Flexera

Software Vulnerability Manager (On-Premises Edition)

User Guide

Legal Information

Book Name: Software Vulnerability Manager (On-Premises Edition) User Guide

Part Number: SVMOPE-December2021-UG00

Product Release Date: December 2021

Copyright Notice

Copyright © 2021 Flexera

This publication contains proprietary and confidential information and creative works owned by Flexera and its licensors, if any. Any use, copying, publication, distribution, display, modification, or transmission of such publication in whole or in part in any form or by any means without the prior express written permission of Flexera is strictly prohibited. Except where expressly provided by Flexera in writing, possession of this publication shall not be construed to confer any license or rights under any Flexera intellectual property rights, whether by estoppel, implication, or otherwise.

All copies of the technology and related information, if allowed by Flexera, must display this notice of copyright and ownership in full.

Intellectual Property

For a list of trademarks and patents that are owned by Flexera, see https://www.flexera.com/legal/intellectual-property.html. All other brand and product names mentioned in Flexera products, product documentation, and marketing materials are the trademarks and registered trademarks of their respective owners.

Restricted Rights Legend

The Software is commercial computer software. If the user or licensee of the Software is an agency, department, or other entity of the United States Government, the use, duplication, reproduction, release, modification, disclosure, or transfer of the Software, or any related documentation of any kind, including technical data and manuals, is restricted by a license agreement or by the terms of this Agreement in accordance with Federal Acquisition Regulation 12.212 for civilian purposes and Defense Federal Acquisition Regulation Supplement 227.7202 for military purposes. The Software was developed fully at private expense. All other use is prohibited.

Contents

1 Software Vulnerability Manager (On-Premises Edition) Help Library 11

Product Support Resources 15

Contact Us 16

2 Introduction 17

The Scan Process – How Does it Work? 17

Software Vulnerability Manager Software Vulnerability Management Life Cycle 18

System Requirements 19

Permissions 20

Software Vulnerability Manager Console and WSUS Compatibility 20

Software Vulnerability Manager with Scanning and Patching Capabilities 22

System Architecture Overview 23

3 Getting Started with Software Vulnerability Manager On-Premises Edition 25

Install Your Software Vulnerability Manager On-Premises Edition Environment 25

Logging on to Software Vulnerability Manager On-Premises Edition 26

Logging on to Software Vulnerability Manager On-Premises Edition Using Single Sign-On 26

Opening a Support Case 28

Download and Install the Software Vulnerability Manager Plug-in 28

Download and Install the Software Vulnerability Manager Daemon 28

Configuring SCCM to Report Windows Update Information 31

Download and Install the Software Vulnerability Manager System Center Plug-in 33

Download and Install the Software Vulnerability Manager Patch Publisher 33

SVM Patch Publisher 34

Working with SVM Patch Publisher Interface 35

Toolbar in the SVM Patch Publisher 35

Output/Progress windows in the SVM Patch Publisher 36

SVM Connection Settings 36

Distribution Systems . . . 38
Adding a New Distribution Connection . . . 38
Adding Windows Server Update Services (WSUS) Connection . . . 38
Adding Microsoft Intune Connection . . . 39
Adding VMWare Workspace ONE Connection . . . 40
Deleting an Existing Distribution Connection . . . 43
Download and Install the Software Vulnerability Manager Client ToolKit . . . 43
Flexera SVM Patch Configuration . . . 45
Flexera WSUS Management Tool . . . 50
Patching Information . . . 51
Configuration . . . 54
Flexera SVM Client Data Tool . . . 55
Create Database Connection . . . 56
Add Account . . . 58
Sync Data . . . 58
Schedule Automation for Sync data . . . 60
Generating Data Trend Reports . . . 63
Join Flexera's Customer Community . . . 67

4 The Dashboard . . . 69

5 Agent Administrative Privileges and Data Collection . . . 71
Agent Administrative Privileges . . . 71
Agent Data Collection . . . 72
Agent Caching of Scan Rules . . . 73

6 Scanning . . . 75
Agent-Based Scan – Requirements for Windows . . . 76
Agent-Based Scan – Requirements for Mac OS X . . . 77
Agent-Based Scan – Requirements for Red Hat Enterprise Linux (RHEL) . . . 77
Remote/Agent-less Scan – Requirements (Windows) . . . 78
Remote Scanning Via Software Vulnerability Manager (Agent-less Scan) . . . 79
Quick Scan . . . 79
Scan Groups . . . 80
Scan Progress . . . 81
System Center Inventory Import . . . 81
System Center Import Schedules (Requires the Software Vulnerability Manager Daemon) . . . 83
Remote Scanning Via Agents . . . 83
Software Vulnerability Manager Agent Command Line Options . . . 84
Help . . . 84
Version . . . 84
Install . . . 84
Install the Agent via SCCM . . . 85
Uninstall . . . 86

Modify Settings. . . . 87
Controlling the Service . . . 87
Scanning from the Command Line . . . 87
Randomizing the Agent Scan Schedule . . . 87
Agent Configuration Options . . . 88
Network Appliance Agents . . . 93
Network Appliance Groups . . . 93
Download Network Agent . . . 93
Scanning Via Local Agents . . . 94
Scan Types . . . 95
Single Host Agents. . . . 95
Download Local Agent . . . 98
Run Scan from System Center Configuration Manager (SCCM) . . . 101
Scanning Mac OS X . . . 105
Download the Software Vulnerability Manager Agent for Apple Mac OS X. . . . 105
Prepare Your Mac. . . . 106
Install the Mac Agent. . . . 107
Scanning Red Hat Enterprise Linux (RHEL) . . . 108
Installing the Software Vulnerability Manager Agent for Red Hat Linux . . . 108
Filter Scan Results . . . 109
Scan Paths. . . . 109
Custom Scan Rules . . . 110
Completed Scans . . . 111

7 Results. . . . 115

Sites . . . 115
Smart Groups . . . 115
Host Smart Groups. . . . 117
Create a New Host Smart Group . . . 117
Overview and Configuration . . . 119
Configured Host Smart Groups . . . 120
Filter Host Smart Groups on missing Microsoft Knowledge Base (KB) articles . . . 121
Filter Host Smart Groups on Operating System Build Version . . . 122
Product Smart Groups. . . . 123
Create a New Product Smart Group . . . 123
Overview and Configuration . . . 127
Last Scan Date for Product Smart Groups . . . 127
Configured Product Smart Groups . . . 128
Filter Product Smart Groups on Operating System Build Version . . . 129
Advisory Smart Groups . . . 130
Overview and Configuration . . . 130
View/Edit Smart Group Configuration . . . 131
Configured Advisory Smart Groups . . . 131
View All Advisories . . . 132

8 Reporting ... 133

Report Configuration ... 133

Smart Group Notifications ... 137

Activity Log Notifications ... 139

Database Access ... 140

Database Console ... 141

Database Cleanup ... 142

Scheduled Exports ... 142

9 Patching ... 145

Flexera Package System (SPS) ... 145

Flexera SPS Page Features ... 146

Product display criteria for SPS ... 146

Language selection for SPS ... 147

Patch update searches by Common Vulnerabilities and Exposures (CVE) ... 148

Advisory Published date ... 148

SPS Concepts and Terminology ... 148

What does a SPS package consist of? ... 149

Applicability Rules ... 149

SPS Package ... 149

Execution Flow Script ... 150

Files ... 150

Creating a Patch with the Flexera Package System (SPS) ... 150

Create an Update Package ... 151

Create an Uninstall Package ... 151

Create a Custom Package ... 152

The SPS Package Creation Wizard ... 152

Step 1 of 4: Package Configuration ... 153

Step 2 of 4: Package Contents ... 154

Step 3 of 4: Applicability Criteria - Paths ... 155

Importing Bulk File Paths in the SPS Package Creation Wizard ... 156

Step 4 of 4: Applicability Criteria - Rules ... 158

Vendor Patch Module ... 159

Vendor Patch Module Page Features ... 159

Product display criteria for Vendor Patch Module ... 160

Patch update searches by Common Vulnerabilities and Exposures ... 162

Advisory Published date in Vendor Patch Module ... 163

Threat Score in Vendor Patch Module ... 163

Creating a Patch with the Vendor Patch Module ... 163

Create an Update Package ... 164

View Installations ... 164

Patch Information ... 165

Package Creation Wizard in Vendor Patch Module ... 166

Step 1 of 4: Package Configuration ... 166

Step 2 of 4: Package Contents ... 167

Step 3 of 4: Applicability Criteria - Paths . . . 168
Step 4 of 4: Applicability Criteria - Rules . . . 169
Automating Patch Deployment . . . 171
Subscribe to Package . . . 171
Edit Subscription . . . 173
Agent Deployment . . . 174
Add Proxy Settings . . . 176
WSUS/System Center . . . 177
Available . . . 177
Deployment . . . 178
Creating the WSUS-CSI GPO Manually . . . 178
Deploying the Update Package Using WSUS . . . 183
Deploying the Update Package Using System Center . . . 184
Integrate SVM with WSUS/SCCM and Deploy a Patch . . . 184
Patch Configuration . . . 187
External Package Signing . . . 187
WSUS/System Center . . . 188
Step 1 – Connection Status . . . 189
Step 2 - Certificate Status . . . 190
Step 3 – Group Policy Status . . . 192
Setting Up Clients to Access WSUS . . . 193
Third-Party Integration . . . 194
Create and Publish the Package . . . 194
Patch Template . . . 195
QuickPatch . . . 200
Patch Automation . . . 201
External Package Signing for Software Vulnerability Manager Client Toolkit . . . 205
Intune Publishing . . . 207
Set up a Distribution Connection in Flexera SVM Patch Configuration for Microsoft Intune . . . 208
App Registration . . . 208
Create Client Secret . . . 211
API Permissions . . . 211
Assignment Groups . . . 214
Workspace ONE Publishing . . . 215
Set up a Distribution Connection in Flexera SVM Patch Configuration for Workspace ONE . . . 215
Basic or Certificate Authentication Type . . . 216
Create Tenant ID / API Key . . . 220

10 Administration . . . 223

Roles . . . 223
User Management . . . 225
Create a New Administrator . . . 225
Create a New User . . . 225
Active Directory (Requires the Software Vulnerability Manager Plug-in) . . . 227

IP Access Management (Requires the Software Vulnerability Manager Plug-in) . . . 228
Password Policy Configuration . . . 229

11 Configuration . . . 231
Settings . . . 231
Scan Threads . . . 232
Live Updates . . . 232
Collect Network Information . . . 232
Zombie File Settings . . . 233
Check for Missing Microsoft Security Update Settings . . . 233
Flexera Software Package System (SPS) Timestamp . . . 233
Mask paths that show user names . . . 234
Configure Agent's Status Polling . . . 234
Java Assessment Settings . . . 235
Default Recipient Settings . . . 235
Windows Update Settings . . . 235
Single Sign-On (SSO) Settings . . . 237
Configure Single Sign-On (SSO) . . . 238
Configure Single Sign-On (SSO) with Azure . . . 245
Create an Enterprise Application . . . 245
Assign Users to the Enterprise Application . . . 247
Set up Single Sign-On (SSO) in Azure . . . 249
Log Messages . . . 253
Activity Log . . . 253
Suggest Software . . . 255
Security . . . 256
Change Password . . . 256
Password Recovery Settings . . . 256

A Appendix A - Software Vulnerability Manager Partition Management . . . 259
Introduction . . . 259
Partition Management . . . 259
Overview . . . 260
Permissions . . . 261
Host and User Licenses . . . 261
Create a New Partition Administrator . . . 261
Grant User Access to all Completed Scans and Single Host Agent Entries . . . 263

B Appendix B - About Secunia Advisories . . . 265
CVSS (Common Vulnerability Scoring System) . . . 265
CVE References . . . 266
Where (Attack Vector) . . . 266
Criticality (Severity Rating) . . . 266
Impact (Consequence) . . . 267

C Appendix C - CSV Export File Cross-References 269
Host Smart Group 270
Advisory Smart Group 270
Product Smart Group 271
Scan Result 271
Completed Scan 272
Scheduled Exports 272
Single Host Agent 273
Smart Group Notifications 273
User Management 274

D Appendix D - Threat Intelligence 275
Evidence of Exploitation 276
Criteria for the Threat Score Calculation 276
Threat Score Calculation - Examples 278
Threat Intelligence Data for Operations and Security 280
Threat Score Locations 280
Dashboard Threat Score 281
Completed Scan Page Threat Score 281
All Advisory Popup Threat Score 282
All Installation Popup Threat Score 283
Advisory Summary Threat Score 284
Host Smart Group Threat Score 285
Product Smart Group Threat Score 286
Smart Group Criteria Threat Score 286
All Advisory Threat Score 287
All Advisory Smart Group Criteria Threat Score 287
Zero Day Advisory Threat Score 288
Flexera Package System (SPS) List Threat Score 289

E Appendix E - Optimization Features 293
Web 293
No scan option 293
Increase Smart Group worker threads for on-Prem customers 294
Changing scan result as completed (status 4) for old incomplete scans 294
Agent 295
Agent scan randomization during agent deployment 295
Stop status API polling 295
Add timeout for Windows Update Agent (WUA) calls 295
Agent now supports recovery settings 295
Support Type 1 scanning for SCCM imports 296
Detect missing security updates from Microsoft System Center 296
Good to know options 296

Restarting the Smart Group Daemon Resets the In-Progress State. . . . 296
Flexera Software Package System (SPS) Timestamp . . . 297
Include --delete-all-settings for Mac agents . . . 297
Support Type 1 Scanning for SCCM Imports . . . 297
Thread Priority for Agent . . . 297
Live Update for Microsoft Products . . . 297
To skip submitting scan frequency . . . 298

F Appendix F - Troubleshooting Techniques . . . 311

Intune . . . 311
Pre-requisites . . . 311
Publishing . . . 312
SVM Patch Configuration . . . 313
SVM Patch Configuration / General Tab . . . 313
Troubleshooting Tips . . . 314
FAQs . . . 315

Patch Daemon . . . 316
Pre-requisites . . . 316
Publishing a Package from Patch Daemon without Local Administrator Rights . . . 316

1

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: • 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	Provides details of how to perform the following tasks: ● Install Your Software Vulnerability Manager On-Premises Edition Environment ● Logging on to Software Vulnerability Manager On-Premises Edition ● 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 Patch Publisher ● Download and Install the Software Vulnerability Manager Client ToolKit ● Join Flexera's Customer Community
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.
Agent Administrative Privileges and Data Collection	Provides details on the following: ● Agent Administrative Privileges ● Agent Data Collection ● Agent Caching of Scan Rules

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

Topic	Content
Scanning	Provides details on the following: ● 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	Provides details on the following: ● Sites ● Smart Groups ● Host Smart Groups ● Product Smart Groups ● Advisory Smart Groups
Reporting	Provides details on the following: ● Report Configuration ● Smart Group Notifications ● Activity Log Notifications ● Database Access ● Scheduled Exports

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

Topic	Content
Patching	Provides details on the following: ● 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 ● Integrate SVM with WSUS/SCCM and Deploy a Patch ● Patch Configuration ● Patch Template ● QuickPatch ● Patch Automation ● Intune Publishing ● Workspace ONE Publishing
Administration	Provides details on the following: ● 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	Provides details on the following: ● Settings ● Log Messages ● Activity Log ● Suggest Software ● Security

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

Topic	Content
Appendix A - Software Vulnerability Manager Partition Management	Provides an Introduction and details of Partition Management.
Appendix B - About Secunia Advisories	Explains Secunia Advisory terminology for: • 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.
Appendix E - Optimization Features	Explains Optimization Features for: • Web • Agent • Good to know options
Appendix F - Troubleshooting Techniques	This appendix explains the troubleshooting techniques of the Software Vulnerability Manager.

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

2

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.

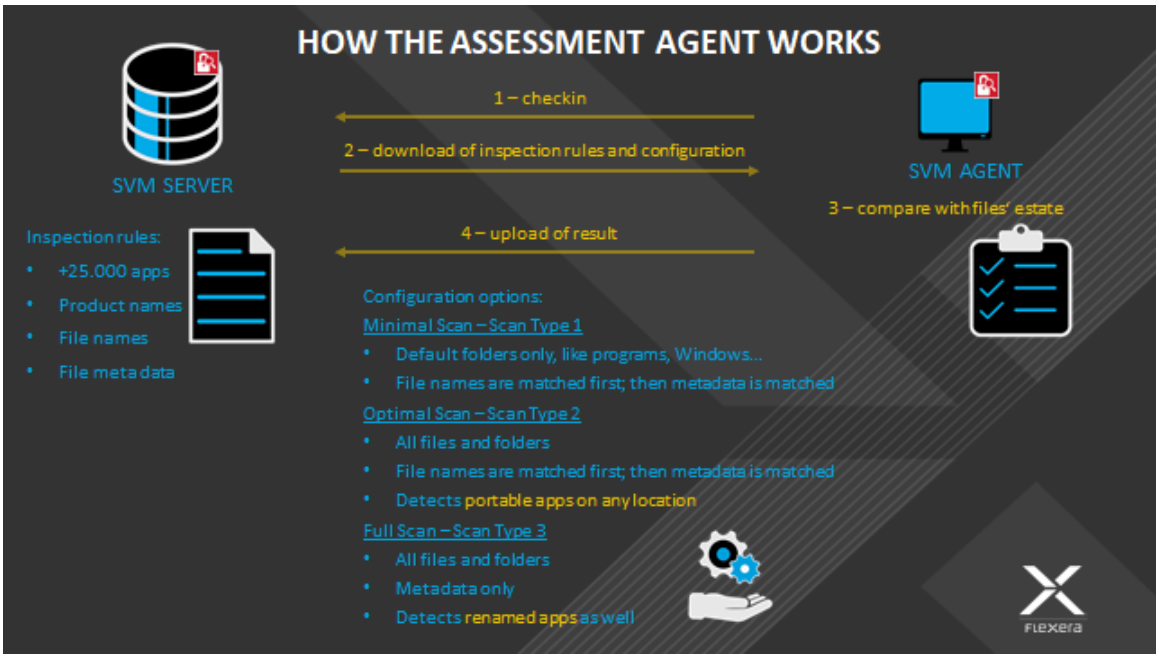
Since the scan process works by looking at the actual files on the system being scanned, the result is extremely reliable as a product cannot be installed on a system without the actual files required being present.

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.

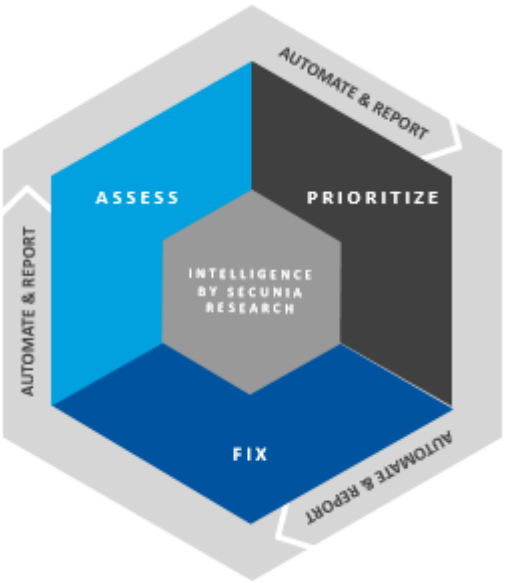


Software Vulnerability Manager Software Vulnerability Management Life Cycle

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 `http(s)://csi_server_name/`.
Sites to Whitelist	You are required to allow-list the following sites: • The `http(s)://csi_server_name/` should be allow-listed in the Firewall/ Proxy configuration. • https://sync.secunia.com should be allow-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: • 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

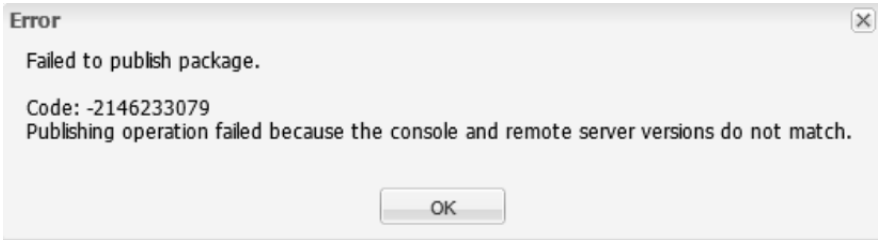
Permissions

The following permissions should be present:

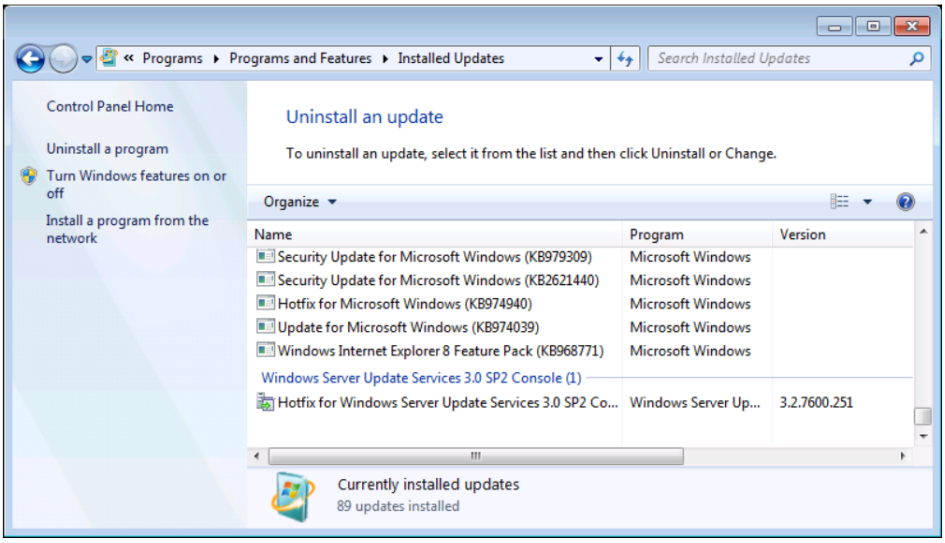
- Connect and Select permissions to the user (or service account) at the SQL Server Host of your System Center database. See Download and Install the Software Vulnerability Manager Daemon.
- WSUS Administrator Group privileges (located locally on your WSUS Server)
- (Optional) Domain Administrator privileges 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 1.2** is 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.

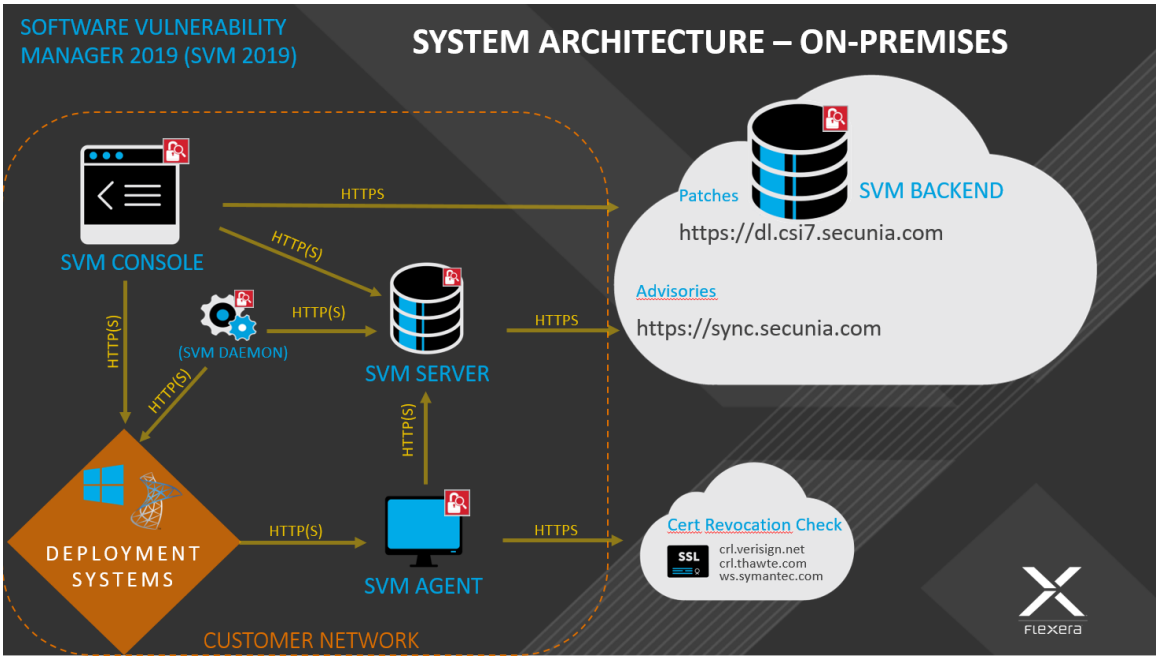


Figure 2-1: Software Vulnerability Manager System Architecture - On-Premises

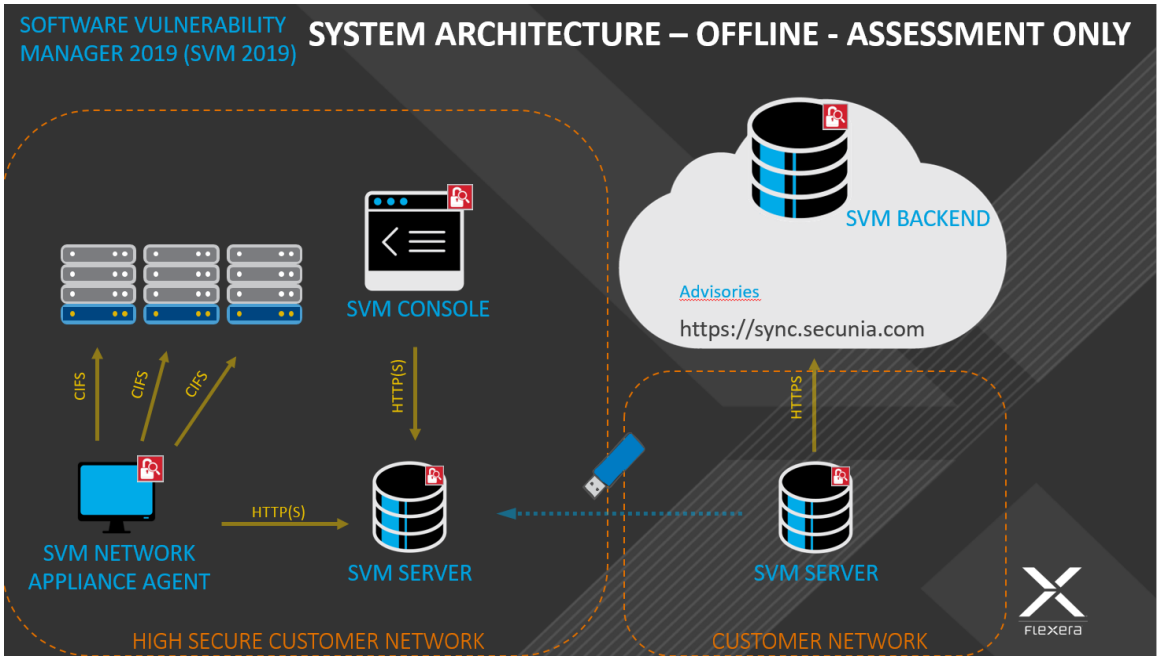


Figure 2-2: Software Vulnerability Manager System Architecture - Offline - Assessment Only

3

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
- Logging on to Software Vulnerability Manager On-Premises Edition
- 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 Patch Publisher
- 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.*

Logging on to Software Vulnerability Manager On-Premises Edition

On the login page of Software Vulnerability Manager, you will be prompted for authentication with your user name/password. Please use the credentials supplied by Flexera personnel. The initial password issued by Flexera is a one-time only password that must be changed upon the first login. 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 Recovery Settings, so that you can recover the Root Admin password without having to open a support case to have the password reset.*

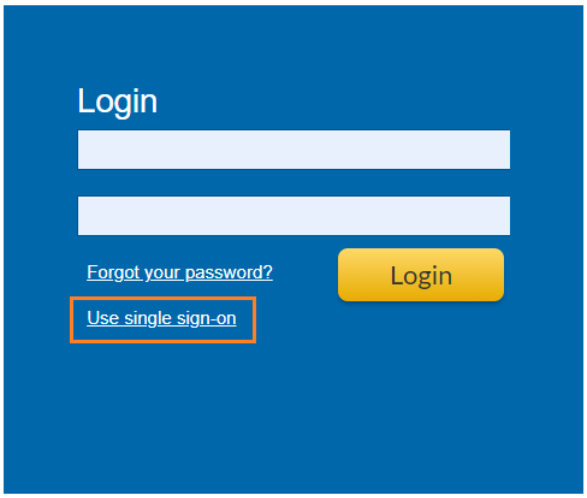
Important • *For security purposes, Software Vulnerability Manager has a session timeout that will log you off after 2 hours of inactivity.*

Logging on to Software Vulnerability Manager On-Premises Edition Using Single Sign-On

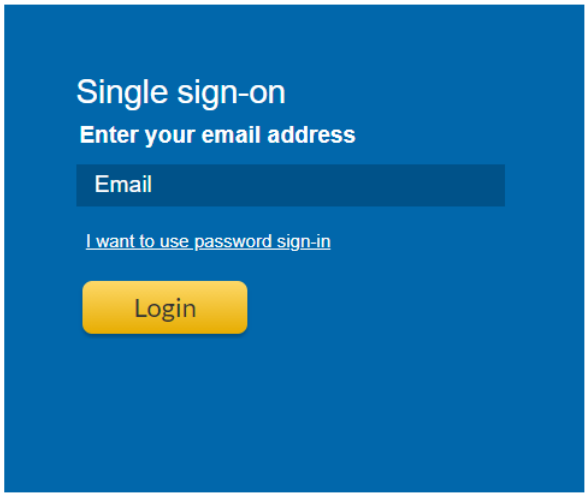
Perform the following steps to login to Software Vulnerability Manager using single sign-on for Azure SSO or Okta users.

Task ***To login to Software Vulnerability Manager using single sign-on:***

1. On the Login page, click **Use Single Sign-On**.



The **Single sign-on** login page prompts for authentication with your single sign-on email address.



2. Enter a valid email address and click **Login**.

   Once logged in, the Identity Provider page prompts for authentication with your user name/password.

3. Enter your valid user name and password, and then click **Sign In**.

   Upon successful login, Software Vulnerability Manager is accessible.

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

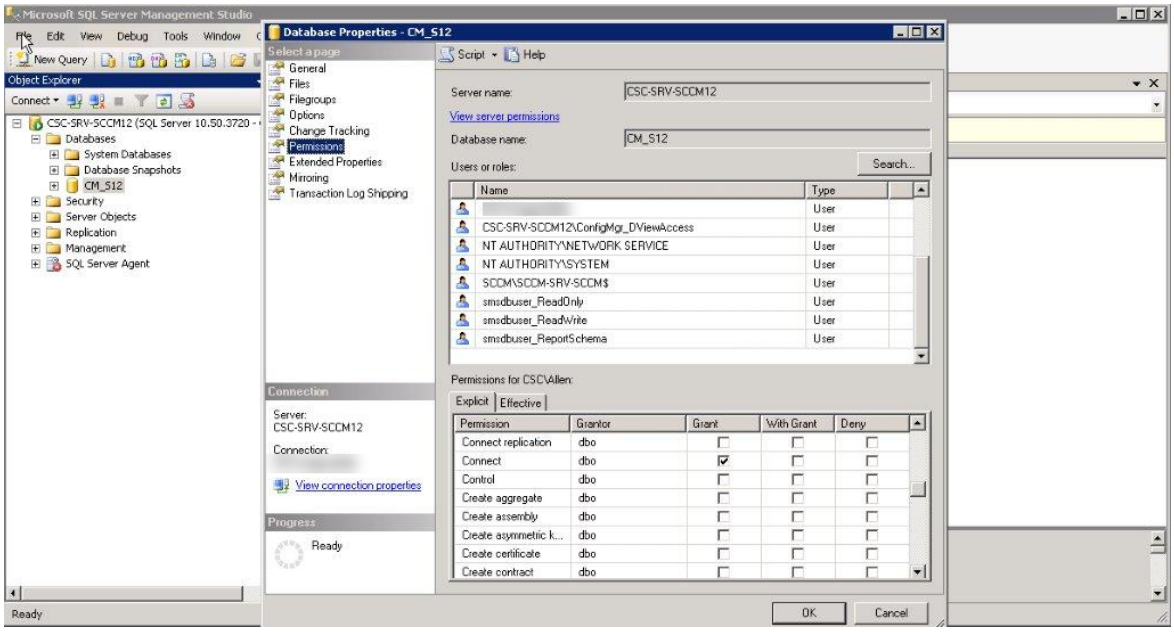
To assign Connect and Select permissions to the user (or service account) that will be used to run the Daemon service, perform the following steps.

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.

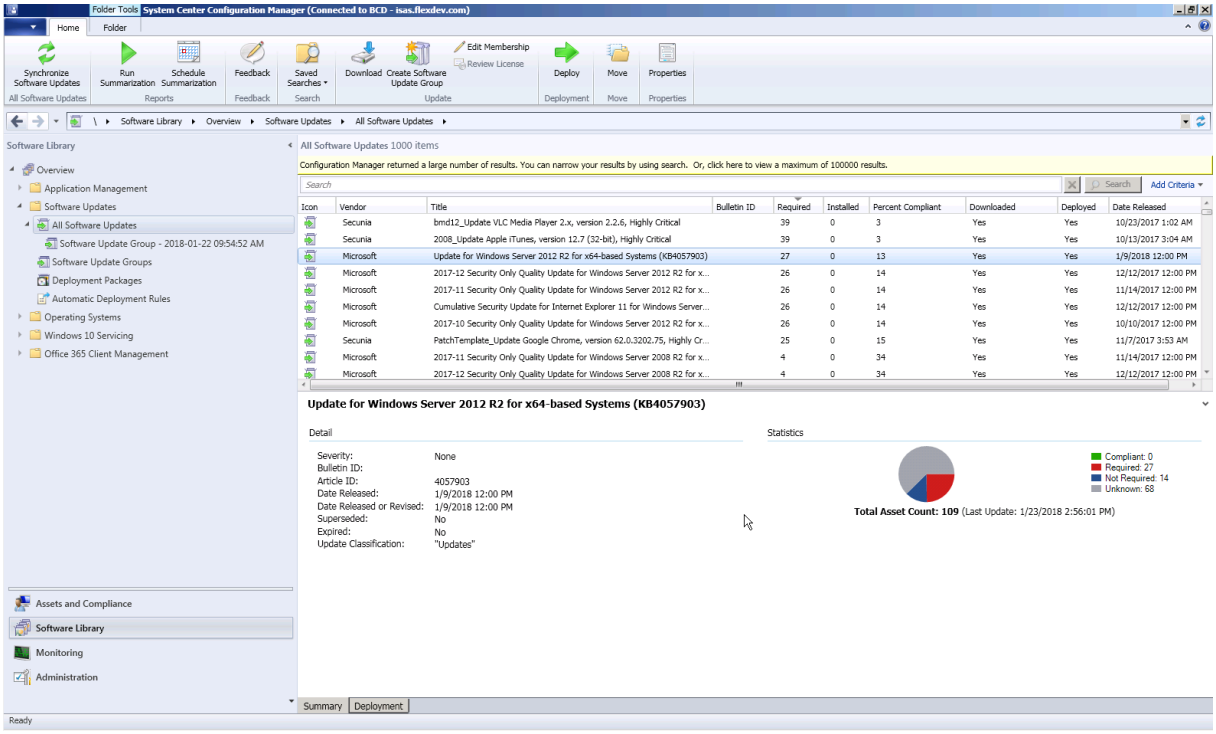
The Daemon uses the System Center SQL Database Settings that are specified in the Configure dialog. If those settings haven't yet been specified when the Daemon has been run then it will check for them again in 10 minutes and every 10 minutes afterwards until it gets them.

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:



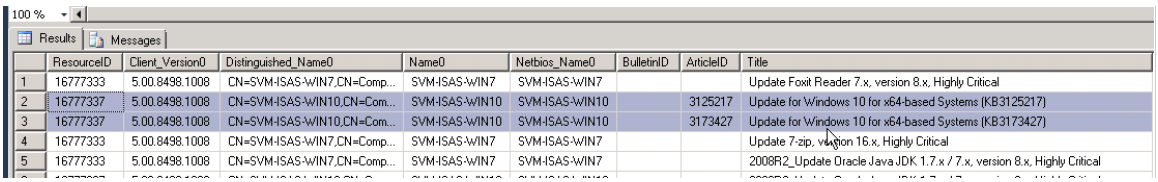
You want to make sure that the Windows updates have the following results:

- "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.

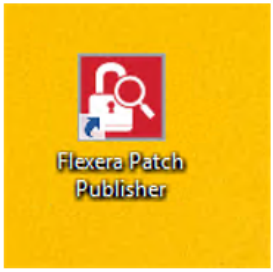
Login with your Software Vulnerability Manager Account credentials (User name/Password).

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

Download and Install the Software Vulnerability Manager Patch Publisher

To ease SVM Patch Publisher, you must download and install Software Vulnerability Manager Patch Publisher ToolKit. To download this tool kit click here.

Upon installing the new tool, the Flexera Patch Publisher shortcut will be created on the desktop to launch the tool.



Prerequisites

The below prerequisites required to install Patch Publisher:

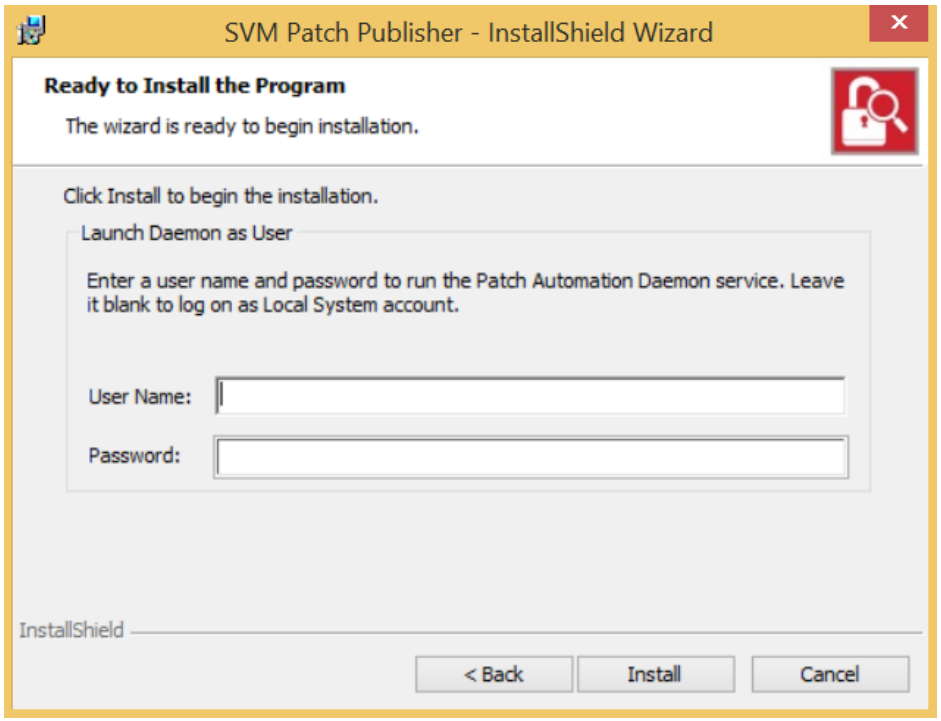
- OS Windows 8 or later
- Windows 2012 R2 or later
- .Net framework version 4.7.2 or later
- RSAT should be enable and needs to be installed
- Architecture - 64 bit operating systems
- You can install in Local admin/domian admin

Download and Install the SVM Patch Publisher

To download and install the SVM Patch Publisher perform the following steps.

Task ***To Download and install:***

1. Download the Software Vulnerability Manager Patch Publisher from the SVM Patch Publisher Tool Kit.
2. Double click the set up file, you will be prompted to enter credentials. Click Install.



Tip • *On successful installation, one shortcut for Software Vulnerability Manager Patch Publisher will get created in your desktop.*

3. On successful installation, click Finish. SVM Patch Publisher windows pane appears. For more information, see SVM Patch Publisher.

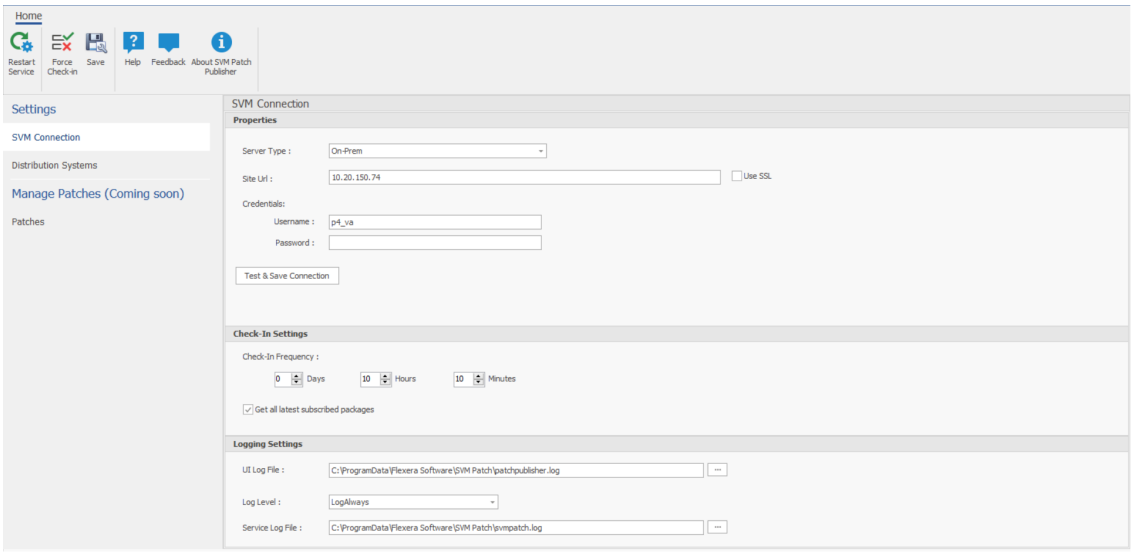
Note • *If you are migrating Patch Daemon to SVM Patch Publisher, make sure that the SVM Test connections and Distribution Connections are* ***Test & Saved****.*

SVM Patch Publisher

SVM Patch Publisher inherits its current functionalities from the Patch Daemon. SVM Patch Publisher enables you to configure connections to the SVM server and to the supported end point management systems. The tool polls SVM on a configured frequency to look for new patches resulting either from a manual publish or Patch Automation to publish patches to the specified end point management system.

The following section describes how to access the Patch Publisher.

- Working with SVM Patch Publisher Interface
- SVM Connection Settings
- Distribution Systems



Working with SVM Patch Publisher Interface

The SVM Patch Publisher interface has various UI elements. This section includes topics that explain how to perform basic tasks and the use of these elements.

- Toolbar in the SVM Patch Publisher
- Output/Progress windows in the SVM Patch Publisher

Toolbar in the SVM Patch Publisher

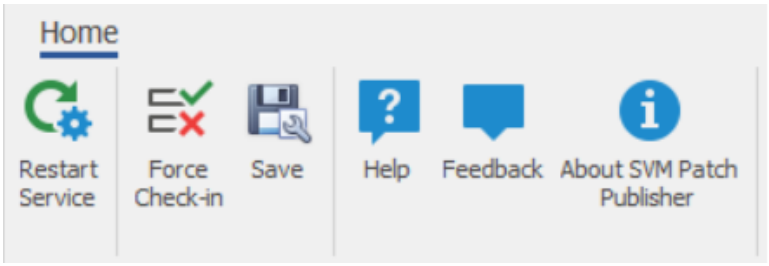
The SVM Patch Publisher has the following ribbon buttons:

Table 3-1 • SVM Patch Publisher / Ribbon Buttons

Buttons	Description
Restart Service	Click to restart the daemon service for the changes to take effect. Upon clicking this button, the state of the service is checked.
Fore Check-In	Click and the pull the subscribed packages without waiting for the schedule time from the server for the Daemon service to execute.
Save	Click to save the changes to the settings file.
Help	Click to open the SVM help library.

Table 3-1 • SVM Patch Publisher / Ribbon Buttons

Buttons	Description
Feedback	Used to provide ideas and / or suggestions.
About SVM Patch Publisher	Click to launch the SVM Patch Publisher window and view the information about the tool.



Output/Progress windows in the SVM Patch Publisher

When you perform any tasks like save, force check-in, and restart service on subscribed packages, the Output Window appears at the bottom of the interface.

- Lists the Errors, Warnings, and other log messages that are generated while perform a task on subscribed package.
- Displays logs while performing functional testing of the subscribed package.

SVM Connection Settings

You can configure connections to the SVM server to the supported end point management systems. Perform the following steps to configure the SVM connections.

Task ***To configure SVM connection:***

1. On **Settings** menu, click **SVM Connection** in the left pane.

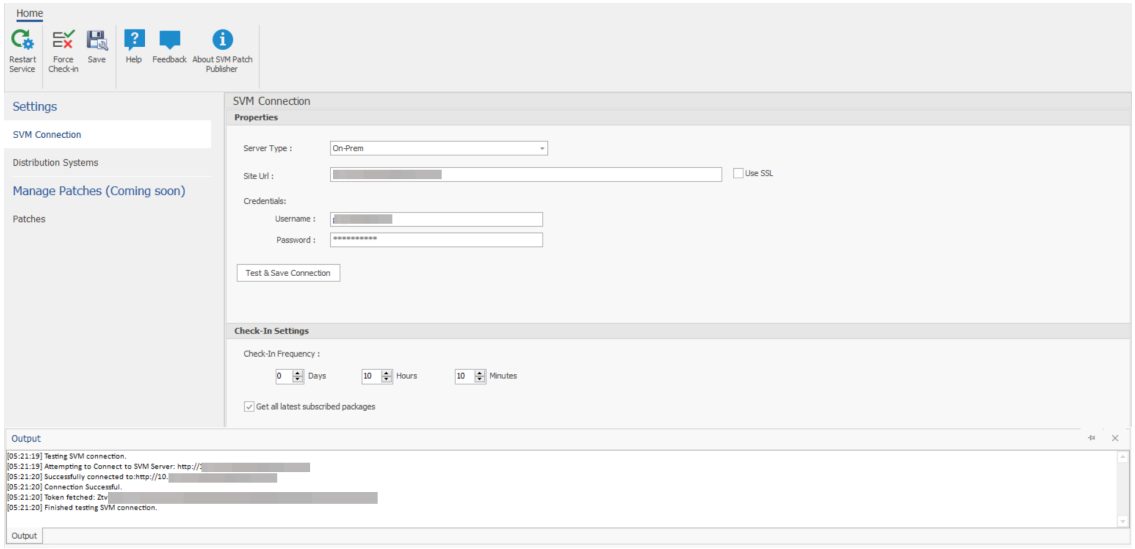
   The **SVM Connection** page appears.

2. To configure the SVM connection, enter the following information:

Field	Description
Server Type	Select one of the following Server Type: • Cloud • On-Prem
Site URL	Enter the URL for SVM Connection.

Field	Description
Use SSL	Select the Use SSL Connection check box if your SVM Connection is configured to accept SSL connections.
Credentials	Enter valid User Name and Password for the specific site url.
Check-In Settings	Set the frequencies to pull the relevant packages from the server.
Get all latest subscribed packages	Select if you want to get latest subscribed packages.
Log Level	Set one of the Log levels: ● LogAlways ● Critical ● Error ● Warning ● Informational ● Verbose
Log File	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`
Test & Save Connection	Click to test to see if the settings that you entered can be used to successfully connect to this SVM server.

3. On successful connection you will receive a Token in the **Output** window.



4. Click **Restart Service** ribbon for the change to take effect.

Distribution Systems

In Distribution Systems, you can configure multiple distribution connections.

This section includes the following topics:

- Adding a New Distribution Connection
- Deleting an Existing Distribution Connection

Adding a New Distribution Connection

You can add connections for the following Distribution Systems.

- Adding Windows Server Update Services (WSUS) Connection
- Adding Microsoft Intune Connection
- Adding VMWare Workspace ONE Connection

Adding Windows Server Update Services (WSUS) Connection

To add Windows Server Update Services (WSUS) connection, perform the following steps.

Task ***To add WSUS connection:***

1. On **Settings** menu, click **Distribution Systems** in the left pane.

   The **Distribution Systems** pane appears.

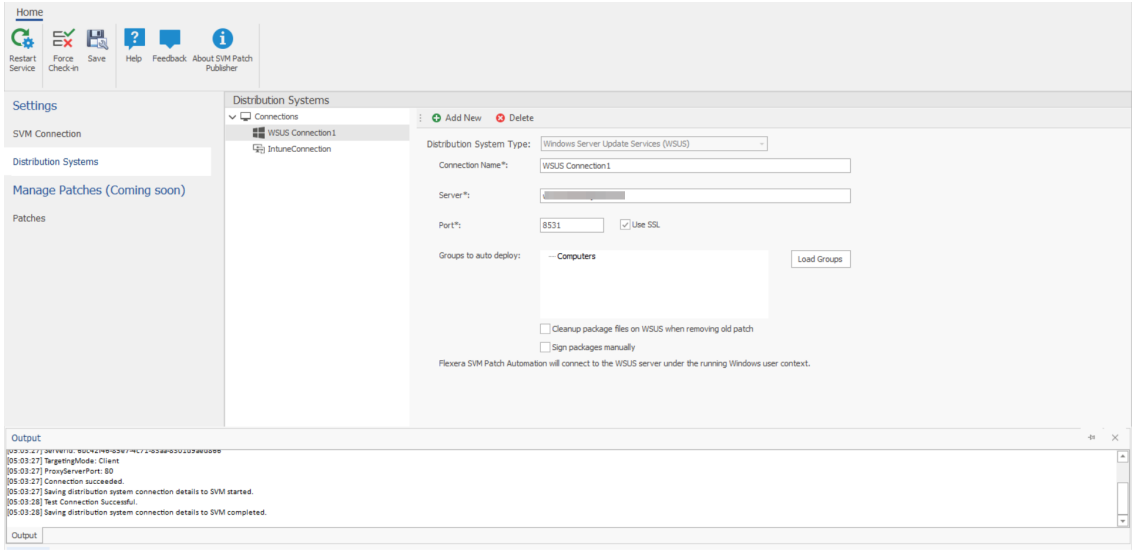
2. Click **Add New**.

3. Use the following fields to add the Windows Server Update Services (WSUS) connection:

Field/Button	Description
Distribution System Type	Select distribution system type as **Windows Server Update Services (WSUS)**.
Connection Name	Enter the connection name.
Server	Enter the server details.
Port	Enter the port number.
Use SSL	Only select the Use SSL Connection check box if your WSUS is configured to accept SSL connections.
Load Groups	Click load group.

Field/Button	Description
Groups to auto deploy	Displays a list of computer groups configured in WSUS Server. Select the computer groups which you wanted to deploy the packages. ***Note*** • *Only displayed when Load Groups button is clicked.*
Cleanup packages files on WSUS when removing old patch	If you enable, old package will be removed during the publish. By default this option will be unchecked.
Sign packages manually	Select **Sign package manually** check box to external package signing.

4. Click the **Test & Save Connection** button to ensure the settings you entered can be used to successfully connect to this service. You will receive a successful message in the **Output** window.



5. On successful connection, the WSUS Distribution System is added to the connections.
6. Restart the SVM Patch Publisher so that the selected groups will be assigned for the end point deployments.

Adding Microsoft Intune Connection

To add Microsoft connection, perform the following steps.

Task ***To add Microsoft Intune connection:***

1. On **Settings** menu, click **Distribution Systems** in the left pane.

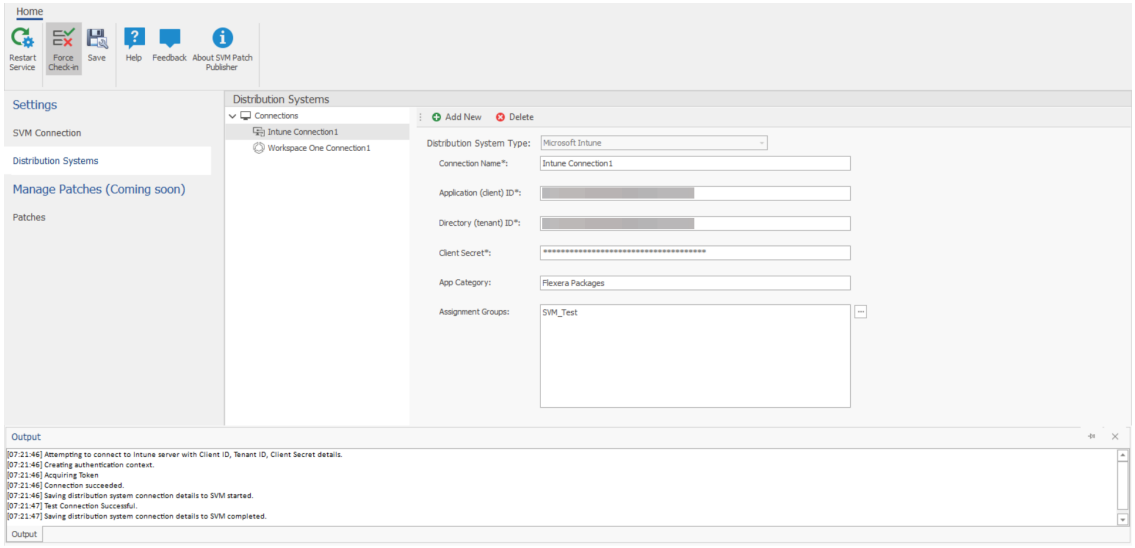
   The **Distribution Systems** pane appears.

2. Click **Add New**.

3. Use the following fields to add the Microsoft Intune connection:

Field	Description
Distribution System Type	Select distribution system type as **Microsoft Intune**.
Connection Name	Enter name of the connection.
Application (client) ID	Enter the registered application (client) id. For more information on generating Application (client) Id, see App Registration.
Directory (tenant) ID	Enter the registered directory (tenent) id. For more information on generating Directory (tenant) Id, see App Registration.
Client Secret	Enter client secret. For more information on generating Client Secret, see Create Client Secret.
App Category	Enter the application category.
Assignment Groups	Choose a group or multiple groups and make assignments for end point deployments. For more information, see Assignment Groups.

4. Click the **Test & Save Connection** button to ensure the settings you entered can be used to successfully connect to this service. You will receive a successful message in the **Output** window.



5. On successful connection, the Microsoft Intune Distribution System is added to the connections.

6. Click **Restart Service** ribbon for the change to take effect.

Adding VMWare Workspace ONE Connection

To add VMWare Workspace ONE connection, perform the following steps.

Task ***To add VMWare Workspace ONE connection:***

1. On **Settings** menu, click **Distribution Systems** in the left pane.

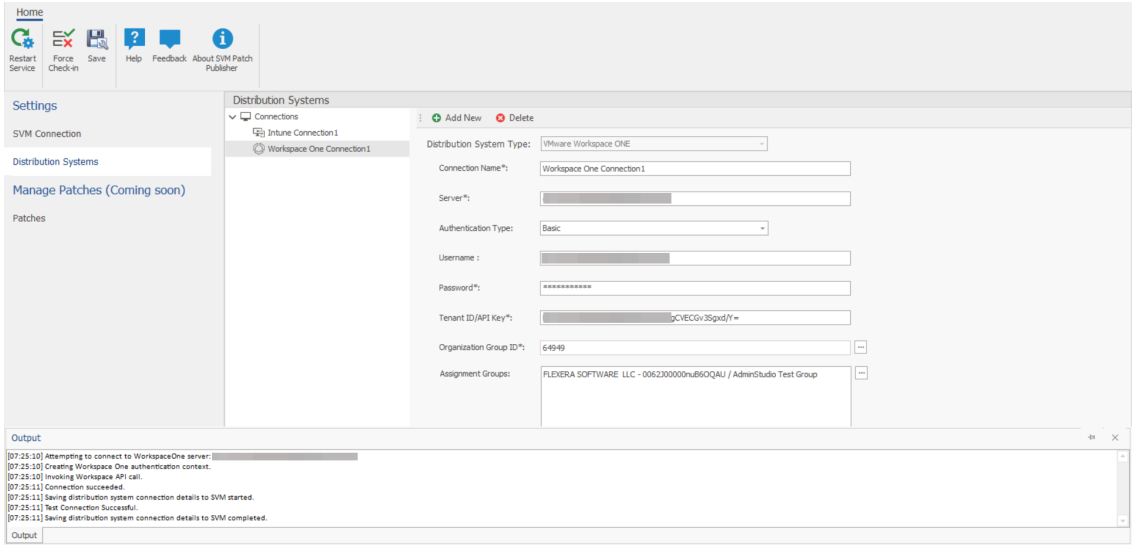
   The **Distribution Systems** pane appears.

2. Click **Add New**.

3. Use the following fields to add the VMWare Workspace ONE connection:

Field	Description
Distribution System Type	Select distribution system type as **VMWare Workspace ONE**.
Connection Name	Enter connection name.
Server	Enter the server details.
Authentication Type	Select one of the authentication type: • Basic - If you select this authentication type, then enter the valid credentials of the VMWare Workspace ONE. • Certificate - If you select this option, you can select the registered certificate. For more information, see Basic or Certificate Authentication Type.
Thumbprint	Choose required certification for the authentication. ***Note*** • *This field appears only when you select Authentication Type as Certificate.*
Tenant ID/API Key	Enter the registered tenant id. For more information, see Create Tenant ID / API Key.
Organization Group ID	Choose the required organization group id.
Assignment Groups	Choose a group or multiple groups and make assignments for end point deployments. For more details, see VMWare Workspace ONE Assignment Groups.

4. Click the **Test & Save Connection** button to ensure the settings you entered can be used to successfully connect to this service. You will receive a successful message in the **Output** Window.



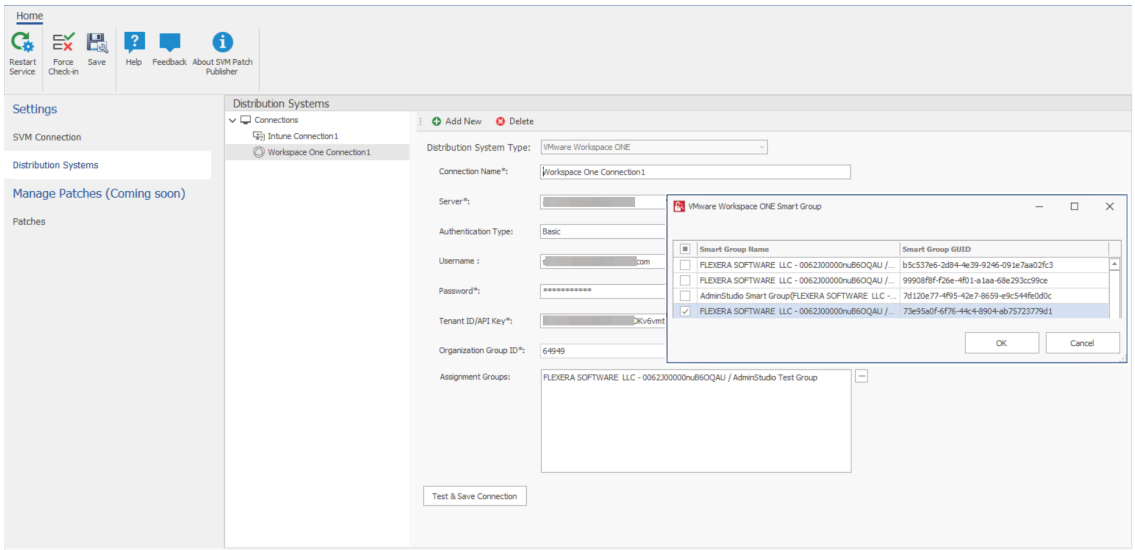
5. On successful connection, the VMWare Workspace ONE Distribution System is added to the connections.
6. Click **Restart Service** ribbon for the change to take effect.

VMWare Workspace ONE Assignment Groups

To make assignments for end point deployments in the SVM Patch Publisher for Workspace ONE publishing, perform the following steps.

Task ***To make assignments for end point deployments in the SVM Patch Publisher:***

1. In **Assignment Groups** (optional) field, click context menu icon. The **Workspace ONE Smart Group window** appears. Select the desired groups from the list and then click **Ok**.



Note • *Make sure that the Assignment Groups are selected before restating the service.*

2. Click **Restart Service** ribbon for the change to take effect.
3. The selected groups will be assigned for the end point deployments.

Deleting an Existing Distribution Connection

To delete an existing Distribution Connection, perform the following steps.

Task ***To delete a connection:***

1. On the **Settings** menu, click **Distribution Systems**. The list of connections appears under the **Connections** pane.
2. Select required connection form the list and click **Delete**.
3. Click **Yes** and confirm to proceed the changes.
4. Upon confirming, the selected connection will be removed from the Connections pane.

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
- Flexera SVM Client Data Tool

Important • *You must install **Software Vulnerability Manager Patch Client ToolKit** to utilize the Vendor Patch Module and SPS Automation, see Automating Patch Deployment and Patch Automation.*

Prerequisites

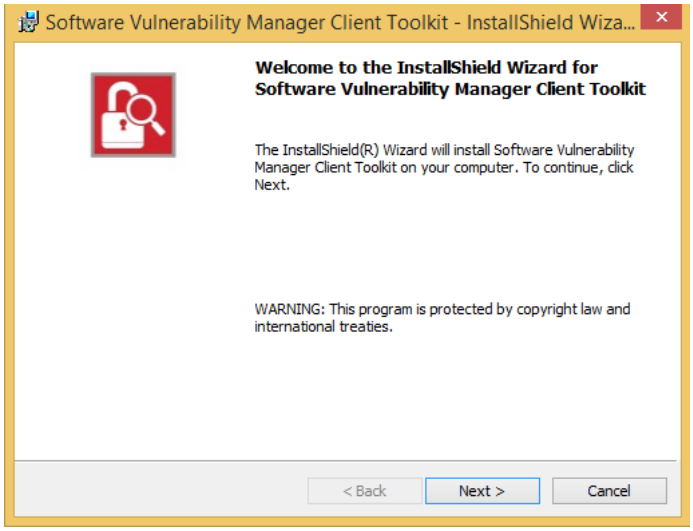
The below prerequisites are required:

- 64 Bit Operating System. Windows 7 +
- Windows Server Update Services (WSUS) administrative console (RSAT) needs to be installed. You need to install the administrator tools version that corresponds to your WSUS server.
- Access Privileges to run the Daemon as a service.

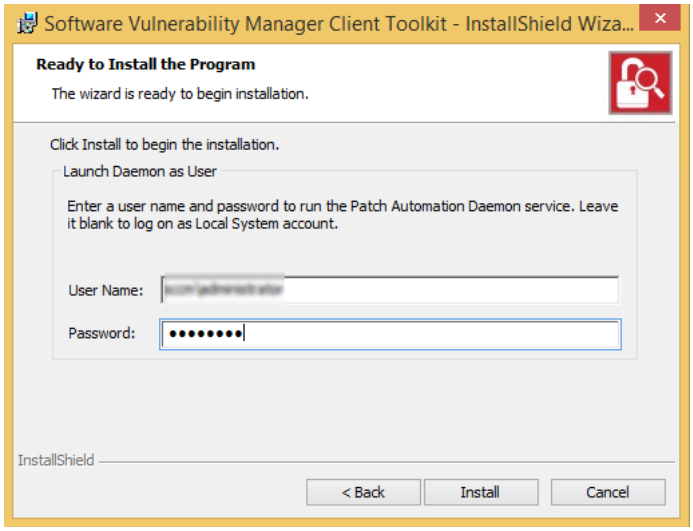
- Access Privileges to makes changes to the WSUS server.
- Internet Connection – SSL/TCP to a SVM server.
- .Net Framework 4.7.2 or above.
- OS Requirements:
  - Install Software Vulnerability Manager Client ToolKit in Windows Server 2012 or Windows 8, for Windows 2012 WSUS.
  - Install Software Vulnerability 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**.



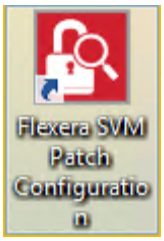
Tip • *On successful installation, one shortcut for* ***Flexera Software Vulnerability Manager Patch Configuration*** *and one shortcut for* ***Flexera WSUS Management Tool*** *will get created in your desktop.*

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.

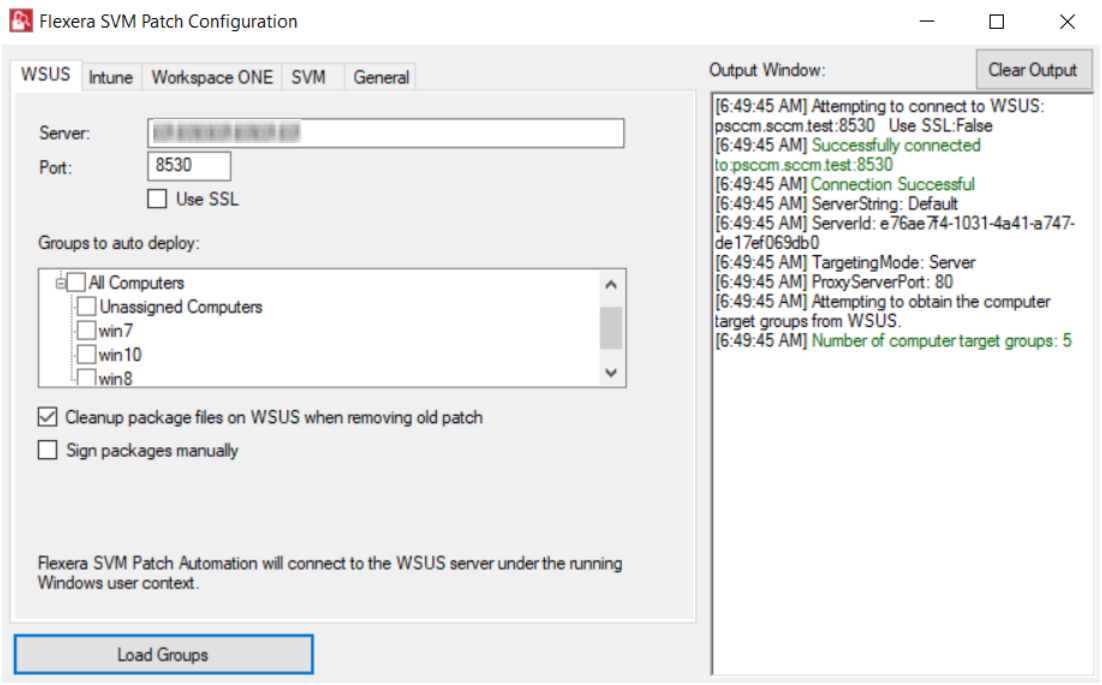


Task ***To use Flexera Software Vulnerability Manager Patch Configuration follow the below steps:***

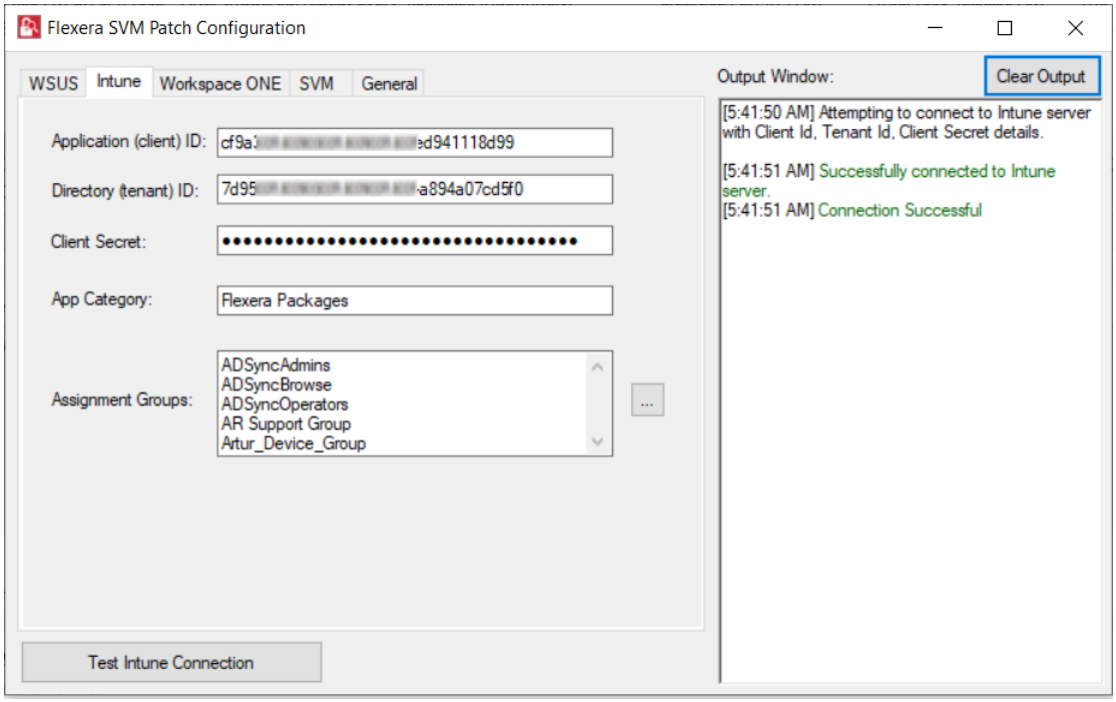
1. Double click on the shortcut created on your desktop, **Flexera SVM Patch Configuration** windows pane appears.
2. It consists of five tabs:
   - WSUS Tab
   - WorkspaceONE Tab
   - Intune Tab

- SVM 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. To external package signing, select **Sign package manually** option.

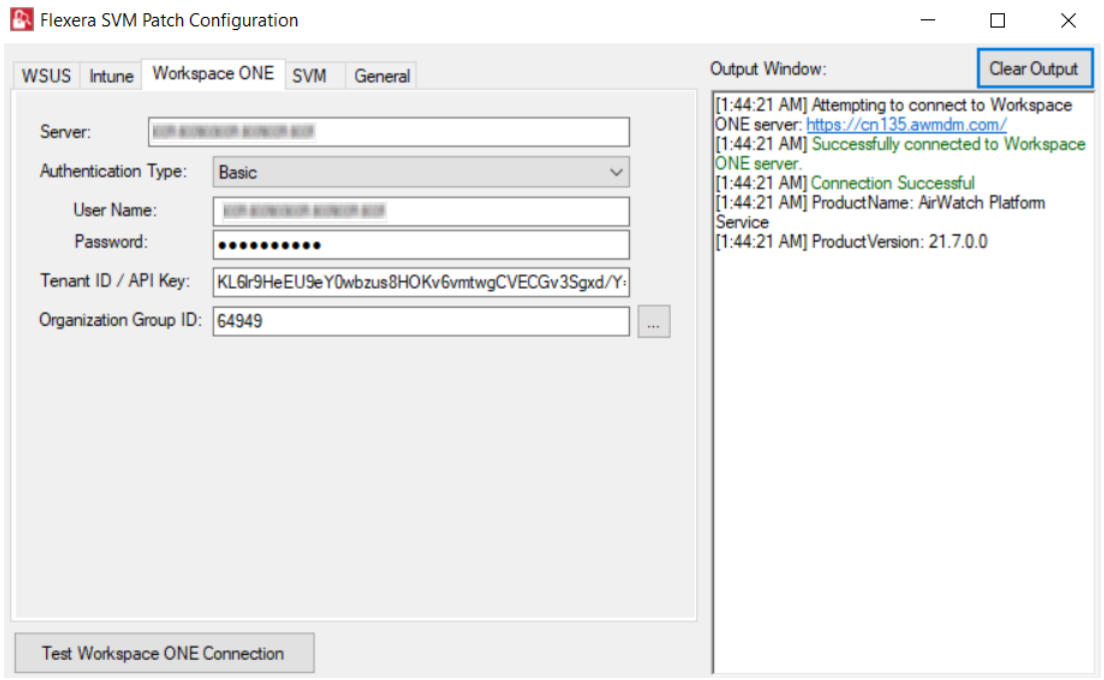


7. In **Intune Connection** tab, you will be prompted to enter your Intune credentials like Application (Client) ID, Directory (tenant), Client Secret. To know more details on configure Intune credentials, see Set up a Distribution Connection in Flexera SVM Patch Configuration for Microsoft Intune.
8. In Assignment Groups (optional) field, choose a group or multiple groups and make assignments for end point deployments. For more information, see Assignment Groups.
9. Click **Test Connection** button, on successful connection you will receive a successful message in the Output Window.



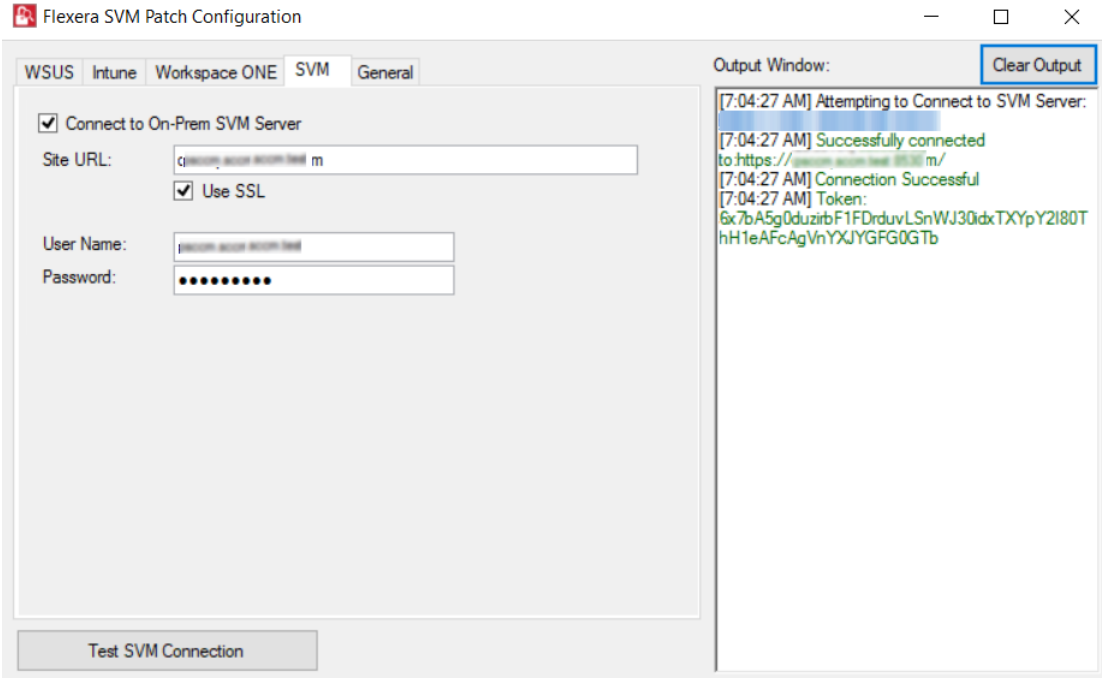
10. In Workspace ONE tab, you will be prompted to enter the valid Workspace ONE connection details like Server name, Authentication Type, Tenant ID/API Key, and selecting Organization Group ID. To know more details on configuration, see Set up a Distribution Connection in Flexera SVM Patch Configuration for Workspace ONE.

11. Click **Test Workspace ONE Connection** button, on successful connection you will receive a successful message in the Output Window.



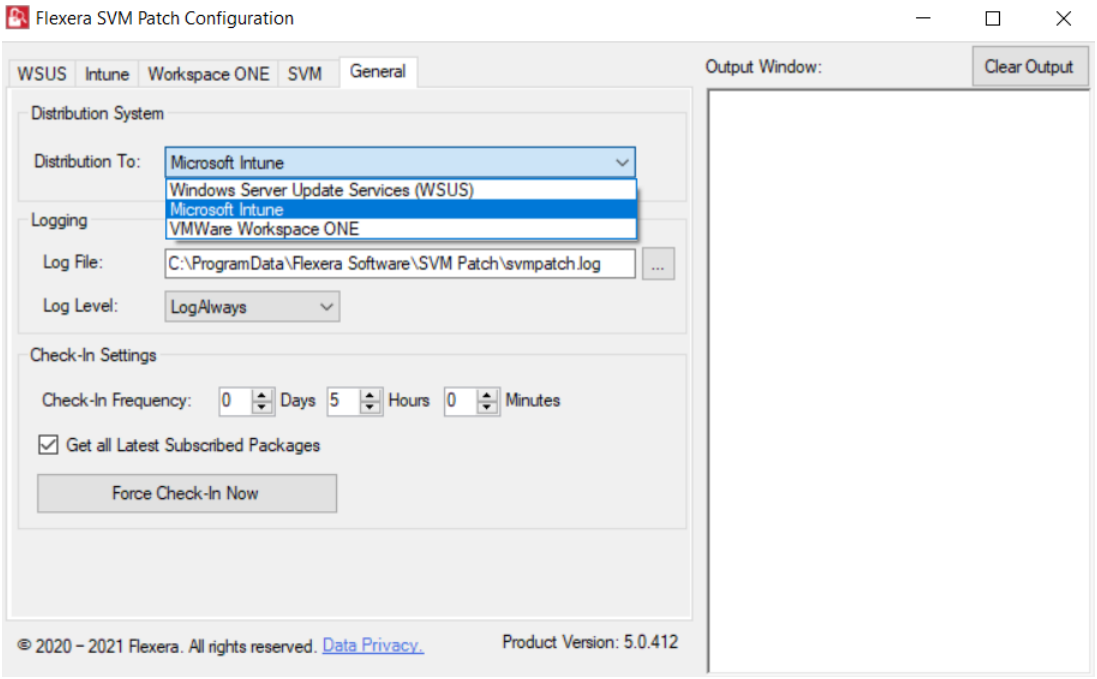
12. In SVM Connection tab, you will be prompted to enter your Software Vulnerability Manager On-Premises credentials.

13. Click **Test Connection** button, on successful connection you will receive a Token in the Output Window.



14. In the General tab, you can set any one of the below distribution system.

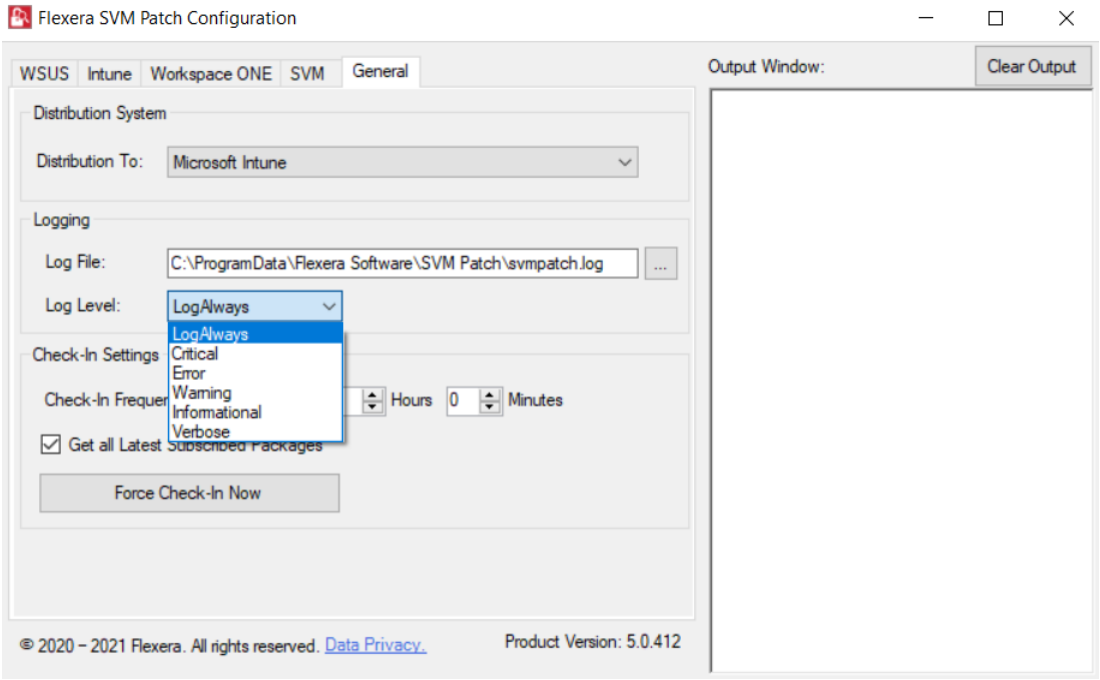
- Windows Server Update Services (WSUS)
- Microsoft Intune
- VMWare Workspace ONE



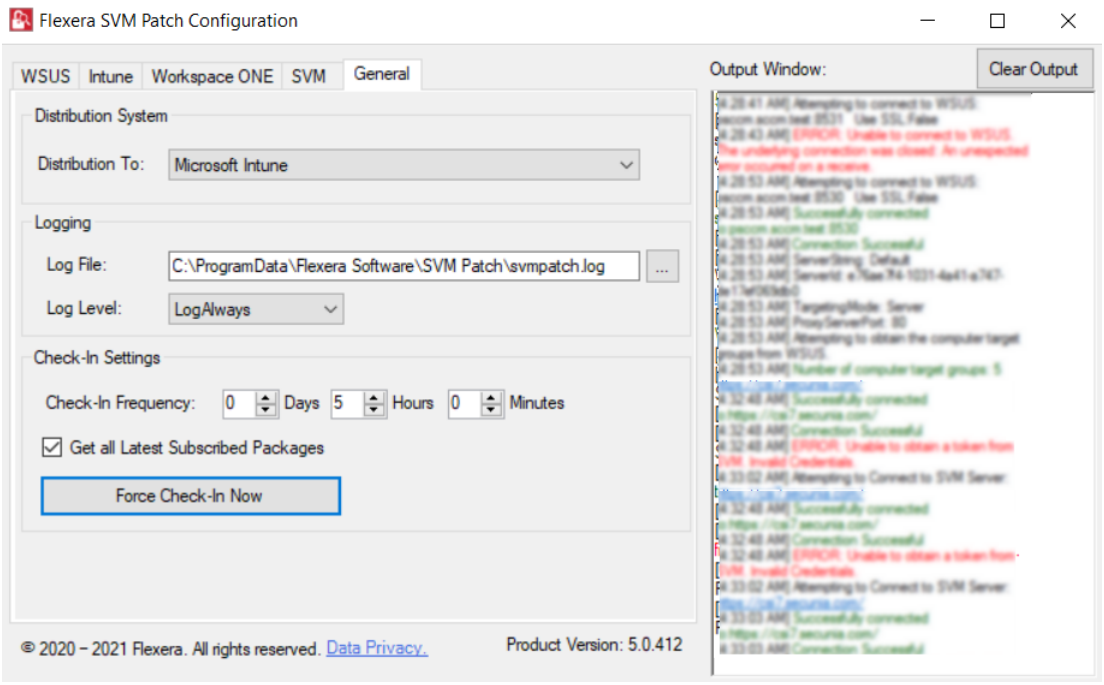
15. You can edit the folder path to save the action logs of this Tool. By default, the folder path will be: **C:\ProgramData\Flexera Software\SVM Patch\svmpatch.log**.

16. You can set any one of the below preferences to save the log files:

    - LogAlways
    - Critical
    - Error
    - Warning
    - Informational
    - Verbose

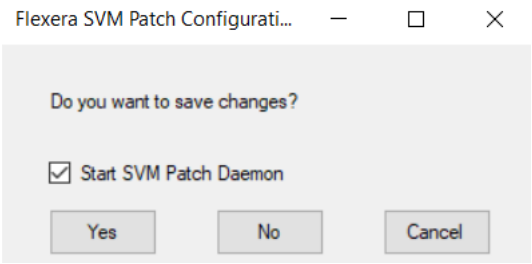


17. In **Check-In Settings**, you can set the frequencies to pull the relevant packages from the server.



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

18. Click check box button if you want to get all latest subscribed packages.
19. To run the services, click close button. You will be prompted to enable **Start SVM Patch Daemon** in the closing window. Click Yes to restart the Patch Daemon for the change to take effect.



***Note** • If any changes added in the Workspace ONE tab or SVM tab, then make sure that Test Connection to be done and then Restart the Patch Daemon for the changes to take effect.*

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 consists of two tabs:

- Patching Information
- Configuration

Patching Information

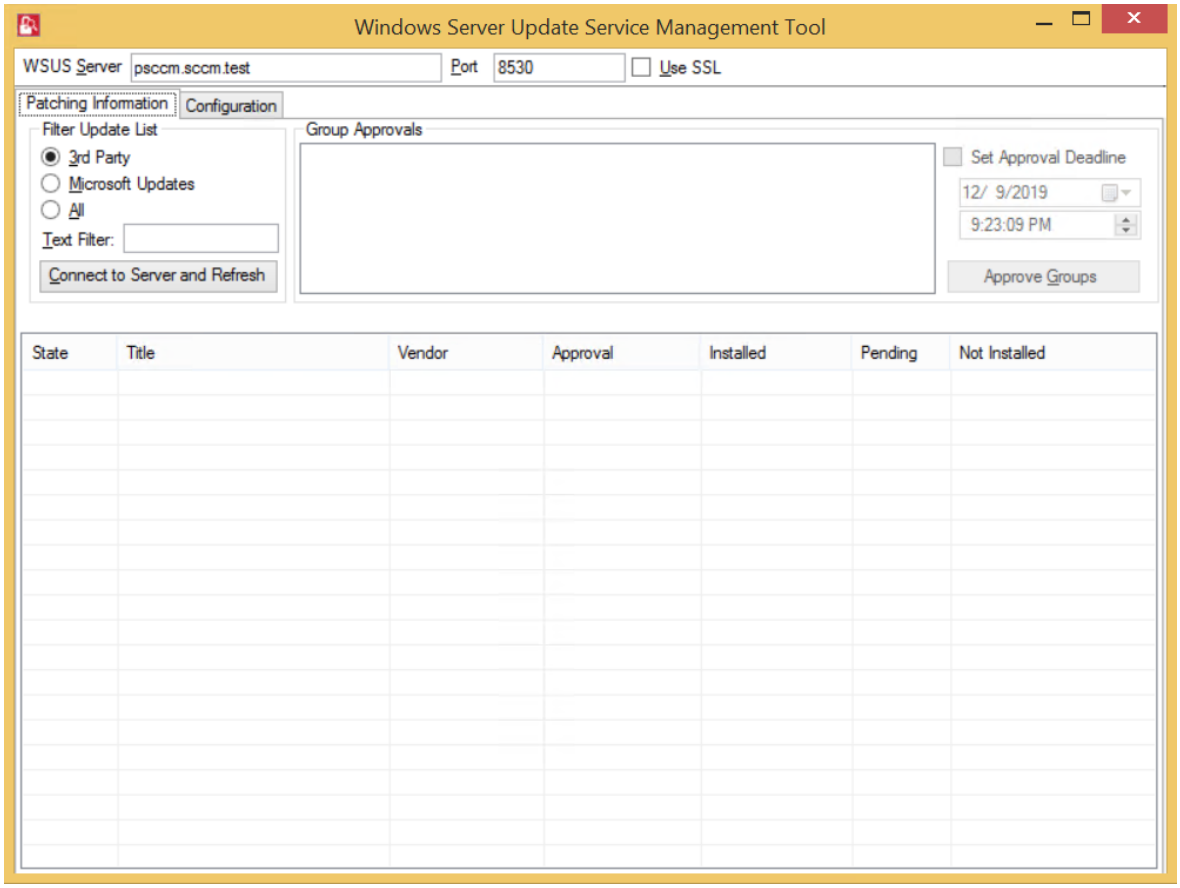
Patching Information tab prompts you to connect to the WSUS server to view the packages, based on the selected filter option, either 3rd party, Microsoft updates, or both. It also allows you to approve, delete, decline the selected patches and select a computer groups where you want to deploy these approved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

It consists of three sections:

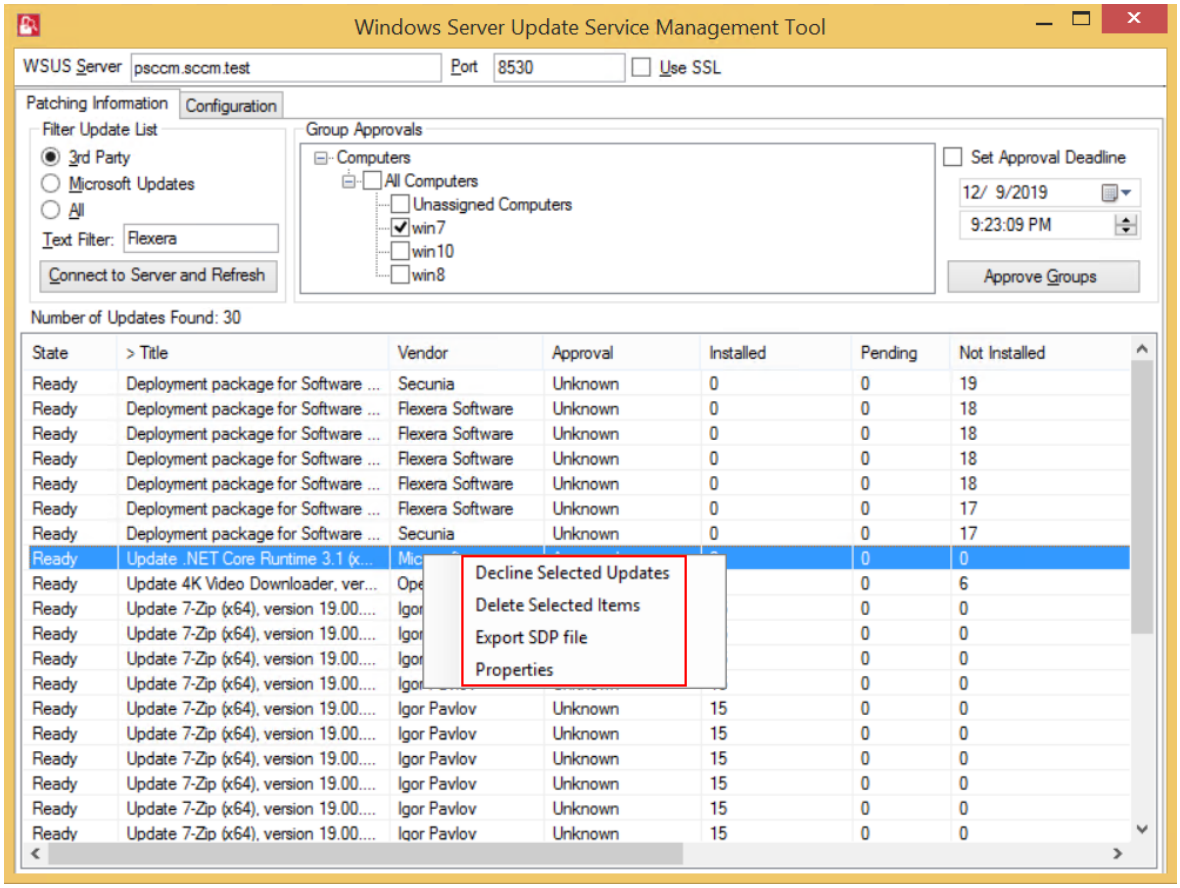
- Filter Update List
- Group Approvals
- Set Approval Deadline

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.

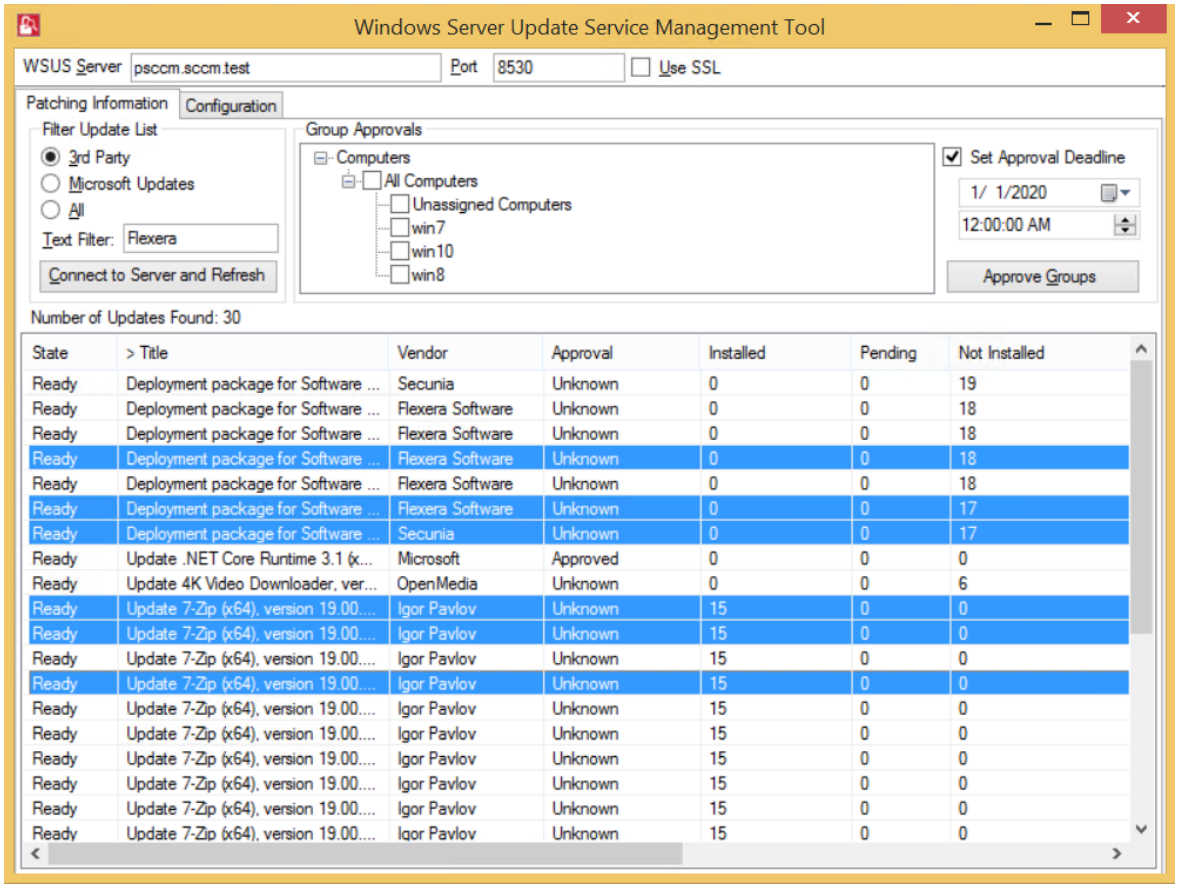


2. In the **Filter Update List**, you can either select 3rd Party Patches, Microsoft Updates, and All. You can enter the patch name or vendor name in the **Text Filter** box to fetch a quick patch list.
3. Click **Connect to Server and Refresh**, list of patches based on the selected **Filter Update 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.*

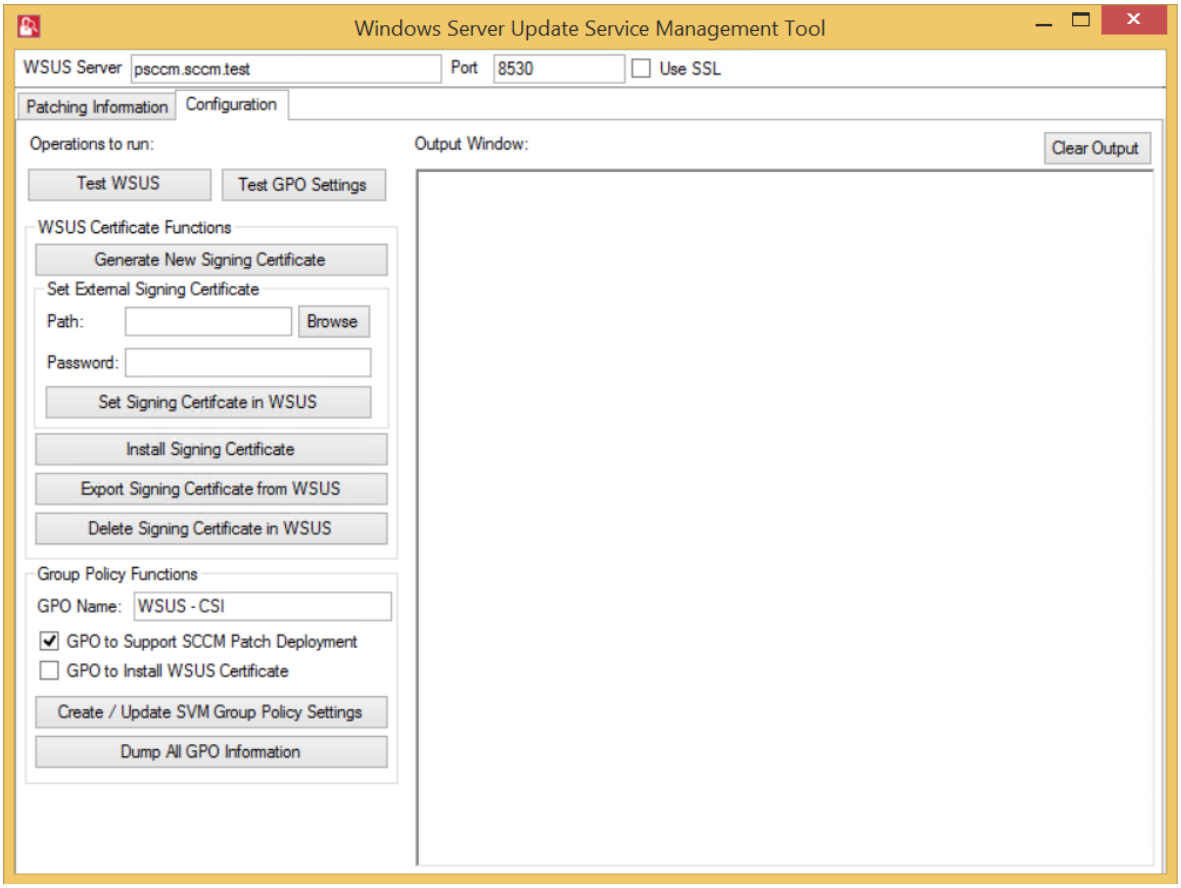


7. To approve the selected patches, click **Approve Groups**. You can see the **Approved** status from the **Approval** Column.

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



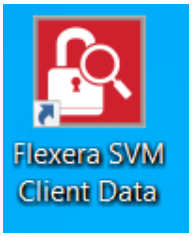
Flexera SVM Client Data Tool

Flexera SVM Client Data Tool will allow you to pull and store your SVM data in a Microsoft SQL database to keep for as long as you wish.

On successful installation of Software Vulnerability Manager Client ToolKit, a new shortcut **SVM Client Data** tool will get created in your desktop.

To pull data, perform the following process:

- Create Database Connection
- Add Account
- Sync Data



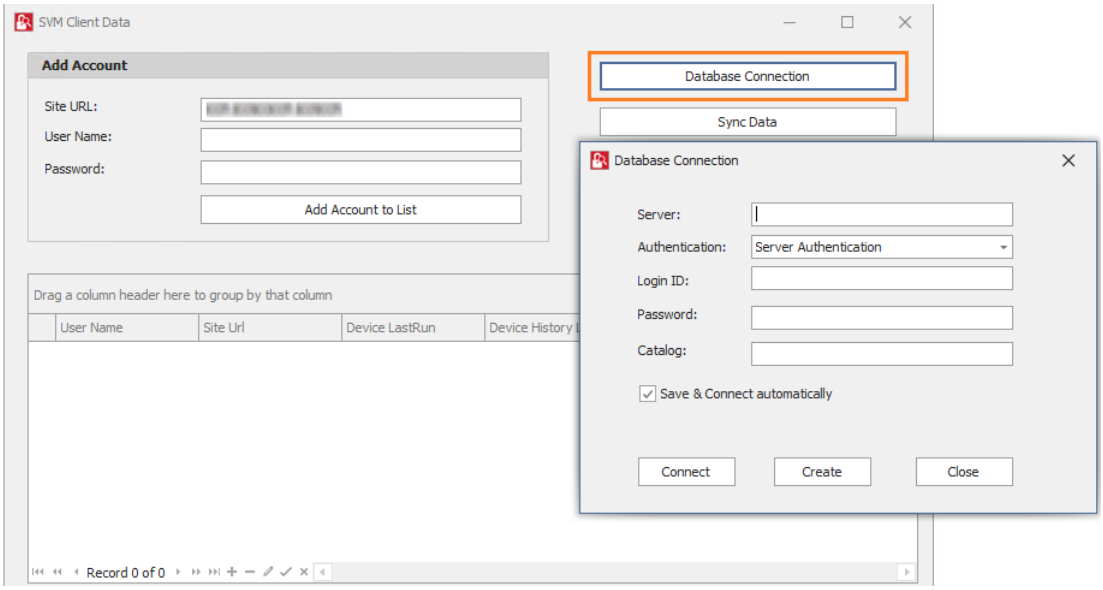
Alongside the SVM Client Data Tool, PowerBI templates have been included. With these Power BI templates, you can generate trend reports for the existing data. For more information on generating reports, see Generating Data Trend Reports.

Create Database Connection

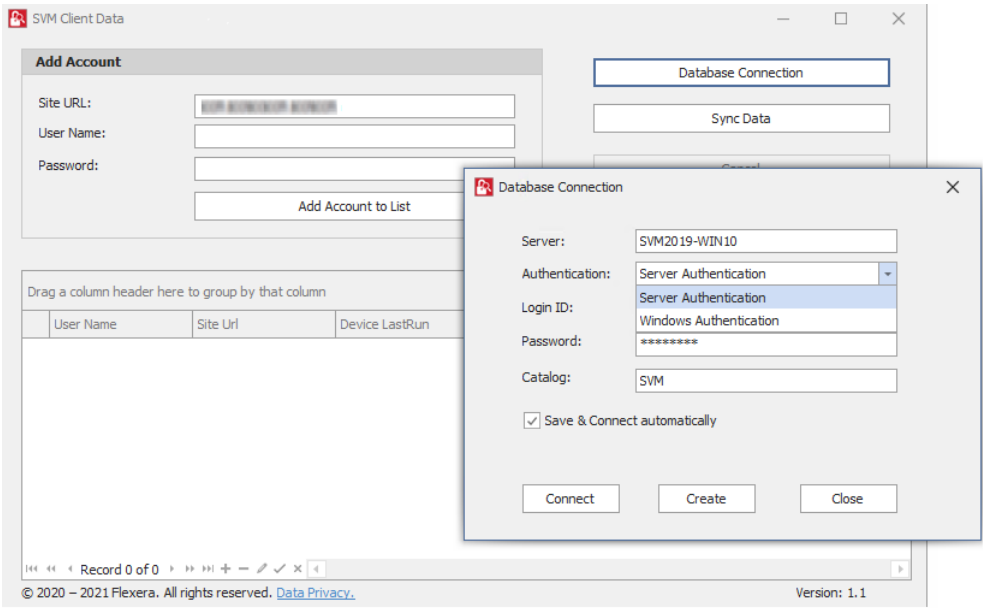
To create a Database connection in Client Data Tool, perform the following steps.

Task ***To create a Database connection:***

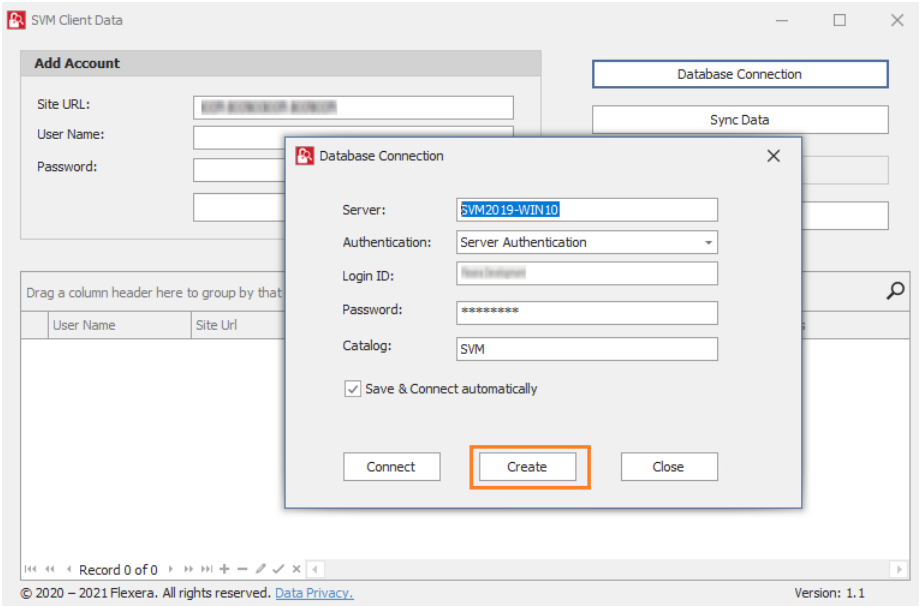
1. Double click on the shortcut created on your desktop, **Flexera SVM Client Data** windows pane appears.
2. Click **Database Connection** button. The Database Connection window appears.



3. In **Server** field, enter SQL Server name.
4. In **Authentication** field, you can select authentication type as either **Server Authentication** or **Windows Authentication**.



5. If you select **Server Authentication**, then enter Login ID and Password.
6. In **Catalog** field, enter the catalog name.
7. After entering the details, click **Create** button.



8. Upon successful action, Database created in the Microsoft SQL Server.
9. Once Database created, you can **Connect** to the Database.

Note • *To connect the database server, make sure to install the SSL certificate in Trusted publisher and trusted root certificate authority where client data is installed.*

Add Account

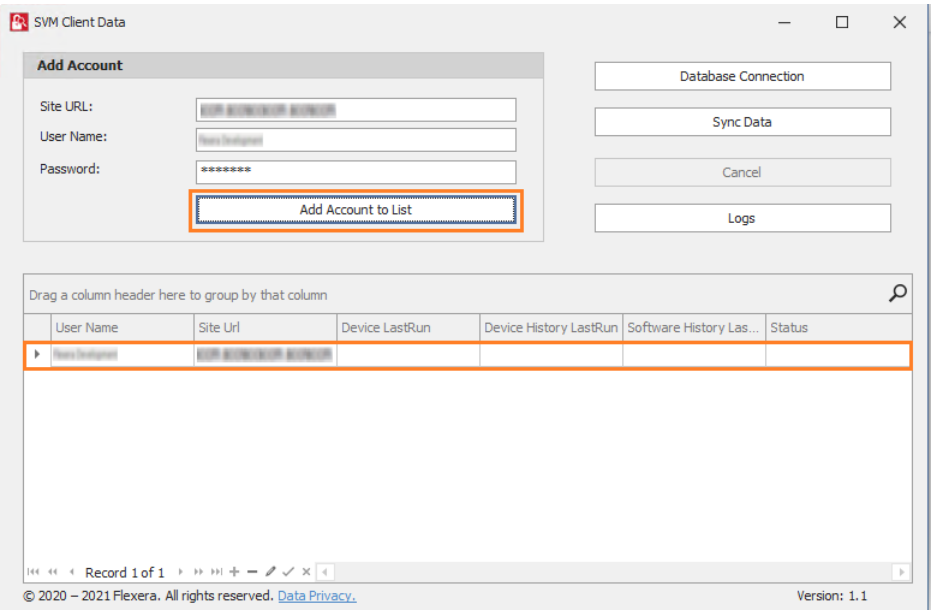
To add account in Client Data Tool, perform the following steps.

Note • *Make sure that the Database is connected. For more information, see Create Database Connection.*

Task ***To add account:***

1. In Add Account, enter **Site URL** in the text field.
2. Enter the User Name and Password, and click **Add Account to List** button.

   Added account will then be listed in the below section.



Sync Data

To pull data to Microsoft SQL server, perform the following steps.

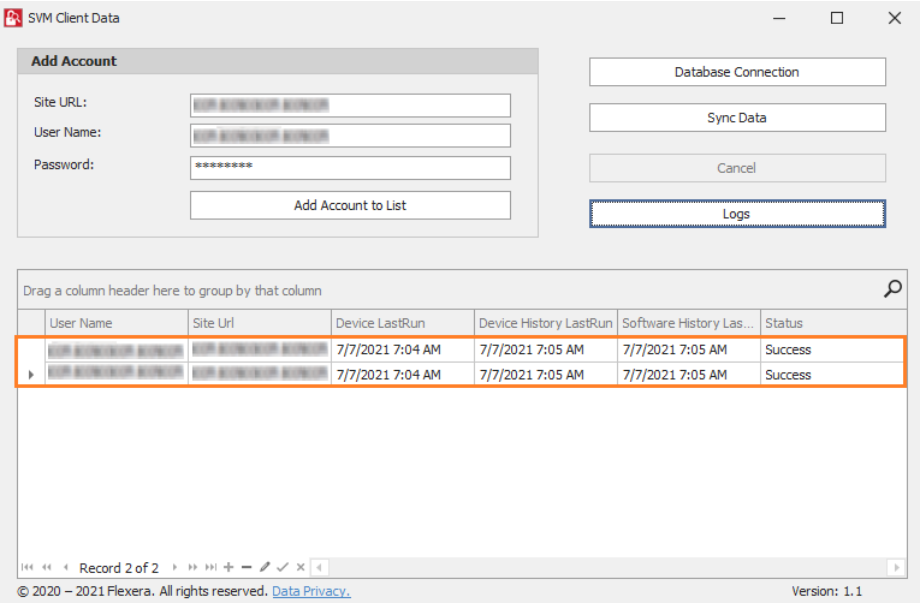
Note • *Make sure that the Database is connected and SVM account is added. For more information, see Create Database Connection and Add Account.*

Task ***To pull data to Microsoft SQL server:***

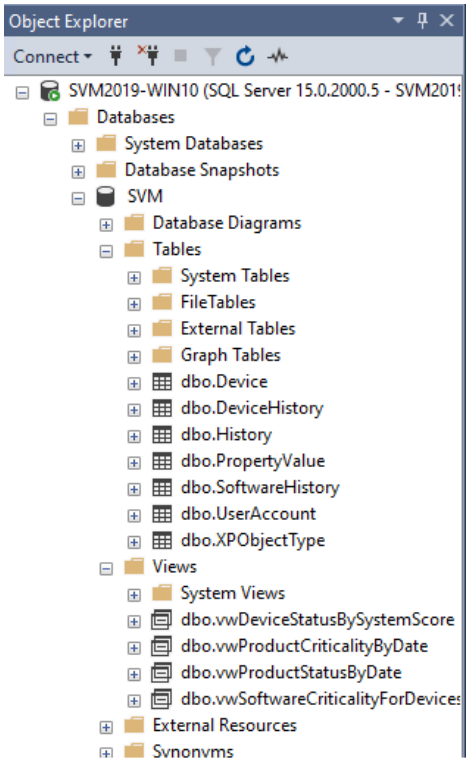
1. In Client Data Tool, click **Database Connection** and connect to the database server. for more information, see Create Database Connection.
2. If required, you can add multiple SVM accounts. For more details on adding the account, see Add Account.

3. Click the **Sync Data** button. It starts pulling data to the Database.

4. Upon successful action, sync details will display in the below section.



5. Sync data will be available in tables and views.



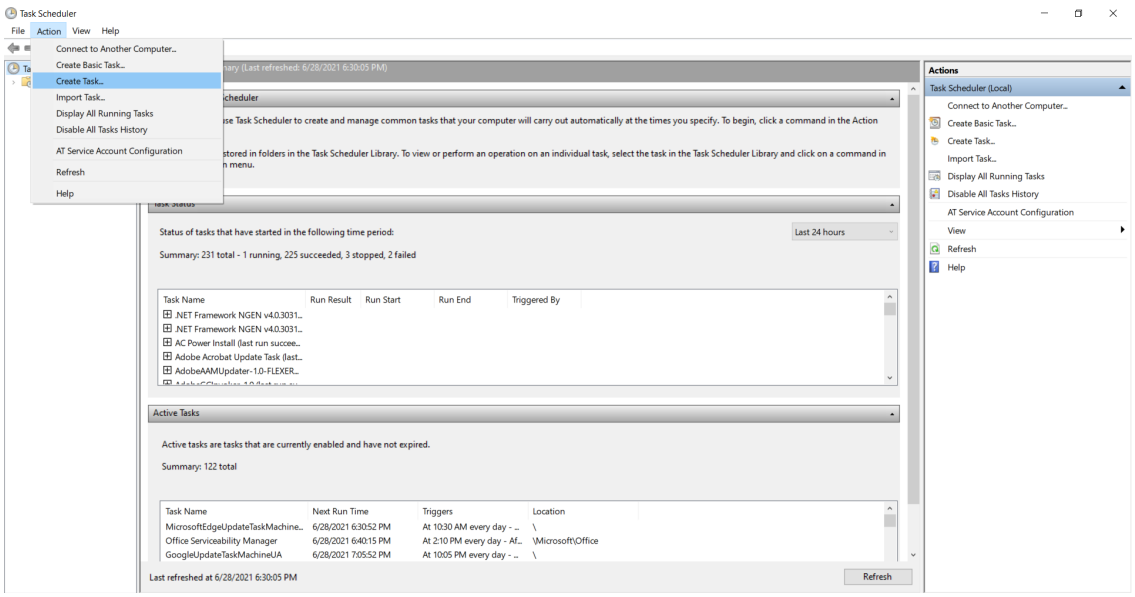
6. You can manually sync data or you can schedule automation for the data sync. To schedule automation, see Schedule Automation for Sync data.

Schedule Automation for Sync data

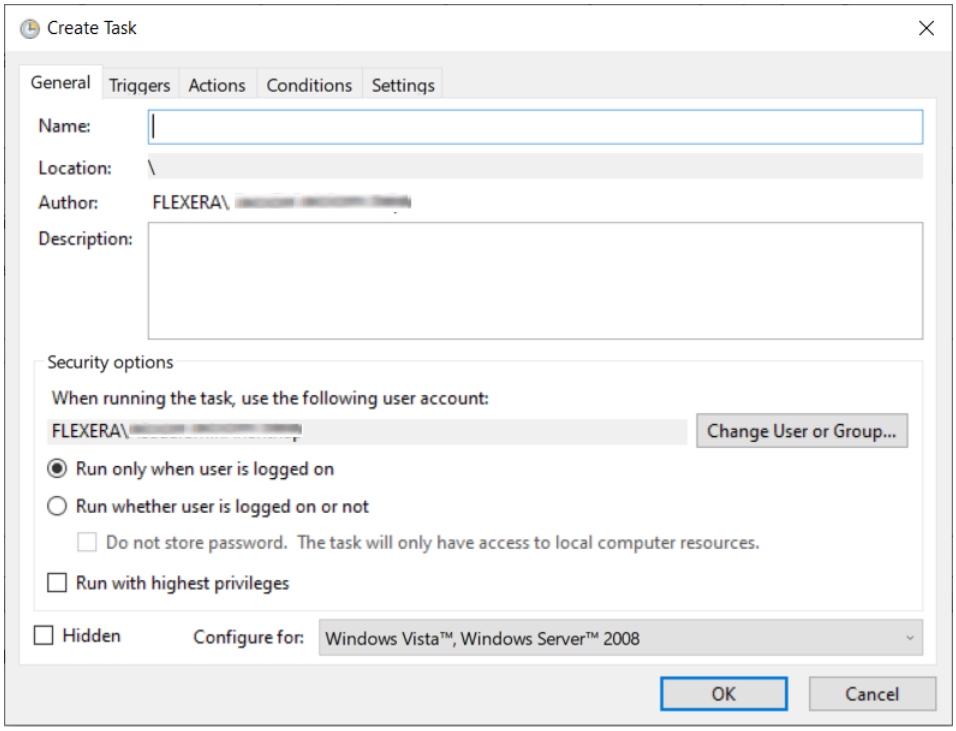
To schedule automation for sync data, perform the following steps.

Task ***To schedule automation for Sync data:***

1. Type Task Scheduler in the Windows **Start** menu and click on **Task Scheduler** to launch task scheduler.
2. On the **Actions** tab menu, select **Create Task** option. The **Crete Task** dialog box appears.

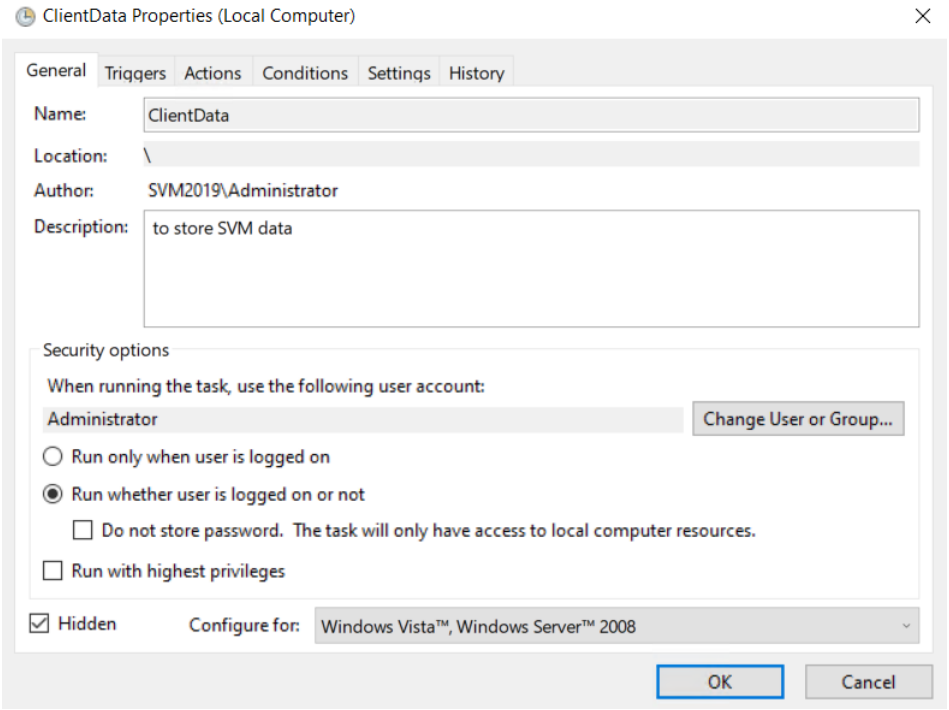


3. It consists of five tabs:
   - General
   - Triggers
   - Actions
   - Conditions
   - Settings



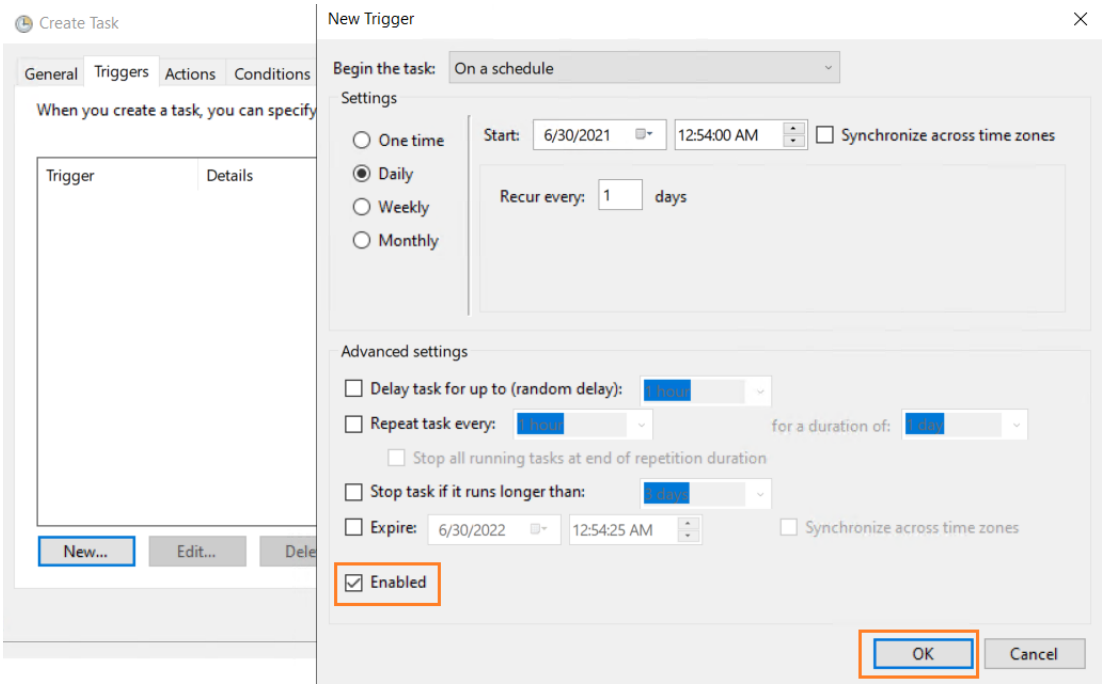
4. In **General** tab.

   - In Name field, enter the task name.
   - In Description field, enter description for the task.
   - In **Security options** section, you can configure which administrator account can run the task.
   - Select the **Run whether user is logged on or not** option.
   - Select the **Run with highest privileges** option, If the task requires the highest privileges.
   - Select the **Hidden** option, If you want to hide the task.
   - The **Configure for** settings are changed only when you are required to use a different compatibility option.
   - Click **Ok** button.



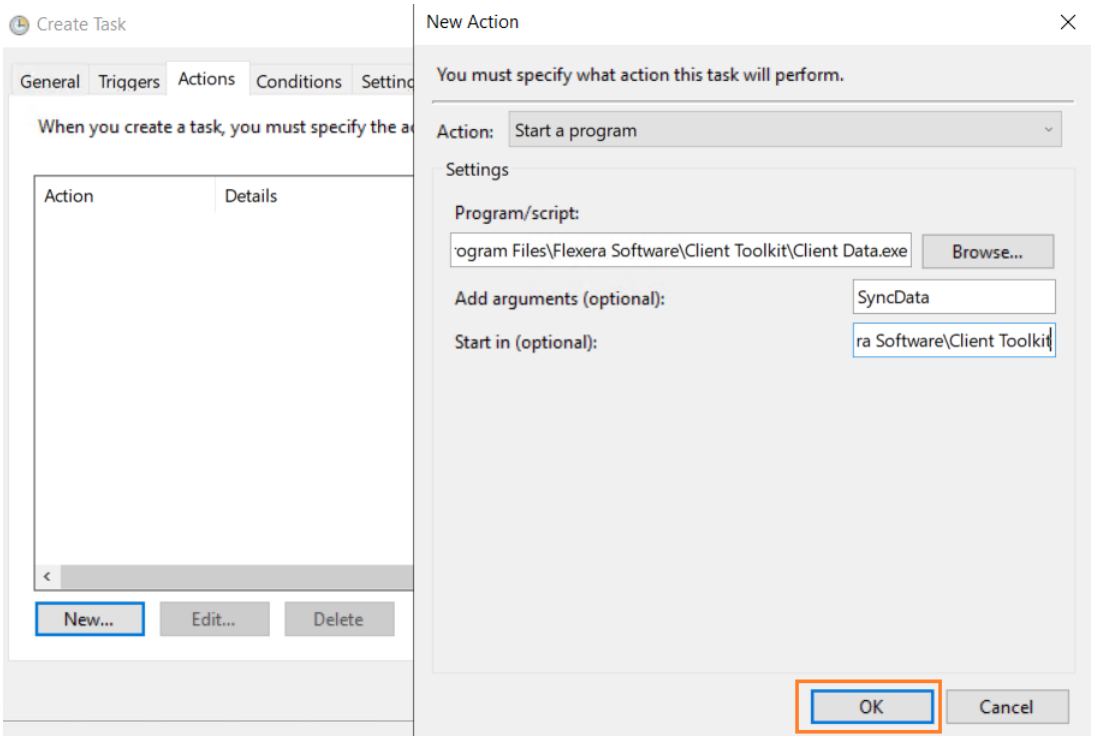
5. In Triggers tab.

   - Click the **New** button. The **New Trigger** dialog box appears.
   - Click the **Begin the task** drop-down and select one of the triggers from the list.
   - Select Daily, Start date and time, and then enable the settings. Click **Ok** to schedule the task.



6. In the **Action** tab.

- Click the **New** button. The New Action dialog box appears.
- Click the **Action** drop-down and select one of the actions from the list.
- Under the **Settings** section, in the **Program/script** field, specify the path for the application (SVMClientData.exe).
- In the **Add arguments (optional)** field, you can specify Sync Data.
- In the **Start in (option)** field, specify the installation folder of the SVMClientData.exe
- After selecting the above fields, click the **Ok** button.



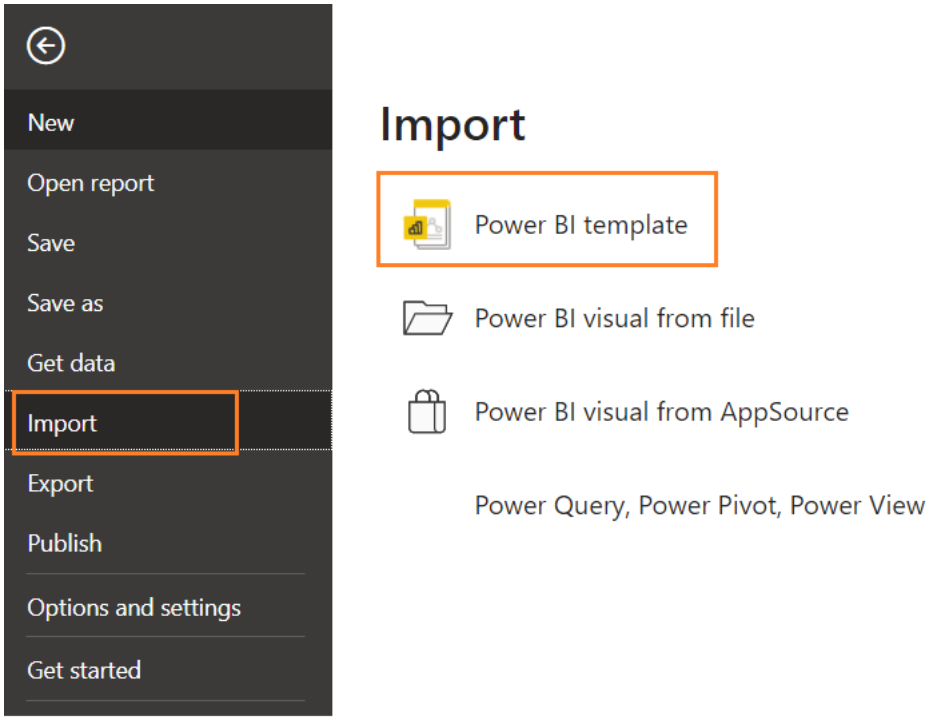
7. After completing the steps, authenticate with your account credentials, and then the task will run automatically on schedule or event using the specified settings.

Generating Data Trend Reports

With the Power BI templates you can generate a trend reports for the existing data. To generate a data trend reports, perform the following steps.

Task ***To generate Data Trend Reports:***

1. Download Power BI Desktop (https://powerbi.microsoft.com/en-us/downloads/).
2. Open the Power BI Desktop.
3. Click on the **File** menu, select **Import**, and select **Power BI Template**.



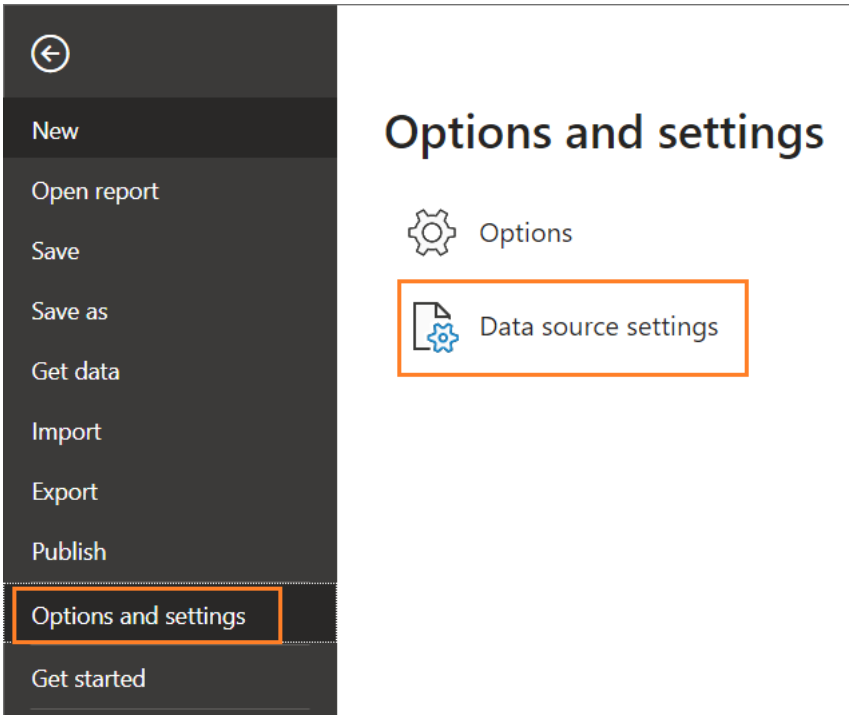
4. Select the desired template from the Client Data Tool\Report Templates\Power BI folder.

Note • *Alongside the SVM Client Data Tool, Power BI templates have been included.*

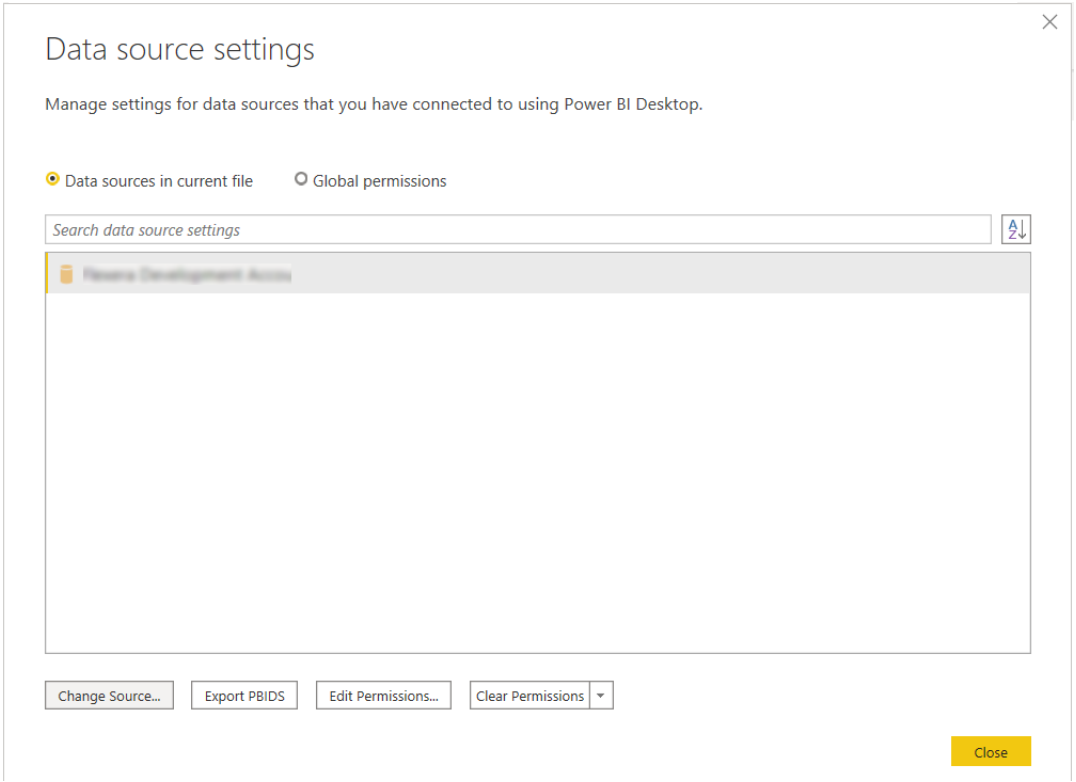
5. Once the template is selected, change the database source as mentioned in the below steps:

   - Click on the **File** menu, select **Options and settings**, and select **Data source settings**.

     The **Data source settings** dialog box appears.



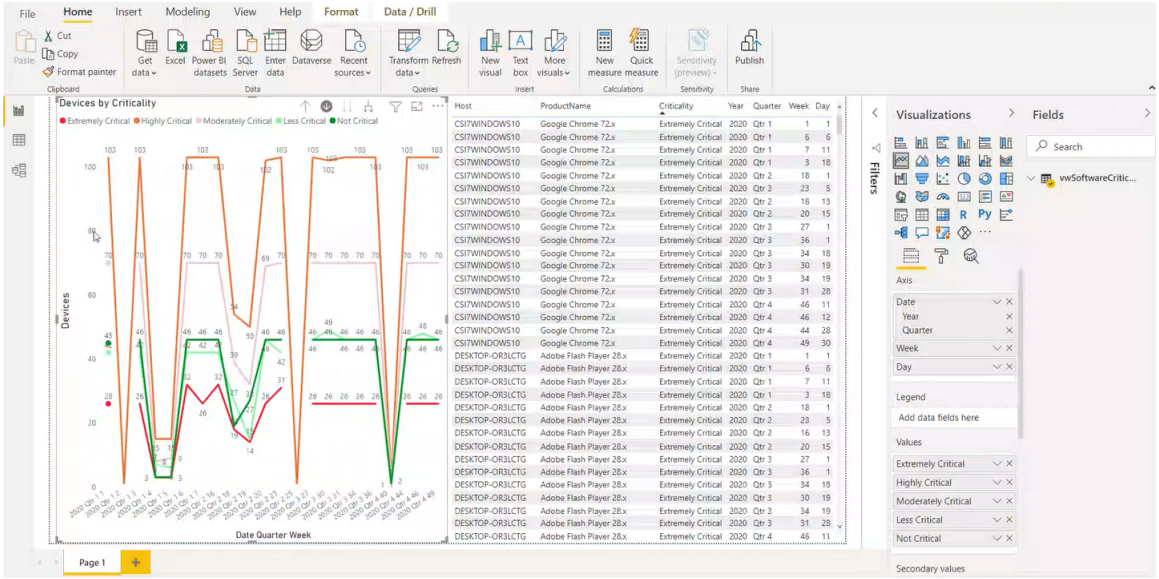
- In the **Data source settings**, select **Data sources in current file** by clicking on the radio button, and click the **Change Sources** button. The SQL Server database dialog box appears.



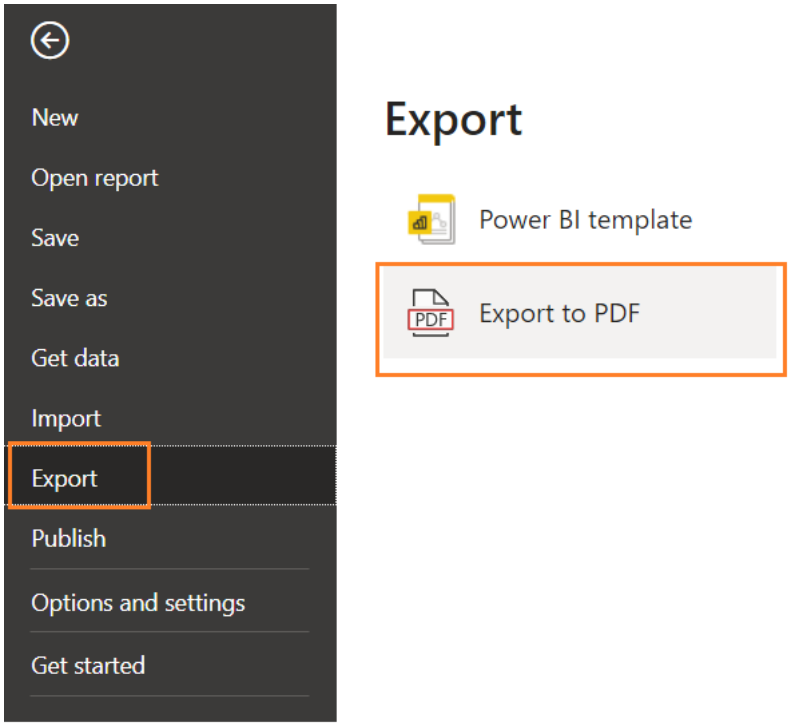
- In the **SQL Server database**, enter the server (port) details and the database details. Click **Ok** button.

- Upon successful action, the database source is updated.

6. You can see the report for the selected Template.



7. You can generate reports:
   - Criticality status by device
   - Criticality status by product
   - Device status by system score and date
   - Secure status by product
8. On the **File** menu, click **Save** to save your changes.
9. On the **File** menu, click **Save As**. The Save As dialog box opens. The **Save As** dialog box lets you specify the name and location where you want to save the template.
10. To export the report, select Export > Export to PDF from the File menu.



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:

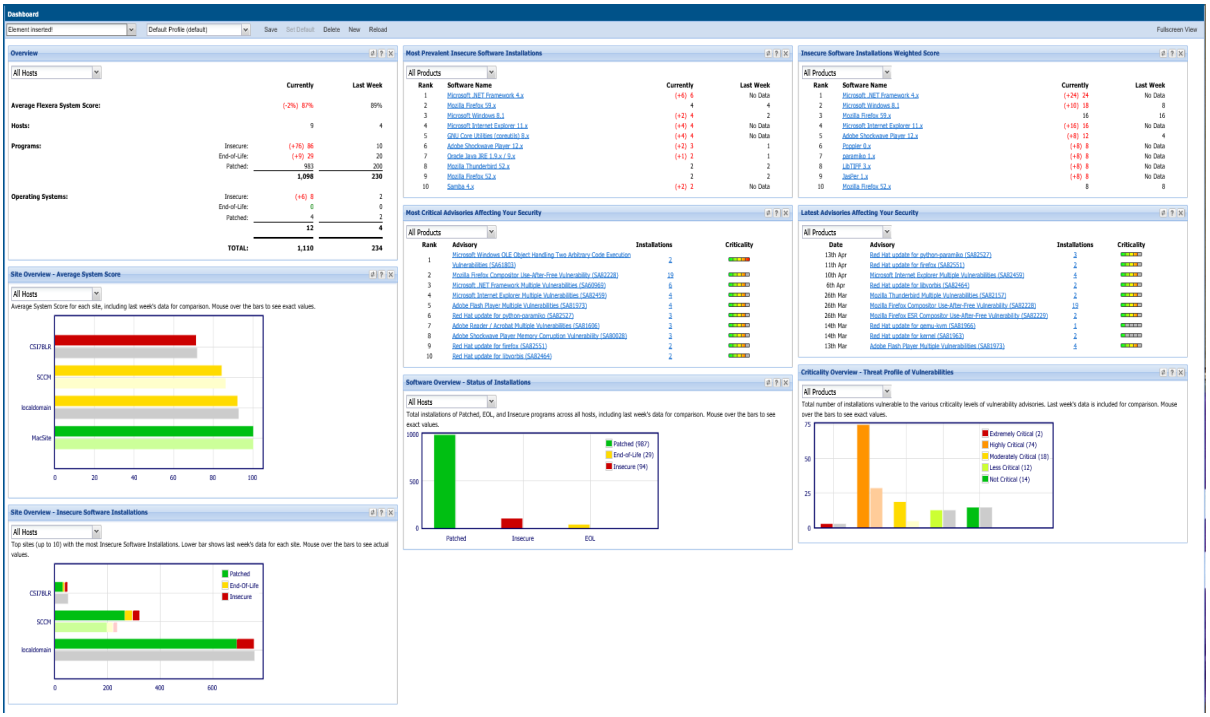
- Register (https://rebrand.ly/welcome-to-flexera) for a Welcome to Flexera session. These sessions are hosted by our Customer Success team. You'll get a high level overview of Flexera and its product and support resources.
- Visit our Customer Community (https://community.flexera.com/t5/Software-Vulnerability-Manager/ct-p/Software-Vulnerability-Manager). We extend case management privileges to two individuals per organization. If you need to update your technical contacts in Flexera's Customer Community, the following video explains how to do that: https://www.youtube.com/watch?v=bSD28T432QA&list=PLCuhlHqMRwWqqBAOs0_DKa30XEIim5ORR&index=6.
- Anticipate an email from our Community containing your user credentials. Your organization's administrative contact (many times an individual in procurement or finance) has the ability to assign case management privileges.
- Request (https://community.flexerasoftware.com/register.php) access to 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.*

5

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 Caching of Scan Rules

Agent Administrative Privileges

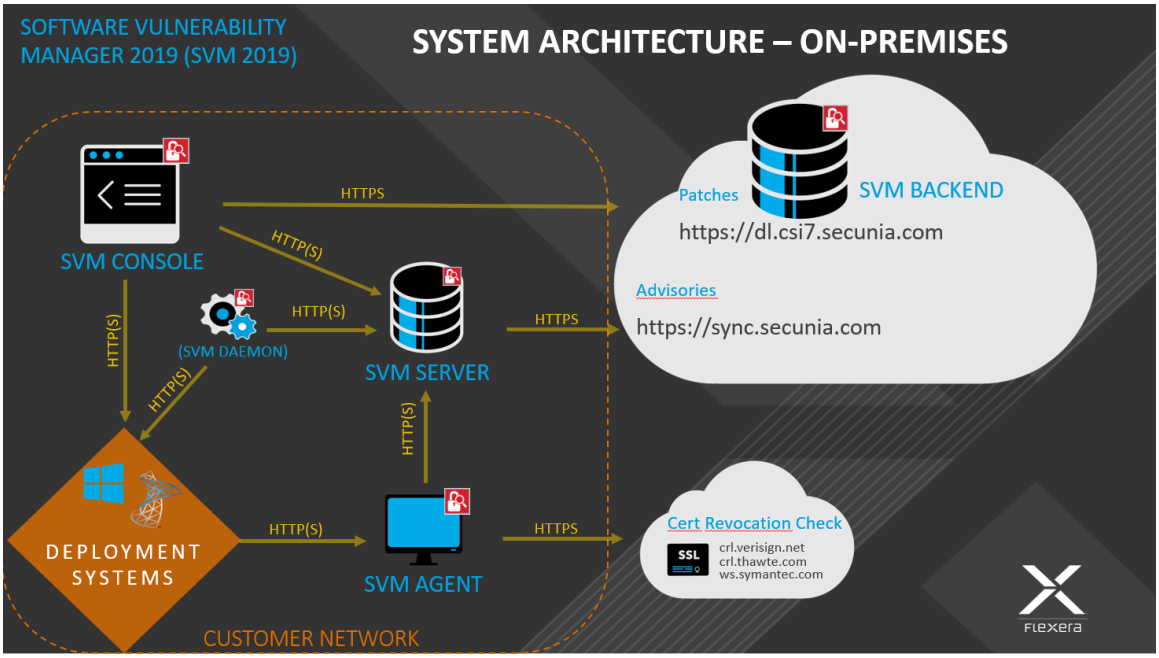
The Software Vulnerability Manager Agent requires administrative or root privileges for the following functionality:

- 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 SVM 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.

Agent Caching of Scan Rules

New scan agents available with this release, will now cache scan rules. Agents servers will determine if the agent needs a new set of rules and will only push these rules if needed. This will result in decrease in the amount of network traffic generated by the scan agents which will be especially beneficial in very large environments. To take benefit of this enhancement, the current version of the scan agent in your environment should be upgraded to the new version of the agent - 7.6.1.15

6

Scanning

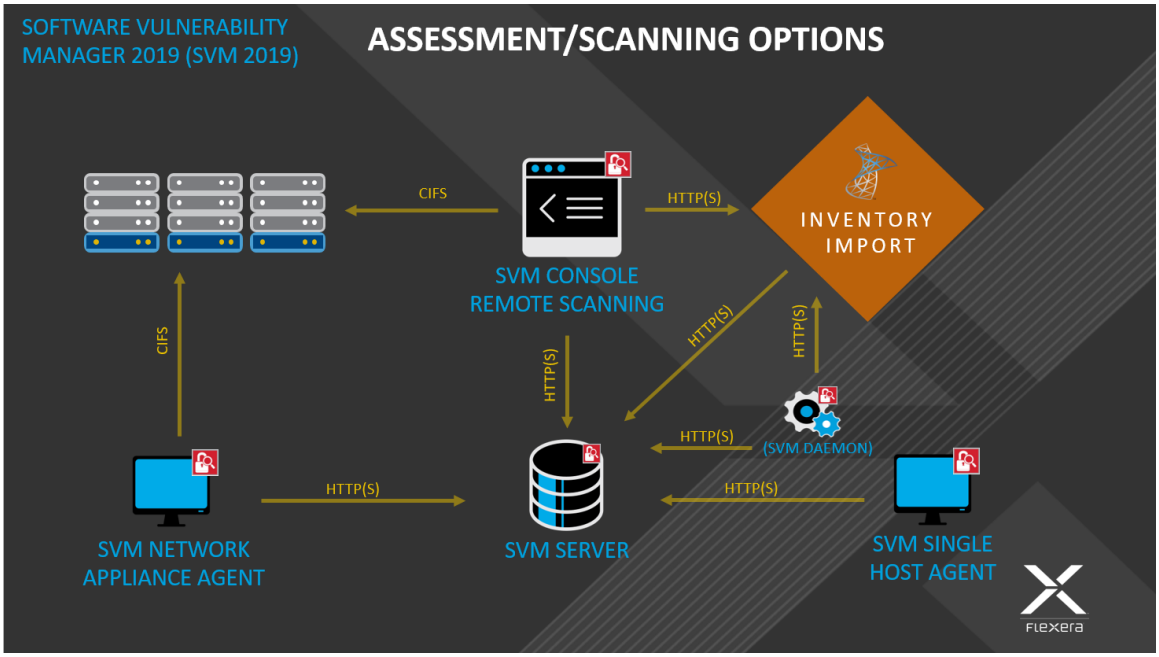
Software Vulnerability Manager allows scanning of target hosts using the following approaches:

- 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 allowed 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
  - 10.15 Catalina
  - 11 Big Sur
- 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).

Note • *To install and scan Mac Agent in Mac OS Big Sur with ARM Architecture, you need to install Rosetta software.* `softwareupdate --install-rosetta`

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:

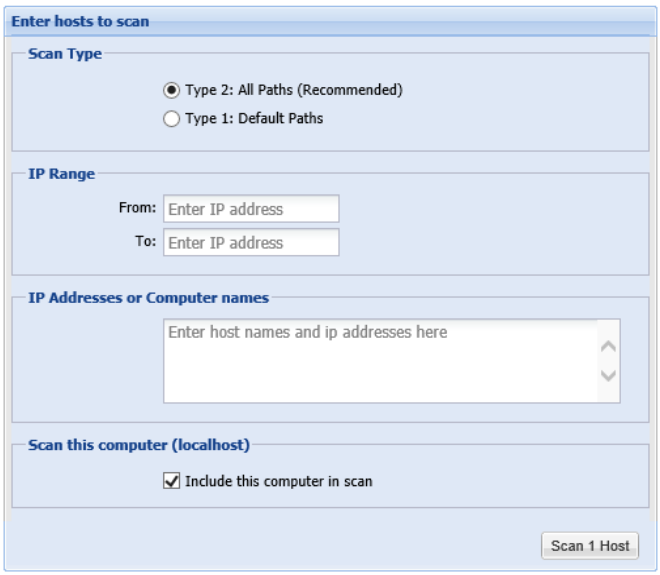
- Quick Scan
- Scan Groups
- Scan Progress

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**.

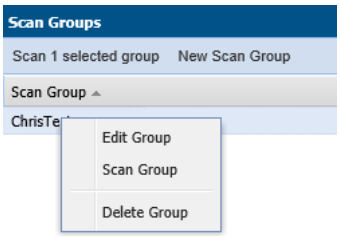


To make sure that you are able to remote scan the target host, please ensure that all the system requirements for the remote scan are in place.

The progress can be seen under Scan Progress.

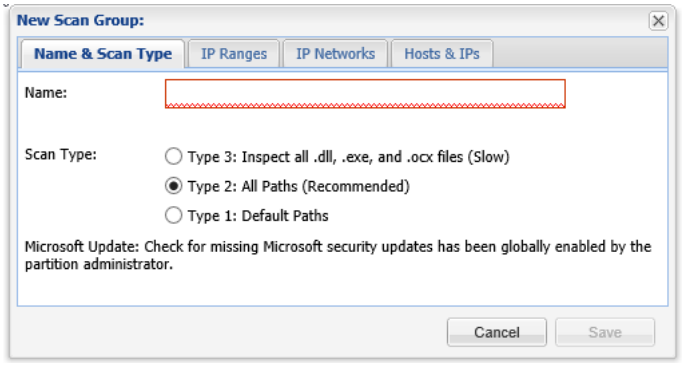
Scan Groups

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.

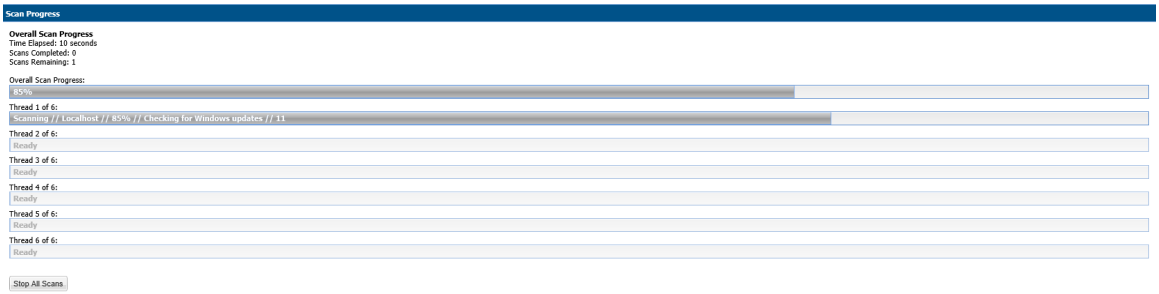
Click **New Scan Group** to create and configure a group of hosts to be scanned.



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:

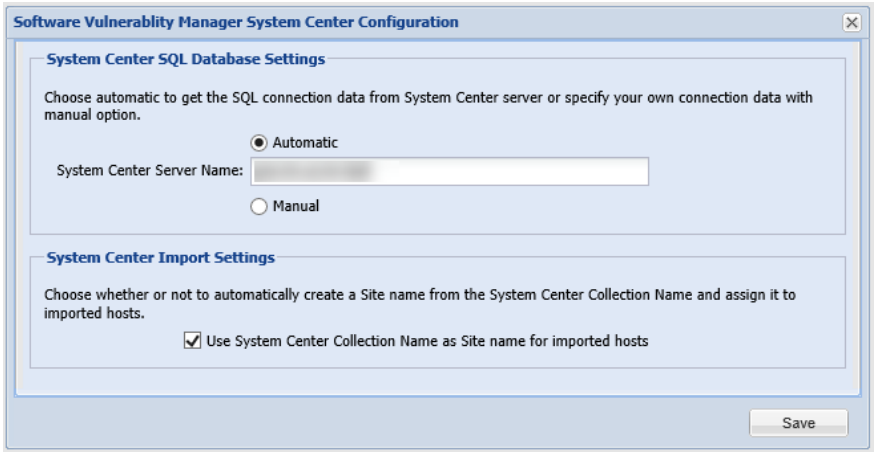
- **Setting up authentication**—The user running the Software Vulnerability Manager console must have access to the database containing the data of the System Center. For System Center Configuration Manager the database is named CM_<site_code> and for System Center Configuration Manager 2007 it is named 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.

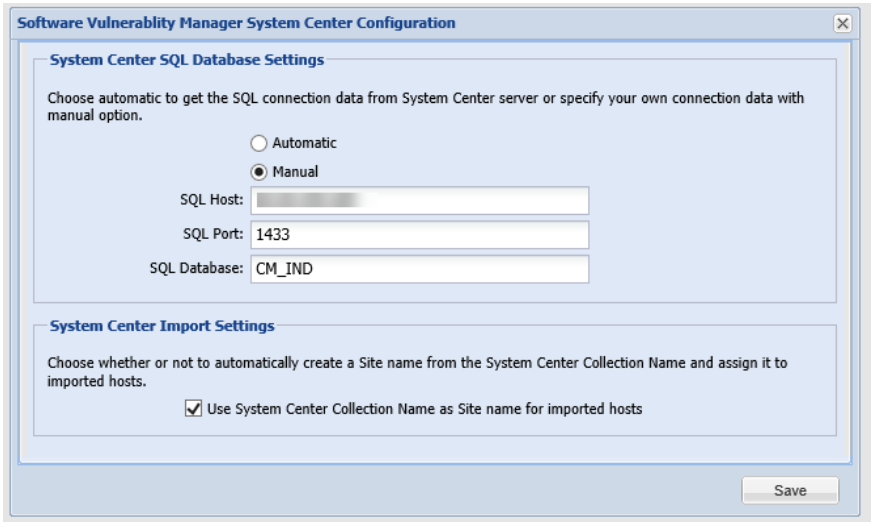
- **Increasing the software inventory file size**—In addition, you might want to consider increasing the software inventory file size from the default of 5 MB to 12 MB. To accomplish this, change the following registry key on the System Center Server:

  `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.



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

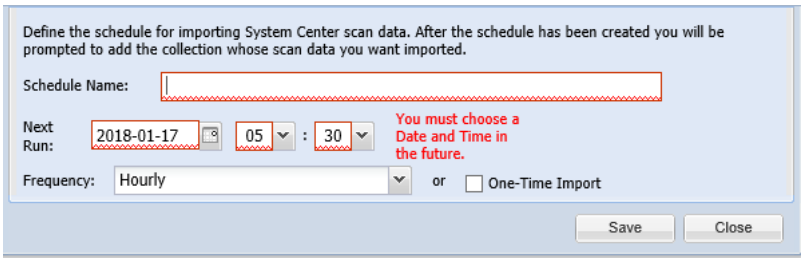
scan performed by the System Center integration and the csia. It may also result in some products not being detected correctly. For higher quality scan results Flexera recommends using the csia.

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.

3. 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>

4. 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.
5. 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`).
6. Install the `csia.exe` via the command line: `Start cmd with run-as-admin`.
7. 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`
8. 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` 120 would mean that the scanning agent will start scanning after a delay of random minutes, which could be from 1 to 120 minutes.

Agent Configuration Options

The following table lists the Agent configuration options.

Table 6-1 • Agent Configuration Options

Configuration Option	Description
Program Options:	
-A/--network-appliance	Run in Network Appliance mode.
-c/--cli	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
-d <path> --debug <path>	Write diagnostic information to the specified file.
--getfileinfo <path>	Directory for output file
-h/--help	Display this message and exit.
-n/--checkin-interval <interval>	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
-o/--outdir <path>	Directory for output file
-oc/--output-csv <file>	Output inspection results to a CSV file.
-ox/--output-xml <file>	Output inspection results to an XML file.
-si/--scantime_interval <minutes>	Set a random range to delay running software inspection. 0 means no random range, or 1-60 minutes.
--skip-wait/--skipwait	Skip the initial 10 minute wait before the first check in.
-v --verbose	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.)

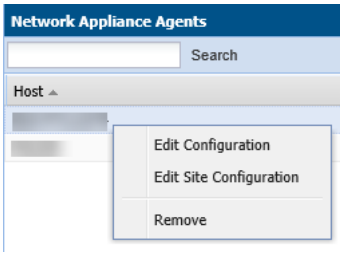
Configuration Option	Description
--manual	When installing, set service to only be started manually, rather than automatically
-N/--no-registry-write	When installing, do not write any settings to registry. When removing, do not delete settings from registry.
-p/--copy <dest>	Before installing, copy executable 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:

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 ***Note*** • *Scan Type 2 is the default scan type.*	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

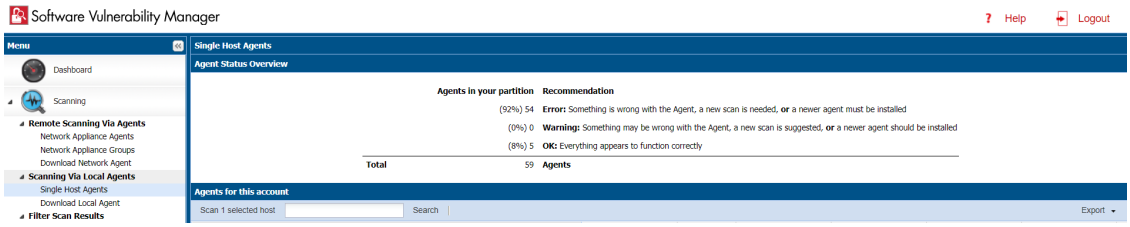
Single Host Agents

This page allows you to:

- Search for a site name to edit the configuration for agents joined to different sites.
- Manage configurations and schedule scans for the hosts where the Agent is installed as a service in Single Host mode.

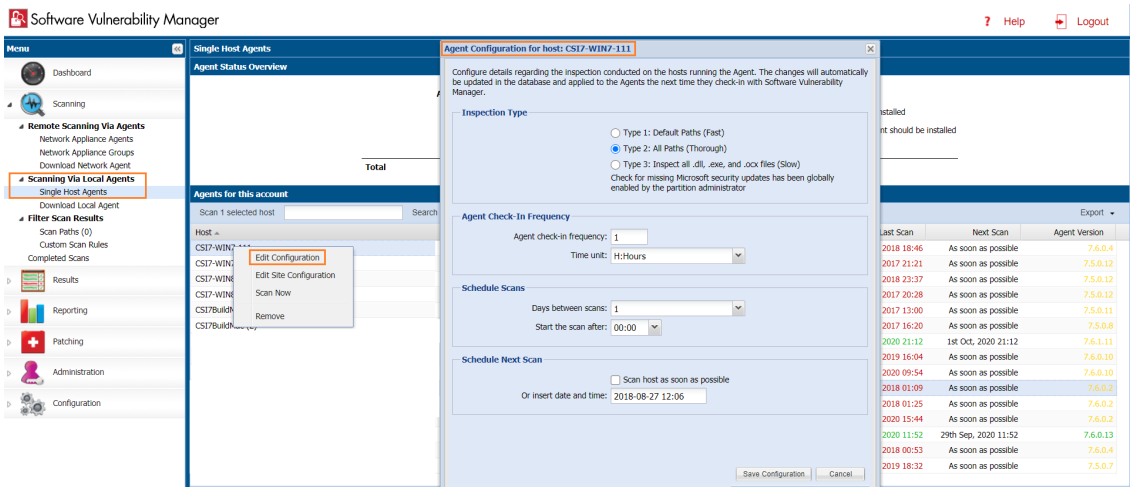
Task ***To search for a site name to edit the configuration for agents joined to different sites:***

1. Navigate to the **Single Host Agents** view.
2. In the **Scan 1 selected host** search box, enter the site name and host name using the “OR” condition to show the respective result.



Task ***To manage the configuration of the selected Agent and change its settings (Inspection type, Check-in frequency, Days between scans):***

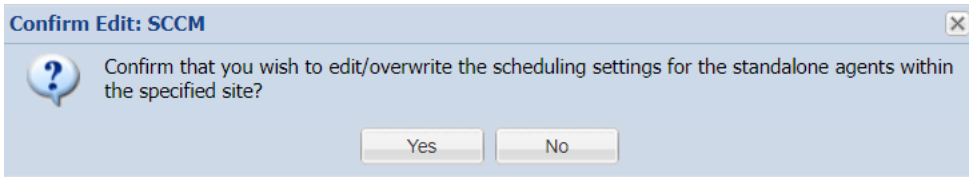
1. Double-click a host or Right-click a host name and select **Edit Configuration**. **Agent Configuration for host** wizard opens.



2. Change the below settings as required:
   - Inspection Type
   - Agent check-in frequency
   - Schedule Scans
   - Schedule Next Scan
3. Select **Save Configuration** to save the changes.

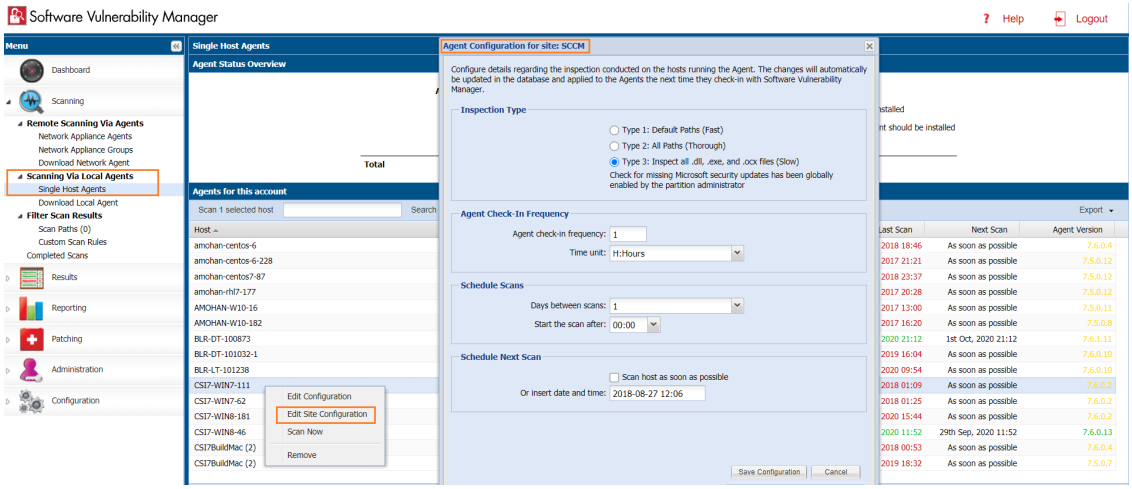
Task ***To manage the configuration of the selected Site and change its settings (Inspection type, Check-in frequency, Days between scans):***

1. Right-click a host name and select Edit Site Configuration to manage the configuration for all the hosts in that Site.
2. Select **Yes** in the **Confirm Edit** alert box.



3. **Agent Configuration for site** wizard opens, you can change the below settings as required:
   - Inspection Type
   - Agent check-in frequency
   - Schedule Scans
   - Schedule Next Scan

Note • *A Site is linked to multiple hosts, Edit Site configuration reflects the setting changes in all the hosts in that Site.*



4. Select **Save Configuration** to save the changes.

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.

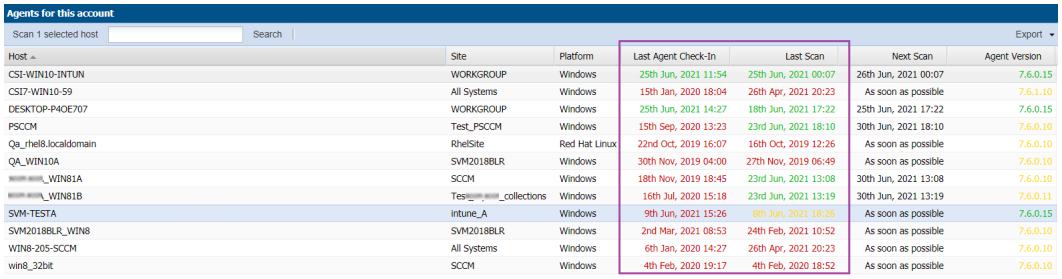
Note • *When the agent runs as a service agent, It reads CSIAUser, CSIAToken, CSIAHost, CSIAPort, ProxyURL, and other optional settings from registry HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Secunia\CSI Agent.*

When the agent runs manually from the command line, the agent reads only CSIAUser, CSIAToken, CSIAHost, and CSIAPort from the registry unless required settings are specified on the command line or embedded in the executable. Other optional settings such has ***ProxyURL*** *to be specified on the command line. The Agent doesn't read them from the registry.*

Note • *Flexera SPS page now available in non-IE browser also. In order to use complete feature of patching, need to install Software Vulnerability Manager Plugin.*

5. The color coding are as mentioned below:

- Last Agent Check-In
  - If date is more than 7 days (604800 seconds) => Red
  - If date is more than 1 day (86400 seconds) => Yellow
  - If date is less than 1 day => Green
- Last Scan
  - If date is more than 32 days (2764800 seconds) => Red
  - If date is more than 8 day (691200 seconds) => Yellow
  - If date is less than 8 day => Green



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
  - Macintosh OS X - 64bit

- Macintosh OS X - 32bit
- Red Hat Linux 7.x
- Red Hat Linux 6.x

The following Signed Agents are available:

- Download Signed Agents without Token
  - Microsoft Windows
  - Macintosh OS X - 64bit

Important • *Note the following for Signed Agents:*

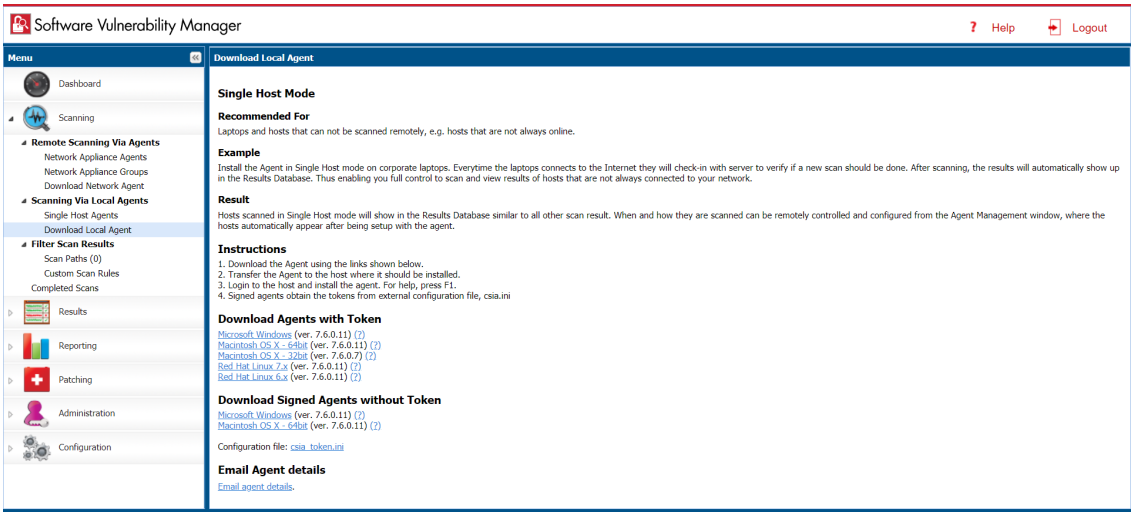
- *To install signed agent for Windows, download csia_token.ini and place it in the same folder where agent is saved.*
- *To install signed agent for MacOS, see Prepare Your Mac.*

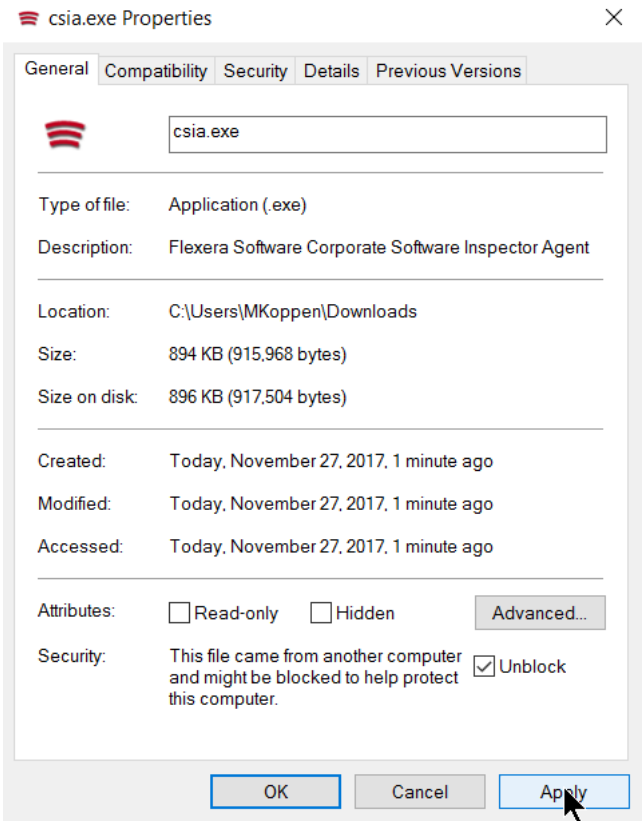
If your intention is to deploy the Software Vulnerability Manager Agent through WSUS/System Center please refer to Agent Deployment for further information.

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

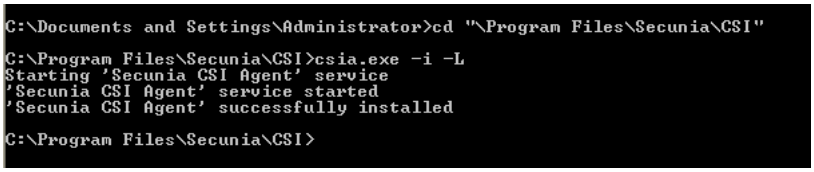
Hosts scanned with the Agent in Single Host mode will be displayed in **Results > Host Smart Groups**.

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:



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.*

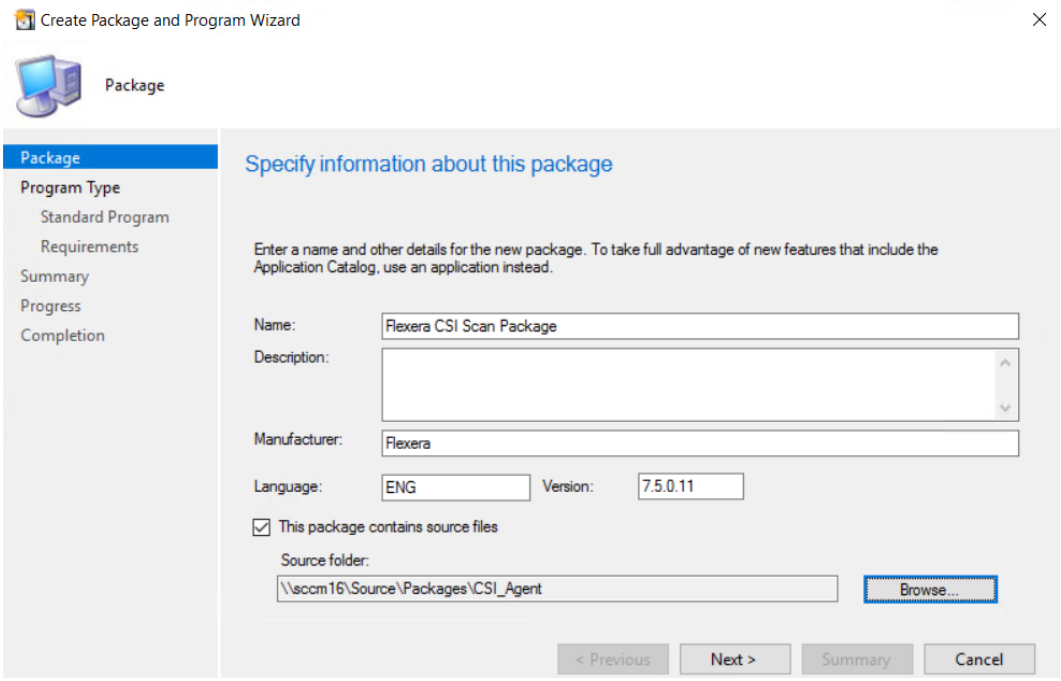
Once the Agent is installed it will automatically scan after ten minutes. You can also initiate an on demand scan by executing **csia.exe –c**.

Run Scan from System Center Configuration Manager (SCCM)

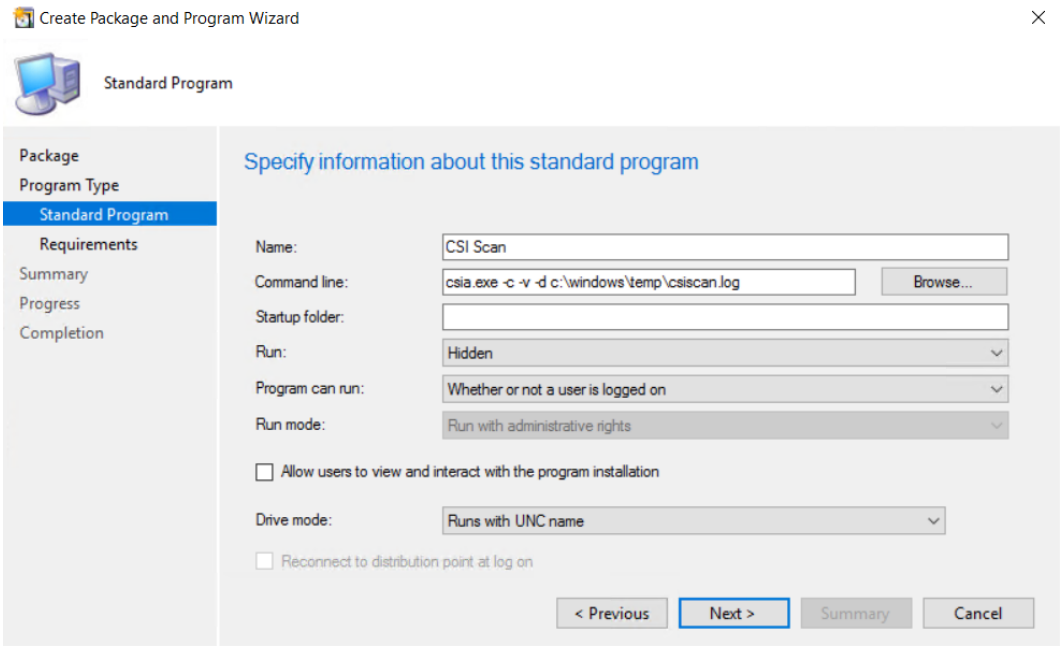
The Software Vulnerability Manager Agent does not have to be installed on the local host to do a scan. You can create a traditional package in SCCM and run the scan on a weekly basis. To do this, you first need to be able to connect to <your CSI on-prem server host name>.

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

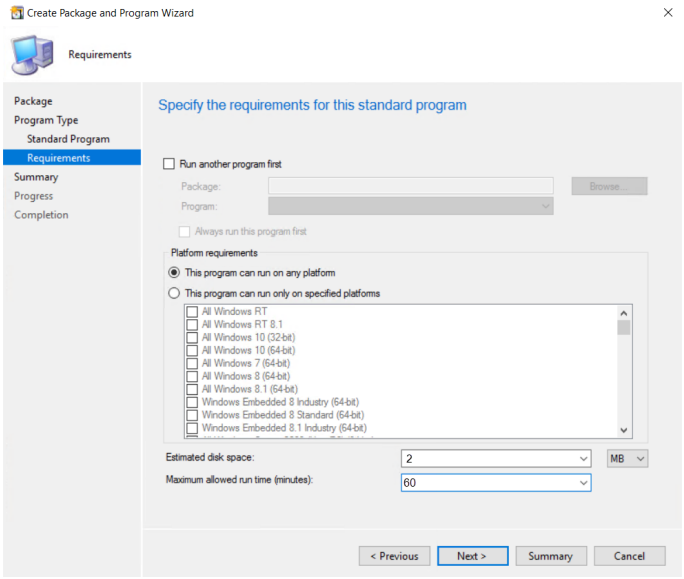
1. Download the latest Software Vulnerability Manager Agent as per Download Local Agent.
2. Launch the ConfigMgr console. Select **Software Library > Application Management > Packages**.
3. From the ribbon, click **Create Package**.
4. Complete the package information and click **Next**.



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 -si 120 -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**

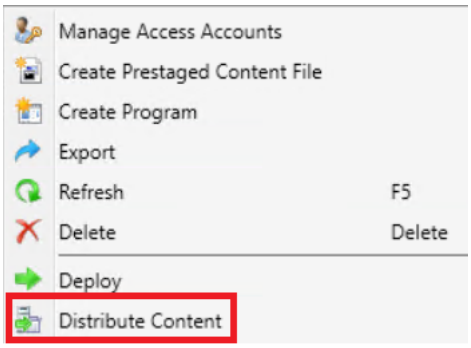


7. On the **Requirements** page, complete the requirements as shown below and click **Next**.



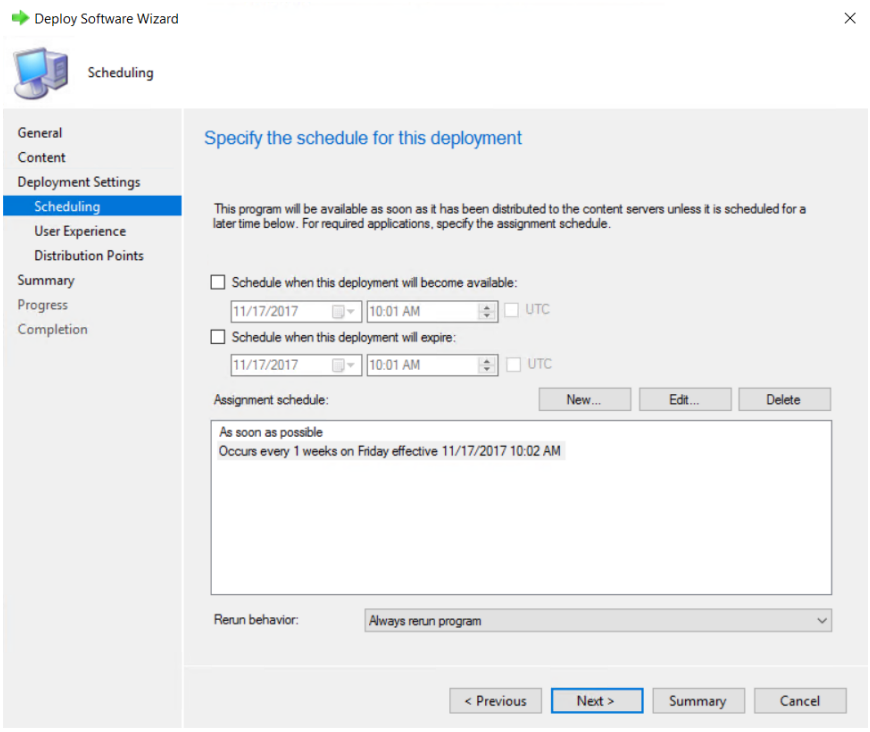
8. Finish the wizard.

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:***

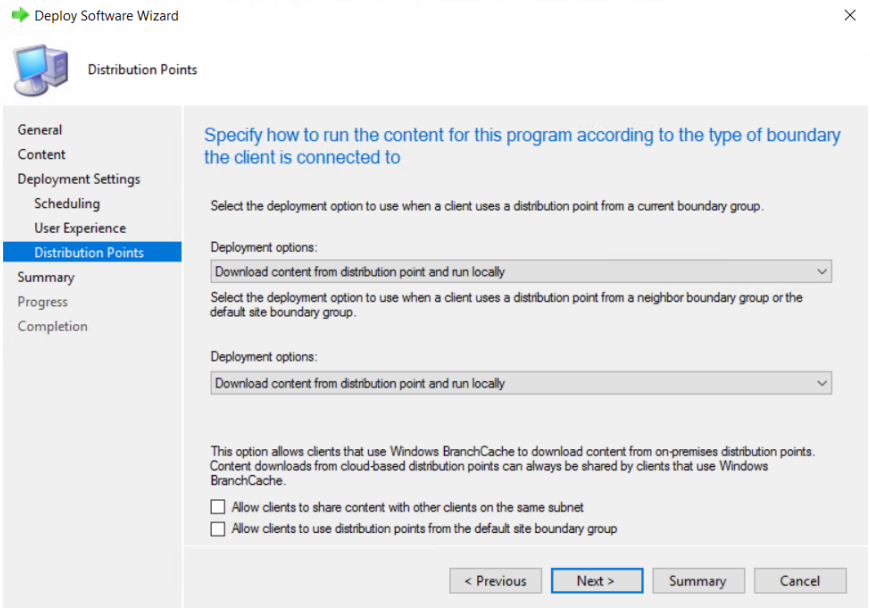
1. Select the Package and click **Deploy** on the ribbon.
2. On the **General** page, select the target collection and click **Next**.
3. On the **Content** page, verify that the content is distributed and click **Next**.
4. On the **Deployment Settings** page, ensure the purpose is Required and click **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**.



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.

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

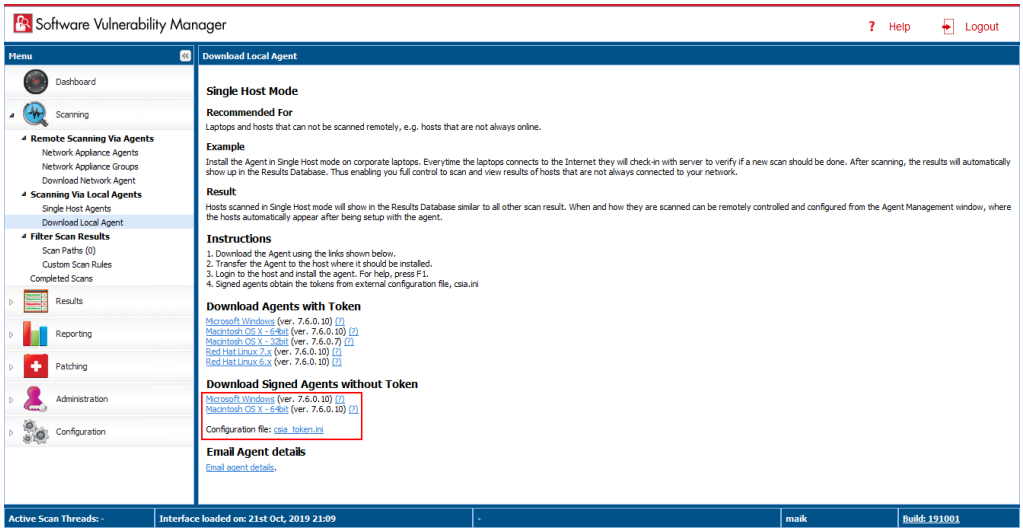
In case the permissions do not include execute rights (the '**x**' character) for any user, you should set them for the root account by using the **chmod +x** command.

```
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, procps, coreutils, glibc(x86-32), libcurl(x86-32), libconfig(x86-32), libuuid(x86-32), yum, yum-security

The RHEL 7 Agent requires: bash, sed, gawk, procps, 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

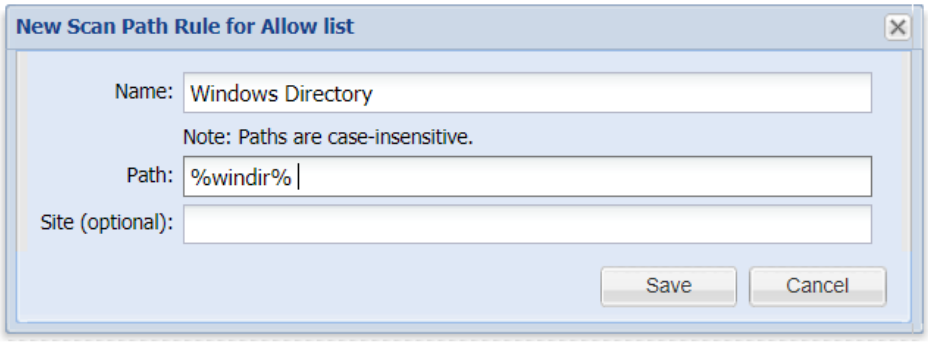
Use this feature to create either a Allow list or Block list of paths/locations to restrict the locations inspected by the Software Vulnerability Manager scan.

You can add environment variables to the Allow list and Block list in the Scan Paths view. The environment variables will be resolved to the full path by the windows agent while scanning a host and will appropriately be either scanned or skipped.

For Example:

If **%windir%** is added to the Block list in the Scan Paths, then the agent will skip **C:\Windows** folder and its subfolders while scanning a host.

Click Add Allow list Rule or Add Block list Rule and enter the Name, Path and Site (optional) details.



Important • *This feature is not applicable to RHEL.*

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

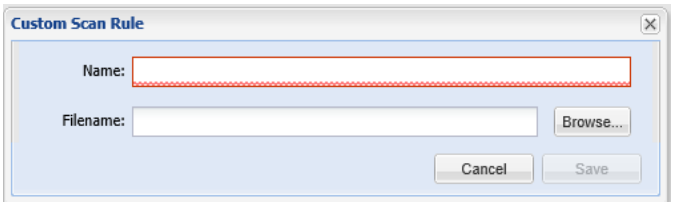
If using the Block list, all the locations/paths block-listed will be ignored and any other paths are inspected by the Software Vulnerability Manager scan.

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 Block list and a Allow list.*

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.

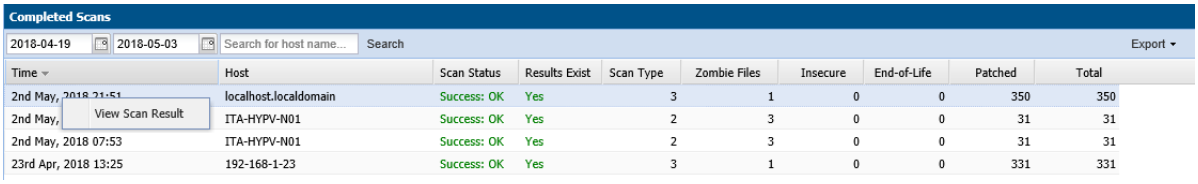


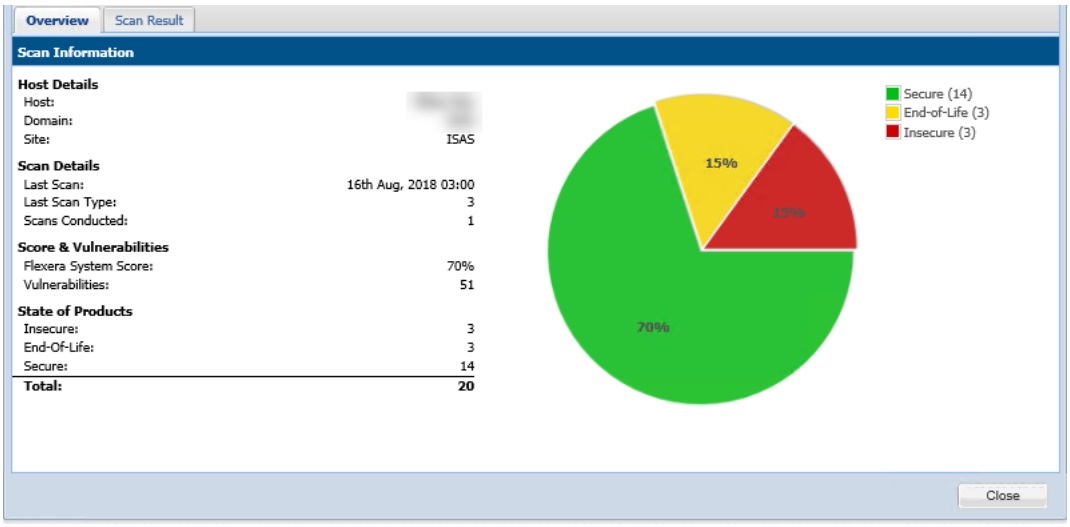
Right-click a rule in the grid to edit or delete the rule.

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	The scan was partially successful. An error occurred during the Windows update check due to possibly one or all of the following reasons: **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. NOTE: This means that certain Microsoft products for this Host are listed with a potential incorrect security state.
Failure	Scan failed.
Failed: License Limit Reached	You have reached the limit of your CSI License Key. To resolve this issue: **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	The scan started, but it could not be completed due to possibly one or all of the following reasons: **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.

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

Scan Status	Possible Reasons
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.
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.

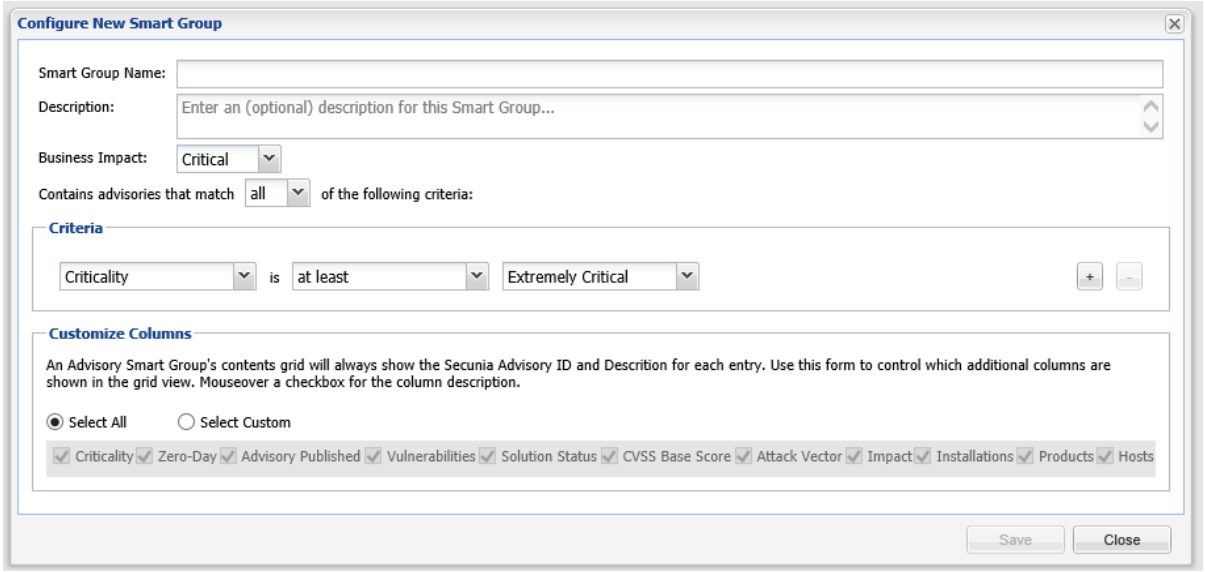
Note • *Smart Groups are generated periodically, and the data you see is only as current as the last time the Smart Group was compiled. At any time you can queue the recompilation of a Smart Group to get the most current data.*

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.



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:

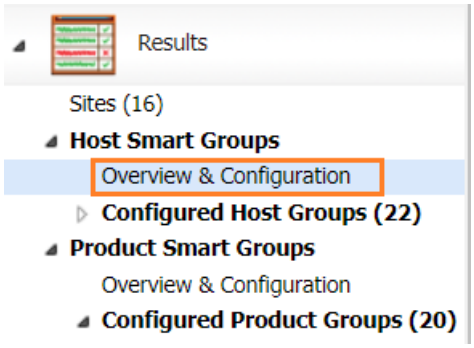
- Create a New Host Smart Group (see Create a New Host Smart Group)
- View existing configured Host Smart Groups (see Overview and Configuration)
- Configure new Host Smart Groups (see Configured Host Smart Groups)
- Cross-Reference Host Smart Group Values - User Interface Versus CSV File (see)
- Filter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

Create a New Host Smart Group

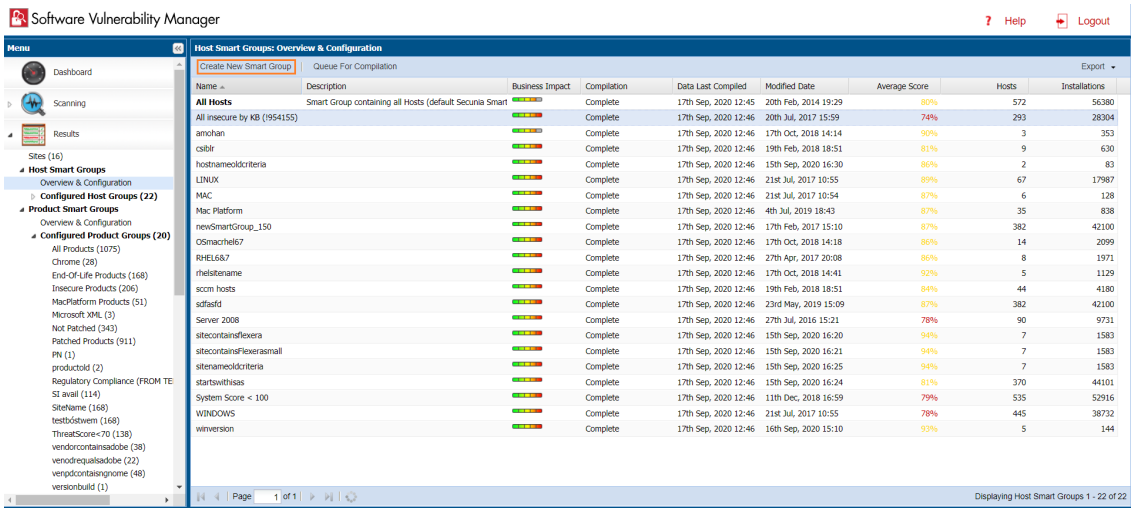
This page describes how to create a new Host Smart Group.

Task ***To create a new Host Smart Group:***

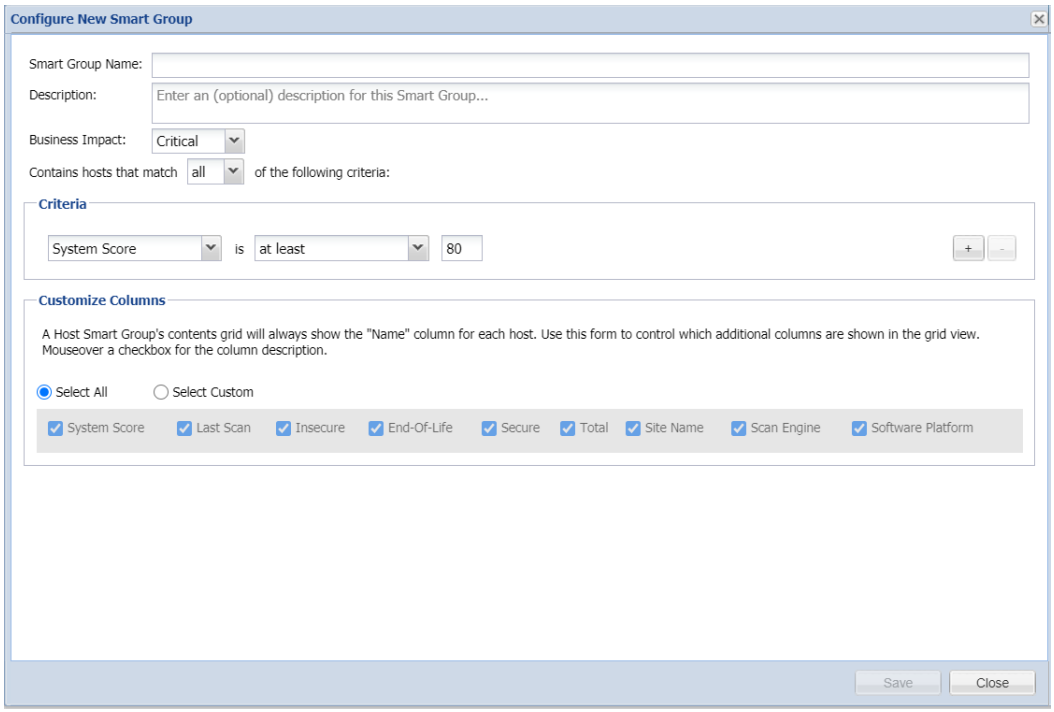
1. Navigate to **Host Smart Groups** > **Overview & Configuration**.



2. A list of created Host Smart Groups appears. To create a new Smart Group, click **Create New Smart Group** link.



3. **Configure New Smart Group** dialog box opens.



4. Enter the valid name in the **Smart Group Name** field.
5. Enter the description of the smart group (optional) in the **Description** field.
6. From the **Business Impact** list, select the type of impact you want to add. You have the following options:

Table 7-1 • Business Impact list

Impact Type	Description
Critical	This value is typically used for remotely exploitable vulnerabilities that can lead to system compromise. It resembles the red color.
High	This value is typically used for remotely exploitable vulnerabilities that can lead to system compromise. It resembles the orange color.
Medium	This value is typically used for remotely exploitable Denial of Service vulnerabilities and for vulnerabilities that allow system compromises but require user interaction. It resembles the yellow color.
Minor	This value is typically used for cross-site scripting vulnerabilities and privilege escalation vulnerabilities. It resembles the light green color.
Low	This value is typically used for very limited privilege escalation vulnerabilities and locally exploitable Denial of Service vulnerabilities. It resembles the green color.

7. From the Criteria list, select the type of smart group criteria you want to add. You have the following options:

Table 7-2 • Smart Group Criteria Options

Smart Group Criteria	Description
System Score	Filter by system score.
System Platform	Filter by system platform.
Last Scan Date	Filter by last scan date of the host.
Site	Filter by site name.
Host	Filter by host name.
Missing KB Article	Filter hosts with missing Microsoft KB article.
CVE Number	Filter host by CVE Number from selected CVE list.
Host Name	Filter host name using begins with, starts with, and contains condition. This filter supports options like **contains**, **starts with**, and **equals**. Then enter the Host name in the text field.
Site Name	Filter site name using begins with, starts with, and contains condition. This filter supports options like **contains**, **starts with**, and **equals**. Then enter the Site name in the text field.
Operating System	Filter by operating system from selected list.
Operating System Build	Filter by specific version of the Operating System. For more details, see Filter Host Smart Groups on Operating System Build Version.

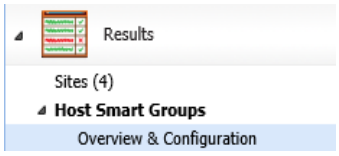
8. After updating the above fields, click **Save** button to create a new Host Smart Group.

Overview and Configuration

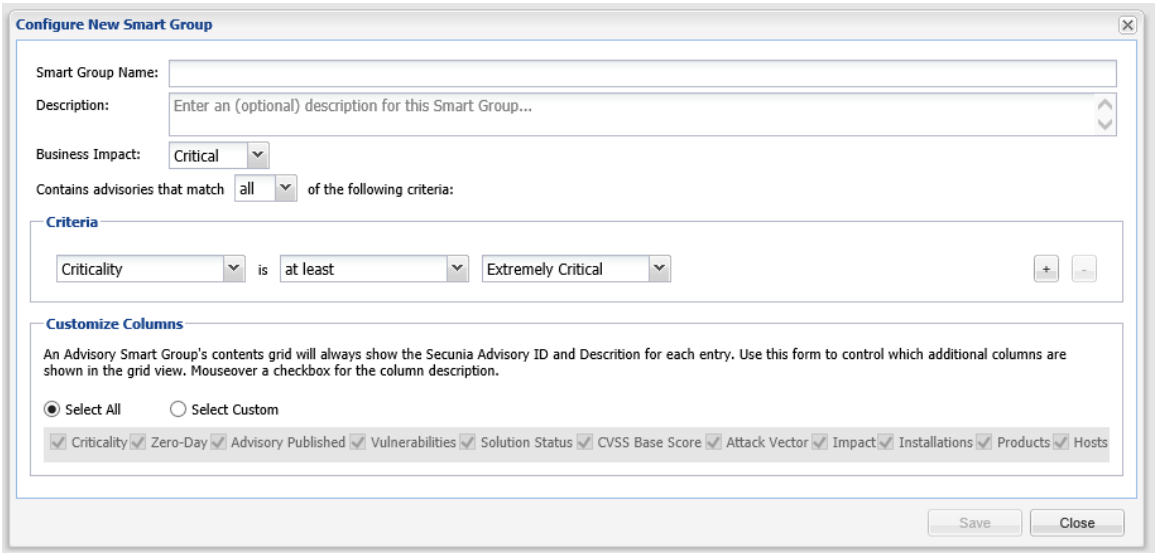
This page describes how to view existing configure Host Smart Groups and to configure new Host Smart Groups.

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

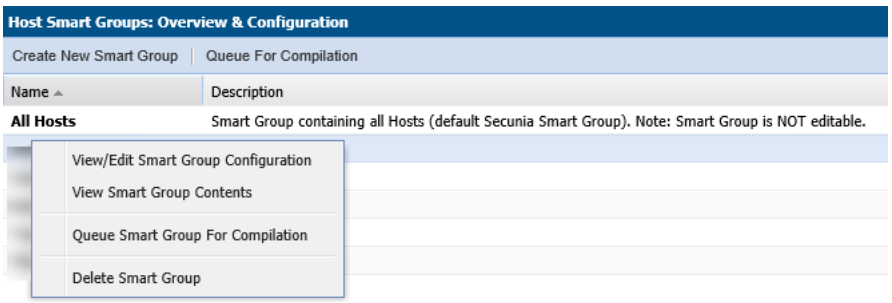
1. Navigate to Host Smart Groups Overview & Configuration.



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.

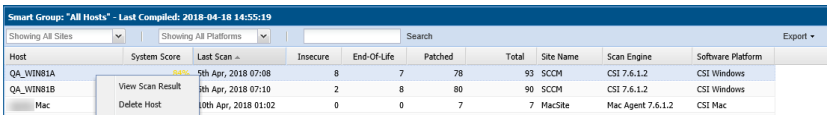


Note • *All Hosts is the default Smart Group and cannot be edited or deleted.*



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.

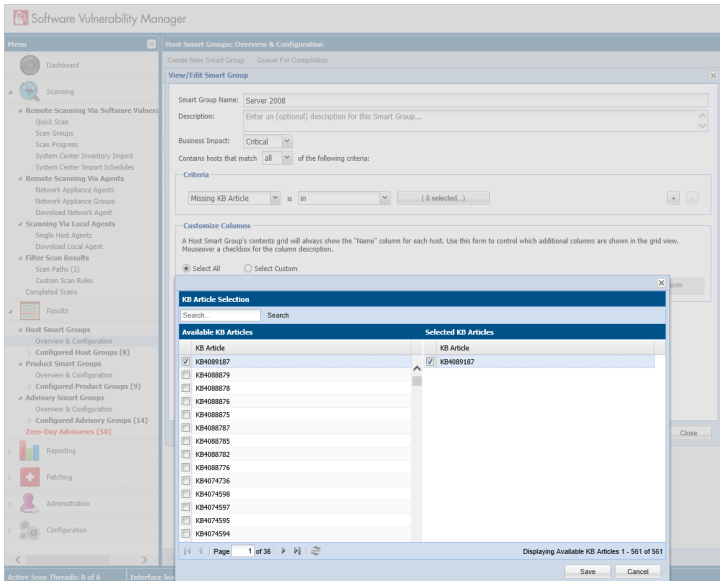


Filter Host Smart Groups on missing Microsoft Knowledge Base (KB) articles

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**.

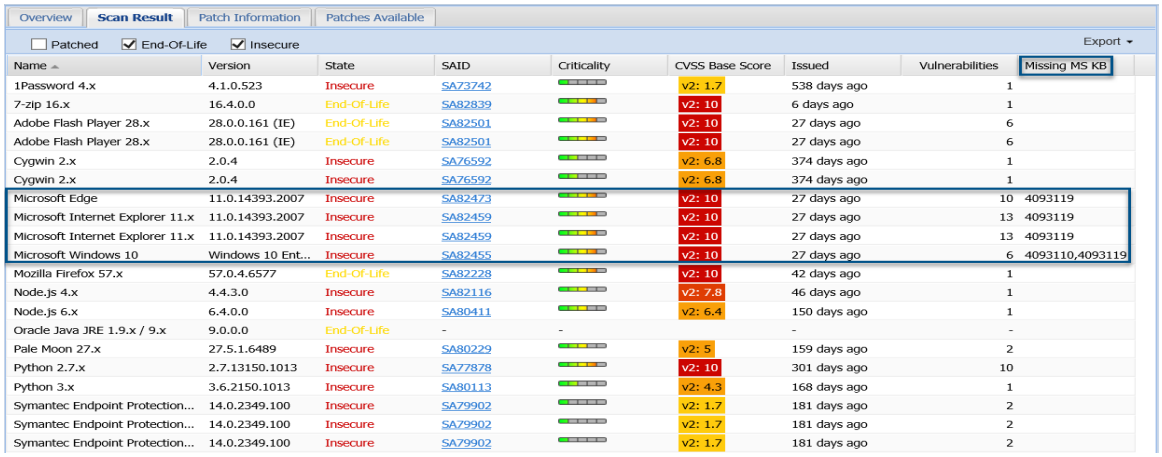


Important • *The following conditions affect the availability of selecting and listing missing Microsoft KB's.*

- *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.



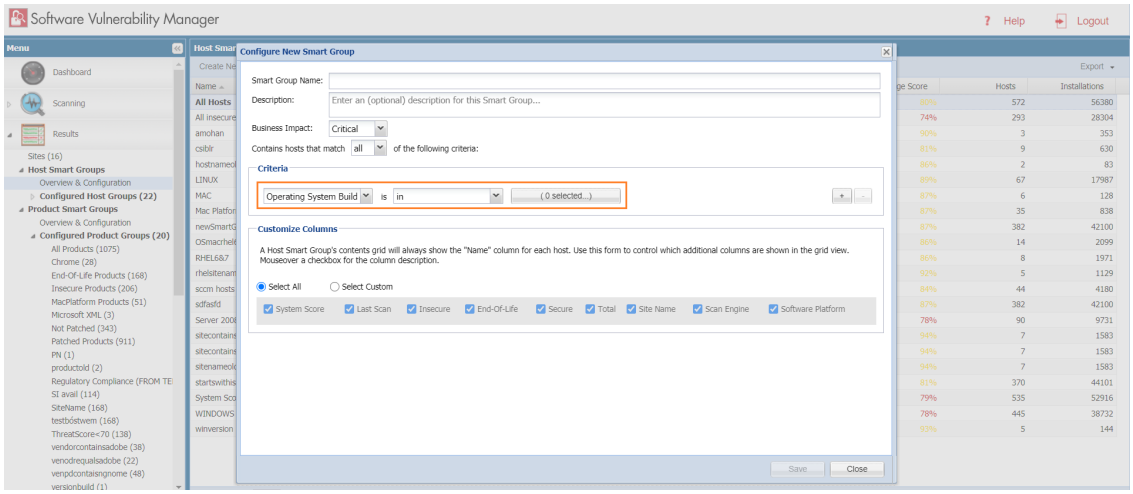
Name	Version	State	SAID	Criticality	CVSS Base Score	Issued	Vulnerabilities	Missing MS KB
1Password 4.x	4.1.0.523	Insecure	SA73742		v2: 1.7	538 days ago	1	
7-zip 16.x	16.4.0.0	End-Of-Life	SA82839		v2: 10	6 days ago	1	
Adobe Flash Player 28.x	28.0.0.161 (IE)	End-Of-Life	SA82501		v2: 10	27 days ago	6	
Adobe 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	

Filter Host Smart Groups on Operating System Build Version

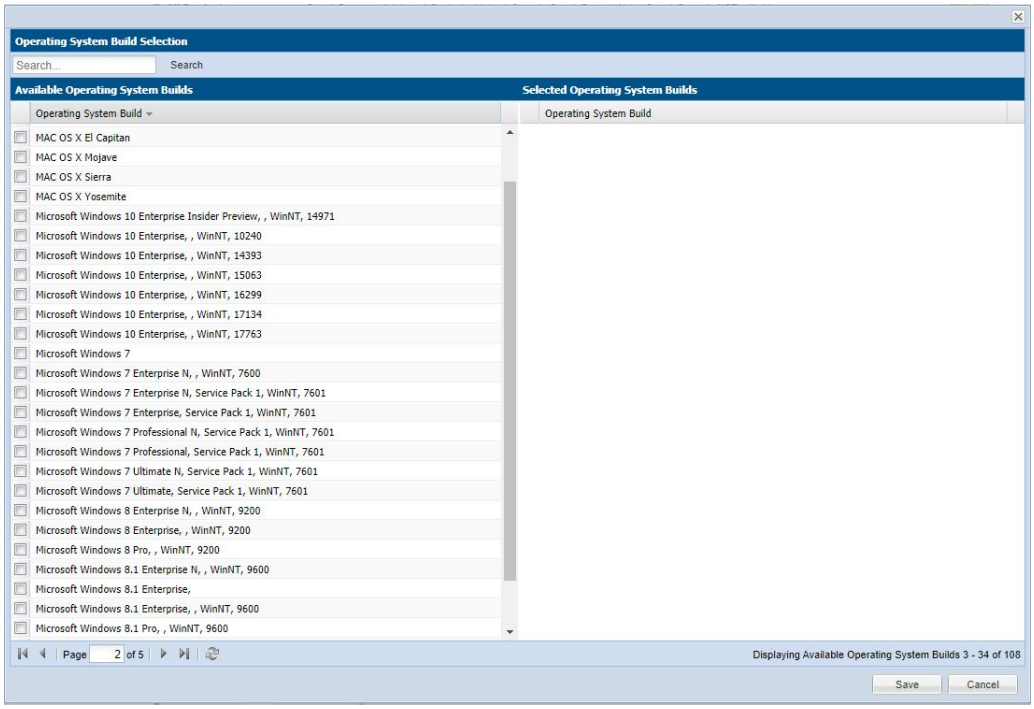
One option for filtering Host Smart Group information is by Operating System Build. This filtering can be used for new or existing Host Smart Groups.

Task ***To create a new Host Smart Group for Operating System Build:***

1. Navigate to **Host Smart Groups** > **Overview & Configuration**.
2. In the **Criteria** field, select the **Operating System Build** and the appropriate **in** or **Not in** option.



3. In the **Operating System Build Selection**, search for the available Operating System Builds.
4. Place a check mark in front of the appropriate Operating System Builds to include in the Host Smart Group and click **Save**.



Product Smart Groups

This section describes how to:

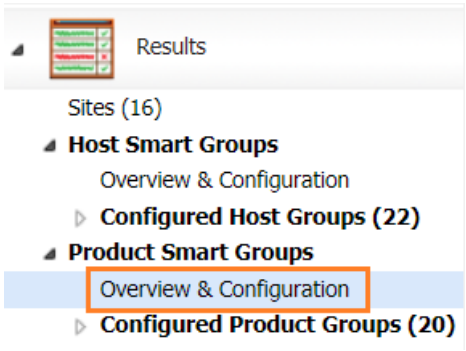
- Create a new Product Smart Group (See Create a New Product Smart Group)
- View existing configured Product Smart Groups (see Overview and Configuration)
- Configure new Product Smart Groups (see Configured Product Smart Groups)

Create a New Product Smart Group

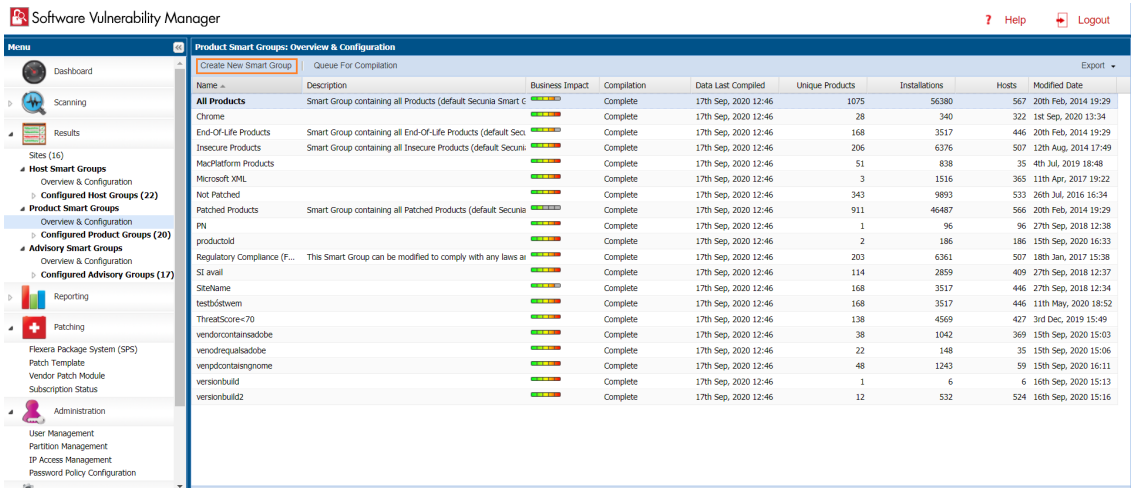
This page describes how to create a new Product Smart Group.

Task ***To create a new Product Smart Group:***

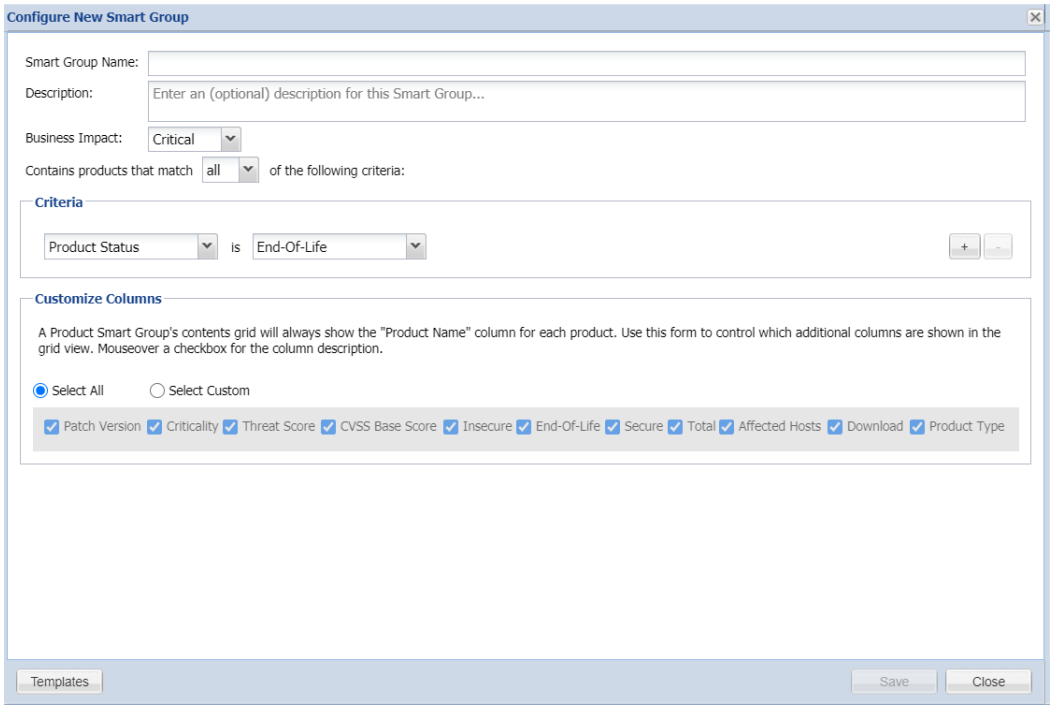
1. Navigate to **Product Smart Groups** > **Overview & Configuration**.



2. A list of created Product Smart Groups appears. To create a new Smart Group, click **Create New Smart Group** link.



3. **Configure New Smart Group** dialog box opens.



4. Enter the valid name in the **Smart Group Name** field.
5. Enter the description of the smart group (optional) in the **Description** field.
6. From the **Business Impact** list, select the type of impact you want to add. You have the following options:

Table 7-3 • Business Impact list

Impact Type	Description
Critical	This value is typically used for remotely exploitable vulnerabilities that can lead to system compromise. It resembles the red color.
High	This value is typically used for remotely exploitable vulnerabilities that can lead to system compromise. It resembles the orange color.
Medium	This value is typically used for remotely exploitable Denial of Service vulnerabilities and for vulnerabilities that allow system compromises but require user interaction. It resembles the yellow color.
Minor	This value is typically used for cross-site scripting vulnerabilities and privilege escalation vulnerabilities. It resembles the light green color.
Low	This value is typically used for very limited privilege escalation vulnerabilities and locally exploitable Denial of Service vulnerabilities. It resembles the green color.

7. From the **Criteria** list, select the type of smart group criteria you want to add. You have the following options:

Table 7-4 • Product Smart Group Criteria Options

Smart Group Criteria	Description
Product Status	Filter by product status.
Criticality	Filter by criticality.
Threat Score	Filter by threat scores.
SAID Creation Date	Filter by SAILD creation date.
Last Scan Date	Filter by last scan date of the host.
Silent Installation	Filter by silent installation.
Site	Filter by site name.
Host	Filter by host name.
Product	Filter by product name.
System Platform	Filter by system platform.
Software Type	Filter by software type.
CVSS2 Score	Filter by CVSS2 score.
CVSS3 Score	Filter by CVSS3 score.
Product Name	Filter product name using **begins with**, **starts with** and **contains** condition. Then enter the Product name in the text field
Host Name	Filter host name using **begins with**, **starts with** and **contains** condition. Then enter the Host name in the text field.
Site Name	Filter site name using **begins with**, **starts with** and **contains** condition. Then enter the Site name in the text field.
Vendor Name	Filter vendor name using **begins with**, **starts with** and **contains** condition. Then enter the Vendor name in the text field.
Operating System	Filter by operating system from selected list.
Operating System Build	Filter by specific version of the Operating System. Fore more information, see Filter Product Smart Groups on Operating System Build Version.

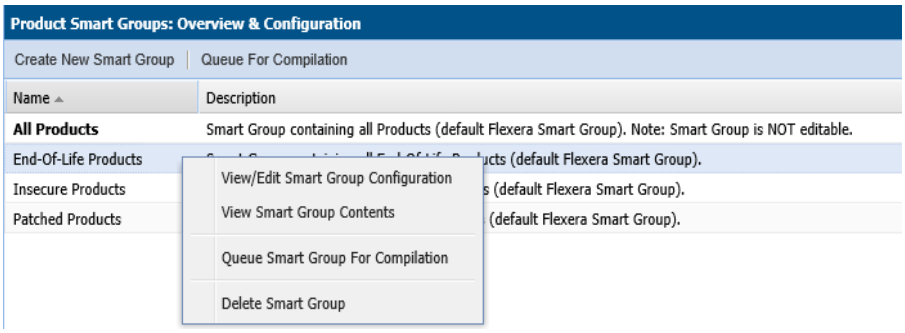
8. After updating the above fields, click **Save** button to create a new Product Smart Group.

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.

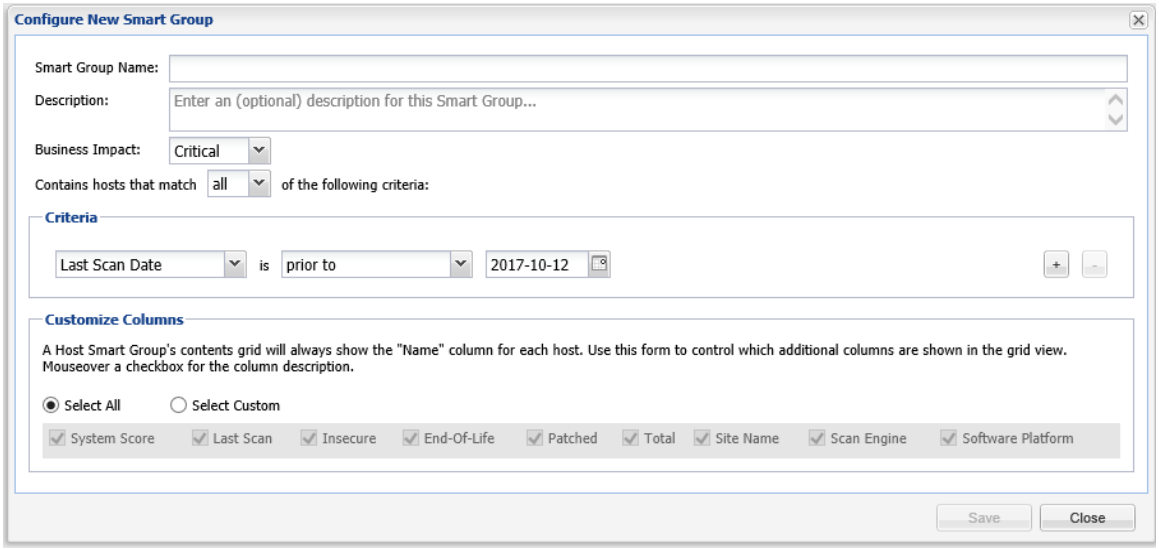
The other default Smart Groups for End-Of-Life Products, Insecure Products, and Patched Products have been pre-created for you by Flexera. You can right-click to view, edit, compile or delete these Smart Groups.



Last Scan Date for Product Smart Groups

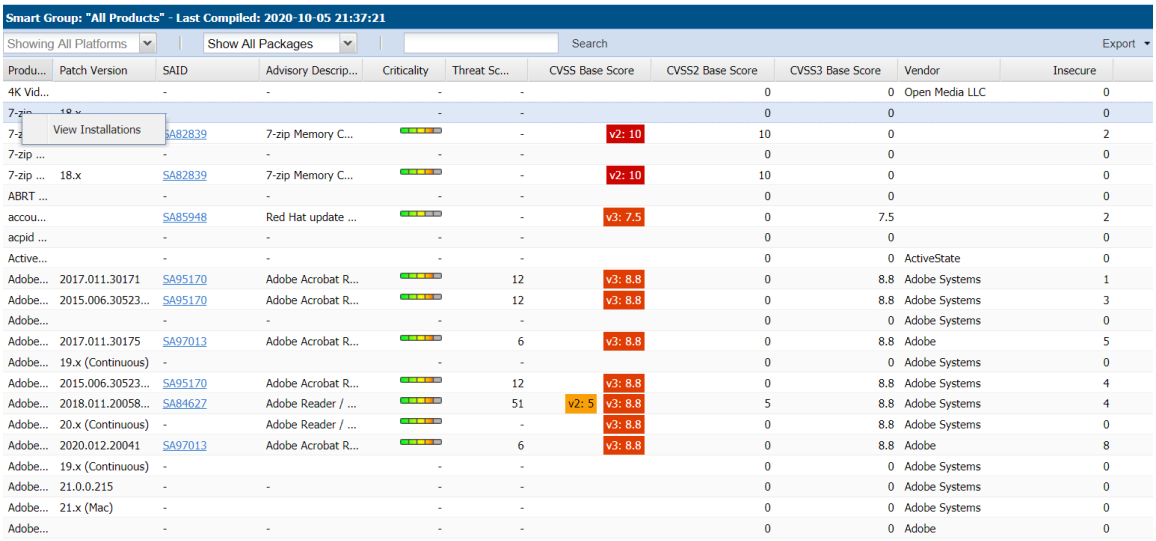
Product Smart Groups can be filtered by **Last Scan Date**. This filter option lists products that were detected within a specified time interval using one of the following Last Scan Date options: exactly, prior to, after, older than, and within last.

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.

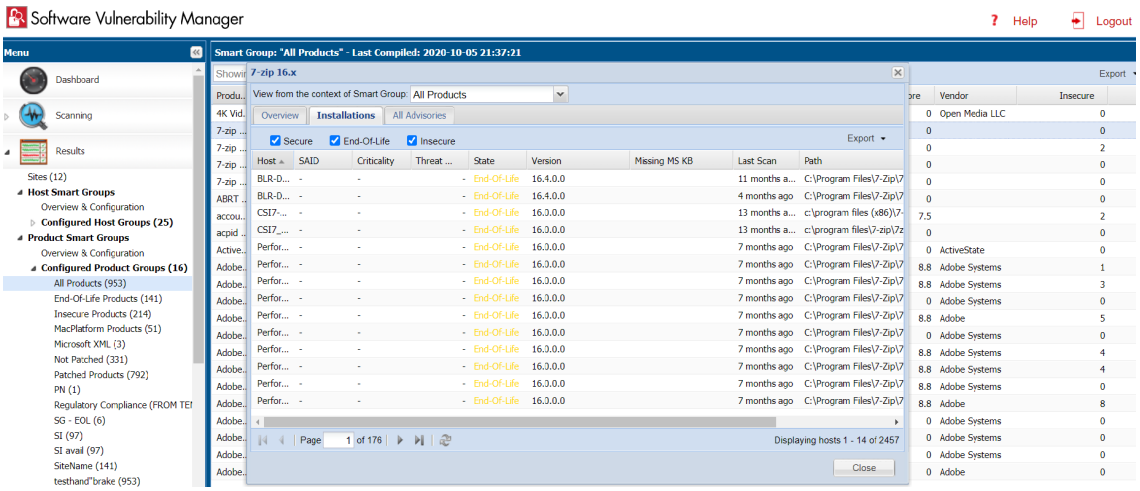


Configured Product Smart Groups

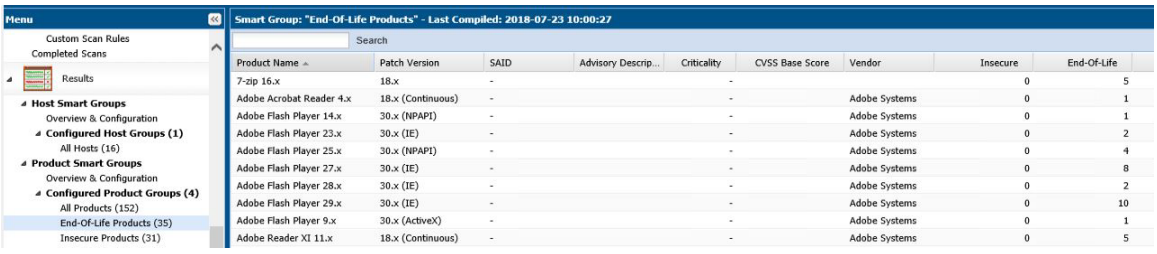
Use this page to view the information for each Product Smart Group you created. Right-click an item in the grid and select **View Installations** to display the installation details.



A dialog box opens with the installation details of the selected item.



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

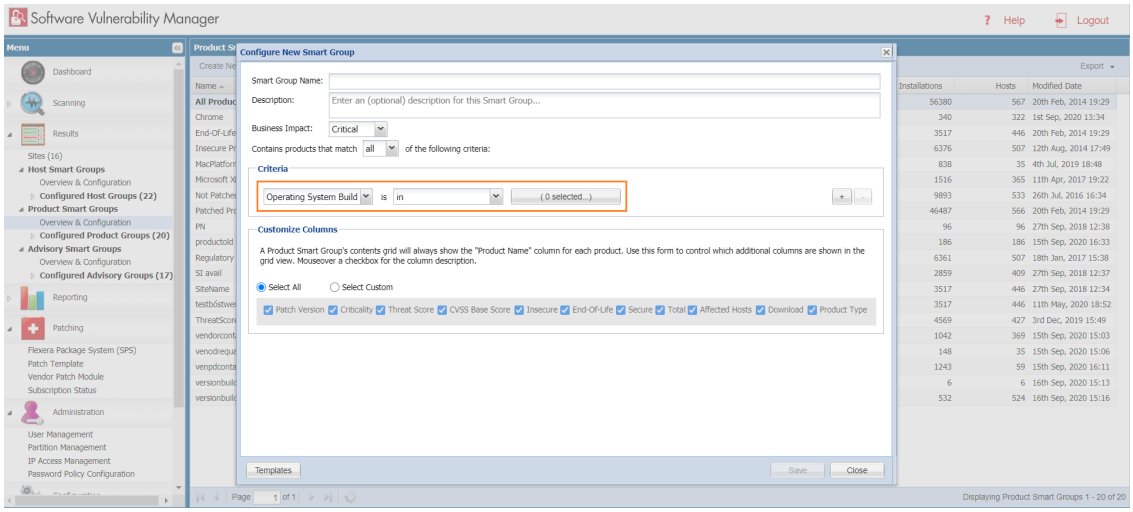


Filter Product Smart Groups on Operating System Build Version

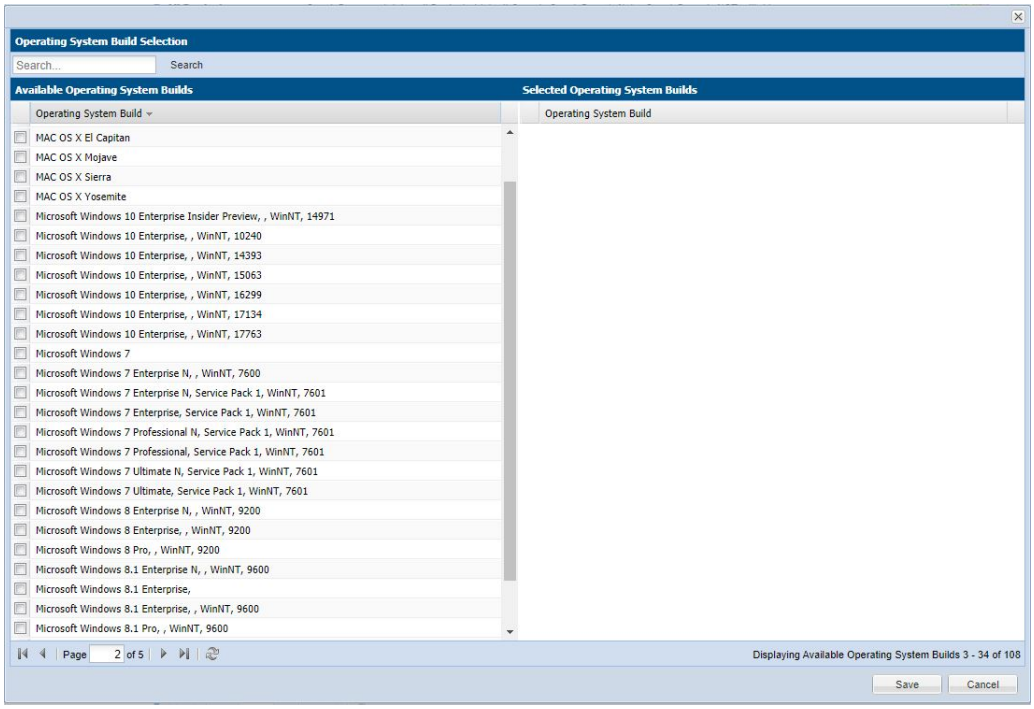
One option for filtering Product Smart Group information is by Operating System Build. This filtering can be used for new or existing Product Smart Groups.

Task ***To create a new Product Smart Group for Operating System Build:***

1. Navigate to **Product Smart Groups** > **Overview & Configuration**.
2. In the **Criteria** field, select the **Operating System Build** and the appropriate **in** or **Not in** option.



3. In the **Operating System Build Selection**, search for the available Operating System Builds.
4. Place a check mark in front of the appropriate Operating System Builds to include in the Product Smart Group and click **Save**.



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)

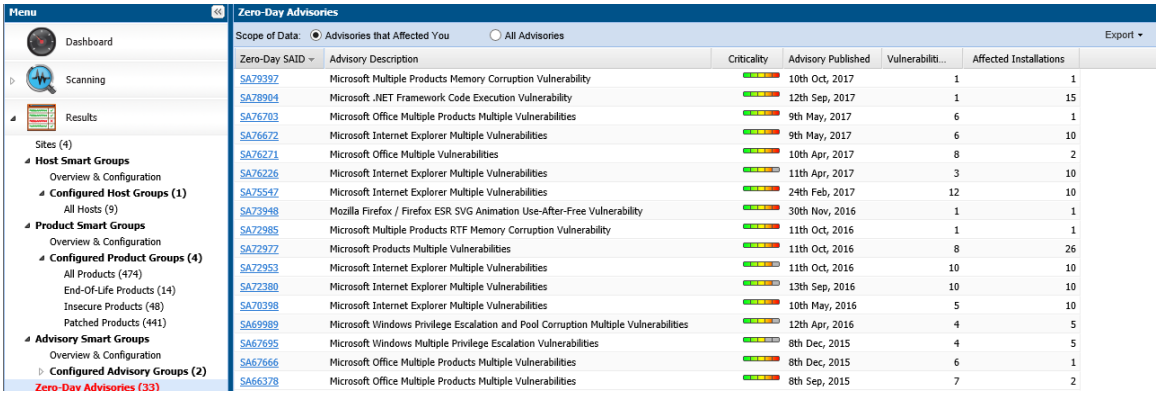
Overview and Configuration

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.

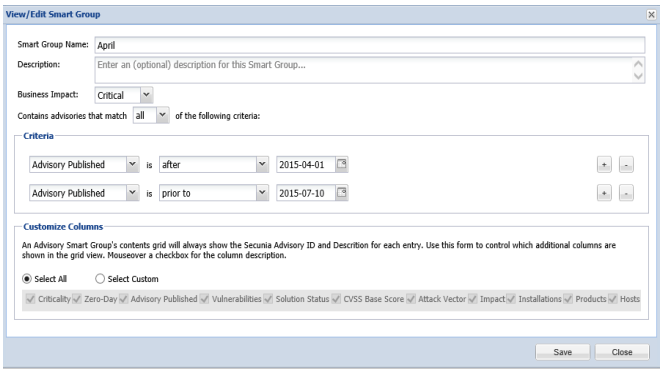
Zero-Day Advisories reference a vulnerability that is actively exploited prior to its disclosure. These advisories can be filtered by **Advisories that Affected You** and **All Advisories**.



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.

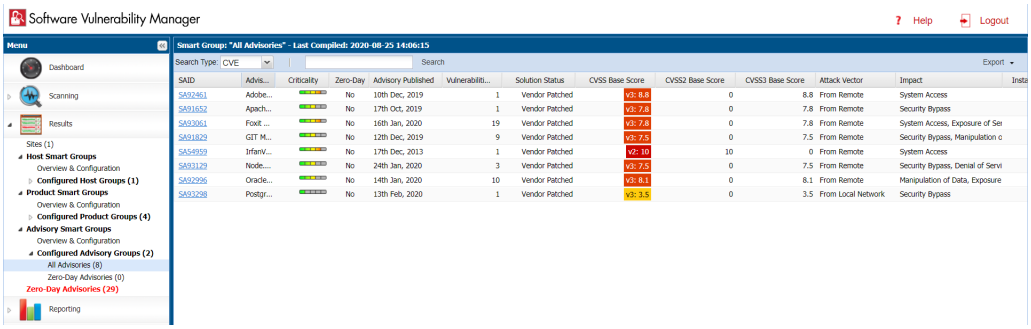
In the **View/Edit Smart Group** menu, you can filter results by date for the following criteria: Advisory Published, Last Scan Date, and Secunia Advisory ID (SAID) Creation Date. This filtering by date creates a list of all Advisories published on that date.



Configured Advisory Smart Groups

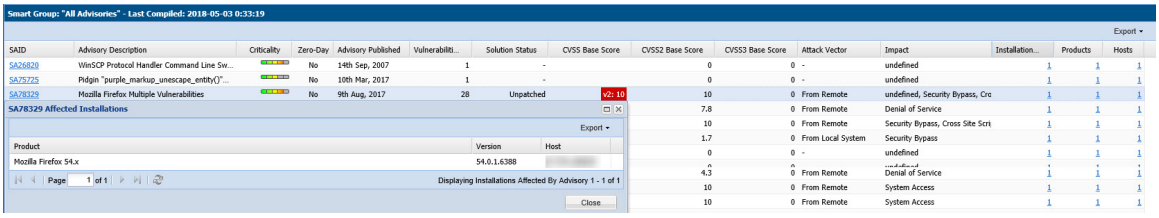
Use this page to view the information for each Advisory Smart Group you created. Click a Secunia Advisory ID **(SAID)** in the grid to display the details. For further details, see View All Advisories.

Note • *you can search Advisory either by CVE, SAID, or Description.*

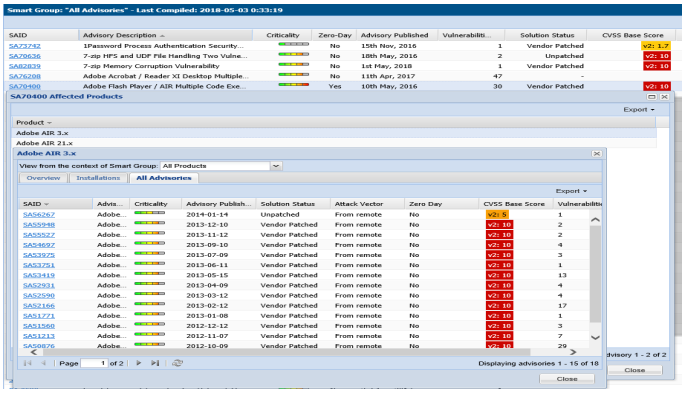


View All Advisories

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.



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.



8

Reporting

This chapter describes the following Software Vulnerability Manager reporting features:

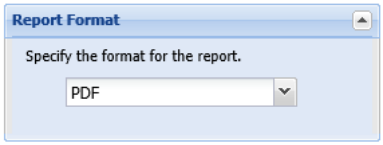
- Report Configuration
- Smart Group Notifications
- Activity Log Notifications
- Database Access
- Scheduled Exports

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.

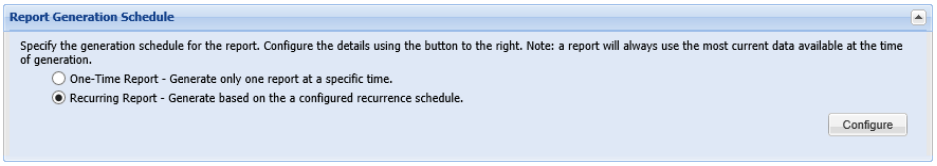
Task ***To configure a report:***

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

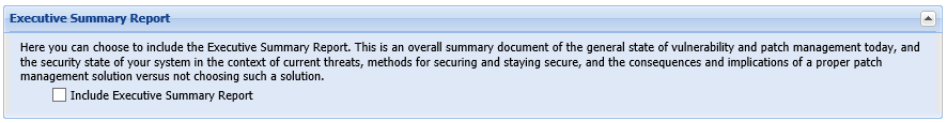


Note • *When using the CSV option for the report format, unused options are disabled. For more information, see Select the CSV Option for the Report Format.*

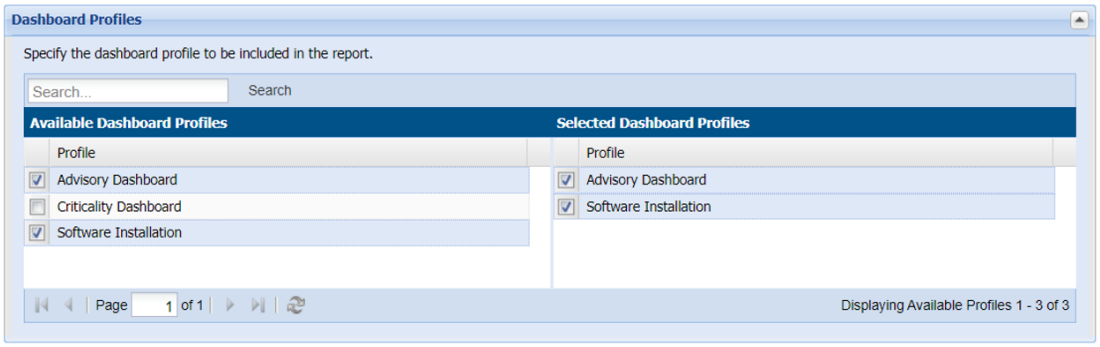
2. Choose between a One-time only report or a recurring one (daily, weekly, monthly) and click **Configure** to select the report distribution date or frequency schedule.



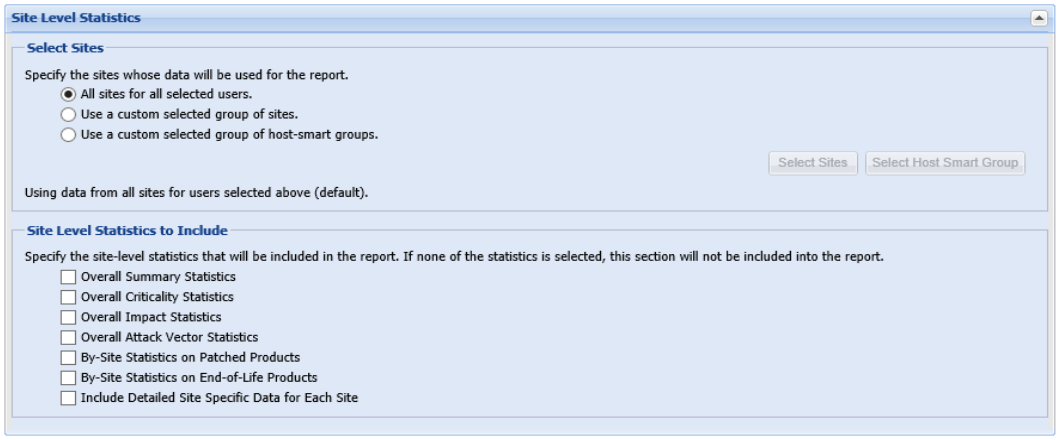
3. Choose to include the Executive Summary Report which provides an overall summary with the general state of vulnerability and patch management.



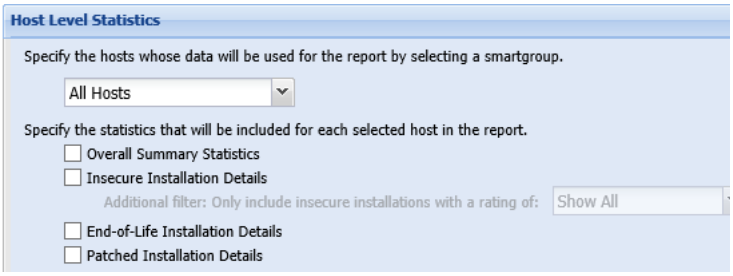
4. Choose the dashboard profile to be included in the report.



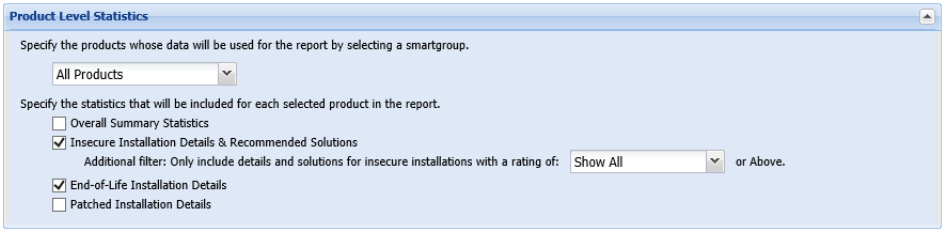
5. Choose which sites should be included together with which statistics to include.



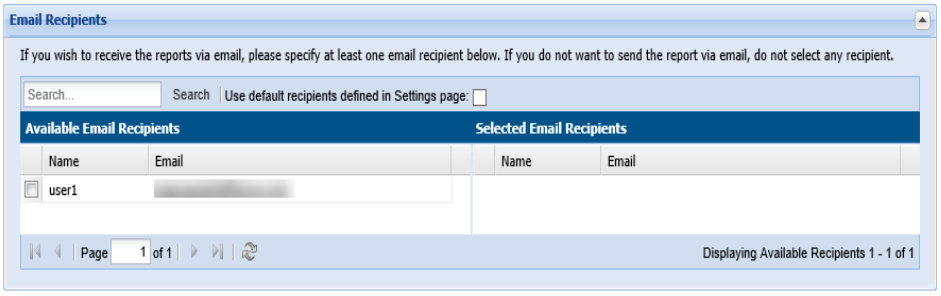
6. Choose a Host Smart Group to be included together with which statistics to include.



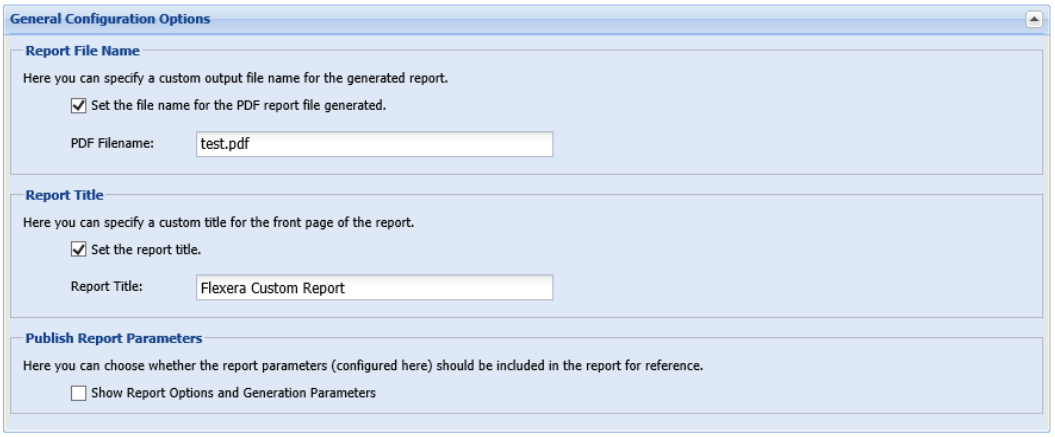
7. Choose a Product Smart Group to be included together with which statistics to include.



8. 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.



9. 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.

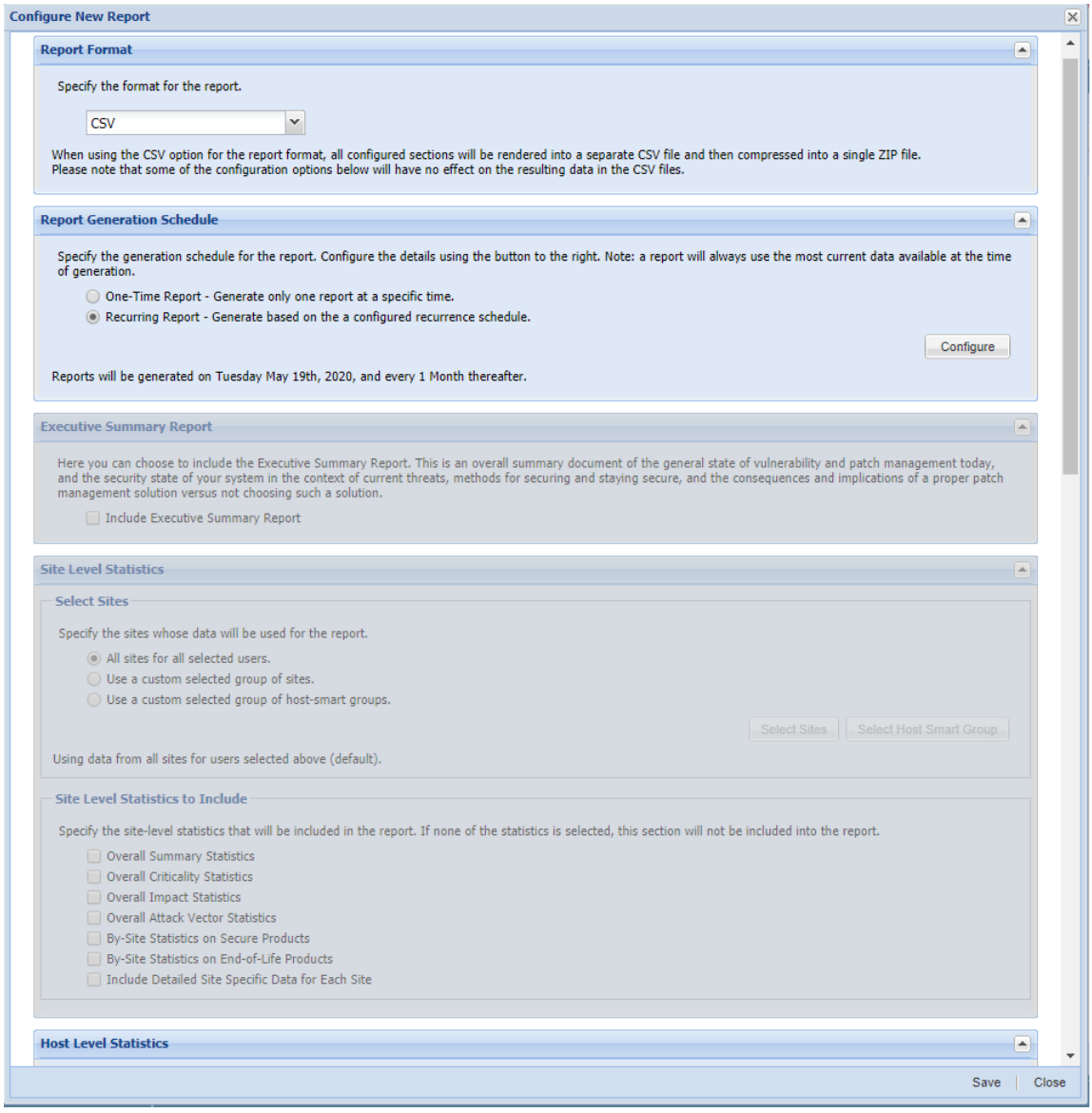


Important • *The emails containing the PDF reports will be sent by your configured mail server. The mail server must be configured before users receive the PDF reports.*

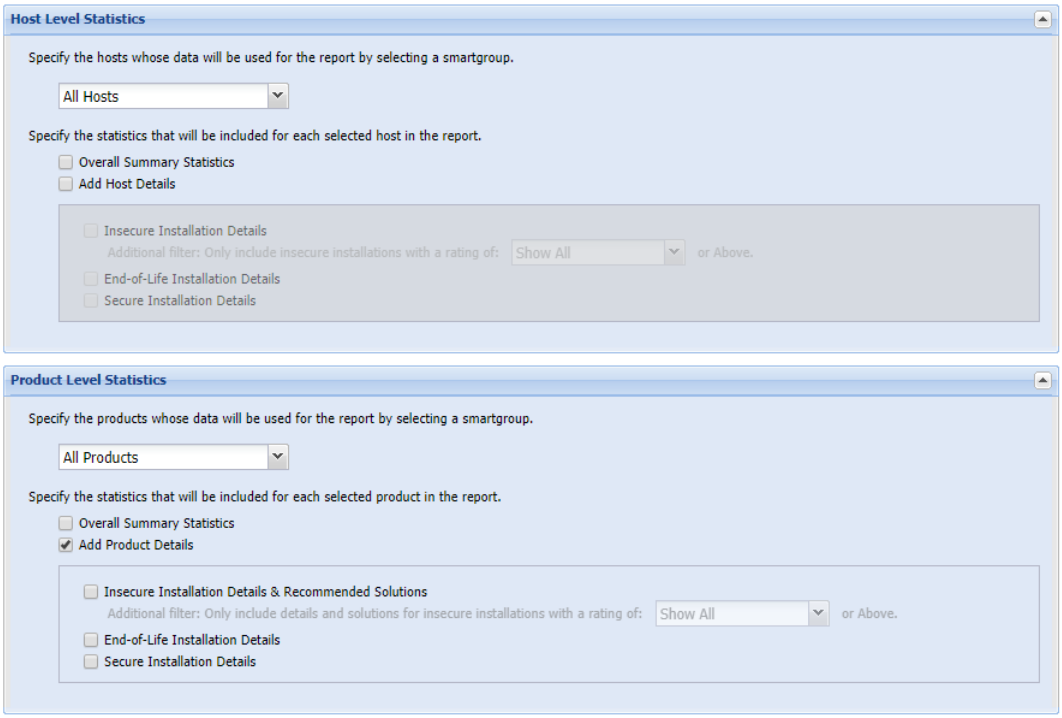
Select the CSV Option for the Report Format

When you select the CSV option for the report format, the following sections and options are disabled:

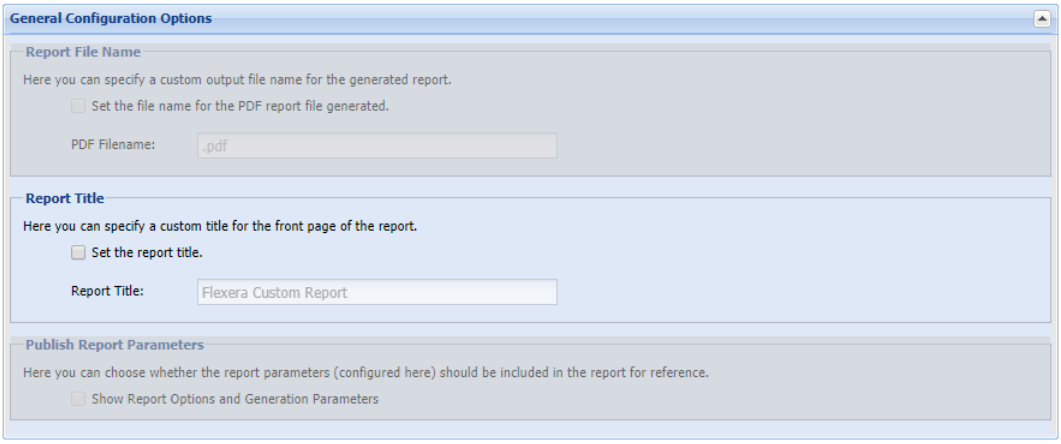
- **Executive Summary Report**, **Site Level Statistics**, and **Overall Summary Statistics** check box for both **Host Level Statistics** and **Product Level Statistics** are disabled.



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



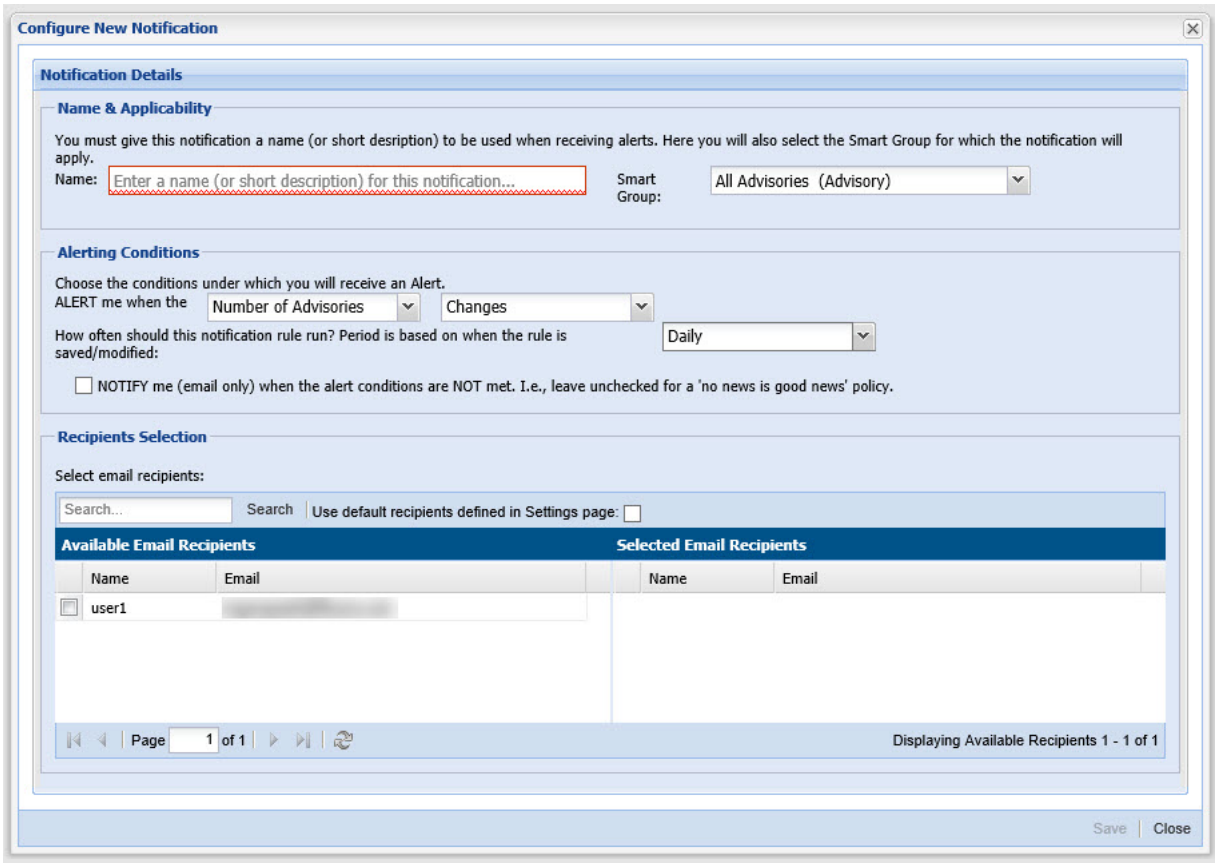
- **PDF Filename** tab and **Publish Report Parameters** sections are disabled.



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 desription) to be used when receiving alerts. Here you will also select the Smart Group for which the notification will apply.
Name:
Enter a name (or short description) for this notification...
Smart Group:
All Advisories (Advisory)
Alerting Conditions
Choose the conditions under which you will receive an Alert.
ALERT me when the
Number of Advisories
Changes
How often should this notification rule run? Period is based on when the rule is saved/modified:
Daily
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...
Search
Use default recipients defined in Settings page:
Available Email Recipients
Selected Email Recipients
Name
Email
Name
Email
user1
Page 1 of 1
Displaying Available Recipients 1 - 1 of 1
Save
Close

Activity Log Notifications

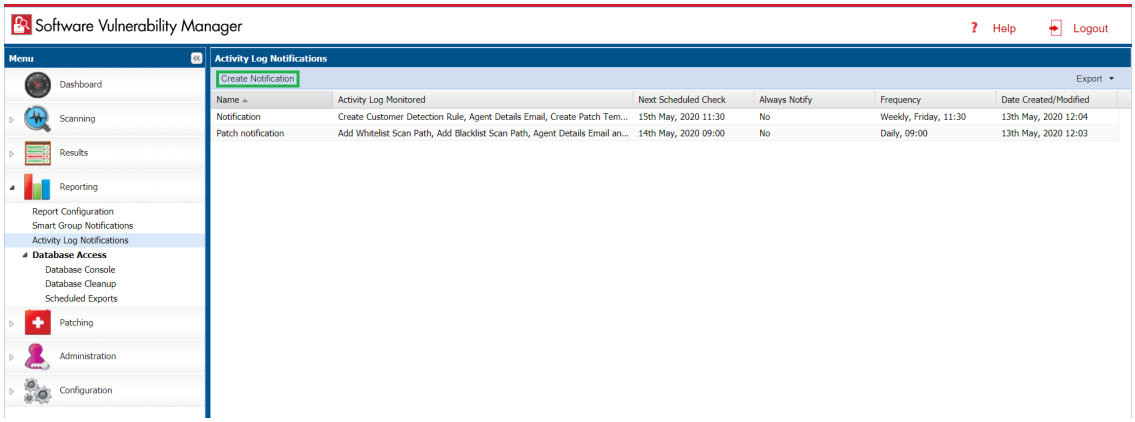
Use this page to schedule multiple notification digests for the respective events through emails.

Creating Notifications for the Activity Log

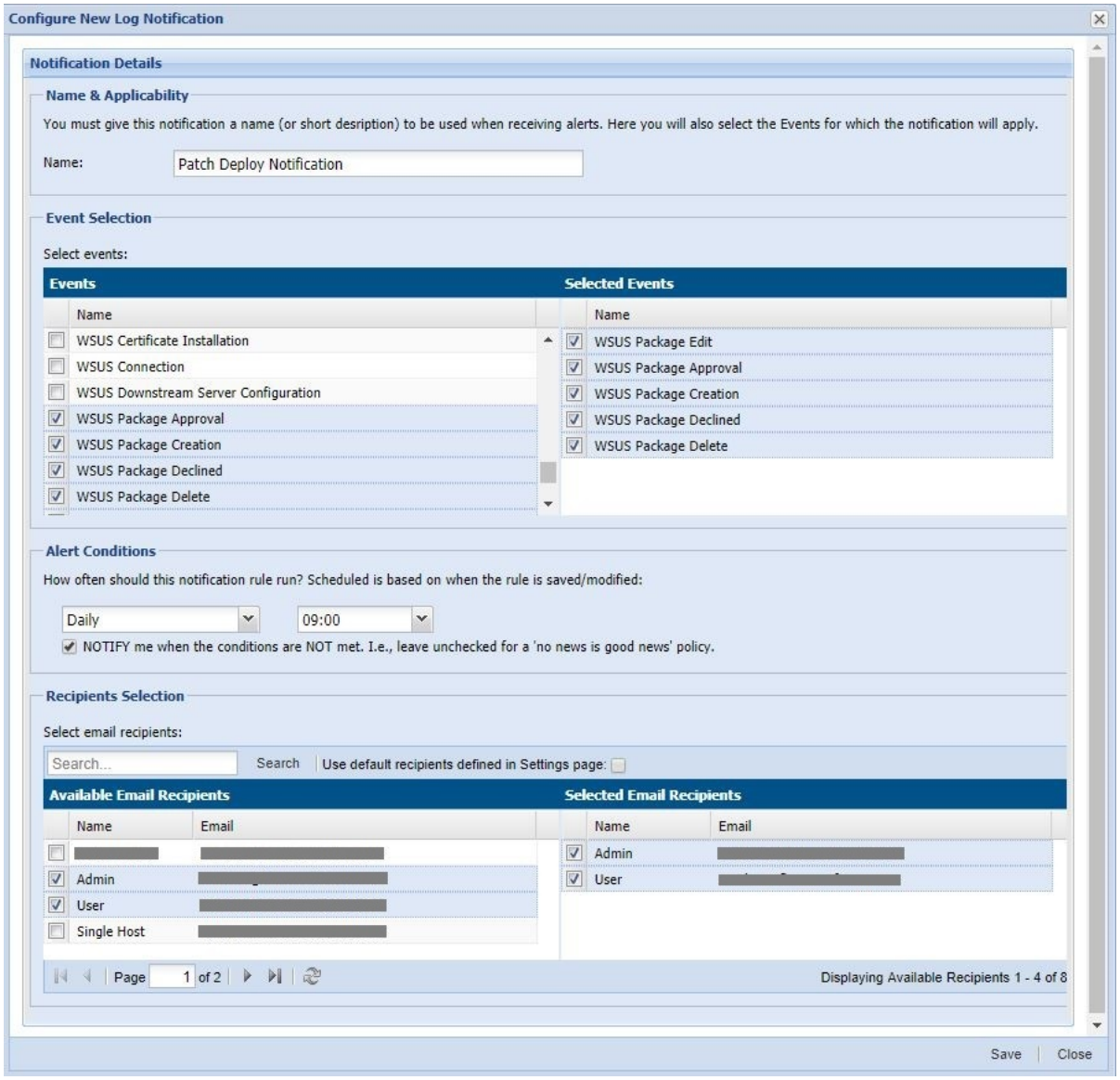
To create notifications for the Activity Log, perform the following steps.

Task ***To create notifications for the Activity Log:***

1. Click **Create Notification**.



The **Configure New Log Notifications** dialog box opens.



2. Describe notification name, select the required events, and then select notification schedules.
3. These email notifications can be scheduled on an **Hourly**, **Daily**, **Weekly**, or **Monthly** basis. If you select the **Daily**, **Weekly**, or **Monthly** option, then choose the time duration for the selected day.
4. Choose the recipients and then click **Save**.

Database Access

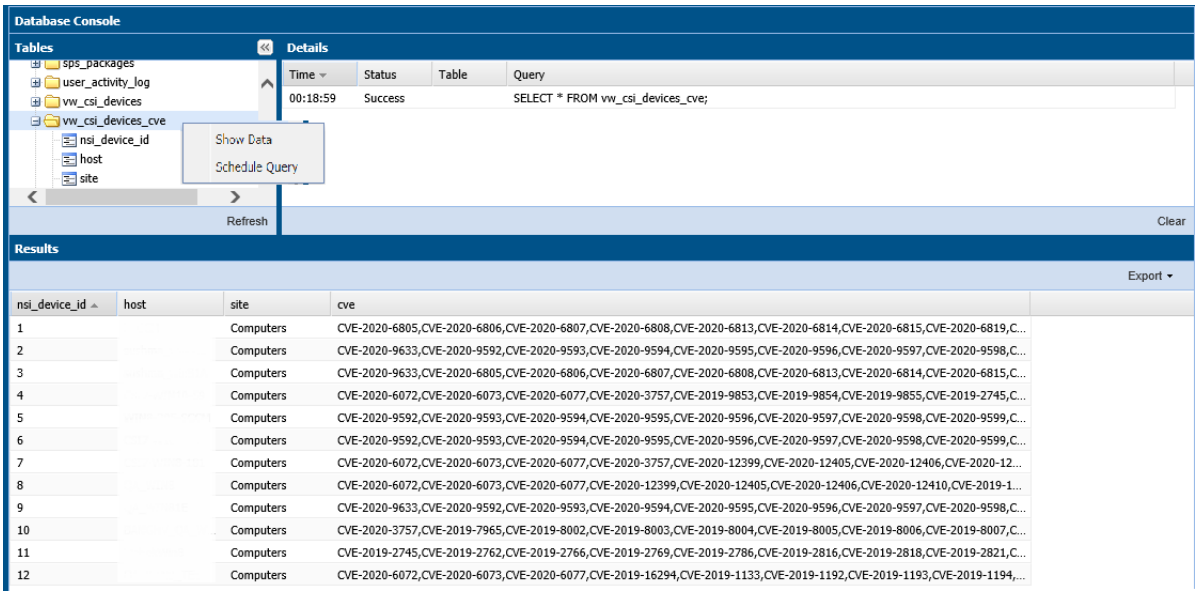
- To access Flexera's SQL database, see Database Console.
- To delete hosts from your Software Vulnerability Manager account by configuring rules that check for certain criteria, see Database Cleanup.

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.



Summary of the SQL Data in the Database Console Tables

The following table lists the SQL Data in the Database Console Tables:

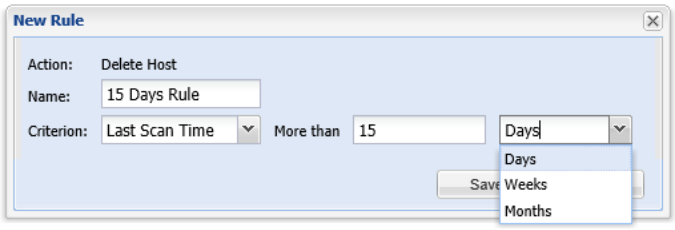
SQL Data	Description
vw_csi_devices	List of hosts with mac address & ip address
vw_csi_devices_cve	List of hosts affected by CVE
vw_host_eol	List hosts with End of Life software
vw_host_unpatched_os	List hosts with insecure operating system and operating system version
vw_host_insecure	List hosts with insecure software and software version

Database Cleanup

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

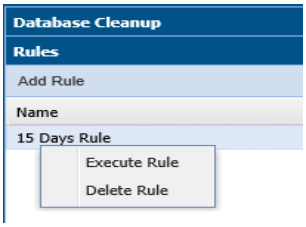
You can use this page, for example, to delete all the hosts that have not been scanned for more than 15 days.

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



The 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**.



Scheduled Exports

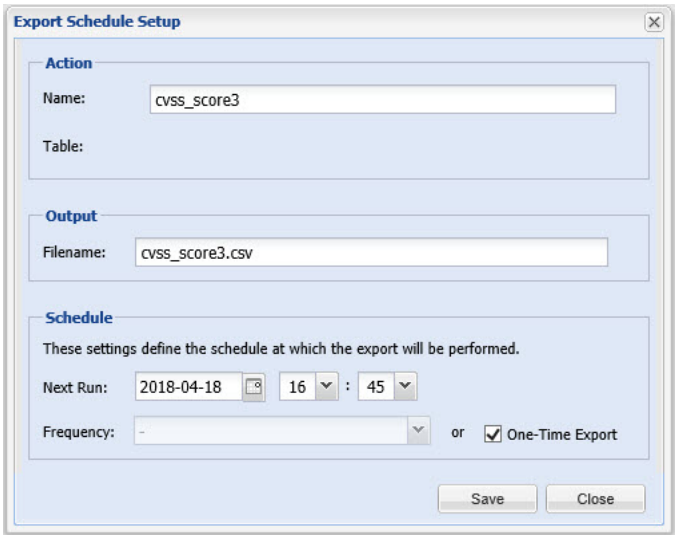
Use this page to view, edit or delete automated data extraction schedules.

Important • *To schedule exports you must first download and install the Software Vulnerability Manager Daemon from https://www.flexera.com/svm-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.



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
- QuickPatch
- Patch Automation
- Intune Publishing
- Workspace ONE Publishing

Flexera Package System (SPS)

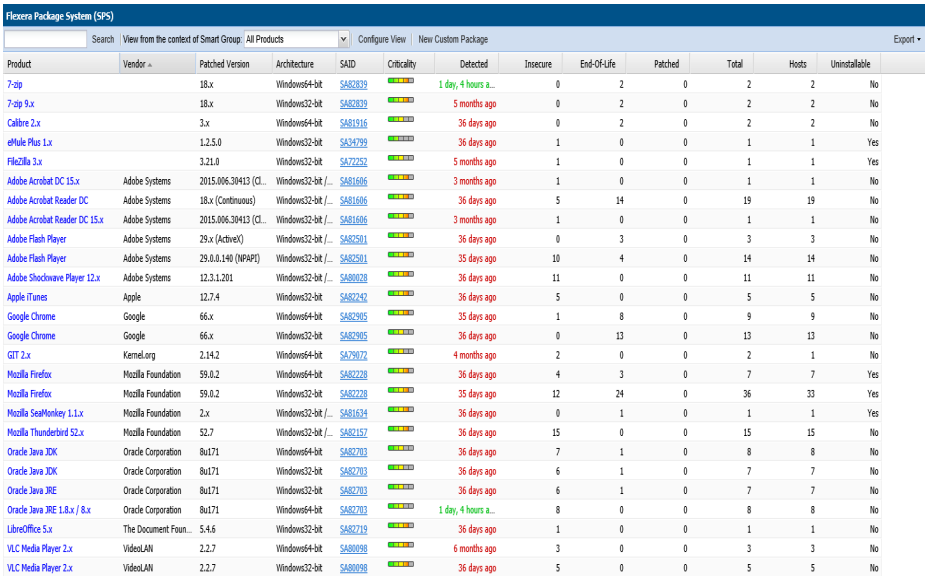
This section provides further information regarding:

- 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.



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
GIT 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	SA82719		36 days ago	1	0	0	1	1	No
VLC Media Player 2.x	VideoLAN	2.2.7	Windows64-bit	SA80098		6 months ago	3	0	0	3	3	No
VLC Media Player 2.x	VideoLAN	2.2.7	Windows32-bit	SA80098		36 days ago	5	0	0	5	5	No

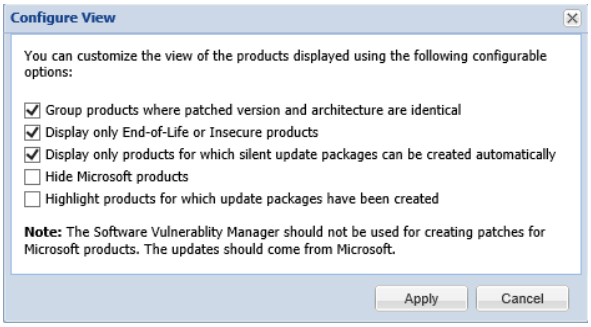
The **Flexera Package System (SPS)** features include:

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

Note • *Flexera SPS page now available in non-IE browser also. In order to use complete feature of patching, need to install Software Vulnerability Manager Plugin.*

Product display criteria for SPS

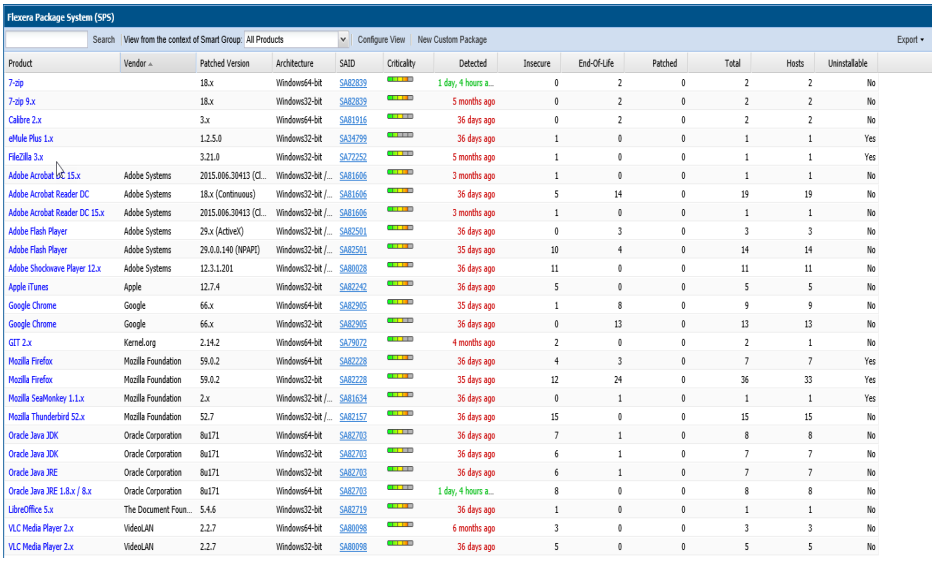
Click Configure View to select the criteria that will be used to display the products in this view.



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.



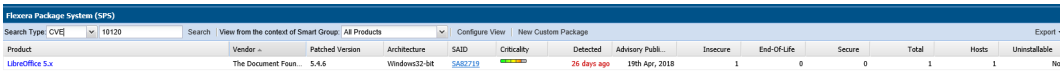
Note • *An SPS package created when the Group products where patched version and architecture are identical check box is selected (grouped mode) can cover multiple product rows that are displayed when the check box is not selected (ungrouped mode). Consequently this can lead to a discrepancy when determining 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.



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.*

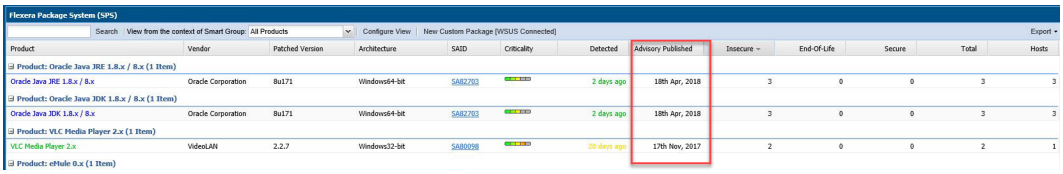


Figure 9-1: Flexera Package System (SPS) ungrouped view

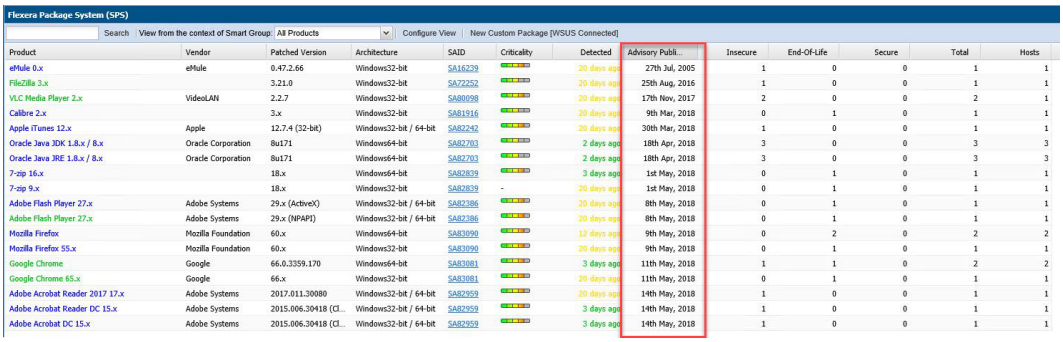


Figure 9-2: Flexera Package System (SPS) grouped view

SPS Concepts and Terminology

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

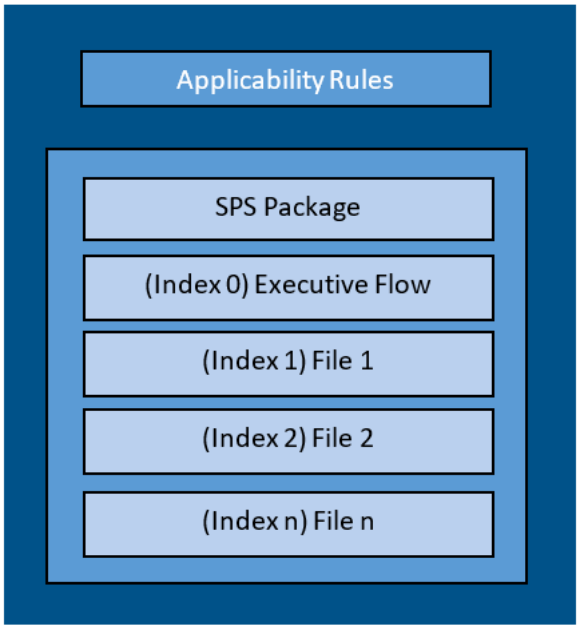
- What does a SPS package consist of?
- Applicability Rules
- SPS Package
- Execution Flow Script

- 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.

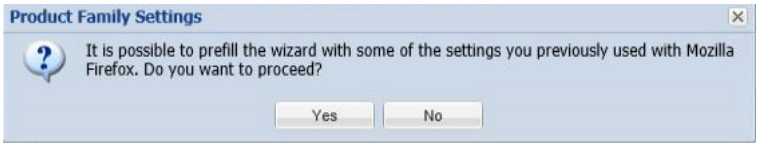
The execution flow script for an Update package can also be customized for additional functionality. You can also configure your patching package SPS Installer Parameters using dynamic check box options (where applicable) based on product functionality, including:

- 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

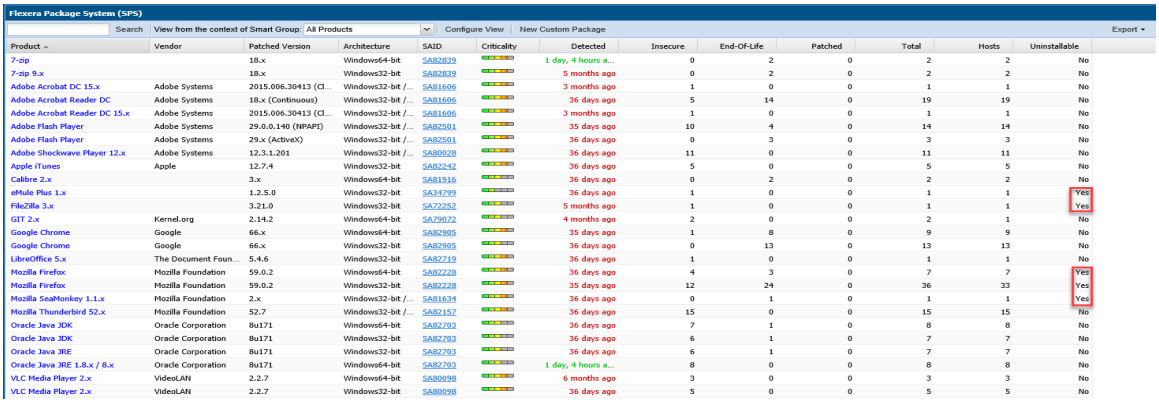
A Product will be displayed in blue if the vendor provides unattended/silent installation parameters for its patches. Any Product listed in blue is available to have an update created in a three-step process. Right-click or double-click one of these Products and select **Create Update Package** to start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



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

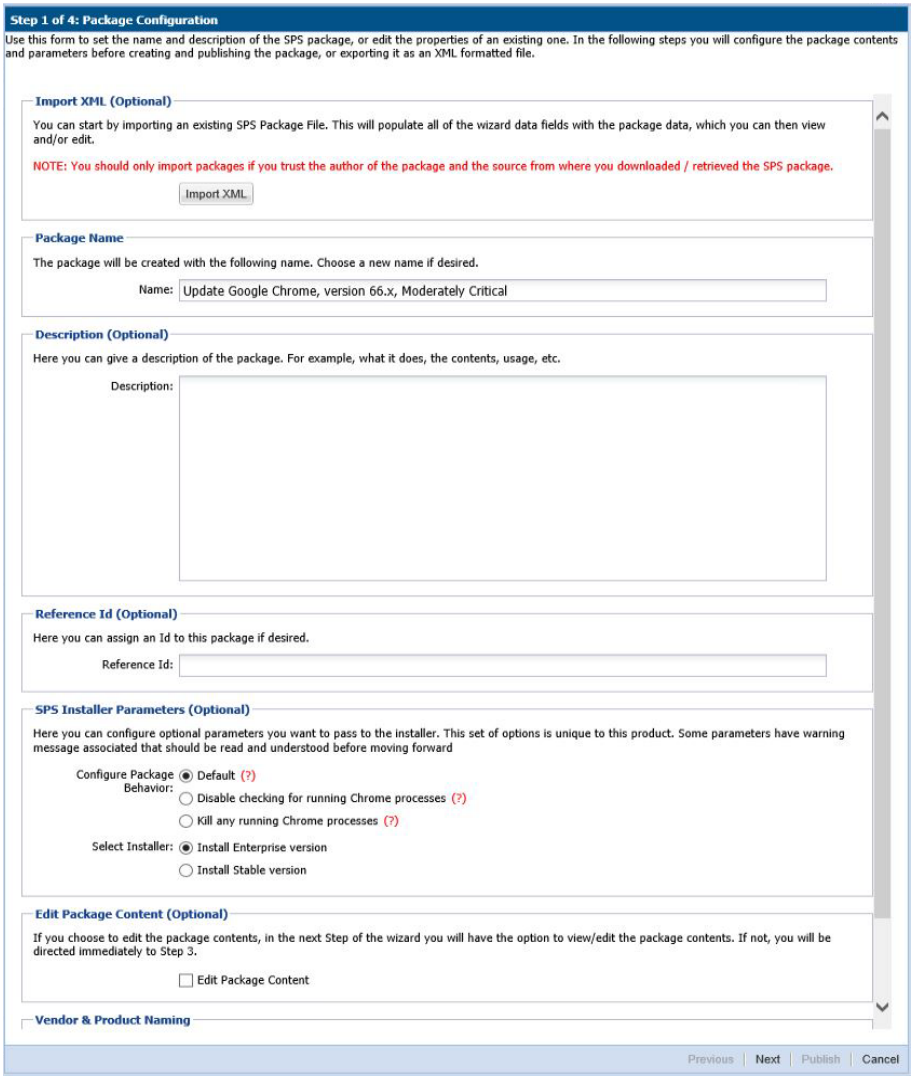
Creating an SPS Package involves a four-step process:

- Step 1 of 4: Package Configuration

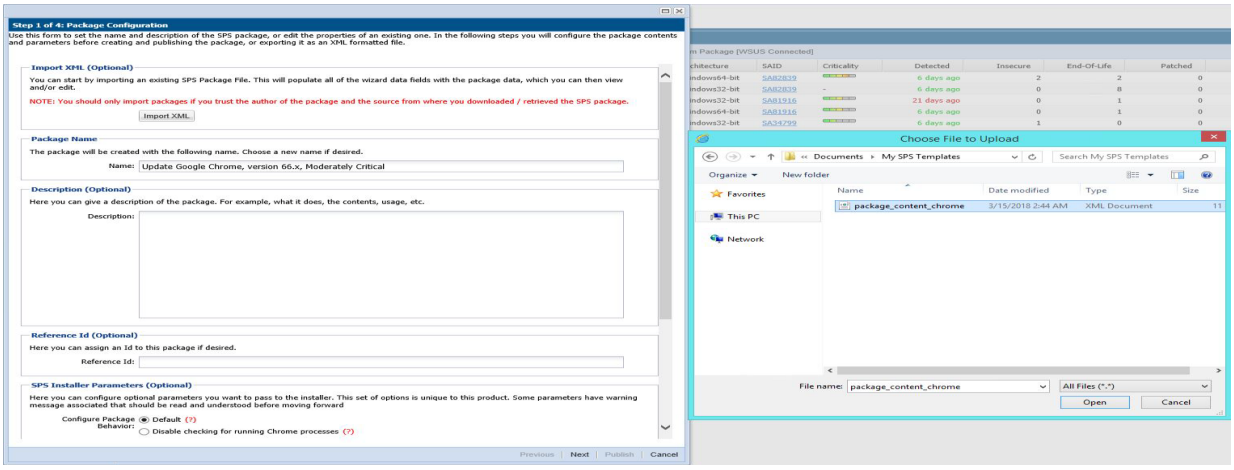
- Step 2 of 4: Package Contents
- Step 3 of 4: Applicability Criteria - Paths
- Step 4 of 4: Applicability Criteria - Rules

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.



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.

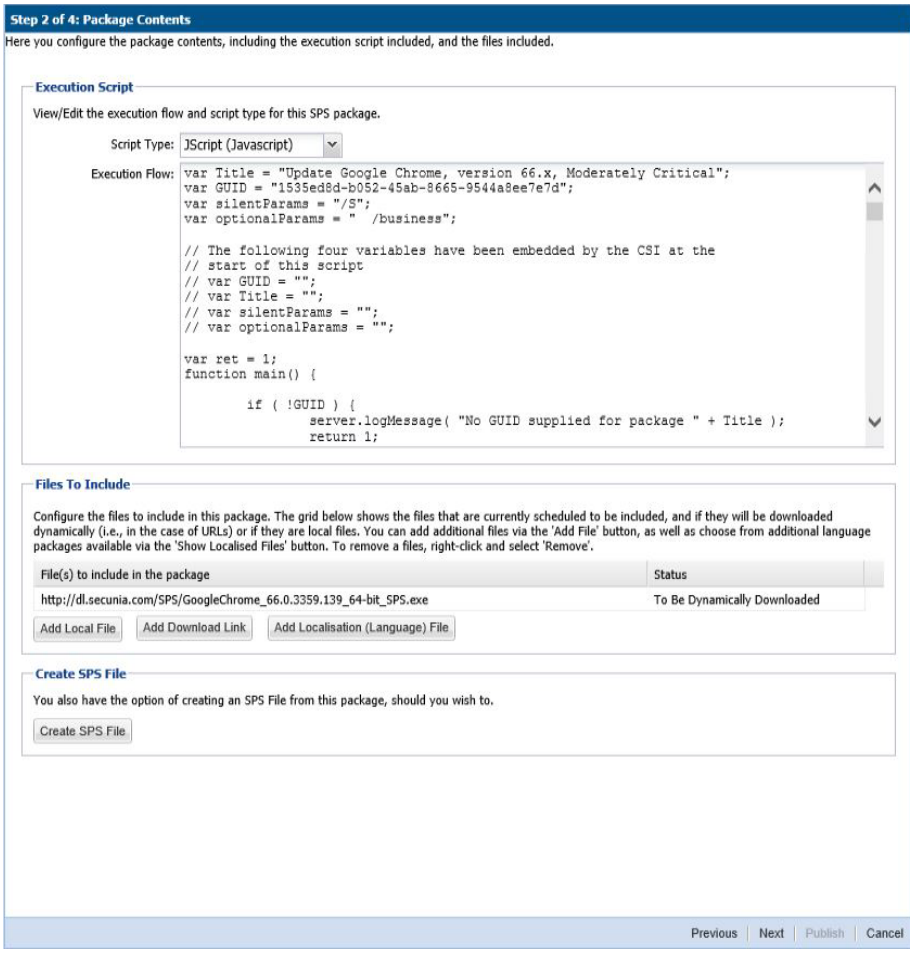
Step 2 of 4: Package Contents

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.

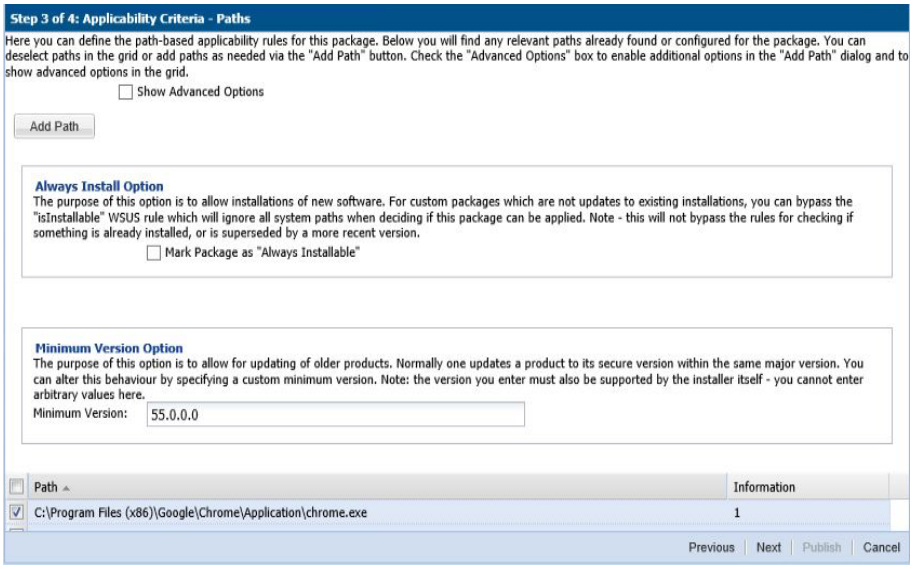
This SPS.exe file will include the execution flow script and the files to be included, but not the applicability rules.



Step 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.



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.

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.

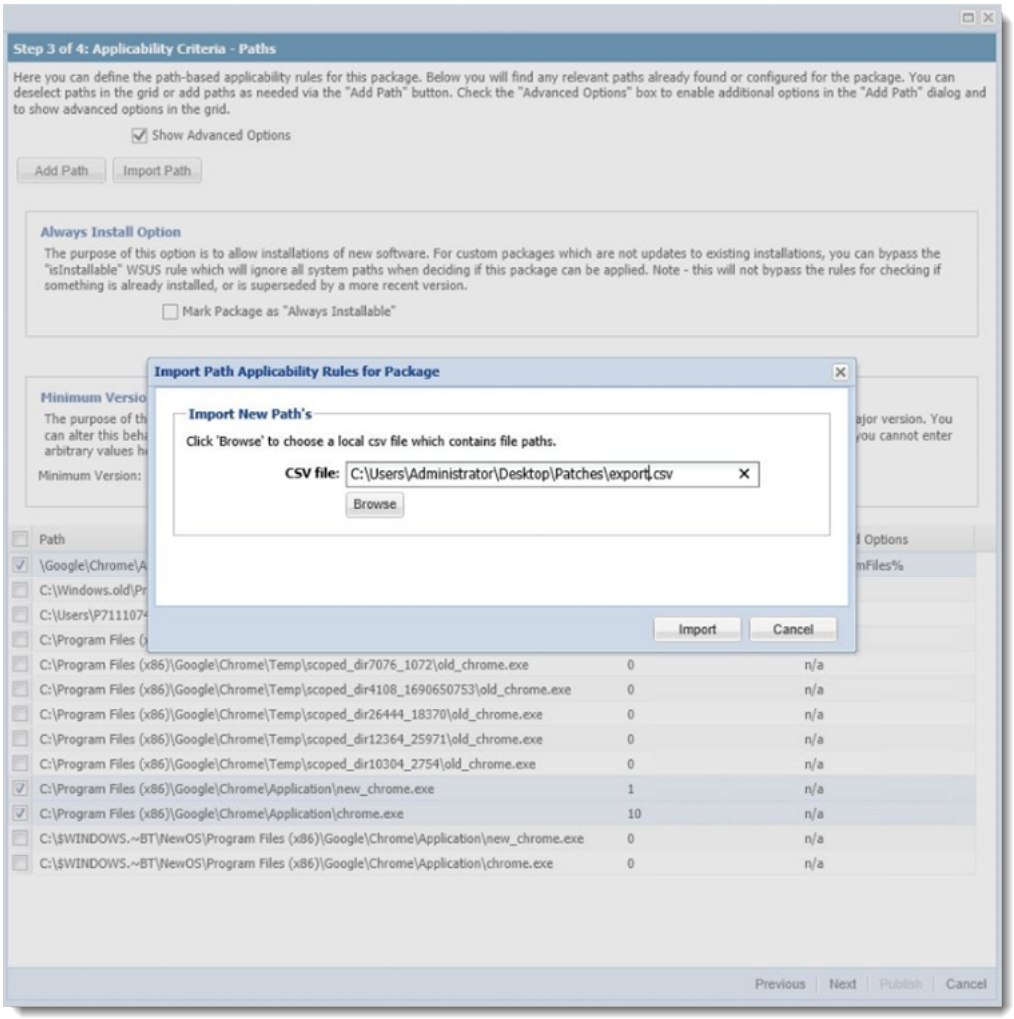


Figure 9-3: Import Path Applicability Rules for Package Dialog Box

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
```

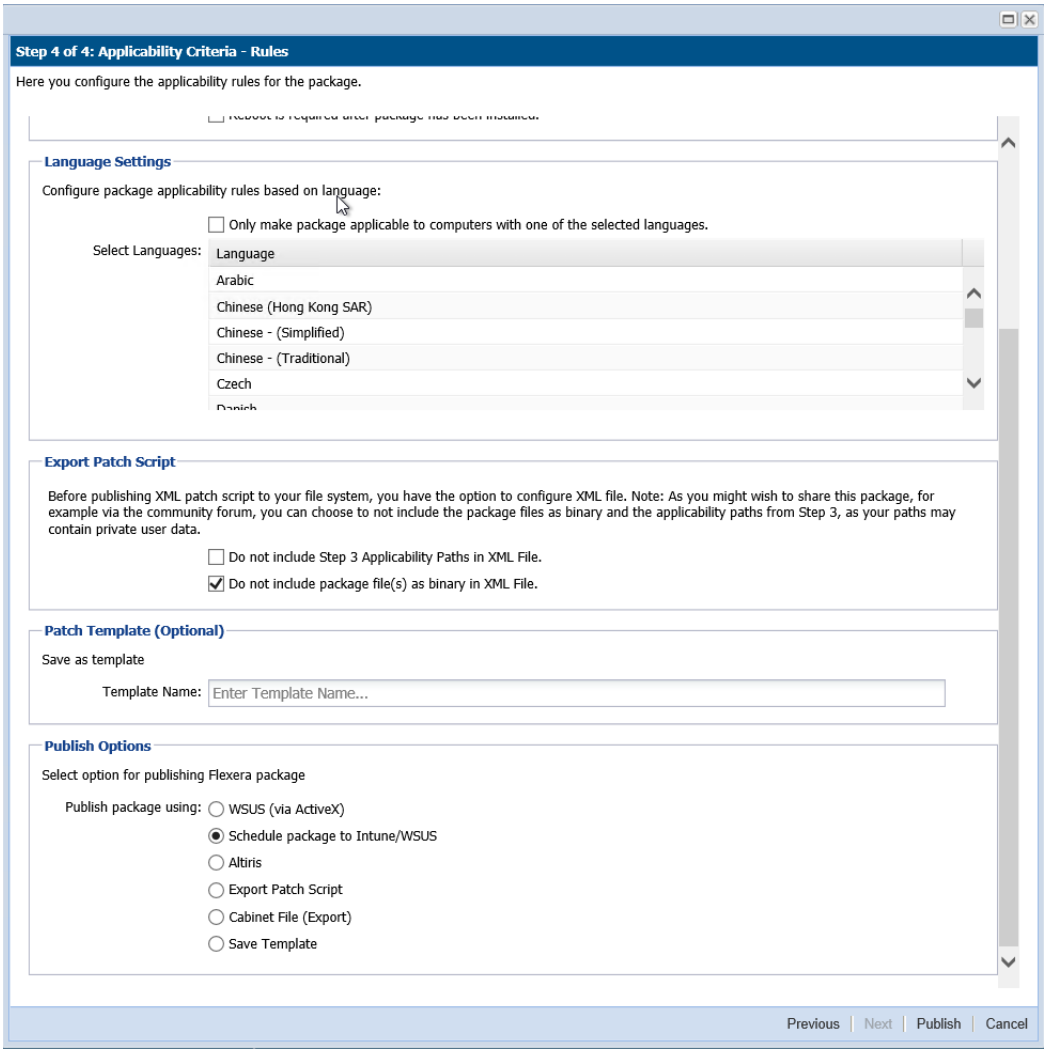
Note • *The CSV file does not need to have comma-separated values, but just a list. You don't have to use quotes when there are spaces in a file path. The CSV file can essentially be a text list with just one column. As a single column list of values, simply provide one file path per line (no header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

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

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



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:

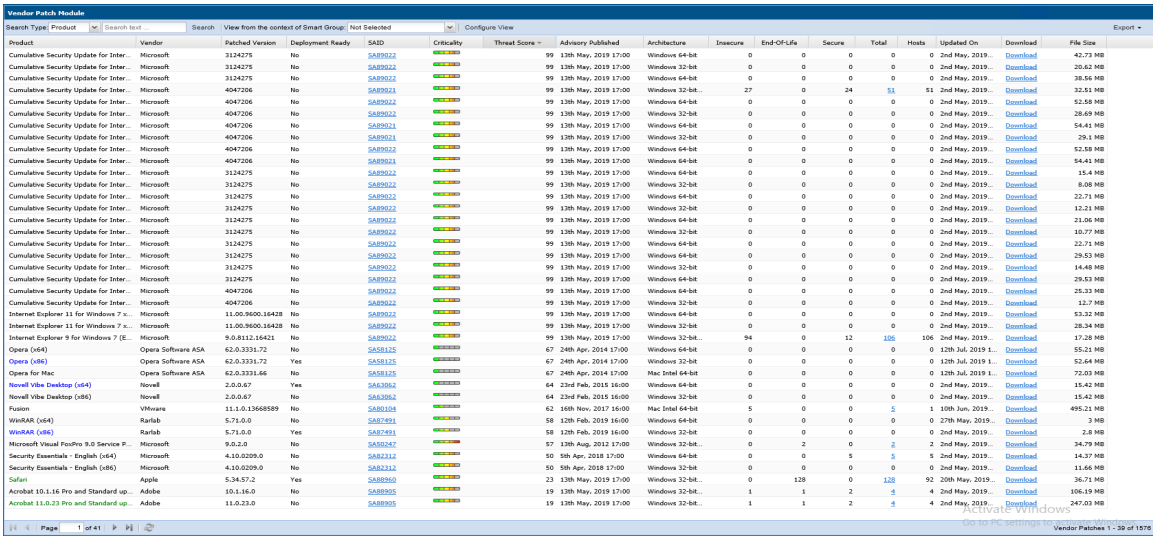
- Vendor Patch Module Page Features
- Creating a Patch with the Vendor Patch Module
- Package Creation Wizard in Vendor Patch Module
- Automating Patch Deployment

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.



The **Vendor Patch Module** features include:

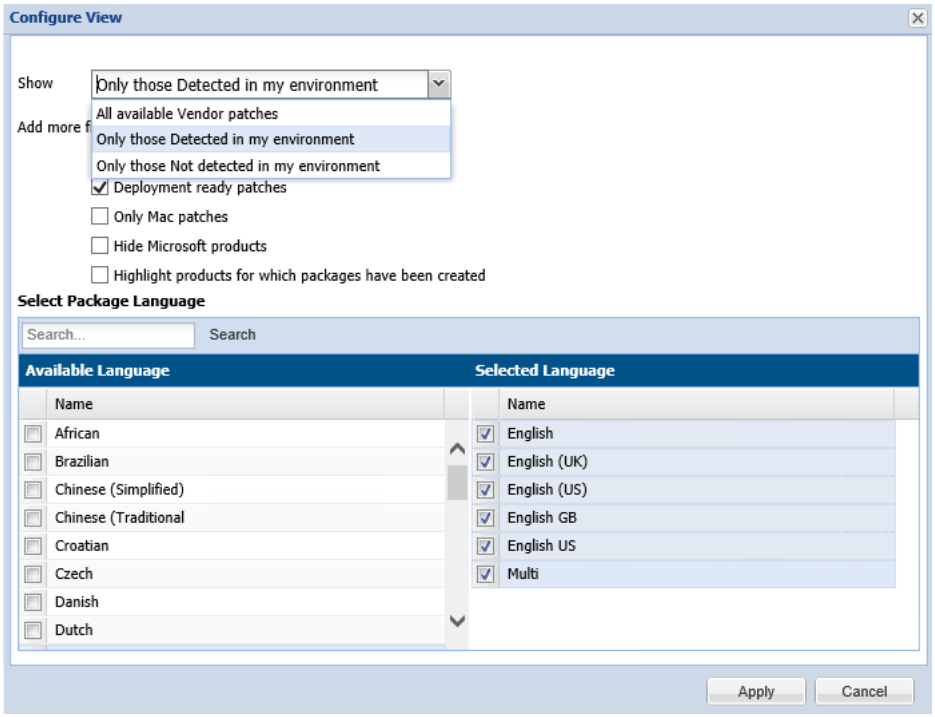
- Product display criteria for Vendor Patch Module
- Patch update searches by Common Vulnerabilities and Exposures
- Advisory Published date in Vendor Patch Module
- Threat Score in Vendor Patch Module

Product display criteria for Vendor Patch Module

Click **Configure View** to define a criteria from either or both the **Show** drop down and the **Add more filters** check boxes. This criteria will be used to display the filtered products in this view.

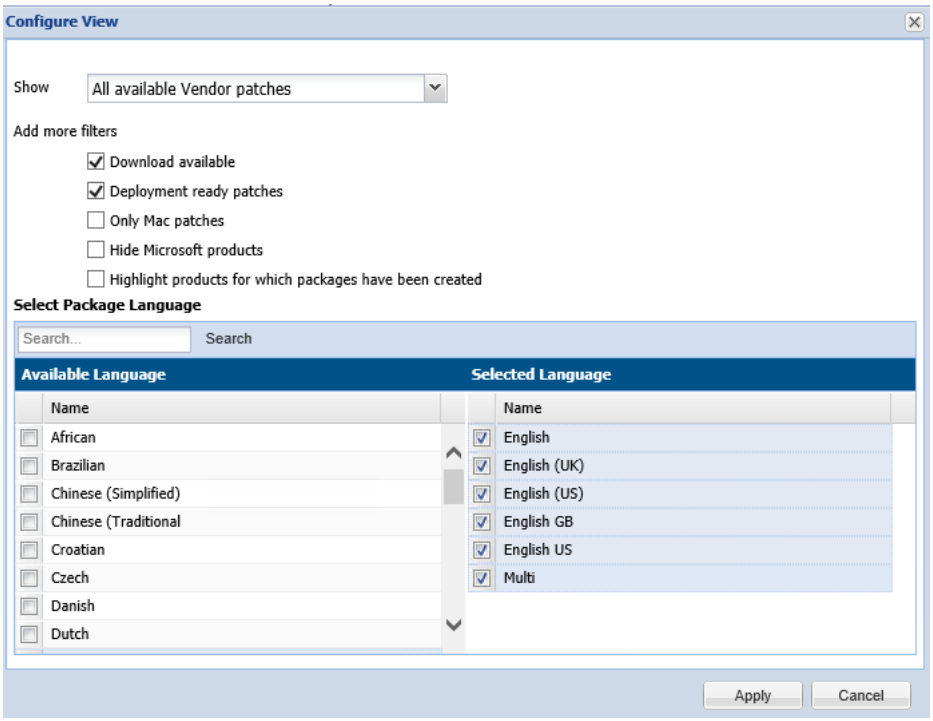
Select one of the following **Show** options:

- **All available Vendor patches**—Displays he vendor patches which are available in vendor patch module.
- **Only those Detected in my environment**—Displays a list of out of the box patches available for applications which are already installed in the user environment.
- **Only those Not Detected in my environment**—Displays a list of out of the box patches available for other applications which are not deployed in the user environment.



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.
- **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.

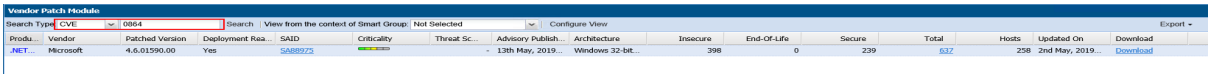
By default, the following package language is selected:

- 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.

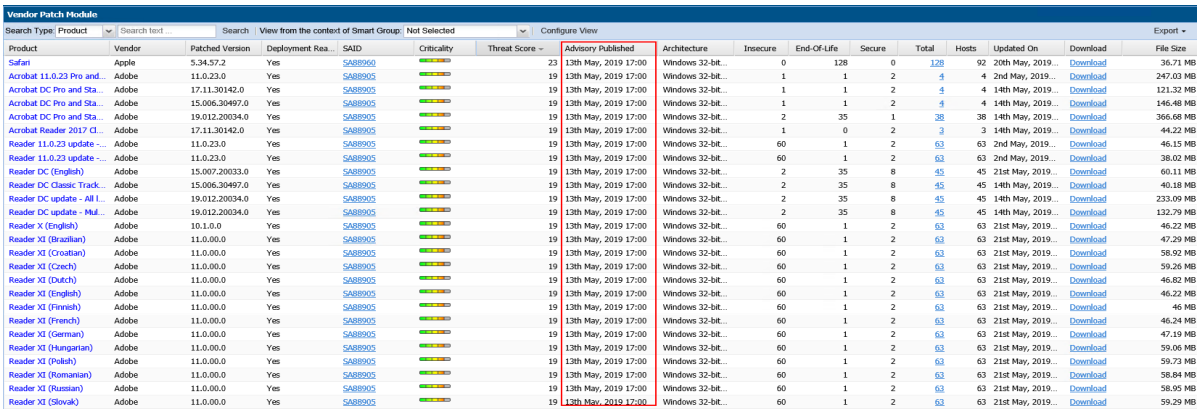
Patch update searches by Common Vulnerabilities and Exposures

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.



Advisory Published date in Vendor Patch Module

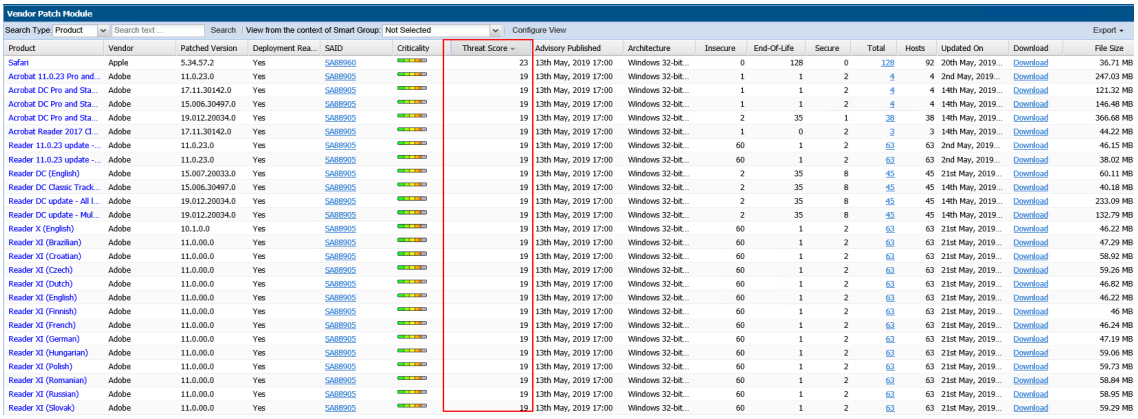
The **Advisory Published** date is listed in the **Vendor Patch Module** provides a quick reference for the latest patching information.



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*



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

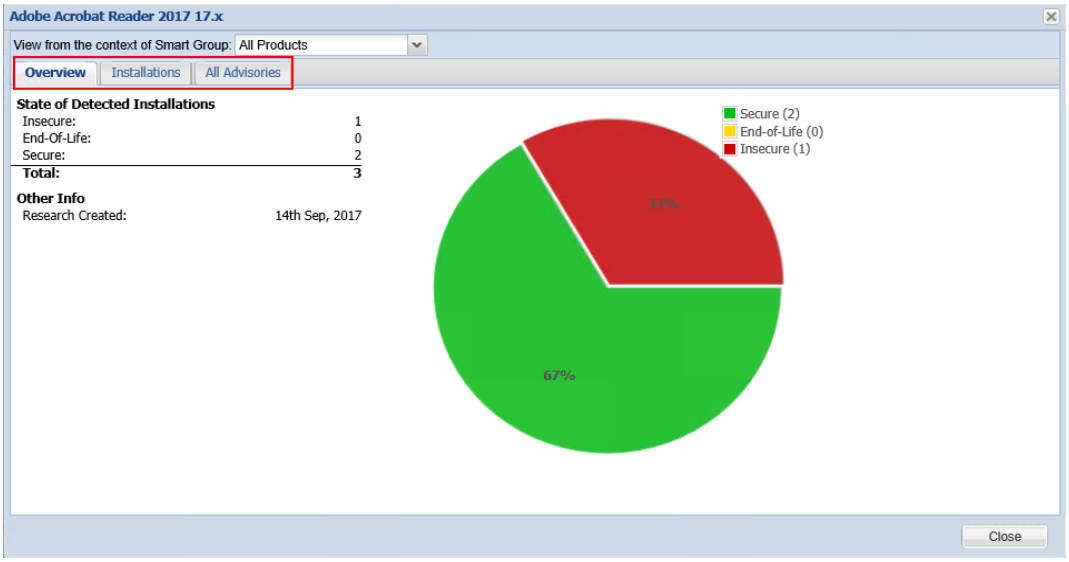
To display the installation details of a product in the Vendor Patch Module, Right-click one of a product and select **View Installations** to open the wizard,

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.

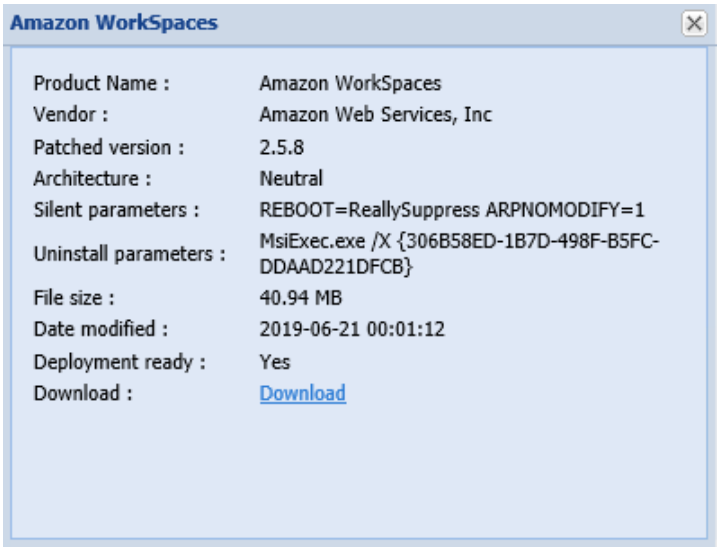


Patch Information

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



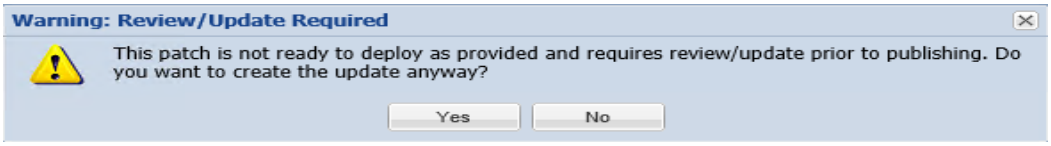
Package Creation Wizard in Vendor Patch Module

The following steps explain how to create update Package:

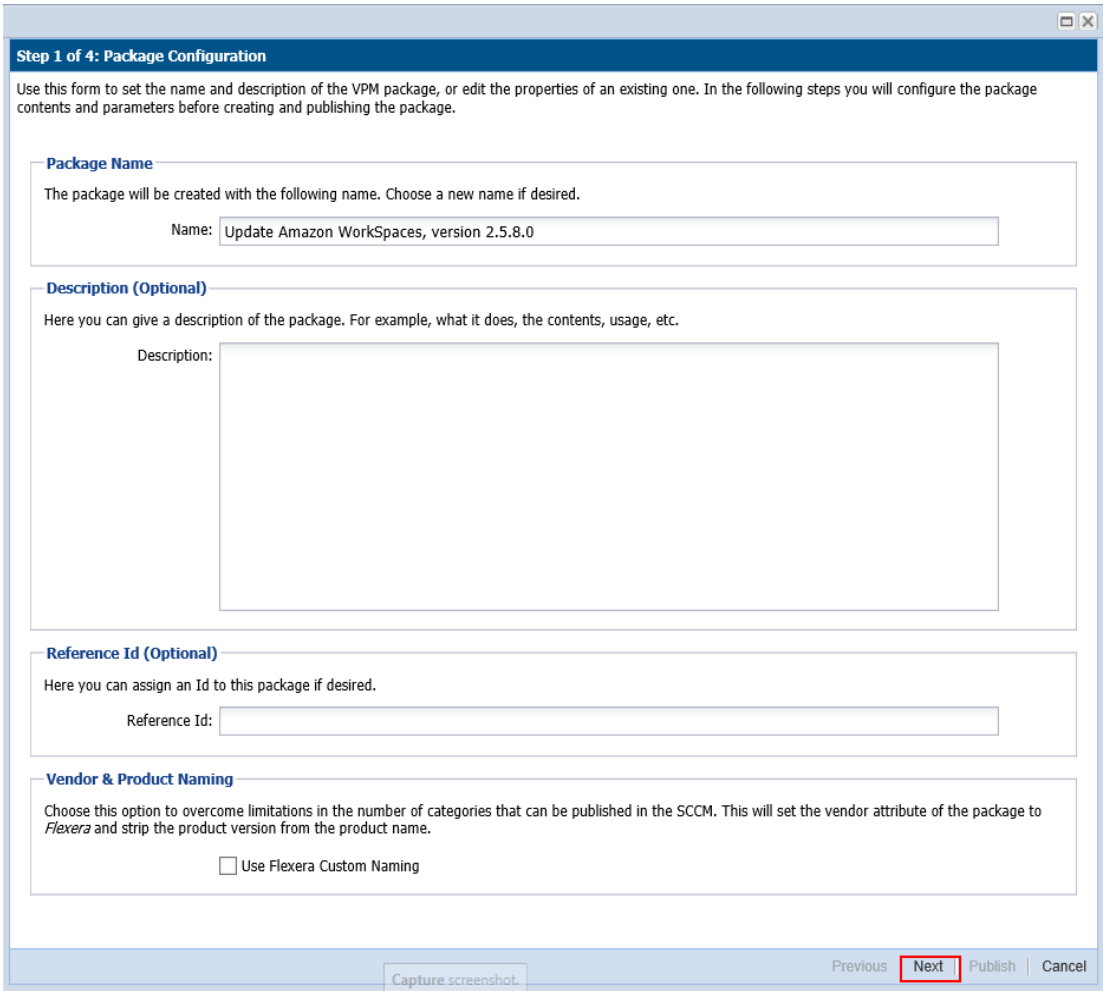
- Step 1 of 4: Package Configuration
- Step 2 of 4: Package Contents
- Step 3 of 4: Applicability Criteria - Paths
- Step 4 of 4: Applicability Criteria - Rules

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.



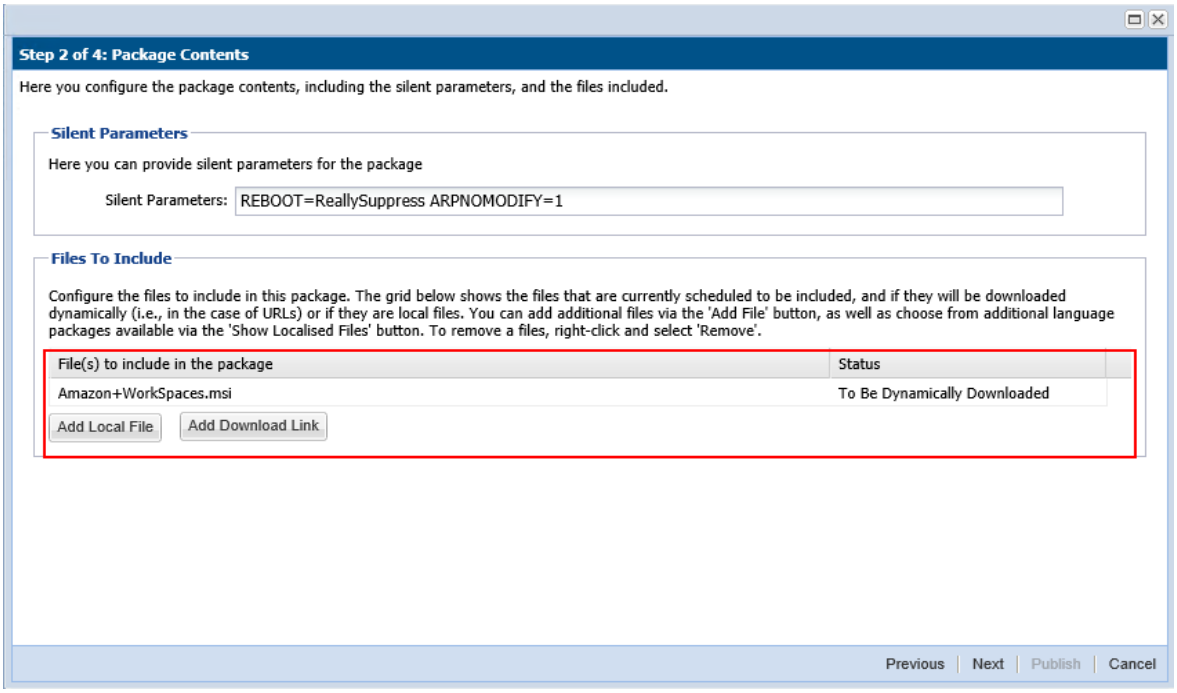
In the Package Configuration wizard, click **Next**.



Step 2 of 4: Package Contents

Step 2 provides the following package details:

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



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.

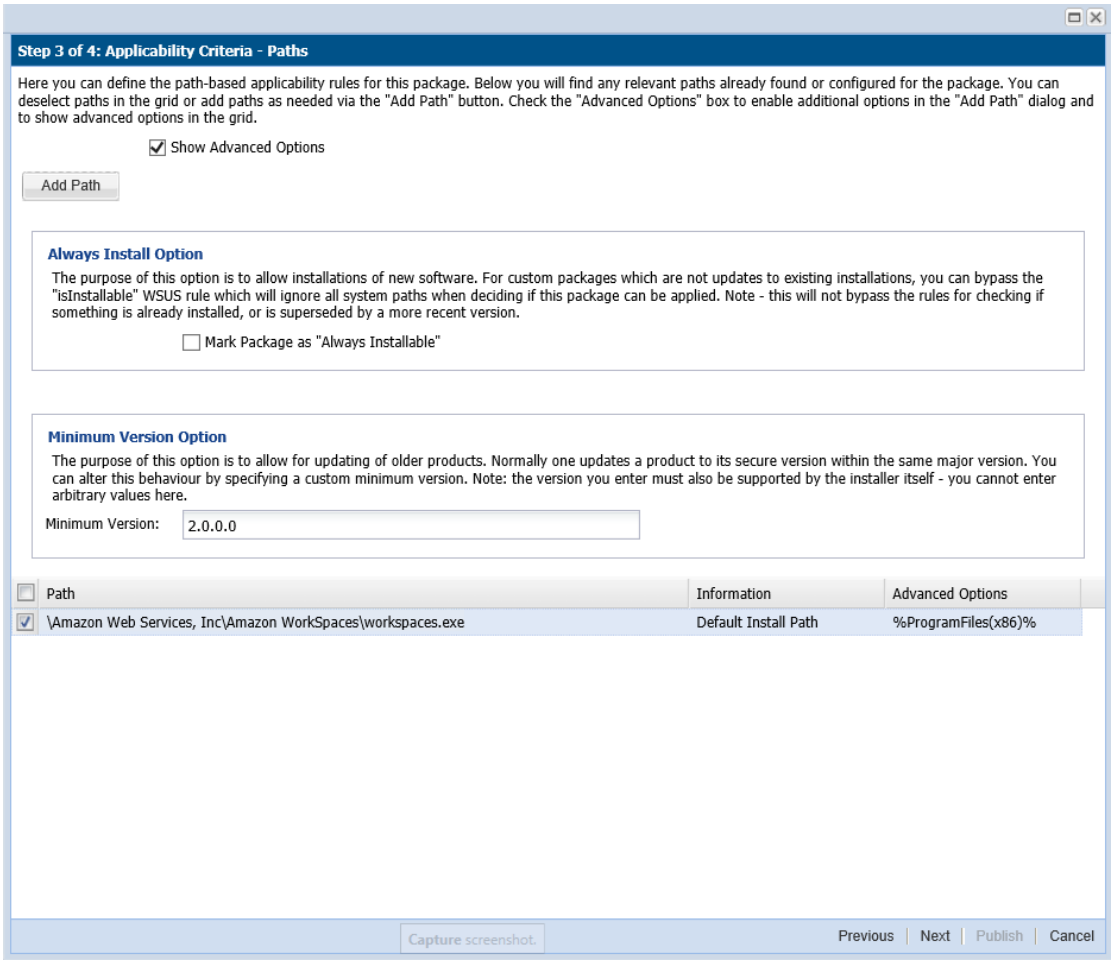
Note • *Note the Following:*

- *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.



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.

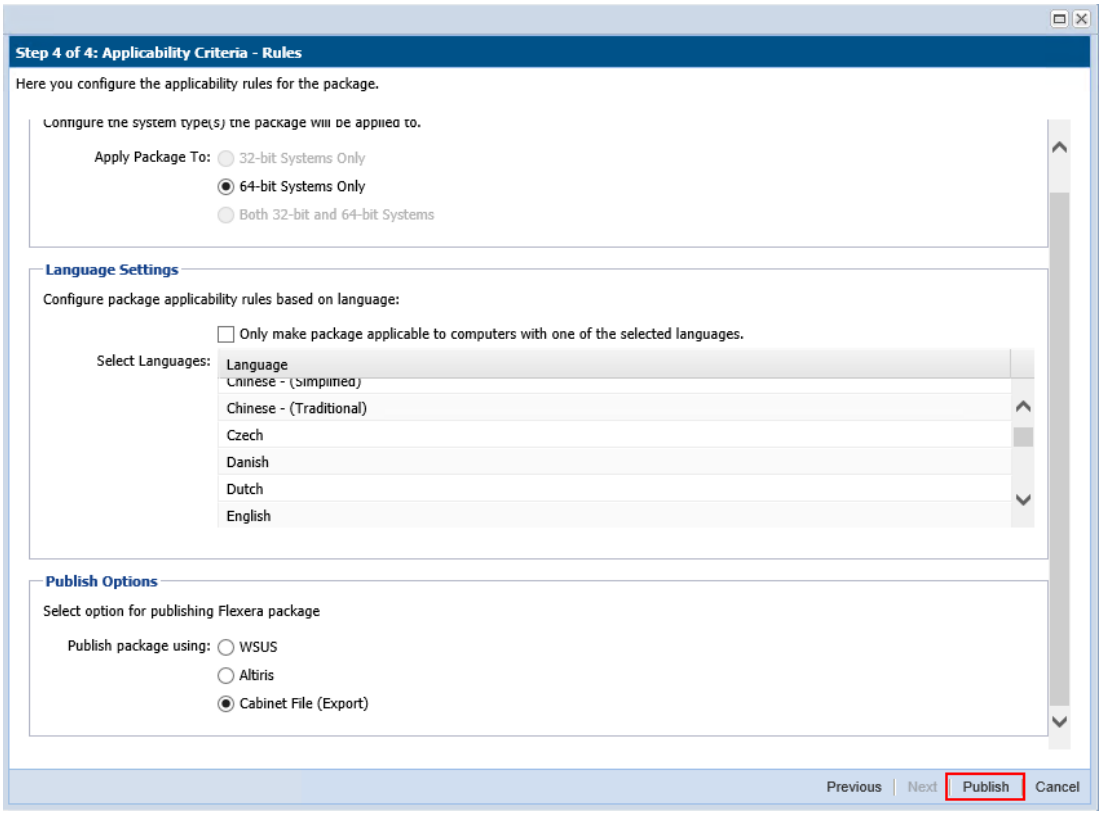
Note • *The minimum version you enter must also be supported by the installer itself - you cannot enter arbitrary values here.*

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.

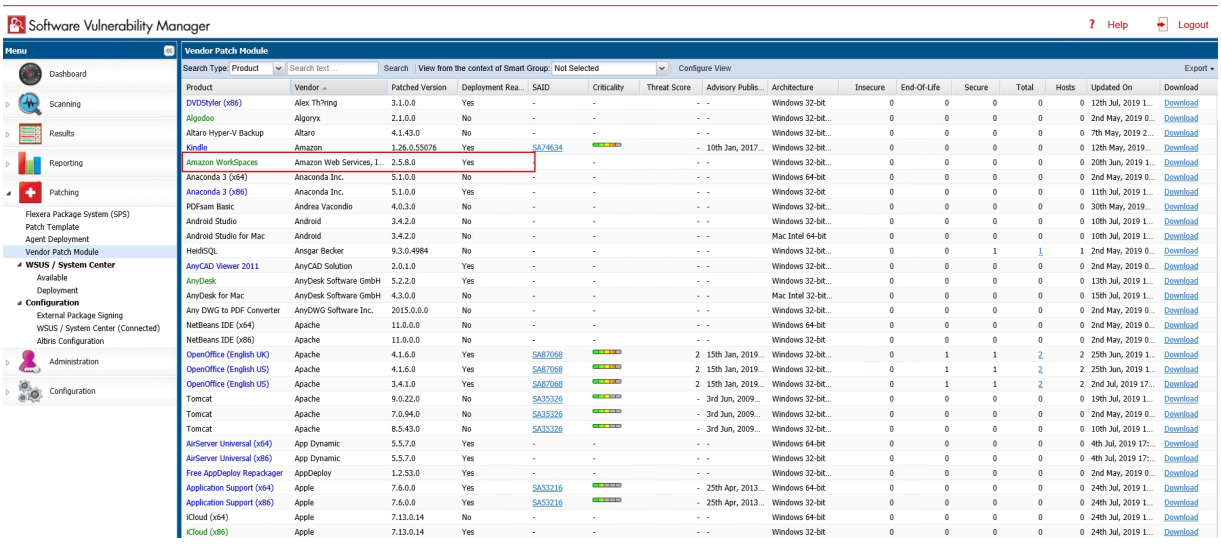
The WSUS option will be unavailable if the WSUS Connection is not established.

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



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.



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.

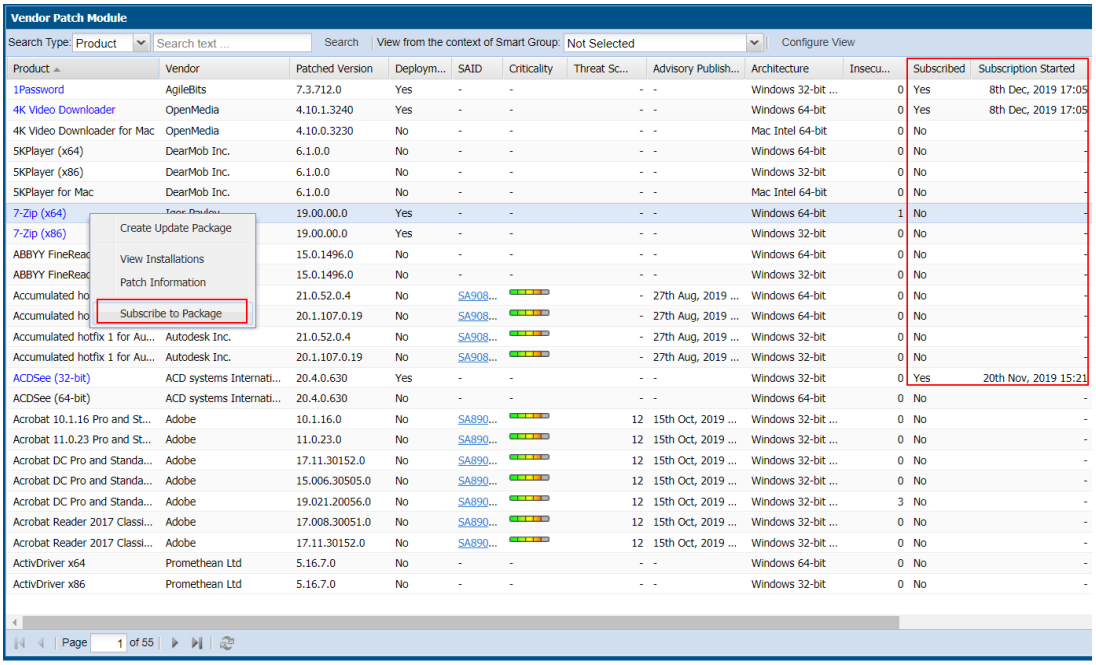
To use this option, navigate to **Patching >> Vendor Patch Module**. List of patches appears.

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.*



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.

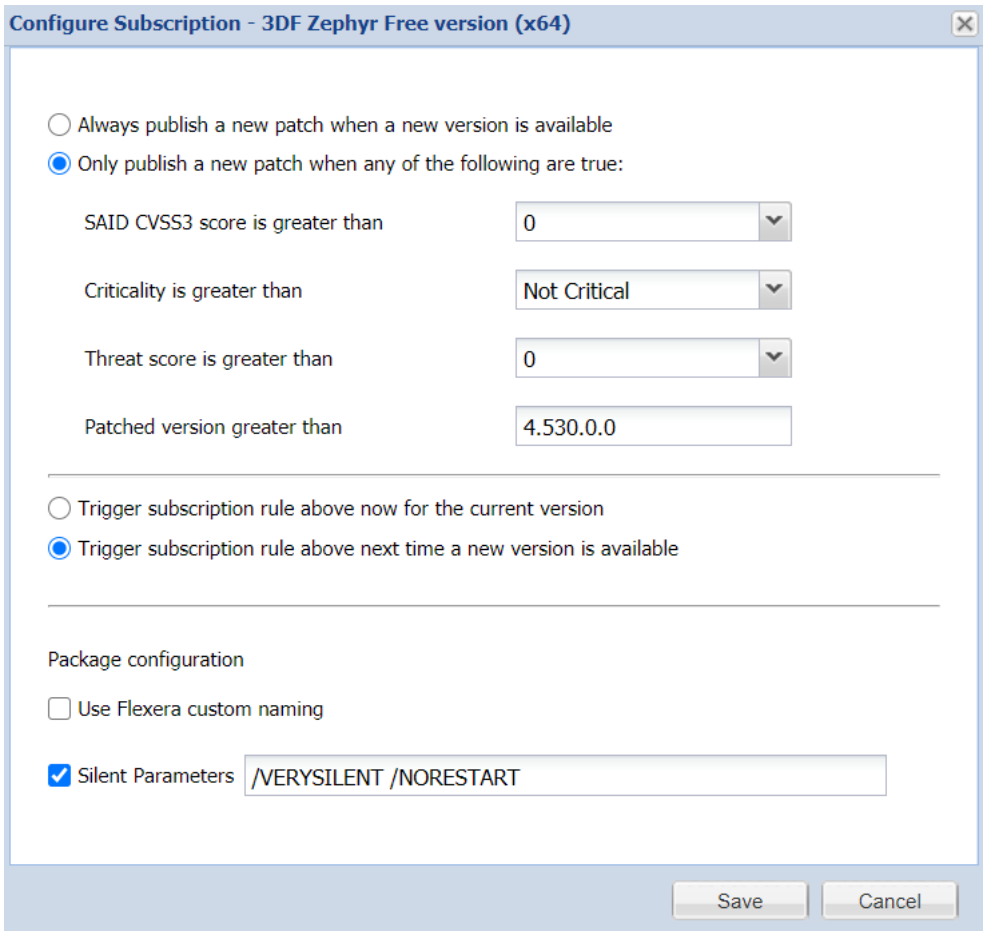
- **SAID CVSS3 score is greater than**
- **Criticality is greater than**
  - Extremely Critical
  - Highly Critical
  - Moderately Critical
  - Less Critical
  - Not Critical
- **Threat score is greater than**
- **Patched version greater than -** By default current version of a patch will be displayed

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
- **Silent Parameters** - Saves custom silent parameters for VPM subscription.

Task ***To automate a patch deployment do the below following:***

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

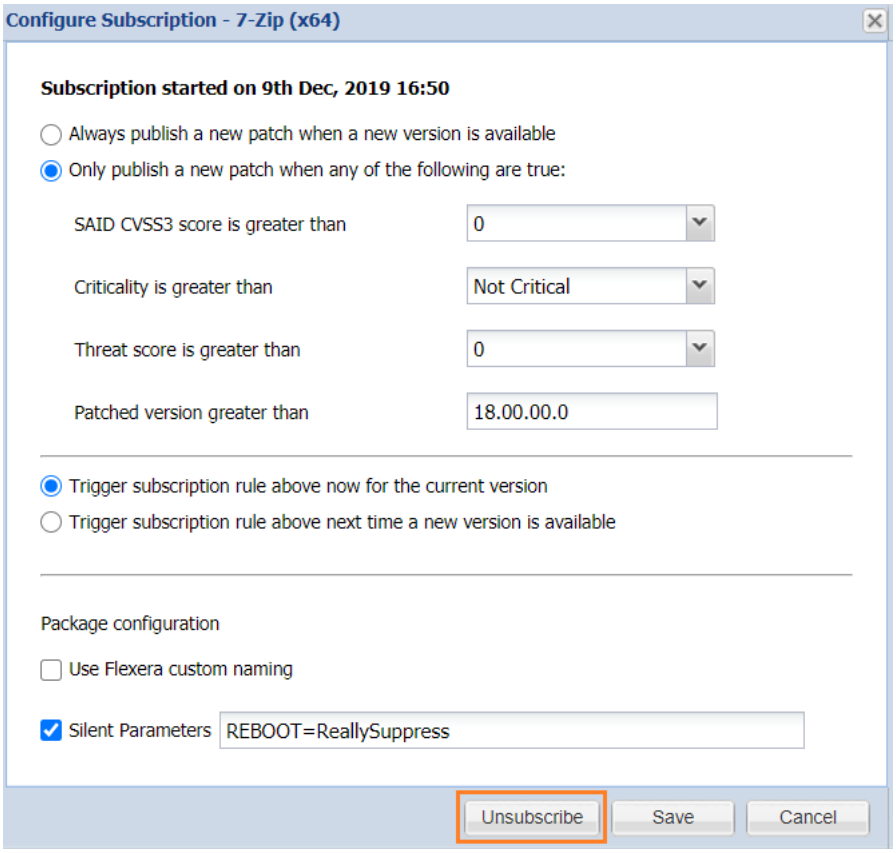


2. Choose your preferences and select your deployment schedule. Click **Save**.

Note • *To unsubscribe the subscription, see Edit Subscription.*

Edit Subscription

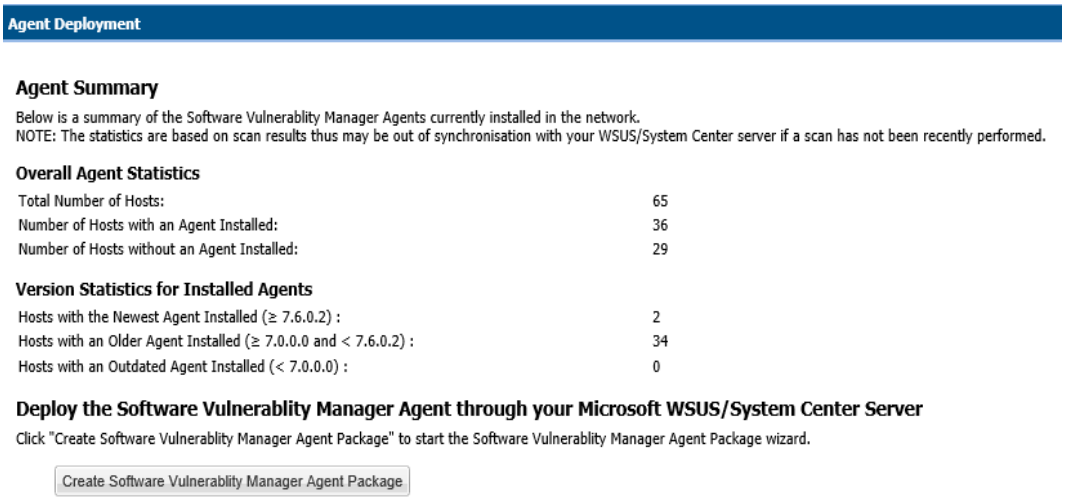
If the package is already subscribed as explained in Subscribe to Package, you can right click and select **Edit Subscription** to edit the configured preferences. To unsubscribe the subscription, click **Unsubscribe** button.



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.

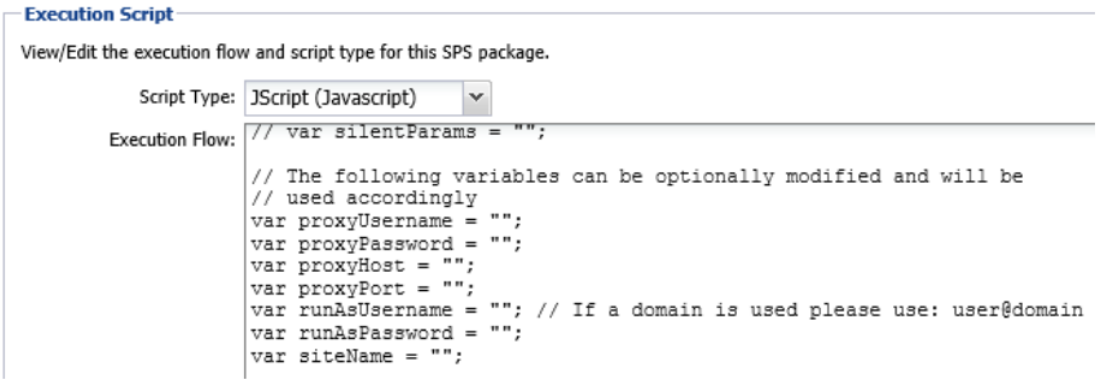


The Software Vulnerability Manager Agent Package can be created and managed just like any other SPS package. You can also Add Proxy Settings.

SVM Agent Deployment Package Configurations

The Agent Deployment package allows the configuration of a variety of agent installation options that can be used to customize the agent prior to deploying the package.

The command-line options of the agent can be set in the script that is provided at step 2 of the SPS Agent Deployment package configuration wizard.



Configure **runAsUsername** when you intend to install and run the agent under service account different than **LocalSystem**. You are required to configure the **runAsPassword** together with that.

Configure **runAsUsername** and **runAsPassword** when the network proxy will block **LocalSystem** to perform online connections. Then you will be required to use a service account to run the agent as an authenticated user to have it easily bypass network blocking.

Configure **ProxyUsername** and **ProxyPassword** variables when the username and password for the network proxy are not shared with active directory and are verified only against the proxy server.

Configure **proxy host** and **proxyPort** variables when you want to specify which proxy should be used by the local agent to successfully connect to its target online servers at Flexera.

Configure the **SiteName** variable when you want to define a custom site grouping in the management interface. This method should never be combined with the use of Active Directory feature in Software Vulnerability Manager. You must decide which you will use and stick to it.

SiteName is also used when extra options like debugging parameters or scan interval randomization commands must be included in the installation command of the agent.

The next command will install the agent with custom site Hi, scan interval 30 minutes, and will create a log file of the installation of the agent that will run until you uninstall the agent.

```
siteName = “Hi –si 30 –d c:\agent-log.txt –v”;
```

Preliminary Package Testing

After your settings are configured in the script SPS gives you the option to export the file on the local file system and execute it. The exported file is always called sps.exe. This executable is ready to install, and it includes the settings you have set in the execution flow script.

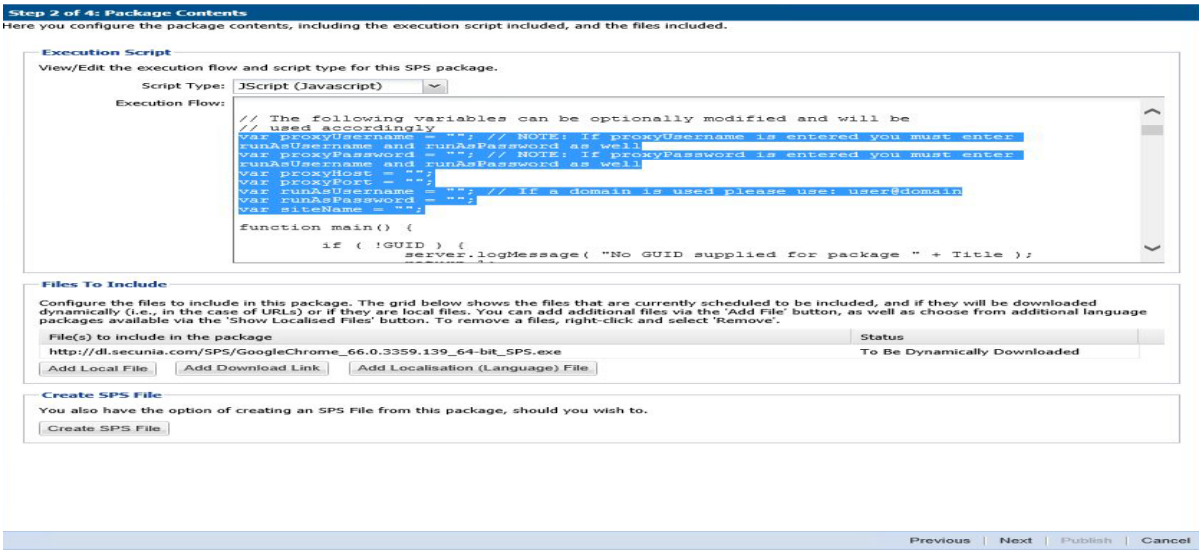
For each script change, you can export different package and test until you get a working package. This is your final goal, an agent deployment package that installs an agent that successfully communicates with its server without errors.

Agent Package Applicability

The agent deployment package enables you to publish the installer as a software update to WSUS. Its applicability rules are set to always install. It will execute on any endpoint where it has not been installed, or where a previous agent version exists without having to pass SCCM package applicability evaluation which is traditional for every other 'update' type of package published through SVM.

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.



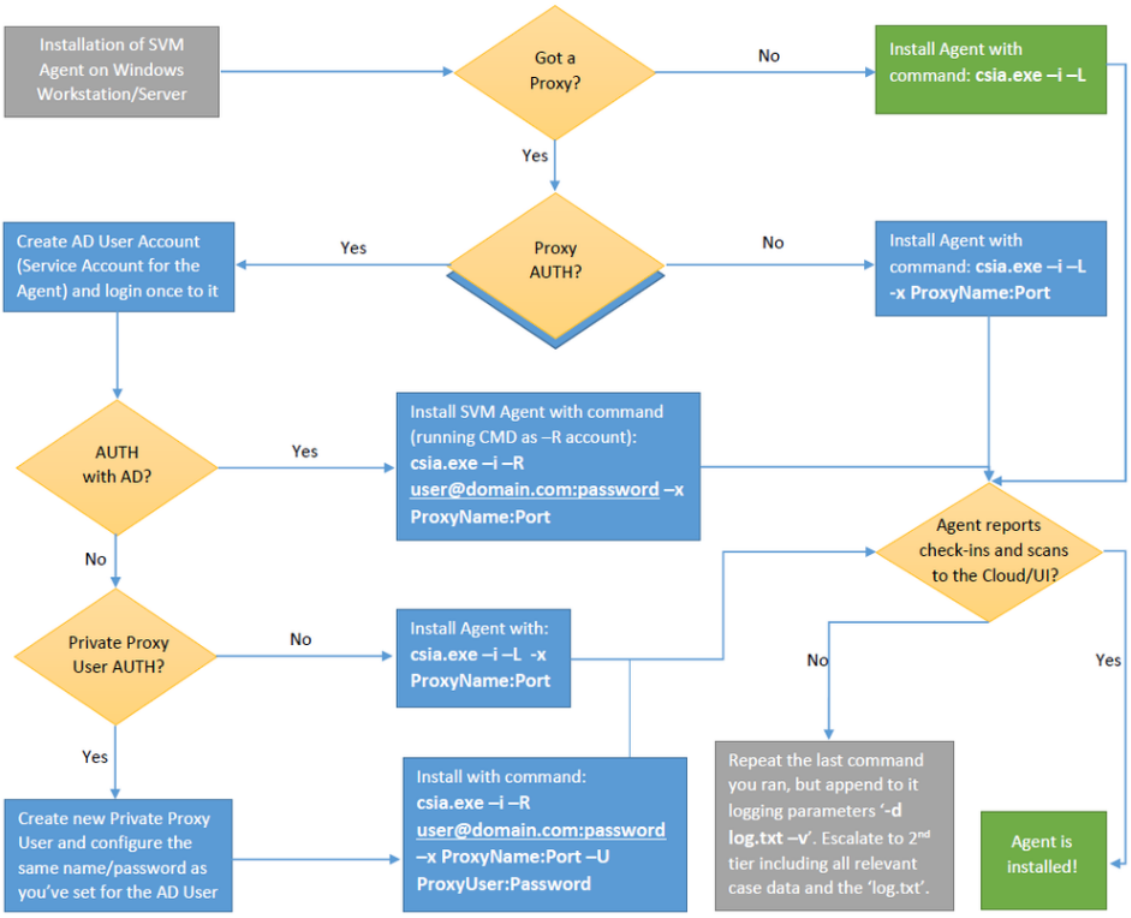
SVM Agent Deployment Logic to Avoid Proxy Blocking

When there is a proxy on the network, in many cases you might be best suited to install agents under managed domain service account which can authenticate through the proxy successfully, especially when the LocalSystem account is disallowed to connect online by Proxy or local domain policies.

When there is no proxy or the existing proxy does not require client/user authentication to allow online access, installing the Single Host Agent under LocalSystem account and setting up the netsh winhttp forwarding to the correct proxy server is sufficient to have the Agent bypass the network successfully.

You should use this logic flow to match the correct way to set up your Agent based on the networking requirements of your estate. -L symbolizes installation under "LocalSystem" while -R symbolizes "RunAs" installation under a managed domain service account.

This type of planning can save you from having to revert to a different configuration because of network proxy blocking and permission problems that prevent SVM Agents to report back scan results.



You can use automated deployment and configure the correct parameters in the Agent configuration. For more information see, SVM Agent Deployment Package Configurations.

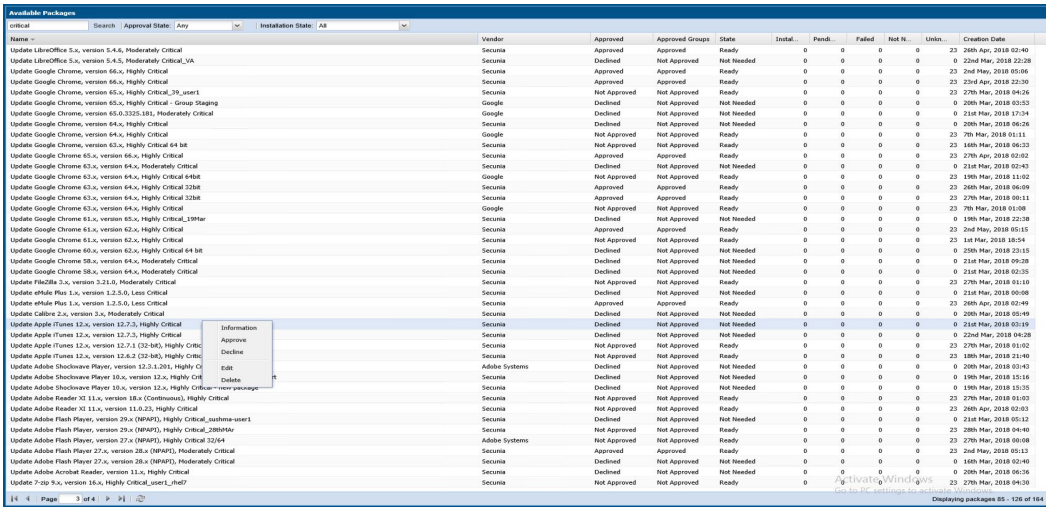
WSUS/System Center

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.



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.

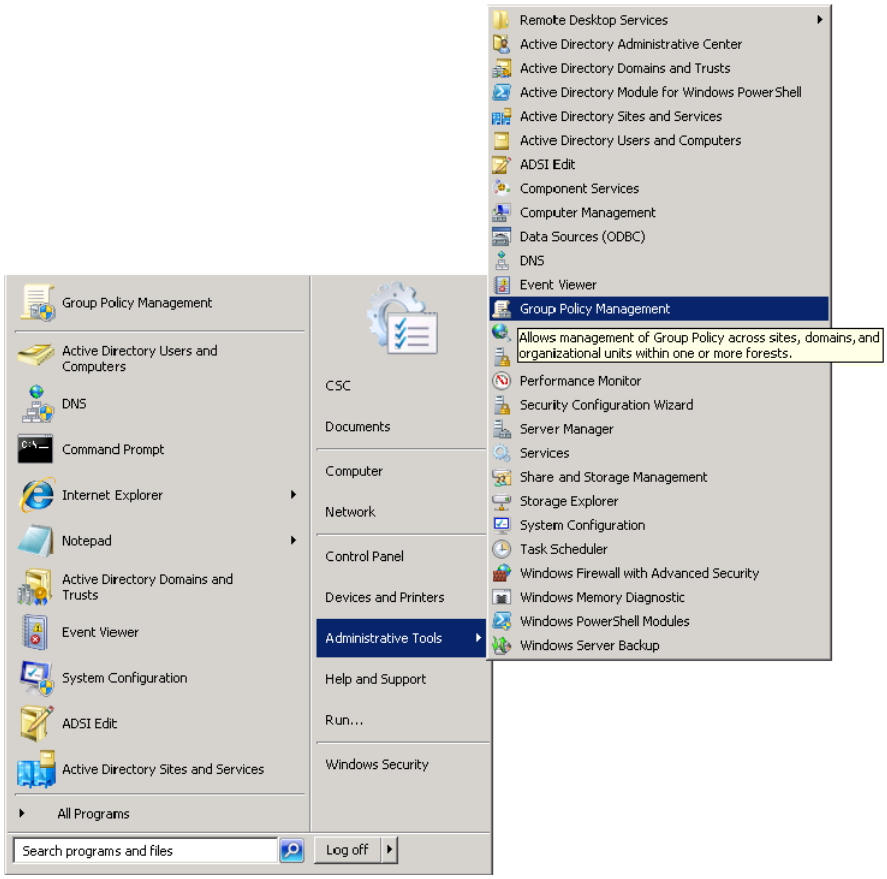
In order for Software Vulnerability Manager to connect to WSUS and to create packages successfully, Internet Explorer must be run **As Administrator** in most cases (right-click and select Run as administrator). Also note that the Remote Registry must be enabled on hosts for which you intend to install 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.

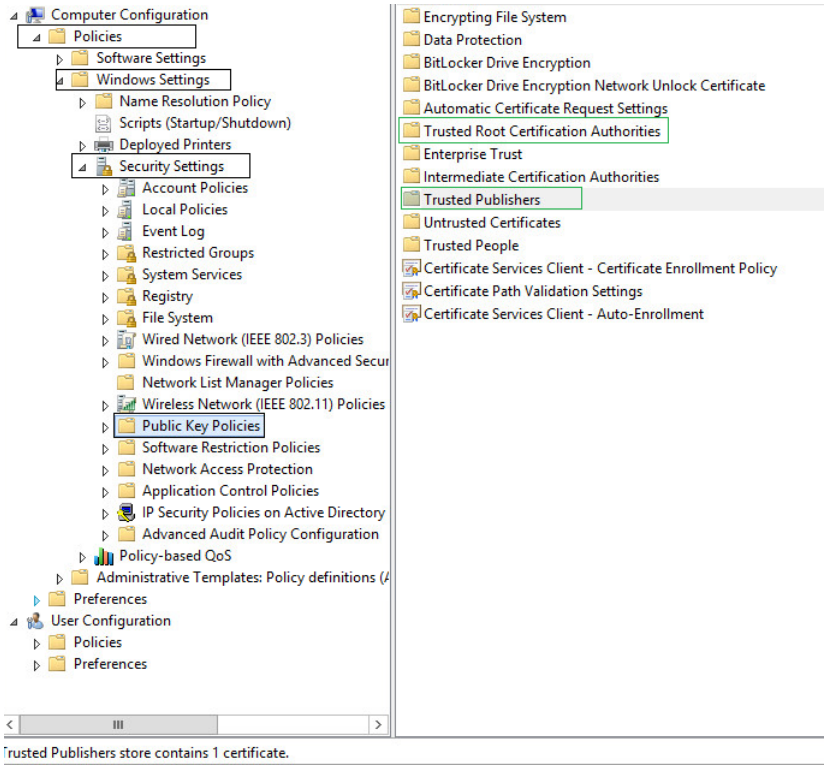
Creating the WSUS-CSI GPO Manually

Task ***To create the WSUS-CSI GPO manually:***

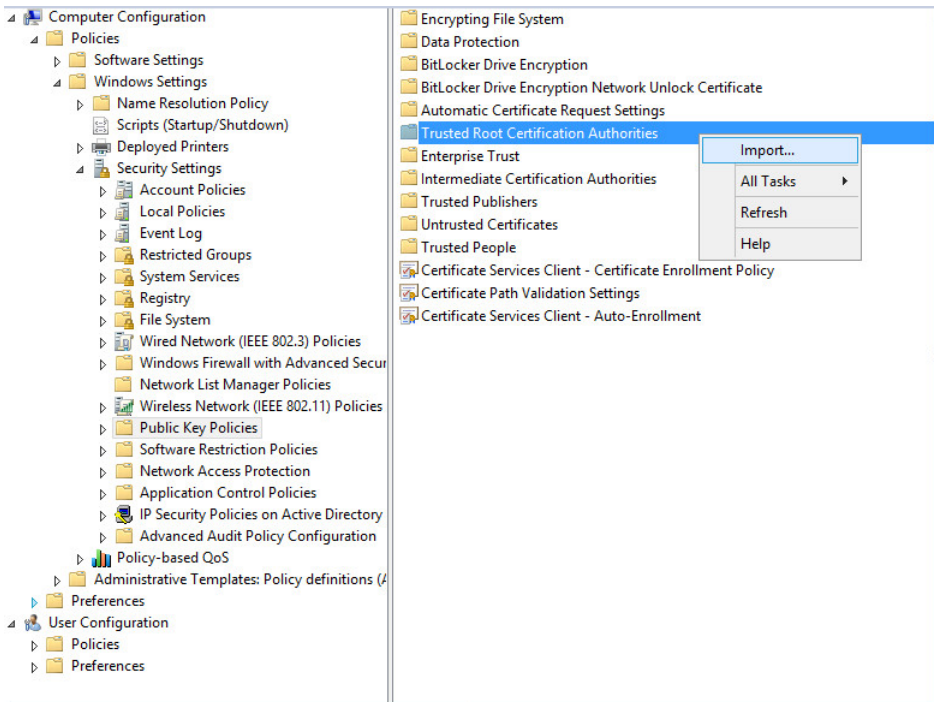
1. Export the WSUS Self-Signed Certificate.
2. On the Domain Controller, click **Start > Administrative Tools > Group Policy Management**. Right-click your Domain name and select **Create a GPO in this domain, and Link it here**. Alternatively you can edit an existing GPO.



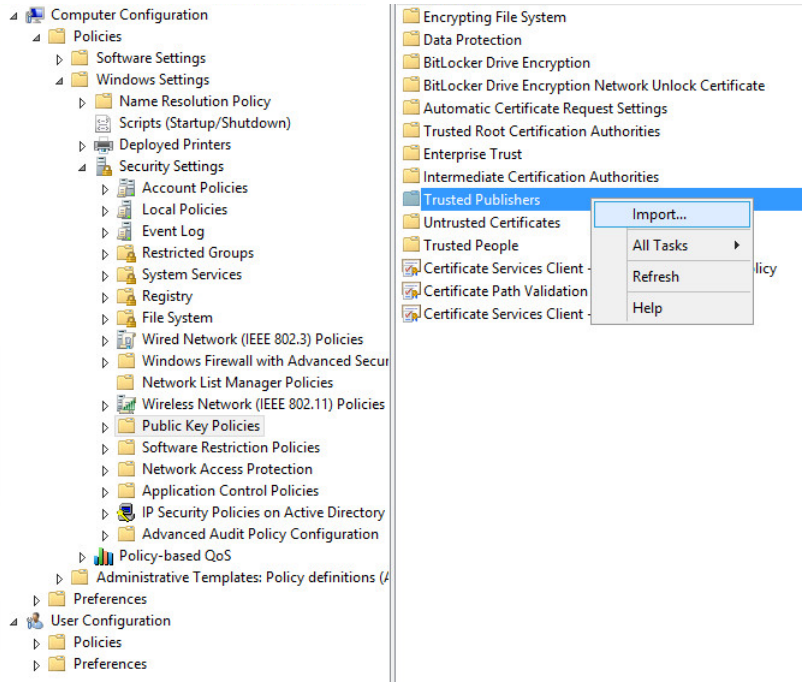
3. Right-click the GPO that you created/edited in the previous steps and select **Edit**.
4. Navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.



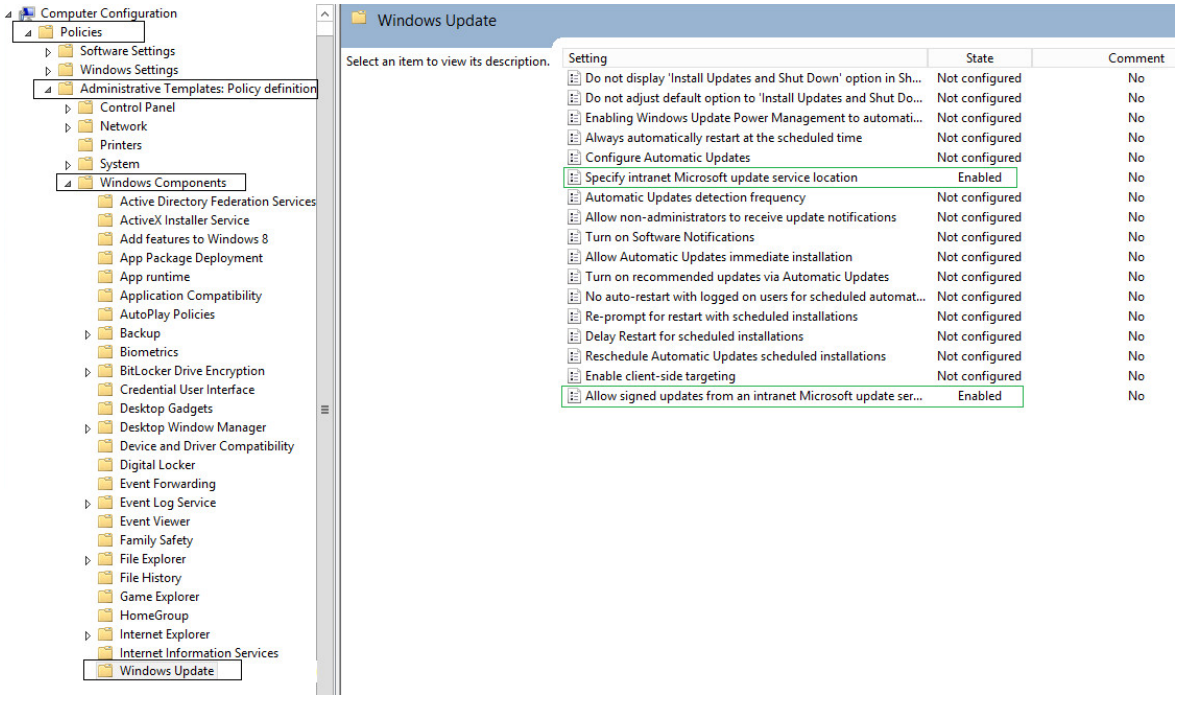
5. Right-click **Trusted Root Certification Authority** and select **Import**. Import the certificate that you exported in Step 1.



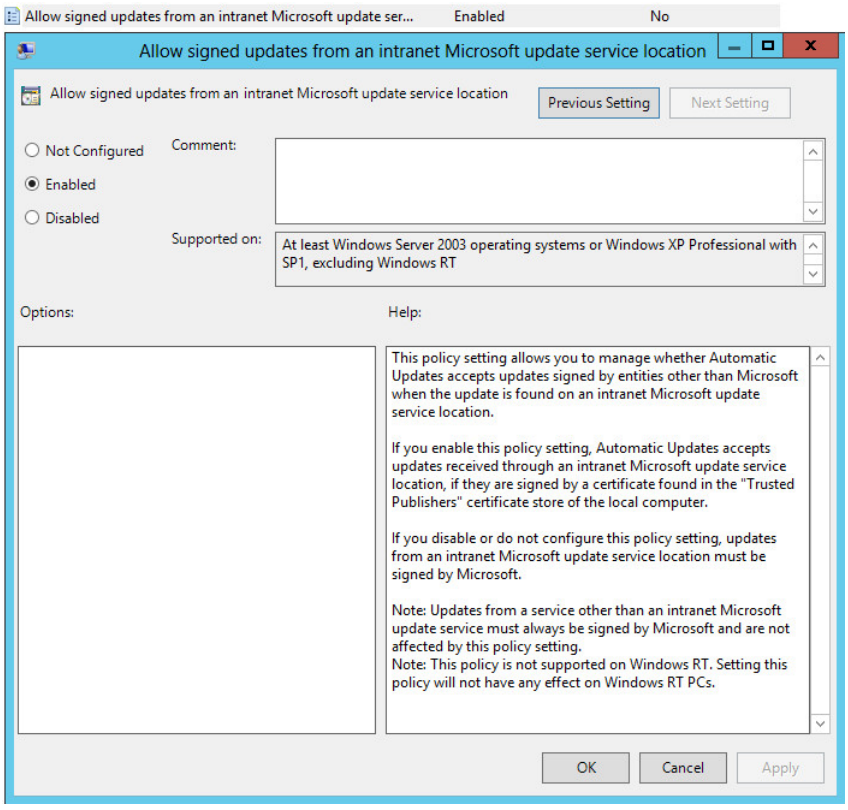
6. Repeat Step 4 and import the certificate for **Trusted Publishers**.



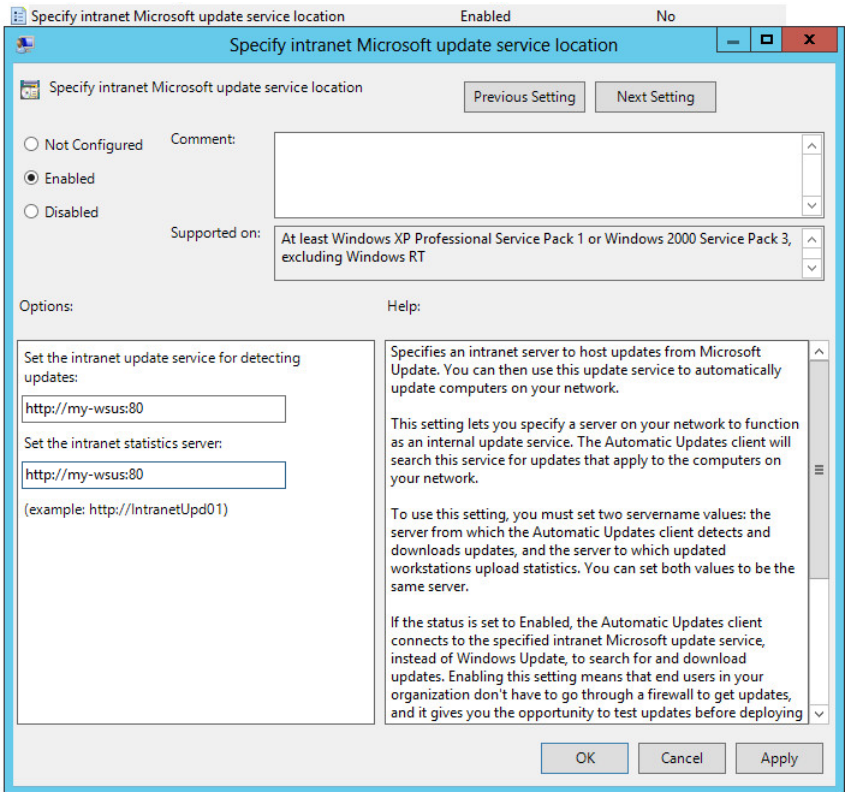
7. Navigate to **Computer Configuration > Administrative templates > Windows Component > Windows Update**.



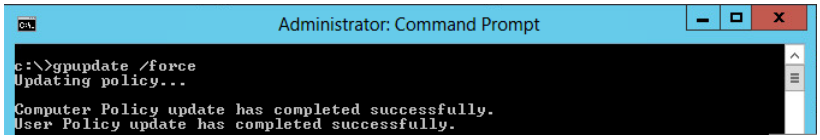
8. On the right side menu, double-click **Allow signed updates from an intranet Microsoft update service location**. Select **Enabled** and click **OK**.



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.

Integrate SVM with WSUS/SCCM and Deploy a Patch

Users often require additional help for the logical process workflow when it comes to integrating the Software Vulnerability Manager software to their internal WSUS or SCCM servers for patching.

In most, users need additional elaboration on what is the right sequence of steps to integrate SVM and what actions will be needed to troubleshoot expected errors that come in their way as part of the deployment process.

Flexera has made a logic flow map that provides essential knowledge of the steps involved to integrate the SVM to your internal server infrastructure and the steps to troubleshoot basic errors or exceptions that might come in your way while you're performing this process. We also provided an extensive amount of additional information that can help you investigate package errors in the different phases of the deployment process of a package made with SVM and handled for deployment in WSUS/SCCM/CCM.

Customers are highly encouraged to follow this diagram at their best effort, before reporting support cases to Flexera Support, as they would also receive a greater knowledge in learning each step of the integration while following the diagram.

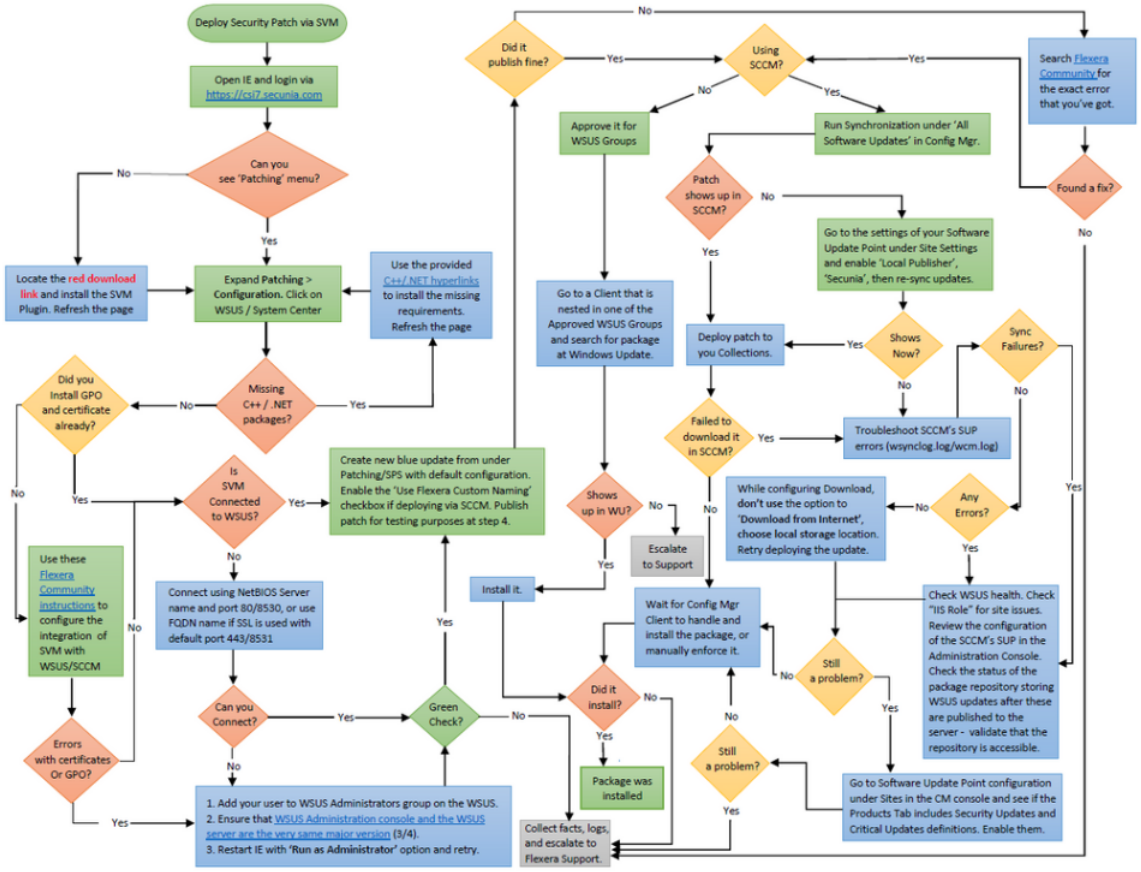


Figure 9-4: Logic Flow Map

You can download the attached PDF document under this KB for a better resolution of the logic map.

Customers are highly advised to include the relevant log files that enable visibility when they send their cases to the Flexera Support team. Depending on where the problem occurred (in which phase), the following log files can be relevant:

Patch Creation phase

If there was a technical problem not covered by the logic flow map, the first course of action should always be to search the error you see inside this Flexera Community site, as Flexera Support issues KBs for each new error that is detected with customers. The chance of finding a solution here is very high.

If that did not help you solve the issue or move further in the mapping process, find the **%userprofile%\My Documents\csi_pluginlog.txt** file on the system where you tried creating a patch and submit that to our Support team adding as much as information about your case as possible.

Patch Deployment phase

The patch was published successfully, but there is an issue with your WSUS server not sending the update to the recipients you approved it for. This may be expected if the recipients did not have the same software already installed (hence, the patch is not applicable, that's why it is not showing up). This is where you have to check the patch applicability rule configured in the SPS wizard -> steps 3 and 4 and verify all enabled requirements of the patch against the clients not receiving it.

If the patch was published to SCCM, you should first and foremost ensure that your SCCM/WSUS (SUP) configuration is intact. If it is and you're successfully publishing Microsoft patches that way, then you can troubleshoot the **wsynclog.log** file for errors that might shed more light on what is causing a problem with the synchronization of the patch between the WSUS DB and the SCCM's own database.

Patch Download/Installation phase

If the patch has shown up and you've deployed it to hosts, but the hosts failed to install it, you can look into the respective client logs for the CCM Client service, Windows Update, or the Secunia Logs as well:

- Check C:\Windows\SecuniaPackage.log for any traces of installation - did package ran to install?

If it ran - patch applicability rules are fine - there's an execution error, however.

If it did not run at all and there are no traces of that - there are most likely patch applicability issues or management point download issues. Such problems can be diagnosed in the log files (to name a few):

`C:\Windows\CCM\Logs\UpdatesDeployment.log`

`C:\Windows\CCM\Logs\UpdatesHandler.log`

- If the patch ran and there's an obvious error in the SecuniaPackage.log file - check the "C:\Windows\WindowsUpdate.log" file next. You can also find more information on the CCM->WUA patch passing in the C:\Windows\CCM\Logs\WUAHandler.log file.

Windows Update is the last service to touch the patch upon execution and the first one to handle the incoming errors - disregarding if you use SCCM or WSUS - that's the case for both scenarios. This log file will contain many lines of error description that you can check against MS Technet first.

- If you deploy patch via SCCM and your WUA service, CCM service, and SecuniaPackage.log all indicate that the package was installed correctly (hence, exit code = 0), but your SCCM is showing wrong compliance of the patch, then you are likely to be looking at a known bug in the CCM "state message" handling of the CCM service that transmits the wrong execution status to its server (for which you can only talk to Microsoft about as Flexera cannot be helpful to solve known CCM-related bugs).

This issue can be identified using some of the following logs:

`C:\Windows\CCM\Logs\StateMessage.log`

`C:\Windows\CCM\Logs\SCNotify_<domain>@>WindowsUsername>`

`C:\Windows\CCM\Logs\SCClient_<domain>@>WindowsUsername>`

as well as the following local WMI classes where CCM stores the incorrectly handled package execution status, and the incorrect state messages being sent to the SCCM server database (to name a few):

`root\ccm\SoftwareUpdates\UpdatesStore -Class CCM_UpdateStatus`

`root\ccm\SoftwareUpdates\DeploymentAgent -Class CCM_TargetedUpdateEx1`

`root\ccm\SoftwareUpdates\DeploymentAgent -Class CCM_AssignmentCompliance`

`root\ccm\ClientSDK -Class CCM_SoftwareUpdate`

`root\ccm\SoftwareUpdates\WUAHandler.`

Patch Configuration

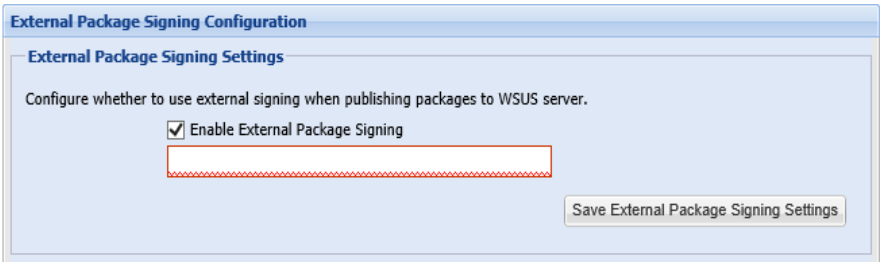
The following patch configurations are available in Software Vulnerability Manager:

- External Package Signing
- WSUS/System Center
- Setting Up Clients to Access WSUS
- Third-Party Integration
- Create and Publish the Package

External Package Signing

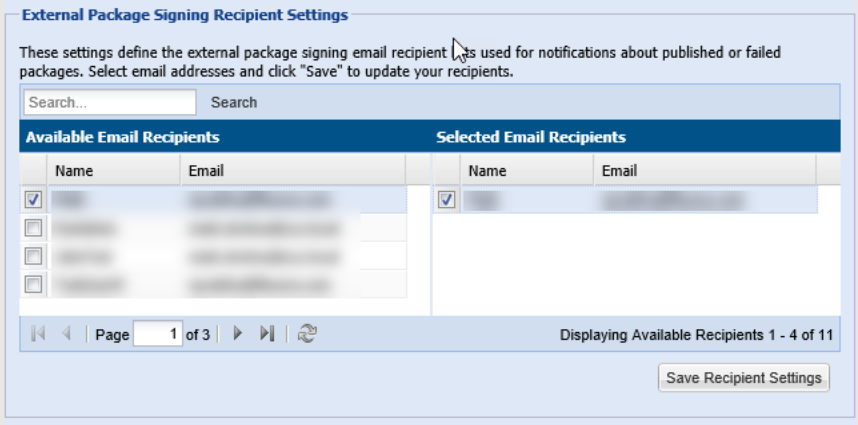
Software Vulnerability Manager allows you to export packages as Cabinet files (.cab) which can be used to publish signed cab files using the Software Vulnerability Manager Daemon. To enable this feature, you must run `daemon.exe -S --publish-dir <PATH>` after the Daemon has been installed. This will 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.*

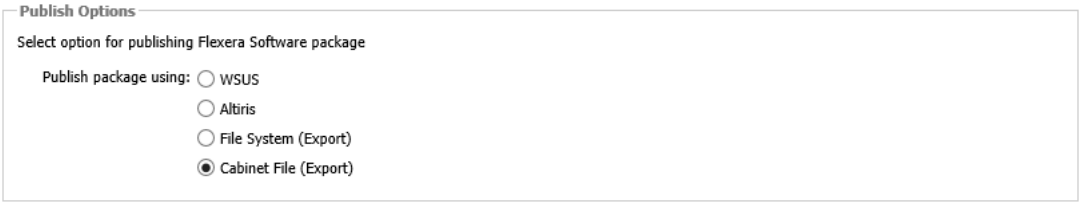


Select **Enable External Package Signing** on the configuration page and provide a path to where the packages will be exported. Similar to the Software Vulnerability Manager Daemon, a subdirectory (`Flexera Software IO`) will be added for security reasons.

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.

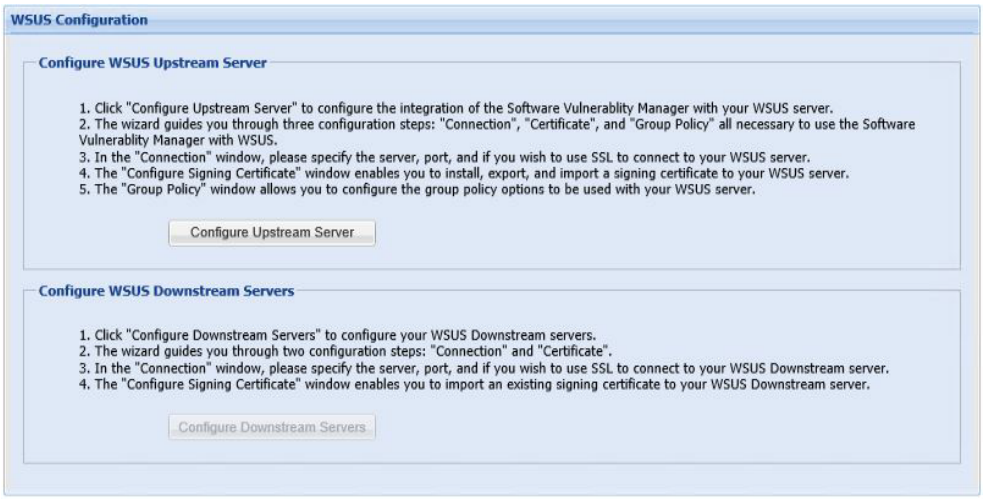
A notification email will be sent to the account email of the user running the Daemon to inform the user know about success or failure for published packages.

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.



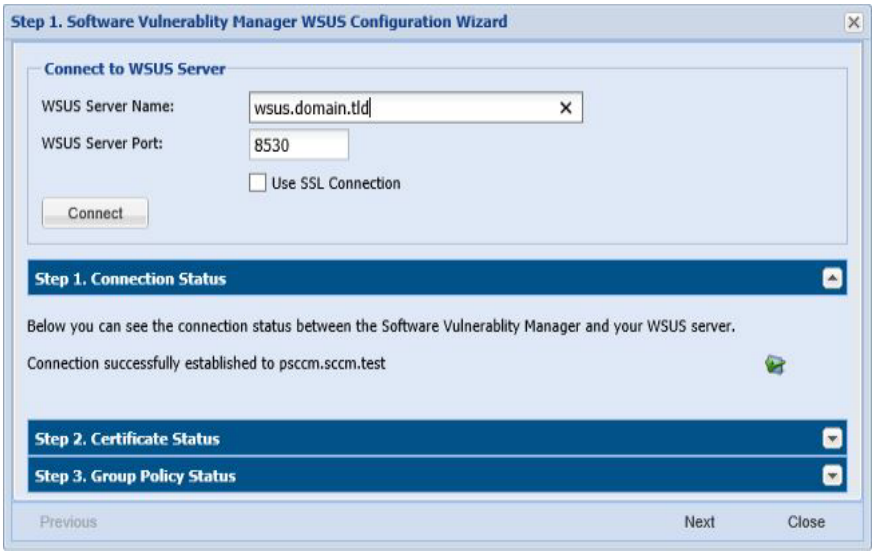
Follow the wizard steps to successfully integrate Software Vulnerability Manager with your Microsoft WSUS.

- Step 1 – Connection Status
- Step 2 - Certificate Status
- Step 3 – Group Policy Status

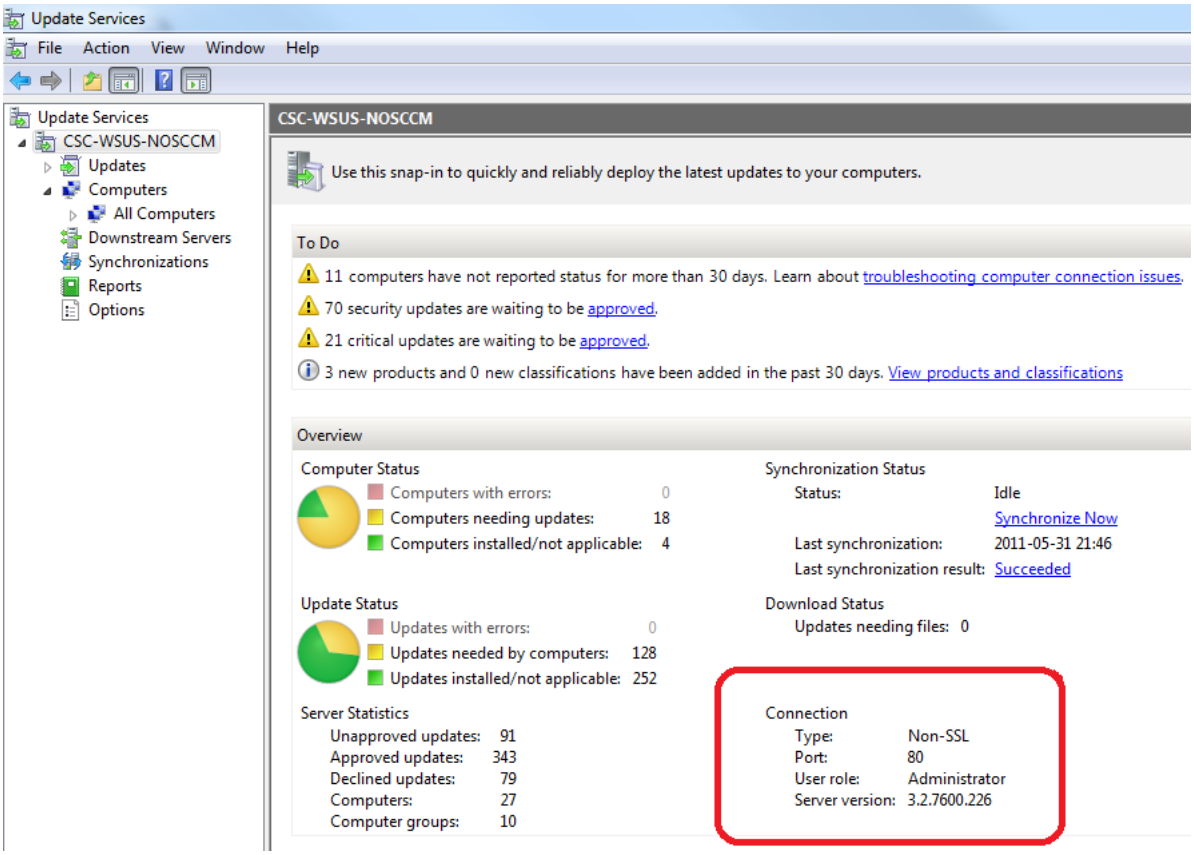
Step 1 – Connection Status

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

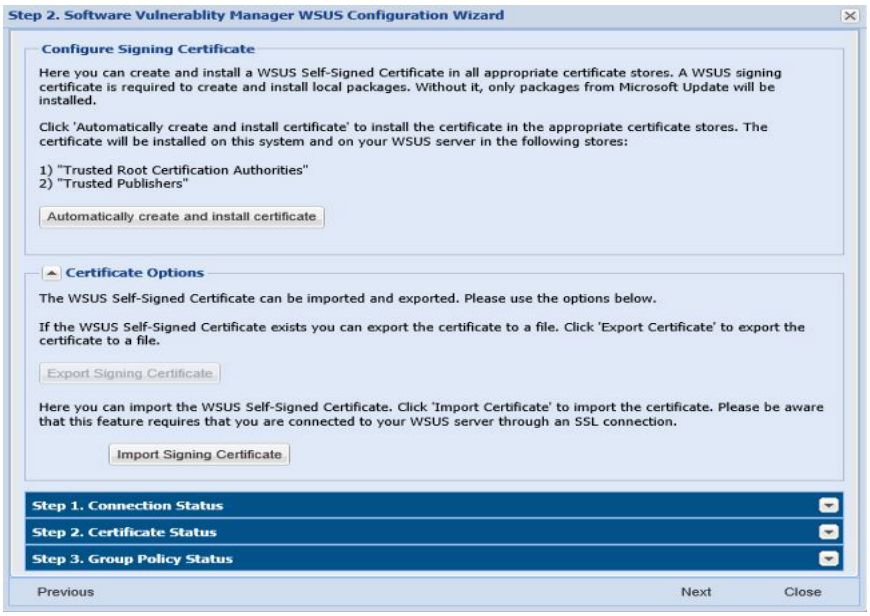
  The system running Software Vulnerability Manager (note that the certificate must also be installed on the system running the Software Vulnerability Manager console)

- 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

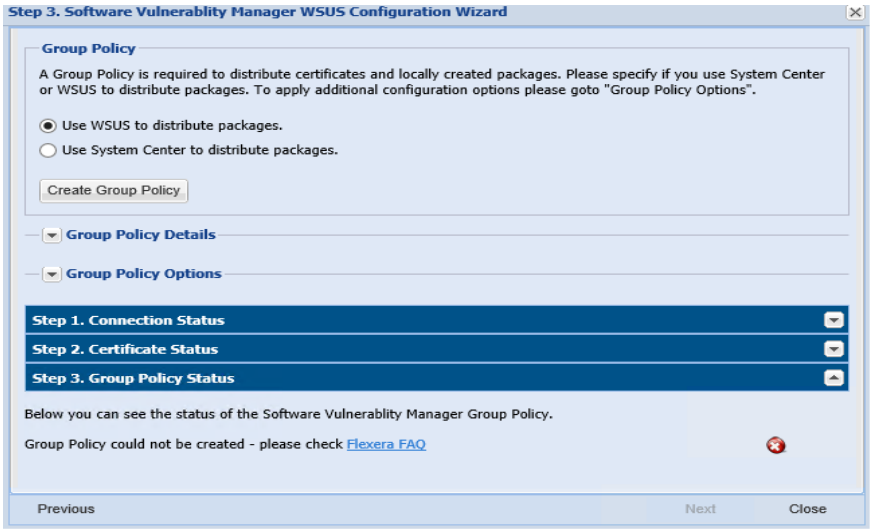
Expand the Certificate Options to access the import and export certificate features.

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)
3. If Windows update not working, then check whether:
   - WUServer contains WSUS server, WSUSStatusServer contains WSUS server:portnumber, AcceptTrustedPublishedCerts:1 in location

     [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]

     ```
     "WUServer"="psccm.sccm.test"

     "WUStatusServer"="psccm.sccm.test:8530"

     "ElevateNonAdmins"=dword:00000001

     "AcceptTrustedPublisherCerts"=dword:00000001
     ```

   - In registry location, [HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU], check"UseWUServer"=1

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

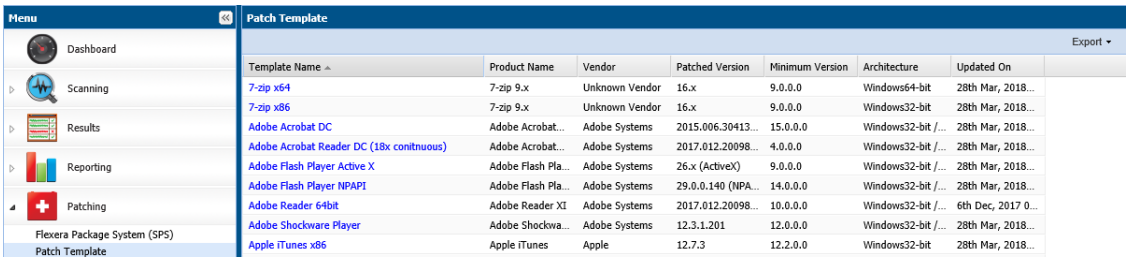
Task ***To create and publish the package:***

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.

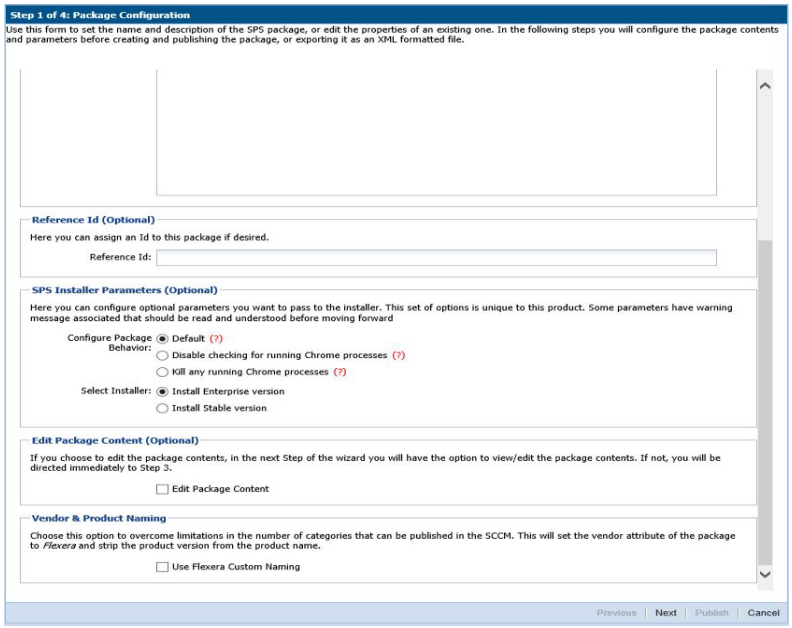
Patch Template

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.

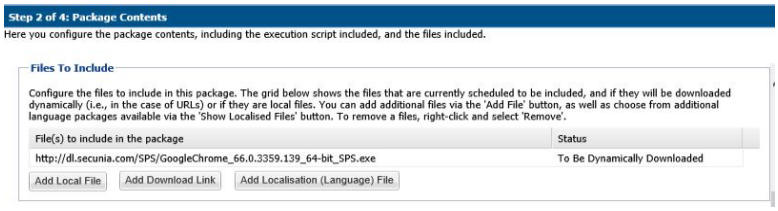


Task ***To create a Patch Template:***

1. 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**.
2. 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.

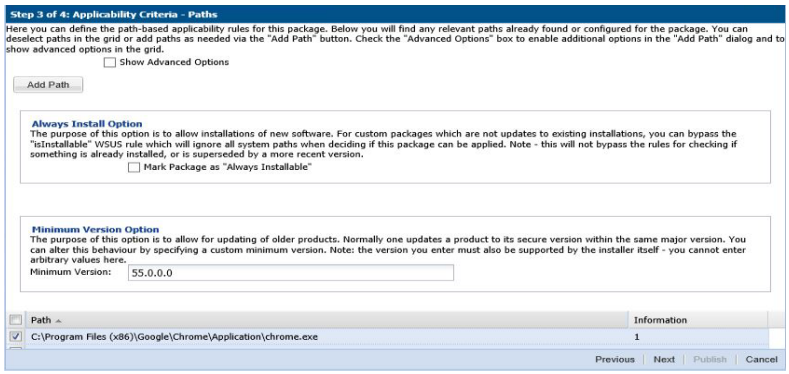


3. Step 2 of 4 of the SPS wizard (**Package Contents**) lists the latest files to include in the package. Click **Next**.

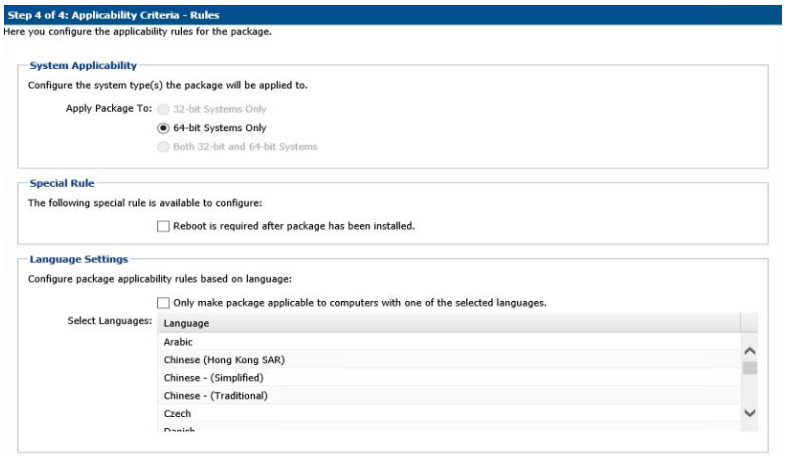


4. In Step 3 of 4 of the SPS wizard (**Applicability Criteria - Paths**), select the appropriate paths to save the package. Click **Next**.

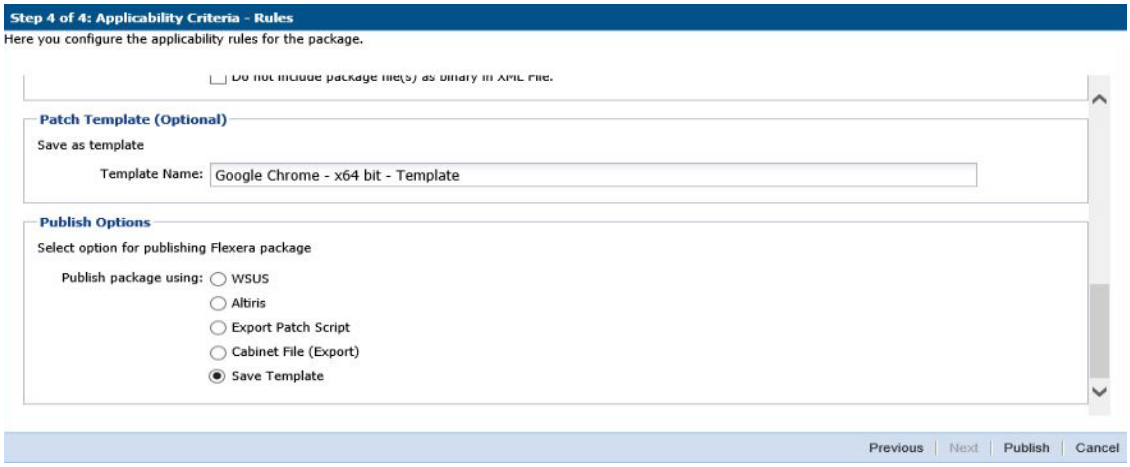
Note • *The Patch Template will always shows paths based on the latest assessment.*



5. In Step 4 of 4 of the SPS wizard (**Applicability Criteria - Rules**), select the appropriate **System Applicability**, **Special Rules**, and **Language Settings**.

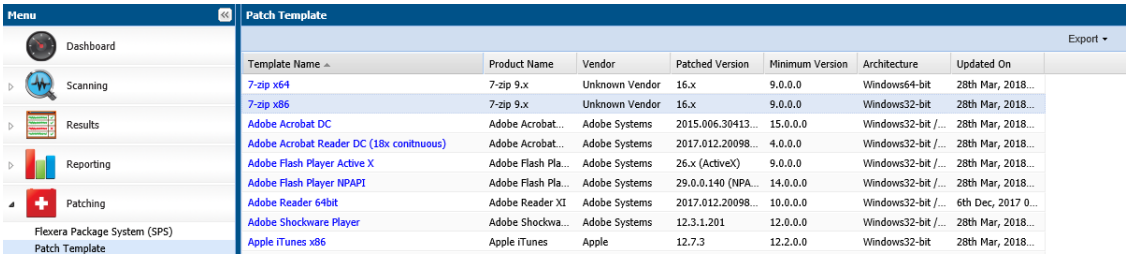


6. In the **Patch Template (Optional)** field, enter the `Template Name` and select **Save Template**. Click **Publish** to create the new template, which is saved under the **Patch Template** tab.



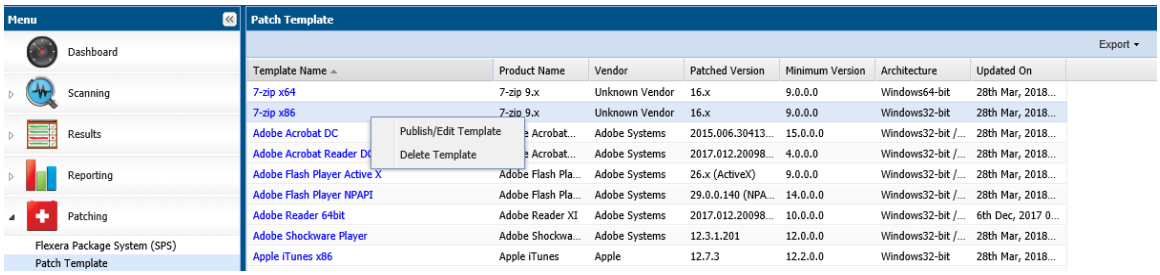
Note • *Providing a template name while publishing a package to WSUS will publish and create a template at the same time. If the template name is empty, it will only publish the package as a regular workflow.*

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.



Task ***To edit a Patch Template or to publish from a Patch Template:***

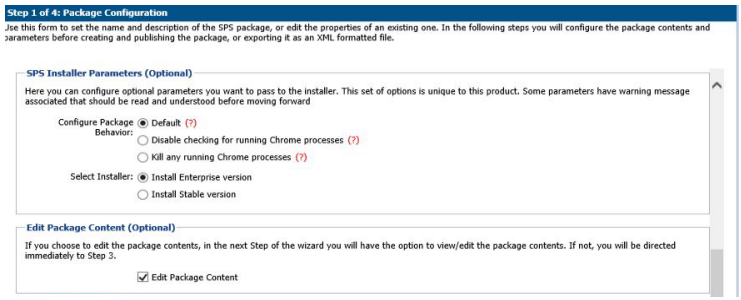
1. From the **Patching > Patch Template** tab, select a template and select **Publish/Edit Template** from the context menu.



2. 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.

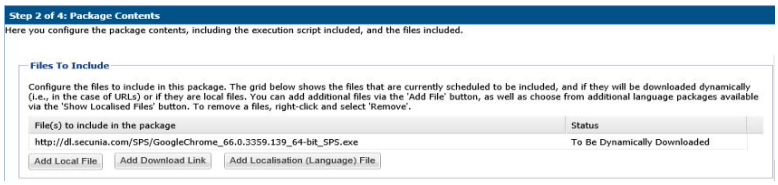
3. To update the Patch Template to the latest patched version:

   - *Select **Edit Package Content** in the Edit Package Content field and click **Next**.*



***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**.*



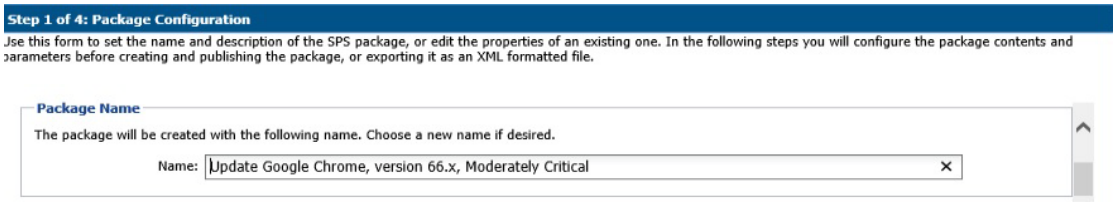
   - *When Step 3 of 4 of the Flexera SPS wizard appears, click **Next**.*
   - *When Step 4 of 4 of the Flexera SPS wizard appears, click **Publish**.*

Task ***To delete a Patch Template:***

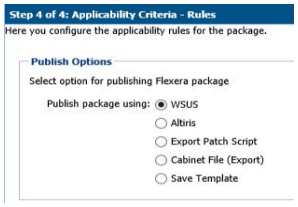
1. From the **Patching > Patch Template** tab, select a template and select **Delete Template** from the context menu.
2. Select **Yes** or **No** to confirm whether or not to delete the Patch Template.

Task ***To publish a Patch Template to WSUS:***

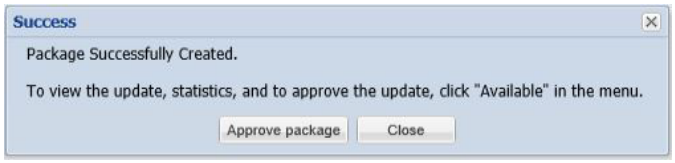
1. From the **Patching > Patch Template** tab, select the template to be published to WSUS. Right click and select **Publish/Edit Template** from the context menu.
2. When Step 1 of 4 of the SPS wizard (**Package Configuration**) appears, update the **Package Name** to indicate this package is for WSUS publishing and click **Next**.



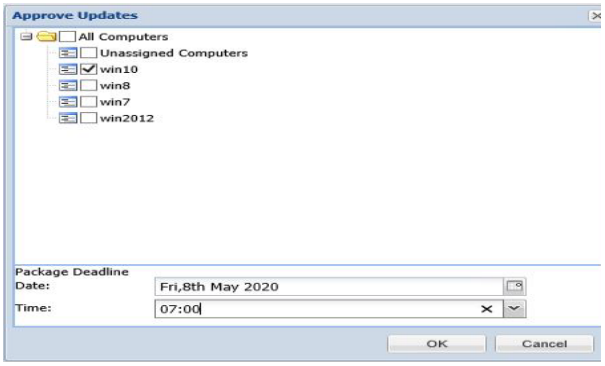
3. When Step 3 of 4 of the SPS wizard (**Applicability Criteria - Paths**) appears, click **Next**.
4. In Step 4 of 4 of the SPS wizard (**Applicability Criteria - Rules**), select **WSUS** for the publishing option and click **Publish**.



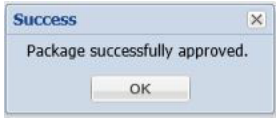
5. The **Attempting to Publish Package - Please Wait** status appears. After the WSUS package is successfully created, a **Success** pop-up window appears. Click **Approve package**.



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**.

QuickPatch

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

To do so, right click on any SPS template or VPM patch and select **Publish with QuickPatch** from the context menu.

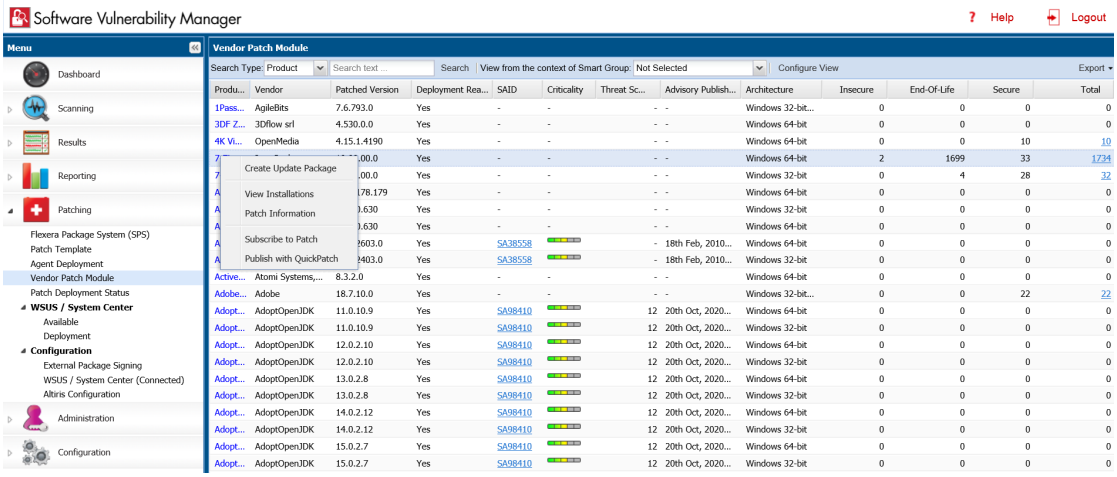


Figure 9-5: Select Publish with QuickPatch from the Context Menu

In the **Publish with QuickPatch** dialog box, select Silent Parameters (if required), and then click **Publish**.

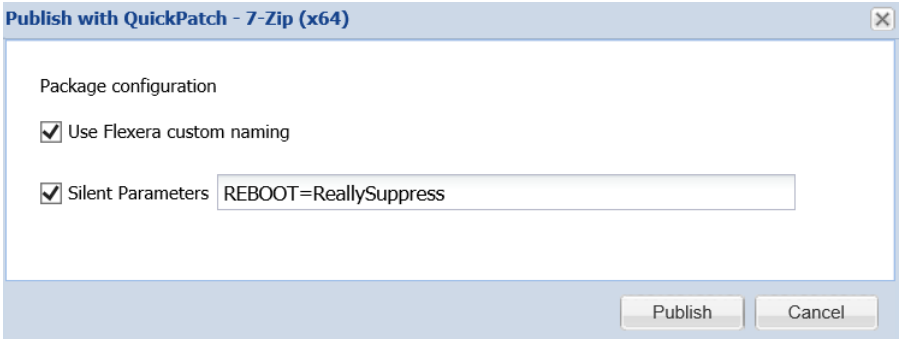


Figure 9-6: Click Publish

Click **Ok** and agree the confirmation dialog which appears.

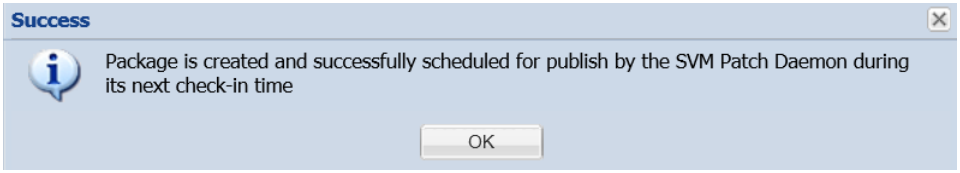


Figure 9-7: Click Ok

The selected patch will be published to Patch Daemon.

Once the patch published, status in the **Patch Deployment status** will appear as **Success**.

If the same version of patch is published, then an error popup will be shown that **Already sent to Patch Daemon**.

Note • *Patches are published based on the versions.*

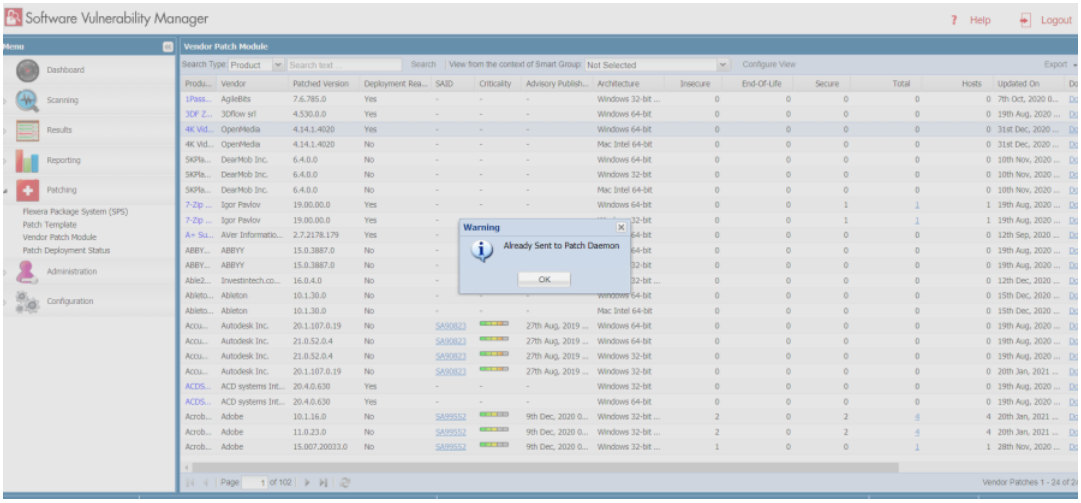


Figure 9-8: Error popup appears

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.

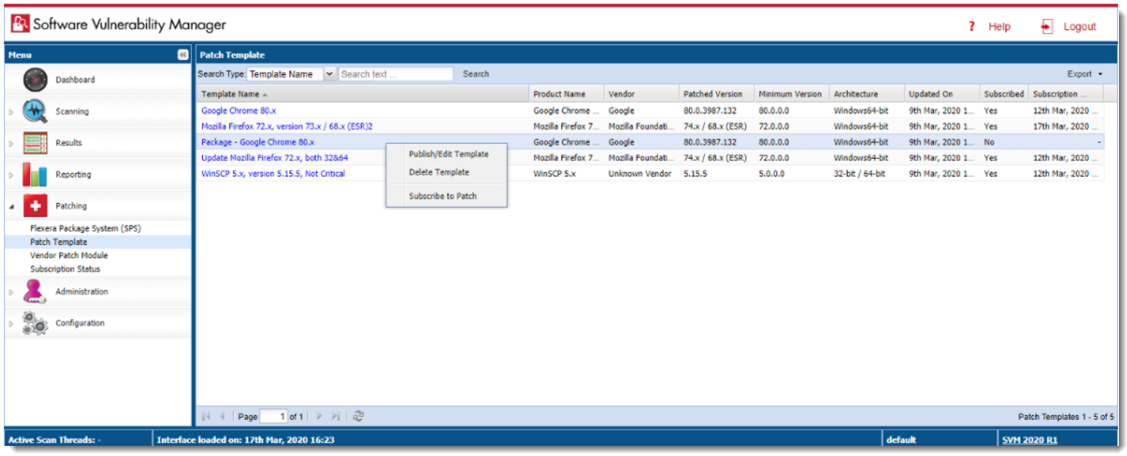


Figure 9-9: Selecting Subscribe to Patch from the Context Menu

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).

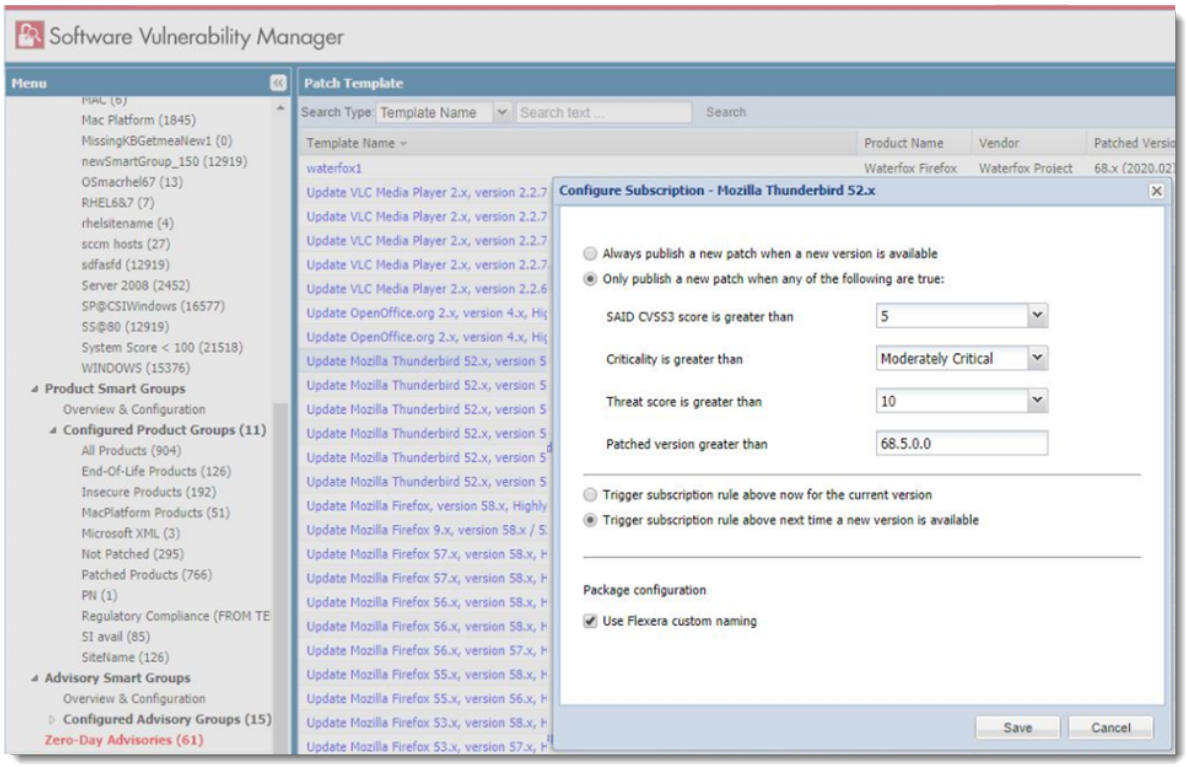


Figure 9-10: Configure Subscription Dialog Box

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.*

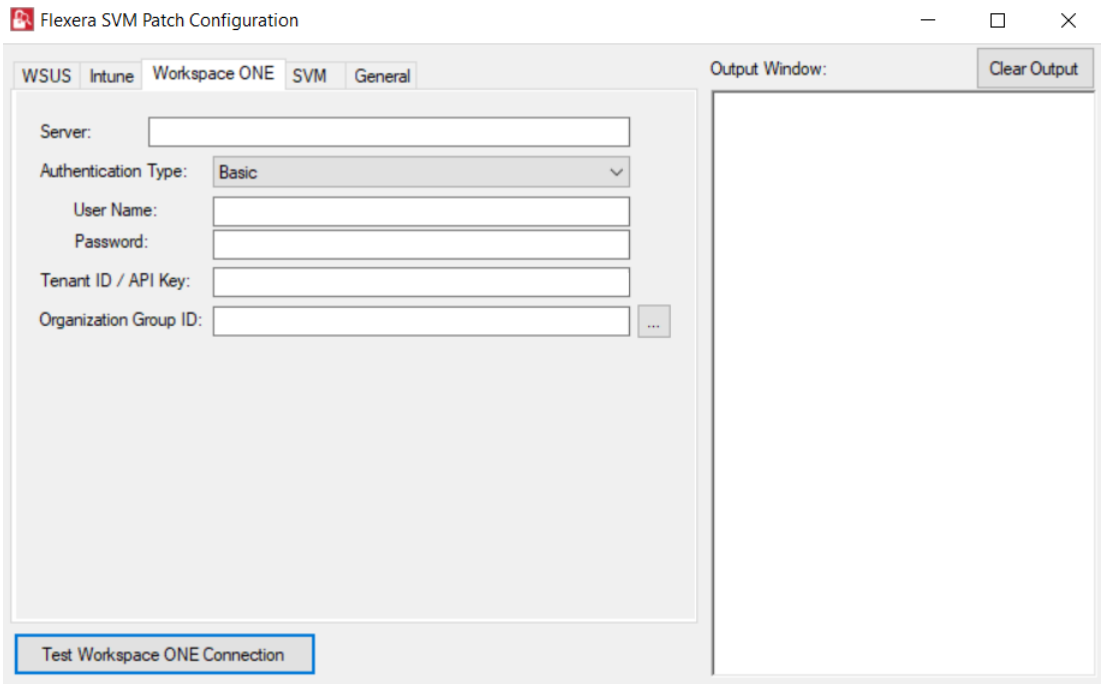


Figure 9-11: Flexera SVM Patch Configuration Dialog Box

You can see the status and details of patches published automatically on a new page named **Patch Deployment Status**, which is opened by selecting **Patch Deployment Status** on the **Patching** menu.

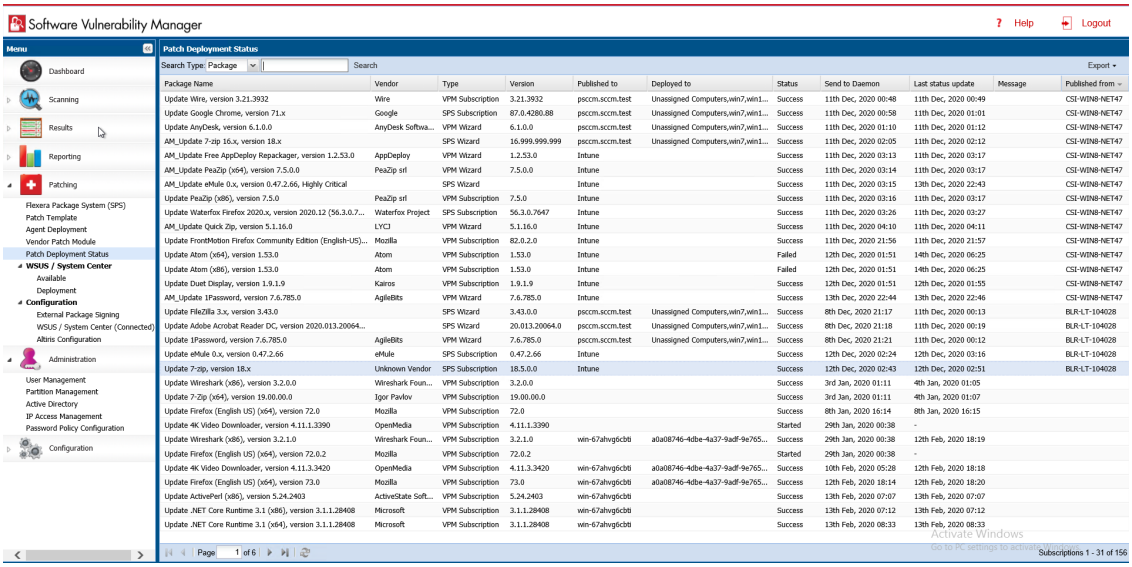


Figure 9-12: Patch Deployment Status Page

All the patch level activities are also recorded in the Activity Log, which is opened by selecting **Activity Log** on the **Configuration** menu.

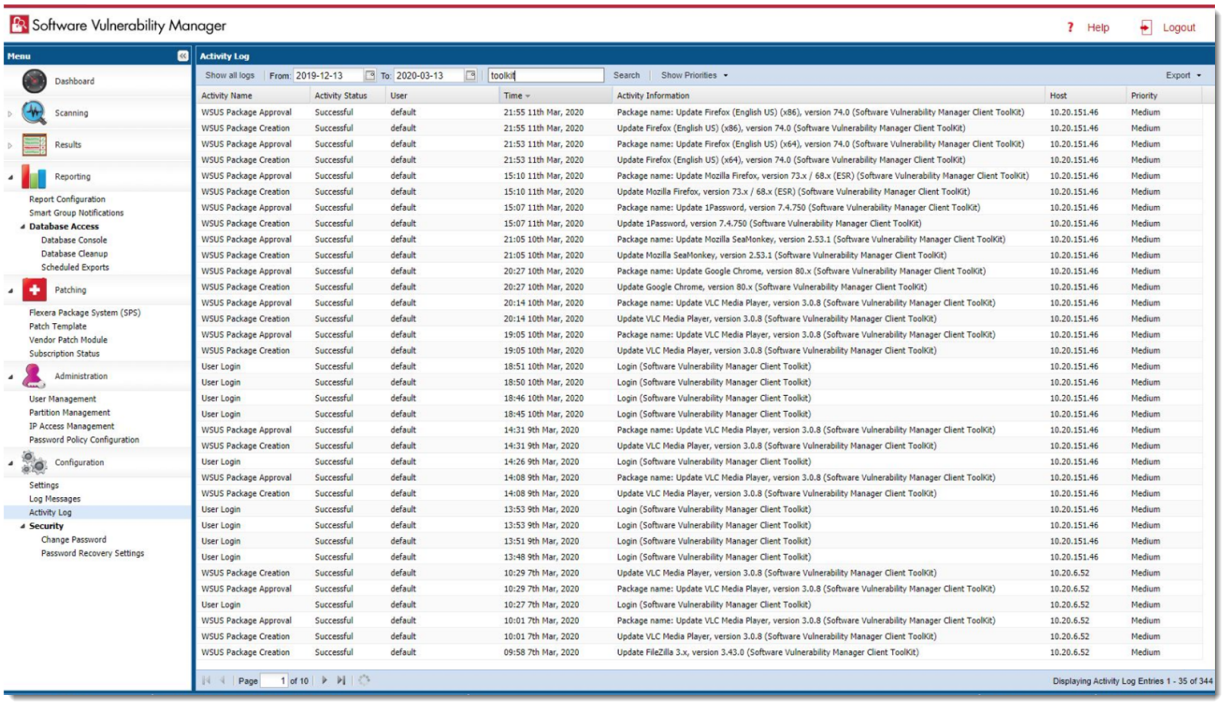


Figure 9-13: Activity Log Page

Unsubscribe Automatic publishing of the Patches

To unsubscribe automatic publishing of the patches, right click on any subscribed VPM Patch, and then select **Edit Subscription** from the context menu.

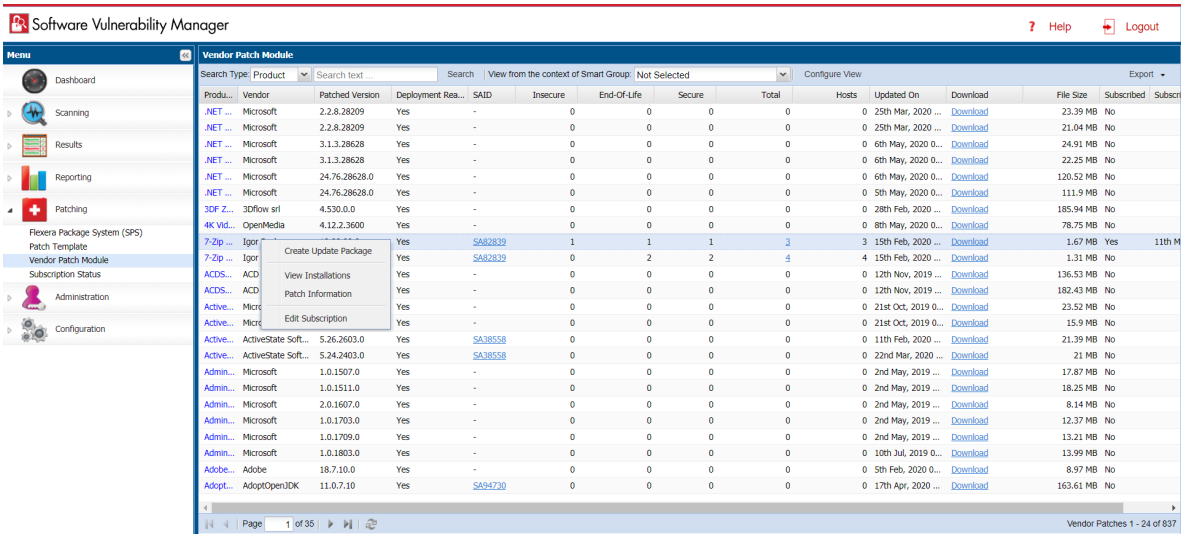


Figure 9-14: Select Edit Subscription

On **Configure Subscription** dialog box, select **Unsubscribe**.

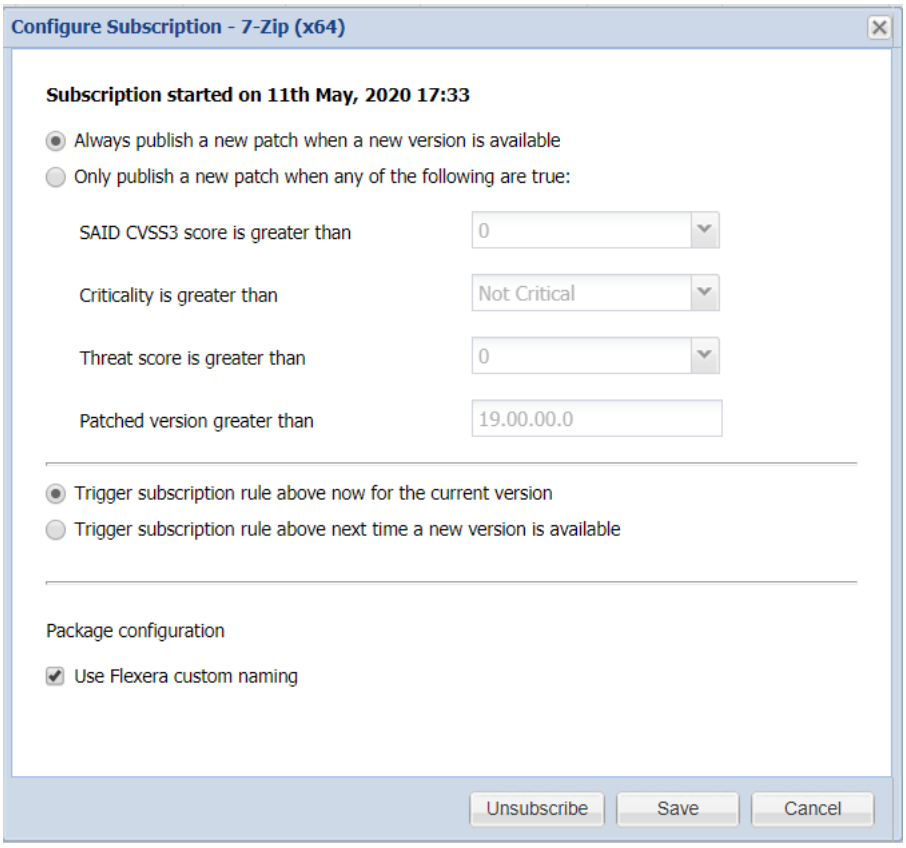


Figure 9-15: Select Unsubscribe

Click **Ok** and agree the confirmation dialog which appears.

External Package Signing for Software Vulnerability Manager Client Toolkit

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

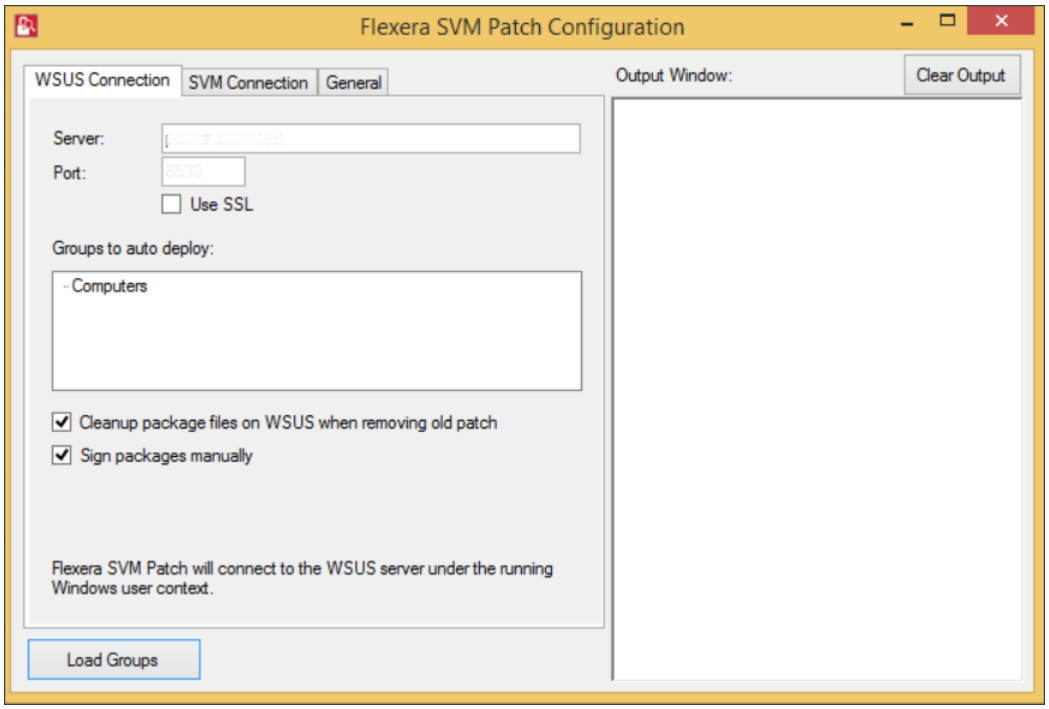
Prerequisites

The below prerequisites are required:

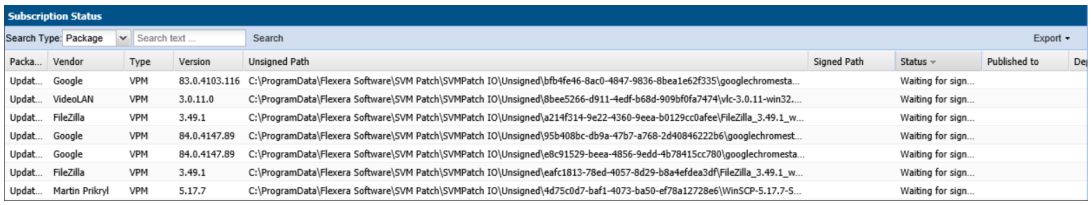
- pfx certificate needs to be installed in WSUS m/c in Trusted publisher and Trusted CA.
- pfx certificate needs to be installed in Trusted publisher and Trusted CA in the m/c where patch daemon is installed.

Task ***To External Package Signing, perform the following steps:***

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



2. Restart the patch daemon.
3. Subscribe VPM packages and wait for patch daemon to fetch the tasks.
4. Patch daemon creates unsigned .cab files and places in the unsigned folder location.
5. The Unsigned folder location is available in the subscription status page as an unsigned path.



6. Sign the cab file using the format below and place the signed .cab file in the signed folder.

   For example:

   C:\ProgramData\Flexera Software\SVM Patch\SVMPatch IO\Signed\package_id\

Note • *Private Keys are typically stored in .pvk files, and public keys are stored in .cer or .pfx files.*

7. During the next check-in, the daemon picks and publishes the signed cab files.

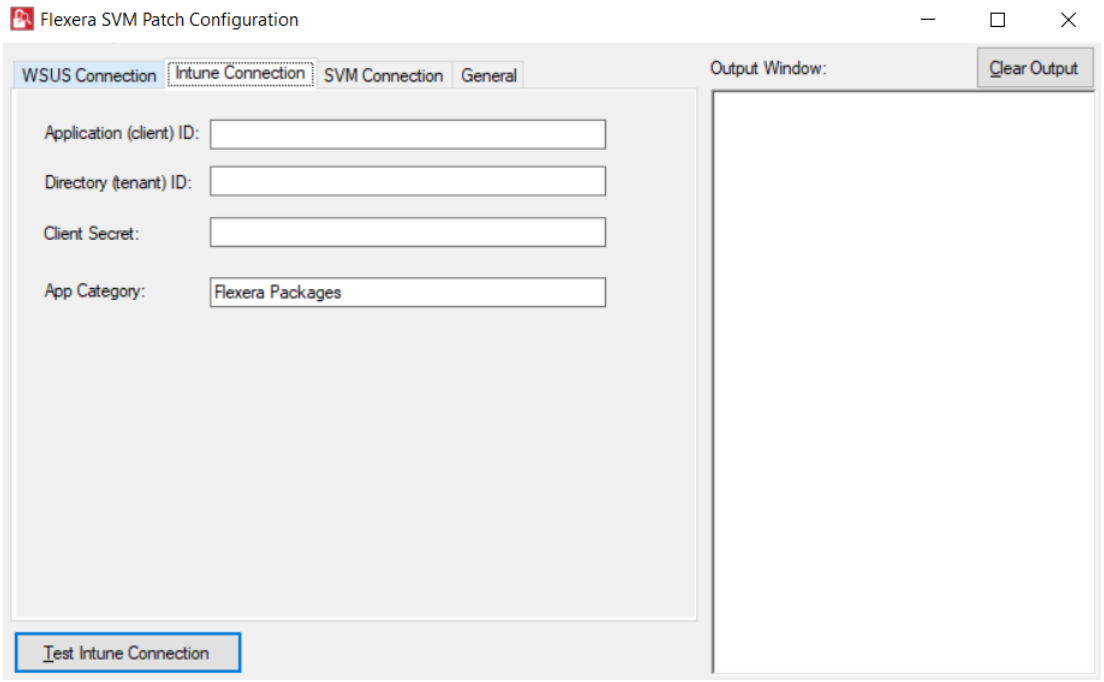
Intune Publishing

Software Vulnerability Manager (On-Premises Edition) can now publish SPS/ VPM patches to Microsoft Intune.

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

To publish patches to Intune, it will be necessary to configure patch daemon with valid Intune credentials and token. For more details, see Set up a Distribution Connection in Flexera SVM Patch Configuration for Microsoft Intune.

For Intune publishing, you can now choose a group or multiple groups and make assignments for end point deployments in the SVM Patch Configuration. For more details. see Assignment Groups.



Once this is setup, you can use either Patch Automation or ActiveX to publish SPS/ VPM patches to Intune.

Note • *Patch daemon convert the patch to intunewin format before publishing.*

Note • *The Patch Daemon may be installed on any workstation or server. The prerequisites are:*

- *For Windows 10 RSAT must be installed which can be obtained here https://www.microsoft.com/en-us/download/details.aspx?id=45520*
- *For Windows 8.1 RSAT must be installed which can be obtained here https://www.microsoft.com/en-us/download/details.aspx?id=39296&displaylang=en*
- *Minimum version of .Net 4.7.2 must be installed.*

Set up a Distribution Connection in Flexera SVM Patch Configuration for Microsoft Intune

To obtain the required credentials to set up a distribution connection for Microsoft Intune, perform the following process.

- App Registration
- Create Client Secret
- API Permissions

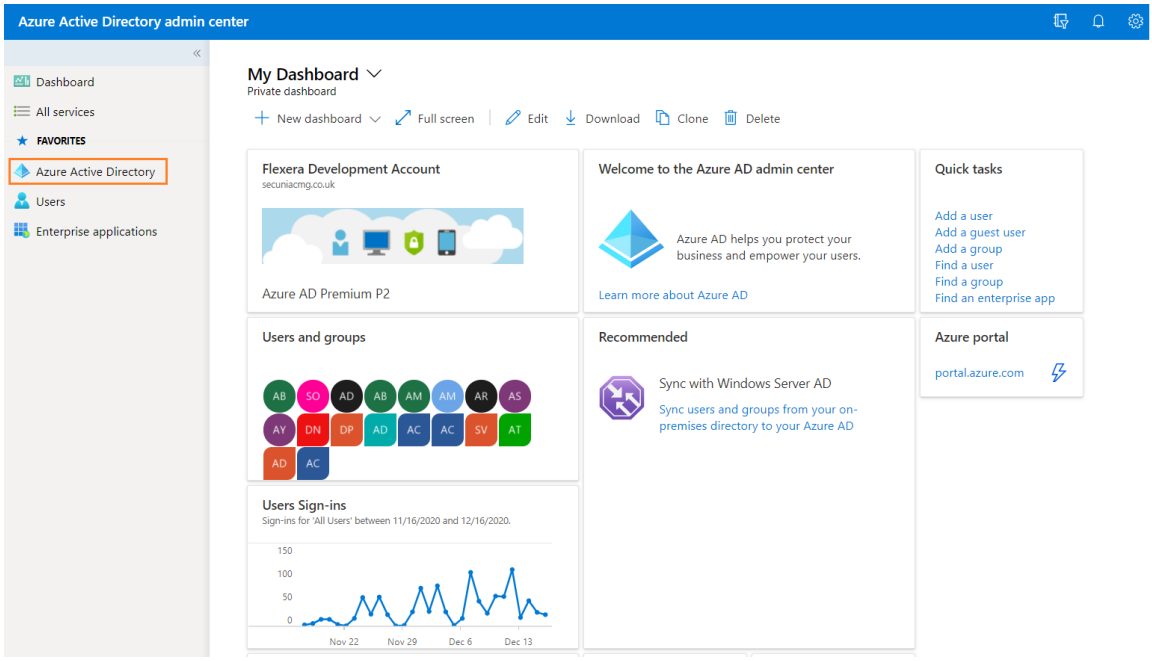
App Registration

To register an application perform the following steps.

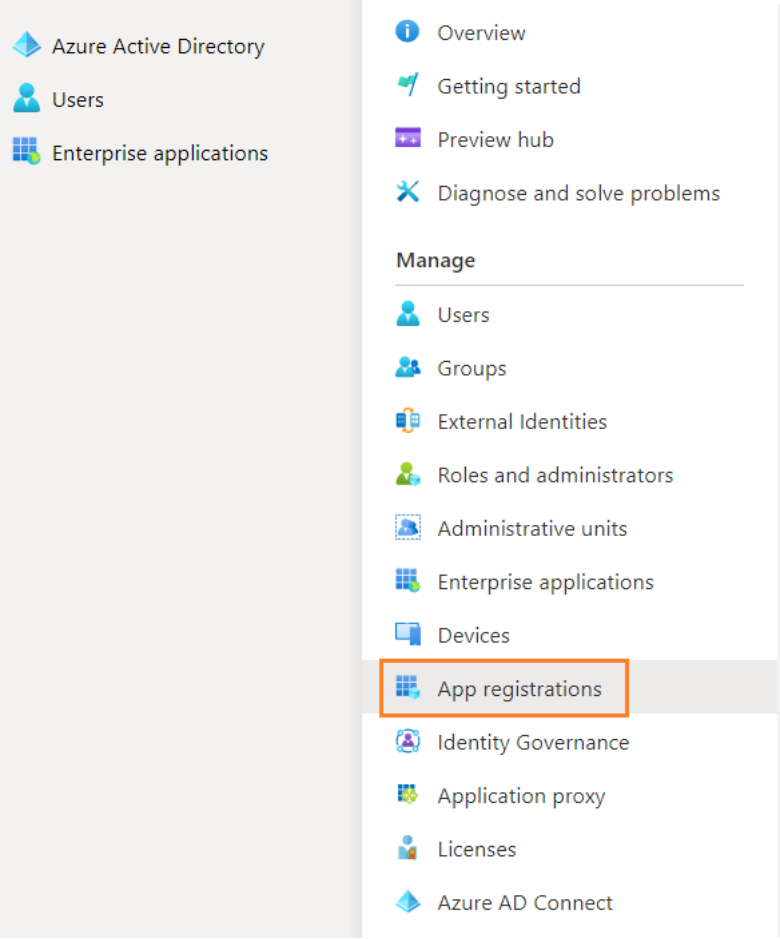
Task ***To register an application:***

1. Obtain login credentials for Intune services on Microsoft Azure.
2. Log in to Microsoft Azure using the obtained credentials.

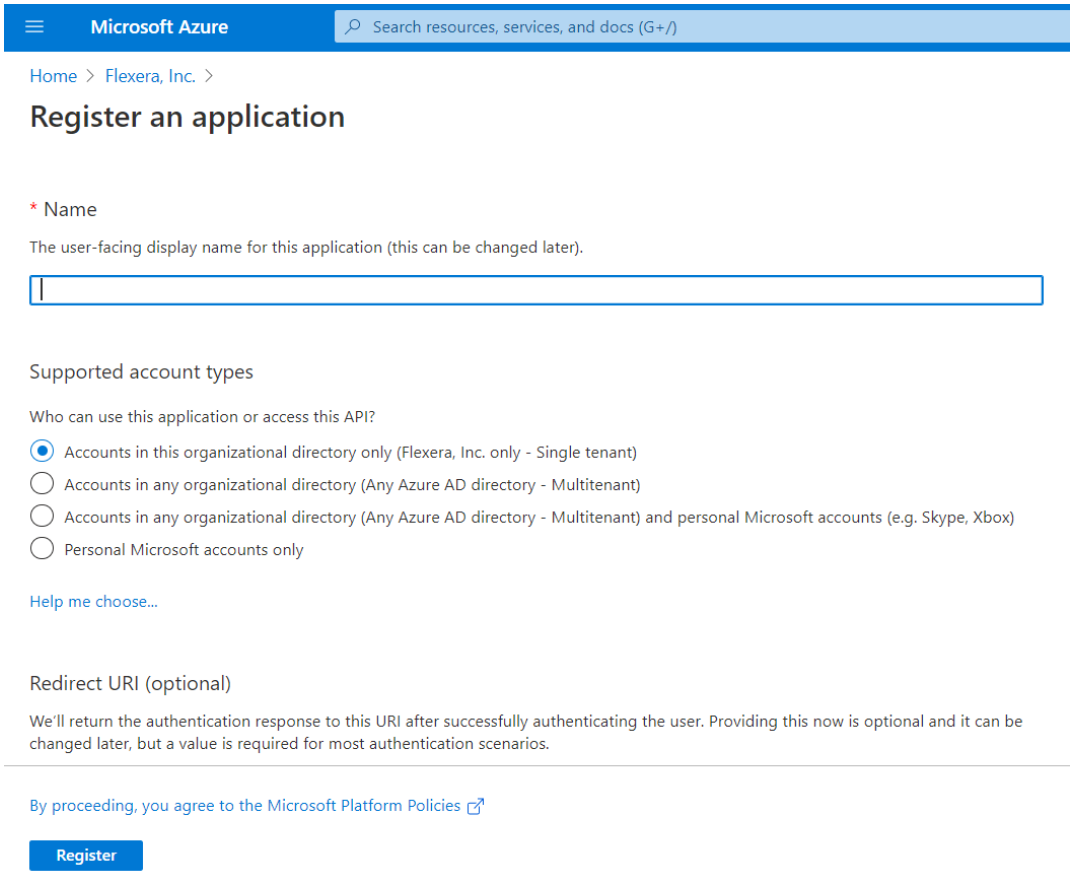
   https://azure.microsoft.com/en-in/account/
3. Once logged in, from the list of available Azure services, choose **Azure Active Directory**.



4. After selecting, it navigates to overview page of the **Dashboard**, select **App registrations** in the left panel.

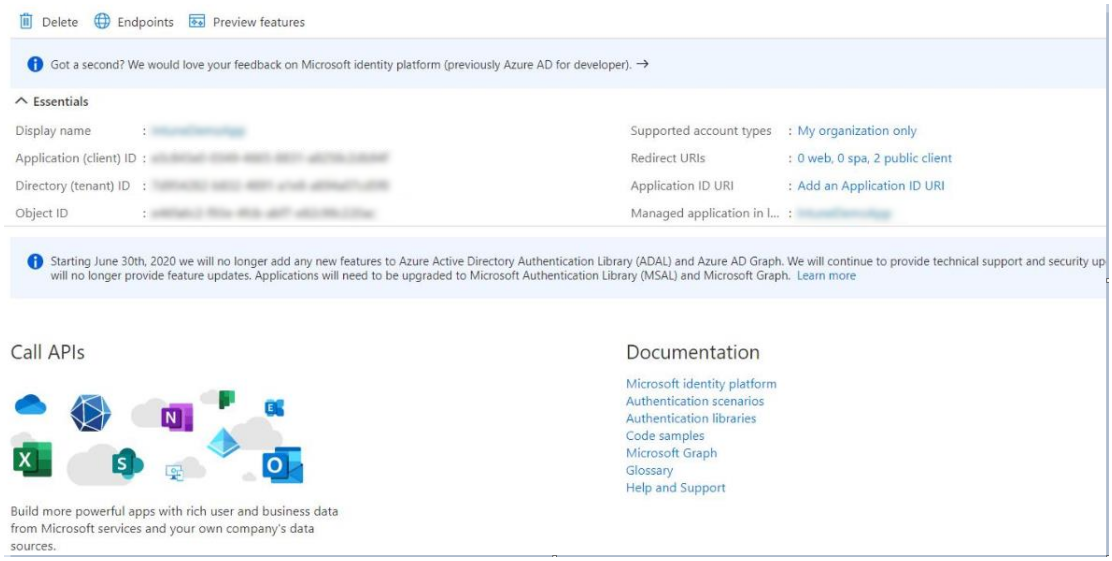


5. Click on **New registration** and enter values to complete the registration.



6. Click **Register**. The new registered application will be listed.

7. Click on the registered account to get Intune connection details like **Application (client) ID** and the **Directory (tenant) ID**, which will be used later for authentication purposes.

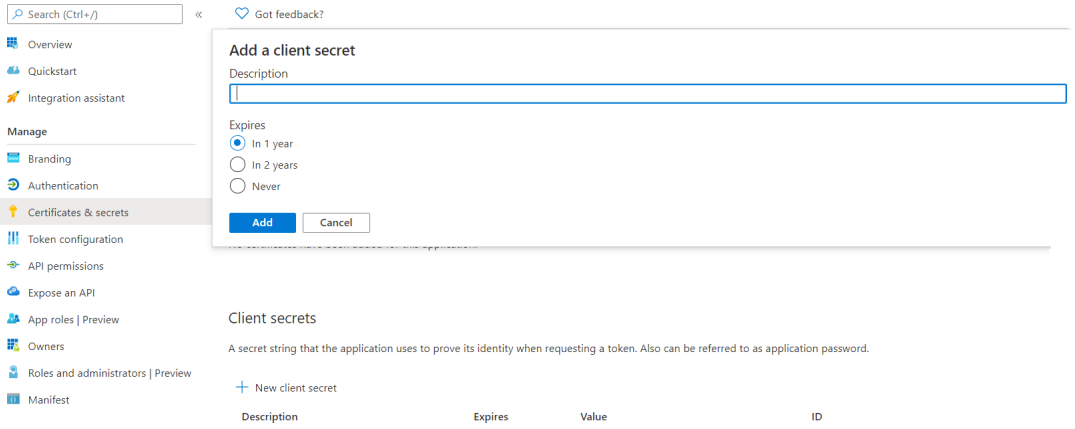


Create Client Secret

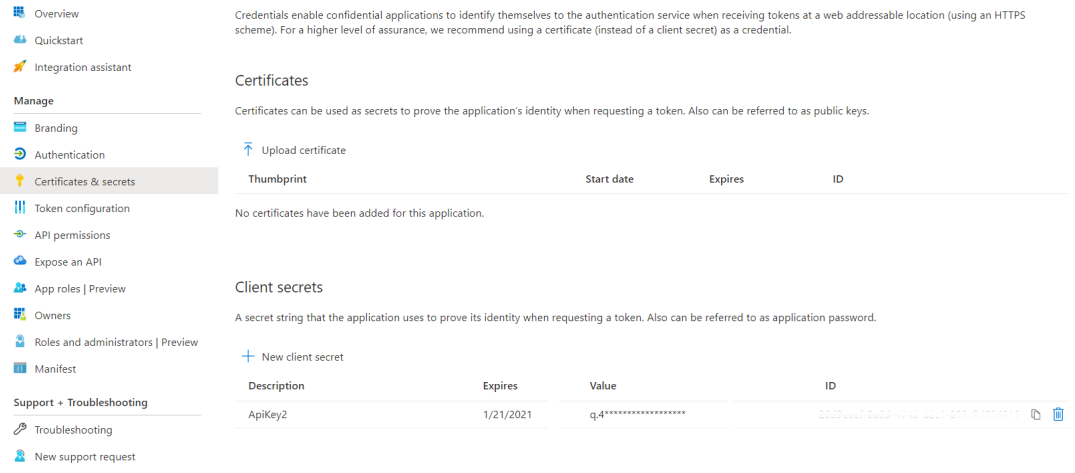
To obtain client secrets for the registered account, perform the following steps.

Task ***To obtain client secrets:***

1. On the application account details page, select **Certificates & secrets** from the left panel.
2. To get new client secret, click **New client secret**.
3. Provide a description to describe your client secret, choose the expiration date you wish to set, and then click **Add**. The Client secret will then be listed in the Client Secrets section.



4. The Client secret will then be listed in the Client Secrets section, copy the client secret Value, as it will only be visible and available to the user now.

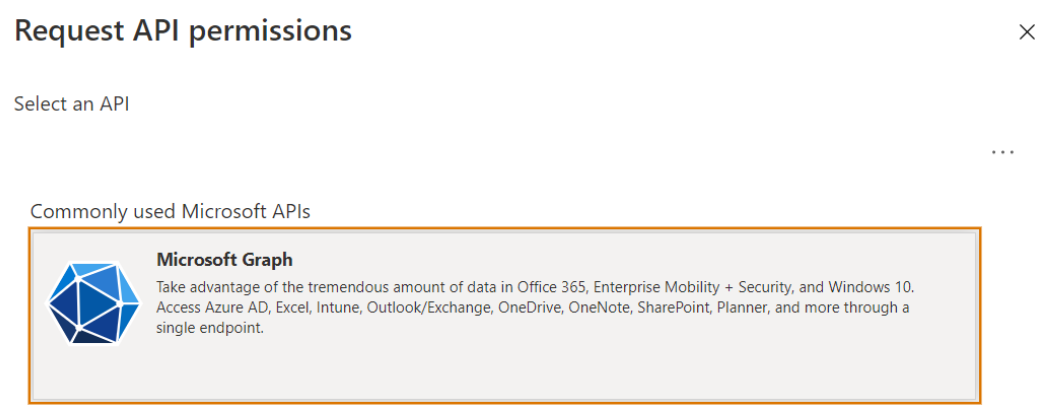


API Permissions

To obtain API permissions for the registered application, perform the following steps:

Task ***To obtain API permissions:***

1. Select the registered account.
2. Select **API permissions** from left navigation panel.
3. Click **Add a permission**. The **Request API permissions** panel appears, select **Microsoft Graph**.



4. In the Microsoft Graph, select **Application Permissions**.
   a. **Device Management Permission**—Under **DeviceManagementApps**, select **DeviceManagementApps.Read.All** and **DeviceManagementApps.ReadWrite.All**, and then click **Add permissions**.

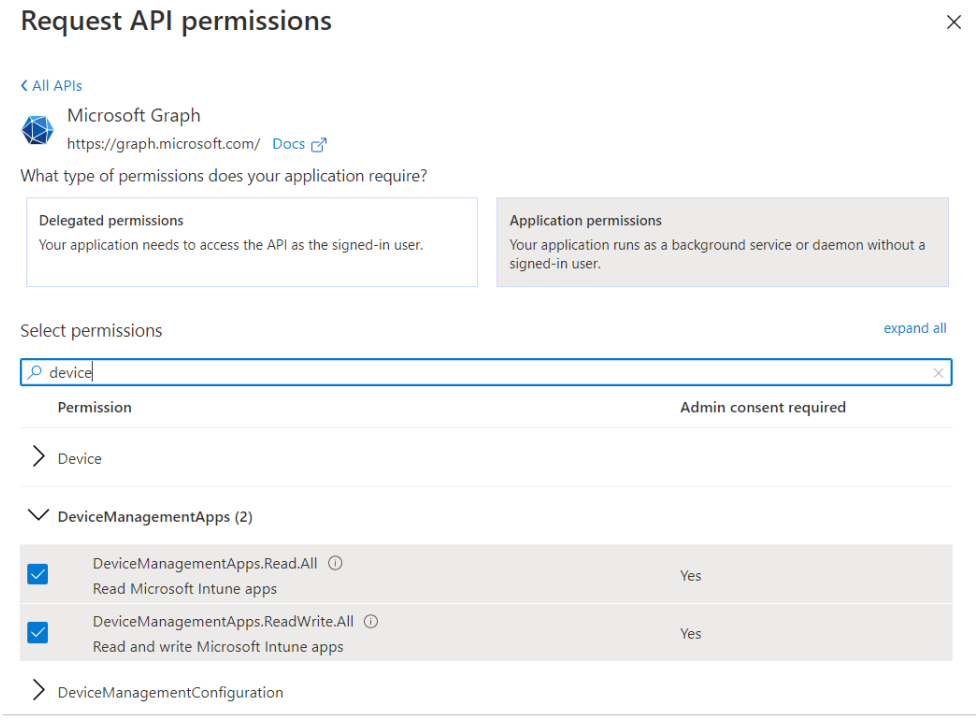


Figure 9-16: Request API permissions page

   b. **Group Permission**—Under **Group**, select **Group.Read.All**, and then click **Add permissions.**

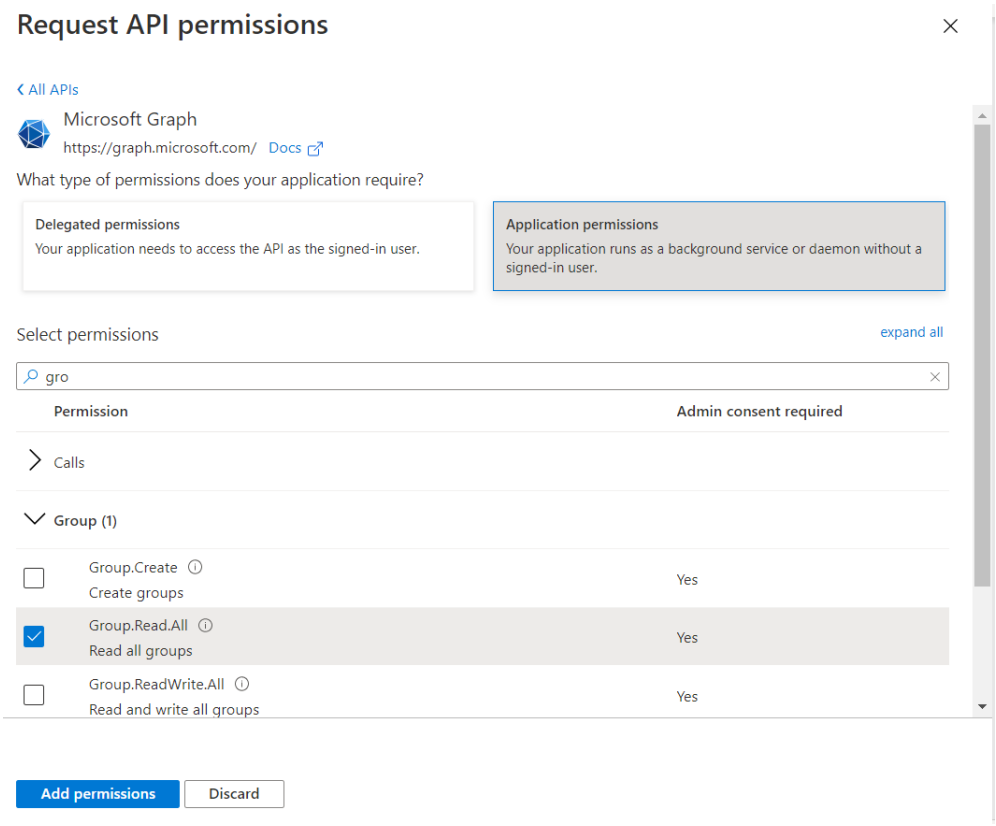


Figure 9-17: Add Group Permissions

5. Click on **Grant admin consent for Flexera Development Account** and consent to the permissions. The status will turn to **Granted**. Make sure the permissions are of type Delegated.

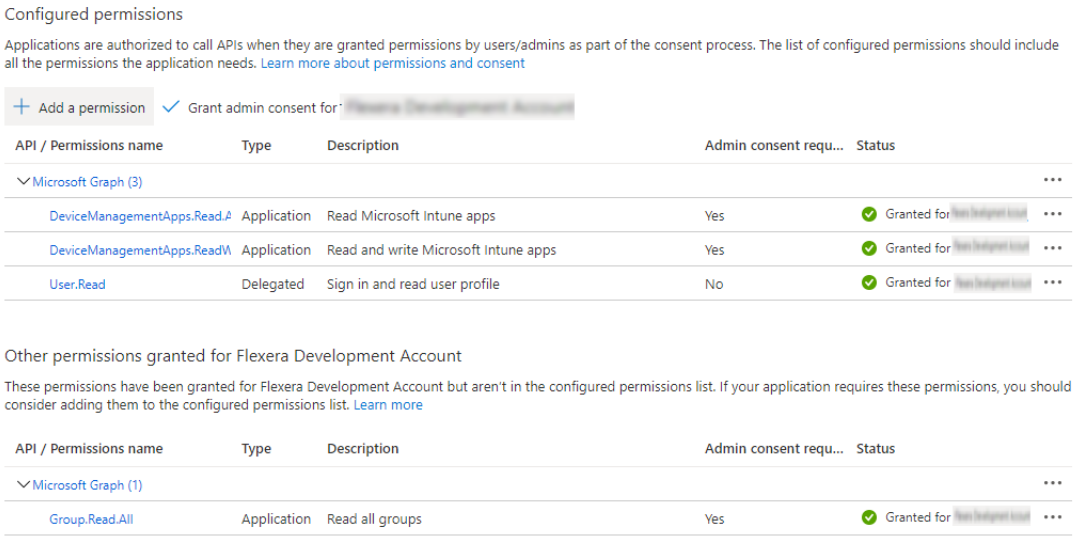


Figure 9-18: Configured permissions page

Assignment Groups

To make assignments for end point deployments in the SVM Patch Configuration for Intune publishing, perform the following steps.

Task ***To make assignments for end point deployments in the SVM Patch Configuration:***

1. In Assignment Groups (optional) field, click context menu icon. The **Intune Assignment Groups** window appears. Select the desired groups from the list and then click **Ok**.

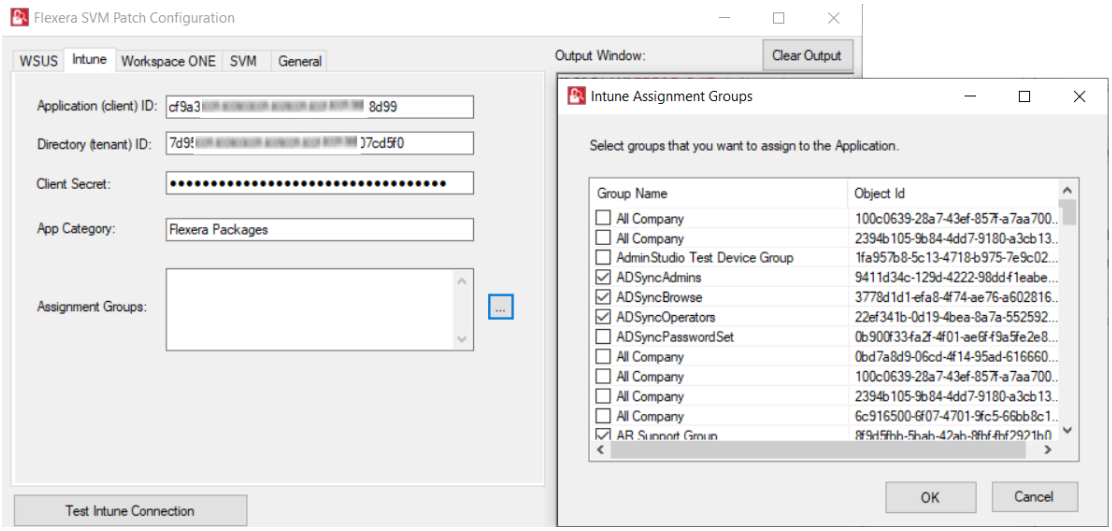


Figure 9-19: Select desired Assignment Groups

2. Restart the SVM Patch Configuration so that the selected groups will be assigned for the end point deployments.
3. If Group.Read.All permissions are not added for registered account, then the following error popup will be displayed while assigning group in Patch Configuration.

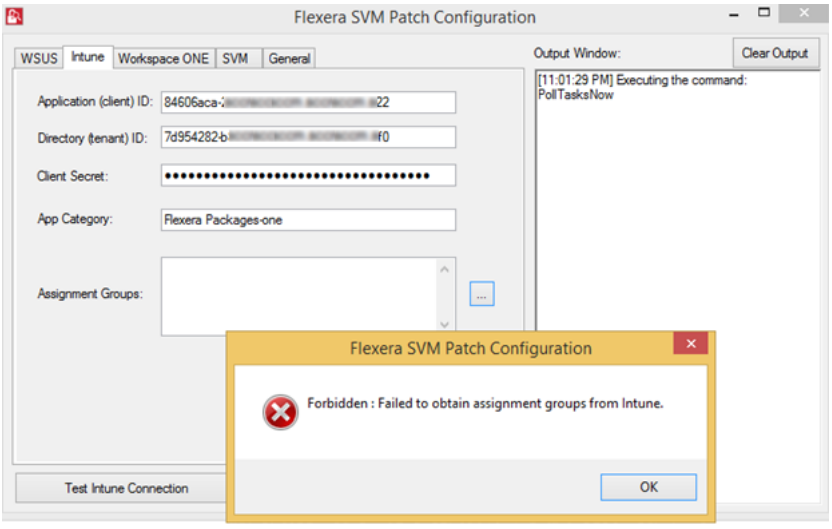


Figure 9-20: Error popup appears

Workspace ONE Publishing

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

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

To publish patches to Workspace ONE, it will be necessary to configure patch daemon with valid Workspace ONE connection details. For more details, see Set up a Distribution Connection in Flexera SVM Patch Configuration for Workspace ONE.

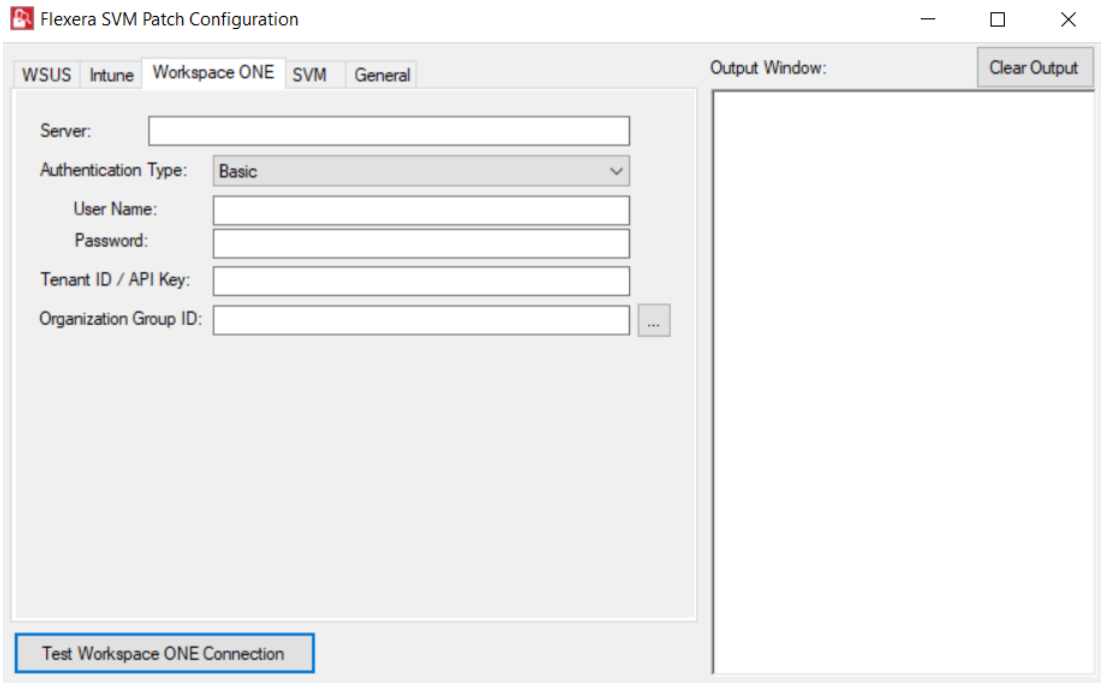


Figure 9-21: Workspace ONE Tab

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

Note • *Workspace ONE permits publishing a single application only once to an Organization Group. Therefore, if you attempt to publish an application to an Workspace ONE Organization Group that already contains that application, the publication will fail.*

Set up a Distribution Connection in Flexera SVM Patch Configuration for Workspace ONE

To set up a distribution connection for Workspace ONE, perform the following process.

- Basic or Certificate Authentication Type
- Create Tenant ID / API Key

For more details on Test Connections, see Flexera SVM Patch Configuration.

Basic or Certificate Authentication Type

In SVM Patch Configuration for Workspace ONE, you can select Authentication Type as either Basic or Certificate.

If you selected authentication type as a **Basic**, then enter your Workspace ONE **User Name** and **Password**.

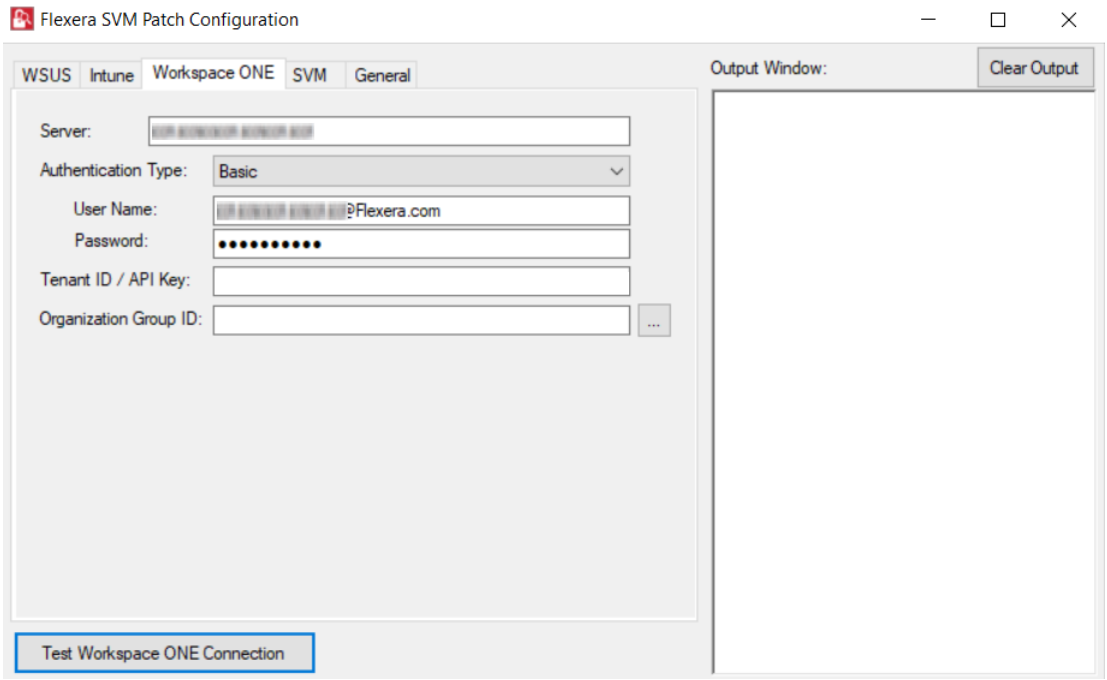


Figure 9-22: Authentication Type

If you selected authentication type as a **Certificate**, then provide certificate details as mentioned in the below steps:

Task ***To provide Certificate authentication:***

1. Log in to Workspace ONE using the valid credentials.
2. Once logged in, choose **Accounts** in the left panel.
3. Under **Administrators**, choose **List View**.

   The Admin users will then be listed in the **List View** page.

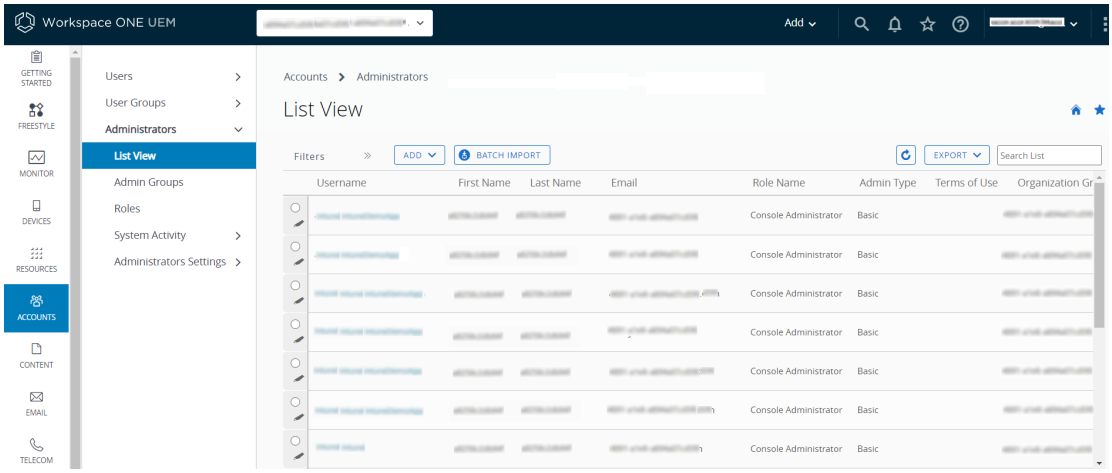


Figure 9-23: List View Page

4. Click the **Username**. The **Add/Edit Admin** panel appears. Choose **API** tab.
5. In the API tab, generate a certificate export password by entering the valid values in the **Certificate Password** test box, and then click the **Export Client Certificate** button.

   Certificate has been exported to the local folder.

Note • *This password will be used later for importing the certificate.*

Note • *By default **Certificates** authentication will be selected.*

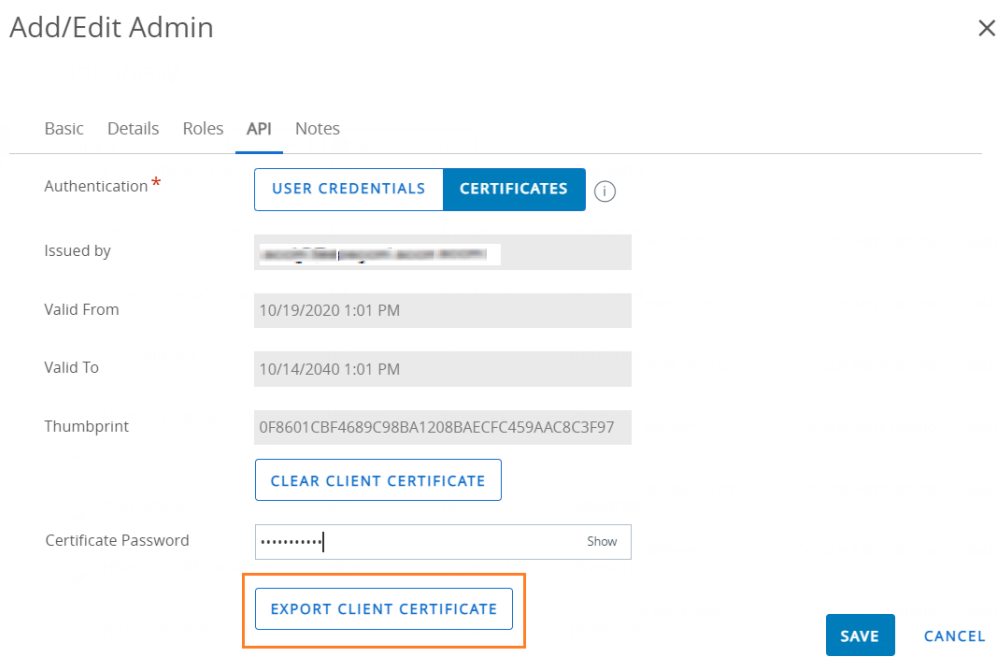


Figure 9-24: Generate Certificate Password

6. Double click the exported certificate, the **Certificate Import Wizard** dialog box appears.

   Select the store location to **Local Machine**, were you can import the certificate. Click **Next**.

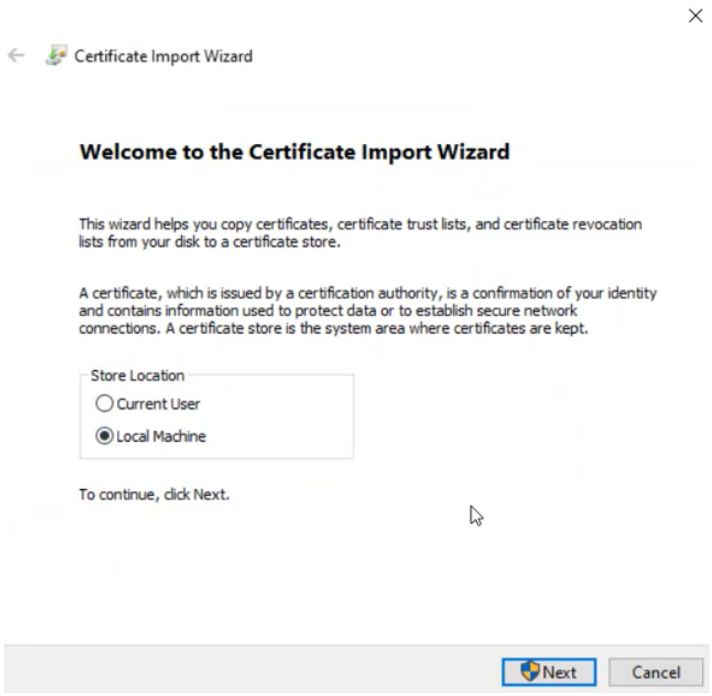


Figure 9-25: Select Local Machine

7. In the **File to Import** page, optionally, specify the file you want to import. Click **Next**.

8. In the **Private key protection** page, enter the certificate password, and then click **Next**.

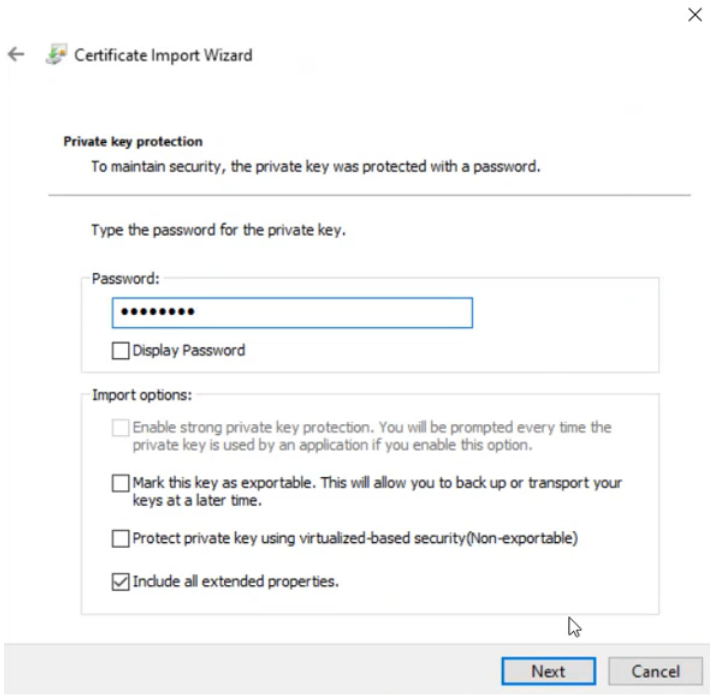


Figure 9-26: Enter Certificate Password

9. In the **Certificate Store** page, select **Place all Certificate in the following store** radio button, and then browse to the **Personal** folder were you can install the certificate. Click **Next**.
10. Click **Finish** to import the certificate.

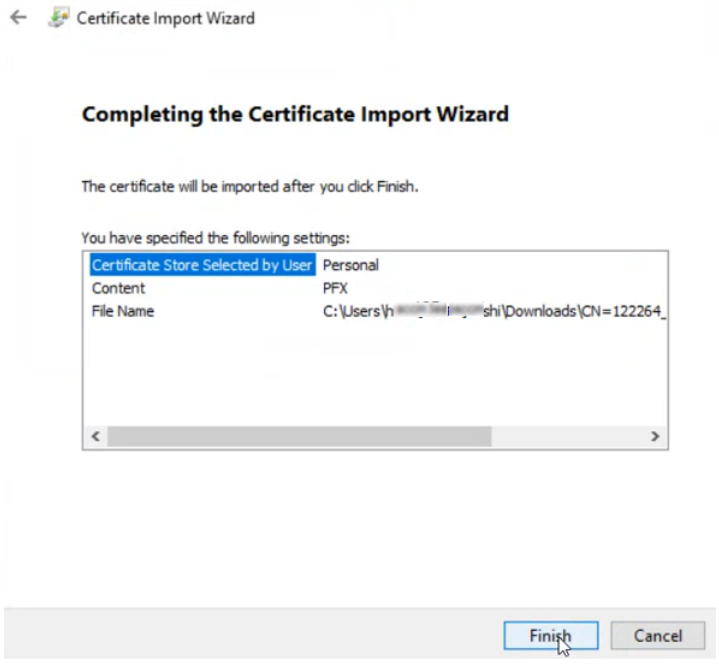


Figure 9-27: Click Finish

11. Click **Ok** and agree the confirmation dialog which appears.
12. In the Flexera SVM Patch Configuration, click **Thumbprint**, browse and select the **Certificate**.

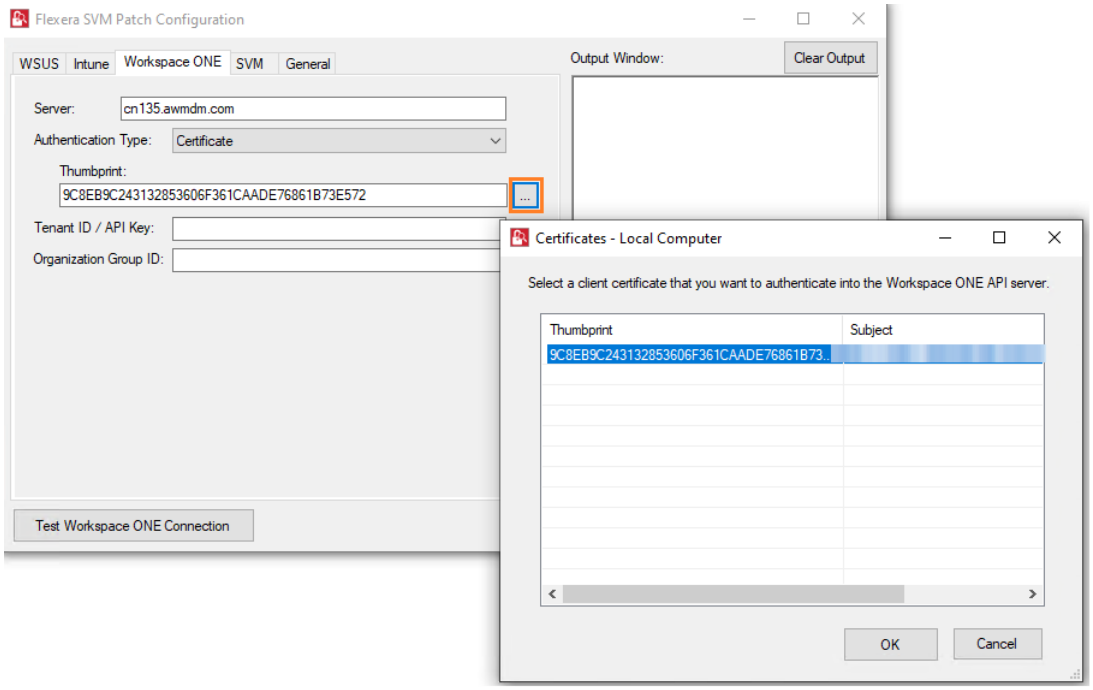


Figure 9-28: Browse and select Certificate

13. In the SVM Patch Publisher, click Thumbprint, browse and select the Certificate.

Create Tenant ID / API Key

To obtain Tenant ID / API Key for the registered account, perform the following steps.

Task ***To obtain Tenant ID / API Key:***

1. In the application page, select **GROUPS & SETTINGS** from the left panel.

   The **Groups & Settings** page appears.

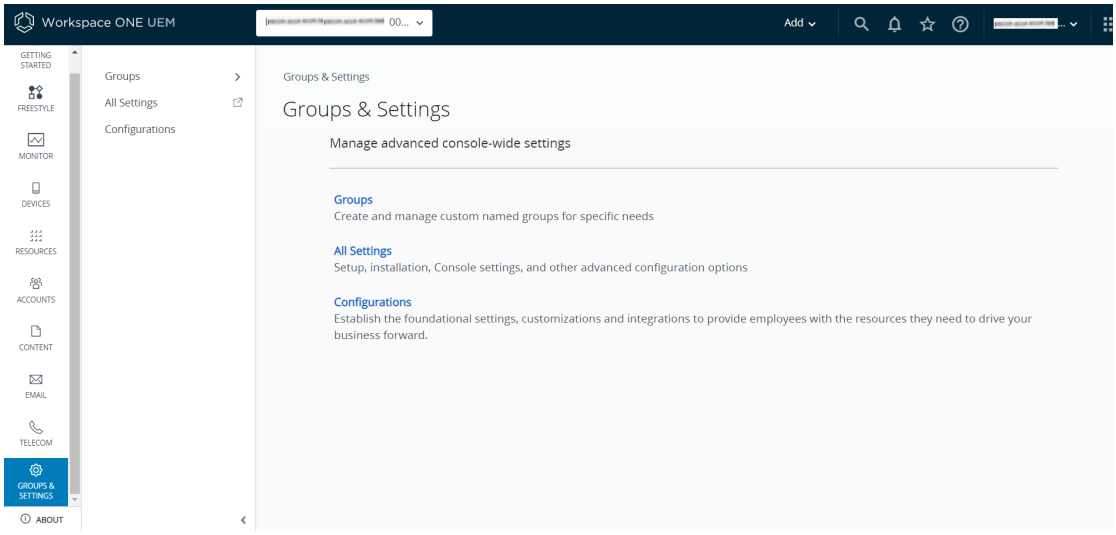


Figure 9-29: Groups & Settings page

2. On the **Group & Settings > All Settings > Systems > Advanced > API > REST API**.

Note • *Make sure that the **Enable API Access** field should be **ENABLED**.*

3. In the **REST API** page, The Tenant ID / API Key details will be listed in the **API Key** column.

4. To get new Tenant ID / API Key, click **Add**.

5. Provide a service name, description to describe your API, choose the account type you wish to set, and then click **Save**. The Tenant ID / API Key will then be listed in the **API Key** column.

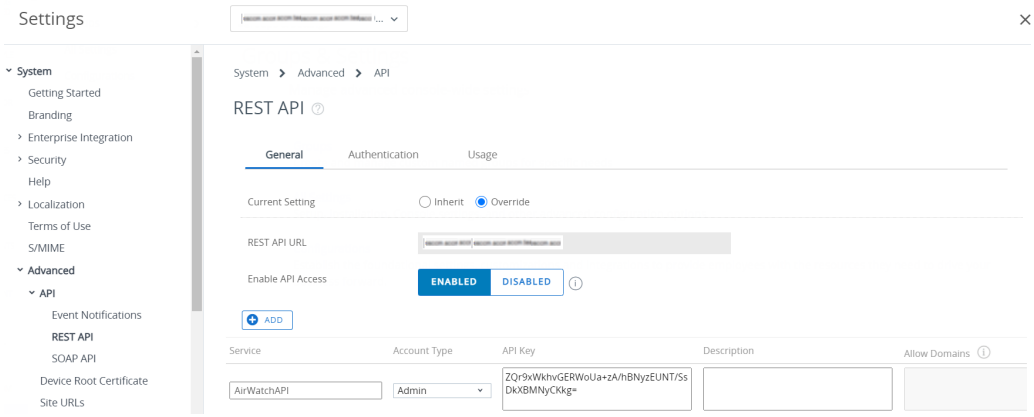


Figure 9-30: Click Add

10

Administration

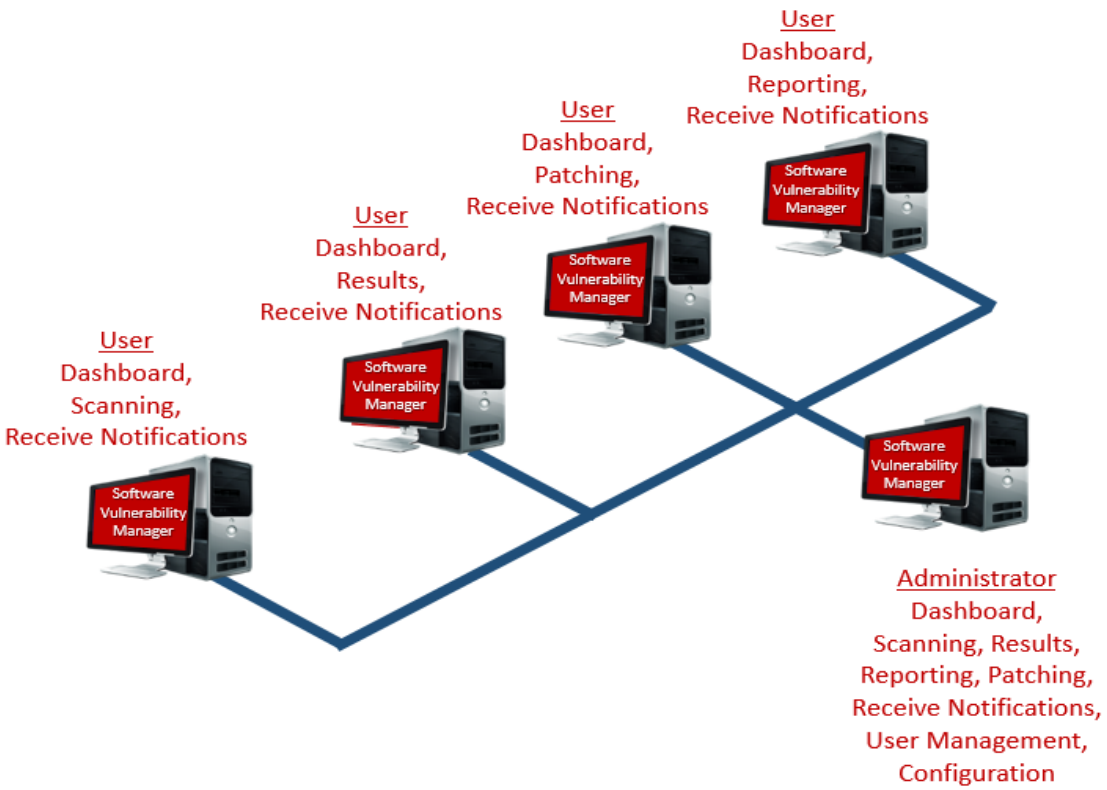
This chapter discusses the following Software Vulnerability Manager administrative features:

- 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 Allow list and Block list 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

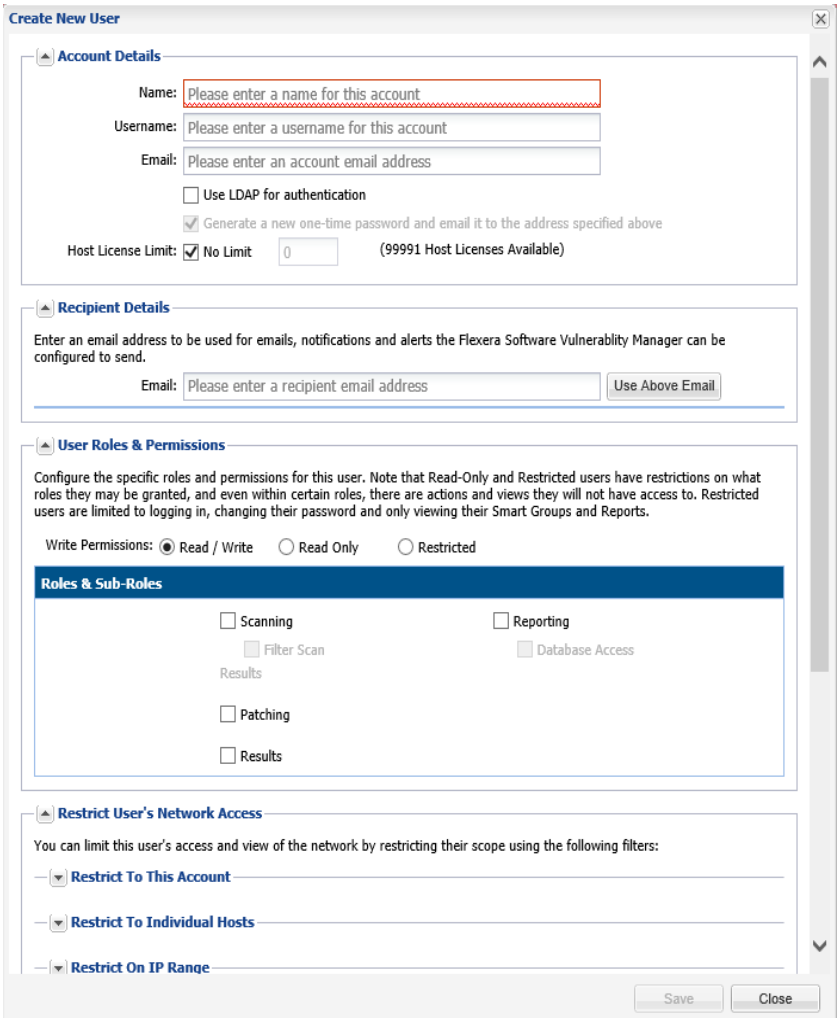
Click **Create New Administrator** and fill in the form, providing all the necessary details about the administrative user and include the limits to assign to the user.

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.



Important • *To create a user using LDAP authentication, the Software Vulnerability Manager Username must be the same as the LDAP Username.*

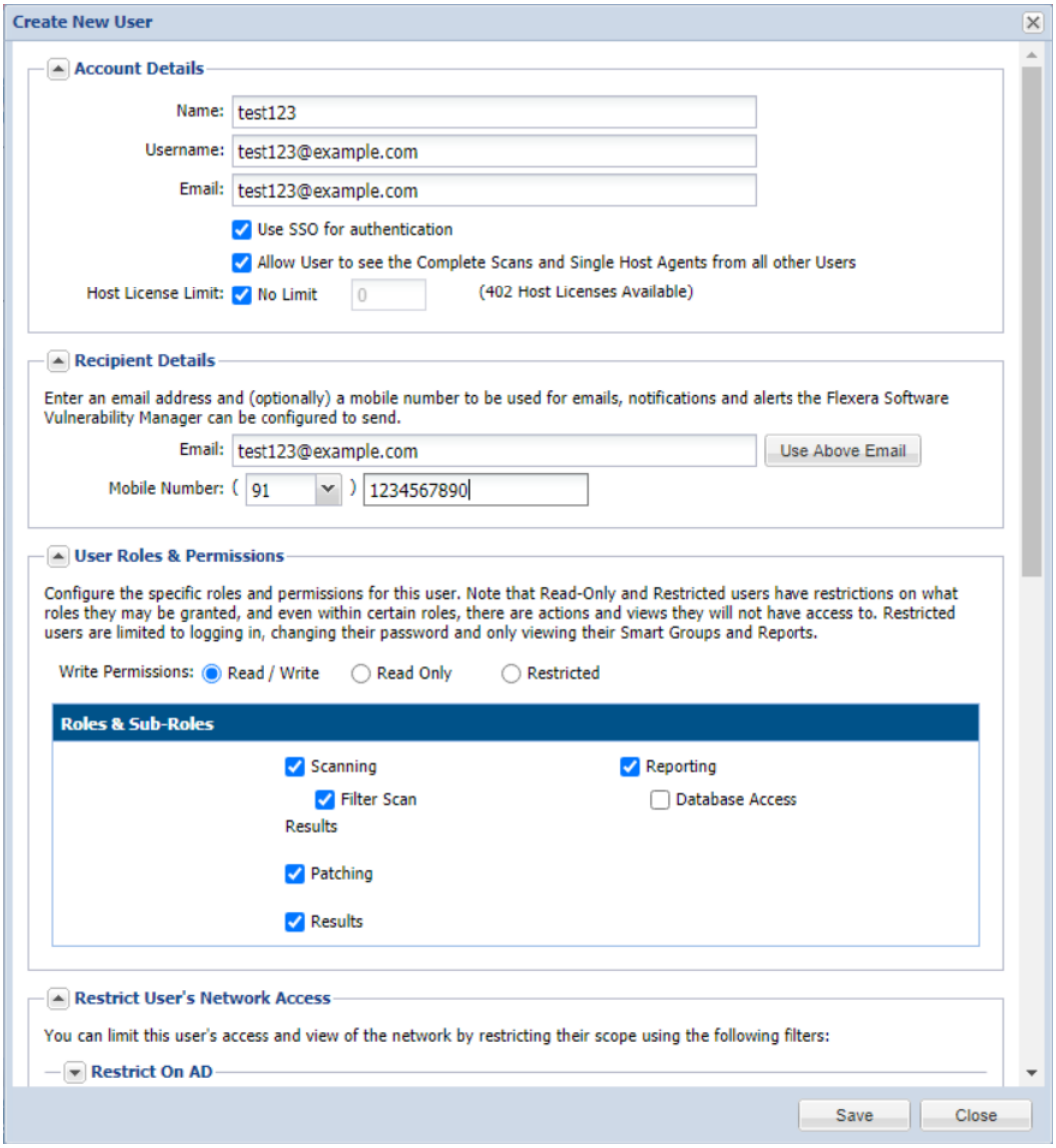
A confirmation email with activation instructions will be sent to the email address provided.

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.*

Create a New User for Single Sign-On (SSO)

To create a new user account, click Create New User and fill in the form, providing all the necessary details about the user. Select Use SSO for authentication and then select the User Roles & Permissions to assign the roles to the user.



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.

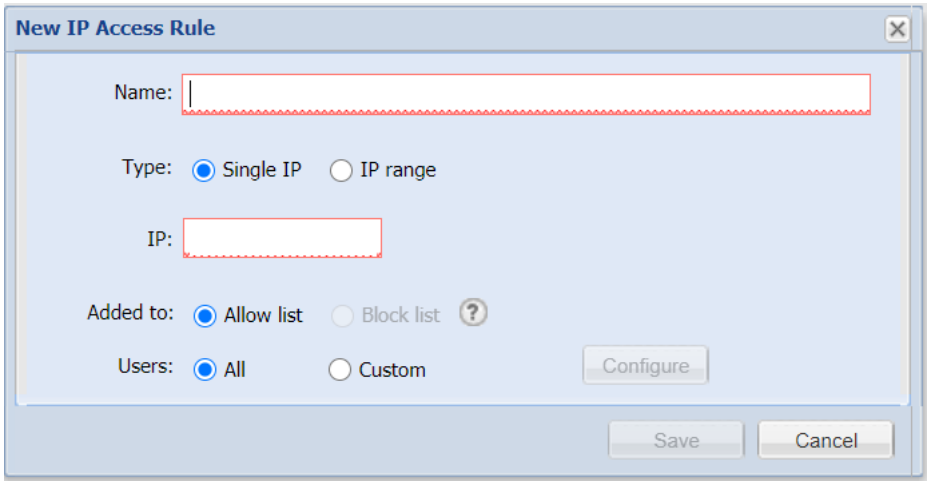
IP Access Management (Requires the Software Vulnerability Manager Plug-in)

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 Allow list 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".*

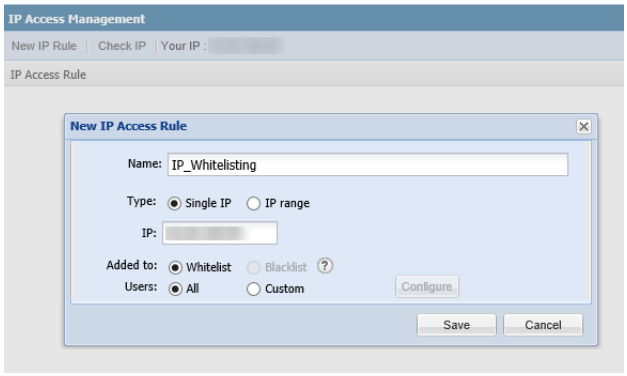
Task ***To create a new rule:***

1. Click **New IP Rule**. Enter a name for the rule, the IP address or IP range, select to add the rule to a allow list or block list, 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 allow list rule. If you allow list one IP address (the one you are using), then all other IP addresses are block-listed by default.



2. Once you have created a allow list rule with an IP range, you can then block list a Single IP or an IP range within the allow list 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.

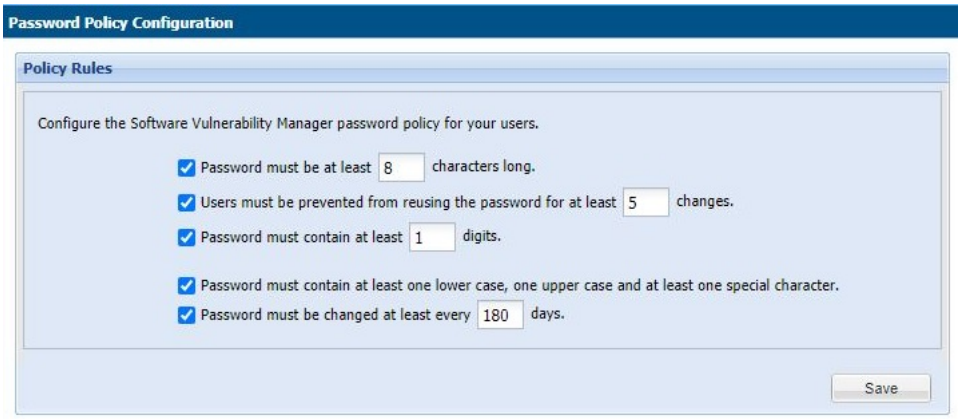


4. All IPs that have been added to a allow list are able to use Software Vulnerability Manager and IPs added to a block list are not able to connect.

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.


Password Policy Configuration
Policy Rules
Configure the Software Vulnerability Manager password policy for your users.
Password must be at least 8 characters long.
Users must be prevented from reusing the password for at least 5 changes.
Password must contain at least 1 digits.
Password must contain at least one lower case, one upper case and at least one special character.
Password must be changed at least every 180 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.

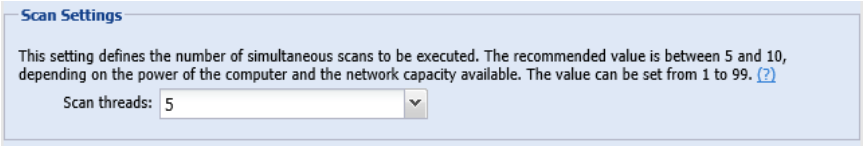
- Scan Threads
- Live Updates
- Collect Network Information
- Zombie File Settings
- Check for Missing Microsoft Security Update Settings
- Flexera Software Package System (SPS) Timestamp
- Mask paths that show user names
- Configure Agent's Status Polling
- Java Assessment Settings
- Default Recipient Settings
- Windows Update Settings
- Single Sign-On (SSO) Settings

- Configure Single Sign-On (SSO)
- Configure Single Sign-On (SSO) with Azure

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.



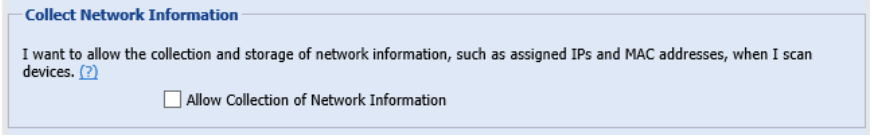
Live Updates

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.

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.*



Zombie File Settings

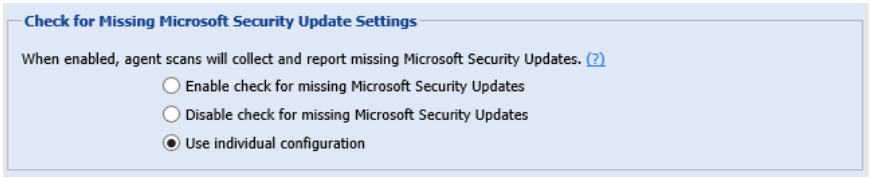
Zombie files are files that were left behind after removing or applying a product/patch. Software Vulnerability Manager will pick up these files since these are listed in Software Vulnerability Manager file signature as being related to an Insecure or End-Of-Life product. Select the **Hide Zombie Files** 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:

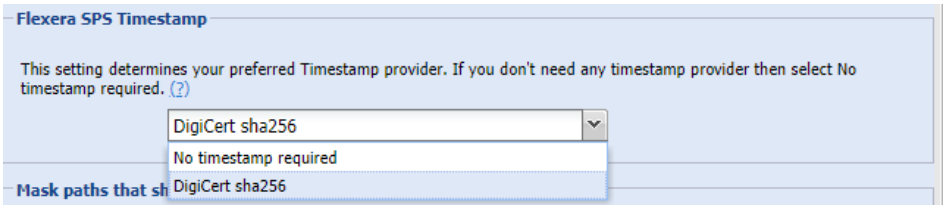
- Enable check for missing Microsoft Security Updates – All agents will check for missing Microsoft updates, using the Windows Update Settings.
- Disable check for missing Microsoft Security Updates – No agents will check for missing Microsoft updates.
- Use individual configuration – Agents will use 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.

URL Allowlist for new Timestamp server

New DigiCert timestamping service IP address:

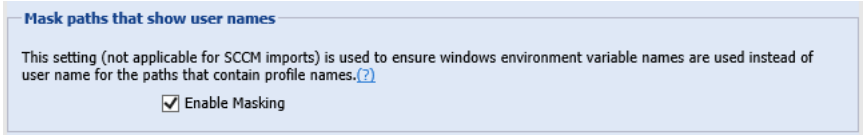
If necessary, allow this service so that you can access it on your network. It recommended to allow by domain name (timestamp.digicert.com), but if you are required to allow by IP, the new IP address will be: 216.168.244.9

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.

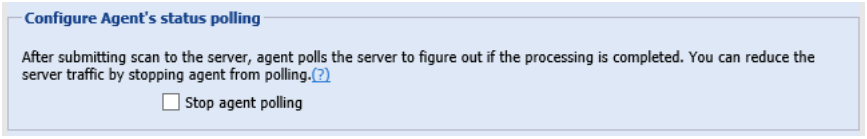
Note • *This setting is only available beginning with the Software Vulnerability Manager May 2018 release.*



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.

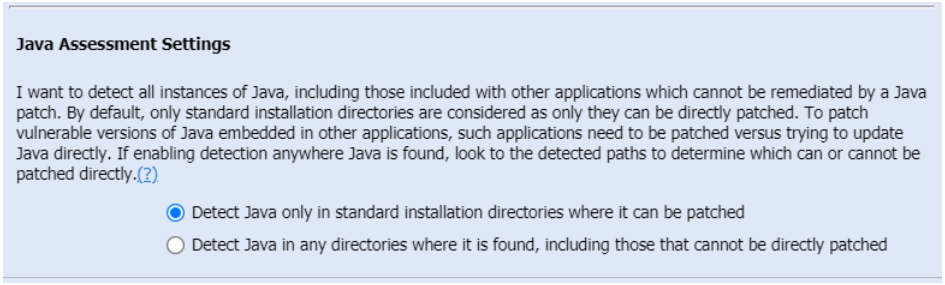


- Agent code includes a logic to determine if the scan data being uploaded to the server is the same as the prior scan. If it is, then the agent does not upload the data to the server, thereby decreasing traffic on the server. On the server side, this logic is turned off by default and is only recommended 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.

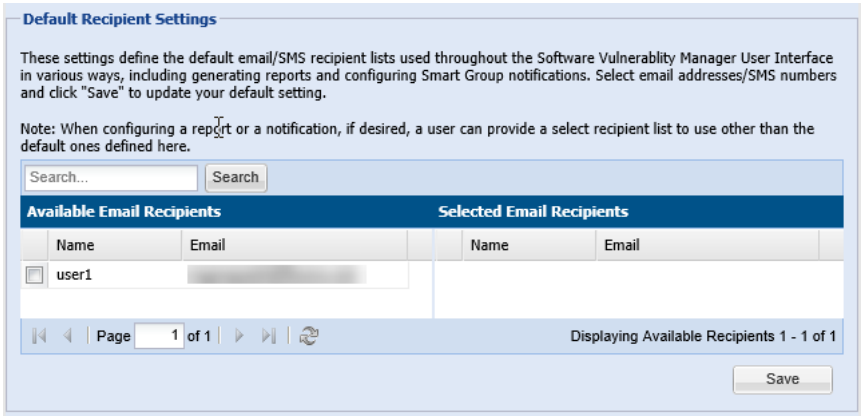
Java Assessment Settings

The Java Assessment Settings allows to you specify if you want to detect Java instances in the standard installation directories alone or in all the directories.



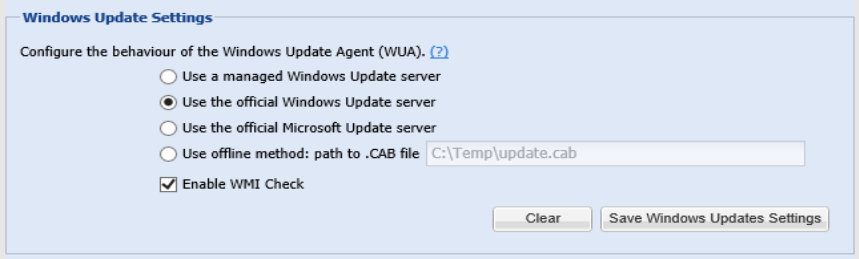
Default Recipient Settings

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.



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.



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 "WUServer 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

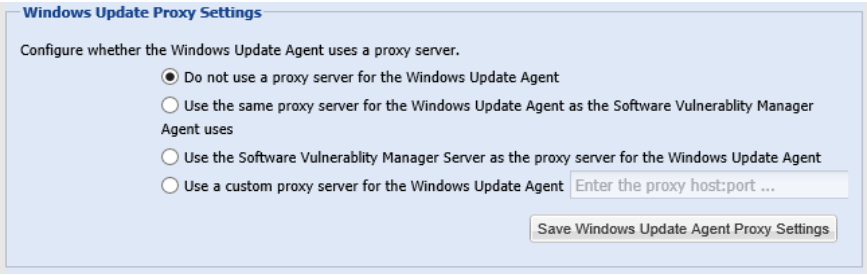
The `csia.exe` agent will request a check for updates through the public Windows Update server. This check will return a superset of the "Windows Update server" results that include Windows updates and updates for Microsoft products such as Office (non App-V, non App-X installs only) and MSVC redistributables.

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.

Single Sign-On (SSO) Settings

On the **Configuration > Settings** tab, you can specify SSO Settings.

IdP Configuration Instructions

Under SSO Settings on the **Configuration > Settings** tab, you can specify the following IdP Configuration Instructions settings.

Table 11-1 • SSO SETTINGS / IdP CONFIGURATION INSTRUCTIONS

Settings	Description
Single Sign On URL	This field lists the application's single sign-on URL. You will need to enter this URL into the settings for your chosen Identity Provider.
Account Key	Set this field in your Identity Provider (IdP) as a SAML attribute named accountKey.
Generate and Show Key	Click to generate and display the Account Key. ***Note*** • *This key is not stored on the Software Vulnerability Manager server. Make sure that you keep it in a safe place. If you lose it, you may regenerate the key, but doing so will invalidate the old key.*
Service Provider Metadata URL	Lists the Service Provider Metadata URL.

Service Provider Configuration

Under SSO Settings on the **Configuration > Settings** tab, you can specify the following Service Provider Configuration settings.

Table 11-2 • SSO SETTINGS / SERVICE PROVIDER CONFIGURATION

Settings	Description
SSO Enabled	Select this option to enable Single Sign-On.

Table 11-2 • SSO SETTINGS / SERVICE PROVIDER CONFIGURATION

Settings	Description
Disable standard login	If you are using Single Sign-On at your organization, select this option to disable standard login options for all of your users (except root). ***Important*** • *Before selecting this option, make sure that SSO is working correctly, to prevent user lockout.*
Upload IdP Metadata XML file	Select this option if you want to upload the IdP metadata XML file.
Provide IdP Metadata URL	Select this option if you want to enter the identity provider metadata URL into the **IdP Metadata URL** field.
Automatically create new users	Select this option to automatically create new users.
Default groups for new users	Specify the default group for new users.

Note • *For more information on Single Sign-On, see Configure Single Sign-On (SSO).*

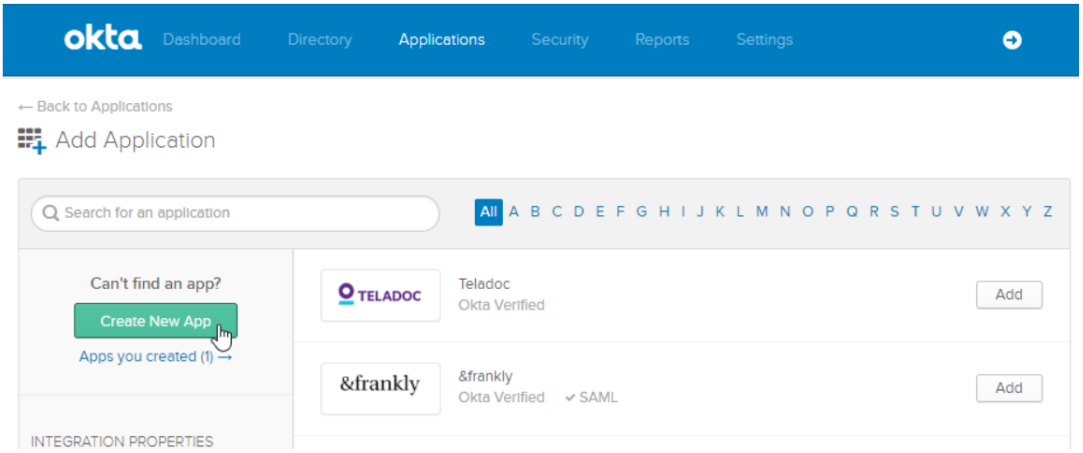
Configure Single Sign-On (SSO)

The following information is unique to the single sign-on vendor Okta (SAML 2.0). Single sign-on procedures from other vendors may vary.

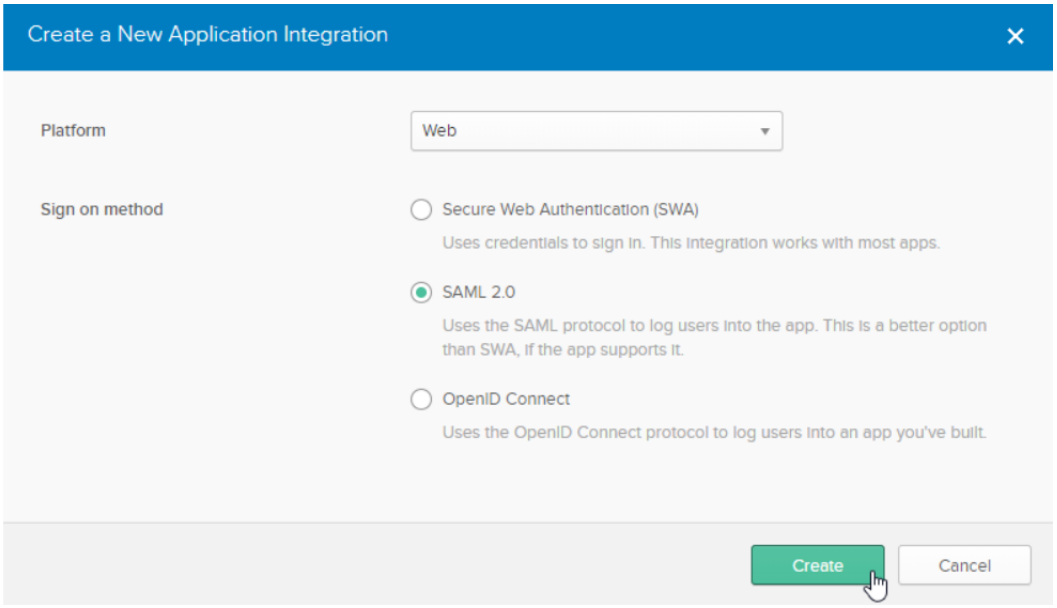
Perform the following steps to configure Single Sign-On (SSO).

Task ***To set up Okta (SAML 2.0) to use as a single sign-on (SSO) with Software Vulnerability Manager:***

1. Sign in to Okta.
2. Create an admin account.
3. Click **Create New App** to create a new Okta SSO app.

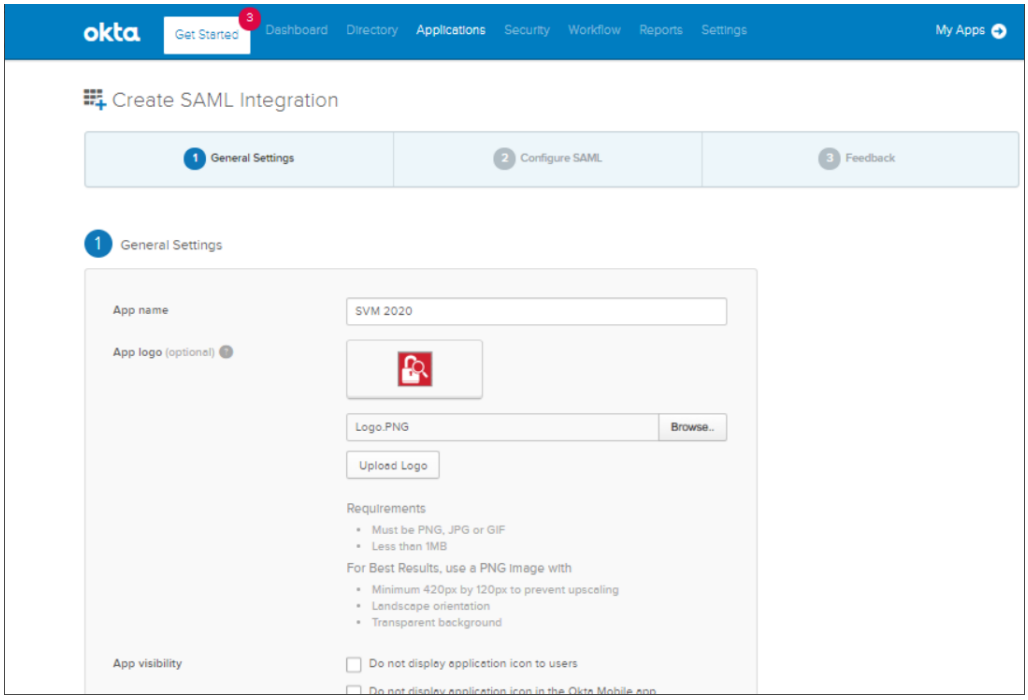


4. Choose **Web** for the Platform and **SAML 2.0** for the Sign on method. Then click **Create**.



5. Enter an **App name** (Example: SVM) and **App logo**. Then click **Next**.

Note • *Username needs to be in email format.*

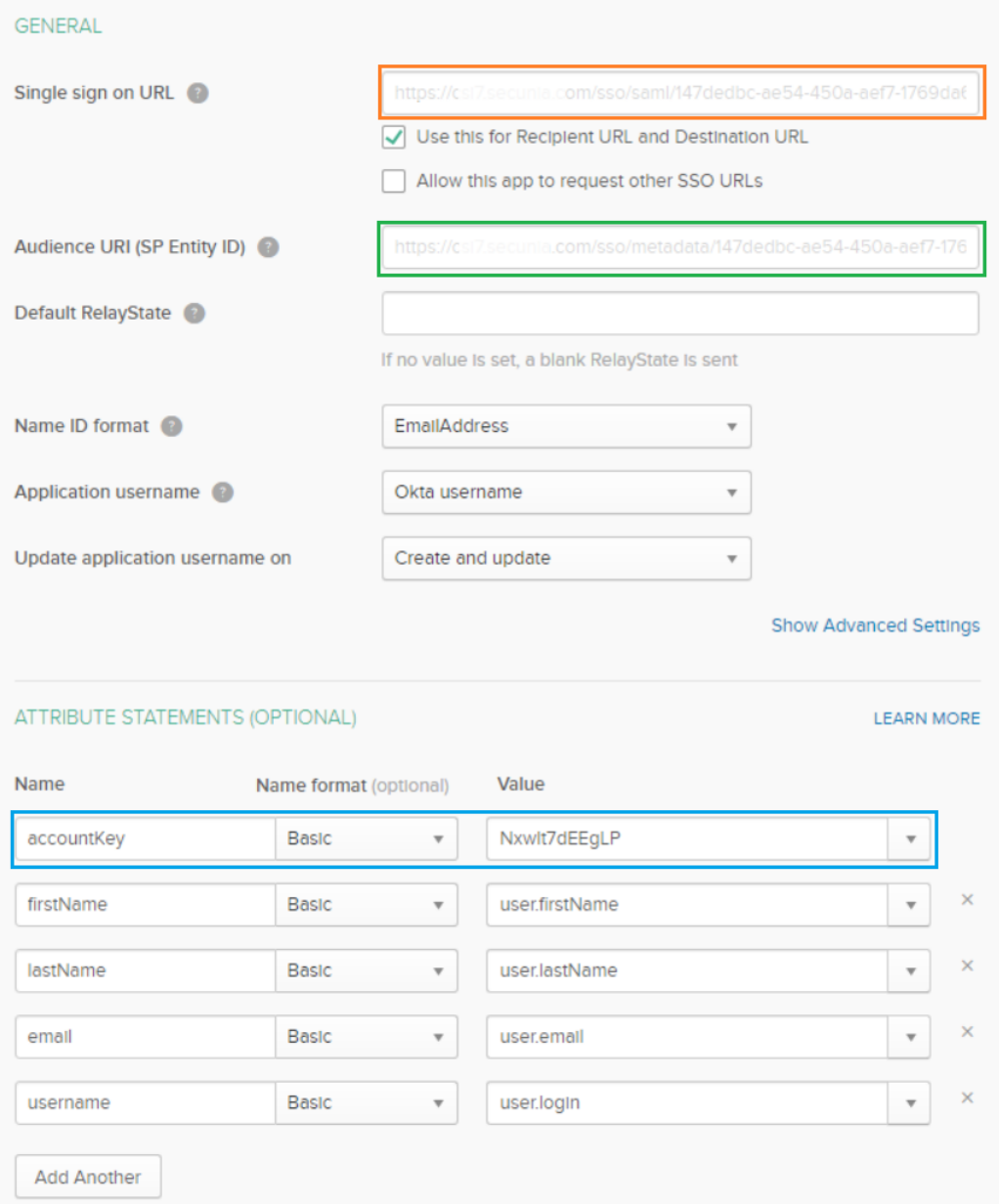


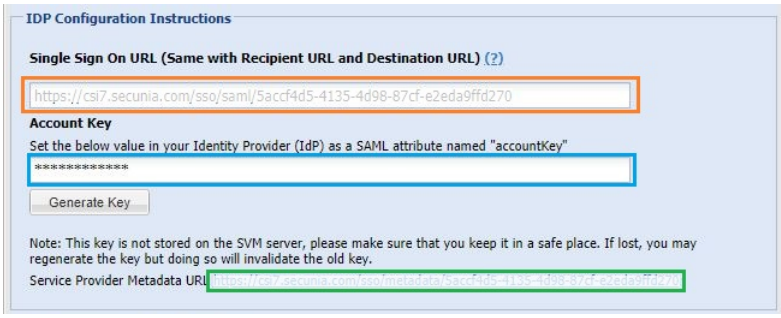
6. Copy the following from the Software Vulnerability Manager **Configuration > Settings** fields and paste in the **Okta SAML Settings** > fields:

   - Single Sign On URL (Same with Recipient URL and Destination URL) to Single sign on URL and Audience URL (SP Entity ID)
   - Select EmailAddress for Name ID format
   - Account Key to accountKey Value

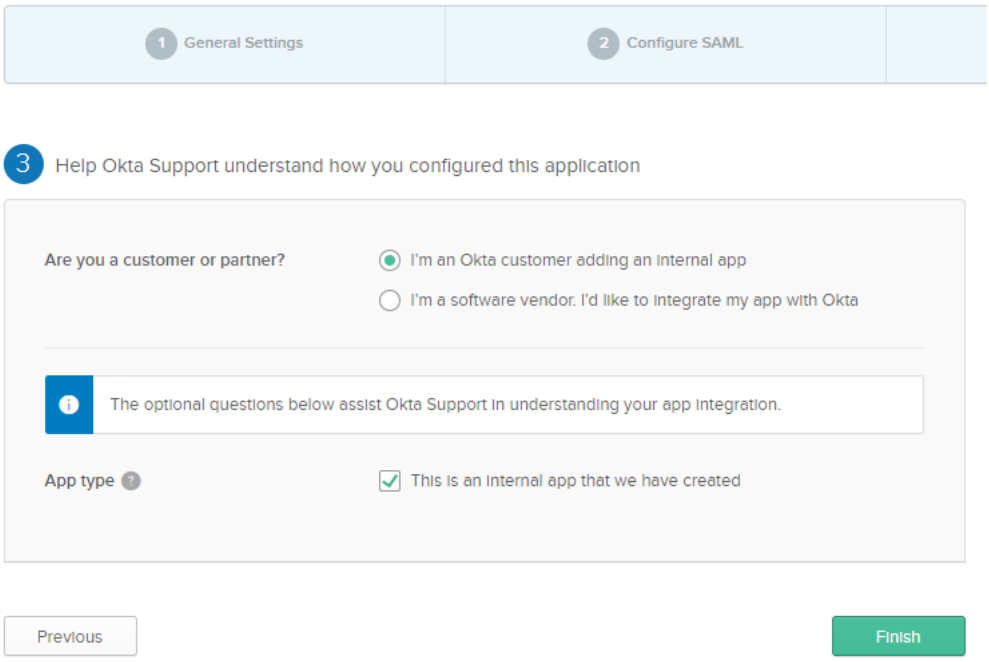
   Complete the remaining Okta SAML Settings > Attribute Statements (Optional) name and value fields using the field's drop-down list:

   - firstName
   - lastName
   - email
   - username

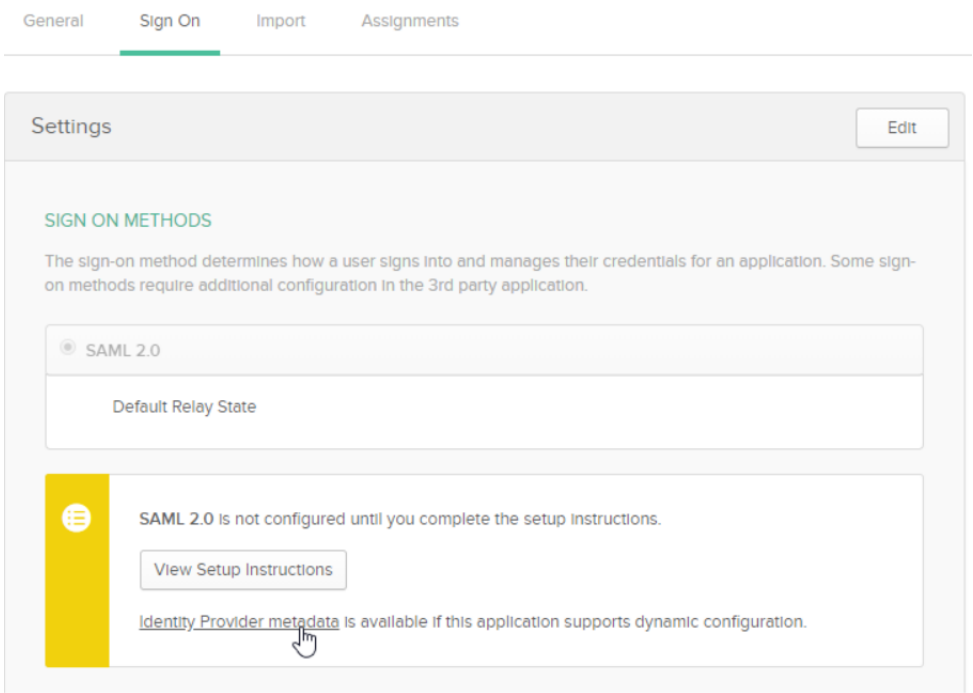




7. Click (if not already selected) **I'm an Okta customer adding an internal app** for the Create SAML Integration - Step 3 Feedback screen.



8. At the Okta Sign On Settings screen, click the **Identity Provider metadata** link.

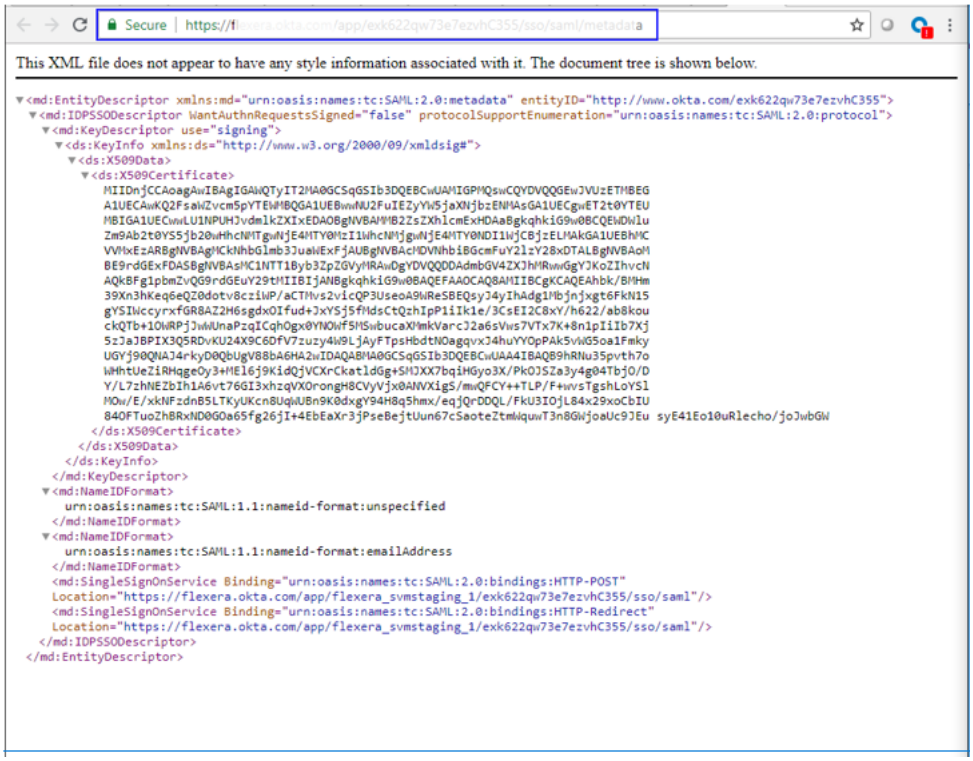


9. Copy the Identity Provider metadata URL from Okta, login into the partition admin, browse **Configuration >Settings > Service Provider Configuration**, and then check **SSO Enabled**. Select Identity Provider metadata UR and paste the copied IdP metadata URL into the text box. Select **Automatically create new user** check box and selected the template user from the combo box.

Note • *Single Sign-On settings can be updated only by the partition admin.*

Note • *For Binaries like Daemon, sc2012 plugin, Client toolkit will be logged in only by the standard login credentials. If disable standard login is selected, then the binaries will be logged in only by the partition administrator.*

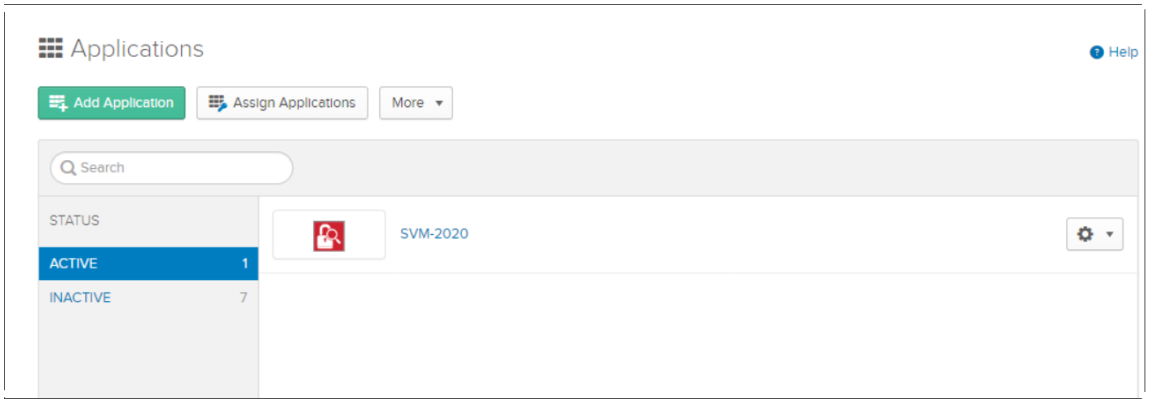
Note • *For a secure connection, the Assertions Signed (or similarly named) setting should be enabled on your IDP.*



10. If you want to disable standard login options for all of your users (except root), select the **Disable standard login** option.

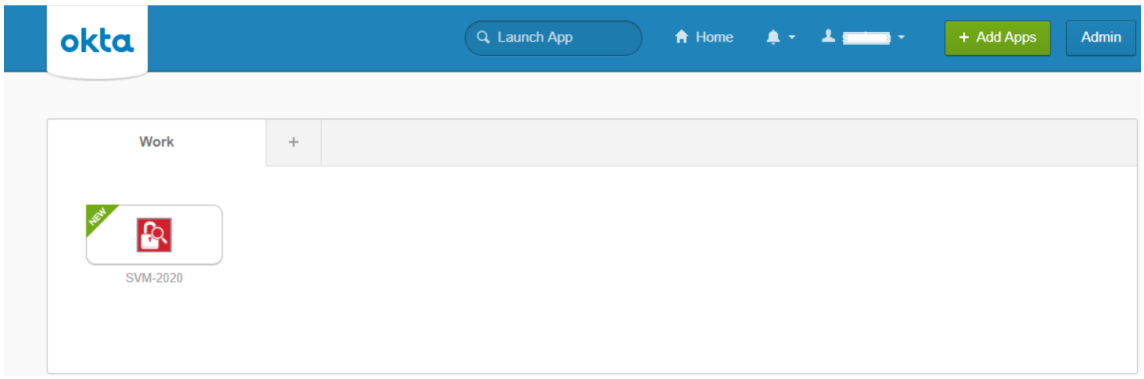
Important • *Before selecting this option, make sure that SSO is working correctly, to prevent user lockout.*

11. Click **Save Service Configuration** on the **Configuration > Settings** page.
12. Add Software Vulnerability Manager users to the Okta SSO account.



13. Assign Software Vulnerability Manager users to the Okta SSO app.

14. Users can login to Okta by entering the valid credentials and then click on SVM app to access the application.



15. Users are then logged into the Software Vulnerability Manager Login page.

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

Configure Single Sign-On (SSO) with Azure

To configure SSO in Azure, perform the following steps:

- Create an Enterprise Application
- Assign Users to the Enterprise Application
- Set up Single Sign-On (SSO) in Azure

Create an Enterprise Application

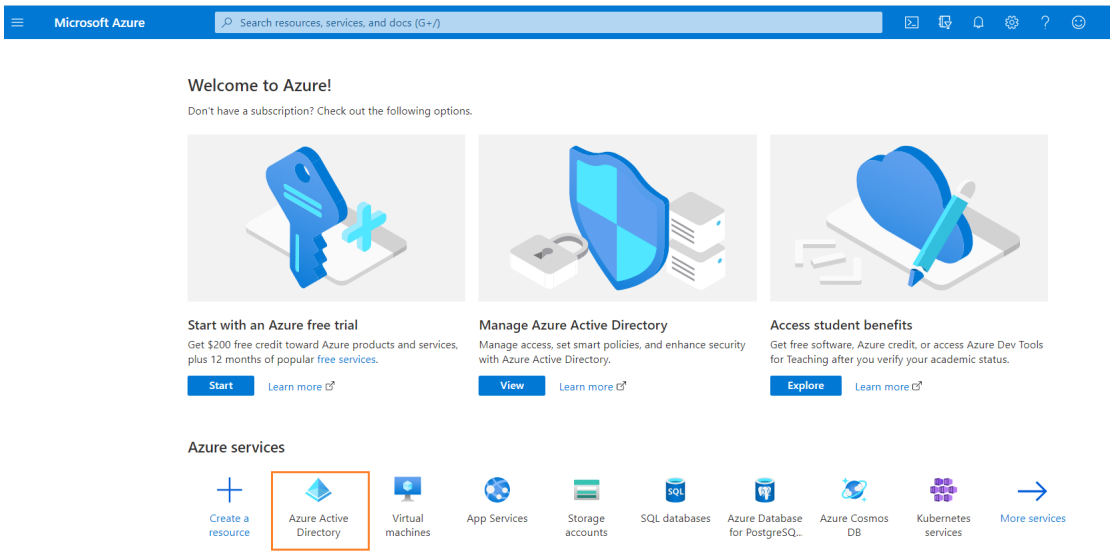
Perform the following steps to add Software Vulnerability Manager as an Enterprise Application Azure Active Directory.

Task ***To create an Enterprise Application:***

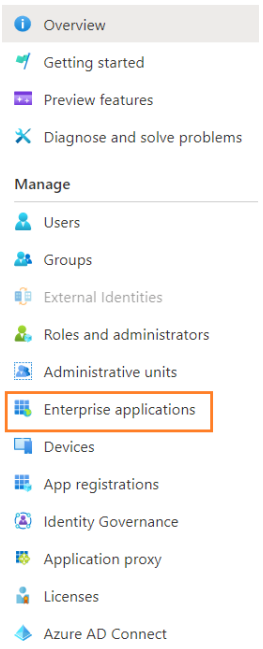
1. Log in to Microsoft Azure using the obtained credentials.

   https://azure.microsoft.com/en-in/account/

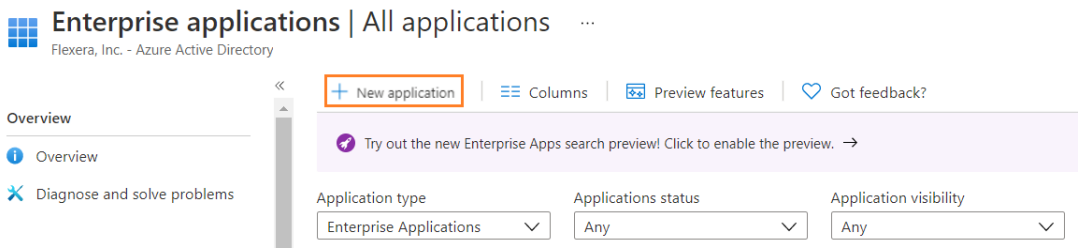
2. From the list of available Azure services, choose **Azure Active Directory**.



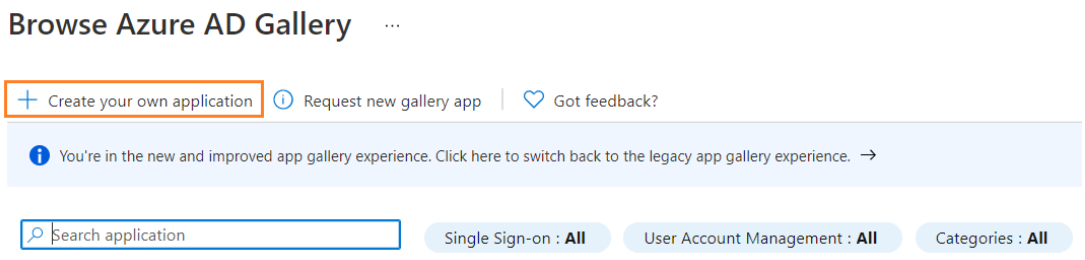
3. Click on **Enterprise applications** in the left pane.



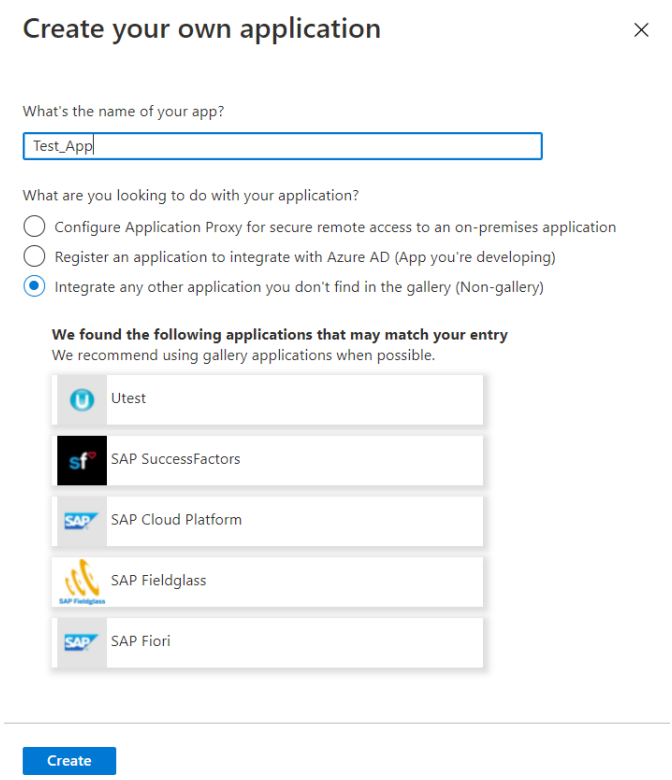
4. Click **+ New application**.



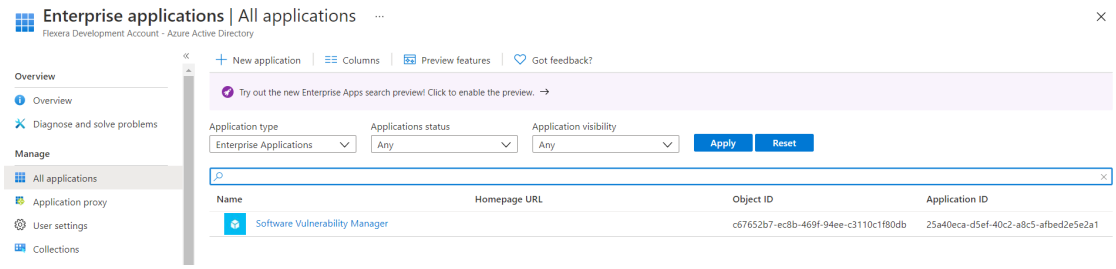
5. Click **+ Create your own application**.



6. Enter a name for the application.



7. Click **Create**. The new enterprise application will be created.

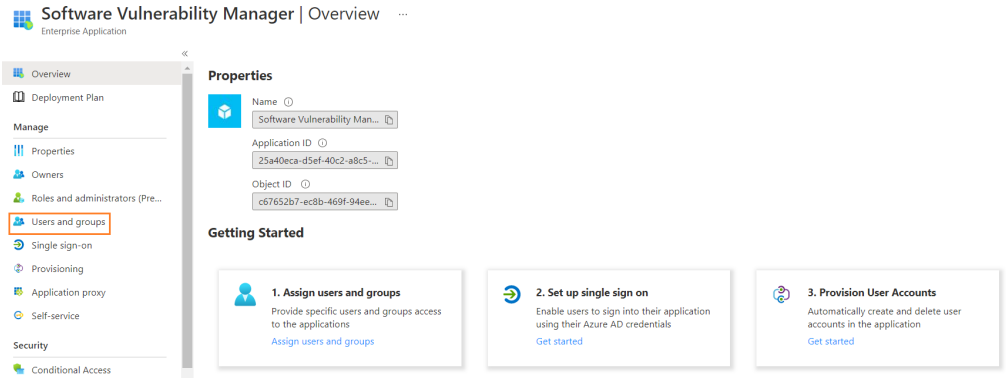


Assign Users to the Enterprise Application

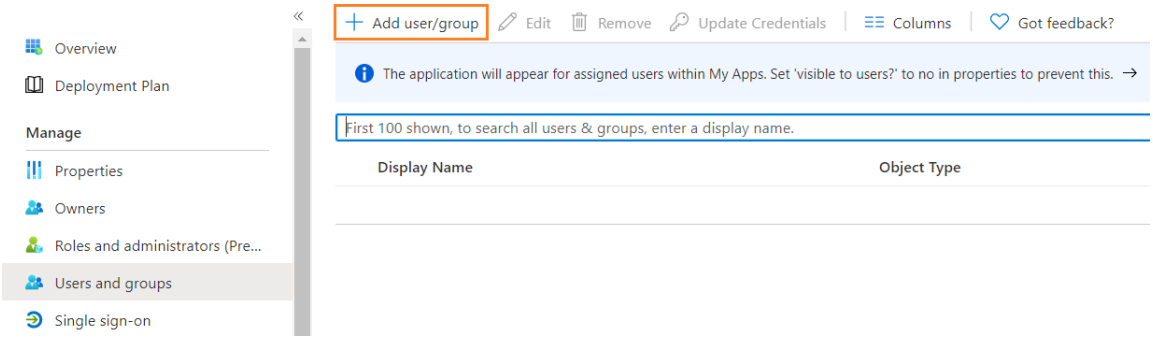
To assign users or groups to the enterprise application, perform the following steps.

Task ***To assign User:***

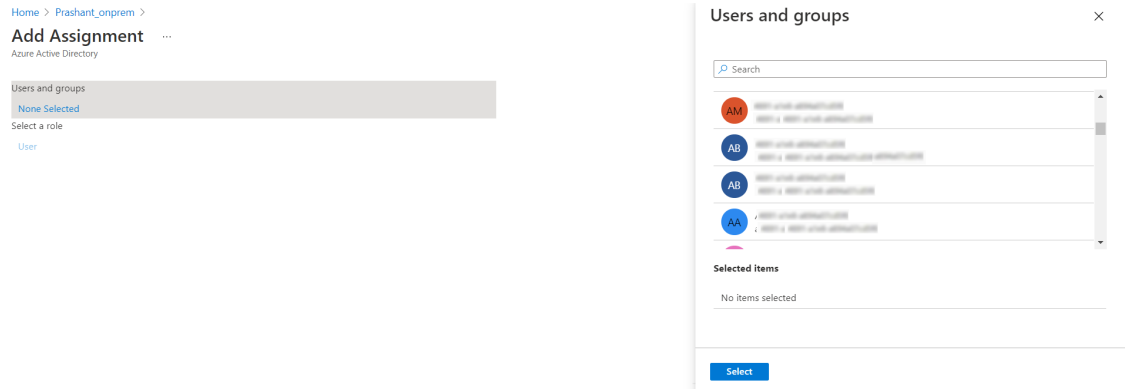
1. On the application account details page, select **Users and groups** from the left panel.



2. Click **+ Add user/group**.



3. Under **Add Assignment > Users and groups** click **None Selected** link. Search and select desired users and groups, and then click **Select**.



4. After selecting, click **Assign**.

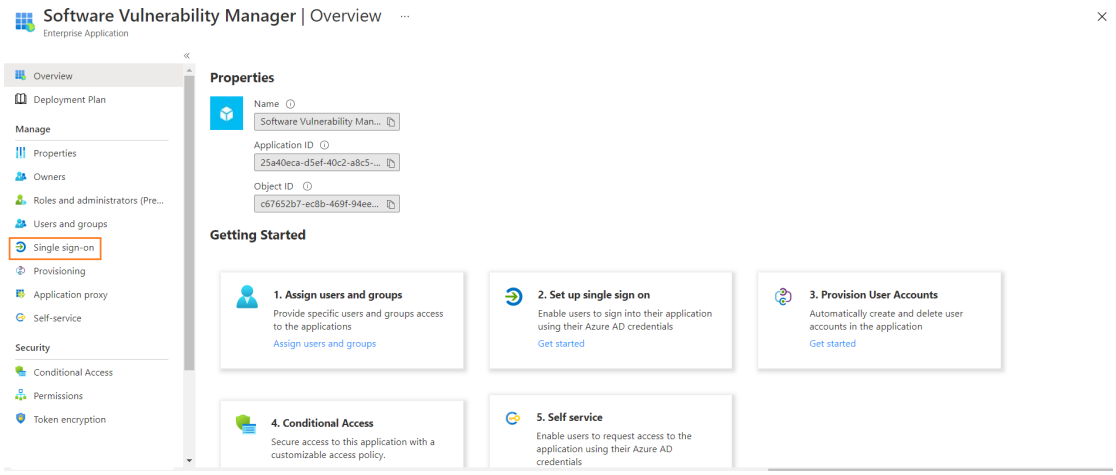
   The Users and groups then assigned to the Enterprise Application.

Set up Single Sign-On (SSO) in Azure

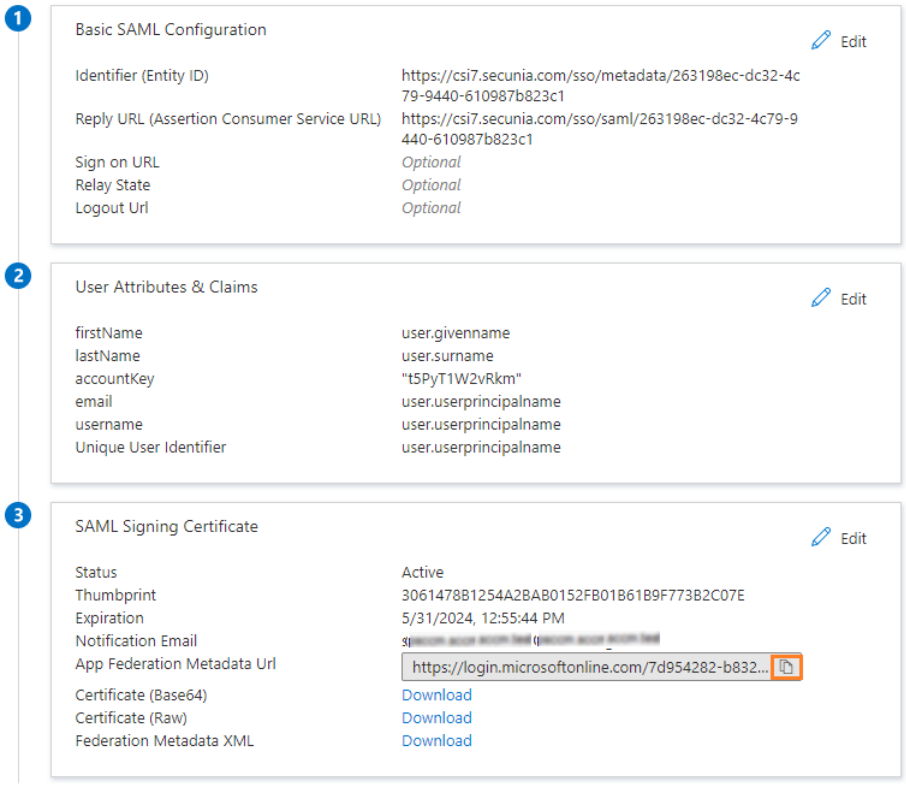
For setting up single sign-on in Azure, perform the following steps.

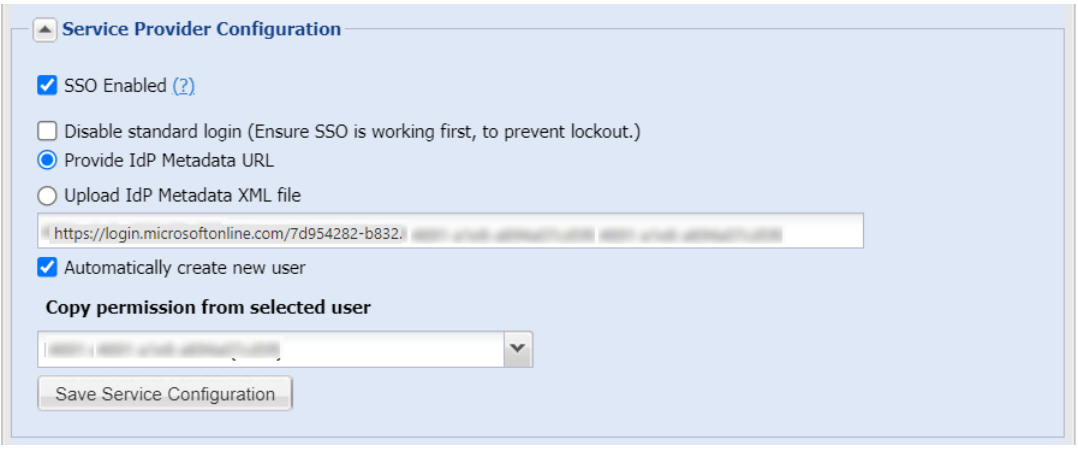
Task ***To set up single sign-on:***

1. On the application account details page, select **Single sign-on** from the left panel. You can also select from the Overview page by clicking Get started link.



2. Click SAML.
3. The **Set up Single Sign-On with SAML** page appears. Under **SAML Signing Certificate** field copy Metadata Url, login to Software Vulnerability Manager, browse **Configuration > Settings > Service Provider Configuration**, and then check **SSO Enabled**. Paste the copied URL into the text box.



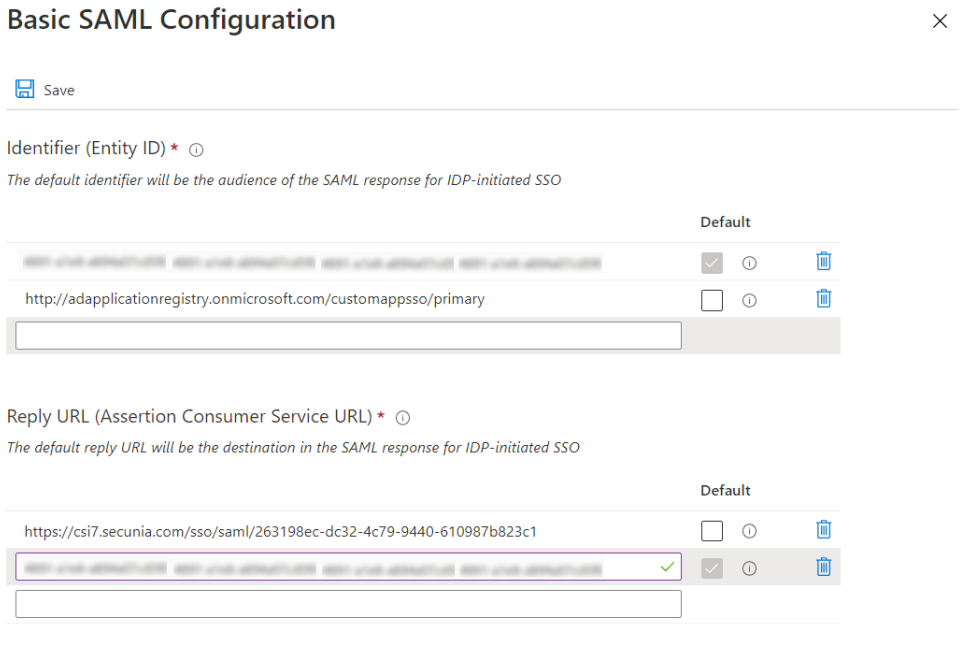


4. Generate an account key from the Software Vulnerability Manager **Configuration > Settings > IdP Configuration Instructions** and then click **Save Service Configuration** button. Click **Ok** and agree the confirmation dialog which appears.

5. Copy the following from the Software Vulnerability Manager **Configuration > Settings** fields and paste in the Azure **Single sign on > Set up Single Sign-On with SAML > Basic SAML Configuration**:

   - Single Sign On URL (Same with Recipient URL and Destination URL) to Reply URL (Assertion Consumer Service URL).
   - Single sign on URL and Audience URL (SP Entity ID) to Identifier (Entity ID).

   After selecting the details click **Save**.

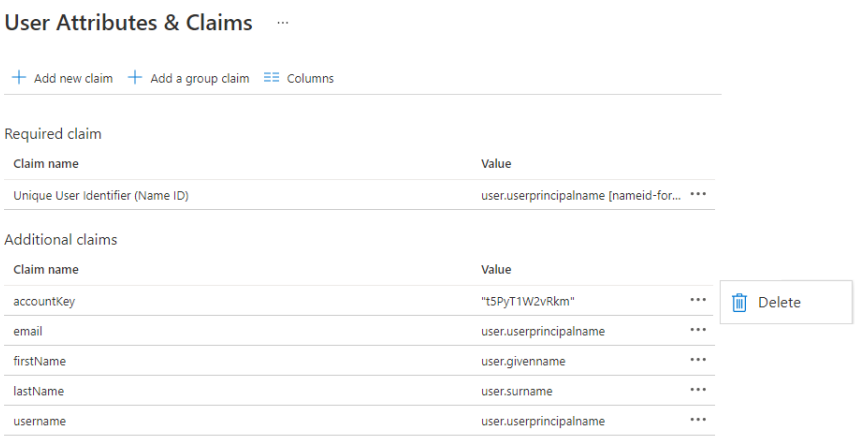


Note • *Metadata URL can not be used for the multiple applications.*

6. Edit the User Attributes & Claims

- Click Edit.

- The User Attributes & Claims page appears.
- Delete all old attributes and claims by clicking the context menu icon.



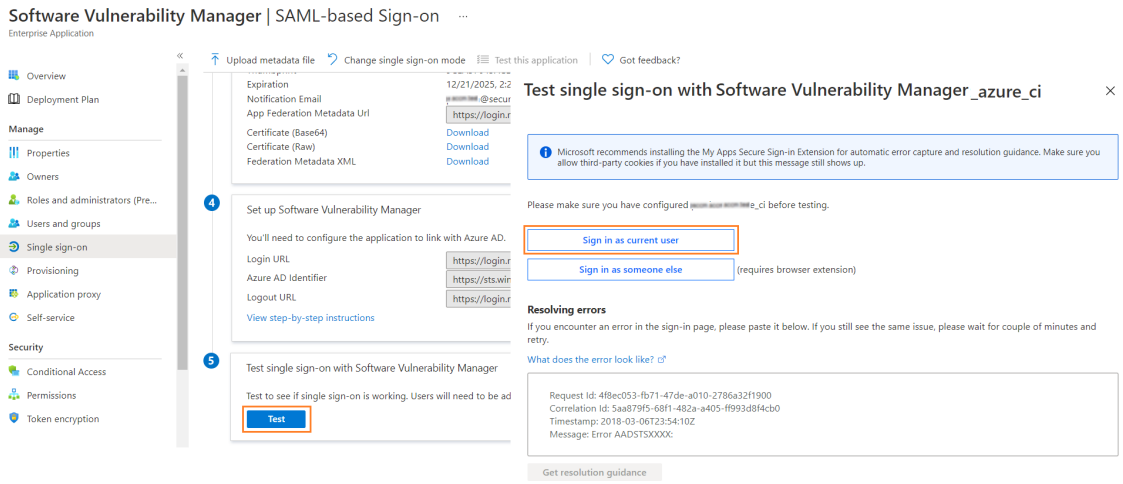
- Click + Add New claim to add new attributes and claims.
- The Manage claim page appears.
- Enter name in the text field.
- Select the source attributes from the drop down list.
- After selecting, click **Save**.

Follow the above steps and add attributes and claims for the following:

- firstName
- lastName
- email
- username
- accountKey

Note • *While selecting accountKey attributes paste the generated Account key which is copied from the Software Vulnerability Manager Configuration > Settings > IdP Configuration Instructions.*

7. After configuring, click **Test**, and then click **Sign in as current user** link.



8. After successful action it navigates to the Software Vulnerability Manager application.

Note • *You can also access through the Service Provider (SP) login for the created application by using the assigned user.*

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.

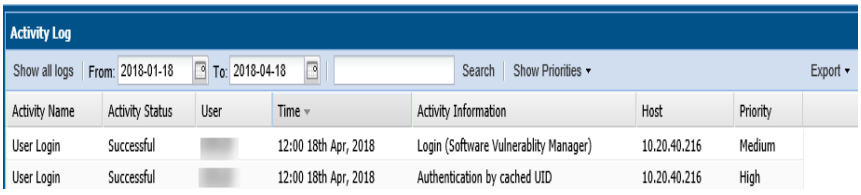
Right-click or double-click a message to copy the row data to the clipboard. Click **Clear** to remove all log entries. In the event of a support request you may be requested to provide relevant information from this page.

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.

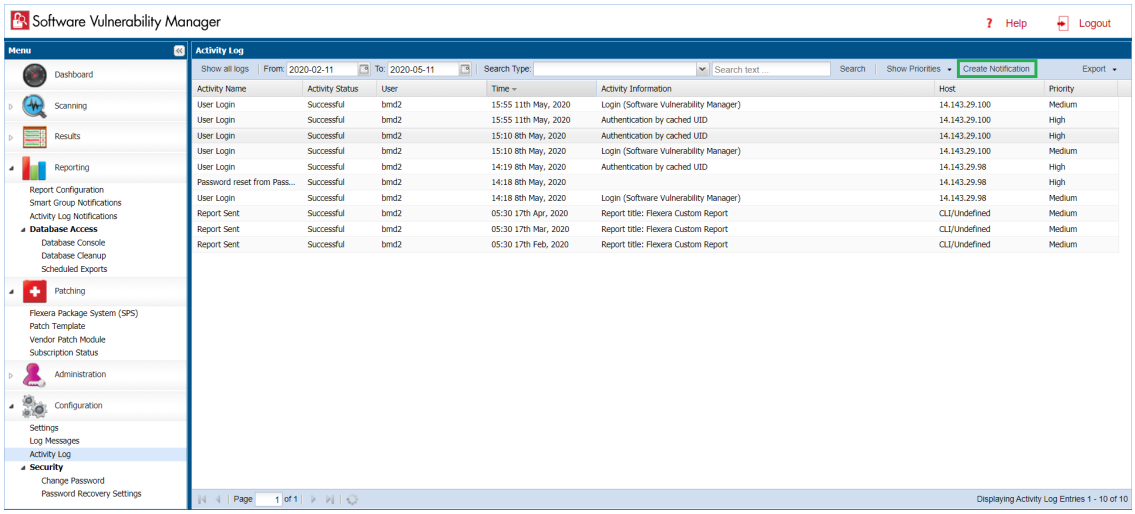


Create Notifications for the Activity Log

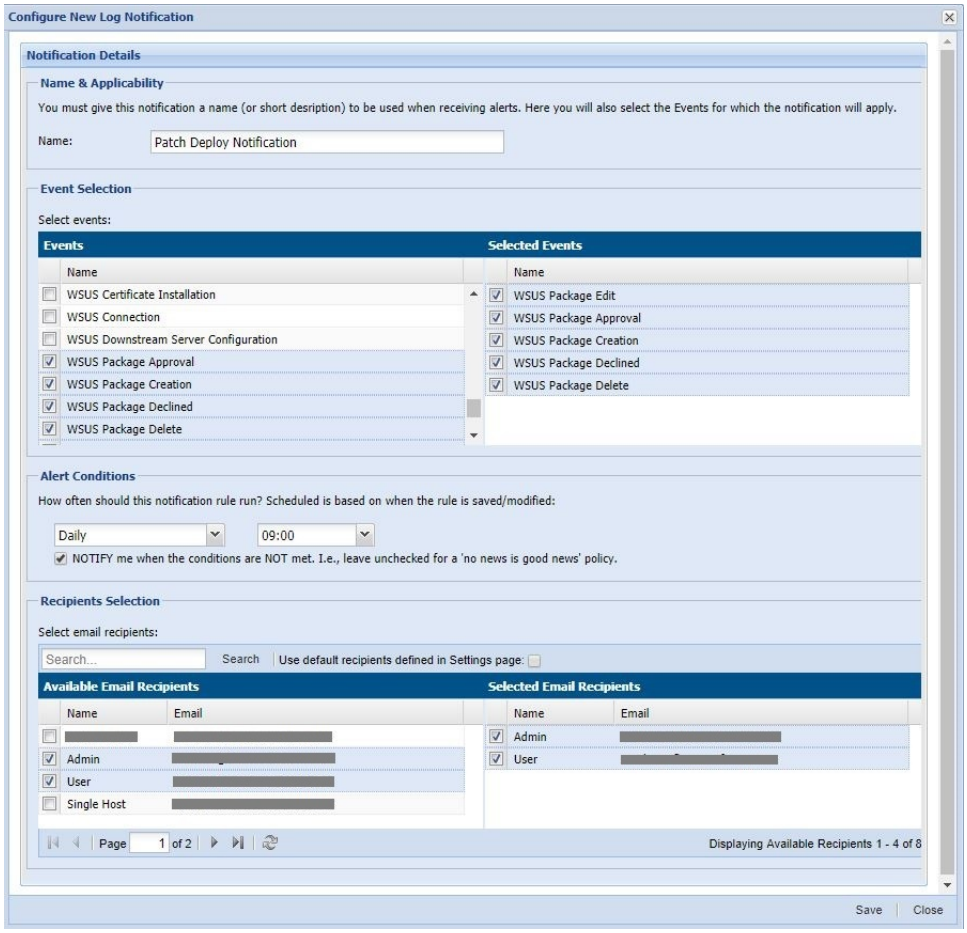
With this configuration, you can schedule multiple notification digest for the respective events through emails.

Task ***To create Notifications:***

1. Click **Create Notification**.



2. **Configure New Log Notifications** dialog box opens.

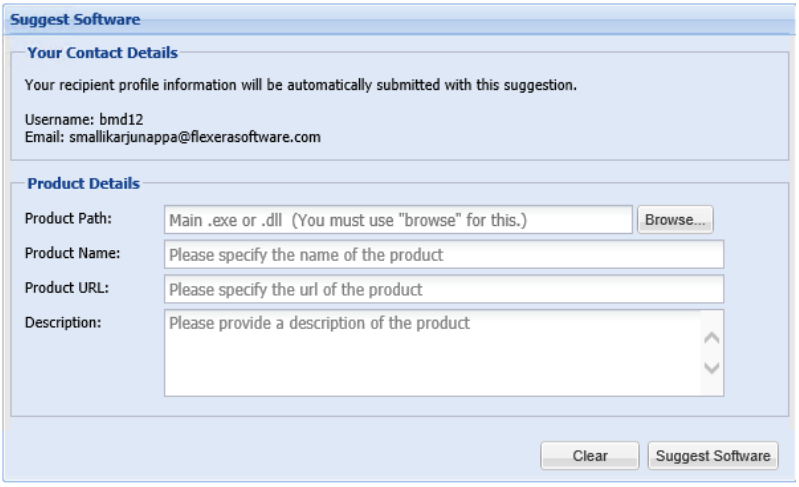


3. Describe notification name, select the required events, and then select notification schedules.
4. These email notifications can be scheduled on an **Hourly**, **Daily**, **Weekly**, or **Monthly** basis. If you select **Daily**, or **Weekly**, or **Monthly** option, then you choose the time duration for the selected day.
5. Choose the recipients and then click **Save**.

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.



Security

Software Vulnerability Manager provides the following security features for user passwords:

- Change Password
- Password Recovery Settings

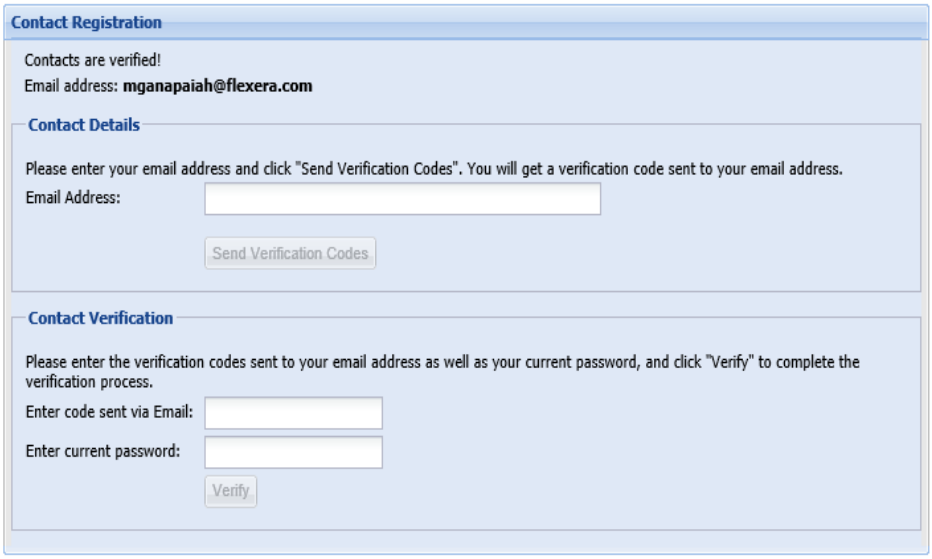
Change Password

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.

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:
Send Verification Codes
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:
Verify

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

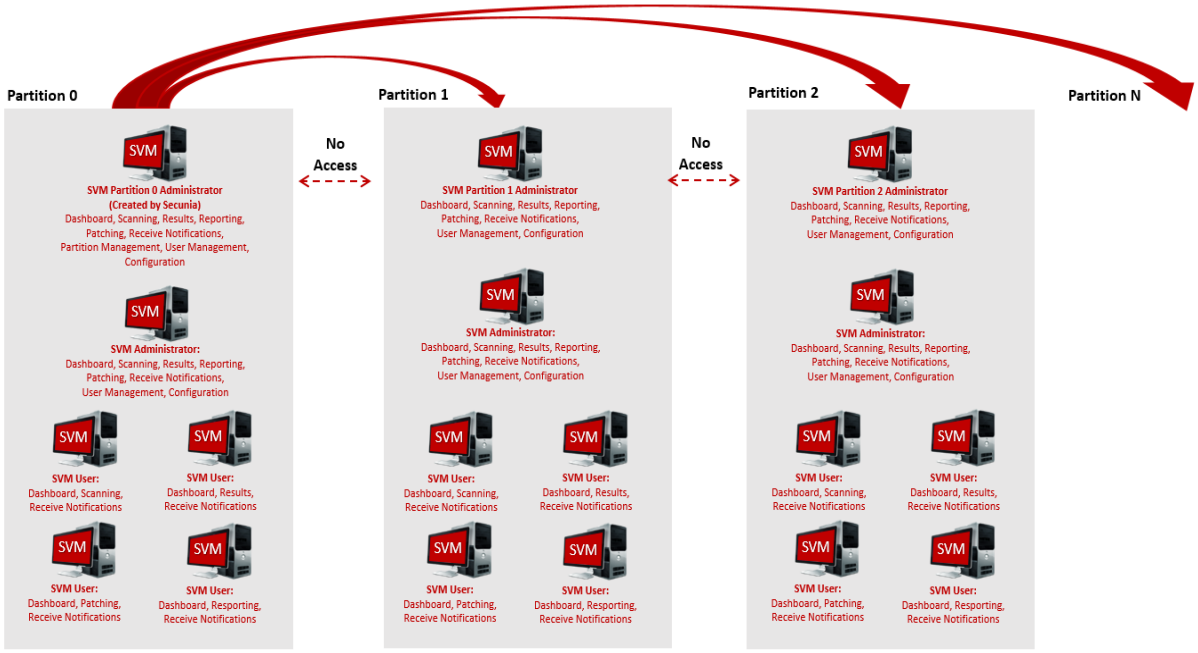
- Create a New Partition Administrator
- Grant User Access to all Completed Scans and Single Host Agent Entries

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.

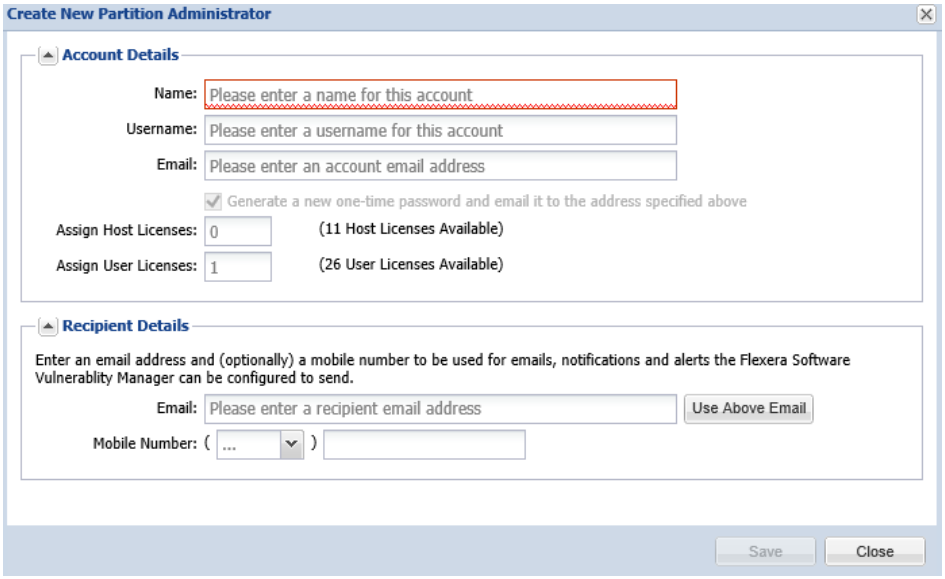
The Host and User licenses in a given partition belong to a shared pool. Any user who scans hosts will use host licenses from this pool. When a user is created, an Administrator can limit how many active licenses they can claim – note, this is only an upper bound of the licenses they can use, and should 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

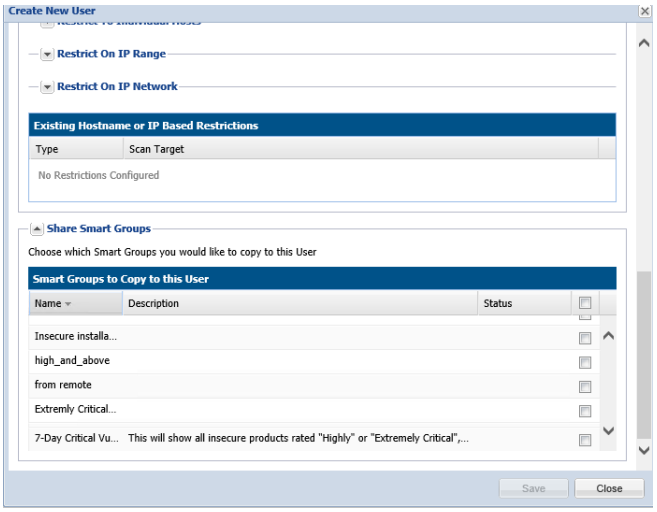
Click **Create New Partition Administrator** and fill in the form, providing all the necessary details about the Partition Administrator and include the number of host and user licenses to assign.



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.



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.

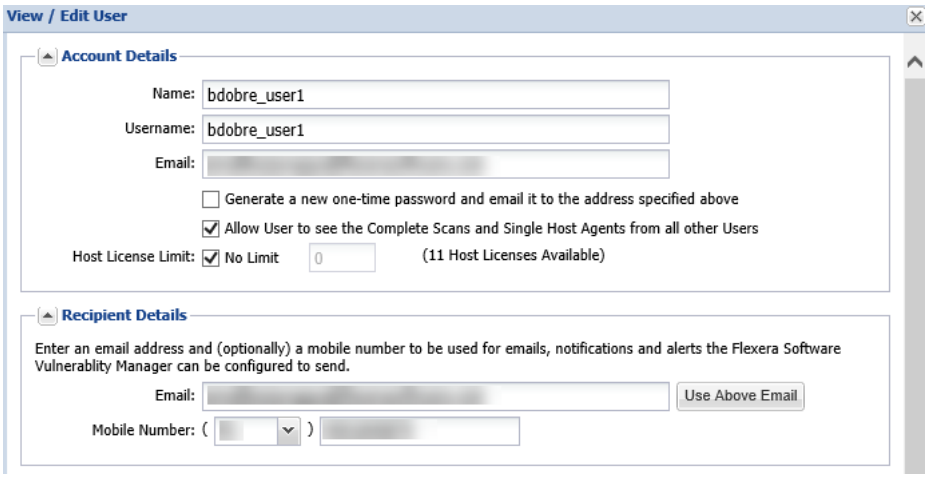
If the Partition Administrator modifies the Smart Group, all shared copies are also modified.

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.



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.*

B

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 and easily exploitable vulnerabilities that are otherwise designated “highly critical” but also have been exploited in the wild before their publication (zero-day). These vulnerabilities typically exist in services like FTP, HTTP and SMTP or specific client systems such as email programs or browsers. Operating systems can also be prone to them—e.g., when font handling is performed on operating system level.

Highly Critical

- This value is generally used for remotely and easily exploitable vulnerabilities that can lead to system compromise.

- Successful exploitation doesn't usually require any interaction, but there are no known exploits available at the time of disclosure.
- These vulnerabilities typically exist in services like FTP, HTTP and SMTP or specific client systems such as email programs or browsers. Operating systems can also be prone to them—e.g., when font handling is performed on operating system level.

Moderately Critical

This value is usually used for remotely and easily exploitable denial-of-service vulnerabilities against services like FTP, HTTP and SMTP. Additionally, easily exploitable vulnerabilities that could lead to information disclosure or affect the integrity of a product can result in this criticality level.

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 and local 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

D

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
- It has been linked to POC verified
- It has been linked to vulnerability developed tools
- It has been linked to verified intelligence

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	Medium	+2
Historically Linked to Remote Access Trojan	Low	+1
Recently Linked to Ransomware	Medium	+2
Historically Linked to Ransomware	Low	+1
Recently Linked to Penetration Testing Tools	Medium	+2
Historically Linked to Penetration Testing Tools	Low	+1

Table D-1 • Rules, Severity and Value

Rule	Severity	Value
Recently Linked to Malware	Medium	+2
Historically Linked to Malware	Low	+1
Recently Linked to Exploit Kit	Medium	+2
Historically Linked to Exploit Kit	Low	+1
Linked to Recent Cyber Exploit	Low	+1
Linked to Historical Cyber Exploit	Low	+1
Recently exploited in the wild	Very Critical	+5
Exploited in the wild in the past year	Critical	+4
Historically exploited in the wild	High	+3
Recent remote code execution POC verified	Critical	+4
Recent POC verified	High	+3
Historical remote code execution POC verified	Medium	+2
Recent possible POC	Medium	+2
Historical POC verified	Low	+1
Tools to exploit the vulnerability developed recently	Medium	+2
Tools to exploit the vulnerability developed historically	Low	+1
Recently verified intelligence	High	+3
Historically Verified intelligence	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

Table D-2 • Criticality - Ranges

Criticality	From	To
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
  - Recent remote code execution POC verified
- **CVE2 triggers**
  - Historically Linked to Exploit Kit

The Threat Score would be **51**.

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
Recent remote code execution POC verified	+4

Item	Value
Linked to Recent Cyber Exploit	+1
Historically Linked to Remote Access Trojan	+1
Threat Score (Sum of above values)	**51**

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**
  - Recently Linked to Malware

The Threat Score would be **23**.

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 13 and 23.

Item	Value
Base Score	+13
Recently Linked to Malware	+2 * 7 CVE = +14
Threat Score (Sum of above values)	**27** ***Note*** • *At this point, we have exceeded the maximum for a critical threat, which is 23, so the score is 23.*

Example 3

A SAID has one CVE and it comes back as exploited.

Triggered Rules

The following rule is triggered:

- **CVE1 triggers**
  - Historically exploited in the wild

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
Historically exploited in the wild	+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
• Offers a Threat Score at the Advisory level	• 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

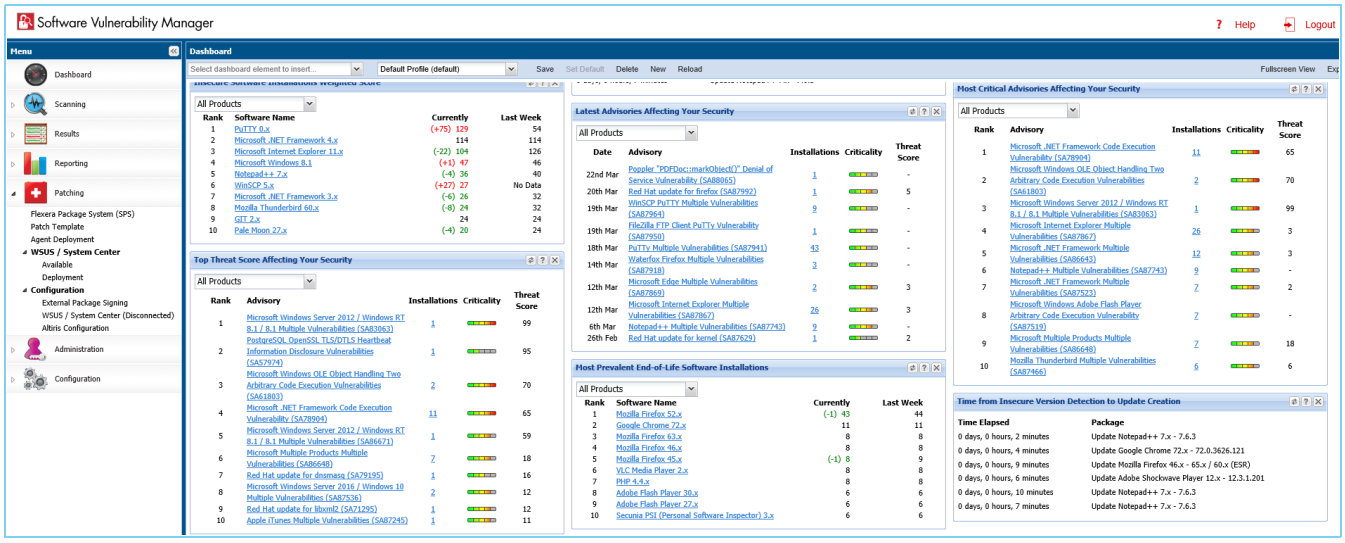
In Software Vulnerability Manager, subscribed users can find the Threat Score in the following places:

- 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

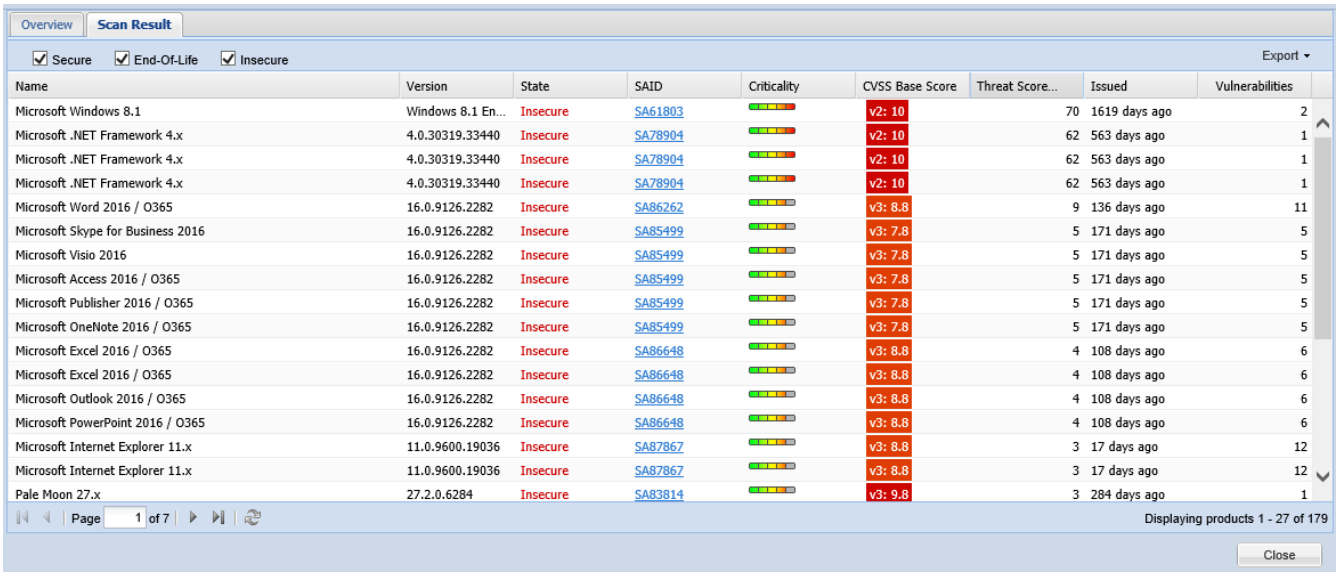
Dashboard Threat Score

The following image is an example of the Dashboard Threat Score.



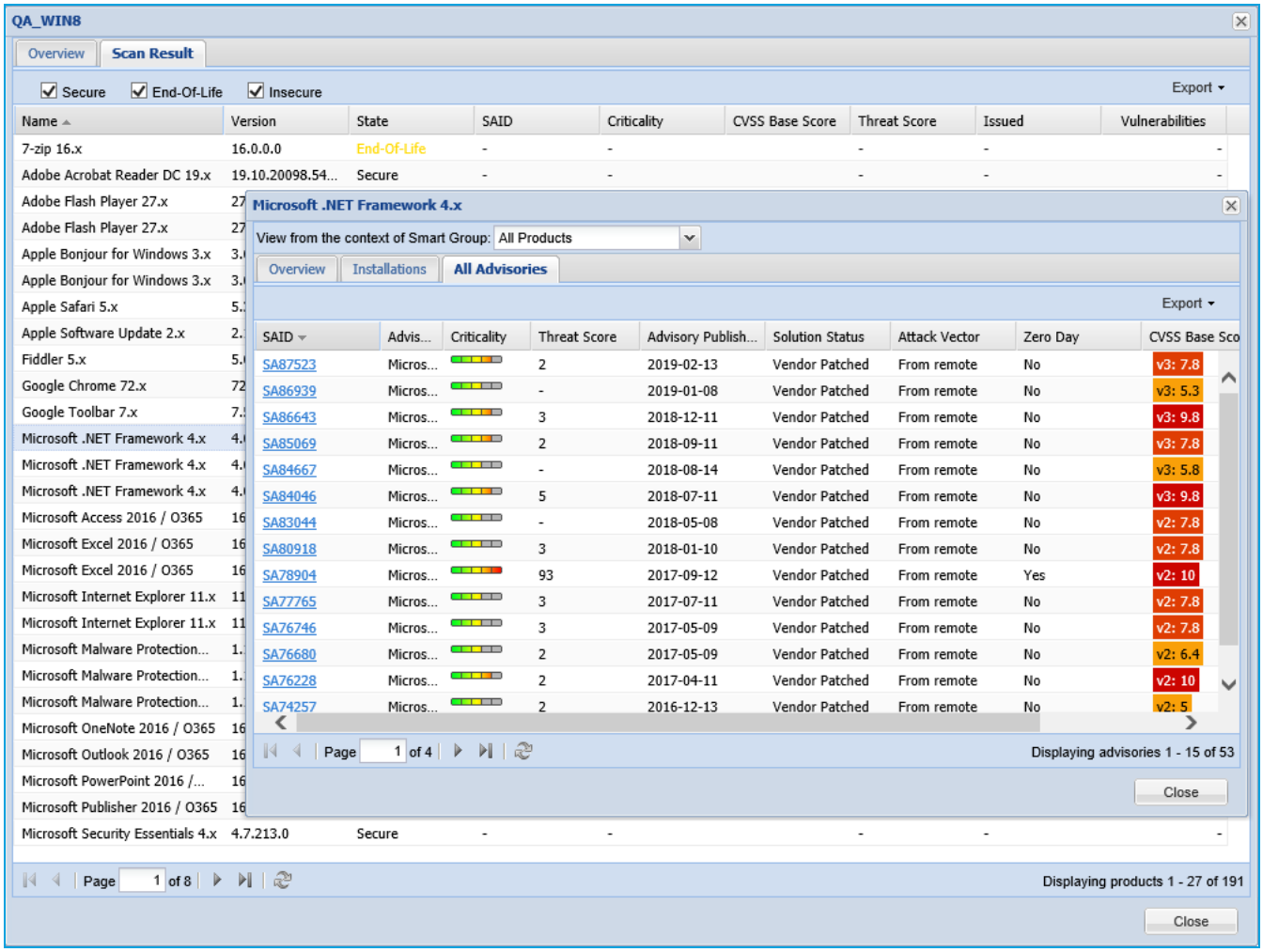
Completed Scan Page Threat Score

Once the scan is completed, the user can see the **Threat Score** in the **Scan Result**.



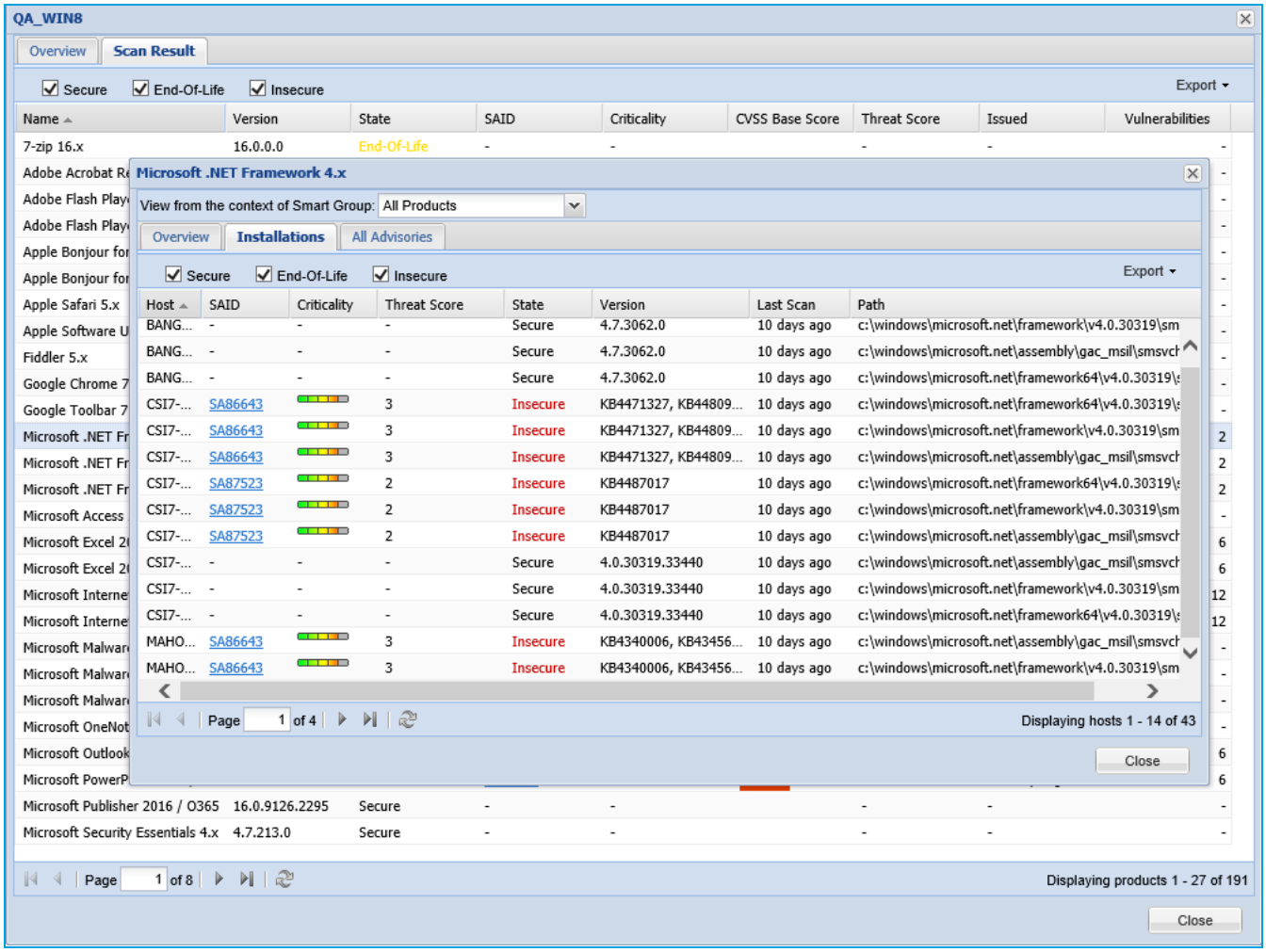
All Advisory Popup Threat Score

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**.



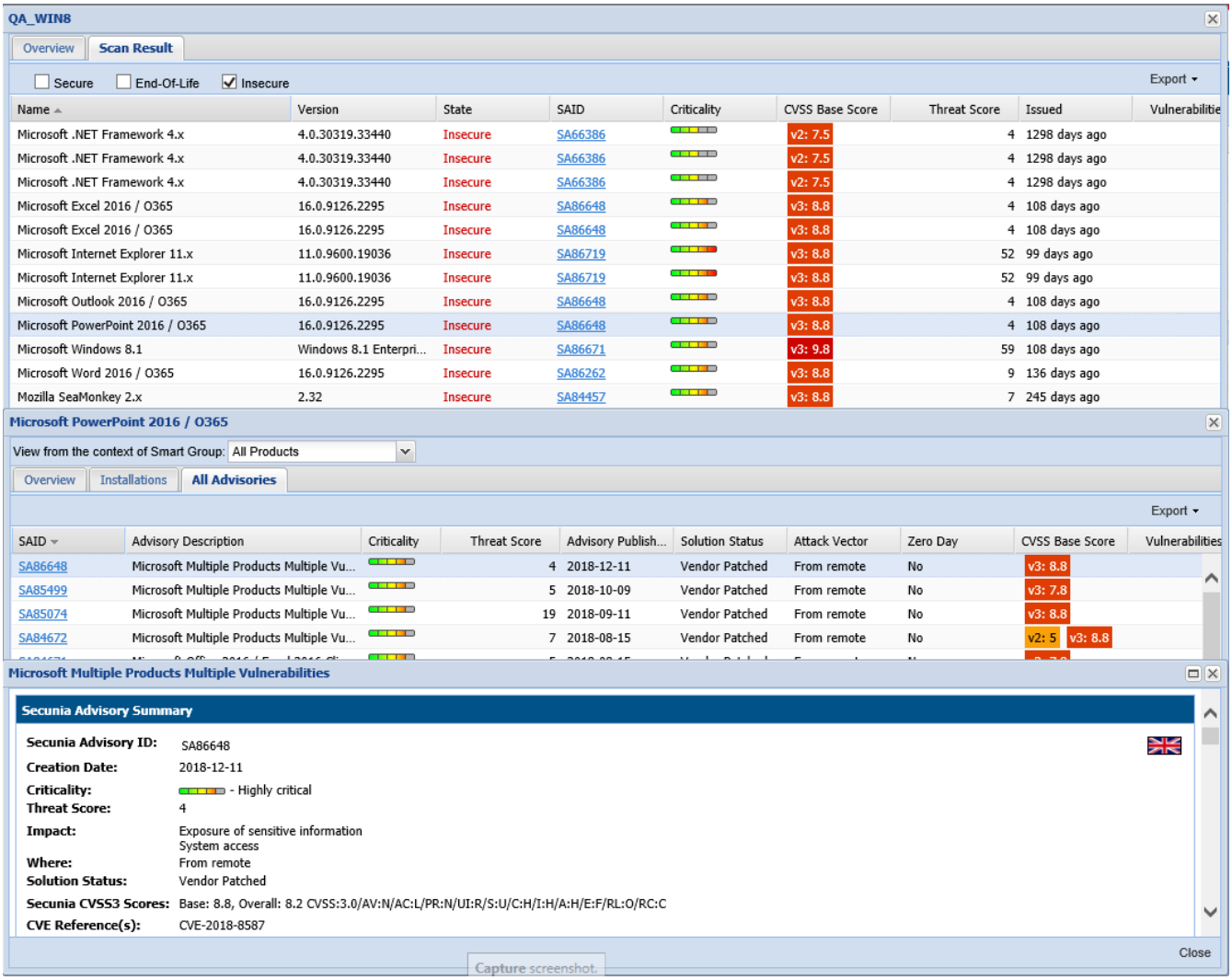
All Installation Popup Threat Score

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**.



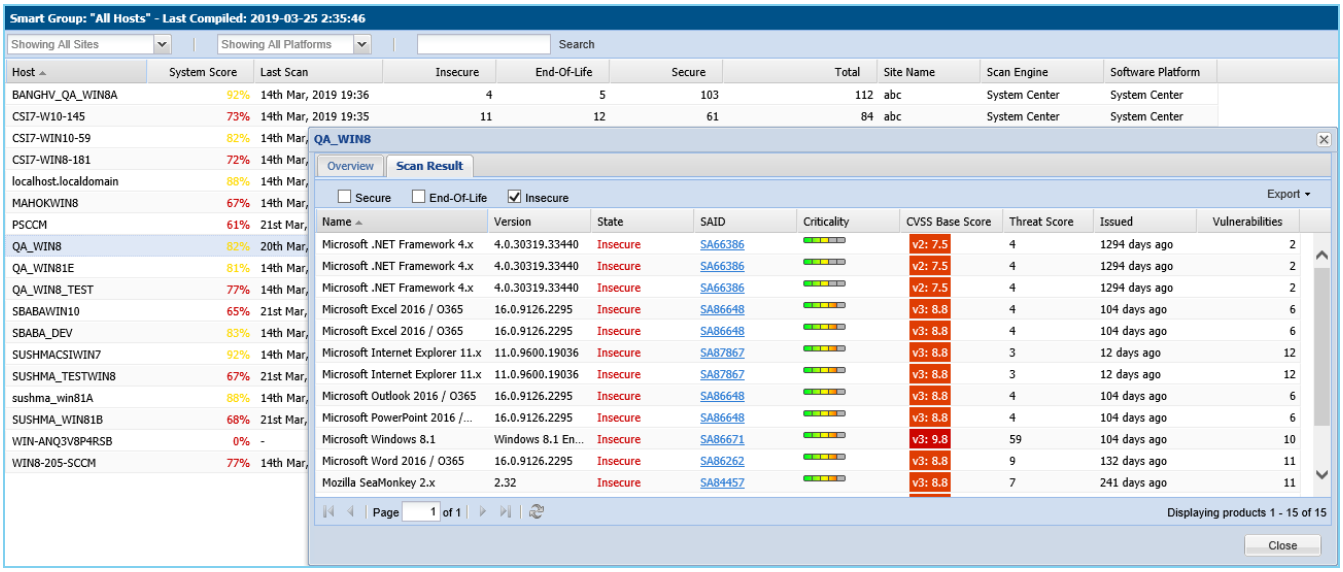
Advisory Summary Threat Score

After Clicking on any **SAID**, a popup appears with the **Threat Score** and other required details.



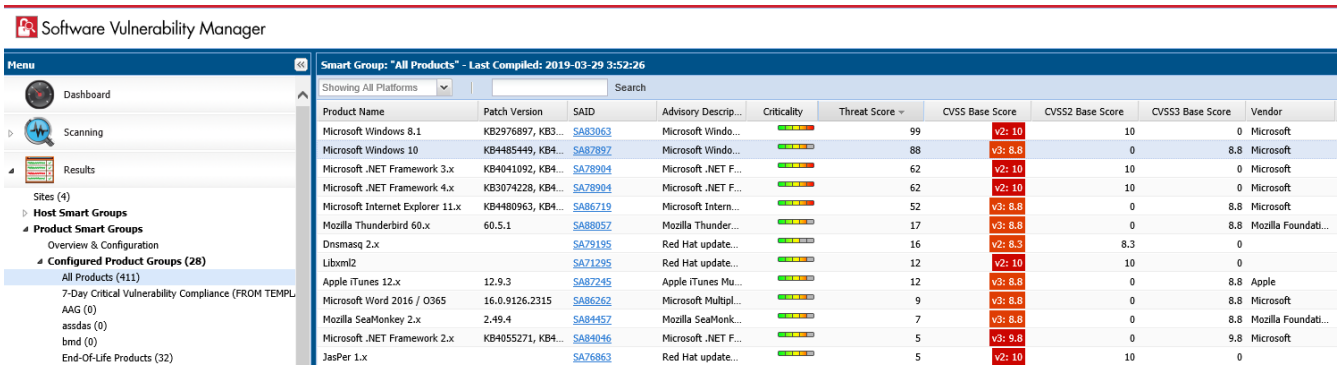
Host Smart Group Threat Score

The **Threat Score** appears for all the products on the **Host Smart Group Scan Result** page.



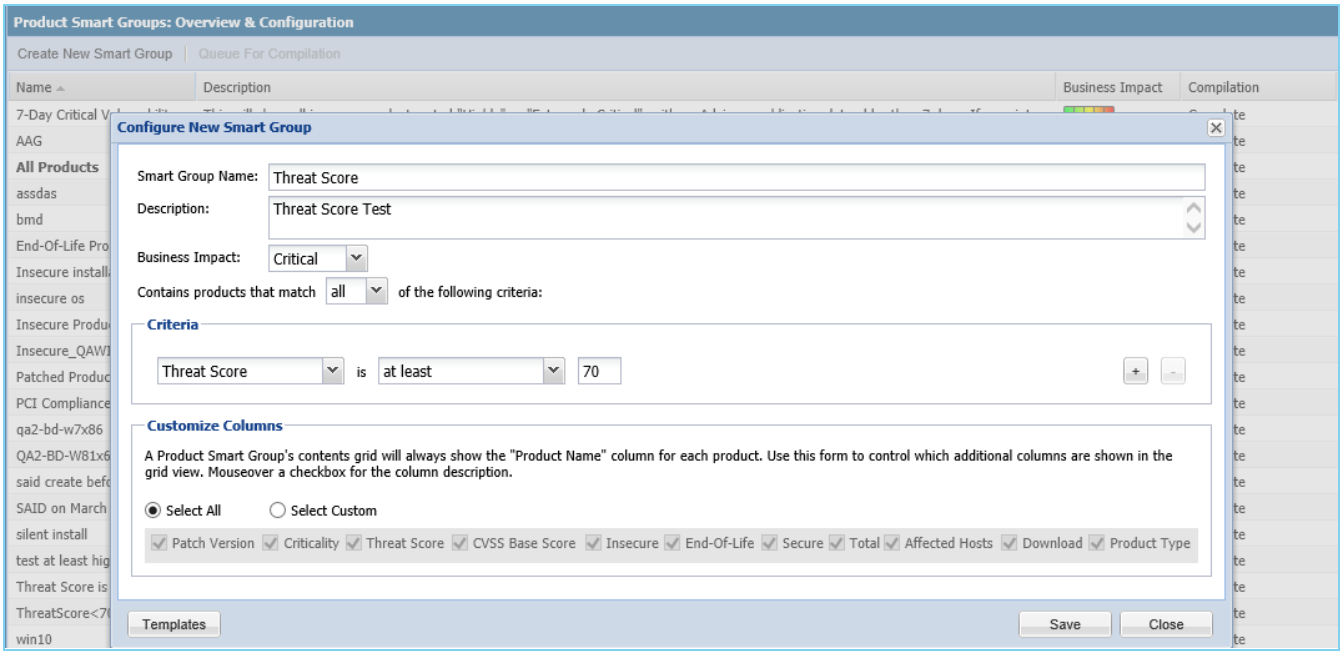
Product Smart Group Threat Score

The **Threat Score** appears for all the products on the **Product Smart Group Result** page.



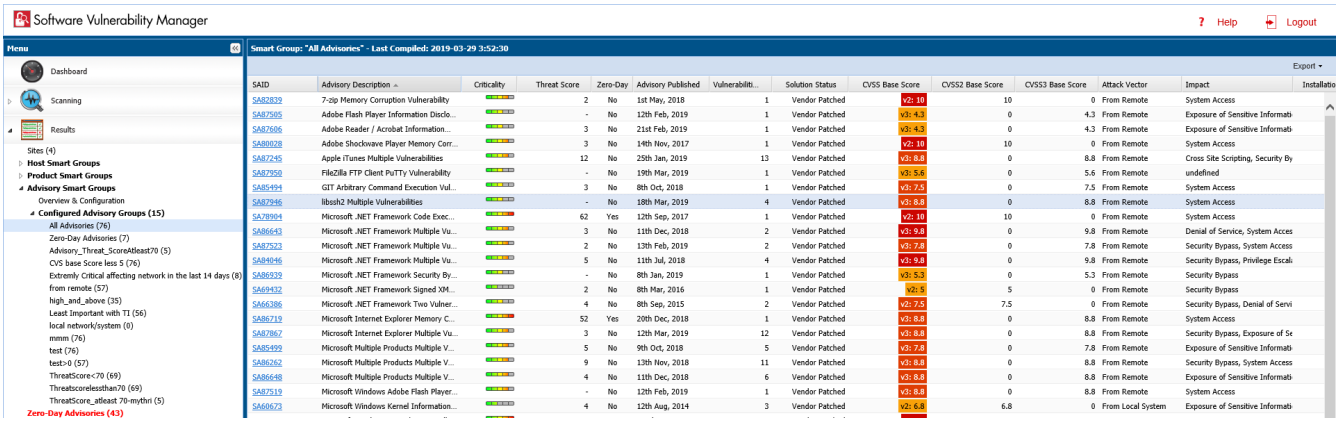
Smart Group Criteria Threat Score

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**.



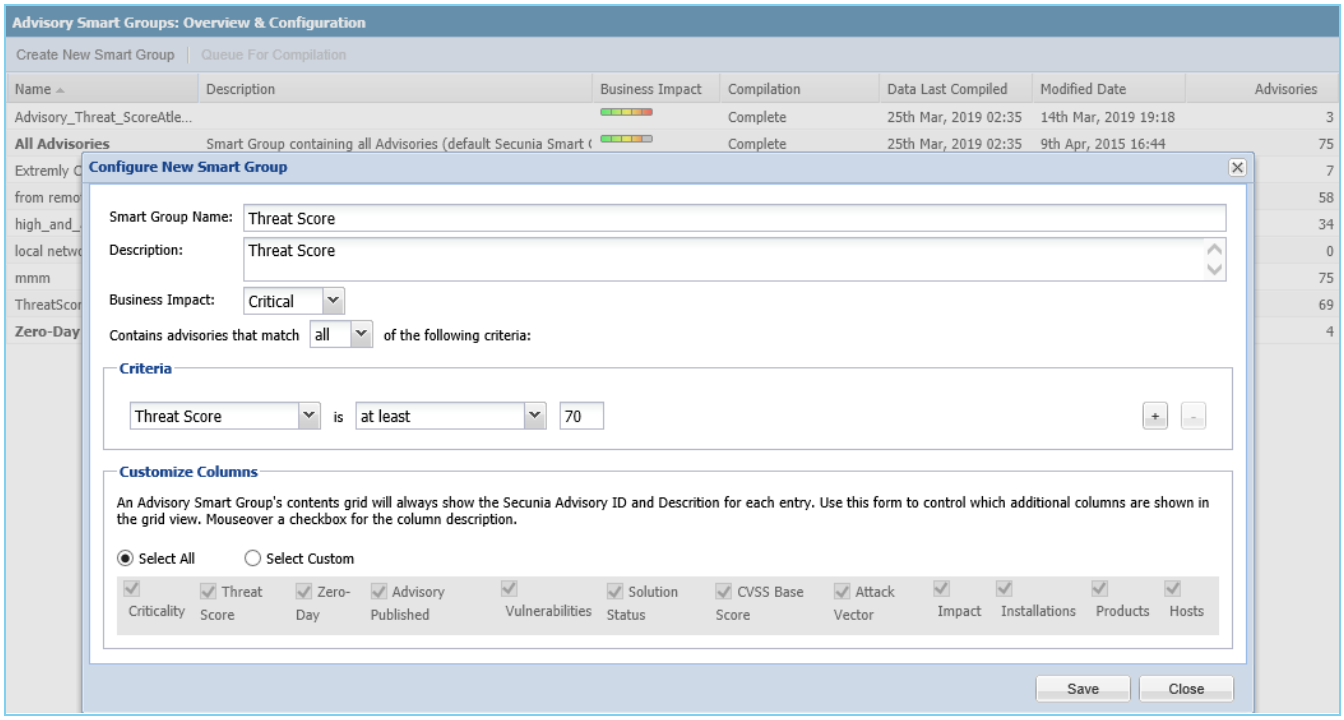
All Advisory Threat Score

The **Threat Score** is made available in the **All Advisories** page.



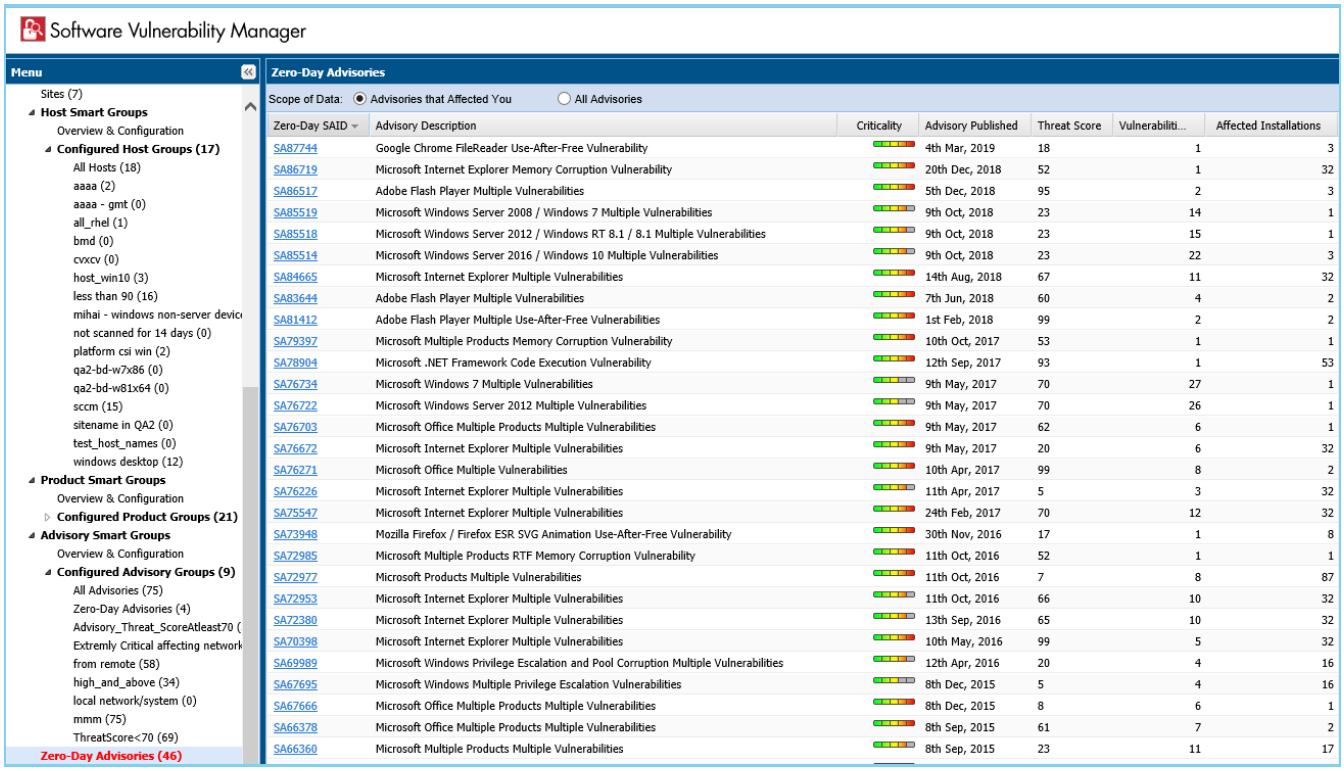
All Advisory Smart Group Criteria Threat Score

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**.



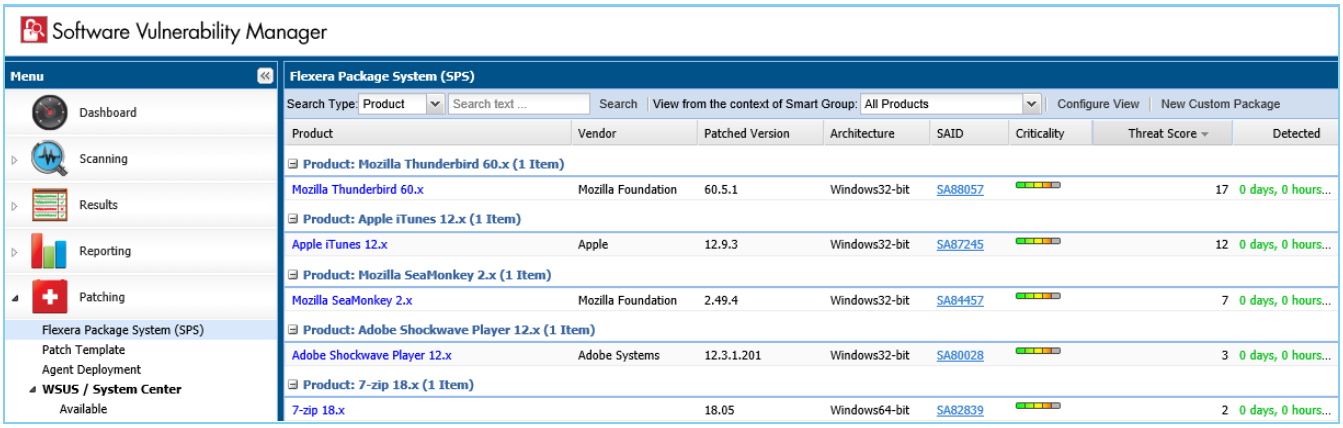
Zero Day Advisory Threat Score

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 form the vulnerability track table.



Flexera Package System (SPS) List Threat Score

The Threat Score appears in the Flexera Package System (SPS) list, which helps user to prioritize patches.



Appendix E - Optimization Features

This appendix explains Optimization Features of the Software Vulnerability Manager:

- Web
- Agent
- Good to know options

Web

This section includes the following topics:

- No scan option
- Increase Smart Group worker threads for on-Prem customers
- Changing scan result as completed (status 4) for old incomplete scans

No scan option

To prevent the SVM Agent from flooding the server by uploading the data file very time to the server. We have added a feature where agents checks the hash value of the last data file and the current data file. If both the hash are send then agent will not upload the data file to the server instead it will call another API (no_change). So server will get to know that last data file and current data file both are same and hence copy the previous result and reprocess it.

Specifies the frequency to skip submitting scan (.gz file) to server if previous submitted scans match with new scan

Applicable to single host agent scan

Specify 0 to opt out of this feature

Default value 3, If scan frequency is daily, value of '3' will skip processing scan on server for 3 days if no new inventory is detected on client machine.

```
Add entry to

/usr/local/Secunia/csi/config/config.ini or /usr/local/Secunia/ config.ini

SKIP_ON_SAME_SCAN_HASH = 0
```

Increase Smart Group worker threads for on-Prem customers

Smart Groups compilation can often take more time than what customers assume, or effortlessly define as acceptable by themselves, and you may need to know the exact way compilation of Smart Groups is performed.

Find out more by running the following commands in the Linux terminal that will output useful definition of the compilation processing:

```
cd /usr/local/Secunia/csi/cronjobs/sgdaemon

more configuration.ini
```

There is an easy to understand logic that allows measurement and predictability of the process workings, and workers. The compilation process basically has the following simple logic:

File config.common.ini (path: Secuina/csi/api/config) having defined constant **SMARTGROUP_GENERATION_FAST_LIMIT** which decides smart group compile time duration to consider as 'fast track' or slow track.

Support can check the column 'time elapsed' column in table ca.csi_smartgroup_generation for existing partitions and can intelligently guess the required time to consider any partition as 'fast_track'.

If a Smart Group has last compiled for less than 5000ms (as example) - put it for next compilation in the "fast track"

If the Smart Group has last compiled for more than 5000ms (as example) - it will be forwarded through the "slow track"

Count of FastWorker and SlowWorker can be modified in file configuration.ini (Path: cronjobs/sgdaemon) based on existing CRON server load.

After making changes in configuration.ini, please restart the sgdaemon (systemctl restart sgdaemon).

The last compilation time depends on the value of each Smart Group as provided under the 'time elapsed' column that is present in the ca.csi_smartgroup_generation database table of the SVM server.

The server directory /usr/local/Secunia/csi/cronjobs/sgdaemon stores the smart group compilation and configuration settings at the configuration.ini file. Kindly restart.

In it, you could enable Smart Group generation logging as follows:

```
file_logging=1 sets logging for the SGDaemon service and writes the data at the /tmp/
secunia_smartgroup_daemon_log.txt file
```

Changing scan result as completed (status 4) for old incomplete scans

Changing scan result as completed (status 4) for old incomplete scans, default value 7 days and input zero or negative integer value(i.e. -1) if pending scan queue cleanup is not required.

```
'SCAN_OLD_DAYS_CHANGE_STATUS'
```

Agent

This section includes the following topics:

- Agent scan randomization during agent deployment
- Stop status API polling
- Add timeout for Windows Update Agent (WUA) calls
- Agent now supports recovery settings
- Support Type 1 scanning for SCCM imports
- Detect missing security updates from Microsoft System Center

Agent scan randomization during agent deployment

SVM now has a command line option to 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 120 would mean that the scanning agent will start scanning after a delay of random minutes, which could be from 1 to 120 minutes.

Stop status API polling

To prevent the SVM Agent from flooding the server with requests for scan status every second, new polling logic has been implemented. This new polling logic helps increase the scalability of the web server to support more agents.

Add timeout for Windows Update Agent (WUA) calls

The SVM agent has a new time-out mechanism that enables one to configure a time-out period for WUA searches. This option prevents the SVM agent from being stuck waiting for the WUA service to return with data. The default timeout is 30 minutes and is configurable via the -- wua-timeout option. A value of zero means the SVM agent will wait indefinitely for the WUA call to respond back.

Example: csia.exe -I -L - wua-timeout 5

Agent now supports recovery settings

When installing the Software Vulnerability Manager Agent for Windows, Administrators can configure the agent recovery settings on a per deployment basis. The agent recovery settings are co-located in the agent package with the Run-As-User, Proxy and Site variables. For the online help reference, see Agent Configuration Options.

Support Type 1 scanning for SCCM imports

SCCM Imports now support Type 1 scans via ActiveX or the Daemon.

To enable this advanced feature, edit the following registry keys:

- For the Daemon, you can specify the inspection type using the -t command line parameter or the Daemon registry key: [HKEY_CURRENT_USER\Software\Secunia\Daemon]"InspectionType" = dword:00000001
- For ActiveX, you can specify the inspection type using the CSI Plugin registry key: [HKEY_CURRENT_USER\Software\Secunia\CSI Plugin]"InspectionType" = dword:00000001

Detect missing security updates from Microsoft System Center

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.

Good to know options

This section includes the following topics:

- Restarting the Smart Group Daemon Resets the In-Progress State
- Flexera Software Package System (SPS) Timestamp
- Include --delete-all-settings for Mac agents
- Support Type 1 Scanning for SCCM Imports
- Thread Priority for Agent
- Live Update for Microsoft Products
- To skip submitting scan frequency

Restarting the Smart Group Daemon Resets the In-Progress State

If the Smart Group Daemon is shut down unclean, such as when there is an unscheduled database server shutdown, then the daemon can leave generations in an in-progress state. Previously, the Daemon would reset stuck states after a certain period of time (hours or days). Now when the Smart Group Daemon restarts, it will check for generations that are in the in-progress state within intervals as set by the configuration setting.
SMARTGROUP_GENERATION_ABANDON_INTERVAL_PER_SMARTGROUP. If the daemon finds such a generation it will reset them, so that they could be processed again.

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 SPS.

Include --delete-all-settings for Mac agents

The new Mac agent includes the --delete-all-settings parameter that will wipe out all information, including GUID, from the system to ensure it is clean to accommodate a new installation.

Support Type 1 Scanning for SCCM Imports

SCCM Imports now support Type 1 scans via ActiveX or the Daemon.

To enable this advanced feature, edit the following registry keys:

- For the Daemon, you can specify the inspection type using the -t command line parameter or the Daemon registry key: [HKEY_CURRENT_USER\Software\Secunia\Daemon]"InspectionType" = dword:00000001
- For ActiveX, you can specify the inspection type using the CSI Plugin registry key: [HKEY_CURRENT_USER\Software\Secunia\CSI Plugin]"InspectionType" = dword:00000001

Thread Priority for Agent

By default, the agent sets the lowest thread priority (THREAD_PRIORITY_IDLE), and begins background processing mode so that it can perform background work without significantly affecting activity in the foreground. The thread priority can be changed via command line (--scan-thread-priority) or registry (ScanThreadPriority) by specifying one of the following values:

0: THREAD_PRIORITY_NORMAL

1: THREAD_PRIORITY_BELOW_NORMAL

2: THREAD_PRIORITY_LOWEST

3: THREAD_PRIORITY_IDLE

ScanThreadPriority is a DWORD registry value. The agent reads the setting from HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Secunia\CSI Agent when running under the Local System account, and from HKEY_CURRENT_USER\SOFTWARE\Secunia\CSI Agent when running under other user.

Live Update for Microsoft Products

To include Microsoft products for Live Update:

Include the following configuration option in **/usr/local/Secunia/csi/api/config/config.ini** file:

INCLUDE_MS_PRODUCTS_FOR_LIVE_UPDATE = 1

To skip submitting scan frequency

Include the following configuration option in **/usr/local/Secunia/csi/api/config/config.ini** file:

Specifies the frequency of skip submitting scan (.gz file) to server if previously submitted scans match with new scan. It skips 3 times for value 3.

SKIP_ON_SAME_SCAN_HASH=3

F

Appendix F - Troubleshooting Techniques

This appendix explains Troubleshooting Techniques of the Software Vulnerability Manager:

- Intune
- Patch Daemon

Intune

This section includes the following topics:

- Pre-requisites
- Publishing
- SVM Patch Configuration
- SVM Patch Configuration / General Tab
- Troubleshooting Tips
- FAQs

Pre-requisites

Intune POC (Proof of Concept) requires the following prerequisites:

- For Intune connection details, refer Add Intune API Application (Client) ID and Directory (Tenant) ID on Intune Connection. For more details, see Intune Publishing and Set up a Distribution Connection in Flexera SVM Patch Configuration for Microsoft Intune.
- To get Application (Client) ID, Directory (Tenant) ID, and Client Secret app registration need to be done. For more details, see App Registration and Create Client Secret.

- Make sure that the following Intune Graph API Permission are available to the user. For more details, see API Permissions.
- Make sure that you have at least five to eight distribution endpoints in your sample test environment.
- To enroll a device/endpoint to an Intune follow this link https://docs.microsoft.com/en-us/mem/intune/user-help/enroll-windows-10-device
- For each endpoint, please ensure:
  - Endpoints have been recently booted up to ensure there are no pending updates that could hinder Intune publishing.
  - The credentials that will publish to endpoint has permissions to run PowerShell scripts - not required.
  - If installing Win32 apps then antimalware settings should exclude the following directories

    On x64 client machines:

    - C:\Program Files (x86)\Microsoft Intune Management Extension\Content
    - C:\windows\IMECache

    On x86 client machines:

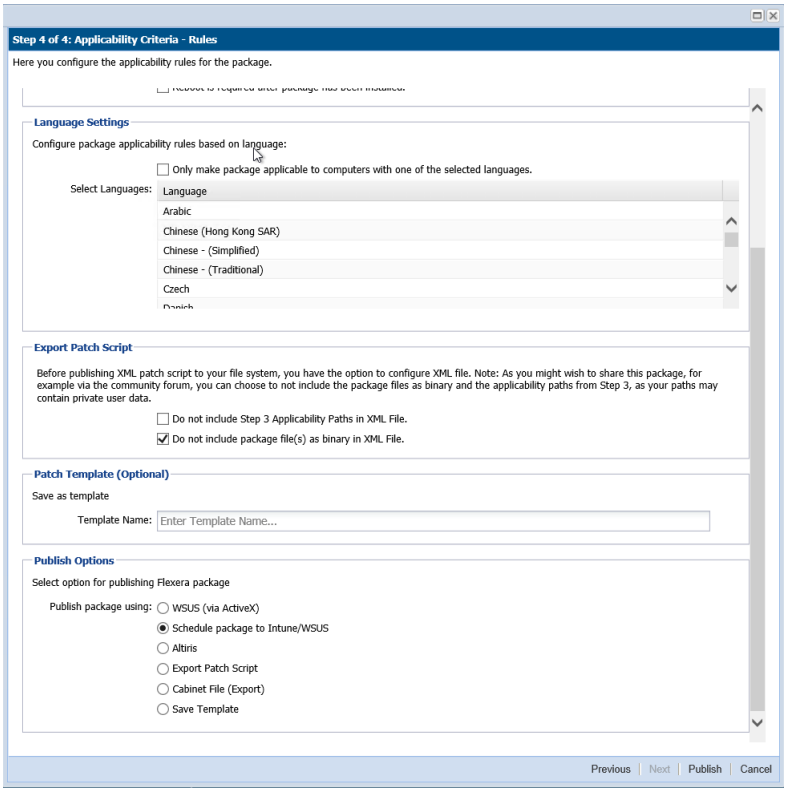
    - C:\Program Files\Microsoft Intune Management Extension\Content
    - C:\windows\IMECache

Publishing

Once the pre-requisites are completed, you can begin publishing from the SVM console.

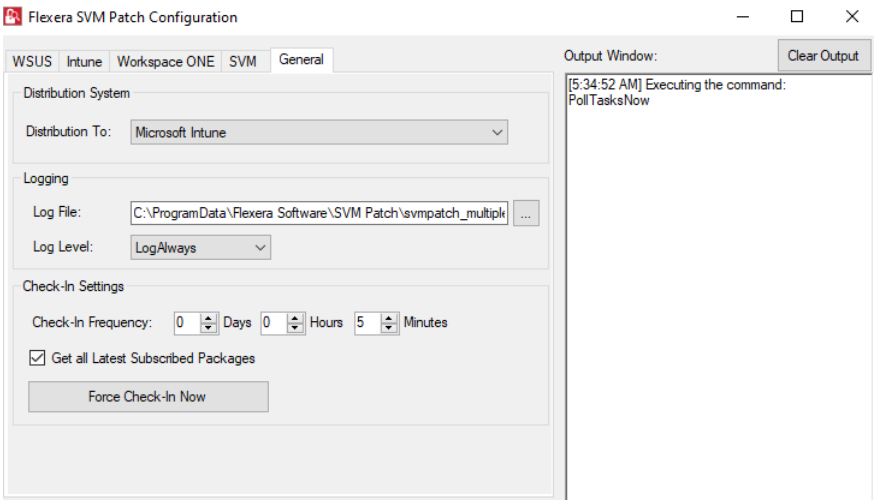
To create and publish the package, see Create and Publish the Package.

In Step 4 of the Publishing Wizard, use Schedule package to Patch Daemon and publish.



SVM Patch Configuration

The Flexera SVM Patch Configuration Tool can control the publish into Intune.



For more information on Intune connection, see Flexera SVM Patch Configuration.

SVM Patch Configuration / General Tab

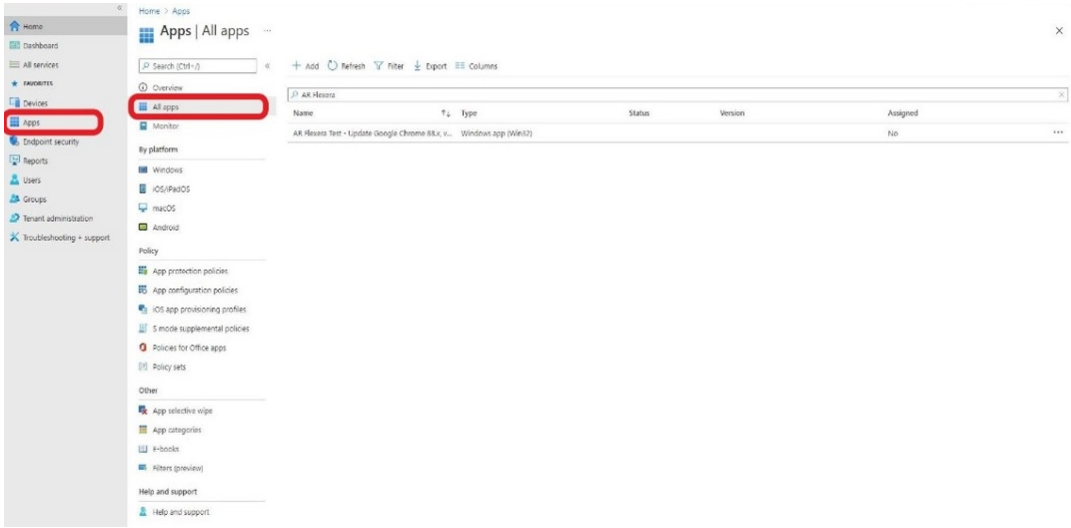
To set SVM Patch Configuration, perform the following steps.

Task ***To configure:***

1. In the General Tab set the **Distribution To: Microsoft Intune**.
2. You can click **Force Check-In Now** to distribute to Intune immediately or wait for the Check-In.
3. You can check log file (c:\ProgramData\Flexera Software\SVM Patch\svmpatch.log) for confirmation that publishing happened to Intune. Here is a sample line:

   [26/05/2021 16:09:35|V] [POST data]: {"data":{"package_id":"f8072330-ddd2-469f-8762-e3cd28a2969d","error":""},"status":"success","task_type":"publish_package"}

4. You can then check for your app in Intune.



5. Now that your Application is in Intune, you can decide how to distribute.

Troubleshooting Tips

Following are the troubleshooting tips for Intune:

- Intune log file location is C:\ProgramData\Microsoft\IntuneManagementExtension\Logs. For detailed debugging check IntuneManagementExtension.log. Search for package name / Application ID.
- Use %WinDir%\CCM\CMTrace.exe tool to read Intune logs.
- Installation status of SPS package logged at C:\windows\SecuniaPackage.log
- If install fails most time the reason is, the file in use by other application. In such cases, restart the machine. Some other common reasons are listed here.

- Debugging for PowerShell script not running, refer https://docs.microsoft.com/en-us/mem/intune/apps/intune-management-extension#issue-powershell-scripts-do-not-run
- Check whether the service **Microsoft Intune Management Extension** is running in endpoint.
- Intune Management extension polls for packages for every hour. We can do force polling by restarting the Microsoft Intune Management Extension service.
- Once the package gets installed, it takes at least five minutes to reflect in Apps section of Intune interface. Sort by Date created to list recently published packages.

FAQs

The following table provides answers to frequently asked questions regarding Intune application.

Table F-1 • FAQs

Question	Answer
Do endpoints need to have PowerShell execution policy to allow script execution?	Not required to have execution permissions for a patch to get installed. We made **Enforce script signature check and run script silently** in detection scripts to No for an Intune application. Hence it bypasses the execution-policy and runs irrespective of the execution policy being set in endpoint.

Do any files be excluded from virus scanning in endpoints?	Antimalware settings should exclude the following Intune directories:
	• On x64 client machines:
	  • C:\Program Files (x86)\Microsoft Intune Management Extension\Content
	  • C:\windows\IMECache
	• On x86 client machines:
	  • C:\Program Files\Microsoft Intune Management Extension\Content
	  • C:\windows\IMECache
	More details, see https://docs.microsoft.com/en-us/mem/intune/apps/apps-win32-troubleshoot

Is it possible to deploy the agent via Intune?	Yes via a feature in the product introduced in the April release of the Patch Daemon (version 5.0.385 and above).
What permissions does the Patch Daemon account require? Does it require PowerShell script execution rights?	• It requires an account which has access directory as an administrator with rights to create new app registrations. • It does not require PowerShell execution permissions as PowerShell is not leveraged when publishing a package to Intune.

Patch Daemon

This section includes the following topics:

- Pre-requisites
- Publishing a Package from Patch Daemon without Local Administrator Rights

Pre-requisites

Patch Daemon requires the following pre-requisites:

- Software Vulnerability Management Patch Daemon needs RSAT (Remote Server Administration Tools) for Windows 10, to manually install for Windows 1809 and below, download from https://www.microsoft.com/en-us/download/details.aspx?id=45520. For latest Windows 10, Settings > Optional Features > Add Feature > RSAT: Windows Server Update Services Tools.
- Download SVM Patch Daemon at https://resources.flexera.com/tools/SVM/SVMClientToolkitInstall.msi

Publishing a Package from Patch Daemon without Local Administrator Rights

Perform the following steps to publish a package from Patch Daemon without local Admin rights.

Task ***To publish a package from Patch Daemon without Local Admin Rights:***

1. Install the patch daemon, configure it using local Administrator account and perform the following steps:
   a. Add your **Flexera Software Vulnerability Manager Patch Daemon** service account user (for example: test_user) to local Administrators and WSUS Administrators groups on your DC.

      Note • *Some of the security policies in environments do not allow adding users to the local Administrators group but only to WSUS Administrators.*

   b. To resolve permission issues when you cannot add a user to the local Administrators group, you would need to configure the below settings in the machine where the patch daemon is installed to allow your user to publish a package successfully.

      Give your service user account Full control over all the below items and perform all actions using an administrative account.

   c. Ensure that test machine contains WSUS certificate. If not, please export the certificate from WSUS machine from path Trusted publishers and install in the test machines in Trusted root certification authority and Trusted publishers.
2. Registry
   a. Add permission to the below registries to your service account (test_user) in the test machine where patch daemon is installed.

HKEY_LOCAL_MACHINE\Software\Flexera

HKLM\SOFTWARE\Microsoft\EnterpriseCertificates\Disallowed

HKLM\SOFTWARE\Policies\Microsoft\SystemCertificates\Disallowed

HKLM\Software\Microsoft\SystemCertificates\Disallowed

HKLM\Software\Microsoft\Update Services\Server\Setup

b. Add permission to the below registries to your service account (test_user) in the WSUS machine.

HKLM\SOFTWARE\Classes\AppID

{8F5D3447-9CCE-455C-BAEF-55D42420143B}

You might have to take ownership of this key. A logged-in user, which is used to configure all permissions, needs full control of this key. This is required when configuring DCOM permissions. Settings for currently logged-in users can be changed back when all is completed.

c. Windows Explorer in test machine.

C:\ProgramData\Microsoft\Crypto

C:\ProgramData\Flexera Software\SVM Patch

d. Shares and groups

- The service user account needs to be added to WSUS administrators.
- WSUS administrators need to have full access to WSUS content location. Share and NTFS.

e. DCOM - Distributed Component Object Model in WSUS machine.

Open Dcomcnfg and go to Component Services > Computers > My Computer > DCOM Config, and modify WSUSCertServer security settings:

- Launch and Activation permissions - give Local Launch and Local Activation rights to WSUS administrators group/your service user
- Access permissions - give Local Access rights to WSUS administrators group/your service user.
- Reboot the machine, after changing DCOM settings.

3. Service Login and publishing.

a. Change logon user to the test_user and restart the service.

b. Once service restarted you can login to the test machine though your test user and publish patches.

Note • *test_user does not have a privilege to restart patch daemon service.*