# Flexera

# Software Vulnerability Manager 2018 (Cloud Edition) Quick Start Guide

# **Legal Information**

Book Name: Part Number: Software Vulnerability Manager 2018 (Cloud Edition) Quick Start Guide

SVM-2018-QSG02

**Product Release Date:** 

November 2018

### **Copyright Notice**

Copyright © 2018 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/producer/company/about/intellectual-property/. 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 2018 (Cloud Edition) Quick Start Guide	3
	Using Help	4
	Contact Us	5
2	Getting Started	7
_	System Dequirements	7
	Bermissione	
		8
	Software Vulnerability Manager 2018 with Scanning and Patching Capabilities	8
	Download and Install the Software Vulnerability Manager 2018 Internet Explorer Plug-in	9
	Download and Install the Software Vulnerability Manager 2018 Daemon	10
	Download and Install the System Center Plug-in	12
3	Scanning	13
	Remote Scanning Via Software Vulnerability Manager 2018 (Agent-less Scan)	13
	Ouick Scan.	14
	Scan Groups	
	Scanning Via Local Agents	15
	Agent-based Scan Requirements (Windows)	15
	Single Host Agents	10
	Download Local Agent	16
	Agent Denlovment	18
	Add Proxy Settings	19
	System Center Inventory Import	19
	System Center Import Schedules (Requires the Software Vulnerability Manager 2018 Daemon)	20
л	Penorting	72
1		23
	Report Configuration.	23

	Smart Group Notifications
5	Patching
	Patch Configuration
	WSUS/System Center
	Step 1 – Connection Status
	Step 2 - Certificate Status
	Step 3 – Group Policy Status
	Creating the WSUS-CSI GPO Manually
	Creating a Patch with the Flexera Software Package System (SPS)
	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
	Deploying the Update Package Using WSUS
	Deploying the Update Package Using System Center
A	Appendix A - Certificates
	WSUS Self-Signed Certificate (Microsoft)
	Using Your Own Certification Authority (CA) Certificate
	CA Verification and Validation

1

# Software Vulnerability Manager 2018 (Cloud Edition) Quick Start Guide

Flexera's Software Vulnerability Manager 2018 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 2018, 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 2018 integrates seamlessly with Microsoft<sup>®</sup> WSUS and System Center Configuration Manager.

Торіс	Content		
Getting Started	The following topics provide further information for getting started with Software Vulnerability Manager 2018:		
	System Requirements		
	• Permissions		
	• Software Vulnerability Manager 2018 with Scanning and Patching Capabilities		
	• Download and Install the Software Vulnerability Manager 2018 Internet Explorer Plug-in		
	• Download and Install the Software Vulnerability Manager 2018 Daemon		
	Download and Install the System Center Plug-in		

Table 1-1 • Software Vulnerability Manager 2018 (Cloud Edition) Quick Start Guide

Table 1-1 • Software Vulnerability	/ Manager 2018 (C	Cloud Edition)	Quick Start Guide	(cont.)
------------------------------------	-------------------	----------------	-------------------	---------

Торіс	Content
Scanning	This following topics describe the various Software Vulnerability Manager 2018 scanning methods:
	• Remote Scanning Via Software Vulnerability Manager 2018 (Agent-less Scan)
	Quick Scan
	Scan Groups
	Scanning Via Local Agents
	System Center Inventory Import
	• System Center Import Schedules (Requires the Software Vulnerability Manager 2018 Daemon)
Reporting	Software Vulnerability Manager 2018 includes a report function to document your scanning results.
	• To configure your reports and to schedule your report generation, see Report Configuration.
	• To create and configure reminders, notifications, and alerts for a Smart Group, see Smart Group Notifications.
Patching	The following topics describe how to configure and deploy Software Vulnerability Manager 2018's patching function.
	Patch Configuration
	Creating the WSUS-CSI GPO Manually
	• Creating a Patch with the Flexera Software Package System (SPS)
	Deploying the Update Package Using WSUS
	Deploying the Update Package Using System Center
Appendix A - Certificates	This appendix describes the types of certificates to obtain to deploy patches and how to verify and validate the certificate.
	• WSUS Self-Signed Certificate (Microsoft)
	Using Your Own Certification Authority (CA) Certificate
	CA Verification and Validation

### **Using Help**

Help is available from the Software Vulnerability Manager 2018 (Cloud Edition) interface help icon located at the top right of the screen or click the fields labeled with a "(?)" to access the contextual help.

### **Online Help**

For online help, see https://helpnet.flexerasoftware.com/csi/Default.htm

### **Release Notes**

For the latest product release notes, see https://helpnet.flexerasoftware.com/ ?product=Software%20Vulnerability%20Manager%202018%20Cloud%20Edition&version=2018

For earlier product release notes, see https://helpnet.flexerasoftware.com/ ?product=Software%20Vulnerability%20Manager%202018%20Cloud%20Edition&version=Previous

### **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: https://www.flexera.com/

### **Product Feedback**

Have a suggestion for how we can improve this product? Please come share direct feedback with the product team and vote on ideas submitted by other users in our online community at: Customer Community feedback page for Software Vulnerability Manager.

Chapter 1 Software Vulnerability Manager 2018 (Cloud Edition) Quick Start Guide Contact Us



# **Getting Started**

Flexera's Software Vulnerability Manager 2018 solution is accessible via https://csi7.secunia.com.

You will be prompted for authentication with your username/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 logon. The new password must contain a minimum of eight characters, or comply with the criteria defined in your custom Password Policy Configuration.

The following topics provide further information for getting started with Software Vulnerability Manager 2018:

- System Requirements
- Permissions
- Software Vulnerability Manager 2018 with Scanning and Patching Capabilities
- Download and Install the Software Vulnerability Manager 2018 Internet Explorer Plug-in
- Download and Install the Software Vulnerability Manager 2018 Daemon
- Download and Install the System Center Plug-in

### **System Requirements**

To use the Software Vulnerability Manager 2018 console, your system should meet the following requirements:

- Minimum resolution: 1280x1024
- Internet Explorer 11 or higher (Scan results can also be viewed from other browsers)
- Internet connection capable of connecting to https://csi7.secunia.com
- The following addresses should be white-listed in the Firewall/Proxy configuration:
  - crl.verisign.net
  - crl.thawte.com
  - http://crl3.digicert.com

- http://crl4.digicert.com
- http://\*.ws.symantec.com
- https://\*.secunia.com/
- http://\*.symcb.com
- http://\*.symcd.com
- First-Party cookie settings at least to Prompt (in Internet Explorer)
- Allow session cookies
- A PDF reader

### Permissions

- 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 2018 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 2018 with Scanning and Patching Capabilities

Task

To successfully scan and create updates, the following should also be present when using Software Vulnerability Manager 2018:

- Internet Explorer 11 or higher with Software Vulnerability Manager 2018 Plug-in installed (in order for Software Vulnerability Manager 2018 to connect to WSUS and to create packages successfully, IE must be run as administrator in most cases. Right-click and select **Run as administrator**).
- 2. In IE Tools > Internet options > Advanced, ensure Use TLS 1.1 and Use TLS 1.2 are selected.
- 3. WSUS Administration Console matching your WSUS server's version.
- 4. Visual C++ Redistributable for Visual Studio 2012.
- 5. Microsoft .NET Framework runtime 4 or later.
- 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.

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

¢

Task

- 1. On the Windows Server machine, from the Server Manager, go to Add Roles & Features > Features.
- 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 subfeatures listed underneath it (API and PowerShell cmdlets and User Interface Management Console).
- 9. Proceed to the end of the Add Roles and Features Wizard by clicking Next and then Install.
- 10. Restart Windows and launch Software Vulnerability Manager 2018 from a web browser (for example IE).

### Download and Install the Software Vulnerability Manager 2018 Internet Explorer Plug-in

The first time you log on to Software Vulnerability Manager 2018, click the link on the bottom of the page and follow the onscreen instructions to download and install the Software Vulnerability Manager 2018 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 2018 Plug-in is installed locally and must be installed on the machine you are running the Software Vulnerability Manager 2018 console from. Once the Software Vulnerability Manager 2018 Plug-in has been installed, the download link is removed from the page.

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

- Open Internet Explorer's Internet options
- Go to the Security tab
- Select Trusted Sites
- Add your server's IP or hostname to the Trusted Sites
- Go back to the Security tab and click Custom level
- 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 2018 Daemon

The Software Vulnerability Manager 2018 Daemon is a stand-alone executable that executes various schedules configured in the Software Vulnerability Manager 2018 console. It runs as a background service with no user interaction. You can download the Daemon from: https//secuniaresearch.flexerasoftware.com/support/download/

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 2018:

- Active Directory
- Microsoft<sup>®</sup> 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 2018'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.

**Important** • 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.

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 a log file written for scheduled CSV file output and log file creation
- Membership to the local WSUS group "WSUS Administrators"
- LDAP query privileges
- SQL DataReader privileges
- System Center Configuration Manager Read only Analyst privileges

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

- 1. Open the SQL Server Management Studio software at the SQL Server Host.
- 2. Expand the 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.

						-R - 870	Colored and an	12
						Script + 13 Help	A General	🚆 New Query 📑 📸 📸 📴 📓
•	— I			V SCCM12	Icen ep	C	Files	bject Explorer
				Y-SOUMIZ	leseau	Server name.	Filegroups	onnect 🕶 🛃 🜉 🔳 🍸 🛃 🍒
						View server permissions	Change Tracking	CSC-SRV-SCCM12 (SQL Server 10.50.3720 -
				2	CM_S12	Database name:	Permissions	🗄 🛅 Databases
	sh	Sear				Lisers or roles:	Extended Properties	🗄 🦲 System Databases
			Tun			Name	Mirroring	CM_512
		ч ч	Use				Transaction Log Shipping	III 🚞 Security
		4	Use	ccess	ConfidMar DViewA	CSC-SRV-SCCM12		Server Objects
		¥.	Use	E	NETWORK SERVICE	A NT AUTHORITY		E Management
		a .	A NT AUTHORITY\SYSTEM User			A NT AUTHORITYV		E B SQL Server Agent
		a.	SCDM\SCDM-SRV-SCCM\$ User					
	smsdbuser_ReadOnly User				Inly			
					Vrite			
		R	Use		Schema	smsdbuser_Report		
	-					1		
	Permissions for CSCVAllen:							
	20					Explicit Effective	Lonnection	
		Deny	With Grant	Grant	Grantor	Permission	Server: CSC-SBV-SCCM12	
					dbo	Connect replication	Compositor	
				2	dbo	Connect	Corriscoort	
	and the				dbo	Control	View connection properties	
					dbo	Create aggregate		
					dbo	Create assembly	Progress	
					dbo	Create asymmetric k	Beadu	
					dbo	Ureate certificate	Sal	
					dbo	Lieate contract		

### 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 2018 account and click Install.

**Important** • The Daemon executes scheduled tasks configured in Software Vulnerability Manager 2018. Therefore, the Software Vulnerability Manager 2018 user account used during the Daemon installation must be the same account which set up the scheduled tasks in Software Vulnerability Manager 2018. It can be a user account or an administrator account in Software Vulnerability Manager 2018.

- Enter the credentials for the user account (or service account) that was set up 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. For example, if the user sets the name to *all\_hosts.csv* in Software Vulnerability Manager 2018, then the resulting file will actually be named *all\_hosts\_2016-03-03\_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 will not 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 have not been specified when the Daemon has been run, then the Daemon will check again for the settings in 10 minutes and every 10 minutes afterwards until the Daemon receives the settings.

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. The results are displayed in Software Vulnerability Manager 2018's Completed Scans page.

Log on with your Software Vulnerability Manager 2018 Account credentials (User name/Password).

The machine should have access to https://\*.secunia.com.

### **Download and Install the 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 https://secuniaresearch.flexerasoftware.com/support/download/.

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

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



**Tip** • You can define the sorting of both lines and columns in any grid view to create the layout that best suits your needs. Click the right-hand side of any of the column headings to view the available display options. The column's position can be modified by dragging and dropping the selected column to the desired position.



*Tip* • You can click *Export* in any grid view to save the displayed information as a CSV file. You can configure the file by hiding columns in the grids prior to export.



This following topics describe the various Software Vulnerability Manager 2018 scanning methods:

- Remote Scanning Via Software Vulnerability Manager 2018 (Agent-less Scan)
- Quick Scan
- Scan Groups
- Scanning Via Local Agents
- System Center Inventory Import
- System Center Import Schedules (Requires the Software Vulnerability Manager 2018 Daemon)

### Remote Scanning Via Software Vulnerability Manager 2018 (Agent-less Scan)

These scans are performed in an Agent-less manner, and the credentials used by Software Vulnerability Manager 2018 to authenticate on the target hosts are the same as those of the user that launched the Software Vulnerability Manager 2018 console.



*Important* • Please consider the system requirements for the Scan Groups/Agent-less scans, described in Agent-based Scan Requirements (Windows).

### **Quick Scan**

Q

Use this page to conduct quick, on-demand, scans from your Software Vulnerability Manager 2018 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**.

Enter hosts to scan						
Scan Type						
	Type 2: All Paths (Recommended)					
	O Type 1: Default Paths					
10.0						
IP Kange						
From:	Enter IP address					
To:	Enter IP address					
- IP Addresses or Co	omputer names					
	Enter host names and ip addresses here					
	×					
-Scan this compute	Scan this computer (localhost)					
$\checkmark$ Include this computer in scan						
	Scan 1 Host					

So 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**.

Scan Groups						
Scan 1 selected group New Scan Group						
Scan Group 🔺						
	•					
ChrisTe	Edit Group Scan Group					
	Delete Group					

If you are scanning remote hosts, your current logon 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.

<ul> <li>Type 3: Inspect all .dll, .exe, and .ocx files (Slow)</li> <li>Type 2: All Paths (Recommended)</li> </ul>	Vame:
<ul> <li>Type 3: Inspect all .dll, .exe, and .ocx files (Slow)</li> <li>Type 2: All Paths (Recommended)</li> </ul>	Scan Type:
	۲
○ Type 1: Default Paths	0
2: Check for missing Microsoft security updates has been globally enabled by th strator.	Microsoft Update: Check partition administrator.
trator.	partition administrator.

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

### **Scanning Via Local Agents**

Software Vulnerability Manager 2018 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.



The following sections provide

more information for using an Agent-based deployment:

- Agent-based Scan Requirements (Windows)
- Single Host Agents
- Download Local Agent
- Agent Deployment

### Agent-based Scan Requirements (Windows)

The flexibility offered by Software Vulnerability Manager 2018 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 Agent-based Scan Requirements (Windows), the following requirements should be present in the target hosts:

- Administrative privileges (to install the Software Vulnerability Manager 2018 Agent csia.exe)
- Microsoft Windows XP, 2003, 2008, Vista, 7, 8, 10 or 2012
- Internet Connection SSL 443/TCP to https://\*.secunia.com/
- Windows Update Agent 2.0 or later

### **Single Host Agents**

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

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

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

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

You can also specify a Site name when installing the Agent by using the **-g** parameter or by specifying a site name in the additional parameters when creating the Agent deployment package described in Agent Deployment.

### **Download Local Agent**

Use this page to download the csia.exe file, as well as read an explanation on how to install the Agent in Single Host mode.

If your intention is to deploy the Software Vulnerability Manager 2018 Agent through the 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 2018 console under **Scanning > Scanning via Local Agents > Download Local Agent**.

Menu	« Download Local Agent
Dashboard	Single Host Mode
Common Scanning     Scanning Via Corporate Sof     Quick Scan     Scan Groups     Scan Progress     System Center Inventory Import     System Center Import Schedules	Recommended For Laptops and hosts that can not be scanned remotely, e.g. hosts that are not always o Example Install the Corporate Software Inspector Agent in Single Host mode on corporate lapt Software Inspector. Thus enabling you full control to scan and view results of hosts th Result Hosts scanned in Single Host mode will show in the Results Database similar to all oth
Remote Scanning Via Agents Network Appliance Agents Network Appliance Groups Download Network Agent	Instructions 1. Download the Corporate Software Inspector Agent. 2. Transfer the Agent to the host where it should be installed. 3. Login to the host and install the agent. For help, press F1.
Scanning Via Local Agents     Single Host Agents     Download Local Agent	Cornerate Software Inspector Agent Downloads Microsoft Windows (ver. 7.6.0.1) [?]
<ul> <li>P51 For Windows</li> <li>Filter Scan Results</li> <li>Scan Paths (0)</li> <li>Custom Scan Rules</li> <li>Completed Scans</li> </ul>	Red Hat Linux 7.x (ver. 7.6.0.1) (?) Red Hat Linux 7.x (ver. 7.6.0.1) (?) Email Corporate Software Inspector Agent details Email agent details.

🕿 csia.exe Properties X							
General Compa	atibility Security Details Previous Versions						
()	csia.exe	]					
Type of file:	Application (.exe)						
Description:	Flexera Software Corporate Software Inspector Agent						
Location:	C:\Users\MKoppen\Downloads						
Size:	894 KB (915.968 bytes)						
Size on disk:	896 KB (917.504 bytes)						
Created:	Today, November 27, 2017, 1 minute ago						
Modified:	Today, November 27, 2017, 1 minute ago						
Accessed:	oday, November 27, 2017, 1 minute ago						
Attributes:	Read-only Hidden Advanced						
Security:	This file came from another computer Unblock and might be blocked to help protect Unblock this computer.						
	OK Cancel Apply						

**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 2018 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 2018 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 the Local Admin account using:

csia.exe -i -L

Example of an installation:

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

By using the **-L** parameter, the Agent will be installed as a service running under the LocalService user account. For further information, refer to: http://msdn.microsoft.com/en-us/library/windows/desktop/ms684190%28v=vs.85%29.aspx

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

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

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



**Important** • The csia.exe file is a customized executable, unique and private for your Software Vulnerability Manager 2018 account. This means that the csia.exe automatically links all scan results to your Software Vulnerability Manager 2018 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**.

### **Agent Deployment**

If you choose to scan the target host by using the Software Vulnerability Manager 2018 Agent in Single Host mode (recommended), you can easily distribute and install the Agent by deploying it through the WSUS/System Center.

Click **Create CSI Agent Package** under **Agent Deployment** to start the Software Vulnerability Manager 2018 Agent Package wizard.

Agent Deployment					
Agent Summary					
Below is a summary of the Software Vulnerabity Manager Agents currently installed in the network. NOTE: The statistics are based on scan results thus may be out of synchronisation with your WSUS/System Center server if a scan has not been recently performed.					
Overall Agent Statistics					
Total Number of Hosts:	65				
Number of Hosts with an Agent Installed:	36				
Number of Hosts without an Agent Installed:	29				
Version Statistics for Installed Agents					
Hosts with the Newest Agent Installed (≥ 7.6.0.2) :	2				
Hosts with an Older Agent Installed (≥ 7.0.0.0 and < 7.6.0.2) :	34				
Hosts with an Outdated Agent Installed (< 7.0.0.0): 0					
Deploy the Software Vulnerablity Manager Agent through	your Microsoft WSUS/System Center Server				
Click "Create Software Vulnerability Manager Agent Package" to start the Software Vulnerability Manager Agent Package wizard.					
Create Software Vulnerability Manager Agent Package					

The Software Vulnerability Manager 2018 Agent Package can be created and managed just like any other SPS package. For example, you can Add Proxy Settings.

### **Add Proxy Settings**

You can add proxy settings to the installation script in the SPS wizard when creating the Agent deployment package. In **Step 2 of 4: Package Contents**, modify the variables in the Execution Flow field.

and script typ JScript (Javas	e for this SPS package.		
JScript (Javas	(and )		
	chipo -		-
// The fol	lowing variables can be optionally mo cordingly dername = ""; // NOTE: If prosydaerns ame and runAsPagsword as well assword = ""; // NOTE: If prosydaerns	odified and will be me to entered you must enter	
runAsUsern Var proxyH Mar proxyF Var runAsD Var runAsD Var siteNa	ame and runAsPassword as well lost = ""; ort = ""; sername = ""; // If a domain is used assword = ""; me = "";	please use: user@domain	
function m	ain() ( : ( :GUID ) ( 	oplied for package " + Title );	
in this packag of URLs) or if how Localised	n. The grid below shows the files that are currently sch they are local files. You can add additional files via the Files' button. To remove a files, right-click and select 's	vestuled to be included, and if they will be downloaded 'Add File' button, as well as choose from additional la Remove'.	nguage
kage		Status	
GoogleChrome	_66.0.3359.139_64-bit_5P5.exe	To Be Dynamically Downloaded	
wnload Link	Add Localisation (Language) File		
creating an SPT	i File from this package, should you wish to.		
	In this packag of URLa) or function at function at function at function at at function at at function at the packag of URLa) or func- tion at function at the function at the function	$\begin{array}{c} The set of th$	$ \begin{array}{c} & The product of the second second$

### **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 2018 Agent on each client.

System Center integration requires the following prerequisites:

- Setting up authentication. The user running the Software Vulnerability Manager 2018 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.
- 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 2018 System Center Configuration page, enter the **System Center Server Name** and click **Save**.

System Center SQL Da	tabase Settings	
Choose automatic to get manual option.	he SQL connection data from System Center server or specify	your own connection data with
	<ul> <li>Automatic</li> </ul>	
System Center Server N	ame:	
	O Manual	
System Center Import	Settings	
Choose whether or not to mported hosts.	automatically create a Site name from the System Center Col	lection Name and assign it to
$\checkmark$	Jse System Center Collection Name as Site name for imported	hosts

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.

Software Vulnerablity Manager	System Center Configuration	×
System Center SQL Databas	se Settings	
Choose automatic to get the SQ manual option.	L connection data from System Center server or specify your own connection data with	
	O Automatic	
	Manual	
SQL Host:		
SQL Port:	1433	
SQL Database:	CM_IND	
System Center Import Setti Choose whether or not to autor imported hosts.	ings natically create a Site name from the System Center Collection Name and assign it to ystem Center Collection Name as Site name for imported hosts	
	Save	

### Ì

**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 2018 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 2018 Daemon)

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.

Define the schedule for importing System Center scan data. After the schedule has been created you will be prompted to add the collection whose scan data you want imported.
Schedule Name:
Next Run: 2018-01-17 3 05 C : 30 C Date and Time in the future.
Frequency: Hourly or One-Time Import
Save Close

Click Add Collections and enter the Collections to include in the Import Schedule.

Right-click an Import Schedule in the grid to edit or delete the schedule.

# **4** Reporting

Software Vulnerability Manager 2018 includes a report function to document your scanning results.

- To configure your reports and to schedule your report generation, see Report Configuration.
- To create and configure reminders, notifications, and alerts for a Smart Group, see Smart Group Notifications.

### **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 2018 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.

Report	Format		
Specif	y the format for the report		
	PDF	~	

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

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

3. Choose between a One-time only report or a recurring one (daily, weekly, monthly).



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

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

5. Choose a dashboard profile to be included in the report.

Dashboard Profiles			
Specify the dashboard profile to be included in the report.	Select dashboard profile	~	
			Reset

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

Site Level Statistics	
Select Sites	
Specify the sites whose data will be used for the report.	
<ul> <li>All sites for all selected users.</li> </ul>	
Use a custom selected group of sites.	
Use a custom selected group of host-smart groups.	
	Select Sites Select Host Smart Group
Using data from all sites for users selected above (default).	
Site Level Statistics to Include	
Specify the site-level statistics that will be included in the report. If none of the statistics is selected, this section will n	ot be included into the report.
Overall Summary Statistics	
Overall Criticality Statistics	
Overall Impact Statistics	
Overall Attack Vector Statistics	
By-Site Statistics on Patched Products	
By-Site Statistics on End-of-Life Products	
Include Detailed Site Specific Data for Each Site	

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

Host Level Statistics	
Specify the hosts whose data will be used for the report by selecting a smartgroup.	
All Hosts	
Specify the statistics that will be included for each selected host in the report.	
Overall Summary Statistics	
Insecure Installation Details	
Additional filter: Only include insecure installations with a rating of: Show All 🗸 or Above.	
End-of-Life Installation Details	
Patched Installation Details	

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

Product Level Statistics	
Specify the products whose data will be used for the report by selecting a smartgroup.	
All Products	
Specify the statistics that will be included for each selected product in the report.	
Overall Summary Statistics	
✓ Insecure Installation Details & Recommended Solutions	
Additional filter: Only include details and solutions for insecure installations with a rating of: Show All 💙 or Above.	
✓ End-of-Life Installation Details	
Patched Installation Details	

**9.** 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.

Search Sear	h Use default recipients defined in	Settings page:	
vailable Email Recipients			
		Selected Email F	Recipients
Name Email		Name	Email
user1	and the second se		

**10.** 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 .PDF format and will be emailed to the defined email addresses in accordance with the schedule and recurrence specified. Once generated, a report can also be downloaded directly from the main page.

General Configuration Opti	ons
Report File Name Here you can specify a custo Set the file name	m output file name for the generated report. : for the PDF report file generated.
PDF Filename:	test.pdf
Report Title Here you can specify a custo Set the report tit	im title for the front page of the report. Je.
Report Title:	Flexera Custom Report
Publish Report Parameter Here you can choose whether     Show Report Op	ars ar the report parameters (configured here) should be included in the report for reference. tions and Generation Parameters

Important • The emails containing the .PDF reports will be sent from the Flexera Data Cloud - no-

*reply@flexerasoftware.com.* Be aware that the email server from the recipient may block/filter the email. For example, the size of the attachment may exceed a certain pre-defined threshold. If no email is being received, please check the email Spam filter and/or the Junk folder in the email client.

## **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.

Name & Applicat ou must give this pply.	<b>ility</b> notification a name (or short de	sription) to be used when rece	iving alerts. Here you	will also select the Smart Group for wh	ich the notification will
lame: Enter a n	ame (or short description) for	r this notification	Smart A Group:	All Advisories (Advisory)	Y
Alerting Conditio	ns				
hoose the conditio	ns under which you will receive	an Alert.			
LERT me when the	e Number of Advisories	<ul> <li>Changes</li> </ul>	×	19-12	
aved/modified:					
aved/modified: NOTIFY me ( Recipients Select elect email recipie Search Available Email	email only) when the alert cond tion nts: Search Use default Recipients	ditions are NOT met. I.e., leave	unchecked for a 'no page:	news is good news' policy.	
Aved/modified:  NOTIFY me ( Recipients Select elect email recipie Search Available Email Name	email only) when the alert cond tion nts: Search Use default Recipients Email	ditions are NOT met. I.e., leave	unchecked for a 'no page: Selected Email Name	news is good news' policy. I Recipients Email	
aved/modified:  NOTIFY me ( Recipients Select elect email recipie Search Available Email Name user1	email only) when the alert cond tion nts: Search   Use default Recipients Email	ditions are NOT met. I.e., leave	a unchecked for a 'no page:	news is good news' policy. I Recipients Email	

# 5 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 2018's patching function.

- Patch Configuration
- Creating the WSUS-CSI GPO Manually
- Creating a Patch with the Flexera Software Package System (SPS)
- Deploying the Update Package Using WSUS
- Deploying the Update Package Using System Center

### **Patch Configuration**

Flexera's Software Vulnerability Manager 2018 can be integrated with Microsoft's WSUS/System Center.

### WSUS/System Center

Use this option to configure the integration of Software Vulnerability Manager 2018 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 2018 with WSUS.

After clicking **Configure Upstream Server**, a configuration wizard will be initiated.

nfigure W	5US Upstream Server
1. Click 2. The v Vulnera 3. In th 4. The ' 5. The '	"Configure Upstream Server" to configure the integration of the Software Vulnerablity Manager with your WSUS server. vizard guides you through three configuration steps: "Connection", "Certificate", and "Group Policy" all necessary to use the Software blity Manager with WSUS. e "Connection" window, please specify the server, port, and if you wish to use SSL to connect to your WSUS server. Configure Signing Certificate" window enables you to install, export, and import a signing certificate to your WSUS server. Group Policy" window allows you to configure the group policy options to be used with your WSUS server.
	Configure Upstream Server
nfigure W	5US Downstream Servers
1. Click 2. The v 3. In th 4. The '	"Configure Downstream Servers" to configure your WSUS Downstream servers. vizard guides you through two configuration steps: "Connection" and "Certificate". e "Connection" window, please specify the server, port, and if you wish to use SSL to connect to your WSUS Downstream server. 'Configure Signing Certificate" window enables you to import an existing signing certificate to your WSUS Downstream server.
	Configure Downstream Servers

Follow the wizard steps to successfully integrate Software Vulnerability Manager 2018 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**.

Connect to WSUS Serv	er			
WSUS Server Name:	wsus.domain.tld	×		
WSUS Server Port:	8530			
	Use SSL Connection			
Connect				
	a 100m			-
Step 1. Connection Stat				
				1
elow you can see the conn	ection status between the Software Vul	Inerablity Manager and your WSI	JS server.	<b>^</b>
elow you can see the conn onnection successfully esta	ection status between the Software Vul Iblished to psccm.sccm.test	Inerablity Manager and your WSI	JS server.	Ĺ
elow you can see the conn onnection successfully esta	ection status between the Software Vul Iblished to psccm.sccm.test	Inerablity Manager and your WSI	JS server.	
elow you can see the conn onnection successfully esta 5tep 2. Certificate Statu	ection status between the Software Vul Iblished to psccm.sccm.test	Inerablity Manager and your WSI	JS server.	G
elow you can see the conn onnection successfully esta Step 2. Certificate Statu Step 3. Group Policy Sta	ection status between the Software Vu iblished to psccm.sccm.test is itus	Inerablity Manager and your WSI	JS server.	

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 the WSUS/System Center, so the updates can be deployed as patches. In this step, Software Vulnerability Manager 2018 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 2018 (note that the certificate must also be installed on the system running the Software Vulnerability Manager 2018 console)

• Clients receiving the Update

The created certificate is required, and it will be used for all future publishing. Without the created certificate, 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.

Configure Signing Certificate		
Here you can create and install a WSUS Self-Signed Certificate in all appro certificate is required to create and install local packages. Without it, only installed.	priate certificate stores. A WSUS signing packages from Microsoft Update will be	
Click 'Automatically create and install certificate' to install the certificate in certificate will be installed on this system and on your WSUS server in the	the appropriate certificate stores. The following stores:	
1) "Trusted Root Certification Authorities" 2) "Trusted Publishers"		
Automatically create and install certificate		
Certificate Options		
The WSUS Self-Signed Certificate can be imported and exported. Please us	e the options below.	
If the WSUS Self-Signed Certificate exists you can export the certificate to certificate to a file.	a file. Click 'Export Certificate' to export	the
Export Signing Certificate		
Here you can import the WSUS Self-Signed Certificate. Click 'Import Certifi that this feature requires that you are connected to your WSUS server thro	cate' to import the certificate. Please be ough an SSL connection.	aware
Import Signing Certificate		
itep 1. Connection Status		
itep 2. Certificate Status		
itep 3. Group Policy Status		

*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 recreated 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 2018, 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 2018 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 2018 WSUS Group Policy for the first time, proceed by selecting all the options, and then click **Create Group Policy**.

Step 3. Software Vulnerablity Manager WSUS Configuration Wizard	×
Group Policy	
A Group Policy is required to distribute certificates and locally created packages. Please specify if you use System Cente or WSUS to distribute packages. To apply additional configuration options please goto "Group Policy Options".	er
• Use WSUS to distribute packages.	
<ul> <li>Use System Center to distribute packages.</li> </ul>	
Create Group Policy	
Group Policy Details	
Group Policy Options	
Step 1. Connection Status	
Step 2. Certificate Status	
Step 3. Group Policy Status	
Below you can see the status of the Software Vulnerablity Manager Group Policy.	
Group Policy could not be created - please check Flexera FAQ	
Previous Next Clos	e

**Important** • Besides distributing the certificate through the Software Vulnerability Manager 2018 WSUS GPO, it is also possible to provision certificate to the target computers by going to **Patching > WSUS/System Center > Deployment** and selecting the target hosts where the certificate is to be installed (CTRL+ mouse click for multiple selection). Then right-click and select **Verify and Install Certificate**.

## **Creating the WSUS-CSI GPO Manually**



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.

😥 Computer Configuration	Encrypting File System	
a 🧾 Policies	Cata Protection	
Software Settings	BitLocker Drive Encryption	
a 🚞 Windows Settings	BitLocker Drive Encryption Network Unlock	Certificate
Name Resolution Policy	Automatic Certificate Request Settings	
Scripts (Startup/Shutdown)	Trusted Root Certification Authorities	
Deployed Printers	Enterprise Trust	Import
Security Settings	Intermediate Certification Authorities	All Tasks 🕨
Account Policies	Trusted Publishers	
Local Policies	Untrusted Certificates	Refresh
Event Log	Trusted People	Help
Restricted Groups	Certificate Services Client - Certificate Enrol	Iment Policy
System Services	Certificate Path Validation Settings	interest oney
kegistry	Cartificate Cartinee Client Auto Forellares	
	THE REPORT OF THE SHOULD BE LINED TO A DUTY OF DUTY OF THE	
P Mine System	Sp Certificate Services Client - Auto-Enrollmen	
<ul> <li>Mired Network (IEEE 802.3) Policies</li> <li>Wired Network (IEEE 802.4) Policies</li> </ul>	gu Certificate Services Client - Auto-Enrollmen	n
<ul> <li>         PIE system     </li> <li>         Wired Network (IEEE 802.3) Policies     </li> <li>         Windows Firewall with Advanced Security (International Viet Advanced Security)     </li> </ul>	Certificate services Client - Auto-chrolimen	n
<ul> <li>         ine system         iiii Wired Network (IEEE 802.3) Policies         iiiiiiiiiiiiiiiiiiiiiiiiiiiii</li></ul>	Gu Certuricate Services Client - Auto-Enrollmen	n.
<ul> <li>A rie system</li> <li>Wired Network (IEEE 802.3) Policies</li> <li>Windows Firewall with Advanced Secureming</li> <li>Network List Manager Policies</li> <li>Wetwork Unit Manager Policies</li> <li>Wetwork Policies</li> </ul>	Certricate services Client - Auto-Enrolimen	n.
P a rie system     Wired Network (IEEE 802.3) Policies     Windows Firewall with Advanced Secur     Network List Manager Policies     Wireless Network (IEEE 802.11) Policies     D Public Key Policies     D Schware Retriction Policies	Wetrinicate services Client - Auto-Enfolimen	u
	ign/certificate services Client - Auto-Enfolimen	м
A rise system     A rise	(gyvennkae serves Lient - Auto-Entoimen	и
Partic system     Partic	igy-termcare services Cirent - Auto-Enrolimen	u.
P int system     P	(gyvennkar services Liient - Auto-Enrolimen	A
P inc system     P	igy-termcare services Cilent - Auto-Enrolimen	A
P      Pic system     Pic system     Pic wird Network (EEE 80.2.3) Policies     Windows Firewall with Advanced Secu     Network List Manager Policies     Pic Wirders Network (IEE 80.2.1) Policies     Pic Wirders Network (IEE 80.2.1) Policies     Pic Software Retriction Policies     Pic Software Retriction Policies     Pic Network Access Protection     Pic Advanced Audit Policies     Pic Warned Audit Policies     Pic W	(gyvennkar services Lient - Auto-Enrolimen	A
P      Pic system     Pic syste	(gyvennkar services Liient - Auto-Enrolimen	A
Partic system     Partic	(gyvennkar services Liient - Auto-Enrolimen	A
	(gyvennkar services Liient - Auto-Enrolimen	A

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

▲ Computer Configuration           ▲ Policies           ▶ Software Settings           ▲ Windows Settings           ▶ Delocies           > Scripts (Startup/Shutdown)           ▶ Delocies           > Scripts (Startup/Shutdown)           ▶ Delocies           > Account Policies           > Account Policies           > Excurty Settings           > Restricted Groups           > Restricted Groups           > System Services           > Wired Network (IEE 802.3) Policies           > Wired Network (IEE 802.3) Policies           > Wired Network (IEE 802.1) Policies           > Software Restriction Policies           > Wired Network (IEE 802.1) Policies           > Software Restriction Policies           > Software Restriction Policies           > Software Restriction Policies           > Software Restriction Policies           > By Policies Network (IEE 802.1) Policies           > Delik (Key Policies Network (IEE 802.1) Policies	Encrypting File System Data Protection Bitta Cote Drive Encryption Bitta Cote Drive Encryption Certificate Request Truster Root Certification Aut Enterprise Trust Intermediate Certification Aut Truster Poblichers Untrusted Certificates Truster Rook Services Client Certificate Path Validation Certificate Services Client	twork Unlock Cetifica I Settings thorities Import All Tasks • Refresh Help	licy
P     Peterone     Perferences     Perferences     Perferences     Perferences     Perferences     Perferences     Perferences     Perferences     Perferences			

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

Second Se	Windows Undate			
a 🤗 Policies	windows opuate			
Software Settings	Select an item to view its description.	Setting	State	Commer
Windows Settings		E Do not display 'Install Updates and Shut Down' option in Sh	Not configured	No
Administrative Templates: Policy definition		Do not adjust default option to 'Install Updates and Shut Do	Not configured	No
Control Panel		Enabling Windows Update Power Management to automati	Not configured	No
Network		Always automatically restart at the scheduled time	Not configured	No
Printers		Configure Automatic Updates	Not configured	No
p System		Specify intranet Microsoft update service location	Enabled	No
Active Directory Federation Services		Automatic Updates detection frequency	Not configured	No
Active Unctaller Service		Allow non-administrators to receive update notifications	Not configured	No
Add features to Windows 8		Turn on Software Notifications	Not configured	No
App Package Deployment		Allow Automatic Updates immediate installation	Not configured	No
App runtime		Turn on recommended updates via Automatic Updates	Not configured	No
Application Compatibility		No auto-restart with logged on users for scheduled automat	Not configured	No
AutoPlay Policies		Re-prompt for restart with scheduled installations	Not configured	No
Backup		Delay Restart for scheduled installations	Not configured	No
Biometrics		Reschedule Automatic Updates scheduled installations	Not configured	No
BitLocker Drive Encryption		Enable client-side targeting	Not configured	No
Credential User Interface		Allow signed updates from an intranet Microsoft update ser	Enabled	No
Desktop Gadgets =				
Desktop Window Manager				
Device and Driver Compatibility				
Digital Locker				
Event Forwarding				
Event Log Service				
Event Viewer				
Family Safety				
File Explorer				
File History				
Game Explorer				
interest Evaluation				
p internet information Services				
Windows Undate				

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

Allow signed upo	lates from an intranet Microsoft update service location 📃 🗖	x
Allow signed updates from an intra	net Microsoft update service location Previous Setting Next Setting	
O Not Configured Comment:		^
Enabled		
Disabled		v
Supported on:	At least Windows Server 2003 operating systems or Windows XP Professional with SP1 excluding Windows RT	^
	Si i, cedalig vindovs ki	~
ptions:	Help:	
	when the undate is found on an intranet Microsoft undate	

**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.

🗈 Specify intranet Microsoft update serv	ice location	Enabled	No	
5 Spec	fy intranet Micros	soft update service loca	ation 📃 🗖	x t
Specify intranet Microsoft update s	ervice location	Previous Setting	Next Setting	
O Not Configured Comment:				^
Enabled				
O Disabled				~
Supported on:	At least Windows XI excluding Windows	P Professional Service Pack 1 RT	or Windows 2000 Service Pac	:k 3, ^ ~
Options:	He	lp:		
Set the intranet update service for dete updates:	ting Sp Up	ecifies an intranet server to l date. You can then use this date computers on your net	nost updates from Microsoft update service to automatical twork.	lly ^
http://my-wsus:80	Th	is setting lets you specify a :	server on your network to fun	ction
Set the intranet statistics server:	35	an internal update service. T arch this service for updates	he Automatic Updates client	will
http://my-wsus:80	уо	ur network.		=
(example: http://lntranetUpd01)	To see do wo sat	use this setting, you must s rver from which the Automa wnloads updates, and the si orkstations upload statistics. me server.	et two servername values: the tic Updates client detects and erver to which updated You can set both values to be	e the
	lf t co ins up ori an	the status is set to Enabled, t nnects to the specified intra stead of Windows Update, to dates. Enabling this setting i ganization don't have to go d it gives you the opportuni	he Automatic Updates client net Microsoft update service, search for and download means that end users in your through a firewall to get upda ty to test updates before depl	ates, oying ~
		C	)K Cancel A	apply

**10.** Link the created GPO to an Active Directory container appropriate for your environment.

<b>20</b>	Administrator: Command Prompt	-	x	
c:∖>gpupdate /force Updating policy				^ =
Computer Policy update User Policy update has	has completed successfully. completed successfully.			

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.

For further information on how to configure Automatic Updates by Using Group Policy, see http://technet.microsoft.com/ en-us/library/cc720539(WS.10).aspx.

### Creating a Patch with the Flexera Software Package System (SPS)

The Flexera Software 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 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

Some products are presented in gray because the vendor of the product does not provide silent installation parameters. If you choose to patch one of these products, you must provide (import) the **.MSI/.MSP/.EXE** file together with the parameters for the unattended installation. Software Vulnerability Manager 2018 will then repackage and publish the update through the standard workflow. Packages cannot be automatically created by Software Vulnerability Manager 2018 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 2018, you are able to create three different kinds of packages. Right-click a product and select one of the available options:

- Create Update Package
- Create Uninstall Package
- Create 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

### 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.

	and publishing the package, or exporting it as an XML formatted file.
Import XML (Optional)	
You can start by importing and/or edit.	an existing SPS Package File. This will populate all of the wizard data fields with the package data, which you can then view
NOTE: You should only imp	ort packages if you trust the author of the package and the source from where you downloaded / retrieved the SPS package.
Package Name	
The package will be create	d with the following name. Choose a new name if desired.
Name:	Update Google Chrome, version 66.x, Moderately Critical
Description (Optional)	
Here you can give a descrip	ption of the package. For example, what it does, the contents, usage, etc.
Description:	
Reference Id (Optional)	
Reference Id (Optional) Here you can assign an Id	a this package if desired.
Reference Id (Optional) Here you can assign an Id Reference Id:	l to blis package if desired.
Reference Id (Optional) Here you can assign an Id Reference Id: SPS Installer Paramete Here you can configure opt	i to this package if desired. (Optional) onal parameters you want to pass to the installer. This set of options is unique to this product. Some parameters have warning ould be read and understoo before moving forward
Reference Id (Optional) Here you can assign an Id Reference Id: SPS Installer Paramete Here you can configure opt message assided that si Configure Package Configure Package	In this package if desired.  In this package
Reference Id (Optional) Here you can assign an Id Reference Id: SPS Installer Paramete Here you can configure opt message associated that si Configure Package Behavior:	I to this package if desired.  (c) (c) (c) (c) (c) (c) (c) (c) (c) (c
Reference Id (Optional) Reference Id SPS Installer Parket Here you can configure opt message associated that at Behavior:	In this package if desired. Tra (Optional) Insult parameters you want to pass to the installer. This set of options is unique to this product. Some parameters have warning add be read and understood before moving forward Obtable (f) Deableb checking for maning Chrome processes (f) Deableb checking for maning Chrome processes (f)
Reference Id (Optional) Here you can assign an Id Reference Id: SPS Installer Paramete Here you can configure Package Configure Package Behavior: Select Installer:	In this package if desired. In
Reference Id (Optional) Here you can assign an Id Reference Id: SPS Installer Parameter Select Installer: Select Installer:	I to this package if desired.  ( (Optional)) ( initial Stable version ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (
Reference Id (Optional) Friee you can assign an Id Reference Id: SPS Installer Paramete Selection and Selection Configure Package Behavior Select Installer:	In this package if desired. In
Reference Id (Optional) Here you can assign an Id Reference Id: SPS Installer Parameter Select Installer and Configure Package Configure Package Configure Package Select Installer: Select Installer:	to this package if desired.
Reference Id (Optional) Free you can assign an Id Reference Id: SPS Installer Paramete SPS Installer Paramete Configure Package Configure Package Behavior Select Installer: Edit Package Context (I If you choose to edit the pa directed immediately to Ste	To this package if desired.  To Optional)  To Optional  To Total  Tota  Total  Total  Total  Total  Total  Total  Total  T

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.

	3 8							
Step 1 of 4: Package Configuration		_						
Use this form to set the name and description of the SPS package, or edit the properties of an existing one. In the following steps you will configure the package conte	ents							
and parameters before creating and publishing the package, or exporting it as an XPIC formatted me.		m Package fWS						
		shitestore	FAID	Contraction	Datasted	Taxastura	End Of Life	Databased
Import XFL (Optional)	~	crittecture.	- SALD	Chucanty	Detected	Ansecore	Chu-ch-che	Patenteu
You can start by importing an existing SPS Package File. This will populate all of the wizard data fields with the package data, which you can then view and/or edit.	÷.	indows64-bit	5402039		6 days ago	2	2	0
Note: We should also be address of the address of the analysis and the second data and the second data ( address of the second second data)		indows32-bit		CONTRACTOR OF TAXABLE	21 days ago	0	1	0
NOTET fou should only import packages if you dust the author of the package and the source from where you downloaded / reviewed the ses package.		ndows64-hit		-	6 days ago	0	î	0
Import XML		ndows32-bit			6 days ago	1	0	0
Package Name		6			Choose File to	Unload		×
The package will be created with the following name. Choose a new name if desired.		00		Documents a	Mr SDS Templates		Search Mr. SDS Temp	ater 0
Name: Update Google Chrome, version 66.x, Moderately Critical		00	1 1	bocumenta y	wy 5F5 Templates	÷ 0	Search my 5+5 Temp	ites p
		Organize ·	<ul> <li>New f</li> </ul>	older			8== -	· 🔟 🐵
Description (Optional)		- Envori	ter	Name	·	Date modified	Type	Size
Here you can give a description of the package. For example, what it does, the contents, usage, etc.				(1) pack	age_content_chrome	3/15/2018 2:44	AM XML Document	1 1
Description:		🛤 This P	C					
		🗣 Netwo	ərk					
Reference Id (Optional) Here vou can assion an Id to this package if desired.								
Reference Id:				<				
SPS Installer Parameters (Optional)			Fi	le name: packa	ge_content_chrome	~	All Files (*.*)	~
Here you can configure optional parameters you want to pass to the installer. This set of options is unique to this product. Some parameters have warning message associated that should be read and understood before moving forward							Open	Cancel
Configure Package ( ) Default ( )								-
Behavior: O Disable checking for running Chrome processes (?)	-							
Presidence   Newt   Dublich   Com	Isso							

In Step 4 of 4: Applicability Criteria - Rules, 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 of 4: Package Configuration. 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.



*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.

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.

View/Edit the execution fl	ow and script typ	e for this SF	'S package.			
Script Type	: JScript (Javas	script)	~			
Execution Flow	<pre>var Title var GUID = var silent var option // The fol // start c // var GUI // var GUI // var GUI // var GUI // var GUI // var opt var ret =</pre>	<pre>var Title = ""; var Otto for the second second</pre>				
	function m	main() ( ! ( !GUII se re	) ( rrver.logMessage( "No GU eturn 1;	NID supplied for package " + Title );		
Files To Include						
Files To Include Configure the files to inclu dynamically (i.e., in the c packages available via the	ide in this packag ise of URLs) or if : 'Show Localised	e. The grid they are loo Files' butto	below shows the files that are curr al files. You can add additional file n. To remove a files, right-click and	rently scheduled to be included, and if they will be dow s via the 'Add File' button, as well as choose from add 1 select 'Remove'.	vnloaded itional language	
Files To Include Configure the files to inclu dynamically (i.e., in the c packages available via the File(s) to include in the p	ide in this packag ase of URLs) or if Show Localised backage	e. The grid they are loo Files' butto	below shows the files that are curr al files. You can add additional file b. To remove a files, right-click and	rently scheduled to be included, and if they will be dou s via the 'Add File' button, as well as choose from add select 'Remove'. Status To Be Desvericable Devel	vnloaded itional language	
Files To Include Configure the files to inclu dynamically (i.e., in the c packages available via the File(s) to include in the http://dl.secunia.com/Si Add Local File Add	ide in this packag ise of URLs) or if 'Show Localised backage IS/GoogleChrome Download Link	e. The grid they are loc Files' button 66.0.3359. Add Loca	below shows the files that are curr al files. You can add additional file h. To remove a files, right-click and 139_64-bit_SPS.exe alisation (Language). File	rently scheduled to be included, and if they will be dos s via the 'Add File' button, as well as choose from add I select' Remove'. Status To Be Dynamically Down	vnloaded litional language loaded	
Files To Include Configure the files to inclu dynamically (i.e., in the cc. packages available via thu File(s) to include in the j http://dl.secunia.com/Sil Add Local File Add Create SPS File	ide in this packag ase of URLs) or if 'Show Localised backage 'S/GoogleChrome Download Link	e. The grid they are loc Files' button 	below shows the files that are curr al files. You can add additional file . To remove a files, right-click and 139_64-bit_SPS.exe alisation (Language) File	rently scheduled to be included, and if they will be dou a via the 'Add File' button, as well as choose from add select Remove'. Status To Be Dynamically Down	vnloaded litional language loaded	
Files To Include Configure the files to incl dynamically (i.e., in the co- packages available via this File(s) to include in the j http://dl.secunia.com/SI Add Local File. Add Create SPS File You also have the option	ide in this packag ase of URLs) or if 'Show Localised backage 'S/GoogleChrome Download Link Download Link	e. The grid they are loo Files' button 66.0.3359 Add Loca S File from t	below shows the files that are curr al files. You can add additional file h. To remove a files, right-click and 139_64-bit_SPS.exe alisation (Language) File his package, should you wish to.	rently scheduled to be included, and if they will be dos s via the 'Add File' button, as well as choose from add select 'Remove'. Status To Be Dynamically Downi	vnloaded litional language loaded	
Files To Include Configure the files to incl dynamically (i.e., in the c packages available via th File(s) to include in the http://dl.secunia.com/Sf Add Local File You also have the option Create SPS File	ide in this packag see of URLs) or if 'Show Localised backage Download Link Download Link	e. The grid they are loc Files' button (	below shows the files that are curr al files. You can add additional file n. To renewe a files, right-click and 139_64-bit_SPS.exe Ilisation (Language) File his package, should you wish to.	rently scheduled to be included, and if they will be dos e via the 'Add File' button, as well as choose from add select 'Remove'. Status To Be Dynamically Down	vnloaded litional language loaded	

### 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 2018 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.

you can define the lect paths in the gric advanced options in	sath-based applicability rules for this package. Below you will find any relevant paths a or add paths as needed via the "Add Path" button. Check the "Advanced Options" box the grid. Show Advanced Options	ready found or configured for the package. You can to enable additional options in the "Add Path" dialog
Add Path		
Always Install Op The purpose of this "isInstallable" WSU something is alread	tion option is to allow installations of new software. For custom packages which are not up rule which will ignore all system paths when deciding if this package can be applied. I installed, or is supereded by a more recent version.	dates to existing installations, you can bypass the lote - this will not bypass the rules for checking if
-	Mark Package as "Always Installable"	
Minimum Versior The purpose of this can alter this behav arbitrary values her	Mark Package as "Always Installable"      Option      options      automatic products a products of the products of the product to the     option so by specifying a custom minimum version. Note: the version you enter must also be	secure version within the same major version. You supported by the installer itself - you cannot enter
Minimum Versior The purpose of this can alter this behav arbitrary values her Minimum Version:	Mark Package as "Always Installable"      Option     option is to allow for updating of older products. Normally one updates a product to its     product in the version you enter must also be     55.0.0.0	secure version within the same major version. You supported by the installer itself - you cannot enter
Minimum Version The purpose of this can alter this behave arbitrary values her Minimum Version:	Mark Package as "Always Installable"      Option      Option      Allow for updating of older products. Itemaily one updates a product to ite      for updating of older products. Note: the version you enter must also be      So.0.0	seture vestion while the same major version. You supported by the installer itself - you cannot enter
Minimum Versior The purpose of this can alter this behav arbitrary values Minimum Version: Path *	Mark Package as "Always Installable"      Option     option to allow for updating of older products. Normally one updates a product to it     option is to allow for updating of older products. Note: the version you enter must also be     55.0.0.0	secure version within the same major version. You supported by the installer itself - you cannot enter information

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.

### 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 2018 console. Once this is completed, the Software Vulnerability Manager 2018 console will repackage and publish the update package into the WSUS/System Center.

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

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

System Applicability		
Configure the system type	(s) the package will be applied to.	
Apply Package To:	🔘 32-bit Systems Only	
	64-bit Systems Only	
	Both 32-bit and 64-bit Systems	
Special Rule		
The following special rule i	s available to configure:	
	Reboot is required after package has been installed.	
Language Settings		
Configure package applicat	bility rules based on language:	
	Only make package applicable to computers with one of the selected languages.	
Select Languages:	Language	
	Arabic	
	Chinese (Hong Kong SAR)	^
	Chinese - (Simplified)	
	Chinese - (Traditional)	
	Czech	~
	Danich	
Export Patch Script		
Before publishing XML pate example via the communit contain private user data.	h script to your file system, you have the option to configure XML file. Note: As you might wish to share this package, for y forum, you can choose to not include the package files as binary and the applicability paths from Step 3, as your paths may	60
	Do not include Step 3 Applicability Paths in XML File.	
	Do not include package file(s) as binary in XML File.	
Patch Template (Option	nal)	
Save as template		
Template Name:	Enter Template Name	
Publish Options		
elect option for publishing	J Flexera package	
	WSUS	
Publish package using:		
Publish package using:	() Altiris	
Publish package using:	Altiris     Export Patch Script	

If a reboot is required after the package has been installed, this option 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.

## **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 2018 will be available in your System Center.



# **Appendix A - Certificates**

This appendix describes the types of certificates to obtain to deploy patches and how to verify and validate the certificate.

- WSUS Self-Signed Certificate (Microsoft)
- Using Your Own Certification Authority (CA) Certificate
- CA Verification and Validation

### WSUS Self-Signed Certificate (Microsoft)

A code-signing certificate is needed to publish third-party updates to the WSUS/System Center, so the updates can be deployed as patches. Therefore, the Microsoft WSUS creates its own certificate named WSUS Self-Signed Certificate.

The WSUS Self-Signed Certificate must be installed/provisioned in the following systems:

- WSUS Server: Trusted Root Certification Authorities, Trusted Publishers, WSUS certificate stores
- The system running Software Vulnerability Manager 2018 (note that the certificate must also be installed on the system running the Software Vulnerability Manager 2018 console): Trusted Root Certification Authorities, Trusted Publishers
- Clients receiving the Update: Trusted Root Certification Authorities, Trusted Publishers (both distributed by GPO)



*Important* • To import your own certificate through Software Vulnerability Manager 2018, the WSUS connection must be configured to accept an SSL connection.

### Using Your Own Certification Authority (CA) Certificate

- If you would like to use a signing certificate to sign the updates created by Software Vulnerability Manager 2018, it must be a PKCS #12 format and have the private key included if not already present on your WSUS.
- Generally speaking, the certificate should match the requirements of Microsoft System Update Publisher (SCUP). Click here for more details.
- A Group Policy or a deployment package can be used to distribute certificates for locally created packages. In addition to the root certificate or the public signing certificate in Trusted Root Certification Authorities, the public code signing certificate has to be deployed to the Trusted Publishers folder.
- Furthermore, it is necessary to allow signed packages on target computers in Windows Update settings ("Computer Settings/Policies/Administrative Templates/Windows Components/Windows Updates").

### **CA Verification and Validation**

Each publicly available program must be signed with a signing certificate that proves the identity and integrity of the application.

When enabled, the Check for Publisher Certificate Revocation security feature forces Internet Explorer to verify and validate the Certification Authority (CA) that issued the signing certificate used for signing Software Vulnerability Manager 2018. This feature also verifies whether Software Vulnerability Manager 2018's code-signing certificate was previously revoked or not. Internet Explorer will then attempt to connect to crl.verisign.net to verify the CA issuer or to crl.thawte.com to verify the Software Vulnerability Manager 2018's SSL certificate.

In corporate environments, where advanced Firewall setups or Proxy Servers are used to authenticate and strictly control all inbound/outbound connections, this security feature may cause a potential problem for Software Vulnerability Manager 2018 users.

If the addresses crl.verisign.net, crl.thawte.com and \*.ws.symantec.com are not white-listed in the Firewall/Proxy server configuration, the CA validation check may not succeed. Additionally, Software Vulnerability Manager 2018, and its scanning Agent respectively, will be denied access to system and online resources causing them to fail to start.

White-listed in the Firewall/Proxy server configuration:

- crl.verisign.net
- crl.thawte.com
- \*.ws.symantec.com