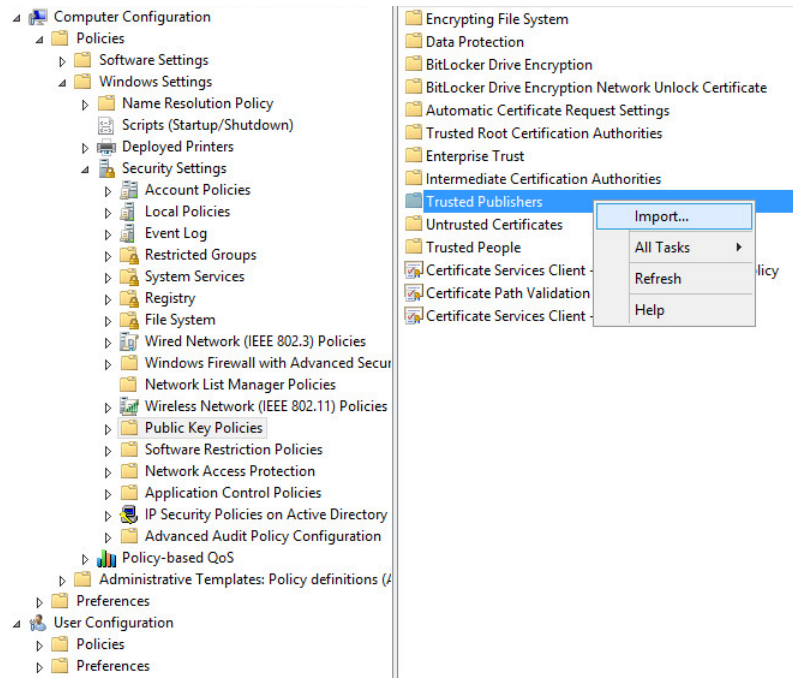
3. Right-click the GPO that you created/edited in the previous steps and select **Edit**.
4. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.



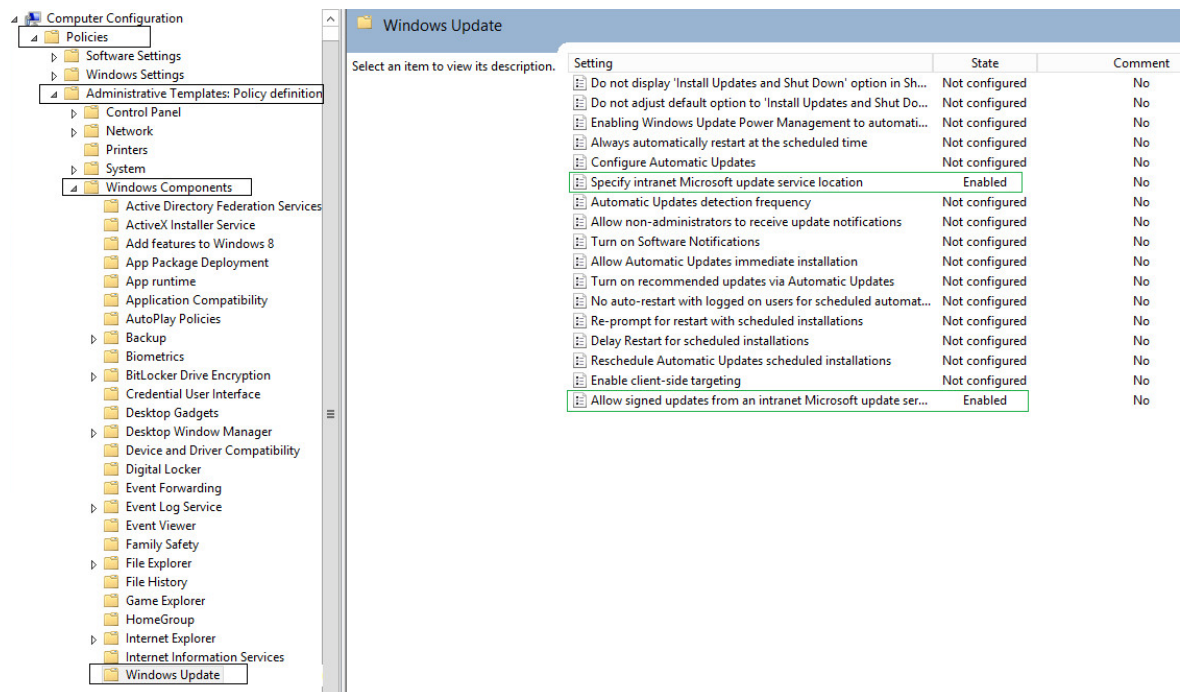
5. Right-click **Trusted Root Certification Authority** and select **Import**. Import the certificate that you exported in Step 1.



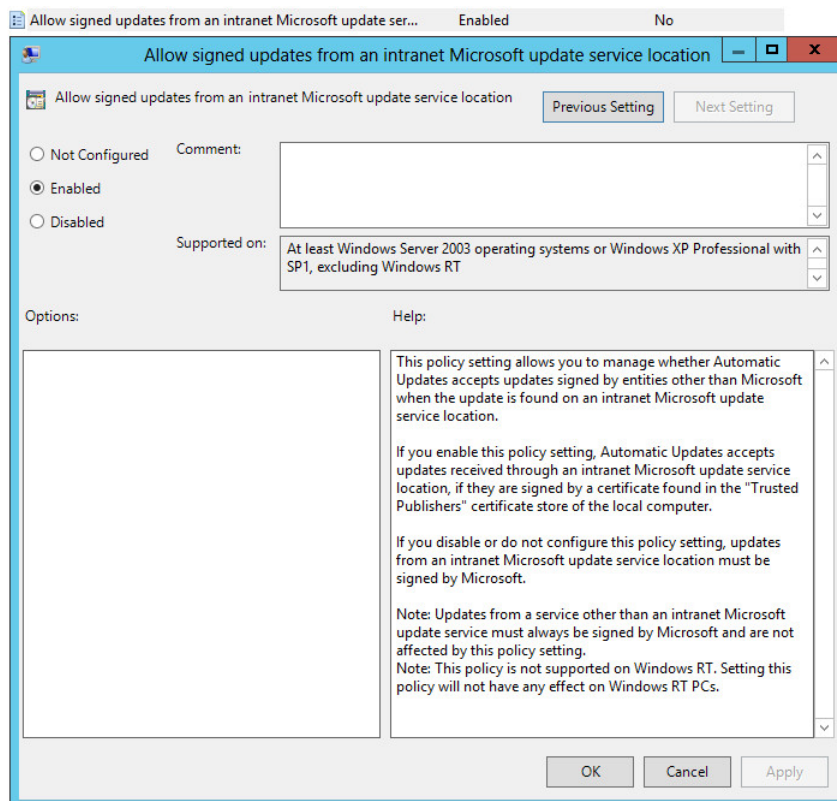
6. Repeat Step 4 and import the certificate for **Trusted Publishers**.



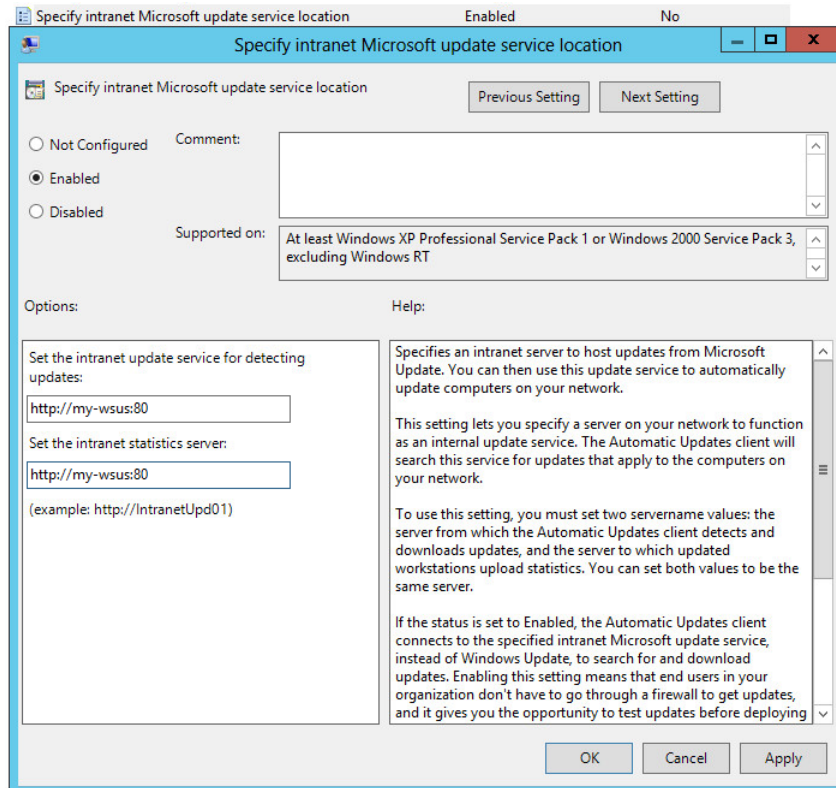
7. Navigate to **Computer Configuration > Administrative templates > Windows Component > Windows Update**.



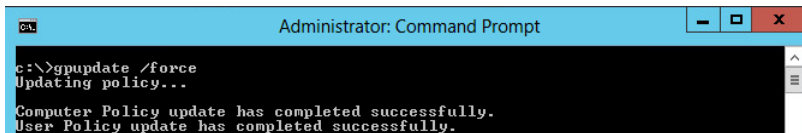
8. On the right side menu, double-click **Allow signed updates from an intranet Microsoft update service location**. Select **Enabled** and click **OK**.



9. On the right side menu, double-click **Specify intranet Microsoft update service location**. Enable this setting and modify the existing empty fields with the intranet address of your WSUS Server. This step is only valid for WSUS integration and is not required for System Center Configuration Manager integration.



10. Link the created GPO to an Active Directory container appropriate for your environment.



The clients affected by the created GPO will install the certificate being distributed (either the WSUS Self-Signed Certificate or your own CA certificate) and acknowledge the Windows Update settings that you have specified in the GPO.

By default, Group Policy refreshes in the background every 90 minutes, with a random offset of 0 to 30 minutes. If you want to refresh Group Policy sooner, you can go to a command prompt on the client computer and type:

```
gpupdate /force
```

Refer to <http://technet.microsoft.com/en-us/library/cc720539> for further information on how to configure Automatic Updates by Using Group Policy.

Deploying the Update Package Using WSUS

To deploy the update package using WSUS, the update package must be approved. After publishing the package into the WSUS, and assuming that the update is visible under **Available**, right-click the package name and select **Approve**.

You will be prompted to select the computer target groups for which you would like to approve the update. These target groups are configured in the WSUS.

The same approach should be used if you wish to decline a previously approved update.

Deploying the Update Package Using System Center

The actions **Approve** and **Decline** are only applicable if the package is to be deployed through WSUS. If you are using the Microsoft System Center, the package created with Software Vulnerability Manager will be available in your System Center.

Patch Configuration

The following patch configurations are available in Software Vulnerability Manager:

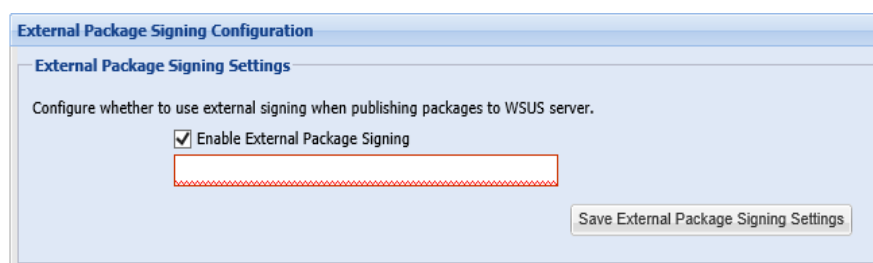
- [External Package Signing](#)
- [WSUS/System Center](#)
- [Setting Up Clients to Access WSUS](#)
- [Third-Party Integration](#)
- [Create and Publish the Package](#)

External Package Signing

Software Vulnerability Manager allows you to export packages as Cabinet files (.cab) which can be used to publish signed cab files using the Software Vulnerability Manager Daemon. To enable this feature, you must run `daemon.exe -S --publish-dir <PATH>` after the Daemon has been installed. This will initiate a monitoring feature in the Daemon which will look for Cabinet files in the directory `<PATH>/Flexera Software IO/`.



Note • `<PATH>` must be an existing directory that is accessible by the user the Daemon is running as and the subdirectory `Flexera Software IO` is added by the Daemon for security reasons.



Select **Enable External Package Signing** on the configuration page and provide a path to where the packages will be exported. Similar to the Software Vulnerability Manager Daemon, a subdirectory (`Flexera Software IO`) will be added for security reasons.

Specify the recipients who will receive an email notification when a package is published or if it failed to do so.

If the External Package Signing option is enabled the SPS Package Wizard will by default select the Cabinet File (Export) option in Step 4.

An export will create a Cabinet file which includes the files required to patch applicable components.

To publish these packages you must sign them and place them in the Daemon monitoring directory. The WSUS server must be set up correctly with the certificate used to sign the packages. Once a Cabinet file has been exported it can be signed using your favorite signing method. Then, after placing it in the directory monitored by the Daemon, it will be picked up and published to the WSUS server. You must ensure that the WSUS server can verify the certificate used for signing.

A notification email will be sent to the account email of the user running the Daemon to inform the user know about success or failure for published packages.

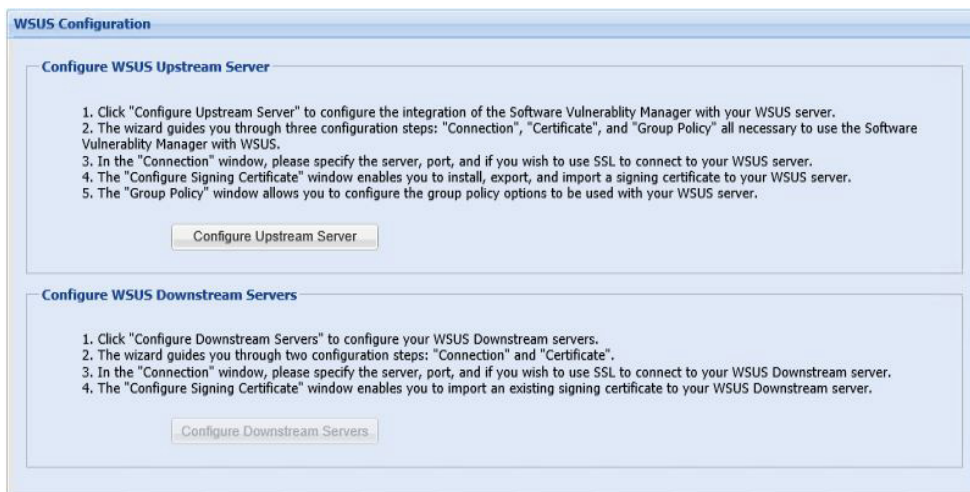


Note • The export and monitoring directories should not be the same since it will try to publish unsigned Cabinet files which will not be allowed.

WSUS/System Center

Use this option to configure the integration of Software Vulnerability Manager with your WSUS server(s). If you have a single WSUS server, which is connected to the Microsoft Updates site, running the **Configure Upstream Server** wizard will be sufficient for setting up Software Vulnerability Manager with WSUS.

After clicking **Configure Upstream Server**, a configuration wizard will be initiated.



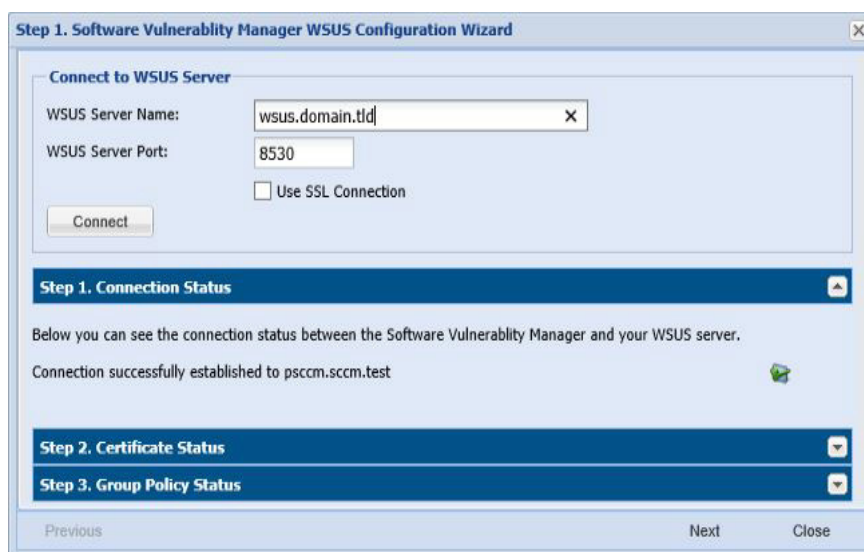
Follow the wizard steps to successfully integrate Software Vulnerability Manager with your Microsoft WSUS.

- [Step 1 – Connection Status](#)
- [Step 2 - Certificate Status](#)
- [Step 3 – Group Policy Status](#)

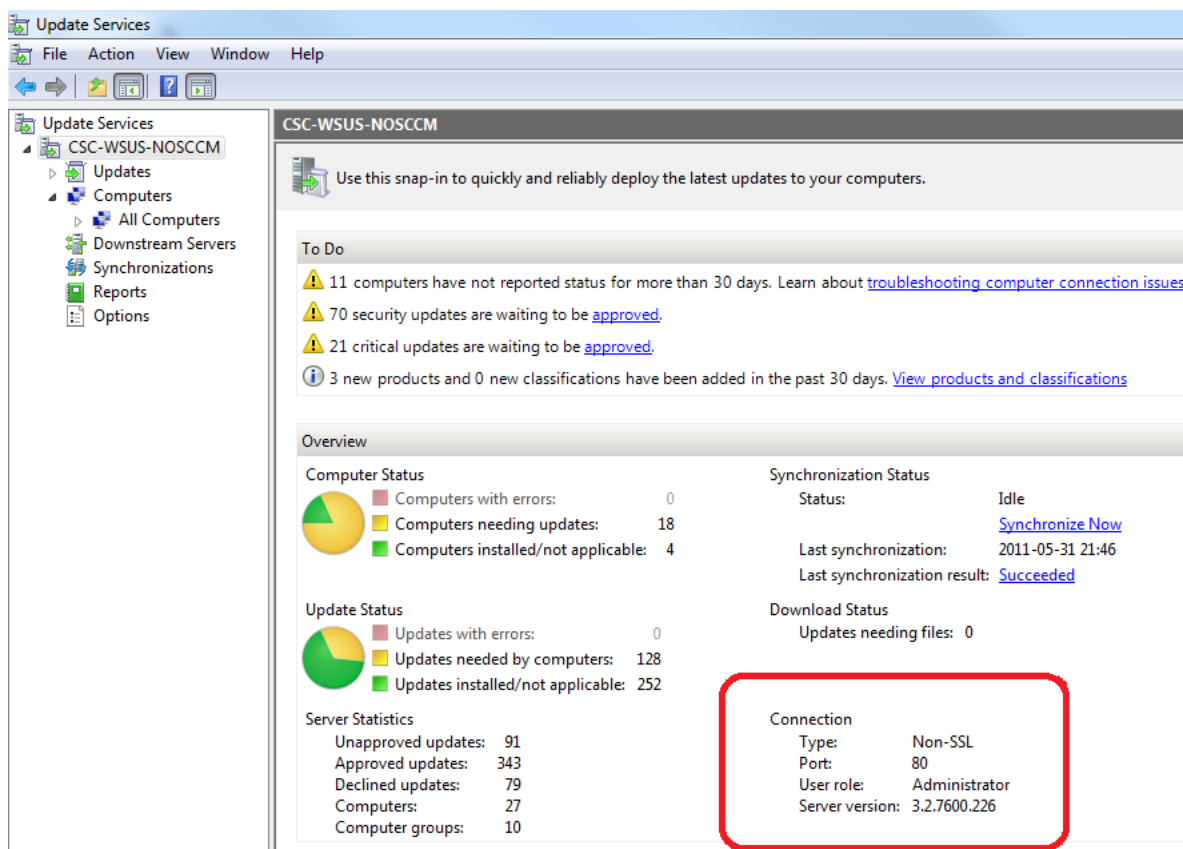
Step 1 – Connection Status

In Step 1 you should provide the relevant information (NetBIOS name and port number) for the main Upstream WSUS server. After inserting the required information, click **Connect**.

To check the status of the connection, expand **Step 1. Connection Status**.



If you are unsure of which port number to use, check your WSUS configuration as shown.



Important • If you have a WSUS server hierarchy with one or more Downstream Replica WSUS server(s) connected to an Upstream WSUS server, please run the **Configure Downstream Servers** after running the **Configure Upstream Server** wizard.



Important • The port number used to connect to your WSUS depends on your settings. Ports 80 or 8530 are commonly used when SSL is not configured. Only select the **Use SSL Connection** check box if your WSUS is configured to accept SSL connections.



Important • Refer to <http://technet.microsoft.com/en-us/library/bb633246.aspx> for further information on how to configure WSUS to use SSL.

Step 2 - Certificate Status

A code-signing certificate is needed to publish third-party updates to WSUS/System Center so they can be deployed as patches. In this Step Software Vulnerability Manager can request the WSUS to create and install the WSUS Self-Signed Certificate.

To create and install a WSUS Self-Signed Certificate in all appropriate certificate stores, click **Automatically create and install certificate**.

The WSUS Self-Signing Certificate must be installed/provisioned in the following systems:

- WSUS Server

The system running Software Vulnerability Manager (note that the certificate must also be installed on the system running the Software Vulnerability Manager console)

- Clients receiving the Update

The created certificate is required and it will be used for all future publishing. Without it, only packages from Microsoft Update will be installed.

If you would like to use your own CA certificate instead of the Microsoft WSUS Self-Signing Certificate, click **Import Signing Certificate**.

At [Step 3 – Group Policy Status](#), the certificate created/imported in this step will be provisioned to all clients through a GPO.



Important • Be careful not to re-provision a signing certificate on a WSUS server that already has a signing certificate assigned. Doing so can cause issues with certificate validation at the WSUS server and target computers unless BOTH certificates (new and old) are left in the appropriate certificates stores (Trusted Publishers and Trusted Root Authorities). It can also cause issues with troubleshooting.

Once a certificate is either inserted or created it does not need to be re-created until it expires or needs to be replaced.

Click **Automatically create and install certificate**. The certificate will be installed on the WSUS server in the following stores:

- Trusted Root Certification Authorities
- Trusted Publishers
- WSUS – The certificate in this location must also contain the private key

Expand the Certificate Options to access the import and export certificate features.

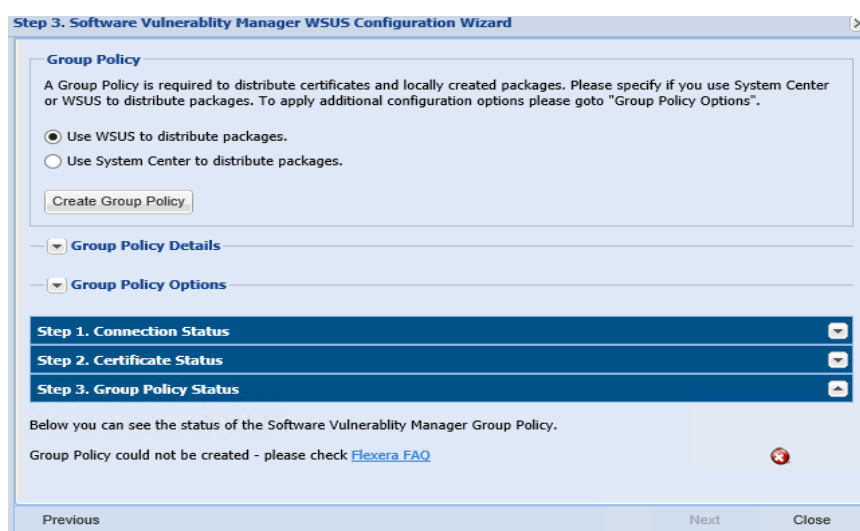


Important • To import your own certificate through Software Vulnerability Manager, the WSUS connection must be configured to accept SSL connections.

Step 3 – Group Policy Status

A Group Policy is required to distribute certificates and locally created packages. Software Vulnerability Manager can easily create this GPO so the WSUS Signing Certificate is distributed to all clients. Please choose to use WSUS or System Center. Once this is completed expand the Group Policy Options.

If you are creating the Software Vulnerability Manager WSUS Group Policy for the first time, proceed by selecting all the options and then click **Create Group Policy**.



Important • Besides distributing the certificate through the Software Vulnerability Manager WSUS GPO, it is also possible to provision certificate to the target computers by going to **Patching > WSUS/System Center > Deployment**, selecting the target hosts where the certificate is to be installed (CTRL+ mouse click for multiple selection) and then right-click and select **Verify and Install Certificate**.

Remote Registry service (disabled by default on Win7/Vista) should be enabled and started for the certificate to be successfully installed.

If you prefer to create your own Group Policy to distribute the WSUS Signing Certificate, please refer to [Creating the WSUS-CSI GPO Manually](#). If you prefer not to create the Software Vulnerability Manager WSUS Group Policy, the existing Windows Updates GPOs must be edited in accordance with [Setting Up Clients to Access WSUS](#).



Important • If you use **Microsoft System Center Configuration Manager** please make sure you **do not select** the first option **Use the WSUS Server specified in Software Vulnerability Manager**.



Important • If you already have the Windows Updates being configured through a Group Policy, we suggest you select the first 3 options in the **Create a new Software Vulnerability Manager WSUS Group Policy** page.



Important • The Software Vulnerability Manager WSUS Group Policy will be created but not linked to your domain. This way you can easily check the details of the newly created GPO and verify that the existing WSUS GPOs are correctly configured.

Setting Up Clients to Access WSUS

If you choose not to create a new Group Policy using the Software Vulnerability Manager WSUS Group Policy wizard, please edit your existing WSUS Group Policy as follows:

1. In the Group Policy Management Console (GPMC), browse to the Group Policy Object (GPO) on which you want to configure WSUS and click **Edit**.
2. In the GPMC, expand **Computer Configuration**, expand **Administrative Templates**, expand **Windows Components**, and click **Windows Update**. Select:
 - **Enable:** Configure Automatic Updates (choose your settings)
 - **Enable:** Specify intranet Microsoft update service location (add the hostname/IP of your WSUS server)
 - **Enable:** Allow signed updates from an intranet Microsoft update service location (**Important** – enables WSUS to distribute patches through Software Vulnerability Manager)



Important • For installing the WSUS server in your environment we recommend reading the **Step by Step Installation Guide** provided by Microsoft:

<http://technet.microsoft.com/en-us/wsus/default.aspx>

Third-Party Integration

Software Vulnerability Manager provides you with the capability of publishing packages using third-party patch deployment solutions, for example Altiris. To support this feature, Flexera has enhanced the package export feature. The exported xml file contains additional information that can be helpful in creating packages in other tools, including:

- The version numbers
- The executable itself
- The vulnerability/criticality

Flexera has retained the simplicity of the xml file by giving you the options to exclude large binary files and applicability paths from the file, in the form of check boxes in the package creation wizard. To perform a complete export, clear the **Do not include package files** check box during Step 4 of the SPS Package Creation Wizard.

In order for Software Vulnerability Manager to integrate with other patch deployment solutions, you need to create a configuration file, a script file and an applicability check script file:

- **Configuration file**—The configuration file is actually a representative of the tool and a visual integration between Software Vulnerability Manager and that tool. The file is an xml file that should contain the tool name, script name and the input/setting fields required to configure the settings for the tool (text fields, radio buttons and check boxes are supported). When Software Vulnerability Manager is launched it checks for the presence of any configuration file and, if there is a valid configuration file in the Extensions folder in the Software Vulnerability Manager path, it dynamically loads a GUI under the — menu of Software Vulnerability Manager. The configuration file also acts as an input file for the script.
- **Script file**—This script file corresponds to the SDK that the user has created to create and dispatch the package in the respective tool. The script file can be an executable, Java, VB, Python, or Perl script. Click **Publish** to execute the script file.
- **Applicability Check script file**—This script file runs the sps.exe on the computer if the applicability checks are cleared. This file is published together with the package to establish if the package is applicable to the system or not.



Important • Running the script is a very strong feature. Use caution and ensure the sanity of the script file before publishing.

Create and Publish the Package



Task

To create and publish the package:

1. Place the configuration and script files in the Extensions folder. The Extensions folder should be created in the same folder as the csi.exe.
2. Launch Software Vulnerability Manager. If the configuration file format is valid, a configuration option will be visible under the **Patching** menu (for example, **Altiris Configuration**).
3. Click the configuration option to open a page where input and settings can be provided and saved.
4. Go to the SPS creation wizard. Complete all the package wizard fields or import a package. In [Step 4 of 4: Applicability Criteria - Rules](#), there will be radio buttons allowing you to select the tool that you want to publish the package with. There will be as many selection options as there are valid configuration files.
5. Clicking **Publish** for any tool other than WSUS will run the script placed in the Extensions folder and named in the xml file.
6. Software Vulnerability Manager waits for the script to finish and, depending upon the execution of the script being successful or not, displays a message.
7. After successful publishing, the package can be seen in the respective tool.

Patch Template

The Software Vulnerability Manager Patching tab includes a Patch Template feature so that users can save a template of their patches for a product. With the Patch Template feature, the user can prepopulate Flexera's Software Package System (SPS) four-step deployment process and publish directly to WSUS using previously selected options.

Menu	Patch Template							Export
Dashboard								
Scanning								
Results								
Reporting								
Patching								
Flexera Package System (SPS)								
Patch Template								
Template Name	Product Name	Vendor	Patched Version	Minimum Version	Architecture	Updated On		
7-zip x64	7-zip 9.x	Unknown Vendor	16.x	9.0.0.0	Windows64-bit	28th Mar, 2018...		
7-zip x86	7-zip 9.x	Unknown Vendor	16.x	9.0.0.0	Windows32-bit	28th Mar, 2018...		
Adobe Acrobat DC	Adobe Acrobat...	Adobe Systems	2015.006.30413...	15.0.0.0	Windows32-bit / ...	28th Mar, 2018...		
Adobe Acrobat Reader DC (18x continuous)	Adobe Acrobat...	Adobe Systems	2017.012.20098...	4.0.0.0	Windows32-bit / ...	28th Mar, 2018...		
Adobe Flash Player Active X	Adobe Flash Pla...	Adobe Systems	26.x (ActiveX)	9.0.0.0	Windows32-bit / ...	28th Mar, 2018...		
Adobe Flash Player NPAPI	Adobe Flash Pla...	Adobe Systems	29.0.0.140 (NPA...	14.0.0.0	Windows32-bit / ...	28th Mar, 2018...		
Adobe Reader 64bit	Adobe Reader XI	Adobe Systems	2017.012.20098...	10.0.0.0	Windows32-bit / ...	6th Dec, 2017 0...		
Adobe Shockwave Player	Adobe Shockwa...	Adobe Systems	12.3.1.201	12.0.0.0	Windows32-bit / ...	28th Mar, 2018...		
Apple iTunes x86	Apple iTunes	Apple	12.7.3	12.2.0.0	Windows32-bit	28th Mar, 2018...		



To create a Patch Template:

- From the **Patching > Flexera Patching System (SPS)** tab, select an insecure product from the grid. Right click and choose an option from the context menu. For example, select **Create Update Package**.
- In Step 1 of 4 of the SPS wizard (**Package Configuration**), select the appropriate SPS Installer Parameters and choose whether you want to edit the package contents. Click **Next** when done.

Step 1 of 4: Package Configuration

Use this form to set the name and description of the SPS package, or edit the properties of an existing one. In the following steps you will configure the package contents and parameters before creating and publishing the package, or exporting it as an XML formatted file.

Reference Id (Optional)
Here you can assign an Id to this package if desired.
Reference Id:

SPS Installer Parameters (Optional)
Here you can configure optional parameters you want to pass to the installer. This set of options is unique to this product. Some parameters have warning message associated that should be read and understood before moving forward

Configure Package: ☒ Default (?)

Behavior:

☐ Disable checking for running Chrome processes (?)

☐ Kill any running Chrome processes (?)

Select Installer: ☒ Install Enterprise version

☐ Install Stable version

Edit Package Content (Optional)
If you choose to edit the package contents, in the next Step of the wizard you will have the option to view/edit the package contents. If not, you will be directed immediately to Step 3.

☐ Edit Package Content

Vendor & Product Naming
Choose this option to overcome limitations in the number of categories that can be published in the SCCM. This will set the vendor attribute of the package to Flexera and strip the product version from the product name.

☐ Use Flexera Custom Naming

Previous Next Publish Cancel

- Step 2 of 4 of the SPS wizard (**Package Contents**) lists the latest files to include in the package. Click **Next**.

Step 2 of 4: Package Contents

Here you configure the package contents, including the execution script included, and the files included.

Files To Include

Configure the files to include in this package. The grid below shows the files that are currently scheduled to be included, and if they will be downloaded dynamically (i.e., in the case of URLs) or if they are local files. You can add additional files via the 'Add File' button, as well as choose from additional language packages available via the 'Show Localised Files' button. To remove a files, right-click and select 'Remove'.

File(s) to include in the package	Status
http://dl.securia.com/SPS/GoogleChrome_66.0.3359.139_64-bit_SPS.exe	To Be Dynamically Downloaded

Add Local File Add Download Link Add Localisation (Language) File

- In Step 3 of 4 of the SPS wizard (**Applicability Criteria - Paths**), select the appropriate paths to save the package. Click **Next**.



Note • The Patch Template will always shows paths based on the latest assessment.

Step 3 of 4: Applicability Criteria - Paths

Here you can define the path-based applicability rules for this package. Below you will find any relevant paths already found or configured for the package. You can deselect paths in the grid or add paths as needed via the "Add Path" button. Check the "Advanced Options" box to enable additional options in the "Add Path" dialog and to show advanced options in the grid.

☐ Show Advanced Options

Add Path

Always Install Option
The purpose of this option is to allow installations of new software. For custom packages which are not updates to existing installations, you can bypass the "isInstallable" WSUS rule which will ignore all system paths when deciding if this package can be applied. Note - this will not bypass the rules for checking if something is already installed, or is superseded by a more recent version.
☐ Mark Package as "Always Installable"

Minimum Version Option
The purpose of this option is to allow for updating of older products. Normally one updates a product to its secure version within the same major version. You can alter this behaviour by specifying a custom minimum version. Note: the version you enter must also be supported by the installer itself - you cannot enter arbitrary values here.
Minimum Version:

Path	Information
<input checked="" type="checkbox"/> C:\Program Files (x86)\Google\Chrome\Application\chrome.exe	1

Previous | Next | Publish | Cancel

- In Step 4 of 4 of the SPS wizard (**Applicability Criteria - Rules**), select the appropriate **System Applicability**, **Special Rules**, and **Language Settings**.

Step 4 of 4: Applicability Criteria - Rules

Here you configure the applicability rules for the package.

System Applicability
Configure the system type(s) the package will be applied to.
Apply Package To: ☐ 32-bit Systems Only
☒ 64-bit Systems Only
☐ Both 32-bit and 64-bit Systems

Special Rule
The following special rule is available to configure:
☐ Reboot is required after package has been installed.

Language Settings
Configure package applicability rules based on language:
☐ Only make package applicable to computers with one of the selected languages.
Select Languages:

Language
Arabic
Chinese (Hong Kong SAR)
Chinese - (Simplified)
Chinese - (Traditional)
Czech
French

- In the **Patch Template (Optional)** field, enter the Template Name and select **Save Template**. Click **Publish** to create the new template, which is saved under the **Patch Template** tab.

Step 4 of 4: Applicability Criteria - Rules

Here you configure the applicability rules for the package.

☐ Do not include package file(s) as binary in XML file.

Patch Template (Optional)
Save as template
Template Name:

Publish Options
Select option for publishing Flexera package
Publish package using: ☐ WSUS
☐ Altiris
☐ Export Patch Script
☐ Cabinet File (Export)
☒ Save Template

Previous | Next | Publish | Cancel



Note • Providing a template name while publishing a package to WSUS will publish and create a template at the same time. If the template name is empty, it will only publish the package as a regular workflow.

A patch template only needs to be created once for the life of the product, provided that there are no changes to the product's architecture (32-bit versus 64-bit) or to the SPS Installer Parameters from **Step 1 of 4: Package Configuration**. Over time, the product's Patched Version listed under the Flexera Package System (SPS) menu will increase. Patch Templates automatically update up to within three patched versions as listed under the Flexera Package System (SPS) menu. After three patched versions, you can edit the Patch Template to deploy the latest patched version to your system.

Menu	Patch Template	Export
Dashboard	Template Name ▲	
Scanning	7-zip x64	7-zip 9.x Unknown Vendor 16.x 9.0.0.0 Windows64-bit 28th Mar, 2018...
Results	7-zip x86	7-zip 9.x Unknown Vendor 16.x 9.0.0.0 Windows32-bit 28th Mar, 2018...
Reporting	Adobe Acrobat DC	Adobe Acrobat... Adobe Systems 2015.006.30413... 15.0.0.0 Windows32-bit / ... 28th Mar, 2018...
Patching	Adobe Acrobat Reader DC (18x continuous)	Adobe Acrobat... Adobe Systems 2017.012.20098... 4.0.0.0 Windows32-bit / ... 28th Mar, 2018...
Flexera Package System (SPS)	Adobe Flash Player Active X	Adobe Flash Pla... Adobe Systems 26.x (ActiveX) 9.0.0.0 Windows32-bit / ... 28th Mar, 2018...
Patch Template	Adobe Flash Player NPAPI	Adobe Flash Pla... Adobe Systems 29.0.0.140 (NPA... 14.0.0.0 Windows32-bit / ... 28th Mar, 2018...
	Adobe Reader 64bit	Adobe Reader XI Adobe Systems 2017.012.20098... 10.0.0.0 Windows32-bit / ... 6th Dec, 2017 0...
	Adobe Shockware Player	Adobe Shockwa... Adobe Systems 12.3.1.201 12.0.0.0 Windows32-bit / ... 28th Mar, 2018...
	Apple iTunes x86	Apple iTunes Apple 12.7.3 12.2.0.0 Windows32-bit 28th Mar, 2018...



To edit a Patch Template or to publish from a Patch Template:

- From the **Patching > Patch Template** tab, select a template and select **Publish/Edit Template** from the context menu.

Menu	Patch Template	Export
Dashboard	Template Name ▲	
Scanning	7-zip x64	7-zip 9.x Unknown Vendor 16.x 9.0.0.0 Windows64-bit 28th Mar, 2018...
Results	7-zip x86	7-zip 9.x Unknown Vendor 16.x 9.0.0.0 Windows32-bit 28th Mar, 2018...
Reporting	Adobe Acrobat DC	Adobe Acrobat... Adobe Systems 2015.006.30413... 15.0.0.0 Windows32-bit / ... 28th Mar, 2018...
Patching	Adobe Acrobat Reader DC	Adobe Acrobat... Adobe Systems 2017.012.20098... 4.0.0.0 Windows32-bit / ... 28th Mar, 2018...
Flexera Package System (SPS)	Adobe Flash Player Active X	Adobe Flash Pla... Adobe Systems 26.x (ActiveX) 9.0.0.0 Windows32-bit / ... 28th Mar, 2018...
Patch Template	Adobe Flash Player NPAPI	Adobe Flash Pla... Adobe Systems 29.0.0.140 (NPA... 14.0.0.0 Windows32-bit / ... 28th Mar, 2018...
	Adobe Reader 64bit	Adobe Reader XI Adobe Systems 2017.012.20098... 10.0.0.0 Windows32-bit / ... 6th Dec, 2017 0...
	Adobe Shockware Player	Adobe Shockwa... Adobe Systems 12.3.1.201 12.0.0.0 Windows32-bit / ... 28th Mar, 2018...
	Apple iTunes x86	Apple iTunes Apple 12.7.3 12.2.0.0 Windows32-bit 28th Mar, 2018...

- Step 1 of 4 of the Flexera SPS wizard will open with the SPS parameters prefilled. From the same SPS wizard, you can either publish the package to various channels or you can save only the template.
- To update the Patch Template to the latest patched version:
 - Select **Edit Package Content** in the Edit Package Content field and click **Next**.

Step 1 of 4: Package Configuration

Use this form to set the name and description of the SPS package, or edit the properties of an existing one. In the following steps you will configure the package contents and parameters before creating and publishing the package, or exporting it as an XML formatted file.

SPS Installer Parameters (Optional)

Here you can configure optional parameters you want to pass to the installer. This set of options is unique to this product. Some parameters have warning message associated that should be read and understood before moving forward

Configure Package (Default) (?)

Behavior:

☐ Disable checking for running Chrome processes (?)

☐ Kill any running Chrome processes (?)

Select Installer:

☒ Install Enterprise version

☐ Install Stable version

Edit Package Content (Optional)

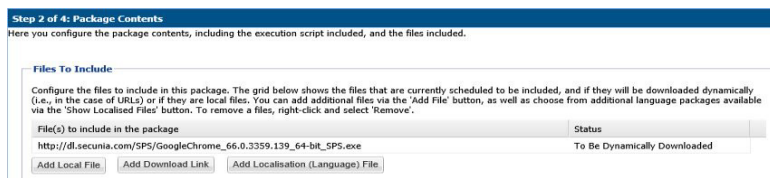
If you choose to edit the package contents, in the next Step of the wizard you will have the option to view/edit the package contents. If not, you will be directed immediately to Step 3.

☒ Edit Package Content



Important • If you need to publish the package from the template without updating the template, update the **Package Name** in Step 1 of 4 of the SPS wizard to identify the package version that you deploy to your system. The package will be published with the updated settings.

- Confirm the updated patched version file appears under **Files to Include** in Step 2 of 4 of the Flexera SPS wizard and click **Next**.



- When Step 3 of 4 of the Flexera SPS wizard appears, click **Next**.
- When Step 4 of 4 of the Flexera SPS wizard appears, click **Publish**.



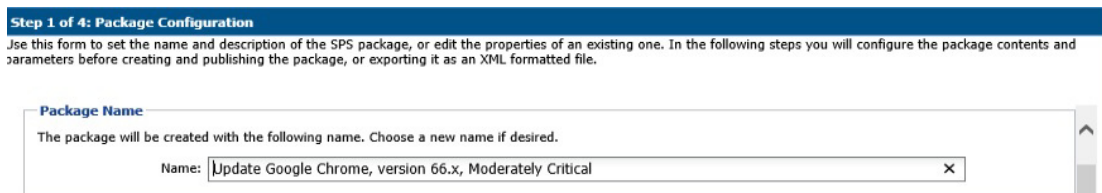
To delete a Patch Template:

1. From the **Patching > Patch Template** tab, select a template and select **Delete Template** from the context menu.
2. Select **Yes** or **No** to confirm whether or not to delete the Patch Template.

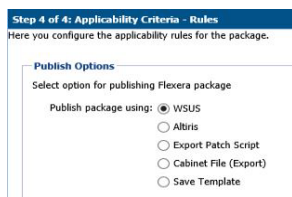


To publish a Patch Template to WSUS:

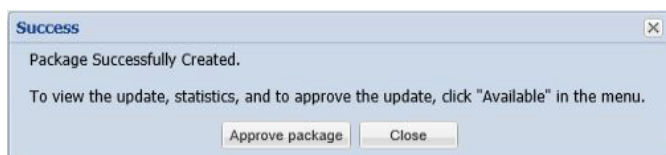
1. From the **Patching > Patch Template** tab, select the template to be published to WSUS. Right click and select **Publish/Edit Template** from the context menu.
2. When Step 1 of 4 of the SPS wizard (**Package Configuration**) appears, update the **Package Name** to indicate this package is for WSUS publishing and click **Next**.



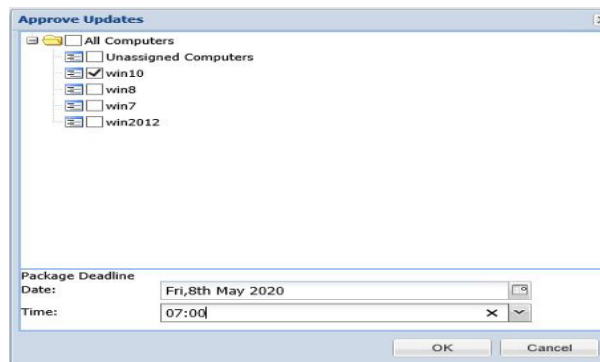
3. When Step 3 of 4 of the SPS wizard (**Applicability Criteria - Paths**) appears, click **Next**.
4. In Step 4 of 4 of the SPS wizard (**Applicability Criteria - Rules**), select **WSUS** for the publishing option and click **Publish**.



5. The **Attempting to Publish Package - Please Wait** status appears. After the WSUS package is successfully created, a **Success** pop-up window appears. Click **Approve package**.



6. When the **Approve Updates** pop-up window appears, select the appropriate computers to deploy the WSUS package to, select the appropriate date and time to deploy the WSUS package, and click **OK**.



7. When the **Success - Package successfully approved** pop-up window appears, click **OK**.



8. You can confirm the WSUS package listing under **Patching > WSUS / System Center > Available Packages**.

Patch Automation

With Software Vulnerability Manager, you can automate publishing of patches. To do so, right click on any SPS template or VPM patch and select **Subscribe to Patch** from the context menu.

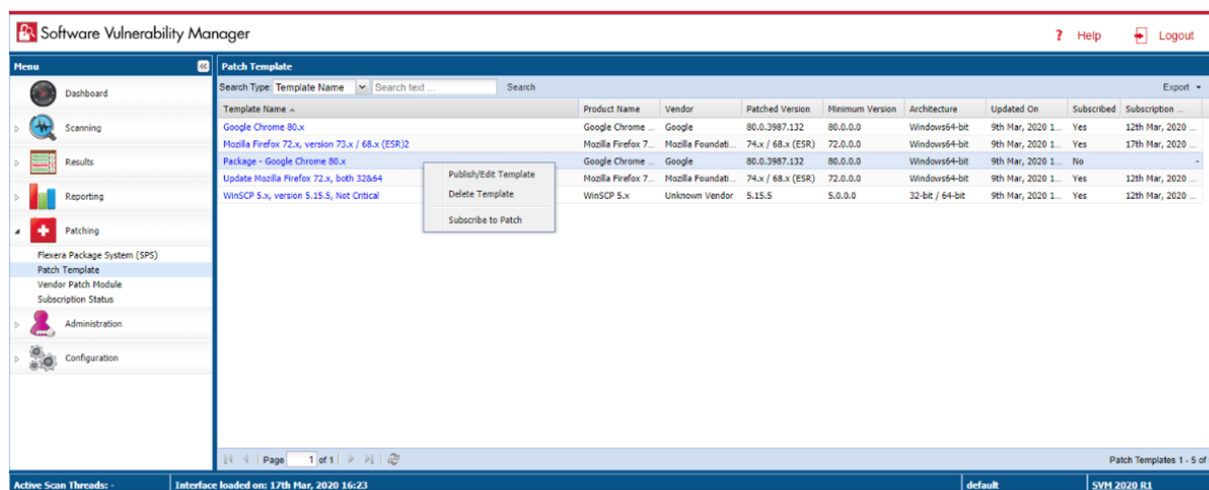


Figure 9-4: Selecting Subscribe to Patch from the Context Menu

On the **Configure Subscription** dialog box, you can choose to always publish a new patch when a new version becomes available, or you can choose to only automate publishing a new patch when certain criteria are met (recommended).

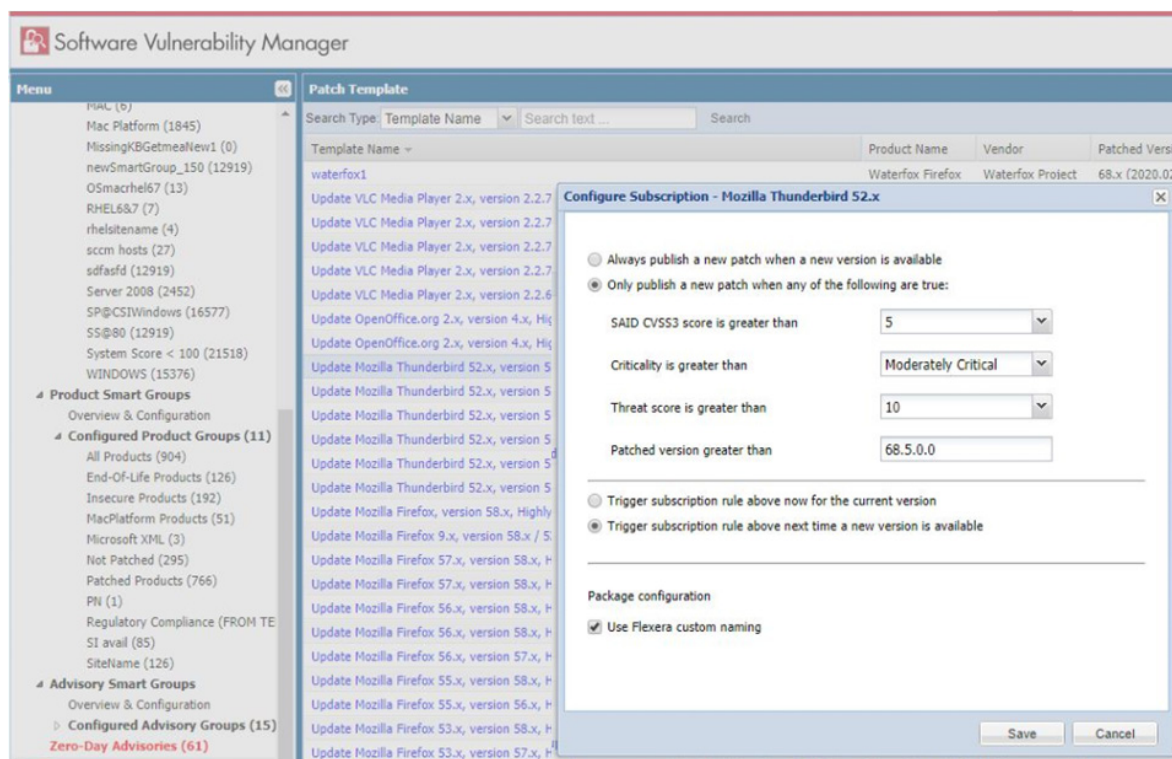


Figure 9-5: Configure Subscription Dialog Box

Patch automation is delivered via a new version of the Flexera SVM Patch Configuration (Version 2.x) tool, which is part of the Software Vulnerability Manager Client Toolkit. For more information on the toolkit, visit the [SVM Toolkit](#) blog in the Flexera Community.

The SVM Toolkit installer contains updates to the Flexera SVM Patch Configuration tool as well as some optional tools documented in our online community. The SVM Toolkit installer can be downloaded at:

<https://resources.flexera.com/tools/SVM/SVMClientToolkitInstall.msi>



Note • If you are already have the SVM Toolkit installed, the installer will upgrade you to the latest version.

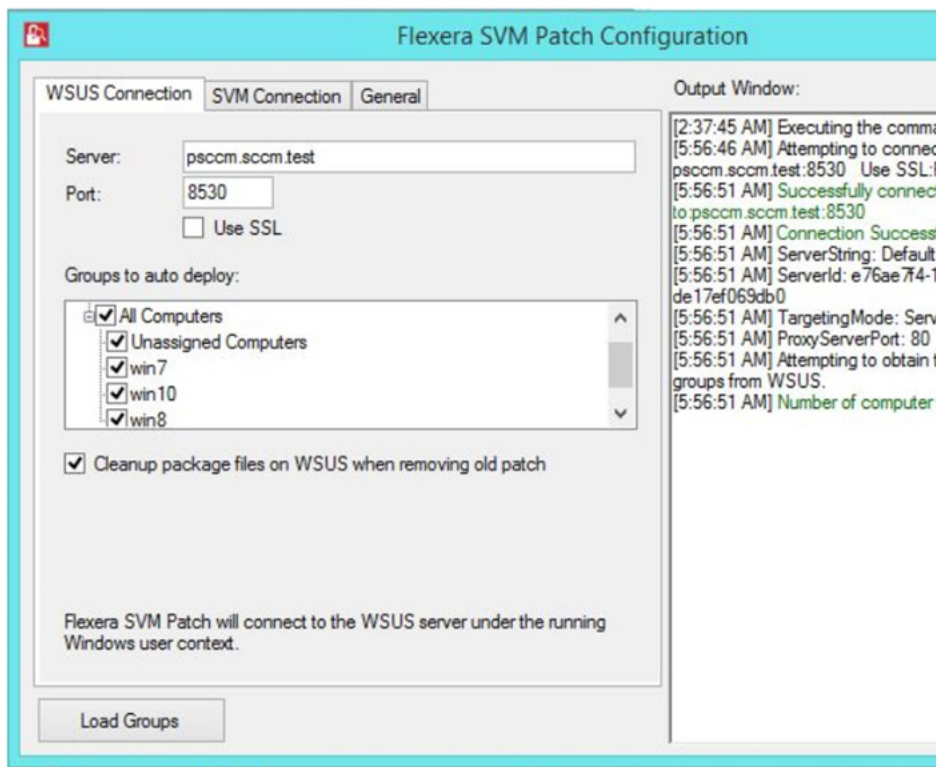


Figure 9-6: Flexera SVM Patch Configuration Dialog Box

You can see the status and details of patches published automatically on a new page named **Subscription Status**, which is opened by selecting **Subscription Status** on the **Patching** menu.

Software Vulnerability Manager									
Subscription Status									
Search Type: Package Search text: Search									
Package Name	Vendor	Type	Version	Published to	Deployed to	Status	Send to Daemon	Last status update	
Update Firefox (English US) (x86), version 74.0	Mozilla	VPM	74.0	pccm.sccm.test	Unassigned Computers,win7,w...	Success	11th Mar, 2020	11th Mar, 2020	09:25
Update Firefox (English US) (x64), version 74.0	Mozilla	VPM	74.0	pccm.sccm.test	Unassigned Computers,win7,w...	Success	11th Mar, 2020	11th Mar, 2020	09:23
Update Mozilla Firefox, version 73.x / 68.x (ESR)	Mozilla Foundation	SPS	73.x / 68.x (ESR)	pccm.sccm.test	Unassigned Computers,win7,w...	Success	11th Mar, 2020	11th Mar, 2020	02:40
Update IPassword, version 7.4.750	AgileBits	VPM	7.4.750	pccm.sccm.test	Unassigned Computers,win7,w...	Success	11th Mar, 2020	11th Mar, 2020	02:37
Update Mozilla SeaMonkey, version 2.53.1	Mozilla Foundation	SPS	2.53.1	pccm.sccm.test	Unassigned Computers,win7,w...	Success	10th Mar, 2020	10th Mar, 2020	08:35
Update Google Chrome, version 80.x	Google	SPS	80.x	pccm.sccm.test	Unassigned Computers,win7,w...	Success	10th Mar, 2020	10th Mar, 2020	07:57
Update VLC Media Player, version 3.0.8	VideoLAN	SPS	3.0.8	pccm.sccm.test	Unassigned Computers,win7,w...	Success	10th Mar, 2020	10th Mar, 2020	07:44
Update VLC Media Player, version 3.0.8	VideoLAN	SPS	3.0.8	pccm.sccm.test	Unassigned Computers,win7,w...	Success	10th Mar, 2020	10th Mar, 2020	06:35
Update VLC Media Player, version 3.0.8	VideoLAN	SPS	3.0.8	pccm.sccm.test	win10,win8	Success	9th Mar, 2020	9th Mar, 2020	02:01
Update VLC Media Player, version 3.0.8	VideoLAN	SPS	3.0.8	pccm.sccm.test	win10,win8	Success	9th Mar, 2020	9th Mar, 2020	01:38
Update VLC Media Player, version 3.0.8	VideoLAN	SPS	3.0.8	win-67ahvgc6b		Success	6th Mar, 2020	6th Mar, 2020	20:59
Update VLC Media Player, version 3.0.8	VideoLAN	SPS	3.0.8	win-67ahvgc6b		Success	6th Mar, 2020	6th Mar, 2020	20:31
Update FileZilla 3.x, version 3.43.0	Unknown Vendor	SPS	3.43.0	win-67ahvgc6b		Success	6th Mar, 2020	6th Mar, 2020	20:28
Update VLC Media Player, version 3.0.8	VideoLAN	SPS	3.0.8	win-67ahvgc6b		Success	6th Mar, 2020	6th Mar, 2020	20:26
Update VLC Media Player, version 3.0.8	VideoLAN	SPS	3.0.8	win-67ahvgc6b		Success	6th Mar, 2020	6th Mar, 2020	11:09
Update VLC Media Player, version 3.0.8	VideoLAN	SPS	3.0.8	win-67ahvgc6b		Success	6th Mar, 2020	6th Mar, 2020	10:54
Update VLC Media Player, version 3.0.8	VideoLAN	SPS	3.0.8	win-67ahvgc6b		Success	6th Mar, 2020	6th Mar, 2020	10:26
Update VLC Media Player, version 3.0.8	VideoLAN	SPS	3.0.8	win-67ahvgc6b		Success	6th Mar, 2020	6th Mar, 2020	10:19
Update VLC Media Player, version 3.0.8	VideoLAN	SPS	3.0.8	win-67ahvgc6b		Success	6th Mar, 2020	6th Mar, 2020	10:14
Update VLC Media Player, version 3.0.8	VideoLAN	SPS	3.0.8	pccm.sccm.test	win10,win8	Success	6th Mar, 2020	6th Mar, 2020	09:53
Update VLC Media Player 2.x, version 3.0.8	VideoLAN	SPS	3.0.8	pccm.sccm.test	win10,win8	Success	6th Mar, 2020	6th Mar, 2020	02:58
Update eHule 0.x, version 0.47.2.66	eHule	SPS	0.47.2.66	pccm.sccm.test	win10,win8	Success	6th Mar, 2020	6th Mar, 2020	00:32
Update VLC Media Player 2.x, version 3.0.8	VideoLAN	SPS	3.0.8	pccm.sccm.test	win10,win8	Success	6th Mar, 2020	6th Mar, 2020	00:32
Update Notepad++ 7.x, version 7.7	Unknown Vendor	SPS	7.7	pccm.sccm.test	win10,win8	Success	6th Mar, 2020	6th Mar, 2020	00:31
Update Zotero, version 5.0.84	Zotero	VPM	5.0.84	win-67ahvgc6b		Success	1st Mar, 2020	1st Mar, 2020	09:58
Update Wireshark (x86), version 3.2.2.0	Wireshark Foundation	VPM	3.2.2.0	win-67ahvgc6b		Success	1st Mar, 2020	1st Mar, 2020	09:57
Update Zotero, version 5.0.83	Zotero	VPM	5.0.83	win-67ahvgc6b		Success	27th Feb, 2020	27th Feb, 2020	06:51
Update Firefox (English US) (x86), version 73.0.1	Mozilla	VPM	73.0.1	win-67ahvgc6b		Success	21st Feb, 2020	25th Feb, 2020	10:27
Update .NET Core Runtime 3.1 (x64), version 3.1.2.28517	Microsoft	VPM	3.1.2.28517	win-67ahvgc6b		Success	21st Feb, 2020	25th Feb, 2020	10:25
Update Firefox (English US) (x64), version 73.0.1	Mozilla	VPM	73.0.1	win-67ahvgc6b		Success	21st Feb, 2020	25th Feb, 2020	10:24
Update Zoom Player Max, version 14.5	Innatrix	VPM	14.5	win-67ahvgc6b		Success	20th Feb, 2020	20th Feb, 2020	07:32
Update Firefox (English US) (x86), version 73.0	Mozilla	VPM	73.0	win-67ahvgc6b		Success	20th Feb, 2020	20th Feb, 2020	07:31
Update Xpdf Lite, version 3.3.4.0	bioPDF	VPM	3.3.4.0	win-67ahvgc6b		Success	20th Feb, 2020	20th Feb, 2020	07:29
Update Yammer (x86), version 3.4.5.0	Microsoft	VPM	3.4.5.0	win-67ahvgc6b		Success	20th Feb, 2020	20th Feb, 2020	07:29
Update Zotero, version 5.0.82	Zotero	VPM	5.0.82	win-67ahvgc6b		Success	20th Feb, 2020	20th Feb, 2020	07:27
Update .NET Core Runtime 3.1 (x64), version 3.1.1.28408	Microsoft	VPM	3.1.1.28408	win-67ahvgc6b		Success	20th Feb, 2020	20th Feb, 2020	07:26
Update PuTTY (x86), version 0.73.0.0	Simon Tatham	VPM	0.73.0.0	win-67ahvgc6b		Success	20th Feb, 2020	20th Feb, 2020	07:25

Figure 9-7: Subscription Status Page

All the patch level activities are also recorded in the Activity Log, which is opened by selecting **Activity Log** on the **Configuration** menu.

Activity Name	Activity Status	User	Time	Activity Information	Host	Priority
WSUS Package Approval	Successful	default	21:55 11th Mar, 2020	Package name: Update Firefox (English US) (x86), version 74.0 (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
WSUS Package Creation	Successful	default	21:55 11th Mar, 2020	Update Firefox (English US) (x86), version 74.0 (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
WSUS Package Approval	Successful	default	21:53 11th Mar, 2020	Package name: Update Firefox (English US) (x64), version 74.0 (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
WSUS Package Creation	Successful	default	21:53 11th Mar, 2020	Update Firefox (English US) (x64), version 74.0 (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
WSUS Package Approval	Successful	default	15:10 11th Mar, 2020	Package name: Update Mozilla Firefox, version 73.x / 68.x (ESR) (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
WSUS Package Creation	Successful	default	15:10 11th Mar, 2020	Update Mozilla Firefox, version 73.x / 68.x (ESR) (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
WSUS Package Approval	Successful	default	15:07 11th Mar, 2020	Package name: Update IPassword, version 7.4.750 (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
WSUS Package Creation	Successful	default	15:07 11th Mar, 2020	Update IPassword, version 7.4.750 (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
WSUS Package Approval	Successful	default	21:05 10th Mar, 2020	Package name: Update Mozilla SeaMonkey, version 2.53.1 (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
WSUS Package Creation	Successful	default	21:05 10th Mar, 2020	Update Mozilla SeaMonkey, version 2.53.1 (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
WSUS Package Approval	Successful	default	20:27 10th Mar, 2020	Package name: Update Google Chrome, version 80.x (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
WSUS Package Creation	Successful	default	20:27 10th Mar, 2020	Update Google Chrome, version 80.x (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
WSUS Package Approval	Successful	default	20:14 10th Mar, 2020	Package name: Update VLC Media Player, version 3.0.8 (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
WSUS Package Creation	Successful	default	20:14 10th Mar, 2020	Update VLC Media Player, version 3.0.8 (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
WSUS Package Approval	Successful	default	19:05 10th Mar, 2020	Package name: Update VLC Media Player, version 3.0.8 (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
WSUS Package Creation	Successful	default	19:05 10th Mar, 2020	Update VLC Media Player, version 3.0.8 (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
User Login	Successful	default	18:51 10th Mar, 2020	Login (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
User Login	Successful	default	18:50 10th Mar, 2020	Login (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
User Login	Successful	default	18:46 10th Mar, 2020	Login (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
User Login	Successful	default	18:45 10th Mar, 2020	Login (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
WSUS Package Approval	Successful	default	14:31 9th Mar, 2020	Package name: Update VLC Media Player, version 3.0.8 (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
WSUS Package Creation	Successful	default	14:31 9th Mar, 2020	Update VLC Media Player, version 3.0.8 (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
User Login	Successful	default	14:26 9th Mar, 2020	Login (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
WSUS Package Approval	Successful	default	14:08 9th Mar, 2020	Package name: Update VLC Media Player, version 3.0.8 (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
WSUS Package Creation	Successful	default	14:08 9th Mar, 2020	Update VLC Media Player, version 3.0.8 (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
User Login	Successful	default	13:53 9th Mar, 2020	Login (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
User Login	Successful	default	13:53 9th Mar, 2020	Login (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
User Login	Successful	default	13:51 9th Mar, 2020	Login (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
User Login	Successful	default	13:48 9th Mar, 2020	Login (Software Vulnerability Manager Client Toolkit)	10.20.151.46	Medium
WSUS Package Approval	Successful	default	10:29 7th Mar, 2020	Package name: Update VLC Media Player, version 3.0.8 (Software Vulnerability Manager Client Toolkit)	10.20.6.52	Medium
WSUS Package Creation	Successful	default	10:29 7th Mar, 2020	Update VLC Media Player, version 3.0.8 (Software Vulnerability Manager Client Toolkit)	10.20.6.52	Medium
User Login	Successful	default	10:27 7th Mar, 2020	Login (Software Vulnerability Manager Client Toolkit)	10.20.6.52	Medium
WSUS Package Approval	Successful	default	10:01 7th Mar, 2020	Package name: Update VLC Media Player, version 3.0.8 (Software Vulnerability Manager Client Toolkit)	10.20.6.52	Medium
WSUS Package Creation	Successful	default	10:01 7th Mar, 2020	Update VLC Media Player, version 3.0.8 (Software Vulnerability Manager Client Toolkit)	10.20.6.52	Medium
WSUS Package Creation	Successful	default	09:58 7th Mar, 2020	Update FileZilla 3.x, version 3.43.0 (Software Vulnerability Manager Client Toolkit)	10.20.6.52	Medium

Figure 9-8: Activity Log Page



Note • In an upcoming release, Software Vulnerability Manager will be introducing an option to get a daily/weekly activity digest via email.

10

Administration

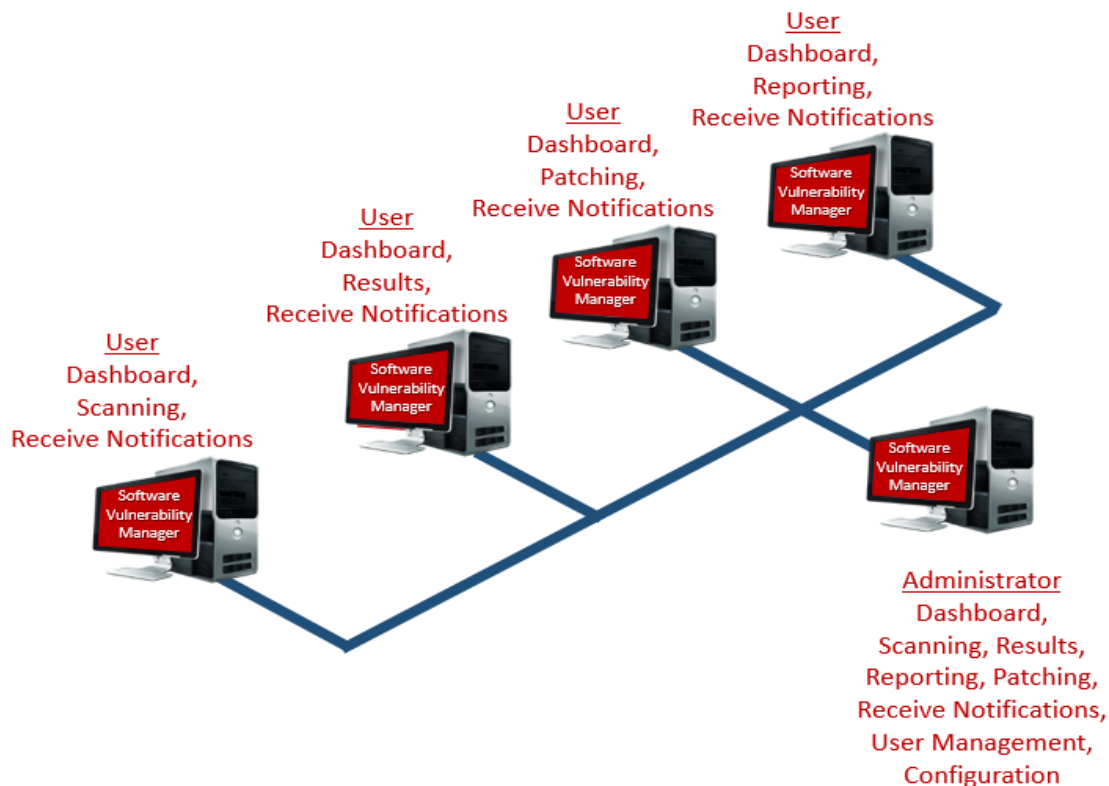
This chapter discusses the following Software Vulnerability Manager administrative features:

- [Roles](#)
- [User Management](#)
- [Active Directory \(Requires the Software Vulnerability Manager Plug-in\)](#)
- [IP Access Management \(Requires the Software Vulnerability Manager Plug-in\)](#)
- [Password Policy Configuration](#)

Roles

Software Vulnerability Manager uses role-based account management. Each Software Vulnerability Manager user is created and assigned a set of roles and limitations as appropriate. These roles determine which parts of Software Vulnerability Manager the user has access to and limits what the user can view and scan.

Every user of Software Vulnerability Manager can receive notifications such as reports, email and SMS.



The roles are as follows:

- **Scanning**—Allows the user to scan hosts and view the Scanning menu of Software Vulnerability Manager.
 - **Filter Scan Results**—Allows the user to access and configure Whitelist and Blacklist filtering and Custom Scan Results.
- **Patching**—Allows the user to access the Patching module.
- **Results**—Allows the user to view scan results via, for example, **Smart Groups**.
- **Reporting**—Allows the user to access various reporting options and the **Database Console** and **Database Cleanup** menus.
 - **Database Access**—Allows the user to access the Database Console and schedule exports. There are no options to restrict the user's network access if this option is selected.
- **Read Only**—Prohibits the user from making any changes that write data to the Flexera Cloud. Read Only users do not have Scanning or Patching capabilities.
- **Restricted**—Users are read only users with limited functionality. A Restricted user is unable to view the default set of Smart Groups and are restricted to:
 - Viewing only the Custom Smart Groups that have been created for them,
 - Viewing the Reports that have been created for them.
 - Changing their password.

Only the Root Administrator can access the Active Directory and Password Policy Configuration. Administrative users have additional capabilities that allow:

- Configuring Software Vulnerability Manager
- Creating users and assigning their roles and restrictions
- Assigning License limits

None of the access limitations apply to an administrative user and they can view all Hosts and Results.

User Management

Use this page to administer your Software Vulnerability Manager users.

- [Create a New Administrator](#)
- [Create a New User](#)

Create a New Administrator

Click **Create New Administrator** and fill in the form, providing all the necessary details about the administrative user and include the limits to assign to the user.

An email will be sent to the user containing a welcome message and their Software Vulnerability Manager login credentials.

Right-click an existing account to view, edit or delete the account.

Create a New User

Click **Create New User** and fill in the form, providing all the necessary details about the user. Select the **Roles & Sub-Roles** check boxes to assign the roles to the user.

Create New User

Account Details

Name:

Username:

Email:

☐ Use LDAP for authentication

☒ Generate a new one-time password and email it to the address specified above

Host License Limit: ☒ No Limit (99991 Host Licenses Available)

Recipient Details

Enter an email address to be used for emails, notifications and alerts the Flexera Software Vulnerability Manager can be configured to send.

Email:

User Roles & Permissions

Configure the specific roles and permissions for this user. Note that Read-Only and Restricted users have restrictions on what roles they may be granted, and even within certain roles, there are actions and views they will not have access to. Restricted users are limited to logging in, changing their password and only viewing their Smart Groups and Reports.

Write Permissions: ☒ Read / Write ☐ Read Only ☐ Restricted

Roles & Sub-Roles

☐ Scanning ☐ Reporting

☐ Filter Scan ☐ Database Access

Results

☐ Patching

☐ Results

Restrict User's Network Access

You can limit this user's access and view of the network by restricting their scope using the following filters:

☒ Restrict To This Account

☒ Restrict To Individual Hosts

☒ Restrict On IP Range



Important • To create a user using LDAP authentication, the Software Vulnerability Manager2018 Username must be the same as the LDAP Username.

A confirmation email with activation instructions will be sent to the email address provided.

Select the check boxes under **Restrict User's Network Access** to specify which network endpoints you would like to allow the user to have access to. You can use existing configured Hostname or IP Based Restrictions. Please note that Hostnames must be entered with the langroup(domain) in the format hostname.langroup. Using only the Hostname will not work as you could have the same Hostname in different domains which will allow users to see hosts they might not be permitted to see.



Note • **Restrict User's Network Access** options are not available when a **Database Access** Role is granted.

Active Directory (Requires the Software Vulnerability Manager Plug-in)

As a Root Administrator, you can select **Enable Active Directory integration** to allow your group policies to be automatically updated in Software Vulnerability Manager when changes are made to the Active Directory.



Important • Switching to Active Directory will hide your current Sites structure and the **Results > Sites** menu. For these to be displayed you must disable the Active Directory integration, logout, and then login to Software Vulnerability Manager. It is **NOT** recommended to toggle Active Directory on and off unnecessarily.

Requirements to integrate Software Vulnerability Manager with the Active Directory Domain:

- Active Directory Domain environment
- Domain User privileges
- Port 3268 (msft-gc protocol) open between Domain Controller and Software Vulnerability Manager Host

Enabling Active Directory imports all discovered computer objects in the Active Directory Schema. Disabling Active Directory does not delete the computer objects in Software Vulnerability Manager. Deleting sensitive computer information in Software Vulnerability Manager must be done manually by the user.

Use the options below to control which Active Directory paths will be scanned. The Active Directory scanner will attempt to fetch the widest structure possible starting from the provided root location. The scanner only analyses Domain Controllers and Organizational Units.

- **All accessible branches**—By looking at the Active Directory Partitions, the scanner determines the accessible Domain Controllers that can be scanned.
- **Specific Domain Controller**—You can specify a certain Domain Controller to be scanned. It must be accessible from the host running Software Vulnerability Manager. Select **Set nETBIOSName manually** to enter the nETBIOSName of the Domain Controller.

The view options help you control how the elements of the Active Directory are displayed. You can select the **Show Distinguished Names for sites instead of single Organizational Units** check box to display multiple Organizational Units with the same name. Note that this does not affect the Site name for server-side exports or generated reports.

You can use the schedule options to set Active Directory scans at regular intervals or perform a manual scan.

IP Access Management (Requires the Software Vulnerability Manager Plug-in)

As a Root Administrator, you can use this page to configure the IP addresses the Software Vulnerability Manager console can be accessed from.



Important • The first IP Access Rule you set up must always be a whitelist rule and must include the external (public) IP address of the console you are creating the rule from. If, for example, you check `ipconfig` you will find the internal IP address, which will not work. You can find your external IP address by using an Internet search engine and typing “find my ip address”.



Task

To create a new rule:

1. Click **New IP Rule**. Enter a name for the rule, the IP address or IP range, select to add the rule to a whitelist or blacklist, and the users to apply the rule to. The rule can contain a Single IP or an IP range, but you need to start with a whitelist rule. If you whitelist one IP address (the one you are using), then all other IP addresses are black-listed by default.

New IP Access Rule

Name:

Type: ☒ Single IP ☐ IP range

IP:

Added to: ☒ Whitelist ☐ Blacklist ?

Users: ☒ All ☐ Custom

2. Once you have created a whitelist rule with an IP range, you can then blacklist a Single IP or an IP range within the whitelist IP range.
3. You can also create an IP Access Rule for your personal IP address. For quick reference, your IP address will appear in the top row of the IP Access Management window so that it can be entered in the IP field.

IP Access Management

New IP Rule | Check IP | Your IP:

IP Access Rule

New IP Access Rule

Name: IP_Whitelisting

Type: ☒ Single IP ☐ IP range

IP:

Added to: ☒ Whitelist ☐ Blacklist ?

Users: ☒ All ☐ Custom

4. All IPs that have been added to a whitelist are able to use Software Vulnerability Manager and IPs added to a blacklist are not able to connect.
5. To test if an IP has access to Software Vulnerability Manager based on the current rules, click **Check IP**.

Password Policy Configuration

Use this page to configure the password policy for users. This policy should be set on a “global” level, that is, the password policy cannot be configured differently for different users. The Administrator defines the policy based on the options displayed in the Policy Rules dialog.

Policy Rules

Configure the Software Vulnerability Manager password policy for your users.

- ☒ Password must be at least characters long.
- ☒ Users must be prevented from reusing the password for at least changes.
- ☒ Password must contain at least digits.
- ☒ Password must contain at least one lower case and one upper case alphabetic character.
- ☒ Password must be changed at least every days.

Save

11

Configuration

This chapter describes the following features that can be configured in Software Vulnerability Manager:

- [Settings](#)
- [Log Messages](#)
- [Activity Log](#)
- [Suggest Software](#)
- [Security](#)

Settings

Use this page to configure various settings within Software Vulnerability Manager.

- [Scan Threads](#)
- [Live Updates](#)
- [Collect Network Information](#)
- [Zombie File Settings](#)
- [Check for Missing Microsoft Security Update Settings](#)
- [Flexera Software Package System \(SPS\) Timestamp](#)
- [Mask paths that show user names](#)
- [Configure Agent's status polling](#)
- [Default Recipient Settings](#)
- [Windows Update Settings](#)

Scan Threads

Define the number of simultaneous scans to be executed. You can set the Scan threads value from 1 to 99 (the default is 5).

Please note that the number of simultaneous scan threads will not affect the scans being performed by the CSIA (Agent), since these scans are made locally by the agents.

Scan Settings

This setting defines the number of simultaneous scans to be executed. The recommended value is between 5 and 10, depending on the power of the computer and the network capacity available. The value can be set from 1 to 99. (?)

Scan threads:

Live Updates

Select the Activate Live Update check box to update your scan results as new Vulnerability Intelligence pertaining to your existing scan results emerges. By doing this you agree that you understand and accept that this is not a replacement for regular scheduled scanning, and could lead to your shown scan results not being the most accurate representation of the current state of your network. Live Update changes will only modify scan data received after enabling this feature. Older scan results will not be affected by this feature. Please note that Live Update does not update Red Hat Agent scan results.

Live Update

I want my scan results to be updated in real time as new Vulnerability Intelligence pertaining to my existing scan results emerges. I understand and accept that this is not a replacement for regular scheduled scanning, and could lead to my shown scan results not being the most accurate representation of the current state of my network. (?)

☐ Activate Live Update

Collect Network Information

Select the Allow Collection of Network Information check box to allow collection and storage of network hardware information, such as assigned IP and Mac addresses, when scanning devices to be able to restrict users based on IP addresses or IP Networks.



Note • The collected information is not visible to users except from the Database Console. This option is only available to the Root Administrator.

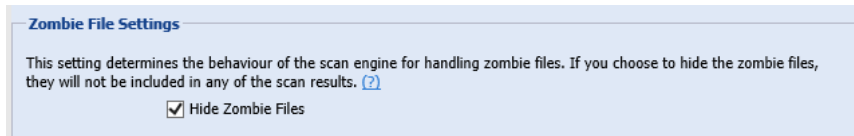
Collect Network Information

I want to allow the collection and storage of network information, such as assigned IPs and MAC addresses, when I scan devices. (?)

☐ Allow Collection of Network Information

Zombie File Settings

Zombie files are files that were left behind after removing or applying a product/patch. Software Vulnerability Manager will pick up these files since these are listed in Software Vulnerability Manager file signature as being related to an Insecure or End-Of-Life product. Select the **Hide Zombie Files** check box to ensure that zombie files will not be included in any of the scan results. With the Hide Zombie Files setting enabled, only the highest version of the discovered product will be displayed in the scan results. To activate the Hide Zombie Files setting, a new scan is needed to change the scan results.

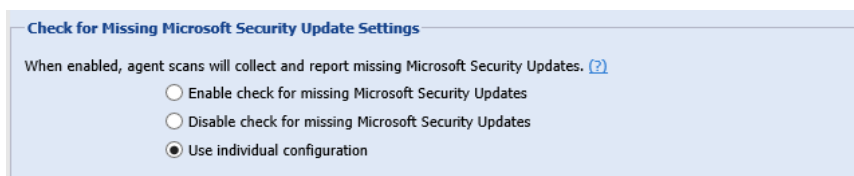


The **Hide Zombie Files** setting is a global setting for a partition that applies to all users of that partition. This option is visible to all users, but only Partition Administrators are able to change it. Refer to [Appendix A - Software Vulnerability Manager Partition Management](#) for more information.

Check for Missing Microsoft Security Update Settings

The **Check for Missing Microsoft Security Update Settings** determines whether or not agents perform the Windows Update check to collect and report missing Microsoft Security Updates:

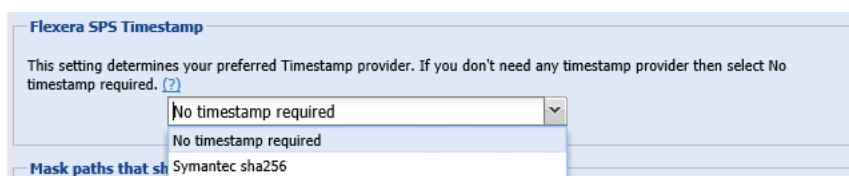
- Enable check for missing Microsoft Security Updates – All agents will check for missing Microsoft updates, using the [Windows Update Settings](#).
- Disable check for missing Microsoft Security Updates – No agents will check for missing Microsoft updates.
- Use individual configuration – Agents will use their site settings or their individual settings for determining whether to check for missing Microsoft updates. If their individual or site setting says that the agent should check for missing Microsoft updates, then that agent will do the check, using the Windows Update Settings.



This option is visible to all users, but only Partition Administrators are able to change it. Refer to [Appendix A - Software Vulnerability Manager Partition Management](#) for more information.

Flexera Software Package System (SPS) Timestamp

The Flexera SPS Timestamp setting allows users to track when a patch was deployed to its system when [Creating a Patch with the Flexera Package System \(SPS\)](#).



Under the **Flexera SPS Timestamp** drop-down menu, you can select the default “No timestamp required” option or the appropriate timestamp provider.

Mask paths that show user names

To comply with the European Union’s General Data Protection Regulation (GDPR), folder names that contain user information (Example: C:\Documents and Settings\Username) can be concealed using environment variables instead of hard-coded paths (Example: %HOMEPATH%).

Select **Enable Masking** to turn on the GDPR functionality of concealing user name information.



Note • This setting is only available beginning with the Software Vulnerability Manager May 2018 release.

Mask paths that show user names

This setting (not applicable for SCCM imports) is used to ensure windows environment variable names are used instead of user name for the paths that contain profile names.[?](#)

☒ Enable Masking

Configure Agent’s status polling

To address a server’s high CPU usage during high volume of scan data:

- Agent polling has been switched off by default as agent polling is intended for debugging purposes only and is not needed for core functionality. You have the ability to turn agent polling ON or OFF.

Configure Agent’s status polling

After submitting scan to the server, agent polls the server to figure out if the processing is completed. You can reduce the server traffic by stopping agent from polling.[?](#)

☐ Stop agent polling

- Agent code includes a logic to determine if the scan data being uploaded to the server is the same as the prior scan. If it is, then the agent does not upload the data to the server, thereby decreasing traffic on the server. On the server side, this logic is turned off by default and is only recommended to be turned on for situations where clients are doing daily scans, Live Update is enabled, and the host machines are relatively stable in terms of software installed on them. Server logic can be further tuned with the parameter SKIP_ON_SAME_SCAN_HASH in config.ini, which controls the number of scans after which the agent is required to send a full scan data to the server. By default, the value of this parameter is zero. Setting it to a number greater than zero will enable this feature.

Default Recipient Settings

Specify the default email and SMS recipient lists used throughout the Software Vulnerability Manager User Interface in various ways, including generating reports and configuring Smart Group notifications.

Default Recipient Settings

These settings define the default email/SMS recipient lists used throughout the Software Vulnerability Manager User Interface in various ways, including generating reports and configuring Smart Group notifications. Select email addresses/SMS numbers and click "Save" to update your default setting.

Note: When configuring a report or a notification, if desired, a user can provide a select recipient list to use other than the default ones defined here.

Search...

Available Email Recipients		Selected Email Recipients	
Name	Email	Name	Email
<input type="checkbox"/> user1			

Page 1 of 1

Displaying Available Recipients 1 - 1 of 1

Windows Update Settings

The **Windows Update Settings** control the behavior of the Windows Update Agent (WUA) used by Software Vulnerability Manager and the Software Vulnerability Manager Agent (csia.exe) to retrieve update information on Windows and other Microsoft products. Each update setting is further explained below.

Windows Update Settings

Configure the behaviour of the Windows Update Agent (WUA). [?](#)

☐ Use a managed Windows Update server
☒ Use the official Windows Update server
☐ Use the official Microsoft Update server
☐ Use offline method: path to .CAB file

☒ Enable WMI Check

Use a managed Windows Update server

The csia.exe agent will request a check for updates through an enterprise managed WSUS instance. On machines not configured through WSUS, this check for updates will result in the error: 0x80244011 "WU Server policy value is missing in the registry".

Use the official Windows Update server

The csia.exe agent will request a check for updates through the public Windows Update server. This check will only return updates related to Windows.

Use the office Microsoft Update server

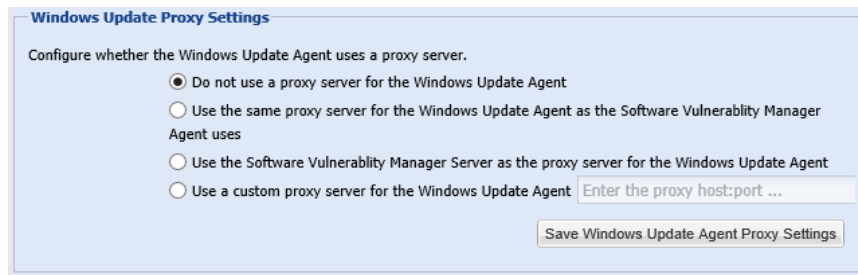
The csia.exe agent will request a check for updates through the public Windows Update server. This check will return a superset of the "Windows Update server" results that include Windows updates and updates for Microsoft products such as Office (non App-V, non App-X installs only) and MSVC redistributables.

Use offline method: path to .CAB file

You should implement the .cab file scanning of windows update for clients that are not connected to the Internet and cannot access WSUS or MU/WU. In such situations Microsoft provides a .cab file that can be used to scan the system. There are limitations to this feature:

- You are responsible for placing the file in a location accessible by Windows Update Services. The file must be on the local file system; placing the file on a shared drive is not supported by Windows Update Services.
- The alternate scan data source (.cab file) only includes high priority updates (security bulletins, critical updates, update rollups) and some service packs. It does not include optional updates (such as updates, feature packs, and tools) and some service packs. If a machine uses this source for scanning, then it is likely that fewer patches will be detected.
- Software Vulnerability Manager should be run as administrator.

For the **Windows Update Proxy Settings**, select “Do not use a proxy server for the Windows Update Agent”.



Enable WMI Check

Agents can be configured to include security updates from SCCM in the scan data. This feature can be used along with an existing missing security update collection or as the only source for missing knowledge base information.

Log Messages

Use this page to view sequential data regarding the actions being performed by Software Vulnerability Manager. It can also be used to detect and fix any issues that you might experience with the Software Vulnerability Manager console. The Log Details page becomes populated when you select the **Configuration > Settings > Debug Logging > Enable Logging** check box.

Right-click or double-click a message to copy the row data to the clipboard. Click **Clear** to remove all log entries. In the event of a support request you may be requested to provide relevant information from this page.

Activity Log

Use this page to view information about user activity within Software Vulnerability Manager, for example “write” actions, logins, and so on, with the exception of scans (due to the volume of data generated). You can access a full activity and login log for compliance monitoring and auditing purposes.

Click the calendar icon next to the From and To fields to set a specific Activity Log date range to view. You can also use the Search field to filter the Activity Log results to specific actions, for example changes to IP access rules.

Select Show Priorities to filter the results by High, Medium or Low Priority.

Activity Log							
Show all logs From: 2018-01-18 To: 2018-04-18 Search Show Priorities ▾ Export ▾							
Activity Name	Activity Status	User	Time ▾	Activity Information	Host	Priority	
User Login	Successful		12:00 18th Apr, 2018	Login (Software Vulnerability Manager)	10.20.40.216	Medium	
User Login	Successful		12:00 18th Apr, 2018	Authentication by cached UID	10.20.40.216	High	

Suggest Software

Use this page to send details about software that you would like to be added to our File Signature database.

It is important to enter as much information as possible to facilitate the processing and acceptance of your request.

Suggest Software

Your Contact Details

Your recipient profile information will be automatically submitted with this suggestion.
Username: bmd12
Email: smallikarjunappa@flexerasoftware.com

Product Details

Product Path:
Product Name:
Product URL:
Description:

Security

Software Vulnerability Manager provides the following security features for user passwords:

- [Change Password](#)
- [Password Recovery Settings](#)

Change Password

Use this page to change the Software Vulnerability Manager account password for the user that is currently logged in. The new password must contain a minimum of eight characters, or comply with the criteria defined in the [Password Policy Configuration](#) rules.



Change Password

Change Stored Password Data

Password must conform to the following policy:

- Be at least 8 characters long.
- Contain at least 1 digit(s).
- Contain both upper and lower case alphabetic characters.

Existing Password:

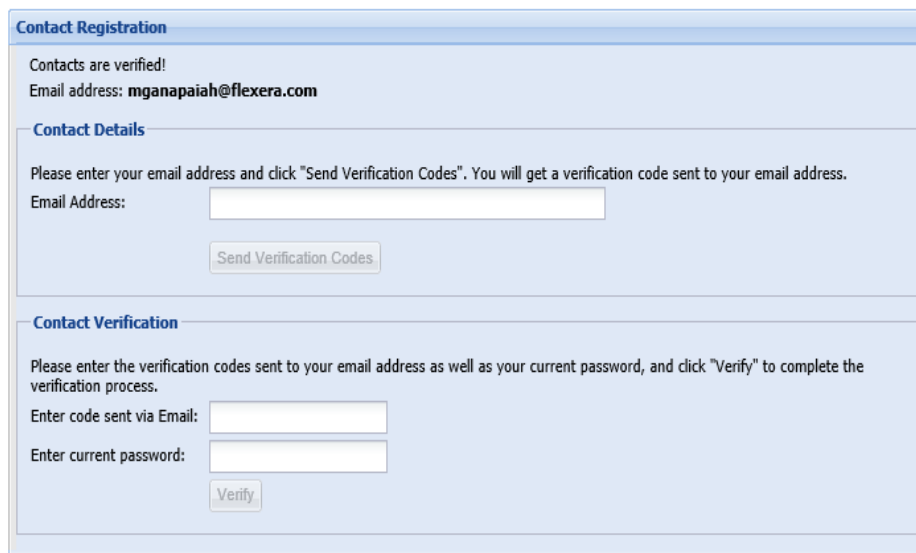
Enter New Password:

Confirm New Password:

Password Recovery Settings

Use this page to verify your email address and mobile number that will be used for password recovery. If your password is lost you can reset it at login using your verified email address and mobile number.

In the Contact Details fields you must provide your email address and a mobile phone number and click Send Verification Codes. The verification code will be received in two separate messages – one SMS on your mobile phone and the second via an email message. When entering your mobile phone number, you should select your country code from the drop-down list.



Contact Registration

Contacts are verified!
Email address: **mganapaiah@flexera.com**

Contact Details

Please enter your email address and click "Send Verification Codes". You will get a verification code sent to your email address.

Email Address:

Contact Verification

Please enter the verification codes sent to your email address as well as your current password, and click "Verify" to complete the verification process.

Enter code sent via Email:

Enter current password:

A

Appendix A - Software Vulnerability Manager Partition Management

This appendix explains how to create and administer your Software Vulnerability Manager Partitions:

- [Introduction](#)
- [Partition Management](#)

Introduction

Use **Administration > Partition Management** to create and administer:

- Additional Software Vulnerability Manager Partitions by assigning a specific number of host and user licenses
- User roles with specific modules and read/write permissions with host licenses

Your overall corporate group of machines is your network. Software Vulnerability Manager gives you the ability to logically partition your network. If you only use one network partition then your network and your network partition are the same thing. If your company is divided across logical and physical partitions, you can mimic that in Software Vulnerability Manager by creating multiple network partitions.

Refer to [Administration](#) for more information regarding [User Management](#).



Note • Using a single WSUS server with multiple partitions is not supported.

Partition Management

Use this page to create and administer your Software Vulnerability Manager Partitions.

- [Overview](#)
- [Permissions](#)
- [Host and User Licenses](#)

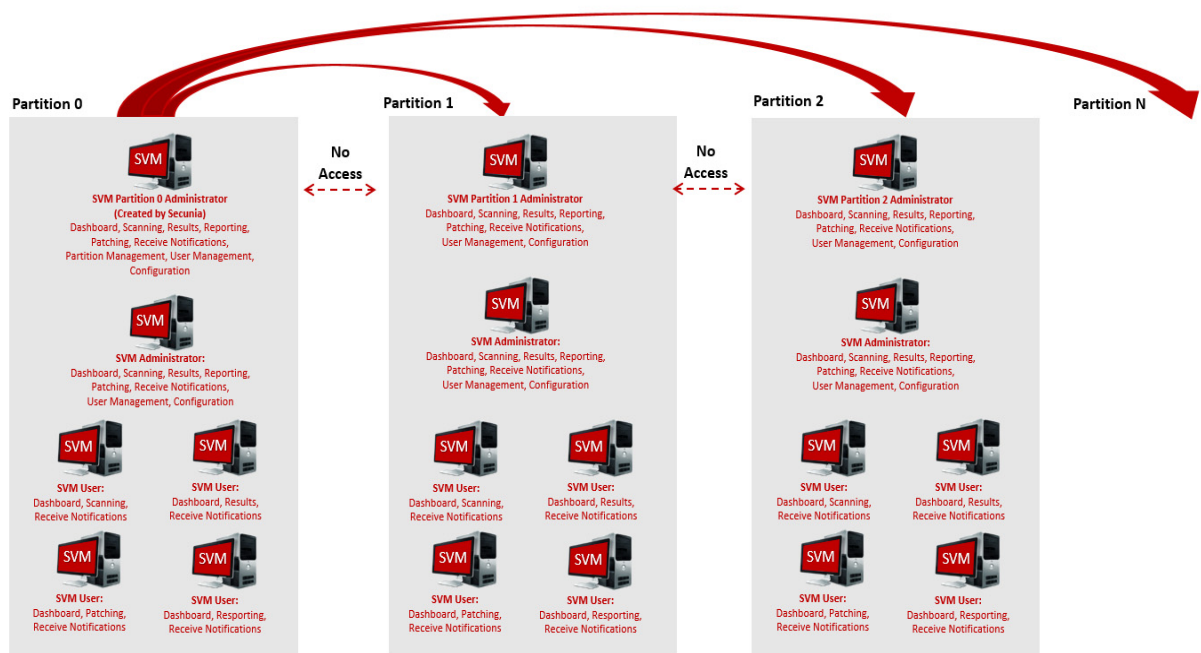
- Create a New Partition Administrator
- Grant User Access to all Completed Scans and Single Host Agent Entries

Overview

When Flexera creates the Software Vulnerability Manager base user, this user is the Partition Administrator of “Partition 0”. The Partition 0 Administrator is the unique global administrator for the company, irrespective of how many partitions are created.

The Partition 0 Administrator can create further network partitions by creating new Partition Administrators. Only the Partition 0 Administrator can create new partitions.

Every partition has identical functionality – the only difference is that an entire partition ($N > 0$) can be deleted by the Partition 0 Administrator.



Note • Just as creating a partition is done by creating a new Partition Administrator, deleting an entire partition is done by deleting the Partition Administrator.

Within a partition, there is only one Partition Administrator. All additional accounts are regular users, however, these users all have specific roles. One of the roles a user can have is Administrator.

The main difference between users who have the Administrator role and those who don't is that Administrators can create and delete other users within their partition. They can delete any non-administration users, but not other Administrator users.

The Partition 0 Administrator can access the **Partition Management** and **User Management** menus.

All other Partition Administrators can only access the **User Management** menu.

Permissions

The MySQL user that is being used to connect to the database requires full privileges on the MySQL server (including the grant option) as in the following SQL statement:

```
GRANT ALL PRIVILEGES ON *.* TO 'secunia_user'@'localhost' WITH GRANT OPTION;
```

The WITH GRANT OPTION is only required when creating Partitions. If you don't want to permanently give the GRANT privilege to Software Inspector's MySQL user, you can give the permission temporarily when creating Partitions and then revoke the permission afterwards.

Host and User Licenses

The Partition 0 Administrator is assigned user licenses from Flexera. When the Administrator creates a new partition, licenses are allocated to the Partition Administrator of that partition. Those licenses are effectively no longer relevant to Partition 0 – and no one in Partition 0 can use them. The Partition 0 Administrator can reclaim **unused** licenses from another Partition by right-clicking an existing account and editing it.

The Host and User licenses in a given partition belong to a shared pool. Any user who scans hosts will use host licenses from this pool. When a user is created, an Administrator can limit how many active licenses they can claim – note, this is only an upper bound of the licenses they can use, and should not be confused with them being “assigned” licenses.

User licenses are used per account. For example, when the Partition 0 Administrator is assigned 100 licenses from Flexera, they use one for their account, so there are 99 left in the pool. The Partition 0 Administrator only assigns them when creating a new Partition. For example, the Partition 0 Administrator creates a user for Partition 1 (that takes 1 license), and gives the Partition 1 Administrator 50 user licenses. The Partition 0 Administrator now has 48 left, and the Partition 1 Administrator has 50, meaning, at most 50 additional users could be created in Partition 1.

When an Administrator in a given partition creates a user, they use 1 user license from the pool in that partition. When that user is deleted, their user license is re-added to the pool.

Create a New Partition Administrator

Click **Create New Partition Administrator** and fill in the form, providing all the necessary details about the Partition Administrator and include the number of host and user licenses to assign.

Create New Partition Administrator

Account Details

Name:

Username:

Email:

☒ Generate a new one-time password and email it to the address specified above

Assign Host Licenses: (11 Host Licenses Available)

Assign User Licenses: (26 User Licenses Available)

Recipient Details

Enter an email address and (optionally) a mobile number to be used for emails, notifications and alerts the Flexera Software Vulnerability Manager can be configured to send.

Email:

Mobile Number: ()

An email will be sent to the User containing a welcome message and the Software Vulnerability Manager login credentials.

Right-click an existing account to view, edit or delete the partition.

Partition Administrators can choose Smart Groups to copy to another account using the Create/Edit User form.

Create New User

☐ Restrict On IP Range

☐ Restrict On IP Network

Existing Hostname or IP Based Restrictions

Type	Scan Target
No Restrictions Configured	

Share Smart Groups

Choose which Smart Groups you would like to copy to this User

Name	Description	Status
Insecure installa...		<input type="checkbox"/>
high_and_above		<input type="checkbox"/>
from remote		<input type="checkbox"/>
Extremely Critical...		<input type="checkbox"/>
7-Day Critical Vu...	This will show all insecure products rated "Highly" or "Extremely Critical",...	<input type="checkbox"/>



Note • Sub-Accounts are not allowed to modify their copy of a Smart Group.

The Partition Administrator can also unshare a copy of a Smart Group.

If the Sub-Account already has a Smart Group of the same name and type, the Partition Administrator cannot share their copy with them.

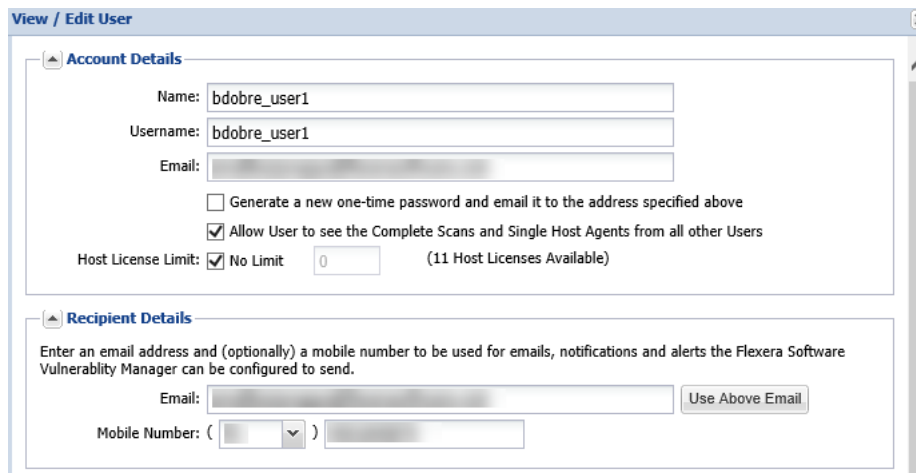
If the Partition Administrator modifies the Smart Group, all shared copies are also modified.

If the Partition Administrator deletes the Smart Group, all shared copies are also deleted.

Grant User Access to all Completed Scans and Single Host Agent Entries

Partition Administrators can permit a user or administrator to view all Completed Scans and Single Host Agents by selecting a check box in the User Account Details form.

When enabled, the user will be able to see the Completed Scans and Single Host Agents from all other users in their partition.



The screenshot shows a 'View / Edit User' dialog box with two main sections: 'Account Details' and 'Recipient Details'.

Account Details:

- Name: bдобре_user1
- Username: bдобре_user1
- Email: [Redacted]
- ☐ Generate a new one-time password and email it to the address specified above
- ☒ Allow User to see the Complete Scans and Single Host Agents from all other Users
- Host License Limit: ☒ No Limit (11 Host Licenses Available)

Recipient Details:

Enter an email address and (optionally) a mobile number to be used for emails, notifications and alerts the Flexera Software Vulnerability Manager can be configured to send.

Email: [Redacted]

Mobile Number: ()



Note • This functionality is not available when editing a Partition Administrator or when creating a new user or administrator, only when editing an existing one.

Appendix B - About Secunia Advisories

This section includes the following articles:

- [CVSS \(Common Vulnerability Scoring System\)](#)
- [CVE References](#)
- [Where \(Attack Vector\)](#)
- [Criticality \(Severity Rating\)](#)
- [Impact \(Consequence\)](#)

CVSS (Common Vulnerability Scoring System)

The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.

CVSS enables IT managers, vulnerability bulletin providers, security vendors, application vendors, and researchers to all benefit by adopting this common language of scoring IT vulnerabilities.

CVSS consists of three groups: Base, Temporal, and Environmental. Each group produces a numeric score ranging from 0 to 10, and a Vector; a compressed textual representation that reflects the values used to derive the score.

- **The Base group** represents the intrinsic qualities of a vulnerability.
- **The Temporal group** reflects the characteristics of a vulnerability that changes over time.
- **The Environmental group** represents the characteristics of a vulnerability that are unique to any user's environment.

For details on interpreting a CVSS vector, refer to <https://www.first.org/cvss/specification-document>.

Secunia Advisories include a Secunia derived CVSS score and vector, as well as a link to an implementation of the NIST CVSS calculator so that a user can adjust temporal and environmental metrics for advisories that match your Watch Lists.

The National Vulnerability Database (NVD) CVSS score/vector for each relevant CVE contained in an Advisory is also shown, and is similarly linked to the NIST CVSS calculator.

CVE References

A CVE (Common Vulnerabilities and Exposures) name represents a unique, standardized name and description for a given vulnerability or exposure.

Searching on a CVE reference (for example CVE-2009-3793 or simply 2009-3793) will find all Secunia Advisories in the database that list that particular CVE as a reference.

An Advisory can contain more than one CVE reference, and not every Advisory has an associated CVE reference.

Where (Attack Vector)

The following are Where (Attack Vector) values.

Local System

Local system describes vulnerabilities where the attack vector requires that the attacker is a local user on the system.

Local Network

From local network describes vulnerabilities where the attack vector requires that an attacker is situated on the same network as a vulnerable system (not necessarily a LAN).

This category covers vulnerabilities in certain services (for example, DHCP, RPC, administrative services, and so on), which should not be accessible from the Internet, but only from a local network and optionally a restricted set of external systems.

Remote

From remote describes vulnerabilities where the attack vector does not require access to the system nor a local network.

This category covers services, which are acceptable to expose to the Internet (for example, HTTP, HTTPS, SMTP) as well as client applications used on the Internet and certain vulnerabilities, where it is reasonable to assume that a security conscious user can be tricked into performing certain actions.

Criticality (Severity Rating)

The following are Severity Rating values.

Extremely Critical

This value is typically used for remotely exploitable vulnerabilities that can lead to system compromise.

Successful exploitation does not normally require any interaction and exploits are in the wild.

These vulnerabilities can exist in services like FTP, HTTP, and SMTP or in certain client systems such as email programs or browsers.

Highly Critical

This value is typically used for remotely exploitable vulnerabilities that can lead to system compromise.

Successful exploitation does not normally require any interaction, but there are no known exploits available at the time of disclosure.

These vulnerabilities can exist in services like FTP, HTTP, and SMTP or in client systems, such as email programs or browsers.

Moderately Critical

This value is typically used for remotely exploitable Denial of Service vulnerabilities against services like FTP, HTTP, and SMTP, and for vulnerabilities that allow system compromises but require user interaction.

This rating is also used for vulnerabilities allowing system compromise on LANs in services like SMB, RPC, NFS, LPD and similar services that are not intended for use over the Internet.

Less Critical

This value is typically used for cross-site scripting vulnerabilities and privilege escalation vulnerabilities.

This rating is also used for vulnerabilities allowing exposure of sensitive data to local users.

Not Critical

This value is typically used for very limited privilege escalation vulnerabilities and locally exploitable Denial of Service vulnerabilities.

This rating is also used for non-sensitive system information disclosure vulnerabilities (for example, remote disclosure of installation path of applications).

Impact (Consequence)

The following are Consequence values.

Brute Force

Used in cases where an application or an algorithm allows an attacker to guess passwords in an easy manner.

Cross-Site Scripting

Cross-Site Scripting vulnerabilities allow a third party to manipulate the content or behavior of a web application in a user's browser, without compromising the underlying system.

Different Cross-Site Scripting related vulnerabilities are also classified under this category, including “script insertion” and “cross-site request forgery”.

Cross-Site Scripting vulnerabilities are often used against specific users of a website to steal their credentials or to conduct spoofing attacks.

DoS (Denial of Service)

This includes vulnerabilities ranging from excessive resource consumption (for example, causing a system to use a lot of memory) to crashing an application or an entire system.

Exposure of Sensitive Information

Vulnerabilities where documents or credentials are leaked or can be revealed either locally or remotely.

Exposure of System Information

Vulnerabilities where excessive information about the system (for example, version numbers, running services, installation paths, and similar) are exposed and can be revealed from remote and, in some cases, locally.

Hijacking

Covers vulnerabilities where a user session or a communication channel can be taken over by other users or remote attackers.

Manipulation of Data

This includes vulnerabilities where a user or a remote attacker can manipulate local data on a system, but not necessarily be able to gain escalated privileges or system access.

The most frequent type of vulnerabilities with this impact are SQL-injection vulnerabilities, where a malicious user or person can manipulate SQL queries.

Privilege Escalation

Covers vulnerabilities where a user is able to conduct certain tasks with the privileges of other users or administrative users.

This typically includes cases where a local user on a client or server system can gain access to the administrator or root account, thus taking full control of the system.

Security Bypass

Covers vulnerabilities or security issues where malicious users or people can bypass certain security mechanisms of the application. The actual impact varies significantly depending on the design and purpose of the affected application.

Spoofing

Covers various vulnerabilities where it is possible for malicious users or people to impersonate other users or systems.

System Access

Covers vulnerabilities where malicious people are able to gain system access and execute arbitrary code with the privileges of a local user.

Unknown

Covers various weaknesses, security issues, and vulnerabilities not covered by the other impact types, or where the impact is not known due to insufficient information from vendors and researchers.



Appendix C - CSV Export File Cross-References

When you export data from the Software Vulnerability Manager user interface to a CSV file, some values may differ. Each data set in this appendix includes a cross-reference table to explain the different values between the user interface and CSV file.



Note • Dates and times in the Software Vulnerability Manager database are created using the Coordinated Universal Time (UTC). In the UI, dates and times in UTC are converted to reflect your local time zone. This UTC date and time conversion is not possible for CSV reports, resulting in a date and time mismatch between the UI and CSV report.



Note • When you set the agent to scan “As soon as possible”, the date and time in the UI will be listed “As soon as possible” with a date in the past as the next scan date. In the CSV report, the scan date is the actual date from the Software Vulnerability Manager database without transformation.

This section provides a cross-reference for the following CSV file values:

- [Host Smart Group](#)
- [Advisory Smart Group](#)
- [Product Smart Group](#)
- [Scan Result](#)
- [Completed Scan](#)
- [Scheduled Exports](#)
- [Single Host Agent](#)
- [Smart Group Notifications](#)
- [User Management](#)

Host Smart Group

For further information regarding the Business Impact terminology, see [Criticality \(Severity Rating\)](#).

Advisory Smart Group

Table C-1 • Advisory Smart Group Values from the User Interface Versus the Exported CSV File

Advisory Smart Group Value	Software Vulnerability Manager User Interface	Exported CSV File
Criticality - Extremely Critical	5 bars (red)	1
Criticality - Highly Critical	4 bars (orange)	2
Criticality - Moderately Critical	3 bars (yellow)	3
Criticality - Less Critical	2 bars (light green)	4
Criticality - Not Critical	1 bar (green)	5
Zero Day	No	0
Zero Day	Yes	1
Solution Status	Unpatched	1
Solution Status	Vendor Patched	2
Solution Status	Vendor Workaround	3
Solution Status	Partial Fix	4
Attack Vector	From remote	1
Attack Vector	From local network	2
Attack Vector	Local system	3
Impact	System Access	1
Impact	Denial of Service	2
Impact	Privilege Escalation	3
Impact	Exposure of Sensitive Information	4
Impact	Exposure of System Information	5

Table C-1 • Advisory Smart Group Values from the User Interface Versus the Exported CSV File (cont.)

Advisory Smart Group Value	Software Vulnerability Manager User Interface	Exported CSV File
Impact	Brute Force	6
Impact	Manipulation of Data	7
Impact	Spoofing	8
Impact	Cross Site Mapping	9

See [Appendix B - About Secunia Advisories](#) for further information regarding the following terminology:

- [Where \(Attack Vector\)](#)
- [Criticality \(Severity Rating\)](#)
- [Impact \(Consequence\)](#)

Product Smart Group

For further information regarding the Criticality terminology, see [Criticality \(Severity Rating\)](#).

Scan Result

Table C-2 • Scan Result Values from the User Interface Versus the Exported CSV File

Scan Result Value	Software Vulnerability Manager User Interface	Exported CSV File
Criticality - Extremely Critical	5 bars (red)	1
Criticality - Highly Critical	4 bars (orange)	2
Criticality - Moderately Critical	3 bars (yellow)	3
Criticality - Less Critical	2 bars (light green)	4
Criticality - Not Critical	1 bar (green)	5
Issued	Number of days ago	Month, Day, Year
Soft Type - OS	1	1
Soft Type - Program	2	2

For further information regarding the Criticality terminology, see [Criticality \(Severity Rating\)](#).

Completed Scan

Table C-3 • Completed Scan Values from the User Interface Versus the Exported CSV File

Completed Scan Values	Software Vulnerability Manager User Interface	Exported CSV File
Time	Date, Month, Year, Time (24-hour clock)	Month, Day, Year, Time (12-hour clock)
Results Exist	Yes	1
Results Exist	No	0
Zombie Files	included	(Blank)
Zombie Files	not included	0

Scheduled Exports

Table C-4 • Scheduled Exports Values from the User Interface Versus the Exported CSV File

Scheduled Exports Values	Software Vulnerability Manager User Interface	Exported CSV File
Frequency	One-Time Export	0
Frequency	Hourly	1
Frequency	Daily	2
Frequency	Weekly	3
Frequency	Monthly	4
Last Execution Status	Failed	0
Last Execution Status	Success	(Blank)

Single Host Agent

Table C-5 • Single Host Agent Values from the User Interface Versus the Exported CSV File

Single Host Agent Values	Software Vulnerability Manager User Interface	Exported CSV File
Platform	Mac OS X	11
Platform	Windows	21 or 31
Platform	Red Hat Linux	41

Smart Group Notifications

Table C-6 • Smart Group Notifications Values from the User Interface Versus the Exported CSV File

Smart Group Notifications Values	Software Vulnerability Manager User Interface	Exported CSV File
Smart Group Type	Host	1
Smart Group Type	Product	2
Smart Group Type	Advisory	3
Always Notify	No	0
Always Notify	Yes	1
Frequency	One-Time Export	0
Frequency	Hourly	1
Frequency	Daily	2
Frequency	Weekly	3
Frequency	Monthly	4

User Management

Table C-7 • User Management Values from the User Interface Versus the Exported CSV File

User Management Values	Software Vulnerability Manager User Interface	Exported CSV File
Host License Limit	No Limit	-1
User Type	User	0
User Type	Root Admin or Admin	1



Appendix D - Threat Intelligence

Software Vulnerability Manager Threat Intelligence helps you prioritize the patching efforts.

In a world where there are more than 18,000 new vulnerabilities every year, being smart about prioritizing remediation efforts is essential. Leveraging our optional Threat Intelligence Module, another valuable layer of insight is provided to help you understand which of the vulnerabilities affecting your environment are actually being exploited in the wild.

Industry reports, including Gartner shows that between 6%-10% of the vulnerabilities disclosed each year actually are exploited in the wild. Turns out that most of these have medium CVSS scores, which are typically overlooked by organizations. With the insights provided by threat intelligence, it is possible better optimize the time spent remediating software vulnerabilities. Avoid spending time and resources in patching vulnerabilities that do not have evidence of exploitation, and favor those that do. Prioritization is crucial for effective risk mitigation and resource utilization.

Leveraging machine learning, artificial intelligence, and human curation from thousands of sources in the open, deep and dark web, our Threat Intelligence Module augments Software Vulnerability Manager's vulnerability intelligence with a Threat Score that provides the ultimate prioritization tool for your busy desktop operations teams.

This appendix explains how the Software Vulnerability Manager Threat Intelligence module helps the enterprises to manage their resources and Patching Vulnerabilities more effectively, the following topics are discussed in this section:

- [Evidence of Exploitation](#)
- [Criteria for the Threat Score Calculation](#)
- [Threat Score Calculation - Examples](#)
- [Threat Intelligence Data for Operations and Security](#)
- [Threat Score Locations](#)



Note • Please note the following:

- *Secunia Advisory Threat Scores and Vulnerability (CVE) Threat Scores are each calculated as described in the [Criteria for the Threat Score Calculation](#) section (an Advisory score is not determined by simply adding related CVE Threat Scores).*

- For pricing and availability, please contact your sales representative or contact us online at: <https://www.flexera.com/about-us/contact-us.html>
- For more details about the SVM or SVR Threat Intel Modules, please see our datasheet: <https://www.flexera.com/media/pdfs/datasheet-svm-threat-intelligence-module.pdf>

Evidence of Exploitation

There are 6 primary rules that can impact the assigned Threat score and they are:

- It has been linked to remote access Trojan
- It has been linked to ransomware
- It has been linked to penetration testing tools
- It has been linked to malware
- It has been linked to an exploit kit
- It has been linked to a cyber exploit

In Software Vulnerability Manager we provide the resulting score for any given Secunia Advisory to add value to the prioritization process. In Software Vulnerability Research, where a security persona requires more insight, we provide these Threat Scores for the Secunia Advisory, and for each vulnerability in the advisory. Further, we will show which of the rules above were triggered to arrive at the threat score presented.

Criteria for the Threat Score Calculation

Triggered rules increase the score by the values identified in the chart below based on the highest severity level triggered.

Table D-1 • Rules, Severity and Value

Rule	Severity	Value
Recently Linked to Remote Access Trojan	Very Critical	+5
Historically Linked to Remote Access Trojan	Critical	+4
Recently Linked to Ransomware	Very Critical	+5
Historically Linked to Ransomware	Critical	+4
Recently Linked to Penetration Testing Tools	Medium	+2
Historically Linked to Penetration Testing Tools	Low	+1
Recently Linked to Malware	High	+3
Historically Linked to Malware	Medium	+2
Recently Linked to Exploit Kit	Very Critical	+5

Table D-1 • Rules, Severity and Value

Rule	Severity	Value
Historically Linked to Exploit Kit	Critical	+4
Linked to Recent Cyber Exploit	Low	+1
Linked to Historical Cyber Exploit	Low	+1

The rule with the highest criticality determines the point range and the starting value for the Threat Score. The ranges for each are as follows:

Table D-2 • Criticality - Ranges

Criticality	From	To
Very Critical	71	99
Critical	45	70
High	24	44
Medium	13	23
Low	1	12
None	0	0



Note • when assigning a Threat Score to the SAID, we do not simply add up the scores for each associated vulnerability, but rather follow the same rules outlined here to calculate the Security Advisory threat score.

Threat Score Calculation - Examples

Some examples to explain how we would arrive at a Threat Score.

Example 1

A SAID has two CVEs; two come back as exploited.

Triggered Rules

The following rules are triggered:

- **CVE1 triggers**
 - Historically Linked to Remote Access Trojan
 - Linked to Recent Cyber Exploit

- **CVE2 triggers**
 - Historically Linked to Exploit Kit

The Threat Score would be **54**.

Calculating the Score

The criticality range is set by the most critical rule triggered, which is critical. This sets the score's maximum and minimum range as between 45 and 70.

Item	Value
Base Score	+45
Historically Linked to Exploit Kit	+4
Linked to Recent Cyber Exploit	+1
Historically Linked to Remote Access Trojan	+4
Threat Score (Sum of above values)	54

Example 2

A SAID has seven CVEs; and all come back as exploited.

Triggered Rules

The following rule is triggered by all CVEs:

- **CVE1, CVE2, CVE3, CVE4, CVE5, CVE6 and CVE7 triggers**
 - Historically Linked to Exploit Kit

The Threat Score would be **70**.

Calculating the Score

The criticality range is set by the most critical rule triggered, which is critical. This sets the score's maximum and minimum range as between 45 and 70.

Item	Value
Base Score	+45
Historically Linked to Exploit Kit	+4 * 7 CVE = +28
Threat Score (Sum of above values)	73



Note • At this point, we have exceeded the maximum for a critical threat, which is 70, so the score is 70.

Example 3

A SAID has one CVE and it comes back as exploited.

Triggered Rules

The following rule is triggered:

- **CVE1 triggers**
 - Recently Linked to Malware

The Threat Score would be **27**.

Calculating the Score

The criticality range is set by the most critical rule triggered, which is high. This sets the score's maximum and minimum range as between 24 and 44.

Item	Value
Base Score	+24
Recently Linked to Malware	+3
Threat Score (Sum of above values)	27

Example 4

A SAID has many CVEs, none come back as exploited.

The score would be **0** because there are no rules triggered.

Advisory with Multiple Vulnerabilities

An advisory Threat Score is based upon each of the CVEs included in an Advisory as specified above. In Software Vulnerability Research, the vulnerabilities that have exploits are indicated with a red circle for easier identification.

Threat Intelligence Data for Operations and Security

Software Vulnerability Manager and Software Vulnerability Research cater to different audiences with different needs. Software Vulnerability Manager (for operations) provides what is needed for Operations to better prioritize remediation efforts. Whereas Software Vulnerability Research (for security) provides more detail to meet the needs of security teams.

Table D-3 • Software Vulnerability Manager vs. Software Vulnerability Research

Software Vulnerability Manager	Software Vulnerability Research
<ul style="list-style-type: none">• Offers a Threat Score at the Advisory level	<ul style="list-style-type: none">• Offers a Threat Score at the Advisory level• Offers a Threat Score at the vulnerability level, within the advisory• Offers a list of which rules were triggered to arrive at the Threat Score displayed

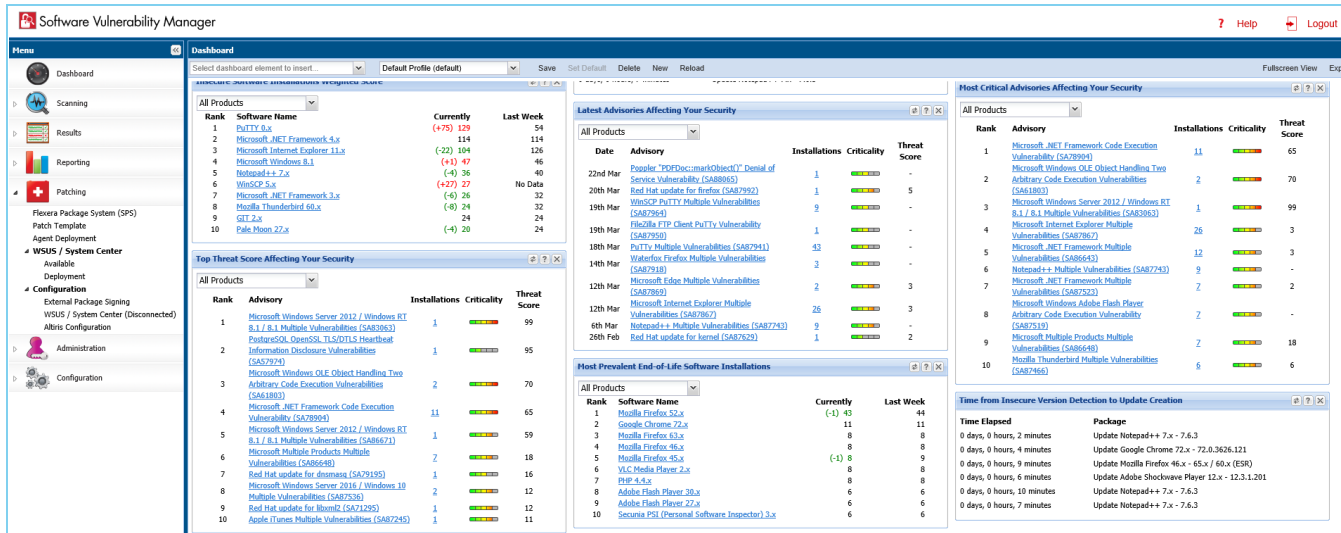
Threat Score Locations

In Software Vulnerability Manager, subscribed users can find the Threat Score in the following places:

- [Dashboard Threat Score](#)
- [Completed Scan Page Threat Score](#)
- [All Advisory Popup Threat Score](#)
- [All Installation Popup Threat Score](#)
- [Advisory Summary Threat Score](#)
- [Host Smart Group Threat Score](#)
- [Product Smart Group Threat Score](#)
- [Smart Group Criteria Threat Score](#)
- [All Advisory Threat Score](#)
- [All Advisory Smart Group Criteria Threat Score](#)
- [Zero Day Advisory Threat Score](#)
- [Flexera Package System \(SPS\) List Threat Score](#)

Dashboard Threat Score

The following image is an example of the Dashboard Threat Score.



Completed Scan Page Threat Score

Once the scan is completed, the user can see the **Threat Score** in the **Scan Result**.

Overview Scan Result									
<input checked="" type="checkbox"/> Secure <input checked="" type="checkbox"/> End-Of-Life <input checked="" type="checkbox"/> Insecure									
Name	Version	State	SAID	Criticality	CVSS Base Score	Threat Score...	Issued	Vulnerabilities	
Microsoft Windows 8.1	Windows 8.1 En...	Insecure	SA61803		v2: 10	70	1619 days ago	2	
Microsoft .NET Framework 4.x	4.0.30319.33440	Insecure	SA78904		v2: 10	62	563 days ago	1	
Microsoft .NET Framework 4.x	4.0.30319.33440	Insecure	SA78904		v2: 10	62	563 days ago	1	
Microsoft .NET Framework 4.x	4.0.30319.33440	Insecure	SA78904		v2: 10	62	563 days ago	1	
Microsoft Word 2016 / O365	16.0.9126.2282	Insecure	SA86262		v3: 8.8	9	136 days ago	11	
Microsoft Skype for Business 2016	16.0.9126.2282	Insecure	SA85499		v3: 7.8	5	171 days ago	5	
Microsoft Visio 2016	16.0.9126.2282	Insecure	SA85499		v3: 7.8	5	171 days ago	5	
Microsoft Access 2016 / O365	16.0.9126.2282	Insecure	SA85499		v3: 7.8	5	171 days ago	5	
Microsoft Publisher 2016 / O365	16.0.9126.2282	Insecure	SA85499		v3: 7.8	5	171 days ago	5	
Microsoft OneNote 2016 / O365	16.0.9126.2282	Insecure	SA85499		v3: 7.8	5	171 days ago	5	
Microsoft Excel 2016 / O365	16.0.9126.2282	Insecure	SA86648		v3: 8.8	4	108 days ago	6	
Microsoft Excel 2016 / O365	16.0.9126.2282	Insecure	SA86648		v3: 8.8	4	108 days ago	6	
Microsoft Outlook 2016 / O365	16.0.9126.2282	Insecure	SA86648		v3: 8.8	4	108 days ago	6	
Microsoft PowerPoint 2016 / O365	16.0.9126.2282	Insecure	SA86648		v3: 8.8	4	108 days ago	6	
Microsoft Internet Explorer 11.x	11.0.9600.19036	Insecure	SA87867		v3: 8.8	3	17 days ago	12	
Microsoft Internet Explorer 11.x	11.0.9600.19036	Insecure	SA87867		v3: 8.8	3	17 days ago	12	
Pale Moon 27.x	27.2.0.6284	Insecure	SA83814		v3: 9.8	3	284 days ago	1	

Page 1 of 7

Displaying products 1 - 27 of 179

All Advisory Popup Threat Score

When the user double clicks any of the products in the above screen, all the advisories related to that product appear along with their **Threat Score**.

The screenshot shows the QA_WIN8 application interface. The main window has tabs for 'Overview' and 'Scan Result'. Under 'Scan Result', there are checkboxes for 'Secure', 'End-Of-Life', and 'Insecure'. A list of products is shown, including 7-zip 16.x, Adobe Acrobat Reader DC 19.x, Adobe Flash Player 27.x, Apple Bonjour for Windows 3.x, Apple Safari 5.x, Apple Software Update 2.x, Fiddler 5.x, Google Chrome 72.x, Google Toolbar 7.x, Microsoft .NET Framework 4.x, Microsoft Access 2016 / O365, Microsoft Excel 2016 / O365, Microsoft Internet Explorer 11.x, Microsoft Internet Explorer 11.x, Microsoft Malware Protection..., Microsoft Malware Protection..., Microsoft OneNote 2016 / O365, Microsoft Outlook 2016 / O365, Microsoft PowerPoint 2016 / ..., Microsoft Publisher 2016 / O365, and Microsoft Security Essentials 4.x.

A popup window titled 'Microsoft .NET Framework 4.x' is open, showing a list of installations. The popup has tabs for 'Overview', 'Installations', and 'All Advisories'. The 'All Advisories' tab is selected, displaying a table of advisories for the selected product.

SAID	Advis...	Criticality	Threat Score	Advisory Publish...	Solution Status	Attack Vector	Zero Day	CVSS Base Sco
SA87523	Micros...	2	2	2019-02-13	Vendor Patched	From remote	No	v3: 7.8
SA86939	Micros...	-	-	2019-01-08	Vendor Patched	From remote	No	v3: 5.3
SA86643	Micros...	3	3	2018-12-11	Vendor Patched	From remote	No	v3: 9.8
SA85069	Micros...	2	2	2018-09-11	Vendor Patched	From remote	No	v3: 7.8
SA84667	Micros...	-	-	2018-08-14	Vendor Patched	From remote	No	v3: 5.8
SA84046	Micros...	5	5	2018-07-11	Vendor Patched	From remote	No	v3: 9.8
SA83044	Micros...	-	-	2018-05-08	Vendor Patched	From remote	No	v2: 7.8
SA80918	Micros...	3	3	2018-01-10	Vendor Patched	From remote	No	v2: 7.8
SA78904	Micros...	93	93	2017-09-12	Vendor Patched	From remote	Yes	v2: 10
SA77765	Micros...	3	3	2017-07-11	Vendor Patched	From remote	No	v2: 7.8
SA76746	Micros...	3	3	2017-05-09	Vendor Patched	From remote	No	v2: 7.8
SA76680	Micros...	2	2	2017-05-09	Vendor Patched	From remote	No	v2: 6.4
SA76228	Micros...	2	2	2017-04-11	Vendor Patched	From remote	No	v2: 10
SA74257	Micros...	2	2	2016-12-13	Vendor Patched	From remote	No	v2: 5

The popup window also shows a 'Page 1 of 4' indicator and a 'Displaying advisories 1 - 15 of 53' message. The main window shows a 'Page 1 of 8' indicator and a 'Displaying products 1 - 27 of 191' message.

All Installation Popup Threat Score

When the user double clicks the product and selects the **Installations** tab, all the installations of that product get appear along with their **Threat Score**.

QA_WIN8

Overview Scan Result

☐ Secure ☐ End-Of-Life ☒ Insecure Export

Name	Version	State	SAID	Criticality	CVSS Base Score	Threat Score	Issued	Vulnerability
Microsoft .NET Framework 4.x	4.0.30319.33440	Insecure	SA66386		v2: 7.5	4	1298 days ago	
Microsoft .NET Framework 4.x	4.0.30319.33440	Insecure	SA66386		v2: 7.5	4	1298 days ago	
Microsoft .NET Framework 4.x	4.0.30319.33440	Insecure	SA66386		v2: 7.5	4	1298 days ago	
Microsoft Excel 2016 / O365	16.0.9126.2295	Insecure	SA86648		v3: 8.8	4	108 days ago	
Microsoft Excel 2016 / O365	16.0.9126.2295	Insecure	SA86648		v3: 8.8	4	108 days ago	
Microsoft Internet Explorer 11.x	11.0.9600.19036	Insecure	SA86719		v3: 8.8	52	99 days ago	
Microsoft Internet Explorer 11.x	11.0.9600.19036	Insecure	SA86719		v3: 8.8	52	99 days ago	
Microsoft Outlook 2016 / O365	16.0.9126.2295	Insecure	SA86648		v3: 8.8	4	108 days ago	
Microsoft PowerPoint 2016 / O365	16.0.9126.2295	Insecure	SA86648		v3: 8.8	4	108 days ago	
Microsoft Windows 8.1	Windows 8.1 Enterpri...	Insecure	SA86671		v3: 9.8	59	108 days ago	
Microsoft Word 2016 / O365	16.0.9126.2295	Insecure	SA86262		v3: 8.8	9	136 days ago	
Mozilla SeaMonkey 2.x	2.32	Insecure	SA84457		v3: 8.8	7	245 days ago	

Microsoft PowerPoint 2016 / O365

View from the context of Smart Group: All Products

Overview Installations All Advisories Export

SAID	Advisory Description	Criticality	Threat Score	Advisory Publish...	Solution Status	Attack Vector	Zero Day	CVSS Base Score	Vulnerabilities
SA86648	Microsoft Multiple Products Multiple Vu...		4	2018-12-11	Vendor Patched	From remote	No	v3: 8.8	
SA85499	Microsoft Multiple Products Multiple Vu...		5	2018-10-09	Vendor Patched	From remote	No	v3: 7.8	
SA85074	Microsoft Multiple Products Multiple Vu...		19	2018-09-11	Vendor Patched	From remote	No	v3: 8.8	
SA84672	Microsoft Multiple Products Multiple Vu...		7	2018-08-15	Vendor Patched	From remote	No	v2: 5 v3: 8.8	

Microsoft Multiple Products Multiple Vulnerabilities

Secunia Advisory Summary

Secunia Advisory ID: SA86648

Creation Date: 2018-12-11

Criticality: - Highly critical

Threat Score: 4

Impact: Exposure of sensitive information
System access

Where: From remote

Solution Status: Vendor Patched

Secunia CVSS3 Scores: Base: 8.8, Overall: 8.2 CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:F/RL:O/RC:C

CVE Reference(s): CVE-2018-8587

Capture screenshot. Close

Host Smart Group Threat Score

The **Threat Score** appears for all the products on the **Host Smart Group Scan Result** page.

Smart Group: "All Hosts" - Last Compiled: 2019-03-25 2:35:46

Showing All Sites Showing All Platforms Search

Host	System Score	Last Scan	Insecure	End-Of-Life	Secure	Total	Site Name	Scan Engine	Software Platform
BANGHV_QA_WIN8A	92%	14th Mar, 2019 19:36	4	5	103	112	abc	System Center	System Center
CS17-W10-145	73%	14th Mar, 2019 19:35	11	12	61	84	abc	System Center	System Center
CS17-WIN10-59	82%	14th Mar, 2019 19:35							
CS17-WIN8-181	72%	14th Mar, 2019 19:35							
localhost.localdomain	88%	14th Mar, 2019 19:35							
MAHOKWIN8	67%	14th Mar, 2019 19:35							
PSCCM	61%	21st Mar, 2019 19:35							
QA_WIN8	82%	20th Mar, 2019 19:35							
QA_WIN81E	81%	14th Mar, 2019 19:35							
QA_WIN8_TEST	77%	14th Mar, 2019 19:35							
SBABAWIN10	65%	21st Mar, 2019 19:35							
SBABA_DEV	83%	14th Mar, 2019 19:35							
SUSHMACSIWIN7	92%	14th Mar, 2019 19:35							
SUSHMA_TESTWIN8	67%	21st Mar, 2019 19:35							
sushma_win81A	88%	14th Mar, 2019 19:35							
SUSHMA_WIN81B	68%	21st Mar, 2019 19:35							
WIN-ANQ3V8P4RSB	0%	-							
WIN8-205-SCCM	77%	14th Mar, 2019 19:35							

Overview Scan Result

☐ Secure ☐ End-Of-Life ☒ Insecure

Export

Name	Version	State	SAID	Criticality	CVSS Base Score	Threat Score	Issued	Vulnerabilities
Microsoft .NET Framework 4.x	4.0.30319.33440	Insecure	SA66386		v2: 7.5	4	1294 days ago	2
Microsoft .NET Framework 4.x	4.0.30319.33440	Insecure	SA66386		v2: 7.5	4	1294 days ago	2
Microsoft .NET Framework 4.x	4.0.30319.33440	Insecure	SA66386		v2: 7.5	4	1294 days ago	2
Microsoft Excel 2016 / O365	16.0.9126.2295	Insecure	SA86648		v3: 8.8	4	104 days ago	6
Microsoft Excel 2016 / O365	16.0.9126.2295	Insecure	SA86648		v3: 8.8	4	104 days ago	6
Microsoft Internet Explorer 11.x	11.0.9600.19036	Insecure	SA87867		v3: 8.8	3	12 days ago	12
Microsoft Internet Explorer 11.x	11.0.9600.19036	Insecure	SA87867		v3: 8.8	3	12 days ago	12
Microsoft Outlook 2016 / O365	16.0.9126.2295	Insecure	SA86648		v3: 8.8	4	104 days ago	6
Microsoft PowerPoint 2016 / ...	16.0.9126.2295	Insecure	SA86648		v3: 8.8	4	104 days ago	6
Microsoft Windows 8.1	Windows 8.1 En...	Insecure	SA86671		v3: 9.8	59	104 days ago	10
Microsoft Word 2016 / O365	16.0.9126.2295	Insecure	SA86262		v3: 8.8	9	132 days ago	11
Mozilla SeaMonkey 2.x	2.32	Insecure	SA84457		v3: 8.8	7	241 days ago	11

Page 1 of 1

Displaying products 1 - 15 of 15

Close

Product Smart Group Threat Score

The **Threat Score** appears for all the products on the **Product Smart Group Result** page.

Software Vulnerability Manager

Menu

- Dashboard
- Scanning
- Results
- Sites (4)
- Host Smart Groups
- Product Smart Groups
 - Overview & Configuration
 - Configured Product Groups (28)
 - All Products (411)
 - 7-Day Critical Vulnerability Compliance (FROM TEMPL)
 - AAG (0)
 - assdas (0)
 - bmd (0)
 - End-Of-Life Products (32)

Smart Group: "All Products" - Last Compiled: 2019-03-29 3:52:26

Showing All Platforms Search

Product Name	Patch Version	SAID	Advisory Descrip...	Criticality	Threat Score	CVSS Base Score	CVSS2 Base Score	CVSS3 Base Score	Vendor
Microsoft Windows 8.1	KB2976897, KB3...	SA83063	Microsoft Windo...		99	v2: 10	10	0	Microsoft
Microsoft Windows 10	KB4485449, KB4...	SA87897	Microsoft Windo...		88	v3: 8.8	0	8.8	Microsoft
Microsoft .NET Framework 3.x	KB4041092, KB4...	SA78904	Microsoft .NET F...		62	v2: 10	10	0	Microsoft
Microsoft .NET Framework 4.x	KB3074228, KB4...	SA78904	Microsoft .NET F...		62	v2: 10	10	0	Microsoft
Microsoft Internet Explorer 11.x	KB4480963, KB4...	SA86719	Microsoft Intern...		52	v3: 8.8	0	8.8	Microsoft
Mozilla Thunderbird 60.x	60.5.1	SA88057	Mozilla Thunder...		17	v3: 8.8	0	8.8	Mozilla Foundati...
Dnsmaq 2.x		SA79195	Red Hat update...		16	v2: 8.3	8.3	0	
Libxml2		SA71295	Red Hat update...		12	v2: 10	10	0	
Apple iTunes 12.x	12.9.3	SA87245	Apple iTunes Mu...		12	v3: 8.8	0	8.8	Apple
Microsoft Word 2016 / O365	16.0.9126.2315	SA86262	Microsoft Multipl...		9	v3: 8.8	0	8.8	Microsoft
Mozilla SeaMonkey 2.x	2.49.4	SA84457	Mozilla SeaMonk...		7	v3: 8.8	0	8.8	Mozilla Foundati...
Microsoft .NET Framework 2.x	KB4055271, KB4...	SA84046	Microsoft .NET F...		5	v3: 9.8	0	9.8	Microsoft
JasPer 1.x		SA76863	Red Hat update...		5	v2: 10	10	0	

Smart Group Criteria Threat Score

When creating the **Product Smart Group**, the **Threat Score** option is available for the **Criteria** specification. The result is displayed based on the selection. By default, the **Threat Score Criteria** is set to **70**.

Product Smart Groups: Overview & Configuration

Create New Smart Group | Queue For Compilation

Name	Description	Business Impact	Compilation
7-Day Critical V...			
AAG			
All Products			
assdas			
bmd			
End-Of-Life Pro			
Insecure install			
insecure os			
Insecure Produ			
Insecure_QAWI			
Patched Produc			
PCI Compliance			
qa2-bd-w7x86			
QA2-BD-W81x6			
said create bef			
SAID on March			
silent install			
test at least hi			
Threat Score is			
ThreatScore<7			
win10			

Configure New Smart Group

Smart Group Name: Threat Score

Description: Threat Score Test

Business Impact: Critical

Contains products that match **all** of the following criteria:

Criteria

Threat Score is at least 70

Customize Columns

A Product Smart Group's contents grid will always show the "Product Name" column for each product. Use this form to control which additional columns are shown in the grid view. Mouseover a checkbox for the column description.

☒ Select All ☐ Select Custom

☒ Patch Version ☒ Criticality ☒ Threat Score ☒ CVSS Base Score ☒ Insecure ☒ End-Of-Life ☒ Secure ☒ Total ☒ Affected Hosts ☒ Download ☒ Product Type

Templates Save Close

All Advisory Threat Score

The **Threat Score** is made available in the **All Advisories** page.

Software Vulnerability Manager

Smart Group: "All Advisories" - Last Compiled: 2019-03-29 3:52:30

SAID	Advisory Description	Criticality	Threat Score	Zero-Day	Advisory Published	Vulnerability	Solution Status	CVSS Base Score	CVSS2 Base Score	CVSS3 Base Score	Attack Vector	Impact	Installation
SAB2839	7-zip Memory Corruption Vulnerability	High	2	No	1st Mar, 2018	1	Vendor Patched	v2: 10	10	0	From Remote	System Access	
SAB7905	Adobe Flash Player Information Disclo...	Medium	-	No	12th Feb, 2019	1	Vendor Patched	v3: 4.3	0	4.3	From Remote	Exposure of Sensitive Informati...	
SAB7606	Adobe Reader / Acrobat Information...	Medium	3	No	21st Feb, 2019	1	Vendor Patched	v2: 4.3	0	4.3	From Remote	Exposure of Sensitive Informati...	
SAB8028	Adobe Shockwave Player Memory Corr...	Medium	3	No	14th Nov, 2017	1	Vendor Patched	v2: 10	10	0	From Remote	System Access	
SAB7245	Apple iTunes Multiple Vulnerabilities	High	12	No	25th Jan, 2019	13	Vendor Patched	v3: 8.8	0	8.8	From Remote	Cross Site Scripting, Security By...	
SAB7950	FileZilla FTP Client PuTTY Vulnerability	Medium	-	No	19th Mar, 2019	1	Vendor Patched	v3: 5.6	0	5.6	From Remote	undefined	
SAB5494	Git Arbitrary Command Execution Vul...	High	3	No	8th Oct, 2018	1	Vendor Patched	v3: 7.5	0	7.5	From Remote	System Access	
SAB7946	libssh2 Multiple Vulnerabilities	High	-	No	18th Mar, 2019	4	Vendor Patched	v3: 8.9	0	8.8	From Remote	System Access	
SAB7004	Microsoft .NET Framework Code Exec...	High	62	Yes	12th Sep, 2017	1	Vendor Patched	v2: 10	10	0	From Remote	System Access	
SAB6443	Microsoft .NET Framework Multiple Vu...	High	3	No	11th Dec, 2018	2	Vendor Patched	v2: 9.8	0	9.8	From Remote	Denial of Service, System Access	
SAB7923	Microsoft .NET Framework Multiple Vu...	High	2	No	13th Feb, 2019	2	Vendor Patched	v3: 7.8	0	7.8	From Remote	Security Bypass, System Access	
SAB6496	Microsoft .NET Framework Multiple Vu...	High	5	No	11th Jul, 2018	4	Vendor Patched	v3: 9.8	0	9.8	From Remote	Security Bypass, Privilege Escal...	
SAB6939	Microsoft .NET Framework Security By...	High	-	No	8th Jan, 2019	1	Vendor Patched	v3: 5.3	0	5.3	From Remote	Security Bypass	
SAB6432	Microsoft .NET Framework Signed XM...	High	2	No	8th Mar, 2016	1	Vendor Patched	v2: 1	5	0	From Remote	Security Bypass	
SAB6386	Microsoft .NET Framework Two Vulner...	High	4	No	8th Sep, 2015	2	Vendor Patched	v2: 7.5	7.5	0	From Remote	Security Bypass, Denial of Servi...	
SAB6719	Microsoft Internet Explorer Memory C...	High	52	Yes	20th Dec, 2018	1	Vendor Patched	v3: 8.8	0	8.8	From Remote	System Access	
SAB7867	Microsoft Internet Explorer Multiple V...	High	3	No	12th Mar, 2019	12	Vendor Patched	v3: 8.8	0	8.8	From Remote	Security Bypass, Exposure of Se...	
SAB5499	Microsoft Multiple Products Multiple V...	High	5	No	9th Oct, 2018	5	Vendor Patched	v3: 7.8	0	7.8	From Remote	Exposure of Sensitive Informati...	
SAB6262	Microsoft Multiple Products Multiple V...	High	9	No	13th Nov, 2018	11	Vendor Patched	v3: 8.9	0	8.8	From Remote	Security Bypass, System Access	
SAB6488	Microsoft Multiple Products Multiple V...	High	4	No	11th Dec, 2018	6	Vendor Patched	v3: 8.8	0	8.8	From Remote	Exposure of Sensitive Informati...	
SAB7319	Microsoft Windows Adobe Flash Player...	High	-	No	12th Feb, 2019	1	Vendor Patched	v3: 8.8	0	8.8	From Remote	System Access	
SAB6673	Microsoft Windows Kernel Information...	High	4	No	12th Aug, 2014	3	Vendor Patched	v2: 6.4	6.8	0	From Local System	Exposure of Sensitive Informati...	

All Advisory Smart Group Criteria Threat Score

When creating the **Advisory Smart Group**, the **Threat Score** option is available for the **Criteria** specification. The result is displayed based on the selection. By default, the **Threat Score Criteria** is set to **70**.

Advisory Smart Groups: Overview & Configuration

Create New Smart Group | Queue For Compilation

Name	Description	Business Impact	Compilation	Data Last Compiled	Modified Date	Advisories
Advisory_Threat_ScoreAtle...			Complete	25th Mar, 2019 02:35	14th Mar, 2019 19:18	3
All Advisories	Smart Group containing all Advisories (default Secunia Smart Group)		Complete	25th Mar, 2019 02:35	9th Apr, 2015 16:44	75

Extremely Critical

from remote

high_and_above

local network/system

mmm

ThreatScore<70

Zero-Day

Configure New Smart Group

Smart Group Name: Threat Score

Description: Threat Score

Business Impact: Critical

Contains advisories that match all of the following criteria:

Criteria

Threat Score is at least 70

Customize Columns

An Advisory Smart Group's contents grid will always show the Secunia Advisory ID and Description for each entry. Use this form to control which additional columns are shown in the grid view. Mouseover a checkbox for the column description.

☒ Select All ☐ Select Custom

☒ Criticality ☒ Threat ☒ Zero-Day ☒ Advisory ☒ Vulnerabilities ☒ Solution ☒ CVSS Base ☒ Attack ☒ Impact ☒ Installations ☒ Products ☒ Hosts

Save Close

Zero Day Advisory Threat Score

The Threat Score appears in the **Zero Day Advisories** page. This result may vary with the data seen in the result section. The **All Advisories** page has the latest result as it is directly pulled from the vulnerability track table.

Software Vulnerability Manager						
Zero-Day Advisories						
Scope of Data: <input checked="" type="radio"/> Advisories that Affected You <input type="radio"/> All Advisories						
Zero-Day SAID	Advisory Description	Criticality	Advisory Published	Threat Score	Vulnerability	Affected Installations
SA87744	Google Chrome FileReader Use-After-Free Vulnerability		4th Mar, 2019	18	1	3
SA86719	Microsoft Internet Explorer Memory Corruption Vulnerability		20th Dec, 2018	52	1	32
SA86517	Adobe Flash Player Multiple Vulnerabilities		5th Dec, 2018	95	2	3
SA85519	Microsoft Windows Server 2008 / Windows 7 Multiple Vulnerabilities		9th Oct, 2018	23	14	1
SA85518	Microsoft Windows Server 2012 / Windows RT 8.1 / 8.1 Multiple Vulnerabilities		9th Oct, 2018	23	15	1
SA85514	Microsoft Windows Server 2016 / Windows 10 Multiple Vulnerabilities		9th Oct, 2018	23	22	3
SA84665	Microsoft Internet Explorer Multiple Vulnerabilities		14th Aug, 2018	67	11	32
SA83644	Adobe Flash Player Multiple Vulnerabilities		7th Jun, 2018	60	4	2
SA81412	Adobe Flash Player Multiple Use-After-Free Vulnerabilities		1st Feb, 2018	99	2	2
SA79397	Microsoft .NET Framework Code Execution Vulnerability		10th Oct, 2017	53	1	1
SA78904	Microsoft .NET Framework Code Execution Vulnerability		12th Sep, 2017	93	1	53
SA76734	Microsoft Windows 7 Multiple Vulnerabilities		9th May, 2017	70	27	1
SA76722	Microsoft Windows Server 2012 Multiple Vulnerabilities		9th May, 2017	70	26	1
SA76703	Microsoft Office Multiple Products Multiple Vulnerabilities		9th May, 2017	62	6	1
SA76672	Microsoft Internet Explorer Multiple Vulnerabilities		9th May, 2017	20	6	32
SA76271	Microsoft Office Multiple Vulnerabilities		10th Apr, 2017	99	8	2
SA76226	Microsoft Internet Explorer Multiple Vulnerabilities		11th Apr, 2017	5	3	32
SA75547	Microsoft Internet Explorer Multiple Vulnerabilities		24th Feb, 2017	70	12	32
SA73948	Mozilla Firefox / Firefox ESR SVG Animation Use-After-Free Vulnerability		30th Nov, 2016	17	1	8
SA72985	Microsoft Multiple Products RTF Memory Corruption Vulnerability		11th Oct, 2016	52	1	1
SA72977	Microsoft Products Multiple Vulnerabilities		11th Oct, 2016	7	8	87
SA72953	Microsoft Internet Explorer Multiple Vulnerabilities		11th Oct, 2016	66	10	32
SA72380	Microsoft Internet Explorer Multiple Vulnerabilities		13th Sep, 2016	65	10	32
SA70398	Microsoft Internet Explorer Multiple Vulnerabilities		10th May, 2016	99	5	32
SA69989	Microsoft Windows Privilege Escalation and Pool Corruption Multiple Vulnerabilities		12th Apr, 2016	20	4	16
SA67695	Microsoft Windows Multiple Privilege Escalation Vulnerabilities		8th Dec, 2015	5	4	16
SA67666	Microsoft Office Multiple Products Multiple Vulnerabilities		8th Dec, 2015	8	6	1
SA66378	Microsoft Office Multiple Products Multiple Vulnerabilities		8th Sep, 2015	61	7	2
SA66360	Microsoft Multiple Products Multiple Vulnerabilities		8th Sep, 2015	23	11	17

Flexera Package System (SPS) List Threat Score

The Threat Score appears in the Flexera Package System (SPS) list, which helps user to prioritize patches.

Software Vulnerability Manager

Menu

Dashboard

Scanning

Results

Reporting

Patching

Flexera Package System (SPS)

Patch Template

Agent Deployment

WSUS / System Center

Available

Flexera Package System (SPS)

Search Type: Product

Search text ...

Search

View from the context of Smart Group: All Products

Configure View

New Custom Package

Product	Vendor	Patched Version	Architecture	SAID	Criticality	Threat Score	Detected
Product: Mozilla Thunderbird 60.x (1 Item)							
Mozilla Thunderbird 60.x	Mozilla Foundation	60.5.1	Windows32-bit	SA88057	<div><div></div><div></div><div></div><div></div><div></div></div>	17	0 days, 0 hours...
Product: Apple iTunes 12.x (1 Item)							
Apple iTunes 12.x	Apple	12.9.3	Windows32-bit	SA87245	<div><div></div><div></div><div></div><div></div><div></div></div>	12	0 days, 0 hours...
Product: Mozilla SeaMonkey 2.x (1 Item)							
Mozilla SeaMonkey 2.x	Mozilla Foundation	2.49.4	Windows32-bit	SA84457	<div><div></div><div></div><div></div><div></div><div></div></div>	7	0 days, 0 hours...
Product: Adobe Shockwave Player 12.x (1 Item)							
Adobe Shockwave Player 12.x	Adobe Systems	12.3.1.201	Windows32-bit	SA80028	<div><div></div><div></div><div></div><div></div><div></div></div>	3	0 days, 0 hours...
Product: 7-zip 18.x (1 Item)							
7-zip 18.x		18.05	Windows64-bit	SA82839	<div><div></div><div></div><div></div><div></div><div></div></div>	2	0 days, 0 hours...

